The Africa Governance Papers

Volume 1 | Issue 4 | October 2023

RESEARCH ARTICLE

Navigating digital sovereignty in Africa: A review of key challenges and constraints

TYLER VENSKE

Abstract

This paper examines the evolving global digital landscape from an African perspective. To do this, the paper problematises the concept of "digital sovereignty" in the African context by exploring the continent's unique challenges. While investments by the United States (US) and particularly China in digital infrastructure projects have increased connectivity and improved lives, they raise ongoing concerns about Africa's over-reliance on external partners and the implications of data exploitation and surveillance for the continent's digital independence. Growing out of these concerns, the central argument of this paper is the need to delink African nation-states from foreign influence and control of the digital sector and to rearticulate or reframe the latter in terms of digital sovereignty. In this light, the paper contends that mainstream research on the Fourth Industrial Revolution in the African context does not sufficiently look past the power repertoires and dynamics of the US and China – whether blaming or crediting - when theorising digital sovereignty. Instead, the paper argues that to fully understand the African continent's battle to establish and maintain a coherent framework for digital independence, it is essential to consider the challenges and constraints of digital sovereignty. Drawing on a review of extant literature, the paper springboards off a set of broad themes and case studies to deepen understanding and highlight key hurdles to Africa's digital independence. The paper suggests that African nations must strive to overcome risks to digital sovereignty if the latter is to genuinely empower nation-states and citizens in the Fourth Industrial Revolution.

Keywords: digital sovereignty, internet governance, data security, China-Africa relations, US-Africa relations, US-China relations, telecommunications, data privacy, global digital economy, cybersecurity, global digital economy, Information Communication Technologies (ICTs), data centres, international relations, African governance

Introduction

This paper is situated within broader political economy and governance concerns, which take as their starting point a digital sovereignty perspective to unpack US and Chinese investments in Africa's digital landscape and address their implications for the continent. In this light, establishing and maintaining a coherent regulatory, governance and economic framework for digital sovereignty has become a central concern of African nations.

This overarching strategic and policy imperative is no more apparent than from Africa's growing

infrastructural and financial dependence on Chinese and American technology systems, which have profoundly mapped the trajectory of technological sovereignty in the continent in recent years.

The most obvious manifestation of the problem is a small number of Tech conglomerates, including Google, Meta, Amazon, Twitter, Huawei, ZTE, Tencent, Alibaba, Baidu, China Telecom, and China Mobile, that collectively command over 90% of revenue and profits in the African market, underscoring glaring disparities and inequities inherent in the global digital landscape (Blakeley, 2021). Given such data, creative remedies towards digital independence have become a priority for African policymakers in recent years. Even while the African digital landscape has expanded, the African Union (AU) has rightly been concerned about stubbornly high levels of concentration and control by Chinese tech giants within digital industries and markets. Anwar & Graham (2020) report that technological foreign investments have rapidly diffused economic activities across the continent. Drawing on data from Insight2impact, the authors found that an estimated 4.8 million African workers reported "having derived an income from digitally mediated or transacted internet platforms across seven of the eight countries for which survey data were available" (Anwar & Graham, 2020, p. 2).

However, while digital technologies are poised to reshape African economies and foster economic growth prospects, seeking technological assistance from the most appealing bidders has long-term repercussions for the continent's economic, political, and financial stability. The central argument within mainstream scholarship is that China's infrastructure investments have come at the cost of Africa's independence. While some see foreign digital investments as an answer to Africa's lag in the digital revolution, these investments are also symbolic of deteriorating digital trade balances and rising surveillance and control of African states and civil societies. Increasingly internationalised technology firms have maintained high profits. At the same time, substantial hurdles to digital sovereignty have weakened Africa's participation in the global digital value chain and made the continent susceptible to digital surveillance and control. The impact has been differentiated: on the one hand, countries with secure, self-regulated information and data systems are better positioned to safeguard their domestic environments (Hindman, 2018) while, on the other, failure to attain stability due to external intrusion within the jurisdiction of African nation-states is bound to impede digital sovereignty's realisation, undermining their capacity to protect and defend their territorial integrity and citizenry (Kwet, 2019).

The ongoing tension between infrastructure investment and the strategic imperative of digital sovereignty calls for renewed consideration of measures available to African governments to reduce dependence on foreign partners and strengthen the continent's control over the digital landscape. To confront these challenges, this paper contends that African nation-states must assert and retain digital control over their sovereignty. With a mere 1% of the world's data centres, many of which are foreign-owned, the paper argues that Africa needs to be equipped to store, process, and govern its data. Big Tech corporations harvest and exploit Africa's data, with limited returns for the continent (Truby, 2020). This predicament underscores the strategic imperative for active engagement by African nations in shaping crucial technological developments on the continent (Birhane, 2019).

Since we are concerned in this paper with harnessing the potential of the Fourth Industrial Revolution for the prosperity of Africa's population, the broad approach undertaken problematises digital sovereignty discourse through a critical exploration of the challenges facing African nations. Drawing on a review of extant literature, the paper springboards off a set of broad themes to deepen insight and highlight key hurdles and solutions to Africa's digital independence. The paper proceeds as follows: The ensuing section articulates the research approach undertaken in the paper. Section 2 puts the concept of digital sovereignty in a historical perspective by exploring the evolution of the models of

sovereignty and digital sovereignty and their contemporary relevance in global politics. In section 3, we focus on discussions from contextual data to problematise digital sovereignty as a critical concern in the 21st century in the African context. Section 4 then thematises the challenges and constraints emerging from the data to Africa's digital sovereignty. Section 5 discusses possible implications for policy and practice, while section 6 concludes.

Methodological considerations

An emerging scholarship on African digital sovereignty treats foreign digital infrastructure investments in the continent as both an opportunity and a challenge of digital transformation. While research on the subject illuminates the ongoing power dynamics shaping Africa's place in the evolving global digital landscape, this paper suggests that it is one aspect of a more complex, nuanced reality. Drawing on a review of literature, including Hendrickson & Zaki (2013), Phee (2021), Munga & Denwood (2022) and others, the paper brings the challenges to digital sovereignty in Africa into the foreground to illuminate the barriers to the continent's digital transformation. The broad approach undertaken in the paper is twofold. First, attempts were made to highlight connections between historical aspects related to the evolution of the digital landscape and the broad challenges of digital sovereignty. For such connections to become visible, it was necessary to reflect on the context in which technology is deployed, as powerful background imperatives influence its development and trajectory. In this way, the data provided a foundation for a thematic understanding of the evolution of Africa's digital landscape.

The identification of the following overarching themes guided the framing of the data and the analysis thereof:

- The global power dynamics of the US and China in shaping the African digital landscape;
- Infrastructure investment;
- Data security and privacy;
- African agency and independence;
- The legal and regulatory environment; and
- Capacity and education.

After that, the focus of the research shifted: each theme was unpacked to arrive at a set of constraints and inhibitors as a basis for remedial measures to take forward in policy discourse and future research. Collectively, these themes contributed to a richer analysis of the intricate relationship between sovereignty, digital transformation, and the global power dynamics that have come to shape Africa's place in the evolving digital landscape. Special attention was paid to aligning programmes and incentives to policies and initiatives, such as those by the African Union (AU) and individual African nations, emphasising the need for a coherent framework or digital sovereignty.

Historical contours of sovereignty

Sovereignty, derived from the Latin word superanus, is a multifaceted concept widely and diversely interpreted, classified, and applied in international discourse (Grimm, 2015). One of the foundational figures in developing sovereignty theory was Jean Bodin, a prominent French political philosopher and jurist whose influence was particularly significant during the sixteenth century.

Bodin's conception of sovereignty emphasised the capacity of the state to act independently, free

from external interference (Akinyetun, 2023). Over time, the notion has been instrumental in legitimising statehood and evolved to accommodate the ever-shifting political imperatives of nation-states. His ideas were instrumental in shaping the understanding of sovereignty as it would later be articulated. This notion was further solidified by the Treaty of Westphalia in 1648, defining sovereignty as the "unlimited and absolute power within the jurisdiction" (Zick, 2005, p. 231). It encapsulated the "whole body of rights and attributes that a state possesses in its territory, to the exclusion of all other states, and also its relations with [other states]" (International Court of Justice, 1949, pp. 39, 43).

These definitions have since become closely associated with state sovereignty, delineating how much a nation-state is endowed with power and authority within its territorial borders (Ziolkowska, 2021). As a result, the state emerged as a coherent and self-sufficient actor, possessing the capacity for autonomy, competence, and independence (Pohle & Thiel, 2020). In contemporary times, state sovereignty has functioned as a tool to justify state policies and actions, domestically and internationally. The eighteenth century witnessed a paradigm shift in the conceptualisation of sovereignty, attributable primarily to the Genevan philosopher Jean-Jacques Rousseau. In his influential work "The Social Contract," Rousseau advocated the idea of popular sovereignty, emphasising the primacy of the people over the ruling class, with the government serving as the elected representative of citizens (Akinyetun, 2023). This transformation required states to ensure that their citizens could exercise their inherent rights (McKay, 2023). Consequently, popular sovereignty recognises individuals as bearers of personal rights and gives them the authority to exercise agency (Coutre & Toupin, 2019).

The end of the Cold War in 1991 marked a pivotal juncture in the evolution of sovereignty, with the emergence of a new global order characterised by dominant Western values, particularly those of the US (Donnelly, 2014). As sovereignty transformed to align with this new international standard, so did international law constraining states' one-time absolute sovereign power. Instead, cooperation amongst governments was emphasised. Simultaneously, rights, protections, and attributes were allocated to the state's citizens (Deng, 2010). This shift in emphasis from state-centric sovereignty to the nation itself was aptly termed national sovereignty (Grimm, 2015). Consequently, sovereignty no longer primarily signified a state's independence in its relations with other states but became an overarching power encompassing all state authorities (Pohle & Thiel, 2020). This dramatic reorientation in the global power configuration brought significant changes in international norms. It addressed institutional, conceptual, and structural challenges while championing liberalism, democracy, and human rights as pivotal values (Cheney, 2019). Through these various conceptions, sovereignty has emerged as a deeply ingrained political concept, denoting the authority vested in a governing body to rule autonomously, free from external interference (Pohle & Thiel, 2020). Central to all these historical interpretations of sovereignty is the significance of a geographical qualification, emphasising the bounded sovereignty of a specific territory as a prerequisite for effectively exercising authority (Grimm, 2015).

Conceptualising digital sovereignty in an evolving political and technological world

The CEO of French radio station Skyrock, Pierre Bellanger, first coined the term "digital sovereignty" in 2008, which he went on to define in his book entitled La *Soruverainete Numerique* as "control of our present destiny … guided by the use of technology and computer networks" to describe the unique path to modernisation (Gueham, 2011, p. 9). At first glance, the word "digital" denotes and emphasises (on the one hand) the contradictory co-existence of diffuse, fluid and shifting constellations of globalised digital networks and sovereignty on the other. This dualism, therefore, seems to challenge the principles of territoriality and statehood in which the concept of digital sovereignty is inured. Yet, while this dualism is still alive in public discourse, it is often framed as a threat rather than

a guarantee. To counter risks to their authority, states have made it possible to enforce national laws and undertake government interventions in the digital realm to address digital governance issues and reinstate the nation-state's authority. The concept "digital sovereignty" here, therefore, refers, more expansively, to the "state's right and authority to regulate and exercise control over the technology, services and digital data in use within a sovereign territory" (Pohle, 2020, p. 6), which was triggered by the contest to political, economic, and legal self-determination of nation-states and their citizens.

In the 1990s, through the first decade of the 2000s, we witnessed the meteoric rise of the digital economy in many different regions of the world. As the shifting of territorial state power to global scales of governance and global economic restructuring took hold, the concept of a post-sovereign world order, where nation-states would no longer maintain their paramount and unassailable position of power, began to gain traction (MacCormick, 1999). The digital impulses driving the proliferation of the internet and telecommunications networks were powerfully evident in the rise of new actors, notably technology-focused corporations, which thrived in the commercialised digital environment that characterises our contemporary era. By the early 1990s, a deterritorialisation narrative emerged in the US, driven by the commercialisation strategy of President Bill Clinton. At the core of the strategy was the prioritisation of US involvement in the early digital economy, ultimately resulting in the US government and corporations shaping and regulating the ideals and institutional architecture of the global Internet (Kuo, 2021). The concept of commercialisation that Clinton introduced included the extension of the internet to national intelligence interests (Kahata, 2021) and the emergence and dominance of a cadre of US firms in the global digital technology sector, including corporate behemoths such as Google, Meta, and Amazon (Jiang, 2022).

These corporate entities possessed substantial material and immaterial resources and wielded remarkable control over vital societal structures (Pohle & Thiel, 2020). By the early 2000s, emphasis on globalisation, primarily as market deregulation and internationalisation, gave way to a fracture in the traditional understanding of sovereignty. This is most usefully understood in terms of Dielbert's & Crete-Nishihita's (2012) contention that the unleashing of digital market forces was evident not merely in the vast resources at the disposal of technology-focused corporations but also in their capacity to exercise control. Not only have these impulses given Tech corporations enormous power to shape societal infrastructures, but their institutional and political imprints on state affairs have challenged sovereignty. From a broad institutional and governance perspective – one that extends well beyond romanticised understandings of globalisation - the profound levels of privatisation and internationalisation in the digital landscape introduced unprecedented threats to national security as the world became increasingly interlinked through technology (Zuboff, 2019). Viewed from this perspective, digitalisation's potential and realised national security threats generated counter-tendencies and demands for nation-states to assert their authority and safeguard sensitive information and citizens from exploitation (Monyae, 2021).

The trajectory through which digital globalisation has brought the role of nation-states in digital affairs into focus has paved the way for an expanded interpretation of sovereignty, extending beyond the geographic confines of sovereign states. Particularly notable over the past two decades is the speed and extent to which digital sovereignty has come to shape countertendencies to the vagaries of information technology in a climate of deep mistrust among nation-states (Pohle & Thiel, 2020). These seismic strategic and policy shifts across the globe are primarily a reflection of the contemporary salience of digital sovereignty as governments push back against digital breaches of state autonomy and reassert their authority over digital technologies (Kahata, 2020).

The rise of US digital surveillance and its implications for sovereignty

From the perspective of digital sovereignty, the evolution of transnational digital corporations across dispersed geographies highlights how breaches of nation-states run far deeper than understandings of traditional sovereignty. In so far as the global digital economy has disabled economic sovereignty, it has also weakened the modalities through which countries are governed. Evidence of this first came to light in 2013, when the release of internal National Security Agency (NSA) documents by Edward Snowden revealed extensive monitoring and analysis of internet traffic worldwide by US law enforcement and intelligence agencies without the consent of other nations or their citizens (Ball, 2013). At a more general level, these surveillance practices, undertaken by US Tech corporations and intelligence services, led to demands, sharply divergent from the transgressive transnationalist trajectory inaugurated by the Clinton administration, for a decoupled digital sphere. Proponents of this new trajectory argued for digital strategies that recentred the state as an instrument of exclusive national control over communications, data, and regulation (Tréguer, 2017). The significance and credibility of digital sovereignty thus became a national strategic and policy imperative in the miasma of highly competitive impulses driving Tech corporations "scramble to control the Internet's global infrastructure and data flows" (Steiger et al., 2017, p. 8).

The threat of the discursive power of digitally enabled globalisation was nowhere more apparent than from the articulation by various nation-states of the risks associated with foreign surveillance and manipulation, citing examples ranging from industrial policy (Álvarez-Pallete López, 2020) to disinformation (Tambiama, 2020) and telecommunication infrastructure (Batuo, 2015). These concrete, intertwined risks opened the way for understanding digital sovereignty as a countervailing strategy against the threat of surveillance and external control. The goal was to empower states to reduce their dependence on digital infrastructure and services provided by foreign powers, notably the US (Akinyetun, 2023). Thus, more policy discourses emerged, enabling diminishing reliance on foreign sovereign powers and corporate actors and allowing states to take autonomous actions and decisions on digital infrastructures and deployments within their national territories. More generally, these emergent discourses and strategies entailed securing the data of sovereign states and, by extension, their territories, rights, and welfare of their citizens.

China's model of digital sovereignty and its global implications

Ironically, one of the fiercest critics of American digital dominance was China. In its drive to secure the state and shift the global balance of power within the digital space, China promoted and nurtured its domestic model of digital sovereignty as an alternative to the Internet and transgressive data flows across national borders (Creemers, 2016).

The official Chinese effort to define its homegrown model emerged in Article 40 of the Personal Information Protection Law, which mandated digital infrastructure operators to store locally collected data within China (China Briefing, 2021). The legislation deployed the logic of "deglobalisation" and its corollary, digital nationalism, to compel technology companies, both domestic and foreign, to abide by its rules, with a focus on restricting the flow of data outside China's borders (Zeng et al., 2017). Personal information could only be transmitted beyond China's borders through a stringent security protocol (Kynge, 2022). The irony with which we began this section is that this approach was accompanied by Chinese notions of censorship and surveillance of its citizens in what now appears as a fundamental departure from the US belief in a free-flowing digital world. The onset of Article 40 marked the inception of tighter controls. The 2017 Data Security Law positioned the state at the centre

of data management and security to safeguard Chinese interests (Perez, 2022). The central premise of the legislation was that locally stored data would enhance state security and reinforce sovereignty by strengthening governmental authority over the state and its citizens (Adegoke, 2021).

Particularly noteworthy was the speed with which China nurtured homegrown Tech companies like Alibaba, Huawei, and Tencent, among others, which have come to dominate the domestic and international markets. These companies' strategic and operational postures provide a vivid description of why Chinese corporate interests are viewed as extensions of the Chinese Communist Party (CCP), with capabilities to collect intelligence, appropriate intellectual property, and monitor users (Agbebi, 2022). Through the Belt and Road's Digital Silk Road initiative, China has propagated technology that promotes its vision of regionalised Internet and localised data controls on a global scale (Yuan, 2019). These articulations and practices are not confined to China. As global networks evolve, other states have grown increasingly wary of their digital vulnerabilities. This awareness has prompted measures towards greater control over digital infrastructure (Pohle & Thiel, 2020). During its presidency of the European Council in 2020, a pivotal shift in strategy occurred when the German government announced its intention "to establish digital sovereignty as a leitmotiv of European digital policy" (The German Presidency of the EU Council, 2020, p. 8). Policy moves such as these prompted other states to confront and rework their understandings of how deeply digital sovereignty and the movement, storage, and processing of data within their jurisdiction to limit foreign intelligence and commercial actors' access are connected.

Digital sovereignty today

The concerns around digital globalisation and digital sovereignty discussed in this section assume particular significance and urgency in nation-states considering the profound irony of China's response to the US model: that the liberalisation of the digital sphere on a global scale coincided with the ascendancy of digital surveillance and foreign control of nation-states, mapping the terrain on which nation-states have come to embrace digital sovereignty. Accordingly, before discussing the African context, we must delve into some of the nuances and complexities of the concept today. As digital sovereignty has expanded in scope over the past two decades, it has become increasingly incompatible with the laissez-faire posture that underpins American global tech supremacy (Monyae, 2021). That US policymakers are inclined to nurture and protect a system that promotes free markets, the unrestricted flow of information, and freedom of expression is a triumphal rendition of its globalisation ambitions that began with the Clinton administration (Willems, 2022). However, a closely related set of arguments suggests that as other nations adopt a more cautious approach to laissez-faire digital globalisation, demanding greater control over their digital domains, a counter-narrative appears to be emerging to US influence over the global digital landscape (Kahata, 2021).

The articulation of the concept in this combined sense has thus brought into the foreground its potential to fracture the international order as major powers, notably the US and China, compete to reconfigure the conditions for the extension or restriction of the concept in other geographic regions of the world. The question, then, is, what are the implications of the global standoff between laissez-faire digital globalisation and digital sovereignty for Africa? In seeking to address this question, it is essential to see the differential impact of the digital sphere not only between regions but also among nations themselves. This necessitates a nuanced understanding of African nation-states' challenges and the consequences of failing to ensure that digital transformation supports and protects their citizens.

Digital sovereignty in Africa: distilling the story so far

As the digital revolution expands worldwide, a vast, sprawling digital ecosystem is also emerging across Africa. If the last three decades have witnessed an unprecedented, exponential expansion of the global digital landscape, a striking manifestation of both the scale and scope of its evolution and growth can be discerned in African nations where the proliferation of internet users across the continent has surged seven times the global average since the turn of the Millennium (Internet World Stats, 2020). To all appurtenances, the Internet has metamorphosed into a cornerstone of Africa's socioeconomic activities, substantially transforming business, governance, and socio-institutional models. This spectacular phenomenon, facilitated by the ubiquitous deployment of undersea and terrestrial cable networks, smartphones, sensors, and artificial intelligence systems, has been mapped onto a population whose access to the internet and data usage pulses in its rapid growth. Africa is home to some of the world's fastest-growing populations. By some estimates, the continent will be home to 2.5 billion people by 2050, with approximately 60% of this population under 30 years old (Munga & Denwood, 2022).

Within this milieu, several possibilities present themselves. Primary among these possibilities are accounts of this demographic that prefigure the continent's potential influence over the future of the global technology industry. Most immediately, population growth is closely tied to the demand for broader internet access and improved data infrastructure. By the end of 2019, African internet penetration lagged 32.5% behind the global average (Mackinnon, 2019). The escalating demand for digital services, coupled with the mounting volume of data generation, has forecasted Africa's digital economy to reach a valuation of $180 billion by 2025, constituting approximately 7.2% of the region's prevailing Gross Domestic Product (GDP) (International Telecommunication Union [ITU], 2019).

The second possibility is foreign actors' control and capture of nation-states through increased surveillance and control. We have seen from the previous section how, in conditions of digital globalisation, foreign corporate agents at the significant switch points of digital ownership and control have assigned the state the responsibility for securing the conditions for surveillance and control of nation-states. At the same time, the nation-state is officially invoked in policy and discourses as the original site of digital sovereignty. Yet these contradictions have been inflected very differently across the US and China, whose rivalry for global dominance of the digital space has ensnared the African continent in a power dynamic and outcome over which it appears to have little control (Qobo, 2022).

However, while these possibilities broadly define sharply divergent trajectories, they do not in any way determine outcomes that, as we have seen, are, in practice, enormously variable. This paper's fundamental premise is that Africa's influence over the digital landscape can only be effectively harnessed if nation-states secure digital sovereignty. This is precisely why the combination of possibilities presupposes challenges that define a critical dimension of the hurdles to digital sovereignty confronting the continent. Digital transformation is a critical mission for many African countries, as the solutions to complex social and economic challenges may lie in new technologies.

Digital technology infrastructure can help African countries achieve universal access, participate in the global digital economy, spark the growth of small and medium enterprises in the digital space, enhance productivity and services across various sectors, and improve disaster management, healthcare, and logistics (Agbebi, 2022). Digital infrastructure can also enable African countries to leverage digital technologies for economic growth and diversification, reducing their reliance on non-renewable commodities like gas and oil (Agbebi, 2022). In the sections below, we first outline the underlying

themes of seven areas of concern emerging from this review, then interrogate them with evidence from research articles and data. Doing so allows us both to focus on some of the critical potential concerns for digital sovereignty, which is increasingly spoken about as a tool for economic development and to provide a base for policy considerations and future research.

Seven overarching concerns for digital sovereignty in Africa

From the perspective of most African nations, there is broad recognition of the centrality of Information and Communication Technologies (ICTs) to their development trajectories, opening new pathways for many to leverage digital technologies to their advantage (Monyae, 2021). The AU underscores the significance of this overarching concern, aiming to connect every government, business, and individual on the continent by 2030 (Xi, 2021). The AU recognises that achieving digital transformation in Africa requires political commitment at the highest levels to align policies and sector regulations and scale up investments and resource allocation (Hruby, 2021). To this end, there is now broad consensus among AU member states that harmonising legal and regulatory frameworks is essential for creating a common digital single market and that developing Internet and digital infrastructure is crucial for Africa's digital ecosystem (Gravett, 2020). Moreover, the importance of collaborative efforts to promote the digital economy through the AU's Digital Transformation Strategy for Africa working group has been stressed as a strategic priority. The organisation has consistently emphasised the strategic imperative of establishing a digital single market in Africa by 2030, aligning with the African Continental Free Trade Area (AfCFTA) (Akinyetun, 2023). Taken as a whole, these strategic objectives aim to promote digital transformation while safeguarding information and data, crucial for addressing persistent social and economic challenges.

Taking into account these strategic objectives, a central concern of this paper has been to engage critical problems facing the African continent in its drive for digital sovereignty, but in ways distinctively different from well-known debates over the power dynamics of China and the US in their battle for global supremacy. Instead, the paper has taken the question of barriers to Africa's digital sovereignty as a departure point. The question of how disarticulated policy and practices are from cohering more broadly for a common purpose is crucial. Yet there are vitally important practical and analytical reasons why the emphasis on identifying barriers is necessary but presently insufficient and why closer attention to the challenges to digital sovereignty is essential. Pursuant to this aim, the paper took as its starting point an analysis of existing knowledge, providing insight into some emerging themes roughly emblematic of general structural challenges and barriers. These challenges were then grouped into seven broad themes emerging from a review of literature (highlighted in Table 1). The various categories formed the basis for a more rigorous analysis of inhibitors and possibilities for digital sovereignty in subsequent sections.

Table 1: Root causes and barriers

Root causes	Barriers
Lack of digital infrastructure	- Weak digital infrastructure, hindering the ability of countries to actively participate in the global digital economy. - Limited access to basic broadband and 5G technology disadvantages countries regarding digital sovereignty.

Coherency in legal frameworks	- Lack of coherency in-laws and frameworks related to the digital sphere across African nations. - Absence of a legal framework and its impact on African countries achieving and sustaining digital sovereignty. - Lack of political commitment to align policies and sector regulation and scale up investments and resource allocation. - Lack of a harmonised legal and regulatory frameworks for creating a common digital single market.
Dependence on external assistance	- Need for international assistance in building necessary digital infrastructure creates a dependence on external entities, limiting Africa's control over its digital development. - This reliance limits Africa's ability to ensure the security of its digital infrastructure and information.
Data security and privacy concerns	- Involvement of foreign entities in funding and building data centres and related concerns about data security and privacy. - Shortfall of 1,000 megawatts of new facility capacity to meet growing demand, equivalent to 700 new data centres.
Financial constraints	- Financial constraints and the lack of interest from external parties make it challenging for African nations to invest in digital infrastructure. - Lack of adequate financial resources hampers efforts to keep pace with the rapidly evolving digital landscape.
Capacity building and education	- Weak political institutions and undereducated populations challenge African nations in negotiating favourable deals and agreements in the digital sphere. - Building a digitally sound ecosystem necessitates investments in education and capacity creation to empower nations in the digital age.
Unequal distribution of power	- Unequal distribution of economic, political, and cultural power in the global digital landscape jeopardises African countries' sovereignty and national security. - Limited control over global digital infrastructure and data value chains undermines Africa's ability to assert its independence.

Discussion

Hurdles to digital sovereignty

This paper began as an attempt to understand how foreign partners and Tech corporations were deploying models from elsewhere – particularly China – to define and delimit possibilities for digital transformation in African nation-states. Digital liberalisation catalysed counter-tendencies towards

digital sovereignty among several nation-states, starting in China and spreading to other nations, to reinstate the authority and control of the state over the Internet and data flows. The African continent, however, has lagged the global trend. The confluence of rapidly spreading digital connectivity, weak digital infrastructure, over-reliance on foreign players, undereducated technology users and workers, incoherent regulatory regimes, and financial constraints has exposed many African nation-states to the vagaries of surveillance and control by foreign partners. The lack of coherence of laws and regulatory frameworks related to the digital sphere, coupled with dependence on international assistance in building digital infrastructure, has hindered the continent's ability to establish and control the trajectory of digital sovereignty.

The continent's growing, youthful population and vastness and diversity, with its complex history, traditions, and people, present numerous exciting and daunting challenges (Phee, 2021). Notably missing in discussions on digital sovereignty as a panacea are misleading presumptions that foreign power repertoires alone account for the African continent's vulnerability to surveillance and control. However, the argument presented in this paper is that the Internet does not exist in some abstract sphere. It is always and already spatially grounded in people and institutions. Thus, building on Peck and Tickell's (2002) call to avoid painting the "global" as an unruly domain that is effectively beyond regulation, our mappings have shown a starting point in identifying the following barriers to digital sovereignty that might alter the existing power repertoires between the US and China: infrastructure constraints, financial constraints and undereducation, foreign dependence and surveillance, data centres, policy, and regulatory regimes.

Infrastructure constraints

The most spectacular contemporary manifestation of the challenge confronting all African nation-states in the sub-Saharan region is the control of global digital infrastructure and data value chains by a few Tech corporations based in some advanced economies. Insufficient capital for infrastructure development poses complex challenges for most African nations. Infrastructure development has led to unequal economic, political, and cultural power, threatening the sovereignty and national security of many countries and regions (Lu, 2022). While African countries have little choice but to accept technological assistance from appealing bidders, these arrangements may have long-term repercussions for the continent's economic, political, and financial stability (Nye, 2021). An illustrative example of the potential risks of Chinese infrastructure projects can be seen in the case of the AU's headquarters in Addis Ababa. China constructed the AU's headquarters through its banks and firms, which was subsequently found to have had its entire network and computer systems compromised for the first five years of operation (Mackinnon, 2019). If China can manipulate and monitor the continent's leading regional organisation, concerns arise about similar activities in other African nations. Misuse of data by Chinese companies and the government hinders African countries' abilities to enforce digital sovereignty, leaving digital infrastructure and citizens' information vulnerable.

Financial constraints and undereducation

African countries have sought financing and expertise to guide the development of their telecoms, data sectors, and infrastructure. Beyond China, enthusiasm from other parties needs to be improved. For instance, when Tanzania proposed projects to multiple donor agencies, including the World Bank, China was the only eager financier to develop critical broadband infrastructure to improve connectivity in Tanzania and the East Africa region (Agbebi, 2022). The lack of interest from other international

partners compelled Tanzania to accept China's involvement in their digital sphere. While access to Chinese technology and infrastructure enhances digital connectivity, it also allows China to harvest data related to internet traffic, hindering progress toward digital sovereignty in Africa.

Foreign dependence and surveillance

China has positioned itself as a dominant supplier of underwater and terrestrial fibre optic cables in Africa, enabling vast data transfer through the Internet (Cheney, 2019). China Mobile, for instance, is establishing the "2Africa" cable, a 37,000km cable network designed to connect Africa directly with the Middle East, supporting the growth of 5G and broadband access (Karasik, 2022). However, this also ties Africa's telecoms and data centres to China's influence, which has raised concerns about data exploitation and surveillance. China's potential availability of data and information to exploit poses a significant challenge to African nation-states safeguarding their territoriality and citizens. US-based companies have also entered the fray to influence Africa's digital infrastructure. Google's Equiano subsea internet cable and Meta's planned subsea cable around the entire African continent aim to improve broadband access and the free flow of information (Francios & George, 2019). While these efforts align with US values of ensuring information flows freely online, it is well known that US intelligence agencies have access to such data, potentially affecting Africa's digital sovereignty. Aside from private American entities, the US government also funds projects to support the free flow of data between nations. The US International Development Finance Corporation funded Africell, a regional mobile network operator, for infrastructure expansion (Munga, 2023). These efforts enhance information flows across borders but also create opportunities for external interference due to the open movement of knowledge, thereby impeding efforts to protect the rights of nation-states.

Data centres

The absence of data centres and control over their construction hamper a nation's ability to maintain digital sovereignty and the right to self-determination. They rely on other states and Tech corporations to access and exploit data disadvantages in Africa, jeopardising its jurisdiction over data and digital infrastructure. China's involvement in data centre construction across the African continent is of particular concern. According to the International Institute for Strategic Studies, China is involved in digital infrastructure projects focusing on data housing and collection (Nye, 2022). The Chinese government and Tech companies have invested billions in infrastructure projects on the African continent (Cheney, 2019). The construction of data centres in African nations, often financed by Chinese entities, raises concerns about the potential access and use of data by Chinese companies and the government. The fear is that China could use big data to pursue its geopolitical objectives on the continent, considering that many African nations have weak political institutions and undereducated populations (Nye, 2022). The case of Huawei's cyber espionage in Uganda demonstrates that data centre projects funded by China may give Chinese corporate entities access to sensitive information, undermining digital sovereignty in African nations.

Policy and regulatory regimes

Notwithstanding the importance of digital transformation and sovereignty, most African nations lack comprehensive digital policies and strategies. Data regulatory schemes are often in their infancy and, where they do exist, need to be more effectively implemented (Mackinnon, 2019). Some countries, such as Gambia, Namibia, and Gabon, have incorporated digital agendas into their national plans (Monyae, 2021). Other nations, including Nigeria, Ethiopia, Botswana, and South Africa, have devel-

oped standalone digital policy documents (Monyae, 2021). These documents address issues relevant to these nations, such as e-commerce, cybersecurity, privacy, and data. South Africa's proposed National Data and Cloud Policy, introduced in April 2021, adopts a multidimensional approach to digital sovereignty and self-determination. The draft policy covers a range of issues, including competition and trade, cybersecurity, local data storage, cross-border data transfer, and skills and capacity development, all of which aim to strengthen the nation's digital sovereignty (Vermeulen, 2021). The policy further seeks to enhance the state's capacity to provide services to its citizens, facilitating informed policy development and data-driven decision-making (South African Government News Agency, 2023). There are presently 25 African countries that have enacted online consumer protection legislation, 39 that have instituted cybercrime laws, 27 that have established data protection and privacy regulations, and 33 that have enacted e-transaction laws (Monyae, 2021). Nevertheless, many countries lack comprehensive legislative provisions for their digital domains. Not only has the dispersed and global nature of regulatory frameworks made it highly challenging for African nation-states to organise effectively, but they have also made it difficult to lobby politicians to represent their interests. Unlike global networks, policymakers are restricted by political boundaries and can only regulate a piece of a much more extensive network. It is in those strategic gaps (because of their network centrality) that policy coherence has agency.

Possible implications for policy and practice

In the rapidly evolving digital landscape, Africa is on the precipice. Pursuing digital sovereignty in a world dominated by technological giants presents formidable challenges. The allure of external investments offers promises of improved connectivity and technological progress. Nevertheless, it comes with the ominous shadow of data exploitation, a lack of information controls, and surveillance. Projects funded by external benefactors are double-edged swords, weakening the ability of African states to protect their digital sovereignty and safeguard their territorial integrity. As this paper has demonstrated, African nation-states grapple with a dual thirst for digital independence and navigating their significant infrastructure financial and regulatory deficits. A multifaceted approach is, therefore, imperative for Africa to chart its digital destiny. Identifying these problems and challenges underscores the complexity of the digital sovereignty landscape in Africa, highlighting the urgent need for strategic planning, international collaboration, and domestic capacity-building to overcome these obstacles.

First, collaboration with international partners is necessary, but it needs to be underpinned by a clear vision of safeguarding Africa's data and digital infrastructure. Reducing reliance on single suppliers is essential. Investments in home-grown solutions, robust data policies, and comprehensive strategies are crucial to harnessing foreign investment to a homegrown model of digital sovereignty. Second, African nation-states must address technological challenges and develop strategies to maximise digital development (Qobo, 2022). While external partners will continue to play a role, the nature of these relationships should evolve from traditional paternalistic models to ones that nurture mutual benefit by contributing value to the African continent. This includes support and investment in human capital and technology sharing without overly restrictive conditions.

Third, achieving this goal requires governments across the continent to invest in the necessary infrastructure and resources to keep pace with the Fourth Industrial Revolution. Africa's digital infrastructure development is capital-intensive and provides a unique opportunity to leapfrog into the latest technological innovations worldwide (*African Development Bank Group*, 2014). This requires substantial development investments from international partners and private companies. Fourth, given the burgeoning importance of the digital sphere in Africa's socioeconomic landscape, the continent

must devise robust regulatory and legislative frameworks to safeguard data assets and bolster digital sovereignty. Regulations could cover the conditions for finance, infrastructure investment, skills development, surveillance and control and policy harmonisation. In short, they could be built on a more inclusive definition of digital trade and a vision that partnerships are embedded in African norms and moral economies.

There is currently minimal political will to achieve these objectives, but that does not mean they are impossible. Such a development is critical for sustainable economic growth, as it enables a more efficient allocation of resources and accelerates economic productivity (Mlambo et al., 2016). Fifth, the critical imperative for Africa should be building a robust digital ecosystem open to partnerships with various stakeholders (Qobo, 2022). This approach ensures that the continent is not overly dependent on a single supplier and can effectively navigate the fast-evolving digital industry (Cha, 2021). Failure to do so will impede Africa's digital leap, hindering the achievement of digital sovereignty.

Conclusion

This article has demonstrated that digital sovereignty is now a strategic imperative for most African nation-states. However, its realisation is undermined by several challenges and constraints that, if left unresolved, may entrench the existing "power repertoires" between the US and China on the continent. By highlighting seven critical concerns in a global but uneven marketplace, the article found that the barriers identified (infrastructure constraints, financial constraints and undereducation, foreign dependence and surveillance, data centres, policy, and regulatory regimes) serve to deracinate the sovereignty of African nation-states unable to navigate the complexities of a global digital landscape.

Overcoming these hurdles is a double-edged sword: their resolution depends on continued investment by external powers, which are themselves part of the problem. However, besides the threat of foreign encroachments on the sovereignty of nations, these findings have more profound implications for the continent's policy and practice. As Coe and Yeung (2015) note, uneven power relations existed long before global digital networks were brought into being and are necessarily entangled in relations of inequality; it is, therefore, worth asking why it is that we might expect digital sovereignty to level the field.

At this nascent stage, it is important to reflect not just on what we already know about the uneven geographies of nation-states but also to envision alternatives and strategies that might bring a fairer playing field into being. This article has offered just such a vision that diverges from much of the hype about the potential of digital sovereignty for economic development by focusing on causalities that have undermined the continent's aspirations. However, a more detailed empirical inquiry into the barriers to digital sovereignty and further research that focuses specifically on financial and regulatory barriers and solutions is still needed. In the Fourth Industrial Revolution, digital sovereignty is not just a matter of economic and political independence but an issue of protecting the future of African nation-states and their citizens. The challenges are formidable, but the opportunity for Africa to carve out its digital destiny remains to be seized. As the African continent continues to awaken and rise to the potential of the digital age, the quest for digital sovereignty will be an integral part of shaping its future success.

References

Adegoke, Y. (2021, December 1). The real reason China is pushing "digital sovereignty" in

Africa. Rest ôf world. https://restofworld.org/2021/the-real-reason-china-is-pushing-digital-sovereignty-in-africa/

African Development Bank Group. (2014). Tracking Africa's Progress in Figures. African Development Bank Group. https://www.afdb.org/en/knowledge/publications/tracking-africa's-progress-in-figures

Agbebi, M. (2022). China's Digital Silk Road and Africa's technological future. Council on Foreign Relations, https://www.cfr.org/sites/default/files/pdf/Chinas%20Digital%20Silk%20Road%20and%20Africas%20Technological%20Future_FINAL.pdf

Akinyetun, T.S. (2023, May 19). Digital sovereignty in Africa: The albatross of digital transformation and autonomy. *Kujenga Amani*. https://kujenga-amani.ssrc.org/2023/05/19/digital-sovereignty-in-africa-the-albatross-of-digital-transformation-and-autonomy/

Álvarez-Pallete López, J.M. (2020, July 30). Introduction. *Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry.* https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/

Anwar, M.A., & Graham, M. (2020). Digital labour at economic margins: African workers and the global information economy. *Review of African Political Economy*, 47(163), 95-105. DOI: 10.1080/03056244.2020.1728243.

Ball, J. (2014, August 21). Edward Snowden NSA files: secret surveillance and our revelations so far. *The Guardian*, https://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations

Batuo, M.E. (2015). The role of telecommunications infrastructure in the regional economic growth of Africa. *The Journal of Developing Areas*, 49(1), 313–330. http://www.jstor.org/stable/24241299

Birhane, A. (2019, July 18). The algorithmic colonization of Africa. *Real Life.* https://reallifemag.com/the-algorithmic-colonization-of-africa/

Blakeley, G. (2021). The big tech monopolies and the state. *Socialist Register*, 57. https://socialistregister.com/index.php/srv/article/view/34949

Cha, J (2021). The future of US-China tech competition: Global perceptions, prospects, and strategies. *National Assembly Futures Institute*, Research Report 21-17.

Cheney, C. (2019). China's digital silk road: Strategic technological competition and exporting political illiberalism. *Pacific Forum*, 19(8).

China Briefing. (2021, August 24). The PRC Personal Information Protection Law (Final): A full translation. https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/

Coe, N.M., & Yeung, H.W. (2015). *Global Production Networks:* Theorizing Economic Develop-

ment in an Interconnected World. Oxford University Press, 2015. https://doi.org/10.1093/acprof:oso/9780198703907.001.0001

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, 21(2), 2305-2322. https://doi.org/10.1177/1461444819865984

Creemers, R. (2016). The Chinese cybersovereignty agenda. European Council on Foreign Relations. https://www.jstor.org/stable/pdf/resrep21667.18.pdf

Deibert, R.J., & Crete-Nishihata, M. (2012). Global governance and the spread of cyberspace controls. *Global Governance*, 18(3), 339-361. https://doi.org/10.1163/19426720-01803006

Deng, B.K. (2010). The evolving concept and institution of sovereignty: Challenges and opportunities. *AISA Policy Brief*, 38(6).

Donnelly, J. (2014). State sovereignty and international human rights. *Ethics & International Affairs*, 28(2), 225–238. doi:10.1017/S0892679414000239

Francios, M.D., & George, C. (2019, June 28). Introducing Equiano, a subsea cable from Portugal to South Africa. Google Blog. https://cloud.google.com/blog/products/infrastructure/introducing-equiano-a-subsea-cable-from-portugal-to-south-africa

Gravett, W. (2020). Digital neo-colonialism: The Chinese model of internet sovereignty in Africa. *African Human Rights Law*, 20, 125–146. http://dx.doi.org/10.17159/1996-2096/2020/v20n1a5

Grimm, D. (2015). *Sovereignty: The origin and future of a political and legal concept.* New York Chichester, West Sussex: Columbia University Press. https://doi.org/10.7312/grim16424

Gueham, F. (2017). Digital sovereignty – steps towards a new system of internet governance. The Fondation pour l'innovation politique.

Hendrickson, J., & Zaki, H. (2013). Modern African ideologies. In M., Freeden, L.T., Sargent, & M., Stears, (Ed.). *The Oxford handbook of political ideologies* (1st ed.). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199585977.001.0001

Hindman, M. (2018). *The internet trap: How the digital economy builds monopolies and undermines democracy.* Princeton: Princeton University Press. https://doi.org/10.23943/princeton/9780691159263.001.0001

Hruby, A. (2021, April 8). The digital infrastructure imperative in African markets. Atlantic Council. https://www.atlanticcouncil.org/blogs/africasource/the-digital-infrastructure-imperative-in-african-markets/

International Court of Justice. (1949, April 9). The Corfu Channel Case (Merits). https://www.icj-cij.org/public/files/case-related/1/001-19490409-JUD-01-00-EN.pdf

Internet World Stats. (2020). Internet penetration in Africa 2020 – Q1 – March, Internet world stats: Usage and population statistics. https://www.internetworldstats.com/stats1.html

International Telecommunication Union. (2019). Economic contribution of broadband, digitization and ICT regulation: Econometric modelling for Africa, https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-EF.BDT_AFR-2019-PDF-E.pdf

Jiang, Y. (2022, January 12). US-China tech war: Beijing unveils grand plan to grow digital economy as US moves forward with competition bill. *South China Morning Post.* https://www.scmp.com/tech/tech-war/article/3163246/us-china-tech-war-beijing-unveils-grand-plan-grow-digital-economy-us

Kahata, A. (2020, November 24). Managing U.S.-China technology competition and decoupling. *CSIS.* https://www.csis.org/blogs/strategic-technologies-blog/managing-us-china-technology-competition-and-decoupling

Karasik, T. (2022, March 23). Africa's digital sovereignty threatened by big power rivalry. *Arab News.* https://www.arabnews.com/node/2049021

Kuo, M.A. (2022, September 26). Trafficking data: China's pursuit of digital sovereignty. *The Diplomat*. https://thediplomat.com/2022/09/trafficking-data-chinas-pursuit-of-digital-sovereignty/

Kynge, J. (2022, May 2). US-China tech race: the great decoupling. *Financial Times.* https://www.ft.com/content/c61ab7b8-65e1-4c4a-b597-57b3e9b4b70b

Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. Race & Class, 60(4), 3–26. https://doi.org/10.1177/0306396818823172

Lu, S. (2022, February 9). A report detailed the tech gap between China and the US. Then it disappeared. *Protocol*. https://www.protocol.com/china/us-china-tech-decoupling

MacCormick, N. (1999). *Questioning sovereignty: Law, state, and nation in the European Commonwealth*. Oxford: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780198268765.001.0001

Mackinnon, A. (2019, March 19). For Africa, Chinese-built internet is better than no internet at all. *Foreign Policy.* https://foreignpolicy.com/2019/03/19/for-africa-chinese-built-internet-is-better-than-no-internet-at-all/

McKay, S. (2023). Plebiscites, referendums, and ballot initiatives as institutions of popular sovereignty: Rousseau's influence on competing theories of popular-vote processes. *The Review of Politics*, 85(1), 23–47. doi:10.1017/S0034670522000912

Mlambo, C., Kushamba, A., & Simawu, M.B. (2016). China-Africa relations: What lies beneath? *The Chinese Economy*, 49(4), 257-276, DOI: 10.1080/10971475.2016.1179023

Monyae, D. (2021, September 28). Africa's digital sovereignty is a timely and relevant debate. *University of Johannesburg News.* https://news.uj.ac.za/news/africas-digital-sovereignty-a-timely-and-relevant-debate-2/

Munga, J. (2023, May 17). How the United States can effectively implement its new digital transformation with Africa initiative. Carnegie Endowment for International Peace. https://carnegieendowment.org/2023/05/17/how-united-states-can-effectively-implement-its-new-digital-transformation-with-africa-initiative-pub-89755#:~:text=Within%20this%20context%2C%20the%20United,Africa%2C%20released%20in%20August%202022

Munga, J., & Denwood, K. (2022, October 3). How will U.S.-China tech decoupling affect Africa's mobile phone market? Carnegie Endowment for International Peace. https://carnegieendowment.org/2022/10/03/how-will-u.s.-china-tech-decoupling-affect-africa-s-mobile-phone-market-pub-88034

Nye, J.S. (2021, December 7). In US-China competition, technology matters, but alliances matter more. *The Strategist.* https://www.aspistrategist.org.au/in-us-china-competition-technology-matters-but-alliances-matter-more/

Nye, J.S. (2022, August 5). America's China challenge. *The Strategist.* https://www.aspistrategist.org.au/americas-china-challenge/

Peck, J., and Tickell, A. (2002). Neoliberalizing space. *Antipode*, 34, 380-404. https://doi.org/10.1111/1467-8330.00247

Perez, C. (2022, January 28). Why China's new data security law is a warning for the future of data governance. *Foreign Policy.* https://foreignpolicy.com/2022/01/28/china-data-governance-security-law-privacy/

Phee, M. (2021, December 15). US Policy Toward Africa: Remarks. *US Department of State.* https://www.state.gov/u-s-policy-toward-africa/

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *International Policy,* 9(4). https://policyreview.info/concepts/digital-sovereignty

Qobo, M. (2022). US-China tech wars: Shaping Africa's agency. *The Political Economy of China-US Relations, Springer International Publishing*, Imprint: Palgrave Macmillan. https://doi.org/10.1007/978-3-030-86410-1_9

South African Government News Agency. (2023, April 13). Government finalising national data, cloud policy. https://www.sanews.gov.za/south-africa/government-finalising-national-data-cloud-policy#:~:text=The%20national%20data%20and%20cloud%20policy%20%E2%80%9Cseeks%20to%20strengthen%20the,sovereignty%20and%20the%20security%20thereof%E2%80%9D

Steiger, S., Schünemann, W.J., & Dimmroth, K. (2017). Outrage without consequences? Post-Snowden discourses and governmental practice in Germany. *Media and Communication*, 5(11), 7–16. https://doi.org/10.17645/mac.v5i1.814

Tambiama, M. (2020). Digital sovereignty for Europe. *European Parliamentary Research Service Papers.* https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

The German Presidency of the EU Council. (2020). Together for Europe's recovery: Programme for Germany's Presidency of the Council of the European Union (1 July to 31 December 2020). Council of the European Union.

Tréguer, F. (2017). Intelligence reform and the Snowden paradox: The case of France. *Media and Communication,* 5(1), 17–28. https://doi.org/10.17645/mac.v5i1.821

Truby, J. (2020). Governing artificial intelligence to benefit the UN Sustainable Development Goals. *Sustainable Development,* 28(4), 946–959. https://doi.org/10.1002/sd.2048

Vermeulen, J. (2021, April 5). South Africa's plan to launch state-owned cloud competing mega-network. My Broadband. https://mybroadband.co.za/news/cloud-hosting/392105-south-africas-plan-to-launch-stated-owned-cloud-computing-mega-network.html

Willems, C. (2022, February 17). The path forward on the US-China technology competition. Atlantic Council. https://www.atlanticcouncil.org/blogs/econographics/the-path-forward-on-the-us-china-technology-competition/

Xi, J. (2021, August 14). Analysts: China expanding influence in Africa via telecom network deals. *VOA News.* https://www.voanews.com/a/economy-business_analysts-china-expanding-influence-africa-telecom-network-deals/6209516.html

Yuan, L. (2019, January 2). Learning China's forbidden history, so they can censor. *The New York Times.* https://www.nytimes.com/2019/01/02/business/china-internet-censor.html?searchResultPosition=1

Zeng, J., Stevens, T., & Chen, Y. (2017). China's solution to global cyber governance: Unpacking the domestic discourse of "internet sovereignty". *Politics & Policy*, 45(3), 432–464. https://doi.org/10.1111/polp.12202

Zick, T. (2005). Are the states sovereign? *Washington University Law Quarterly*, 83(1), 229-337.

Ziolkowska, K. (2021). Distributing authority - state sovereignty in the age of blockchain. *International Review of Law, Computers & Technology*, 35(2), 116–130. https://doi.org/10.1080/13600869.2021.1885108

Zuboff, S. (2019). The age of surveillance capitalism: *The fight for a human future at the new frontier of power*. United Kingdom: Profile.