SADI Journal of Interdisciplinary Research
ISSN: 2837-1976| Impact Factor : 7.01
Volume. 12, Number 2; April-June, 2025;
Published By: Scientific and Academic Development Institute (SADI)
8933 Willis Ave Los Angeles, California
https://sadijournals.org/index.php/sjir|editorial@sadijournals.org

EMERGING TECHNOLOGIES AND THEIR IMPLICATIONS ON AFRICA'S SECURITY ARCHITECTURE

Oluyemi, Opeoluwa Adisa (PhD)
Senior lecturer in the Department of Political Science and International Relations, Achievers University, Owo, Ondo State, Nigeria.
Email: opeoluyemio@gmail.com
DOI:https://doi.org/10.5281/zenodo.15754403

Abstract: Emerging technologies such as Artificial Intelligence (AI), Blockchain (BCT), and the Internet of Things (IoT) hold significant promise for driving economic transformation in developing nations. While many developed economies are already taking initiatives for the effective implementation of these technologies by investing in skills training, improving digital infrastructure, and setting regulatory frameworks, African countries offer unique insights into how these technologies can be applied to meet urgent local needs and advance sustainable development goals. Across the continent, innovative uses of AI, blockchain, and IoT applications are helping to tackle critical challenges in areas like agriculture, healthcare, energy, and public safety. These applications not only promote socioeconomic progress but also align with broader efforts to create inclusive and resilient societies. However, the integration of such technologies also introduces complex risks, including digital insecurity, regulatory gaps, and ethical concerns that must be carefully managed. This study adopts a qualitative research approach grounded in secondary data to explore how emerging technologies are being incorporated into Africa's evolving security architecture. This study analyzes the implications of these tools on national and regional security systems, highlights both the opportunities and vulnerabilities they bring, and offers policy recommendations aimed at maximizing their benefits while minimizing associated threats. The goal is to provide practical guidance for using technology as a catalyst for strengthening African security architecture in a way that is sustainable, inclusive, and forward-looking.

Keywords: Emerging Technologies, Artificial Intelligence (AI), Africa's Security Architecture, Critical Security Studies (CSS), Fourth Industrial Revolution (4IR), Internet of Things (IoT)

Introduction

In today's digital age, nearly every aspect of political life is being shaped by the increasing influence of information technologies. Political scientists are not only employing digital tools in their research but are also critically examining the ways these technologies impact political processes both domestically and internationally. The interconnectedness of digital innovation and international relations, particularly in the realm of warfare, has attracted significant academic interest. The growing use of technologies such as cyber capabilities and unmanned aerial vehicles (drones) by both state and non-state actors is reshaping the nature of conflict and has become a

focal point of scholarly debate. As Horowitz (2020) notes, cyber and drone technologies are increasingly central to modern conflict strategies, while advancements in artificial intelligence (AI) are anticipated to play a major role in redefining the future of warfare. We are entering a transformative period marked by a wave of emerging technologies, such as AI, robotics, automation, 3D printing, deepfake media, and blockchain that are beginning to influence all corners of society. These innovations are not only changing how societies function but also altering the foundational dynamics of international politics. Their implications stretch across multiple dimensions: they are poised to shift the global balance of power, influence the structures and cohesion of alliances and security organizations, and redefine the ways states control information and engage in economic and military competition (Horowitz, 2020; Allen & Chan, 2017).

Moreover, these technologies challenge traditional notions of state sovereignty and governance. They raise pressing questions about how national interests are defined, how political accountability is maintained, and the extent to which human decision-making continues to guide the escalation of conflicts. As Steff, Burton, and Soare (2021) emphasized, such developments may redefine the relationship between governments and their citizens, potentially undermining the state's exclusive authority over the legitimate use of force. The rapid evolution of emerging technologies has significantly influenced global security frameworks, and Africa is increasingly implicated in these shifting paradigms. Technologies such as artificial intelligence (AI), unmanned aerial vehicles (UAVs), blockchain, and advanced cyber systems are not only transforming economic and governance structures but are also redefining the landscape of international security across the continent. These technologies promise new tools for enhancing surveillance, border management, electoral transparency, and conflict monitoring (Turianskyi & Bornman, 2021). For instance, AI-driven predictive analytics and drones are now used in counterterrorism operations and peacekeeping missions, contributing to operational efficiency and risk reduction. According to Distor et al. (2023), emerging technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), and Blockchain Technology (BCT) are poised to significantly enhance the economic advancement of developing nations, offering opportunities to bypass the traditional stages of industrial development. These frontier technologies are not only reshaping business models but also introducing substantial organizational disruptions. IoT, for instance, connects physical objects ranging from everyday devices like smartphones to advanced machinery into digital networks that gather and transmit data, which can subsequently be analyzed and stored using AI and blockchain systems. The integration of IoT applications such as home automation and wearable technologies, is becoming increasingly prevalent. These innovations contribute to energy conservation and health monitoring, with wearable devices offering real-time, noninvasive tracking that supports individual well-being. IoT also plays a growing role in digital governance, particularly in areas like environmental management, smart city development, healthcare, transportation, public safety, commerce, and agricultural supply chain optimization, enhancing productivity and operational performance. Artificial intelligence, which is characterized by machines that learn from and adapt to data, facilitates the automation of complex tasks with minimal human intervention. Its applications are expected to transform public administration and societal systems by addressing unresolved challenges in digital governance. For example, AI-powered chatbots enable governments to respond promptly to public inquiries around the clock. In urban management, AI can aid in forecasting and mitigating natural disasters. Similarly, in agriculture, machine learning is being used for predictive tasks, such as identifying crop diseases and analyzing weather patterns, for more efficient farming practices.

At the continental level, Africa demonstrates how these technologies can address pressing community needs while supporting the realization of sustainable development goals. IoT is being used in rural areas to monitor water usage via sensors and smart meters, promoting conservation efforts. In agriculture, data captured by IoT devices are fed into AI systems to optimize crop management and yield. Moreover, blockchain technology is gaining traction in supply chain management; a notable example is its use in Ethiopia's coffee industry. Two firms collaborated to apply blockchain in tracking the entire journey of unprocessed coffee beans from harvesting and roasting to packaging and export, ensuring transparency and maximizing local economic retention. Importantly, many of these innovations emanated from grassroots initiatives, reflecting a bottom-up approach to technological adoption in Africa (Distor et al., 2023).

However, the adoption of such technologies also introduces new vulnerabilities. Africa's growing digital infrastructure remains uneven, with significant cybersecurity capability gaps, making state and non-state actors increasingly susceptible to cyber threats, digital espionage, and misinformation campaigns (Chikane, 2020). The manipulation of public discourse through AI-powered bots or deepfakes threatens electoral integrity and social cohesion. Moreover, external technological dependencies, especially reliance on foreign cybersecurity infrastructure and AI platforms, could compromise national sovereignty and increase geopolitical vulnerabilities (Mumo, 2022). Furthermore, the dual-use nature of many of these technologies complicates regulatory responses. Blockchain, for example, can bolster financial inclusion and transparent governance, but it can also facilitate illicit transactions and the evasion of financial oversight. Similarly, drones can be deployed for humanitarian surveillance or weaponized by insurgent groups. As such, this research argues that African governments and regional institutions must adopt comprehensive, forward-looking security strategies that account for both the benefits and risks of emerging technologies. To ensure sustainable and resilient security architectures, it is essential to foster multi-stakeholder cooperation, build indigenous technological capacities, and invest in robust cybersecurity governance. Africa's position in the global technology order will depend not only on adoption but also on strategic regulation, local innovation, and integration into continental policy frameworks like the African Union's Digital Transformation Strategy 2020–2030. This research explores how emerging technologies are being incorporated into African security architecture. This study analyzes the implications of these tools on national and regional security systems, highlights both the opportunities and vulnerabilities they bring, and offers policy recommendations aimed at maximizing their benefits while minimizing associated threats.

Theoretical Framework: Critical Security Studies (CSS)

Conventional understandings of security that primarily centered on state sovereignty and military defense (state-centric approach) are increasingly being questioned in today's complex global environment. Nowhere is this shift more apparent than in Africa, where security threats have evolved to encompass not only armed conflict but also governance issues, social inequality, human rights violations, and the disruptive effects of rapidly emerging technologies. Critical Security Studies (CSS), a progressive school in the broader field of security studies, provides a robust framework for analyzing these multifaceted challenges. Unlike traditional security paradigms that prioritize the state, CSS redefines the concept of security by focusing on individual security, communities, and the underlying power structures that frame security narratives. This theoretical framework explores how CSS offers valuable insights into the implications of emerging technologies, such as artificial intelligence, cyber tools, biometric systems, and drone surveillance, on Africa's security architecture. By interrogating how security is constructed and whose interests are served, CSS enables a deeper critique of how these technologies affect

sovereignty, intensify inequality, and impact democratic governance. The aim is to demonstrate how CSS can support more inclusive, equitable, and human-centered approaches to security policy across the African continent.
In understanding CSS as a paradigm shift in security studies, Critical Security Studies emerged as a response to the limitations of traditional security theories, particularly those rooted in Cold War thinking that emphasized national defense and inter-state conflict. Pioneered by thinkers such as Ken Booth, CSS argued that true security involves emancipation and freedom from both physical threats and structural violence. In contrast to fixed definitions of threats, CSS treats security as a contested and socially constructed concept that must be analyzed in terms of power relations, discourse, and historical context. This framework is especially relevant for Africa, where dominant security narratives are often influenced by colonial legacies, international aid conditions, and elite political interests. Instead of merely identifying external threats, CSS urges scholars and policymakers to ask critical questions: Who defines threats? Who benefits from prevailing security policies? How do these policies impact the most vulnerable populations?
To explain cybersecurity and state surveillance in the African context, it is noted that as digital technologies spread across the continent, African states are grappling with a new frontier of security risks, such as cybercrime, digital espionage, and cyberterrorism. However, instead of solely addressing these threats, many governments have used cybersecurity as a justification for expanding their digital surveillance capabilities. These systems, often sourced from international vendors, are deployed to monitor opposition figures, restrict online activism, and limit press freedom. Through the lens of CSS, such practices are not viewed as neutral or purely defensive. Rather, they reflect deeper power dynamics in which technology becomes a tool for consolidating political control. In South Africa, for example, Warricker (2005) highlighted how information networks, while vital for economic and social development, are increasingly exposed to breaches and manipulation, government responses often prioritize elite security over citizen privacy (Warricker, 2005). CSS challenges this approach by emphasizing the need for rights-based digital governance and transparent, accountable cybersecurity policies.
Furthermore, to expound the politics of drone use and militarized technologies, it has been argued that the adoption of drone technologies across various African countries is a clear example of how emerging tools are reshaping the continent's security architecture. Drones are now used for border surveillance, crowd control, counterterrorism, and even environmental monitoring. However, deployment often occurs with minimal oversight, raising concerns about legality, accountability, and misuse. Muriungi and colleagues (2021) observed that while drones present strategic benefits, especially in areas where traditional infrastructure is lacking, their control and technical standards are frequently dictated by foreign powers, limiting local autonomy (Muriungi et al., 2021). CSS interrogates the motivations behind drone use: Are they genuinely enhancing public safety, or are they being used to reinforce authoritarian governance, monitor marginalized communities, and suppress dissent? By focusing on the lived experiences of those most affected often rural populations or political minorities, CSS draws attention to the broader societal implications of these militarized technologies.
In addition, from state security to human-centered approaches, a core contribution of CSS is its commitment to human security defined not by the protection of borders but by the well-being, dignity, and rights of individuals. This perspective is especially pertinent in Africa, where many security threats are internal and rooted in socioeconomic inequalities rather than external aggression. Domson-Lindsay (2015) underscored how the African Union (AU), by transitioning from the Organization of African Unity (OAU), has embraced the concept of "responsible sovereignty." This approach supports the idea that state legitimacy is tied not only to territorial

control, but also to how well a government ensures the safety and rights of its people (Domson-Lindsay, 2015). CSS provides a theoretical foundation for such a shift, particularly in the governance of biometric systems used in elections and national identification programs. These technologies can improve state capacity, but if poorly implemented, they may exclude already marginalized populations. CSS calls for the design and application of such systems to be critically examined for their impact on social justice and inclusivity.

In expounding on global influence and technological dependency, this is considered another important dimension addressed by CSS: the geopolitical context in which security technologies are adopted. African states are not merely passive recipients of technology; they operate within a global system in which power asymmetries shape the availability, terms, and implications of technology deployment. Countries such as China and the United States are increasingly exporting surveillance infrastructure and digital governance models to Africa, often under the guise of development aid or counterterrorism support. Nganje and Ndawana (2020) argued that these external interventions are frequently motivated more by geopolitical interests than by genuine concern for African security needs (Nganje & Ndawana, 2020). From a CSS viewpoint, this dynamic illustrates how security can be "securitized" to serve elite agendas, both domestic and foreign, rather than addressing the real, everyday insecurity faced by African communities. By deconstructing the narratives that justify technological adoption, CSS advocates for African sovereignty and agency when defining the continent's technological future.

To understand the institutional potential and CSS Integration, it is notably argued that, while the African Union has made significant progress in establishing continent-wide security frameworks such as the African Peace and Security Architecture (APSA) and the Conference on Security, Stability, Development and Cooperation in Africa (CSSDCA), their implementation remains uneven. Political divisions, limited funding, and weak institutional capacity often undermine coordinated actions. Franke (2007) pointed out that regional rivalries and overlapping organizational mandates have created inefficiencies that hinder Africa's ability to respond to complex security threats (Franke, 2007). CSS-informed critique can help refine these institutions by promoting participatory governance, inclusivity, and transparency. Empowering civil society organizations, engaging marginalized communities, and democratizing policy processes are all ways to align institutional practices with the emancipatory goals of CSS. In conclusion, Critical Security Studies offers a transformative lens through which to assess the impact of emerging technologies on African security. By moving beyond state-centered paradigms and questioning the power structures that shape security narratives, CSS emphasizes human dignity, inclusivity, and emancipation. As Africa navigates the promises and perils of technological advancement, CSS provides both a critique and a guide, a means to build a more equitable and just security landscape that reflects the continent's diverse realities and aspirations.

Historical Evolution of African Security Architecture

Africa's security architecture is deeply influenced by various historical, political, economic, and international developments. The continent's understanding of security has undergone a significant transformation from the legacy of colonialism to modern-day regional cooperation and responses to transnational challenges. Security in Africa cannot be analyzed purely through the lens of inter-state military engagement; it also encompasses broader themes such as human security, the role of state institutions, external interventions, and the emergence of continental organizations like the African Union (AU). This overview explores how Africa's security has developed through three pivotal phases: the colonial and early post-independence period, the Cold War era, the

post-Cold War and post-9/11 context of regionalism, evolving threats, and the advent of technological advancement.

A. Colonial and Post-Independence Security Foundations: Africa's current security architecture has its roots in the colonial era, where the focus was on maintaining colonial order and resource exploitation rather than protecting African populations. Military structures were designed for internal repression and to uphold colonial dominance. As highlighted by Cawthra (2009), these institutions were not built to defend nations or contribute to regional peace, but to sustain foreign rule. Following independence, newly formed African states largely inherited these institutional frameworks, which were ill-suited for the challenges of nation-building. In many countries, security policy has focused on consolidating power and neutralizing opposition, often leading to militarized politics and the rise of authoritarian regimes. Civil strife, coups, and internal conflict were widespread as governments prioritized regime survival over citizen welfare. Williams (2007) noted that this period was characterized by a narrow, state-focused view of security that marginalized broader societal needs.

B. Cold War Era: Ideological Contest and Militarization: during the Cold War, Africa became entangled in the geopolitical rivalry between the United States and the Soviet Union. Many African governments received military aid and training, not based on democratic credentials but due to their alignment with the global ideological struggle. Sage (2010) argued that this fostered authoritarianism and diverted national security systems away from serving the public interest, reinforcing elite power backed by foreign allies. The Wars in Angola, Mozambique and the Horn of Africa exemplified how foreign interventions intensified and prolonged violent conflicts, often at great cost to regional stability. The era also saw little progress in African-led security initiatives. The Organization of African Unity (OAU), established in 1963, remained largely passive in the face of internal crises, adhering to principles of non-intervention that limited its capacity to act during atrocities, such as the Rwandan genocide in 1994.

C. Post-Cold War Shifts and Regional Security Cooperation: with the Cold War's end came a reconfiguration of security concerns in Africa. Conflicts became increasingly internal, often fueled by ethnic divisions, state collapse, and insurgencies that transcended national borders. This approach exposed the inadequacies of a purely state-based security model and generated broader concepts such as human security and regional security governance. The transformation of the OAU into the African Union (AEU) in 2002 marked a significant shift. The AU adopted a more proactive stance on intervention, establishing the African Peace and Security Architecture (APSA), which prioritizes "non-indifference" over the older doctrine of non-interference. As Domson-Lindsay (2015) explains, this new framework permits intervention in member states in circumstances involving war crimes, genocide, or crimes against humanity. The AU also created key institutions such as the Peace and Security Council (PSC), the African Standby Force (ASF), and the Continental Early Warning System (CEWS). These developments marked a shift toward collective responsibility for peace. Regional blocs like ECOWAS, IGAD, and SADC also emerged as important players, leading interventions in countries such as Liberia and Sierra Leone during the 1990s.

D. Post-9/11: Transnational Threats and the Security-Development Nexus: the early 21st century introduced complex new threats to Africa's security, including terrorism, which rose sharply after the 9/11 attacks. Countries such as Kenya, Nigeria, and Mali became flashpoints for terrorist activities involving groups such as Boko Haram, Al-Shabaab, and AQIM. As a result, many African nations became key partners in global counterterrorism efforts and received enhanced military and financial support. However, Kumah-Abiwu (2021)

warned that blending development assistance with counterterrorism—what some call "securitized development" has sometimes come at the expense of human rights. While regimes gained access to security resources, democratic norms and civil liberties were frequently undermined in the name of stability. Africa has also faced a growing range of non-traditional threats, including maritime piracy, cyber threats, pandemics, and the effects of climate change. Piracy in regions like the Gulf of Guinea and off the Horn of Africa has prompted coordinated naval strategies and multilateral cooperation. Vrey (2010) documented how such efforts have created continental maritime frameworks to address these evolving risks.

E. Technological Development: Recent and ongoing technological developments are significantly reshaping African security architecture. These advancements not only redefine the African traditional notion of state-centric security but also enhance the ability of African nations to manage a diverse range of security threats. From conventional military challenges to emerging risks such as cybercrime, countries are increasingly integrating tools like satellite monitoring, drones, biometric systems, cybersecurity technologies, and artificial intelligence into their national and regional security strategies. For example, the deployment of surveillance drones and satellite imagery has significantly improved governments' ability to oversee hard-to-reach regions, strengthening efforts in border control and anti-insurgency campaigns. In parallel, the introduction of biometric identification systems reinforces national ID programs, which are crucial for securing elections and improving the efficiency of law enforcement agencies. Meanwhile, the growing prioritization of cybersecurity reflects an urgent need to counter digital threats, including hacking, disinformation, and cyber espionage, which are becoming more common across the continent.

Digital technologies have also been pivotal in modernizing early warning and crisis response mechanisms. Platforms like the Continental Early Warning System (CEWS) and various regional security hubs now use real-time data analysis and digital communication networks to detect and respond to potential conflicts more rapidly and accurately. In this way, technology has become an essential enabler of initiatives spearheaded by the African Peace and Security Architecture (APSA). Nevertheless, new risks emerge with these benefits. The rapid uptake of digital tools has raised critical concerns about data security, unequal access to technology and potential abuse of surveillance systems by authoritarian regimes. Thus, while technological innovation holds tremendous promise for advancing peace and security across Africa, it is essential that its application be guided by principles of transparency, inclusiveness, and respect for human rights.

Africa Embracing the Fourth Industrial Revolution

The Fourth Industrial Revolution (4IR) brings together a suite of advanced technologies, such as artificial intelligence (AI), robotics, blockchain, the Internet of Things (IoT), and 3D printing, which are fundamentally reshaping the way modern economies operate. These innovations are not only revolutionizing global production and governance systems but are also gaining traction across the African continent as tools for transformative change. According to Signé (2023), the growing implementation of these technologies in Africa underscores the region's potential to leverage digital innovation as a pathway toward inclusive and sustainable development while positioning itself competitively in the evolving global digital economy. Africa has unique demographic and technological advantages that make it particularly suited to benefit from the 4IR. With a predominantly young population, most of whom are digital natives, combined with rapidly expanding mobile phone usage and a vibrant start-up culture, the continent is well-placed to adopt and scale these technologies. These factors create a fertile environment for innovation-driven development that can address long-standing socioeconomic challenges.

In practical terms, many African countries are already applying 4IR technologies in critical sectors, such as agriculture, healthcare, and education. For instance, AI-driven platforms are being used to diagnose diseases more accurately and efficiently, while IoT-enabled smart farming tools help farmers monitor soil health, optimize irrigation, and improve crop yields. In education, digital platforms and virtual learning tools help bridge gaps in access and quality, particularly in remote and underserved communities. Naudé (2017) observed that the strategic deployment of these technologies is already improving productivity, streamlining service delivery, and opening up new avenues for economic participation and empowerment across the continent. In essence, while challenges remain, Africa's engagement with the Fourth Industrial Revolution is no longer a speculative possibility; it is now a growing reality with transformative promise. With the right investments in digital infrastructure, skills development, and policy support, African nations can harness 4IR not just to catch up with the rest of the world, but to innovate and lead in new domains of global relevance.

Africa's engagement with the Fourth Industrial Revolution (4IR) reflects a broader global shift toward leveraging transformative technologies to reshape economies, governance, and social systems. These emerging technologies, including artificial intelligence (AI), blockchain, 5G, drones, and augmented/virtual reality, present profound opportunities and complex risks for peace, development, and security on the continent. Africa has demonstrated a proactive stance in adopting emerging technologies to address infrastructural and service delivery gaps. In Rwanda, drone technology is revolutionizing health care delivery by transporting blood to hard-to-reach rural areas, significantly enhancing public health outcomes and human security (Signé, 2023). Likewise, nations such as Nigeria and Ethiopia are witnessing the rise of domestic AI ecosystems supported by both private and public initiatives. Multinational organizations also contribute to this growth. Google's AI research center in Ghana and the UN Global Pulse Lab in Uganda exemplify this trend, highlighting Africa not only as a recipient but also as a contributor to technological innovation (Phoobane, 2022). These developments point toward a paradigm in which African nations can leapfrog traditional developmental pathways by integrating 4IR tools into governance, health, education, and economic systems.

Despite these gains, the deployment of emerging technology in Africa is not without significant challenges. Globally, AI has been misused for state surveillance, electoral manipulation, and biased policing practices, raising legitimate concerns over ethics, privacy, and human rights (Chemhuru, 2021). In Africa, where regulatory frameworks remain underdeveloped, these risks are amplified, especially in regions with authoritarian tendencies or conflict-prone environments. There is growing concern that African populations, particularly marginalized groups, are vulnerable to exploitation through data collection practices, biometric surveillance, and algorithmic discrimination. These technologies reinforce symbolic violence and entrench existing inequalities, especially when developed externally and deployed without local oversight (Mamphiswana, 2020). The intersection of emerging technologies and peacebuilding in Africa remains underexplored. While 4IR tools, such as AI-driven sentiment analysis, have been employed to anticipate conflict or guide peacekeeping missions, their broader societal implications are insufficiently understood. For instance, the misuse of digital platforms for disinformation and hate speech has fueled communal violence in Nigeria and Ethiopia, revealing how technology can escalate rather than mitigate tensions (Masunda, 2024). Additionally, technologies such as facial recognition and autonomous weapons, which are often introduced through international defense collaborations, risk militarizing African public spaces under the guise of security. These developments mirror colonial-era practices of

domination, whereby technologies tested in the Global South are later adopted in the North, a process described as the "boomerang effect" (Mude et al., 2021).

To fully harness the benefits of the 4IR, Africa must establish inclusive and context-sensitive regulatory frameworks. These should prioritize ethical AI, protect digital rights, and empower local institutions to oversee the deployment of new technologies. Importantly, African voices must be actively included in international dialogs around the governance of AI and emerging technologies, which are currently dominated by actors from the Global North (Ogbu et al., 2021). Building capacity through education, investment in research and development, and support for local entrepreneurship is also key. As noted by Naudé (2017), integrating 4IR principles into African educational and entrepreneurial frameworks can catalyze sustainable economic transformation (Naudé, 2017). Africa's embrace of the Fourth Industrial Revolution presents both transformative possibilities and critical vulnerabilities. While emerging technologies offer tools to drive development, enhance governance, and support peace, they also risk worsening existing inequalities and creating new forms of exploitation. A balanced approach anchored in ethical governance, inclusive policymaking, and regional innovation is essential for 4IR to advance peace and human security on the continent.

Emerging Technologies and African Security Architecture

The adoption of emerging technologies across Africa is transforming the continent's digital landscape, bringing both unprecedented opportunities and complex risks. While many of these technologies, such as artificial intelligence (AI), facial recognition, biometric surveillance, and social media platforms, hold immense potential to advance peacebuilding, enhance governance, and foster socio-economic development, they also pose significant challenges to community stability and national security (Signé, 2023; Shava, 2021). This chapter examines the multifaceted implications of emerging technologies in Africa, especially in terms of electoral interference, community conflict, symbolic violence, colonial governance practices, and AI weaponization. This paper argues for a robust policy framework that prioritizes digital rights, civilian protection, and local agency in technology governance. Emerging technologies present a paradox in Africa: they are not only powerful tools for development and governance but also potent enablers of violence, surveillance, and disinformation. As the continent becomes increasingly digitized, it must confront the realities of underregulation, foreign technological dominance, and the weaponization of digital tools. A concerted effort is needed to enhance domestic regulatory frameworks, increase transparency in foreign partnerships, and elevate African voices in international tech governance. Without such interventions, the promise of technology may be overlooked by its potential to destabilize peace and security.

A. Disinformation and Community Conflict in the Digital Age: social media has become a central player in African electoral processes, influencing political discourse and public perception. In countries like Nigeria, Kenya, Uganda, and Madagascar, disinformation campaigns some allegedly orchestrated by foreign actors such as Russia's Wagner Group and other non-state entities have fueled social unrest, undermined public trust in democratic institutions, and instilled fear and anxiety among citizens (Chaudhry & Otondi, 2018). For example, during Kenya's 2017 elections, data analytics firm Cambridge Analytica deployed micro-targeted psychological operations based on personal data, including ethnicity and religion, to manipulate voter behavior and intensify tribal divisions. Misinformation has also incited violent inter-communal clashes. In Nigeria, doctored images of mass graves circulated online were used to stoke animosity between Fulani Muslims and Berom Christians, resulting in deadly violence. Similar patterns emerged during Ethiopia's Tigray conflict, where recycled visuals

from unrelated geopolitical contexts were used to mislead and provoke unrest. The proliferation of these digital threats is further amplified by the rise of AI-enhanced tools like deepfakes and generative adversarial networks, which allow actors to produce hyperrealistic fake media with minimal resources (Osee, 2024).

B. Algorithmic Threats: Deepfakes, Echo Chambers, and Trust Erosion: AI-driven media manipulation technologies ranging from deepfakes to shallow or "cheap" fakes are increasingly being weaponized by malicious actors in Africa. These tools manipulate audiovisual content to deceive viewers, often promoting false narratives that incite hatred and violence. Once such content is disseminated via trusted social networks, recipients are more likely to accept and redistribute it without verification, thus magnifying its reach and impact. The psychological implications are severe because individuals internalize disinformation that exploits cultural, ethnic, or emotional vulnerabilities (Naudé, 2017). Algorithms used on major platforms such as Facebook, YouTube, and Twitter, also create echo chambers and addictive feedback loops. This has led to the normalization of extremist rhetoric and misinformation, making political and ideological manipulation easier in both virtual and real-world environments.

C. Biometric Surveillance and Symbolic Violence: emerging biometric technologies, such as facial recognition and predictive analytics, are increasingly being deployed in African contexts without appropriate regulatory oversight. These tools are used in various domains, including border security, health services, and financial identification systems. However, the unregulated use of biometric data raises ethical concerns, especially regarding surveillance capitalism and data colonialism (Lubinga et al., 2023). In countries such as Zimbabwe and Uganda, Chinese companies such as Huawei and CloudWalk Technology have implemented facial recognition projects, often without informed consent or transparency. Such deployments can amount to symbolic violence when used to monitor, categorize, or control marginalized populations, particularly when those affected lack knowledge of how their biometric data is collected, stored, or used. This form of digital exploitation deepens existing power asymmetries and erodes civil liberties, especially in authoritarian regimes where surveillance technologies are used for political repression.

D. Technological Colonialism and Autonomous Weapon Systems: The export of advanced surveillance and military technologies from the Global North to Africa reflects a modern iteration of colonial governance practices. The Foucauldian concept of the "boomerang effect" where techniques of domination used in colonial territories are repatriated to the metropole, applies directly to how technologies are tested in African settings before being mainstreamed in Western countries. This is evident in the proliferation of Lethal Autonomous Weapons Systems (LAWS), which are capable of targeting and eliminating individuals without human oversight (Future of Life Institute, 2024). Although African states have not widely adopted LAWS, their use in other conflict zones, such as Gaza and Iran, serves as a forewarning of the future trajectory of warfare. African states are largely excluded from global forums that govern military AI, such as U.S.-led coalitions, limiting their ability to influence ethical frameworks and regulatory norms. The only significant platform on which African voices are nominally present is the UN Group of Governmental Experts on LAWS in Geneva.

E. Invisible Threats: 5G and Conspiracy Theories: the advent of 5G technology has triggered waves of disinformation and public panic in several African nations. In South Africa, baseless conspiracy theories linking 5G networks to the spread of COVID-19 led to the arson of communication towers in 2021. This highlights how misinformation can result in the destruction of public infrastructure and illustrates the need for digital literacy campaigns and regulatory safeguards (Alabi & Mutula, 2022). The rollout of 5G technology across Africa has sparked a mix of excitement and concern. While many view it as a gateway to advanced digital innovation, others

have expressed skepticism fueled by conspiracy theories and misinformation. These suspicions are often rooted in long-standing mistrust of authorities, low levels of technological awareness and deep socio-economic disparities that have painted 5G as a hidden, dangerous force. The outbreak of the COVID-19 pandemic further amplified these fears, linking the new wireless technology to disease transmission, population control, and various health scares. Africa's encounter with 5G conspiracy theories reflects a global trend shaped by local realities. As noted by Oyekan (2021), the combination of limited health care systems, underdevelopment, and historic political distrust provided perfect conditions for misinformation to thrive during the pandemic. These false narratives often spread rapidly on social media and through informal communication channels, outpacing efforts to correct them. In countries such as Nigeria, South Africa, and Kenya, the spread of 5G conspiracies has visibly influenced public actions. Reports have emerged of protests, deliberate damage to telecom infrastructure, and viral social media posts questioning the safety of 5G radiation (Frith et al., 2023). The lack of widespread scientific understanding allows these fears to gain traction, especially because the electromagnetic waves used by 5G are invisible and difficult to grasp for the general public (Odigie et al., 2021). In addition to public fear, these conspiracies pose deeper challenges to governance and the credibility of scientific communication. Oyekan (2021) emphasized that the failure of many African governments to provide clear, transparent, and science-based explanations has left an informational void one quickly filled by conspiracy theorists and pseudo-scientific claims. Meese et al. (2020) also highlighted how the overlap of pandemic anxieties with technological fears has undermined public health efforts, particularly in regions where media literacy is low and online information is poorly regulated. The effects of these narratives go far beyond health-related misinformation. They threaten to stall Africa's broader digital development by eroding trust in infrastructure investments and technological progress. Bruns and Harrington (2020) argue that the widespread promotion of such beliefs through African social media networks could disrupt efforts to expand the digital economy and delay the adoption of next-generation technologies critical for economic growth. To combat these growing challenges, targeted strategies must focus on strengthening science communication, fostering digital literacy and building community trust. Governments, tech firms, and civil society must work together—engaging trusted local voices and influencers to counter myths with credible information. Without these coordinated efforts, the continent risks widening its digital divide, not only in access to technology, but also in public confidence and understanding.

F. Governing Emerging Technologies for Peace: a growing number of international and regional actors are advocating for the institutionalization of "cyber peace and security." This requires the development of comprehensive frameworks to regulate AI-powered surveillance, cyber weapons, and disinformation campaigns. Initiatives include the use of AI for sentiment analysis in peacekeeping and conflict forecasting, with applications by UN agencies like the Department of Peace Operations. However, the extent to which such tools effectively support peacebuilding remains underexplored. Moreover, Africa's exclusion from global regulatory platforms has exacerbated its vulnerability to exploitative technology transfers. The continent's historical context of colonization amplifies concerns that emerging technologies may perpetuate neocolonial dependencies. For instance, African youth have been recruited to participate in disinformation campaigns that manipulate national histories and social tensions for foreign political gain, as evidenced in the Central African Republic, where Russia-led narratives instigated anti-French protests (Berhe, 2017).

G. The Role of International Actors and External Dependence

Africa's technological security environment is increasingly being shaped by the interventions and strategic objectives of international actors, both emerging powers and established Western states. These external stakeholders frequently introduce digital infrastructure and advanced technologies into African nations not solely for development assistance or humanitarian purposes but often to serve their own geopolitical and economic agendas. As Nganje and Ndawana (2020) observed, such engagement tends to be driven by a desire to consolidate influence over key markets and political alliances, rather than altruistic motives. China, in particular, has emerged as a dominant player in this landscape through initiatives such as the Belt and Road Initiative and the Digital Silk Road, providing African countries with affordable digital infrastructure, including facial recognition systems, 5G networks, and cloud computing platforms. These investments, while beneficial to expanding Africa's technological capabilities, often come with hidden dependencies. African governments frequently lack the technical expertise or regulatory frameworks to independently manage, audit, or secure these systems, resulting in growing concerns about technological sovereignty and the erosion of national control over critical digital assets (Nganje & Ndawana, 2020; Ogbu et al., 2021).

Western nations are also implicated in these dynamics. Through aid programs, security partnerships, and public-private collaborations, countries such as the United States, France, and Germany support digital transformation in Africa but often tie this support to broader strategic interests. Whether in counter-terrorism, border surveillance, or market expansion, technological exports are frequently aligned with national foreign policy goals, which may not always prioritize local needs or transparency. This asymmetrical power relationship raises the specter of "techno-colonialism" a scenario in which African states become deeply dependent on external technologies and platforms that they do not fully understand, control, or own. Such dependence can limit their capacity to develop indigenous innovation ecosystems or to safeguard citizens' data and privacy, particularly in contexts where technologies are used for surveillance, electoral manipulation, or social control (Phoobane, 2022; Shava, 2021). To mitigate these risks, scholars and practitioners advocate for establishing robust digital governance frameworks at both national and regional levels. These should aim to strengthen cybersecurity infrastructure, promote transparency in foreign partnerships, and foster homegrown technological development. Moreover, Africa must be more actively represented in global forums that set standards for digital governance to ensure that its interests are adequately protected in the evolving technological order.

H. Technological Governance and Institutional Development

Africa's evolving security architecture is increasingly being shaped by how emerging technologies are governed and integrated into institutional development frameworks. The growing proliferation of mobile phones and digital communication tools across the continent has redefined traditional governance mechanisms. According to Livingston (2011), these technologies have enabled civil society actors to play more prominent roles in promoting transparency, monitoring political violence, and influencing policymaking, thereby acting as agents of informal security governance (Livingston, 2011). These digital tools are no longer peripheral; instead, they have become central components of state-building and institutional governance efforts. Mobile technology, in particular, has become a transformative instrument for facilitating civic engagement, strengthening accountability and improving service delivery. For example, Asongu and Nwachukwu (2016) demonstrated how mobile phones, when combined with effective governance structures such as regulation quality and political stability, contribute significantly to inclusive human development in Sub-Saharan Africa (Asongu & Nwachukwu, 2016).

In practice, this has manifested in numerous ways. Mobile technology has empowered grassroots movements by facilitating real-time communication and coordination, particularly in politically unstable regions. Lewis (2011) highlighted how the rise of internet and mobile phone networks has amplified activists' voices, enabling them to report injustices, monitor electoral processes, and exert pressure on authorities for reforms (Lewis, 2011). Nevertheless, these advancements are not without challenges. Although digital tools offer immense potential for institutional development, their efficacy depends significantly on the broader governance environment. Asongu and Asongu (2017) found that the positive impact of mobile phones on information and communication technology (ICT) exports is contingent upon the presence of political stability and effective anti-corruption mechanisms (Asongu & Asongu, 2017). In conclusion, mobile and digital technologies in Africa have catalyzed a shift toward more decentralized and participatory governance models. However, their success in enhancing institutional capacity and ensuring sustainable security outcomes is intricately linked to the quality of governance and the inclusiveness of the political environment.

I. Challenges of Technological Integration: While the integration of emerging technologies into African security frameworks is promising, it faces several structural and systemic challenges that constrain their efficacy and equitable deployment. These challenges reflect deeper disparities across the continent's digital landscape, especially in rural and underserved areas. One of the primary obstacles is the uneven development of digital infrastructure. While urban centers in countries like Kenya, Nigeria, and South Africa are advancing technologically, many rural regions remain digitally disconnected, lacking stable electricity, internet access, or even basic digital literacy (Badaru & Mphahlele, 2023). This digital divide restricts the ability of local governments and communities to fully participate in or benefit from the digital transformation sweeping across the globe. Moreover, Africa's regulatory landscape is often ill-equipped to keep pace with the rapid evolution of technology. Many states lack comprehensive legal frameworks to safeguard critical infrastructure, manage cybersecurity threats, or ensure the ethical use of technologies like AI and biometric surveillance (Badaru & Mphahlele, 2023). This regulatory gap not only exposes countries to external manipulation and cyberattacks but also impedes the development of trust in technological systems among citizens.

In addition to infrastructure and regulatory issues, socio-political risks are linked to technological adoption. According to Schoeman (2002), digital technologies may intensify existing inequalities and political fragmentation, especially in fragile states where they empower non-state armed groups or intensify ethnic and communal divisions. This danger is particularly acute where digital tools are used to spread disinformation or manipulate electoral outcomes, undermining democratic institutions and social cohesion. Recent research supports these concerns. For instance, Amoi (2012) emphasized the need for education and cultural integration as critical complements to technological infrastructure to avoid exacerbating regional imbalances and conflict in East Africa's integration efforts (Amoi, 2012). Similarly, Fagbayibo (2021) discussed how the inability to operationalize key security frameworks like the African Standby Force reflects broader institutional and coordination failures, which are crucial for integrating security technologies on the continent (Fagbayibo, 2021). In conclusion, while emerging technologies offer powerful tools for enhancing security, their successful integration into African contexts requires holistic strategies that address infrastructure deficits, regulatory shortcomings, and socio-political vulnerabilities.

Concluding Remarks

The integration of emerging technologies into African security architectures has become an increasingly prominent feature of contemporary policy and governance approaches. As the continent grapples with a wide array of complex security and development challenges, ranging from terrorism and cyber threats to food insecurity

and health crises, technological innovations are playing an increasingly important role in shaping both national defense strategies and broader societal resilience. While these technologies offer unprecedented opportunities to enhance security infrastructure and early warning systems, their deployment raises significant questions about dependency, governance, equity, and long-term sustainability. Among the most notable technological advancements being adopted across Africa are unmanned aerial vehicles (UAVs), commonly referred to as drones. These platforms are increasingly used for tasks such as border surveillance, counter-terrorism, environmental monitoring, and disaster response. The flexibility, real-time data capabilities, and cost-effectiveness of these systems make them particularly valuable in regions with difficult terrain or underdeveloped infrastructure. Research conducted by Muriungi et al. (2021) highlighted the promising role of photonics and drone technologies in transforming Africa's defense and security apparatus. The study advocates for the development of affordable, localized drone systems that can be manufactured and maintained within African states, thereby reducing reliance on costly foreign imports (Muriungi et al., 2021). However, despite this potential, the continent continues to face significant technological and industrial gaps that hinder the widespread adoption of homegrown solutions. Much of Africa's drone technology is still imported, and this dependency not only limits strategic autonomy but also complicates issues of data sovereignty and regulatory oversight.

The debate on artificial intelligence and predictive analytics in conflict management also explains that in addition to drone technology, artificial intelligence (AI) and big data analytics are reshaping how African governments and regional organizations monitor and respond to security threats. AI-powered platforms can analyze vast datasets to identify patterns, detect anomalies, and generate real-time insights that inform policy decisions. These capabilities are especially useful in conflict-prone regions, where early warning systems and predictive models can help anticipate violence, mobilize resources, and protect vulnerable populations. Mbuguah and Gichuki (2024) argued that AI is revolutionizing security-related decision-making in key sectors such as agriculture, public health, energy management, and natural disaster response. For example, AI systems can detect early signs of drought or crop failure in agriculture, preventing food shortages that might otherwise escalate into political instability. Similarly, in the energy and health sectors, machine learning algorithms are being used to predict disease outbreaks, manage health crises, and protect critical infrastructure (Mbuguah & Gichuki, 2024). These applications demonstrate that emerging technologies are not confined to traditional definitions of security focused on territory and military threats; rather, they are reshaping how we understand and address human security. By empowering governments to act swiftly and proactively, AI and analytics provide an essential toolkit for building more resilient and responsive institutions.

In the aspect of human security and the broader purpose of technological innovation, while technological tools can undoubtedly enhance state capacity, their full potential lies in addressing the broader dimensions of human security such as health, climate change, poverty, and social exclusion. This more holistic view of security, championed by scholars such as Carmody (2005), recognizes that real and lasting peace cannot be achieved through military means. Instead, it requires addressing the underlying drivers of insecurity, including economic disparity, weak governance, and environmental degradation (Carmody, 2005). If harnessed inclusively, emerging technologies offer a path toward addressing these structural issues. For example, health technologies such as mobile diagnostics and telemedicine platforms have improved health care delivery in remote regions. Renewable energy technologies like solar grids support rural electrification and economic inclusion. Satellite data can help monitor climate conditions and guide resource allocation in drought-prone areas. These advances not only

enhance national resilience but also contribute to the stability of local communities, reducing conditions that often lead to conflict. However, without deliberate policy intervention, technological innovation can reinforce existing inequalities. Uneven access to technology driven by disparities in infrastructure, education, and investment can create new divides between urban and rural populations, between elites and marginalized communities, and between states with and without technological partnerships. Therefore, it is essential that emerging technologies be governed in ways that prioritize inclusive access, public accountability, and social justice.

In policy implications; governance, cooperation, and capacity building, ensuring that technology contributes to peace rather than worsening instability requires thoughtful governance at both national and regional levels. African countries need not only to adopt technologies but also to invest in building institutional capacity to regulate, adapt, and sustain them. This includes developing robust legal frameworks, cybersecurity protocols, and data protection laws that reflect local realities while aligning with international norms. International cooperation is also vital. Partnerships with global institutions, research centers, and private sector innovators must be structured around principles of mutual benefit and African ownership. Instead of relying solely on foreign-built systems, African governments should encourage knowledge transfer, joint ventures, and regional centers of technological excellence that empower local innovators. In tandem, regional organizations such as the African Union and sub-regional bodies like ECOWAS and SADC must play a more active role in coordinating the continent's technological security strategies. Shared platforms for knowledge exchange, standardized regulations and collective investments in technology infrastructure could help prevent fragmentation and promote a more unified African voice in global digital governance. Emerging technologies are rapidly redefining the meaning of security for Africa, offering both opportunities for transformation and challenges that demand urgent attention. From drone surveillance to artificial intelligence, these innovations can enhance state resilience, support human development, and address the root causes of conflict. However, their impact will depend on how they are governed, who has access to them, and whether they are aligned with the broader goal of human security. The path forward requires a deliberate, inclusive, and ethical approach to technological adoption that prioritizes empowerment over control, equity over elitism, and long-term stability over short-term gains. As Africa continues to assert its place in the global digital order, the responsible integration of emerging technologies into its security and development frameworks will be critical in shaping a more peaceful and prosperous future.

References

Alabi, A. O., and Mutula, S. M. (2022). Human development for the fourth industrial revolution: Which way for Sub-Saharan Africa? Development Southern Africa, 39(4), 528–542.

Allen, G. C., & Chan, T. (2017). Artificial intelligence and national security. Harvard Kennedy School, Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/artificial-intelligence-and-national-security

Amoi, A. (2012). Integrating East Africa. Retrieved from https://consensus.app/papers/integratinamoi/cccb7a65b3f654318c37088bf1b377bb/ Accessed on 28 May 2025.

Badaru, A. I., and Mphahlele, M. (2023). Digital governance and cybersecurity in Africa.

Badaru, K. A., and Mphahlele, R. S. (2023). Effects of emerging technologies on African development: A narrative review of selected African countries. Research in Social Sciences and Technology. https://consensus.app/papers/effects-of-emerging-technologies-on-african-development-a-badaru-mphahlele/cc7b90be95935fa88c826fca1be9036 Accessed on May 23, 2025

Berhe, M. (2017). The norms and structures for African peace efforts: African peace and security architecture. *International Peacekeeping*, 24(5), 661–685.

Bruns, A., & Harrington, S. (2020). 'Corona? 5G? or both?': the dynamics of COVID-19/5G conspiracy theories on Facebook. Retrieved from https://journals.sagepub.com/doi/abs/10.1177/1329878X20946113 Accessed on May 30, 2025

Carmody, P. (2005). Transforming globalization and security: Africa and America post-9/11. Africa Today, 52, 97–120. Retrieved From: https://consensus.app/papers/transforming-globalization-and-security-africa-and-carmody/f558a5df22b0568caa4c33160d9310d6 Accessed on May 20, 2025

Cawthra, G. (2009). African security governance: Emerging issues. Retrieved from https://consensus.app/papers/african-security-governance-emerging-issues-cawthra/294d085bbc245c2a9ef12b035172e9d3 Accessed on May 25, 2025

Chaudhry, S., and Otondi, S. T. (2018). The role of the African Union and regional economic communities as impetus for peace and security. https://consensus.app/papers/the-role-of-the-african-union-and-regional-economic-dr-otondi/9be1ab1f9a235cb981eadc6cdf1a Accessed on May 30, 2025

Chemhuru, M. (2021). The Fourth Industrial Revolution (4IR) and Africa's Future: Reflections from African Ethics. Retrieved from https://consensus.app/papers/the-fourth-industrial-revolution-4ir-and-africa-'-s-future-chemhuru/a6c3ac152f1e50898e2f21a2018545f2 Accessed on 28 May 2025

Chikane, B. (2020). Cybersecurity challenges in Africa: Threats and opportunities. African Journal of Science, Technology, Innovation and Development, 12(4), 399–407.

Collier, P. (2015). Security threats facing Africa and its capacity to respond. Prism: *A Journal of the Center for Complex Operations*, 5(2), pp. 5

Distor, C., Isagah, T., Ruas, I.C., and Dhaou, S.B. (2023). Emerging Technologies in Africa: Artificial Intelligence, Blockchain, and Internet-of-Things Applications and Way Forward. Retrieved from https://collections.unu.edu/eserv/UNU:9381/Distor_2023_Emerging_Tech_in_Africa_-_AI__Blockchain_and_IoT.pdf Accessed on May 30, 2025

Domson-Lindsay, A. K. (2015). Peace and security in Africa: Past, present and future. Retrieved from https://consensus.app/papers/peace-and-security-in-africa-past-present-and-future-domson-lindsay/7801b9017ee85d8e8f61ab66f7f10383 Accessed on June 02, 2025

Fagbayibo, B. (2021). Implementing African Security Regime through a 'Multiple-Speed' Approach: Challenges and Prospect. *Insight on Africa*, 13(1), 160-176.

Franke, B. (2007). Competing regionalisms in Africa and the continent's emerging security architecture. Retrieved from https://consensus.app/papers/competing-regionalisms-in-africa-and-the-continents-franke/c6a51beebe3050a395a5c4e55bd794b0 Accessed on 28 May 2025.

Frith, J., Campbell, S., & Komen, L. (2023). Looking back to look forward: 5G–COVID-19 conspiracies and the long history of infrastructural fears. Retrieved from https://journals.sagepub.com/doi/abs/10.1177/20501579221133950. Accessed on May 28, 2025

Horowitz, M. C. (2020). Artificial intelligence and international security. *International Security*, 45(2), 7–40. https://doi.org/10.1162/isec_a_00392

Kumah-Abiwu, F. (2021). Africa's security landscape of securitized-development and human rights issues. *African Security Review*, 31(2), 99–114. https://doi.org/10.1080/10246029.2021.1980412

Livingston, S. (2011). Africa's evolving infosystems: A pathway to security and stability. https://consensus.app/papers/africas-evolving-infosystems-a-pathway-to-security-and-livingston/f29e74bf0c295165b058d52bdc55ea24 Accessed on June 05, 2025

Lubinga, S., Maramura, T., and Masiya, T. (2023). Fourth Industrial Revolution Adoption: Challenges in South African Higher Education Institutions. *Journal of Culture and Values in Education*. https://consensus.app/papers/the-fourth-industrial-revolution-adoption-challenges-in-lubinga-maramura/739286884dd05dbd9ac97489aa35be Accessed on May 28, 2025

Mamphiswana, R. (2020). The Fourth Industrial Revolution: Prospects and Challenges for Africa. https://consensus.app/papers/the-fourth-industrial-revolution-prospects-and-mamphiswana/76cd0c0dd2d35910a4993bd4e8b3389a Accessed on May 23, 2025

Masunda, O. (2024). Peace Education 4.0: A Curriculum Framework for Africa. https://consensus.app/papers/peace-education-40-a-curriculum-framework-for-africa-masunda/4fa525c68fda56daafd14c4ab133b0b5/ Accessed on May 26, 2025

Mbuguah, S., and Gichuki, D. K. (2024). Leveraging emerging trends for technological advancement in Africa. 2024 4th International Multidisciplinary Information Technology and Engineering Conference (IMITEC), 1–11. https://consensus.app/papers/leveraging-emerging-trends-for-technological-mbuguah-gichuki/e913958d5c7751d6af9504e88c5b Accessed on May 25, 2025

Meese, J., Frith, J., & Wilken, R. (2020). COVID-19, 5G conspiracies and infrastructural futures. Retrieved from https://journals.sagepub.com/doi/abs/10.1177/1329878X20952165 Accessed on May 25, 2025

Mude, T., Maeresera, S., & Maramura, T. (2021). Rising to the Occasion: Africa, the Fourth Industrial Revolution and Lessons from China. https://consensus.app/papers/rising-to-the-occasion-africa-the-fourth-industrial-mude-maeresera/088567db37eb5121ab467d2a760b806f Accessed on May 28, 2025

Mumo, M. (2022). Digital sovereignty and dependency: The politics of Africa's data infrastructure. *Journal of International Affairs*, 75(1), 45–62.

Muriungi, K., Oluoch, E., Murimi, C., Yahya, S., Chebet, B., Ngoda, B., Kimeli, A., & Mwenda, G. (2021). Future applications of photonics and emerging technologies for security and defense using drones in Africa. 2021 IEEE Research and Applications of Photonics in Defense Conference (RAPID), 1–4. https://consensus.app/papers/future-applications-of-photonics-and-emerging-muriungi-oluoch/ Accessed on May 28, 2025

Naudé, W. (2017). Entrepreneurship, education and the Fourth Industrial Revolution in Africa. Development Economics, eJournal. Retrieved From https://consensus.app/papers/entrepreneurship-education-and-the-fourth-industrial-naudé/0e719bb0ef3a56b4a253d8ff2fc45cf8/ Accessed on June 08, 2025

Nganje, F. and Ndawana, E. (2020). The political economy of external intervention in Africa's security. Retrieved from https://consensus.app/papers/the-political-economy-of-external-intervention-in-africa-'-nganje-ndawana/e149ddba87695bdab474f4d1126f4a81/ Accessed on May 29, 2025

Nganje, F. and Ndawana, H. (2020). Geopolitics and the securitization of development aid in Africa. *South African Journal of International Affairs*. https://consensus.app/papers/geopolitics-securitisation-development-aid-africa-nganje/4ceab066f19b51c5a509b5c2cf3a1a25/ Accessed on May 30, 2025

Odigie, E. B., Okungbowa, G. E., and Ajayi, O. O. (2021). Association between COVID-19 and 5G Electromagnetic Radiation: Bursting the World Web Conspiracy Theorists. Retrieved from https://www.ajol.info/index.php/cajost/article/view/217980 (accessed on May 30, 2025

Ogbu, E. O., Okoye, U., and Ome, G. E. (2021). The place of Africa in the Fourth Industrial Revolution. *African Renaissance*, 18(3), 75–92. https://consensus.app/papers/the-place-of-africa-in-the-fourth-industrial-revolution-ogbu-okoye/843d0d7c4a4f51cfbbf2e009 Accessed on May 30, 2025

Osee, U. B. (2024). Integrating artificial intelligence: A step toward African peace and security architecture. *International Journal of Social Science Humanity & Management Research*. https://consensus.app/papers/integrating-artificial-intelligence-a-step-towards-the-osee/fa2621bc24005adf96bd5fa473b68d9c/ Accessed on May 30, 2025

Oyekan, A. O. (2021). Conspiracy theories and pandemic management in Africa: Critical reflections on contexts, contradictions and challenges. Retrieved from https://www.scielo.org.za/scielo.php?pid=S2415-04792021000200003&script=sci_arttext. Accessed on May 30, 2025

Phoobane, P. (2022). Fourth Industrial Revolution research outputs in Africa: A bibliometric review. *Journal of African Technological Advancement*, 7(2). https://consensus.app/papers/fourth-industrial-revolution-research-outputs-in-africa-a-phoobane/22ff83212eba5fe1831c2ec30c4591c6/ Accessed on May 24, 2025

Sage, A. (2010). Africa's irregular security threats: Challenges for U.S. engagement. Retrieved from https://consensus.app/papers/africas-irregular-security-threats-challenges-for-us-sage/893c87b1f6aa59aa952a707865f9671e/ Accessed on 28 May 2025.

Schoeman, M. (2002). Imagining a community—the African Union—as an emerging security community. Retrieved from https://consensus.app/papers/imagining-a-community-the-african-union-as-an-emerging-schoeman/eab3f98b24d35b118c82cc42de78332 Accessed on May 30, 2025

Schoeman, M. (2002). Security community building in southern Africa: A critical perspective.

Shava, E. (2021). The survival of African governments during the Fourth Industrial Revolution. In Africa and the Fourth Industrial Revolution. From https://consensus.app/papers/survival-of-african-governments-in-the-fourth-industrial-shava/87cc54ee05fb539da34c2b0f821844ae/? Accessed on 23 May 2025

Signé, L. (2023). Africa's Fourth Industrial Revolution. Retrieved from https://consensus.app/papers/africas-fourth-industrial-revolution-signé/4707229e3c0a5d57a04942930d865441/ Accessed on 29 May 2025.

Steff, R., Burton, J., & Soare, S. (2021). Emerging technologies and international security: Machines, the state, and war. Routledge

Turianskyi, Y., & Bornman, C. (2021). Artificial intelligence and governance in Africa: Risks and opportunities. South African Institute of International Affairs. Available online: https://saiia.org.za.

Vrey, F. (2010). African maritime security: A time for good order at sea. *Australian Journal of Maritime and Ocean Affairs*, 2(4), 121–132. https://doi.org/10.1080/18366503.2010.10815667

Warricker, A. M. (2005). The status of information security in South Africa. Retrieved from https://consensus.app/papers/the-status-of-information-security-in-south-africa-warricker/ba20a154ff885e74942fd25adba7c3af/ Accessed on May 30, 2025

Williams, P. D. (2007). Thinking about security in Africa. *PRN: Distributive & Economic Justice*. https://doi.org/10.1111/j.1468-2346.2007.00671.x