ISS INSTITUTE FOR SECURITY STUDIES

ISSUE 189 | SEPTEMBER 2026

Peace & Security Council Report



Special edition

Who owns Africa's artificial intelligence future?

Africa's artificial intelligence strategy: opportunity, risk and agency

Artificial intelligence (AI) is set to accelerate development in Africa, but it exposes the continent to threats such as disinformation, deepfakes, cybercrime and surveillance. The African Union (AU) Continental AI Strategy, adopted in July 2024 by the AU Executive Council, was developed as a balancing act between harnessing AI benefits and ensuring safeguards.

The policy process began in 2019 when the Specialised Technical Committee on Communication and Information and Communications Technology tasked member states with forming a working group to determine AI's benefits, risks, capability gaps and cooperation needs. The resulting strategy is a people-centred, development-oriented, 15-action points harnessing benefits, addressing risks, building continental capabilities, fostering cooperation and stimulating investment.

Leapfrogging is central, as AI could allow African economies to bypass conventional agriculture, health, education and public service delivery development stages. The strategy suggests that capturing even a modest share of generative AI's projected global economic value could add over US$100 billion annually to African gross domestic product. This article critically examines the pillars, discussions and normative commitments that shaped the strategy, and the extent to which it offers a credible pathway for Africa to translate this potential into equitable and sustainable development.

Values-driven vision

The strategy moves from a technical to values-laden vision of what AI should do for Africa. It notes there is no universal definition of AI, but offers its own computer systems that simulate natural (human) intelligence processes, essentially learning and adapting, and extracting knowledge from data to achieve objectives set by humans. This keeps the definition broad and functional rather than tied to techniques such as machine learning and generative AI. However, in the absence of clear classification of AI systems, difficulties may arise around potential benefit or harm, level of exposure and the response needed from African countries.

Acronyms and abbreviations

AI	Artificial intelligence
AU	African Union
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbei
PSC	Peace and Security Council
US	United States

While AI is consistently presented as a driving force for economic growth and social progress, several harms exist for a continent prematurely entering an externally owned and governed environment. These include bias from inequitably sourced data, discrimination against women and vulnerable groups, job displacement, threats to indigenous knowledge, disinformation, surveillance and a widening divide between and within countries. The strategy doesn't treat AI as a neutral technology to be adopted uncritically, but as needing active governance and shaping.

The AI strategy covers harnessing benefits, addressing risks, building continental capabilities, fostering cooperation and stimulating investment

It insists on an Africa-centric, development-oriented and inclusive approach. It mentions ubuntu alongside other African norms and universal principles such as human rights and dignity, gender equality and the protection of children and vulnerable persons. AI is framed as something that must be adapted to Africa's context, not the reverse.

Strategy implementation

The strategy sets a common direction for 55 member states starting from very different positions. Countries vary considerably in digital infrastructure, technical expertise, research capacity, regulatory institutions and AI talent. The strategy recognises this, with its first phase focused on governance, national strategies, resource mobilisation and capacity building, before implementation expands to 2030. The challenge is turning continental ambition into national action.

Rwanda offers one of the continent's clearest early examples. Its national AI policy was approved in 2023, while Ghana developed a national AI strategy for 2023 to 2033. Zimbabwe launched its 2026 to 2030 strategy with the accent on developing domestic AI capacity while engaging its diaspora. Meanwhile, countries including Nigeria, Kenya, South Africa, Egypt and Ethiopia are pursuing their own approaches. The AU's role is, therefore, less about imposing uniformity than creating a framework through which countries can develop their own strategies while building greater continental coherence.

That implementation is also being supported by non-government actors. Smart Africa and development partners such as Deutsche Gesellschaft für Internationale Zusammenarbei (GIZ) have provided technical assistance, policy support, training and opportunities for peer learning, including through GIZ's FAIR Forward programme. The programme has supported national AI strategies in several African countries and reached more than 100 000 learners, while increasing access to African training data. GIZ estimates that only around 2% of global AI training data originates in Africa, underscoring

Current PSC Chairperson

H.E. Ambassador Hervé D Djokpe, Permanent Representative of the Republic of Benin to the African Union and PSC Chairperson for September 2026

PSC members

Algeria, Benin, Cameroon, Côte d'Ivoire, Democratic Republic of the Congo, Eswatini, Ethiopia, Gabon, Lesotho, Morocco, Nigeria, Sierra Leone, Somalia, South Africa, and Uganda

the importance of developing datasets that better reflect African languages, economies and societies.

The private sector will be equally important. Governments alone cannot build the computing infrastructure, cloud capacity, connectivity and specialised skills required for AI. Public-private partnerships will be essential. However, the measure of a successful partnership should be more than the investment it attracts. More important is what remains when the partnership ends. Are countries left with stronger institutions, skills, infrastructure, data and technical capacity, or with deeper dependence on external actors?

Data ownership and control pose serious sovereignty challenges for African countries and will need to be addressed. For the continental strategy to deliver on its promise, partnerships must ultimately strengthen Africa's ability not only to adopt AI, but to shape and govern it.

Where strategy meets infrastructure

Connectivity is the most obvious starting point for how African countries will roll out the strategy. The latest information from the International Telecommunication Union suggests that only 38% of Africa's population uses the internet, compared with a global average of 68%. The divide is even sharper between urban and rural areas: 57% of urban Africans are online, compared with just 23% in rural areas.

Fixed broadband remains almost non-existent for most of the population, leaving mobile data as the primary route to the internet. Affordability remains a constraint. Only around 1% of Africans currently have access to 5G. These statistics determine who can access AI-enabled services, participate in digital education and work and ultimately benefit from the technologies governments are promoting.

The electricity gap is another crucial element. Sub-Saharan Africa accounted for 86% of the world's access deficit in 2024, with 563 million people still living without electricity. The scale of initiatives such as that of World Bank and African Development Bank's Mission 300 – which aims to connect 300 million people to electricity by 2030 – illustrates how much basic infrastructure investment is still required. For countries still struggling to provide reliable electricity and affordable broadband, building sophisticated AI ecosystems is difficult.

Data governance presents a more mixed picture. Forty-four African countries have adopted data protection legislation, a significant increase from a decade ago. But laws alone do not create effective data governance. Only 38 have operational data protection authorities, leaving a gap between legislation and the institutional capacity to enforce it. The continent has made considerable progress in putting rules on paper, but less in developing the institutions, technical expertise and resources to implement them.

Forty-four African states have data protection legislation but only 38 have institutions to enforce it

That gap matters for AI regulation because the technical demands are considerably higher. Drafting an AI law or ethics framework is one thing, but assessing whether an AI system complies with it requires regulators who understand model behaviour, risk assessment, evaluation methods and the technologies being deployed. Expertise in these areas is scarcer and more expensive to build than legislative drafting. Some countries may formulate AI rules faster than they can develop enforcement institutions.

This is why regulatory and technical capacity should not come after infrastructure and skills. Africa's challenge is not simply to connect more people or adopt more AI systems, but to build the institutional capacity and conducive environments to govern the technologies that integrate African people and economies.

The AU Continental AI Strategy emerges from a multiyear continental deliberation on a framework that positions Africa not merely as a recipient of AI technology but as a potential shaper of its global trajectory. Its promise rests on leapfrogging conventional development stages and capturing a meaningful share of AI's projected economic value, even as he strategy acknowledges the infrastructural and capability gaps that could widen the continent's AI divide. While the strategy sets a concrete blueprint, its success will determine the extent to which member states implement and adapt it.

How deepfakes are reshaping African politics

Declining United States (US) hegemony has given African nations new opportunities to benefit from renewed geopolitical competition, but major hurdles remain. Many countries continue to grapple with instability and corruption as the lines between state security forces and non-state armed groups blur. Living standards lag behind those of other regions, and civil unrest is rising.

Surveys routinely show that most Africans still prefer democracy over personalist autocracy, military regimes or single-party rule. But amid the battle for hearts and minds, Africa's strongmen, as with those elsewhere, have a powerful new tool: deepfakes. These forgeries, generated by AI, increasingly underpin regimes' efforts to inflate their popularity. The flood of synthetic content also aims to drown out scrutiny.

'These videos of military leaders, often dressed in ceremonial uniforms or surrounded by crowds, are made to look like moments of destiny,' an African fact-checker told *New Lines Magazine* last year. 'They speak directly to people's frustration with democracy and decades of broken promises. Where schools are underfunded and traditional media has been silenced, that imagery becomes powerful, especially for the youth.'

This poses a new threat to African governance, as AI helps authoritarians shape public perception to their own ends. More such campaigns are likely, painting strongmen as the only leaders capable of delivering a better future – at the expense of national development.

Fakes vs reality

Burkina Faso's military leader, Captain Ibrahim Traoré, is the prime example. Online, he is a modern-day Pan-Africanist hero. Hundreds of fake clips circulating on social media have him earning endorsements from A-list pop stars and US President Donald Trump. Crowds of his supporters supposedly dwarf the pope's.

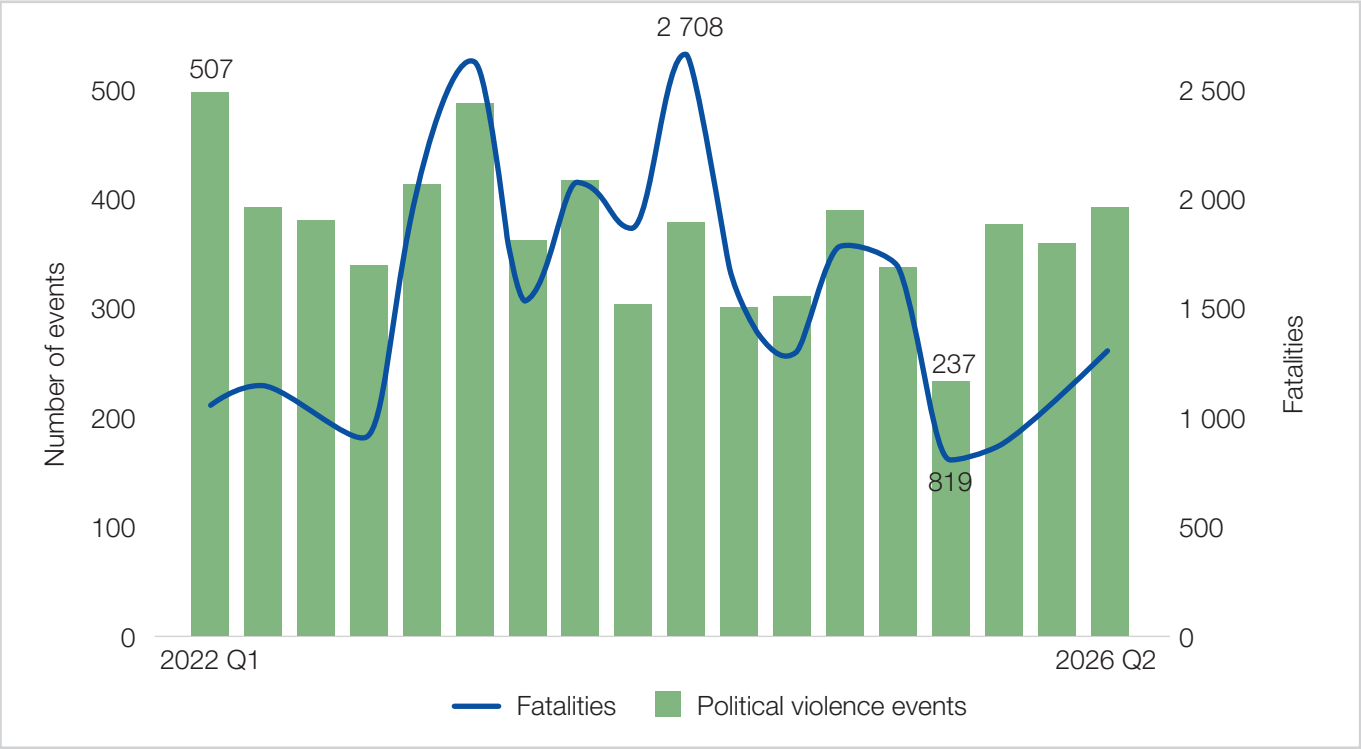
'It's algorithmic populism,' a Burkinabè researcher told *The Africa Report* last year. 'It's about vibe and vision not fact or policy. Social media platforms reward spectacle and Traoré's image fits perfectly into that ecosystem.' In reality, the 38-year-old's rule has been far bleaker.

Since taking power in a 2022 coup, Traoré's heavy-handed security strategy has failed. The jihadist insurgency he promised to quell has intensified, while his military has been accused of massacring civilians. Burkina Faso's exit from the Economic Community of West African States has done lasting diplomatic damage. Political parties are now banned and the country's independent electoral commission has been abolished. Hundreds of civil society organisations have been dissolved on vague grounds. 'Democracy isn't for us,' Traoré told a state broadcaster in April 2026.

'In a region with high mobile phone use and low digital literacy, such misinformation doesn't just go viral,' wrote a journalist for Nigerian news outlet *The Cable* last year, 'it rewrites public memory.'

'IN A REGION WITH HIGH MOBILE PHONE USE AND LOW DIGITAL LITERACY ... MISINFORMATION REWRITES PUBLIC MEMORY'

Chart 1: Political violence events and fatalities in Burkina Faso since 2022



Source: ACLED. Data per quarter and correct as of 2 September 2026. Quarter 3 data for 2026 excluded to avoid skewing data.

Other early adopters of deepfakes and AI-powered propaganda in Africa include the paramilitary Rapid Support Forces in Sudan and Rwanda's government under President Paul Kagame.

This comes as Meta – owner of Facebook, Instagram and WhatsApp – YouTube and Elon Musk's X have all scaled back their content moderation teams. They now favour a crowdsourced approach to policing false information and manipulated material.

Information-integrity guidelines

A March 2025 resolution by the African Commission on Human and Peoples' Rights called on its special rapporteur on freedom of expression and access to information to develop guidelines to uphold information integrity online. It also enlists African civil society groups, regulators and homegrown tech companies to monitor platforms' performance collectively.

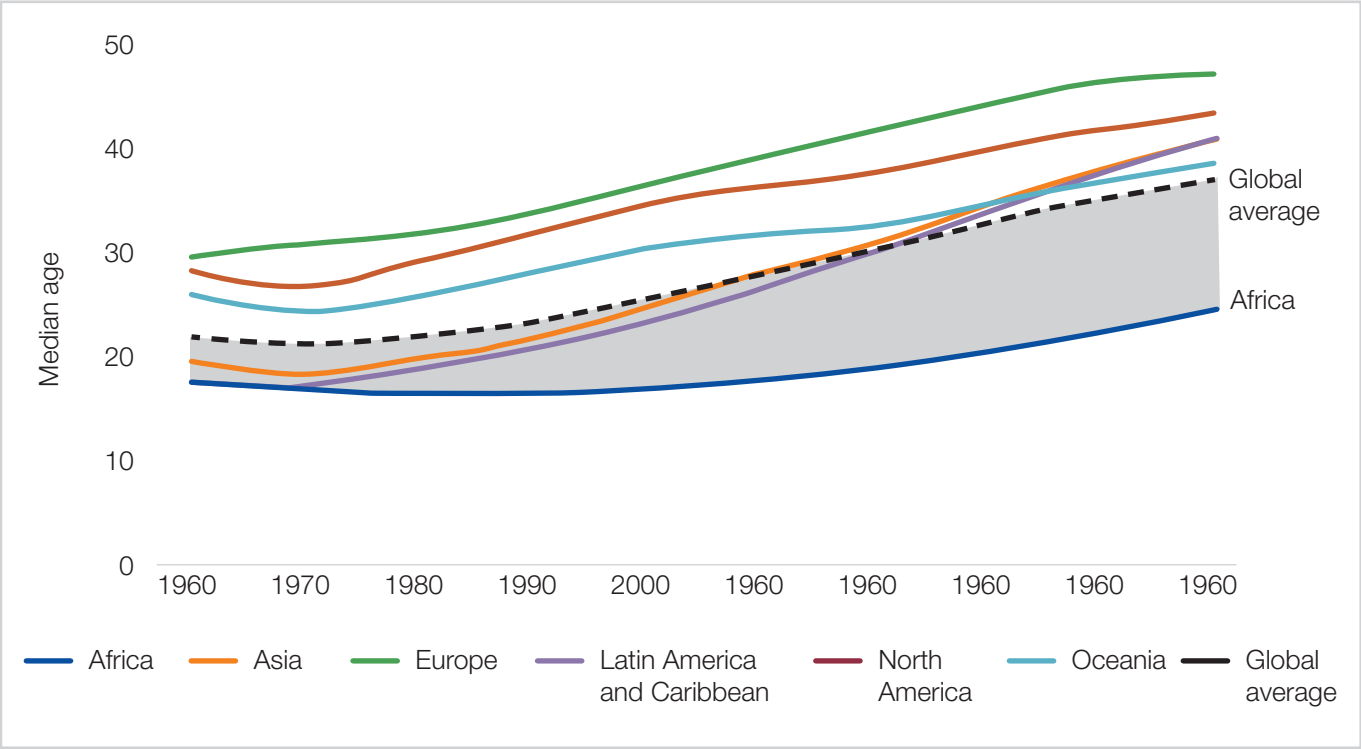
The initiative is worthy, but as technologies evolve, journalists, activists and institutions face an uphill battle to sift through the noise. Compared with human-driven troll farms, generative AI can deploy deepfakes much more cheaply, at greater velocity and on a vastly larger scale.

This proliferation of deepfake propaganda in Africa is both a regional and a global issue. The continent's development goals will be impossible to achieve without new trade agreements and greater foreign investment. And the world desperately needs Africa's critical minerals to power emerging technologies – especially if runaway climate change is to be avoided. And as Africa is by far the world's youngest region, its growth will be a major determinant of international security, global labour supply and migration for decades to come.

None of these challenges will be met if politicians sway elections with fake content, helping underperforming governments cling to power. Ever-more-convincing digital propaganda will make it increasingly difficult for citizens and opposition groups to speak out against rulers who do not deliver on their promises. This is especially true as tens of millions more African citizens will come online for the first time in the coming years.

Cloaking itself in AI-rendered caricatures of sovereignty, Traoré's military government has centralised power, nationalising key portions of its mining sector, militarising the government and silencing criticism. This is despite ISS African Futures research showing that overcoming

Chart 2: Median age per region, 1960–2025



Source: International Futures (data from 2024 are forecasts)

economic fragility requires integrated policy reforms to facilitate private-sector development and economic diversification. However, there are ways to push back.

Disinformation campaigns targeting African voters often display the same hallmarks across jurisdictions – a legacy of the Russian template pioneered by the Wagner Group mercenary outfit. Donor countries, especially Western ones, can help by providing funding and bespoke training for African journalists and researchers to enhance their ability to spot how African autocrats turn established tactics of foreign interference inward.

Accountable governance elsewhere offers voters an alternative to strongman rule

Officials and policymakers elsewhere on the continent can also provide more support for implementing the African Commission's resolution on online information integrity. Meanwhile, cultivating digital literacy is paramount to contain the virulence of fake content. Most social media posts feeding the myth-making around Traoré, for instance, come from outside Burkina Faso. Countries such as Ghana, Kenya and Nigeria are leaders in building national digital literacy programmes, offering a roadmap for other jurisdictions to adapt to their needs.

Structural solutions

African leaders must also draw more attention to the paradox of foreign-agent laws, particularly how their autocratic peers weaponise them for anti-democratic purposes. Much of the attention on countering disinformation focuses on legal frameworks for mitigating cybercrime or foreign interference. But these can be ill-suited to address digital influence campaigns. Such laws tend to be malleable enough that bad actors can readily wield them against civil society by falsely conflating criticism of domestic policies with foreign attempts to destabilise the government.

Yet the surest way to puncture authoritarian propaganda in the digital age is by example. Other African governments should model responsive governance that improves citizens' security, basic services and economic opportunity – and communicate it creatively on the same platforms where strongmen pitch their false realities. Visible, accountable governance elsewhere can offer voters a compelling alternative to strongman rule.

Infrastructure a must to boost Africa's AI sovereignty

At its 1 339th session in Addis Ababa, Ethiopia on 16 April 2026, the AU Peace and Security Council (PSC) took up AI, evaluating its implications for Africa's governance, peace and security. The meeting acknowledged Ethiopian Prime Minister Dr Abiy Ahmed's designation as the AU Assembly AI and digital health champion and underscored the need for Africa to shape, control and assert sovereignty over AI within the broader ecosystem.

These ambitions are backed by a growing normative architecture. The Malabo Convention on Cybersecurity and Personal Data Protection, together with the continental AI strategy, provides Africa's roadmap to AI sovereignty. To operationalise the agenda, the PSC established the AI Advisory Group on Governance, Peace and Security at its 1 214th session to implement the AU AI agenda from 2024 to 2028. The group has five members, one per AU region, with a sixfold mandate covering AI governance in peace and security, as detailed in its information toolkit.

Although the PSC and the AU Commission have made commendable norm-setting advances, the approach remains defensive for many policymakers and experts. Some argue that the AU is trying to regulate something Africa doesn't own or have sovereignty over. This raises a more fundamental question: can Africa achieve AI sovereignty without first closing its infrastructure gap?

Ambition vs infrastructure gap

The AI strategy and the advisory group toolkit clarify AU objectives, as summarised in the chart below. First is setting norms for a safe environment for AI use across domains, including governance, peace and security. Second is institutional control of AI through data protection and countering AI-enabled disinformation, cyber-threats and digital interference. Third is advocating AI-powered tools to enhance conflict anticipation/prevention and, ultimately, improve African citizens' safety and socioeconomic conditions.

In the absence of infrastructure that enables homegrown AI and effective data control, any bid for AI sovereignty will be difficult to sustain. AI infrastructure, according to an information technology expert consulted, comprises four layers: electricity and power supply, computing hardware (graphics processing units, datacentres and servers), cooling and physical infrastructure, and connectivity and data ecosystems. Large language models such as OpenAI's ChatGPT, Google's Gemini and Anthropic's Claude require tens to hundreds of megawatts each – a threshold Africa's power supply cannot reliably meet.

According to the International Energy Agency, Africa represents only 3% of global electricity generation and installed power capacity. The power system is unevenly distributed, with South Africa and North Africa accounting for 65%, even though they represent less than 20% of Africa's population. This deficit is confirmed by the Institute for Security Studies' African Futures, which states that 600 million African citizens remain without electricity.

On current trends, 543 million people will remain without electricity. Such weak, unreliable supply, coupled with shrinking financial resources, prevents the development

Chart 3: Objectives of the continental advisory group's four-year mandate

1	Assessing the impact and implications of AI on peace, security and governance in Africa
2	Promoting the integration of AI into peace, security and democratic processes
3	Supporting responsible use of AI in security and military contexts, in line with international law
4	Countering AI-enabled disinformation, cyber-threats and digital interference
5	Promoting AI-based early warning systems for conflict prevention and response
6	Supporting inclusive AI governance, data protection and cross-border cooperation

Source: PSC communiqué 1 214 (2024) and advisory group information toolkit (2026)

of the computing hardware and connectivity systems that AI requires. Internet access compounds the problem: in 2023, for instance, only 34% of Africa's population had internet access, well below the global 66% – a gap driven primarily by inadequate infrastructure investment.

Risks

AI sovereignty is the ability of a state, institution or company to develop, host, regulate and use AI systems with meaningful autonomy, rather than over-relying on external infrastructure, cloud providers and datasets. The infrastructure deficit impedes the development of two core elements – datacentres and data-hosting servers. Africa's AI ecosystem is already dependent on US, Chinese and European firms and Middle Eastern datacentres. This renders Africa a consumer of imported AI rather than a sovereign and reliable producer.

Endogenous investment across the AI ecosystem is the only path to meaningful sovereignty

Dependence on external providers also creates acute data control and ownership challenges. AI models, particularly large language models and those built on machine/deep learning, require massive datasets spanning sensitive domains – healthcare, finance, biometrics, security. The risks of informational dependency, foreign ecosystem dominance and political influence remain high. Countries and companies that own and/or host key AI infrastructure could leverage their control to achieve strategic, economic or political goals. This is particularly plausible amid current geopolitical fragmentations.

Options

Closing the gap requires massive infrastructure investment. Annual needs are estimated at cost of US$130–US$170 billion, against current investment of US$80 billion. Closing the energy gap alone requires US$64 billion annually by 2030. To sustain Africa's AI ambitions, much more will be needed, according to experts consulted by the *PSC Report*.

A first step could be Grand Inga Dam, an Agenda 2063 flagship. At a projected capacity of 43 200 megawatts, it would go some way toward meeting Africa's average need of 110 000 megawatts — and success could pave the way for continent-wide duplication.

Internet connectivity should be expanded to support large language models, as well as for computer vision, robotics and other AI, essential to domains such as health, education, defence and intelligence. Endogenous investment, blending AU member states and the African private sector, would enable Africa's AI sovereignty across the ecosystem, including power generation and internet provision. The Programme for Infrastructure Development in Africa, under the AU's auspices, offers a ready vehicle to advance this agenda.

AFRICA GENERATES ONLY

3%

OF GLOBAL ELECTRICITY – AI REQUIRES HUNDREDS OF MEGAWATTS

Africa must prepare for AI-powered cyberthreats at scale

Anthropic's recent threat intelligence report reveals how malicious actors are using its own AI agents to conduct cyberattacks, surveillance operations and online influence campaigns. Africa's leaders should be especially vigilant, it warns, given the continent's relatively low digital literacy rates, digital divides and the gap between the pace of AI availability and regulatory lethargy. Citizens are vulnerable to data theft, surveillance at scale and being duped in AI-driven influence campaigns.

The report focused on malicious applications of its AI agent Claude, which is used by about 30 million people worldwide. Those using Claude to mislead include state propaganda institutions, their proxies, politically motivated individuals, criminal groups and commercial entities. Case studies were found in Kenya, Central African Republic, Democratic Republic of the Congo, Sudan and Mali.

AI and crime

AI is being used not simply to create content that deceives users, but as a scaling tool. For example, it enables the rapid generation of multiple social media posts as part of influence campaigns or the writing of tens of thousands of pieces of malicious code that can outpace swift detection. In the wrong hands, Claude can scan computer networks for vulnerabilities and identify phishing targets. Interpol recently warned that 55% of all reported cybercrimes across Africa were AI-enabled.

Currently, human involvement features in most intrusions, Alpha Group Chief Information Officer Justin Hornsby told *ISS Today*, but fully automated attacks could happen. He said tighter controls are needed, including strict rules on which AI models an organisation's staff used and restrictions on data access.

Anthropic's investigation found that its AI agents collected information, conducted 'reconnaissance missions' and built the infrastructure to hack into an (unnamed) North African government technology authority. More than 300 000 national identity records and data from 500 000 companies in the country were exposed.

Potential vulnerabilities across Africa are vast. Some 45 governments are now running digital systems to improve service delivery, according to the African Union Development Agency. As more countries shift towards e-government, exposure to AI risks will increase unless safety controls are ramped up.

> Some 300 000 identity records and data from 500 000 companies in a North African country were exposed

Some Claude models have been used for surveillance operations in Mali, with Anthropic revealing the agent could breach safeguards to target and profile opposition figures. Likewise, concerns are growing about AI attacks on South African street cameras and other linked devices. Some experts are calling for the country's information regulator to review its rules, as these are struggling to keep pace with technological change. But Claude's use has arguably been the most staggering in producing influence campaigns at scale across African countries. Several have been linked to foreign actors, with Russia a key player.

Synthetic media threats

In Central African Republic, investigators detected a web of fake radio stations producing AI-generated content. These actors used Claude to strip away formatting, a sign that material has been synthetically produced. This makes it harder to detect, even by defensive AI systems. Investigations in the country into information manipulation have found that local agents hired by Russia's Wagner Group were tasked with producing pro-Russia content for local audiences.

Anthropic claims that the Democratic Republic of the Congo was part of a network producing fabricated news. Its investigators found 318 articles across several fake news sites that were created and populated with content produced by the company's AI agents. It says Claude appeared to have 'humanize[d] and refine[d] batches of

50 pre-drafted topics and tweets', enabling vast quantities of content to be distributed without adequate human moderation.

Claude has also been used for homegrown influence campaigns, being harnessed to generate batches of 50 tweets made to 'look like spontaneous grassroots commentary rather than a coordinated campaign' ahead of next year's Kenyan elections. Among the false narratives was that Kenya's opposition was 'breaking apart'.

Such astroturfing campaigns, which try to mimic organic engagement, featured previously in Kenya's elections. As in the other cases, Claude planned campaigns, chose targets and created content, exploiting AI's ability to accelerate information distribution.

While Anthropic says it was able to disrupt most of these campaigns, it acknowledges the need for better detection and prevention. This requires intelligence sharing between private sector and government partners. Yet the recent Pentagon boycott of Anthropic in the US may signal a reluctance among governments and tech companies to work together.

Many attacks involving Claude have been linked to foreign actors, with Russia a key player

In countries such as South Africa, which leads the continent in indigenous AI innovation, a siloed approach to cybersecurity persists. Threat intelligence may be shared informally between, for example, banks and government branches, but systematic sharing is slow. The country has a new private-sector-driven Africa cybersecurity centre of excellence, but the state-led cybersecurity coordination centre, promised a decade ago as part of the National Cybersecurity Policy Framework, has not materialised.

Despite being increasingly vulnerable to cyberattacks, South Africa lacks an AI strategy and government agencies invest two-thirds less than corporates in cybersecurity. The state also uses out-of-date legacy systems that are harder to fix, according to experts at a recent tech conference. In contrast, Nigeria, which almost matches South Africa in AI development, has a policy that commits it to responsible, ethical AI development and deployment.

Government regulations

OpenAI's September revelation that its AI agents interacted with US government websites in 'unexpected ways' and unconfirmed reports that the same agents tried unsuccessfully to hack into a US government website have heightened global concerns.

Introducing basic AI usage policies in African countries is an important starting point. Employees and government workers tinkering with AI could not only feed sensitive information into public large language models, but expose themselves and their organisations to further intrusions.

IN SOUTH AFRICA, LEADER IN AFRICAN AI INNOVATION, THE APPROACH TO CYBERSECURITY IS SILOED

Ethiopia charts Africa's path to AI sovereignty

Ethiopian Prime Minister Abiy Ahmed's role as AU AI champion offers opportunity to advance the continental AI strategy. Her Excellency Lemlem Fiseha Minale, Ethiopia's ambassador to the AU, shared her hopes for African-financed energy, digital infrastructure, skills and governance that will allow the continent to develop AI on its own terms

Prime Minister Abiy's appointment as AI champion places Ethiopia at the helm of implementing continental AI policies. What does this mean for the country and what are his priorities?

The appointment was opportune as Africa seeks its rightful place in the digital revolution. The priorities will include placing AI and digitalisation firmly on the policy agendas of African states and strengthening national and continental investment in digital literacy, cyber-infrastructure and digital startups. The Prime Minister will also promote cooperation to bridge the digital divide and ensure the inclusion of African languages.

He will lead efforts to develop responsible AI governance frameworks that promote ethical and accountable AI use. Drawing on Ethiopia's growing experimental capability, the Prime Minister will advocate the application of AI to Africa's development challenges, including improving agricultural productivity, healthcare, education and public service delivery.

What continental and national progress has been made since the 2024 publication of the AU AI strategy?

Despite continuing challenges – particularly in infrastructure, financing, skills development and effective governance – encouraging progress has been made in preparing for the practical application of AI. All AU member states are mainstreaming digitisation and countries are developing strategy-aligned national frameworks. Ethiopia has established an AI institute and is founding an AI university.

The AU Commission signed a memorandum of understanding with Google in February 2026 on cooperation in AI development and governance, research and innovation. It includes a commitment to train three million students and teachers across Africa by 2030, providing free access to tools such as Gemini Pro and additional support for local languages, including Amharic. The AU Development Agency-New Partnership for Africa's Development has launched a complementary continental AI roadmap, while regional economic communities such as the Intergovernmental Authority on Development are developing a common regional artificial intelligence framework and strategy.

Ethiopia has established an AI institute and is founding an AI university

The AU PSC has established an advisory group on AI, Peace, Security and Governance, which is crafting a common African position on and an African charter on AI. During Ethiopia's PSC chairship in April 2026, the Council addressed AI governance, peace and security – all key to achieving strategy targets, particularly generating wealth from AI and ensuring safe and secure use to advance society.

During Ethiopia's recent chairship of the PSC, concerns were raised about the misuse of AI. How do you view the challenges and what sustainable measures should be taken?

AI-enabled cybercrime has increased markedly, while foreign and domestic non-state actors continue to use it to fabricate fake news and destabilise domestic politics. Its proliferation in the military and potential exploitation by terrorist groups are extremely worrying.

African countries' data sovereignty is vulnerable because most AI companies are controlled by major powers outside the continent. Thus, African data could fall into the wrong hands. At its 1 339th meeting, the PSC called for stronger African AI governance and coordination through effective continental and national regulatory frameworks, accelerated development



Her Excellency Lemlem Fiseha Minale

of a common African position on AI and policies to safeguard digital sovereignty.

Calls were voiced for faster integration of AI into continental peace and security mechanisms, particularly for early warning, conflict prevention and risk analysis. The need for stronger member-state capacity to identify and respond to emerging threats was emphasised. These efforts require investment in African AI infrastructure through domestic and international financing for digital infrastructure, research and skills development. They also need technology transfer and cooperation to enable Africa to develop, govern and benefit from AI on its own terms.

If implemented effectively, these decisions and other continental and national initiatives will ensure that Africa is not left behind in discussions about the future of AI.

What steps should be considered to overcome uneven distribution of energy production and overdependence on external providers that compromises data control and ownership?

AI and the digital economy have hastened the need for adequate energy provision and universal access. Investment must increase to develop Africa's diverse hydropower, geothermal, solar and wind resources, while nascent initiatives to build nuclear energy facilities should also be supported. Under the Programme for Infrastructure Development in Africa, the continent can ensure political commitment and financial resources to realise all energy projects, including the Grand Inga dams. Ethiopia is making significant strides, having completed the self-financed 6 000MW Grand Ethiopian Renaissance Dam and launched an energy diversification programme.

African countries must build their own digital infrastructure and governance systems. The strategy's 'local first' priority is crucial in supporting local talent and ecosystems. This will advance AI solutions that serve the public interest and respond to the continent's needs and priorities, while respecting and preserving its cultural values and customs.

The Pan-African University Institute for Basic Sciences, Technology and Innovation, hosted in Kenya, should prioritise AI and expand its reach through programmes across national universities. Investment is needed to integrate African languages through knowledge and infrastructure and developing localised foundation models.

AI and the digital economy have hastened the need for adequate energy provision and universal access

Also essential is a mass digital literacy programme such as Ethiopia's five million coders initiative, which aims to mainstream data education among students and professionals of different ages, particularly schoolgoers.

Financing AI could overstretch African economies. How could the member states secure resources to safeguard AI sovereignty and reduce dependence on external providers?

Domestic financing and self-reliance should be priorities, combining public and private financing. The AU Digital Transformation Strategy (2020 to 2030) advocates partnerships among African actors and harmonised continental, regional and national digital entrepreneurship efforts.

Feasible measures include an online portal through which African entrepreneurs, startups and small and medium-sized enterprises could market their services and skills, and encouraging AU states to source services from local entrepreneurs. They also include creating a conducive environment for digital startups and financing innovation hubs with the private sector. Financing the digital economy is an investment in the

future, with benefits across socioeconomic and security sectors. Bilateral and multilateral cooperation should be maximised while ensuring protection and security.

At the 1 339th session, the PSC asked the AU Commission to finalise the comprehensive study on AI's impact and the common African position. What progress has been made and how could a common position make a difference?

The advisory group, comprising members from the continent's five regions, is carrying out the Council's instructions through consultations with national institutions, the private sector and experts. The PSC is to receive the group's report at its forthcoming sessions.

How, in your view, could African countries, through the AU and individually, reap AI's rewards and mitigate its risks?

Achieving universal digital literacy quickly is essential. This will enable citizens to understand and actively participate in the digital economy. More affordable digital technology will broaden access to AI tools and infrastructure and reduce inequality in digital access.

Africa's young population offers immense potential for innovation and creativity. Greater investment in startups and support for entrepreneurship can turn this potential into homegrown AI solutions. At the same time, countries must strengthen legislative and institutional capacity in data protection and cyber-governance to safeguard users and national security.

Africa's population offers the innovation and creativity potential needed for homegrown AI solutions

This requires not only comprehensive legal frameworks that clearly define stakeholders' responsibilities, but consistent regulation enforcement and transparency in digital operations.

Intra-African cooperation will allow countries to share knowledge, resources and best practices, ensuring that AI benefits the continent in a coordinated and sustainable manner.

Read our latest publications on new technologies and Africa at www.issafrica.org









About the PSC Report

The *Peace and Security Council Report* analyses developments and decisions at the African Union Peace and Security Council (PSC). The monthly publication is the only one of its kind dedicated to providing current analysis of the PSC's work. It is written by a team of ISS analysts in Addis Ababa.

About the ISS

The Institute for Security Studies (ISS) partners to build knowledge and skills that secure Africa's future. Our goal is to enhance human security as a means to achieve sustainable peace and prosperity. Using its networks and influence, the ISS provides timely and credible analysis, practical training and technical assistance to governments and civil society.

Contributors to this issue

Maram Mahdi, Researcher, ISS Addis Ababa

Kyle Volpi Hiebert, Deputy Editor, Africa Conflict Monitor

Moussa Soumahoro, Researcher, ISS Addis Ababa

Karen Allen, ISS Consultant and former BBC foreign correspondent

Ambassador Lemlem Fiseha Minale, Permanent Representative of Ethiopia to the African Union

Contact

Dr Ndubuisi Christian Ani
Senior Researcher and Project Lead
ISS Addis Ababa
Email: apsg@issafrica.org

Development partners

The publication of the *PSC Report* is made possible through support from the Government of the Netherlands and the Government of Denmark. The ISS is also grateful for the support of the following members of the ISS Partnership Forum: the Hanns Seidel Foundation, the Open Society Foundations, the European Union and the governments of Denmark, Ireland, the Netherlands, Norway and Sweden.

© 2026, Institute for Security Studies

Copyright in the volume as a whole is vested in the Institute for Security Studies and the authors, and no part may be reproduced in whole or in part without the express permission, in writing, of both the authors and the publishers.

The opinions expressed do not necessarily reflect those of the ISS, its trustees, members of the Advisory Council or donors. Authors contribute to ISS publications in their personal capacity.

Cover image: Sankai/Getty Images

ISSN 2075-6232