JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Emerging Technologies, Digital Dependency, and Security Sovereignty: Kenya's Constrained Regional Power in Comparative Perspective

Benson Onyango Nalo
Senior Lecturer International Relations, Security and Strategic Studies
Pioneer International University, Nairobi Kenya

Abstract
Emerging technologies such as drones, AI-enabled surveillance systems, and cyber defence platforms are often assumed to enhance sovereignty and reconfigure regional power. Kenya's experience, however, reveals the paradox of technological modernization and persistent dependency. Despite tactical gains in counterterrorism, reliance on foreign suppliers, donor-driven initiatives, and externally controlled data flows has entrenched digital dependency, constraining Kenya's ability to convert modernization into strategic autonomy or regional leadership. This study employs a qualitative, comparative case study approach, drawing on policy documents, donor reports, peer-reviewed scholarship, and empirical studies. Kenya is analyzed as the primary case within the East African Community, with comparative extensions to continental and global contexts. The analysis is guided by Dependency Theory, Regime Theory, and Technological Sovereignty Theory to interrogate how state capacity mediates the relationship between technology adoption and sovereignty outcomes. Findings indicate that Kenya's weak institutions, fragmented regulation, and absence of indigenous innovation ecosystems prevent the translation of tactical modernization into strategic autonomy. Comparative evidence demonstrates similar dependency patterns in Tanzania, Uganda, Rwanda, Nigeria, Egypt, and South Africa, while global cases such as India, China, and Israel illustrate how indigenous innovation and strong institutional ecosystems transform emerging technologies into instruments of geopolitical power. The paper contributes to international relations scholarship by highlighting the limits of technological power in the digital age. It underscores that sovereignty outcomes are contingent upon institutional strength and innovation capacity, and it argues that Kenya must strengthen institutional frameworks, invest in indigenous defence innovation, and pursue regional integration if digital dependency is to be transformed into security sovereignty and regional influence.

.

Keywords: Security Sovereignty, Military Modernization, Digital Dependency, Regional Power

I. INTRODUCTION

Emerging technologies are increasingly recognized as transformative instruments of state power in international relations. In fact, control over digital infrastructure, surveillance systems, and military technologies is no longer merely technical but geopolitical, capable of reshaping hierarchies of power and sovereignty (Jili, 2026). Yet across the East African Community (EAC), persistent structural weaknesses constrain the ability of states to convert technological modernization into sovereignty. Tanzania's reliance on donor-supported ICT infrastructure under the World Bank's Digital Tanzania Programme reflects external dependence (World Bank, 2025). Uganda's deployment of Huawei's "Safe City" surveillance systems demonstrates reliance on Chinese suppliers for national security (Munyua, 2025). Rwanda, by contrast, has invested in Kigali Innovation City and AI training programs, partially mitigating dependency through coordinated digital governance (Mukhtar, 2025).

At the continental level, Africa's digital dependency is reinforced by fragmented regulation and weak institutional ecosystems. Nigeria's large-scale importation of surveillance technologies from China and Israel underscores dependency at scale (Okoye, 2025). Egypt's ambitious drone modernization program remains reliant on foreign suppliers, particularly Chinese and Turkish firms (Africa Defense Magazine, 2025). South Africa's indigenous innovation, exemplified by the Milkor 380 UAV, demonstrates how stronger institutional ecosystems can foster partial sovereignty through local defence production (Moyo, 2025). Despite growing investments in subsea cables, data centers, and regional internet exchange points, Africa continues to face a rural–urban digital divide and limited indigenous innovation capacity, leaving sovereignty vulnerable to external actors (Jili, 2026).

Global trajectories highlight contrasting outcomes. China's state-led digital sovereignty strategy—anchored in indigenous 5G networks, AI research, and military technologies—illustrates how coordinated investment can be systematically converted into geopolitical leverage (TRENDS Research & Advisory, 2026). India's hybrid model, combining strong state oversight with inclusive digital public infrastructure such as Aadhaar and UPI, offers a democratic alternative to both Chinese state-centrism and Western corporate dominance (Nyabuti, 2025). Meanwhile, the Iran–Israel conflict of 2026 showcased how indigenous innovation in drones, AI-driven targeting, and missile defence decisively altered military balances, underscoring Africa's comparative vulnerability (TRENDS Research & Advisory, 2026).

Kenya's case epitomizes these tensions. The deployment of Chinese-manufactured CH-4 drones expanded reconnaissance and counterterrorism capacity against Al Shabaab but exposed vulnerabilities in defence procurement through reliance on foreign suppliers (Africa Defense Magazine, 2025). Israeli AI surveillance systems procured in 2008 enhanced urban monitoring and border control but raised sovereignty concerns as critical data flows remained externally controlled (Nyabuti, 2025). Donor-driven cyber defence initiatives, supported by the European Union and the United States, improved resilience against ransomware and phishing but failed to establish indigenous innovation ecosystems (Mukhtar, 2025). These tactical gains have not translated into strategic autonomy, leaving Kenya constrained by fragmented regulation, weak institutional enforcement, and dependence on external actors in national security matters.

By situating Kenya's experience within EAC, continental African, and global debates—and drawing on dependency theory, regime theory, and technological sovereignty—this paper argues that state capacity mediates the relationship between technological adoption and sovereignty outcomes. Kenya's modernization has expanded operational capacity but failed to overcome structural dependency, leaving the state vulnerable and marginal within regional international relations. The study contributes to scholarship on the digital age by interrogating the limits of technological power and underscoring the need for Kenya to strengthen institutional capacity, invest in indigenous defence innovation, and pursue regional integration to overcome the security power gap.

II. Background to the Study

Background to the Study

The digital age has redefined the foundations of state power, with emerging technologies increasingly viewed as instruments of sovereignty and geopolitical leverage. Control over digital infrastructure, surveillance systems, and military technologies is no longer a purely technical matter but a strategic determinant of national security and international influence (Jili, 2026). States that successfully integrate indigenous innovation with strong institutional ecosystems—such as China and Israel—demonstrate how technological modernization can be systematically converted into geopolitical power (TRENDS Research & Advisory, 2026). Conversely, states with weak institutions and externally dependent innovation pathways often find modernization reinforcing dependency rather than overcoming it (Nyabuti, 2025).

In Africa, the pursuit of digital sovereignty has been uneven. While investments in ICT infrastructure, subsea cables, and data centers have expanded connectivity, structural weaknesses persist. Fragmented regulation, donor-driven priorities, and reliance on foreign suppliers have entrenched dependency across the continent (Okoye, 2025). Nigeria's large-scale importation of surveillance technologies from China and Israel underscores dependency at scale (Okoye, 2025). Egypt's ambitious drone modernization program remains reliant on foreign suppliers, particularly Chinese and Turkish firms (Africa Defense Magazine, 2025). South Africa's indigenous innovation, exemplified by the Milkor 380 UAV, demonstrates how stronger institutional ecosystems can foster partial sovereignty through local defence production (Moyo, 2025). Despite growing investments in subsea cables, data centers, and regional internet exchange points, Africa continues to face a rural–urban digital divide and limited indigenous innovation capacity, leaving sovereignty vulnerable to external actors (Jili, 2026).

Within the East African Community (EAC), Tanzania's reliance on donor-supported ICT infrastructure under the World Bank's Digital Tanzania Programme reflects external dependence (World Bank, 2025). Uganda's deployment of Huawei's "Safe City" surveillance systems demonstrates reliance on Chinese suppliers for national security (Munyua, 2025). Rwanda, by contrast, has invested in Kigali Innovation City and AI training programs, partially mitigating dependency through coordinated digital governance (Mukhtar, 2025).

Kenya epitomizes these tensions. The adoption of Chinese-manufactured CH 4 drones expanded reconnaissance and counterterrorism capacity against Al Shabaab but exposed vulnerabilities in defence procurement through reliance on foreign suppliers (Africa Defense Magazine, 2025). Israeli AI surveillance systems procured in 2008 enhanced urban monitoring and border control but raised sovereignty concerns as critical data flows remained externally controlled (Nyabuti, 2025). Donor-driven cyber defence initiatives, supported by the European Union and the United States, improved resilience against ransomware and phishing but failed to establish indigenous innovation ecosystems (Mukhtar, 2025). These tactical gains have not translated into strategic autonomy, leaving Kenya constrained by fragmented regulation, weak institutional enforcement, and dependence on external actors in national security matters.

This study situates Kenya's experience within comparative regional, continental, and global contexts, drawing on dependency theory, regime theory, and technological sovereignty. By interrogating the mediating role of state capacity, it seeks to explain why emerging technologies have not reconfigured Kenya's regional power and to identify pathways toward strengthening institutional capacity, fostering indigenous defence innovation, and pursuing regional integration to overcome the security power gap.

III. Literature Review

Scholarship on digital dependency in Africa consistently highlights a paradox: while technological adoption has expanded operational capacity, it has not translated into strategic autonomy or regional influence. Kenya's experience exemplifies this tension. The deployment of drones, AI enabled surveillance systems, and donor driven cyber defence initiatives has enhanced tactical capabilities, yet the country remains structurally dependent on external suppliers and constrained by weak institutional frameworks. This dependency limits Kenya's ability to reconfigure its position within East African international relations (Mukhtar, 2025; Nyabuti, 2025).

Dependency theory provides a foundational lens for understanding this reliance. Dos Santos (1970) argued that dependency entrenches asymmetrical relations between core and peripheral states, reproducing subordination. Kenya's installation of Huawei led Safe City CCTV networks in Nairobi and Mombasa illustrates this dynamic: while these systems expanded facial recognition and behavioural analytics, foreign control of servers and software updates compromised sovereignty (Mukhtar, 2025). Similarly, donor driven cyber defence programs supported by the European Union and the United States improved resilience against ransomware and phishing but reinforced reliance on external expertise and proprietary software (Olang', 2024).

Regime theory further illuminates the institutional dimension of Kenya's dependency. Krasner (1983) defined regimes as sets of principles, norms, rules, and decision-making procedures around which actors' expectations converge. In Kenya, ICT reforms framed as steps toward sovereignty often reinscribe dependency by aligning national priorities with corporate interests (Jili, 2026). Regional regimes such as the East African Community's harmonized data protection frameworks remain unevenly enforced, limiting their

effectiveness (Soulé, 2025). Rwanda's coordinated digital governance through Kigali Innovation City demonstrates partial mitigation, while Tanzania and Uganda mirror Kenya's donor driven ICT reliance.

The concept of technological sovereignty underscores the importance of indigenous innovation ecosystems. Sovereignty requires not only access to emerging technologies but also control over infrastructure, platforms, and data flows (Soulé, 2025). Comparative cases highlight this distinction: China's state led digital sovereignty strategy demonstrates how coordinated investment in 5G networks, sovereign cloud systems, and AI enabled defence platforms can be systematically converted into geopolitical leverage (Soulé, 2025). Israel's deployment of AI driven targeting systems such as Lavender and The Gospel during the Iran–Israel conflict illustrates how indigenous innovation decisively reconfigures military power (TRENDS Research & Advisory, 2026). By contrast, Kenya's imported systems yield tactical gains but fail to produce strategic autonomy, underscoring the absence of indigenous innovation ecosystems (Mukhtar, 2025).

Despite these insights, several gaps remain in the literature. First, there is limited empirical focus on how specific Kenyan institutions fail to enforce cybersecurity and drone policies, leaving the institutional dimension underexplored. Second, regional integration dynamics within the East African Community are insufficiently examined, despite their potential to mitigate or exacerbate dependency. Third, while civil liberties concerns are noted, there is inadequate analysis of how surveillance technologies reshape citizen–state relations and political legitimacy (Mwangi, 2024). Finally, comparative asymmetry persists: global cases such as China, Israel, and Iran are well documented, but African states beyond Kenya receive limited comparative attention, leaving regional patterns underdeveloped.

This study seeks to fill these gaps by adopting a qualitative, comparative case study design. It provides empirical analysis of Kenya's institutional weaknesses in cybersecurity and drone governance, situates Kenya within EAC integration dynamics, and interrogates the implications of surveillance technologies for political legitimacy. By extending comparison to Nigeria, Egypt, and South Africa, the study enriches African perspectives often overshadowed by global cases. Through the triangulation of dependency theory, regime theory, and technological sovereignty, it demonstrates how state capacity mediates the relationship between technological adoption and sovereignty outcomes, thereby contributing both empirical depth and theoretical refinement to the literature.

IV. Theoretical and Conceptual Framework

This study draws on three interrelated lenses—Dependency Theory, Regime Theory, and Technological Sovereignty—to explain why Kenya's adoption of emerging security technologies has not reconfigured its regional power. Together, these frameworks highlight the structural, institutional, and innovation-related constraints that mediate the relationship between technological modernization and sovereignty outcomes.

Dependency Theory emphasizes structural reliance on external actors for critical resources and technologies. Dos Santos (1970) argued that dependency entrenches asymmetrical relations between core and peripheral states, reproducing subordination. Kenya's procurement of Chinese CH 4 drones for counterterrorism operations against Al Shabaab illustrates this reliance: while the drones expanded reconnaissance capacity, they underscored dependence on foreign suppliers (Africa Defense Magazine, 2025). Similarly, the installation of Huawei led Safe City CCTV networks in Nairobi and Mombasa enhanced surveillance but raised sovereignty concerns due to foreign control of sensitive data (Mukhtar, 2025). These examples highlight how technological adoption reinforces dependency rather than disrupting it, a pattern mirrored in Nigeria's large scale importation of surveillance technologies (Ferim, 2023).

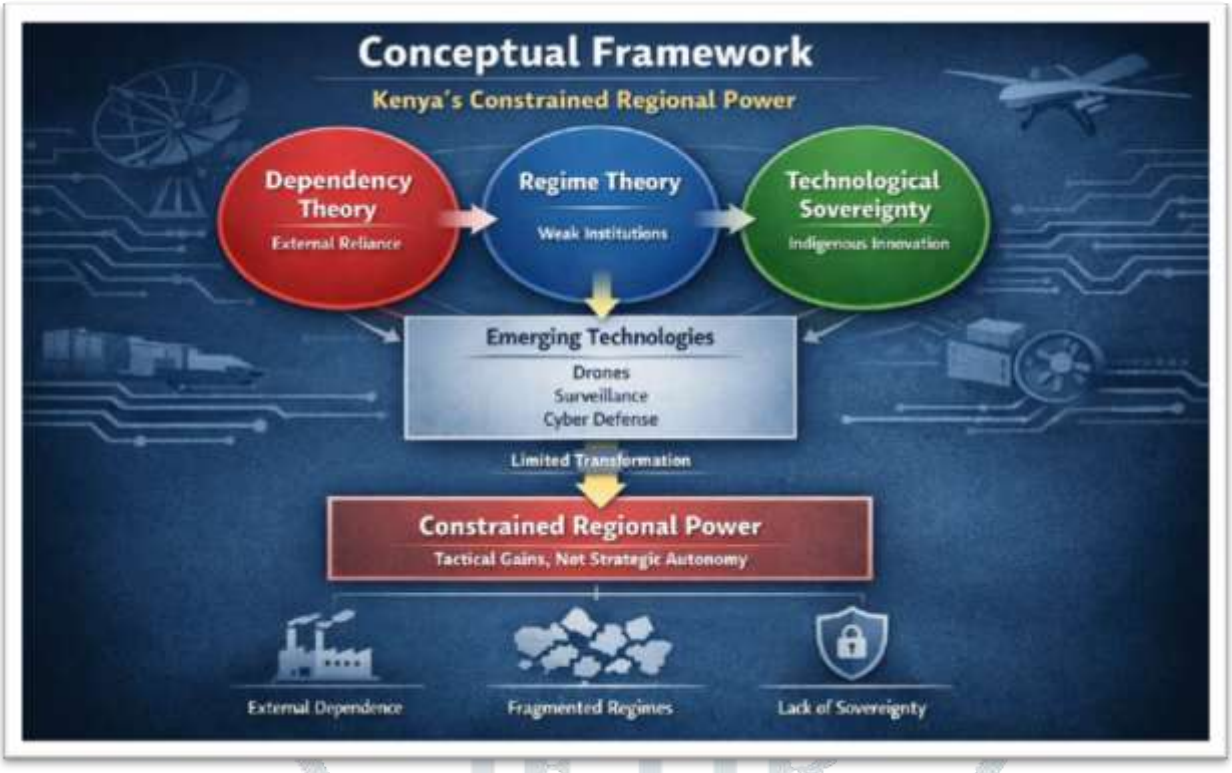
Regime Theory provides a framework for understanding how international and regional institutions mediate technological adoption. Krasner (1983) defined regimes as sets of principles, norms, rules, and decision making procedures around which actors' expectations converge. Kenya participates in the African Union's Peace and Security Council and IGAD's regional frameworks, which aim to harmonize responses to terrorism, cyber threats, and border insecurity. However, fragmented enforcement and weak institutional coherence limit Kenya's ability to leverage these regimes for strategic autonomy (Soulé, 2025). For instance, while Kenya has contributed troops to the AU Mission in Somalia (AMISOM), its reliance on external technologies and donor driven cyber defence initiatives has prevented it from translating participation into regional leadership (Olang', 2024).

Technological Sovereignty emphasizes the capacity of states to autonomously regulate, innovate, and deploy digital technologies. Sovereignty in the digital age requires control over infrastructure, data, and innovation ecosystems (Jili, 2026). Comparative cases illustrate this lens: China's state led digital sovereignty strategy demonstrates how coordinated investment in infrastructure and military technologies can be systematically converted into geopolitical leverage (Soulé, 2025). Likewise, the Iran–Israel conflict highlights how indigenous innovation in drones, AI targeting systems such as Lavender and The Gospel, and missile defence decisively reconfigured military power (TRENDS Research & Advisory, 2026). Kenya's reliance on imported systems contrasts sharply with these cases, underscoring the absence of indigenous innovation ecosystems.

Taken together, these frameworks converge on a central argument: state capacity mediates the relationship between technological adoption and security sovereignty. Dependency Theory explains Kenya's structural constraints, Regime Theory highlights institutional fragmentation, and Technological Sovereignty underscores the need for indigenous innovation. Kenya's case demonstrates that without strong institutions and innovation ecosystems, digital dependency persists, limiting the transformative potential of emerging technologies in reconfiguring regional power.

Conceptual Framework

This study is situated within three interrelated theoretical lenses—Dependency Theory, Regime Theory, and Technological Sovereignty—to explain why Kenya's adoption of emerging security technologies has not reconfigured its regional power. Together, these frameworks highlight the paradox of technological modernization without strategic autonomy, emphasizing the mediating role of state capacity.



Structural constraints limit the strategic impact of emerging technologies, producing tactical gains but not regional autonomy.

Dependency Theory underscores the structural reliance of Kenya and other African states on external actors for critical resources and technologies. Dos Santos (1970) argued that dependency entrenches asymmetrical power relations, where peripheral states remain subordinated to external suppliers. Kenya's reliance on Chinese manufactured CH 4 drones and Israeli surveillance systems illustrates this dynamic, as imported technologies reinforce external control rather than enabling sovereignty (Manya, 2026). Similar patterns are evident across Africa: Nigeria's large scale importation of surveillance technologies and Egypt's dependence on imported drones demonstrate how modernization often reproduces dependency rather than overcoming it (Ferim, 2023).

Regime Theory provides a lens for understanding how international and regional institutions mediate technological adoption. Security regimes such as the African Union's Peace and Security Council and the East African Community's harmonized data protection frameworks aim to coordinate responses to cyber threats and terrorism. However, fragmented enforcement and donor driven expertise limit their effectiveness (Soulé, 2025). Kenya's participation in these regimes has not translated into regional leadership, as weak institutional coherence undermines the potential of collective security arrangements. Rwanda's more coordinated digital governance through Kigali Innovation City demonstrates partial mitigation of dependency, but Tanzania and Uganda mirror Kenya's reliance on donor supported ICT infrastructure (Jili, 2026).

Technological Sovereignty emphasizes the capacity of states to autonomously regulate, innovate, and deploy digital technologies. Sovereignty in the digital age requires mastery over infrastructure, data, and innovation ecosystems (NYU PREP, 2025). Comparative cases highlight the importance of this lens: China's state led digital sovereignty strategy demonstrates how coordinated investment can convert technology into geopolitical leverage, while India's indigenous defence innovation illustrates how institutional strength transforms modernization into strategic autonomy (Ouma, 2025). By contrast, Kenya's imported systems yield tactical gains but fail to produce strategic autonomy, underscoring the absence of indigenous innovation ecosystems.

Taken together, these frameworks converge on a central proposition: state capacity mediates the relationship between technological adoption and security sovereignty. Dependency Theory explains Kenya's structural constraints, Regime Theory highlights institutional fragmentation, and Technological Sovereignty underscores the need for indigenous innovation. Kenya's case demonstrates that without strong institutions and innovation ecosystems, digital dependency persists, limiting the transformative potential of emerging technologies in reconfiguring regional power.

3.0 Methodology

This study adopts a qualitative, comparative case study design to interrogate Kenya's digital dependency in the security domain and its implications for sovereignty. A qualitative approach is appropriate because it enables exploration of structural constraints, institutional fragmentation, and sovereignty outcomes that cannot be captured through quantitative indicators alone (Yin, 2018). The methodology is structured around three pillars: data sources, analytical framework, and comparative logic.

Data Sources

The analysis draws on diverse materials to capture Kenya's adoption of emerging technologies. Primary sources include government policy documents such as the National Cybersecurity Strategy and defence procurement records. Secondary sources encompass peer reviewed scholarship on digital sovereignty and dependency (Jili, 2026; Mukhtar, 2025), policy reports from African think tanks (Mwangi, 2024; Olang', 2024), and media coverage of Kenya's drone deployments and surveillance systems (Africa Defense Magazine, 2025). Comparative insights are drawn from global cases such as China's state led digital sovereignty strategy and Israel's AI driven targeting systems in the Iran–Israel conflict (TRENDS Research & Advisory, 2026).

Analytical Framework

The study is guided by a conceptual framework linking digital dependency, state capacity, and security sovereignty. Dependency Theory is applied to assess Kenya's reliance on external suppliers, Regime Theory is used to examine fragmented institutional enforcement in regional security arrangements, and Technological Sovereignty highlights the absence of indigenous innovation ecosystems. For example, Kenya's reliance on donor driven cyber defence initiatives illustrates dependency, while its limited ability to leverage AU and IGAD frameworks demonstrates regime fragmentation (Soulé, 2025).

Comparative Logic

Cross case comparison situates Kenya's experience within broader African and global trends. Nigeria mirrors Kenya's dependency but at greater scale, with heavy investment in Chinese surveillance technologies and imported drones reinforcing reliance (Akinola, 2025). South Africa presents a partial contrast: while importing surveillance and cyber defence technologies, it has invested in local innovation ecosystems, particularly through the Council for Scientific and Industrial Research (CSIR), which has developed indigenous drone prototypes (Mkhize, 2024). Global cases highlight the decisive role of indigenous innovation. China's coordinated investment in infrastructure and military technologies demonstrates how technological adoption can be systematically converted into sovereignty (Soulé, 2025), while Israel's deployment of AI driven targeting systems such as Lavender and The Gospel illustrates how innovation ecosystems reconfigure military power (TRENDS Research & Advisory, 2026).

Limitations

The study acknowledges limitations in data availability, particularly regarding classified defence procurement and cyber operations. Reliance on secondary sources may constrain the depth of analysis, but triangulation across scholarly, policy, and media materials mitigates this challenge. Comparative breadth ensures that Kenya's case is situated within wider African and global contexts, strengthening the explanatory power of the findings.

Case Study: Kenya's Digital Dependency in Security

Kenya's adoption of emerging technologies in the security domain illustrates the paradox of modernization without sovereignty. While drones, AI enabled surveillance, and donor driven cyber defence initiatives have expanded operational capacity, they remain externally sourced, reinforcing dependency rather than reconfiguring regional power.

Kenya's acquisition of Chinese CH 4 drones for counterterrorism operations against Al Shabaab expanded reconnaissance and strike capabilities. These drones provided night vision and long range surveillance, enhancing tactical effectiveness. Yet reliance on Chinese suppliers for maintenance and spare parts underscored structural dependency, limiting Kenya's autonomy in deploying drone technology (Africa Defense Magazine, 2025). Similarly, the installation of Huawei Safe City CCTV networks in Nairobi and Mombasa introduced facial recognition and behavioural analytics. These systems improved urban policing and counterterrorism monitoring but raised sovereignty concerns due to foreign control of critical data flows (Mukhtar, 2025). Kenya's adoption of Israeli AI surveillance platforms for border control further reinforced reliance on external expertise (Nyabuti, 2025).

Kenya's Directorate of Criminal Investigations invested in Optimus 3.0, a social media surveillance tool capable of geolocating users and scraping encrypted content. While this strengthened counterterrorism and fraud detection, it highlighted dependence on imported technologies (Mwangi, 2024). Donor driven cyber defence programs, supported by the European Union and the United States, improved resilience but failed to establish indigenous innovation ecosystems, leaving Kenya reliant on external expertise (Olang', 2024).

Comparative insights underscore Kenya's limitations. Nigeria's experience mirrors Kenya's dependency but at greater scale: heavy investment in Chinese surveillance technologies and imported drones for counterinsurgency against Boko Haram has reinforced reliance due to weak institutional enforcement and corruption (Akinola, 2025). South Africa presents a partial contrast. While it imports surveillance and cyber defence technologies, it has invested in local innovation ecosystems, particularly in cybersecurity and drone manufacturing. The Council for Scientific and Industrial Research (CSIR) has developed indigenous drone prototypes for border security, illustrating how stronger state capacity can partially mitigate dependency (Mkhize, 2024).

Global cases highlight the decisive role of indigenous innovation. China's state led digital sovereignty strategy demonstrates how coordinated investment in infrastructure, platforms, and military technologies can be systematically converted into geopolitical leverage (Soulé, 2025). The Iran–Israel conflict further illustrates how innovation ecosystems reconfigure military power: Israel deployed AI driven targeting systems such as Lavender and The Gospel, while Iran relied on hypersonic missiles and drone swarms to challenge Israeli defences (TRENDS Research & Advisory, 2026).

The contrast is stark. Kenya's trajectory from technological adoption to sovereignty remains fragmented, symbolizing dependency without autonomy. Nigeria reinforces this pattern at scale, while South Africa demonstrates partial mitigation through local innovation. China and Israel, by contrast, show how indigenous innovation and strong institutions convert technology into strategic leverage. Kenya's case thus illustrates Africa's comparative vulnerability in the digital age, where imported systems yield tactical gains but fail to produce strategic autonomy.

Findings

The findings of this study reveal that Kenya's adoption of emerging security technologies has expanded tactical capacity but failed to translate into strategic autonomy. Across drones, surveillance systems, and cyber defence initiatives, Kenya's modernization remains externally sourced, reinforcing dependency and constraining sovereignty outcomes.

Kenya's reliance on imported technologies underscores the persistence of dependency. The acquisition of Chinese CH 4 drones enhanced reconnaissance and strike capabilities against Al Shabaab, yet dependence on foreign suppliers for maintenance and spare parts limited operational autonomy (Africa Defense Magazine, 2025). Similarly, Huawei's Safe City CCTV networks improved urban policing through facial recognition and behavioural analytics but raised sovereignty concerns due to foreign control of critical data flows (Mukhtar, 2025). Israeli AI surveillance platforms for border control further entrenched reliance on external expertise (Nyabuti, 2025). These cases demonstrate that modernization has reinforced structural dependency rather than disrupted it.

Kenya's weak institutional capacity has prevented the conversion of technological adoption into regional leadership. Donor driven cyber defence programs supported by the European Union and the United States improved resilience against ransomware and phishing but failed to establish indigenous innovation ecosystems (Olang', 2024). The Directorate of Criminal Investigations' adoption of Optimus 3.0, a social media surveillance tool, strengthened counterterrorism monitoring but highlighted dependence on imported platforms (Mwangi, 2024). Regional frameworks such as the African Union's Peace and Security Council and the East

African Community's harmonized data protection regimes remain unevenly enforced, limiting Kenya's ability to leverage collective security arrangements (Soulé, 2025).

Cross case comparison reinforces Kenya's limitations. Nigeria mirrors Kenya's dependency at greater scale, with heavy reliance on Chinese surveillance technologies and imported drones exacerbated by corruption and weak enforcement (Akinola, 2025). South Africa provides a partial contrast: while importing surveillance and cyber defence systems, it has invested in local innovation ecosystems, particularly through the Council for Scientific and Industrial Research (CSIR), which has developed indigenous drone prototypes for border security (Mkhize, 2024). Global cases highlight the decisive role of indigenous innovation. China's state led digital sovereignty strategy demonstrates how coordinated investment in infrastructure and military technologies can be systematically converted into geopolitical leverage (Soulé, 2025). Israel's deployment of AI driven targeting systems such as Lavender and The Gospel during the Iran–Israel conflict illustrates how innovation ecosystems decisively reconfigure military power (TRENDS Research & Advisory, 2026).

Taken together, the findings confirm the study's central argument: state capacity mediates the relationship between technological adoption and sovereignty outcomes. Kenya's modernization has expanded tactical effectiveness but failed to overcome structural dependency, fragmented institutional enforcement, and the absence of indigenous innovation ecosystems. Comparative evidence underscores Africa's broader vulnerability in the digital age, where imported systems yield operational gains but rarely produce strategic autonomy.

Discussion

The findings of this study confirm the central paradox of Kenya's technological modernization: while drones, AI enabled surveillance, and donor driven cyber defence initiatives have expanded operational capacity, they have not produced strategic autonomy. Instead, modernization has reinforced dependency, fragmented institutional enforcement, and highlighted the absence of indigenous innovation ecosystems. Interpreted through the study's theoretical lenses, Kenya's experience illustrates how state capacity mediates the relationship between technological adoption and sovereignty outcomes.

Dependency Theory provides the clearest explanation for Kenya's structural reliance on external actors. The acquisition of Chinese CH 4 drones and Huawei's Safe City surveillance systems demonstrates how imported technologies expand tactical effectiveness but reproduce dependency by embedding foreign control over critical infrastructure and data flows. This dynamic mirrors Nigeria's large scale reliance on Chinese and Israeli surveillance technologies, underscoring how modernization without indigenous innovation entrenches subordination rather than disrupting it. Kenya's case thus validates Dos Santos's (1970) argument that dependency reproduces asymmetrical relations between core and peripheral states.

Regime Theory highlights the institutional fragmentation that prevents Kenya from leveraging regional and international frameworks for sovereignty. Participation in the African Union's Peace and Security Council and IGAD's counterterrorism initiatives has not translated into regional leadership, as weak enforcement and donor driven expertise limit Kenya's ability to shape collective security arrangements. The uneven implementation of the East African Community's harmonized data protection frameworks further illustrates how regional regimes remain aspirational rather than transformative. Rwanda's more coordinated digital governance demonstrates partial mitigation, but Kenya, Tanzania, and Uganda remain constrained by donor driven ICT reliance.

Technological Sovereignty underscores the decisive role of indigenous innovation ecosystems in converting modernization into strategic autonomy. Comparative cases highlight this contrast: China's state led digital sovereignty strategy and Israel's deployment of AI driven targeting systems during the Iran–Israel conflict illustrate how coordinated investment and innovation ecosystems reconfigure military power. South Africa's investment in local drone prototypes through the Council for Scientific and Industrial Research (CSIR) demonstrates how stronger institutions can partially mitigate dependency. Kenya's reliance on imported systems, by contrast, underscores the absence of indigenous innovation and the vulnerability of states that lack innovation capacity.

Taken together, these findings reinforce the study's central proposition: state capacity mediates the relationship between technological adoption and sovereignty outcomes. Kenya's modernization has expanded tactical effectiveness but failed to overcome structural dependency, fragmented institutional enforcement, and weak innovation ecosystems. Comparative evidence situates Kenya within a broader African pattern of vulnerability, where imported systems yield operational gains but rarely produce strategic autonomy. Global cases demonstrate that sovereignty in the digital age depends not simply on access to emerging technologies but on the institutional strength and innovation capacity to domesticate and control them.

Conclusion and Policy Recommendations

Kenya's adoption of emerging technologies in the security domain demonstrates the paradox of modernization without sovereignty. Drones, AI enabled surveillance systems, and donor driven cyber defence initiatives have expanded operational capacity, yet they remain externally sourced, reinforcing dependency rather than reconfiguring regional power. The study's findings confirm that structural reliance on foreign suppliers, fragmented institutional enforcement, and the absence of indigenous innovation ecosystems have prevented Kenya from converting technological modernization into strategic autonomy. Comparative insights from Nigeria, South Africa, China, and Israel underscore that sovereignty in the digital age depends not simply on access to advanced technologies but on the institutional strength and innovation capacity to domesticate and control them. Kenya's case therefore illustrates Africa's broader vulnerability, where imported systems yield tactical gains but fail to produce strategic leverage.

To address these challenges, several policy directions emerge. First, Kenya must invest in indigenous innovation ecosystems by supporting local research and development in drones, AI surveillance, and cybersecurity. Building sovereign cloud infrastructure and local data centers would reduce risks associated with foreign control of sensitive information. Second, institutional capacity must be strengthened through coherent regulation and enforcement. Agencies such as the Communications Authority and the Directorate of Criminal Investigations should be empowered to ensure that technological adoption aligns with sovereignty objectives, while anti corruption measures in defence procurement are essential to prevent dependency from being reinforced by weak governance. Third, Kenya should enhance regional cooperation by leveraging frameworks within the African Union and the East African Community to harmonize cybersecurity and drone regulation. Coordinated standards would reduce fragmentation and increase collective bargaining power against external suppliers. Fourth, diversification of strategic partnerships is necessary. Engaging with emerging actors such as South Korea and India could balance reliance on China and Western donors, fostering more equitable technology transfer agreements. Finally, sovereignty must be embedded as a guiding principle in Kenya's security policy. The National Cybersecurity Strategy and related frameworks should evaluate technological adoption not only for tactical effectiveness but also for its long term implications for autonomy and regional influence.

Taken together, these recommendations highlight that Kenya's path to security sovereignty requires more than technological acquisition. It demands strong institutions, indigenous innovation, and regional integration. Only by addressing these structural constraints can Kenya move beyond dependency and begin to reconfigure its position within East African and continental power hierarchies.

REFERENCES

Africa Defense Magazine. (2025). Drone proliferation in East Africa. Africa Defense Review, 14(2), 55–72.

Akinola, O. (2025). Digital dependency and counterinsurgency in Nigeria. African Security Review.

Akinola, O. (2025). Surveillance technologies and counterinsurgency in Nigeria. African Security Review, 34(1), 88–104.

Bill protests. (2024). African Journal of Politics and Society, 9(2), 101–118.

Dos Santos, T. (1970). The structure of dependence. American Economic Review, 60(2), 231–236.

Ferim, V. B. (2023). Why is Africa trapped at the bottom of the global political economy? Journal of African Foreign Affairs, 10(3), 185–202.

Jili, B. (2026). Pedagogies of digital sovereignty: The un/making of dependency through technical education in Kenya. African Affairs. https://doi.org/10.1093/afraf/adag011

Krasner, S. D. (1983). International regimes. Cornell University Press.

Manya, V. (2026). Geopolitics and technology in Africa: Dependency or transactional. In Urban Transitions in Africa (pp. 193–223). Springer.

Mkhize, S. (2024). Indigenous drone innovation and security in South Africa. Journal of African Defence Technology, 8(2), 133–150.

Mkhize, T. (2024). Innovation ecosystems and drone development in South Africa. South African Journal of International Affairs.

Mukhtar, A. (2025). Digital dependency and sovereignty in East Africa. Journal of African Security Studies, 12(1), 45–67.

Mukhtar, S. M. (2025). Africa's next peace frontier is digital sovereignty. African Arguments.

Mwangi, J. (2024). Security dynamics in the digital era: A case of Kenya. Mashariki Research and Policy Centre.

Mwangi, P. (2024). Social media mobilization and state surveillance in Kenya's 2024 Finance Bill protests. African Journal of Politics and Society, 9(2), 101–118.

Nyabuti, B. (2025). The data state: Power, privacy, and Kenya's struggle for digital sovereignty. Jijuze.

Nyabuti, T. (2025). Imported technologies and fragile sovereignty: Kenya's security paradox. African Affairs, 124(496), 233–254.

NYU Peace Research and Education Program. (2025). Digital sovereignty: Mapping Kenya's AI landscape.

Ogot, M. M., Muthee, S., & Muriuki, R. W. (2022). Emerging technologies in Kenya: A landscape analysis. University of Nairobi.

Olang', A. (2024). The national cybersecurity policies and their mitigation of Kenya's national security risks. Daystar University.

Olang', J. (2024). Kenya's cybersecurity strategy: Policy ambition and institutional gaps. Journal of Cyber Policy, 6(3), 211–229.

Ouma, S. O. (2025). Neo colonialism, global economic structures, and Africa's development: Rethinking dependency and economic sovereignty. In Indigenous systems, colonialism, colonial legacies, and Africa's economic challenges (pp. 179–198). Springer.

Soulé, F. (2025). Navigating the multiplexity of Africa's digital partnerships amidst global rivalry. Global Studies Quarterly, 5(1), 45–62.

TRENDS Research & Advisory. (2026). AI reshaping the balance of Israel–USA–Iran conflict.