UNIVERSITY OF LEEDS
School of Law

KONRAD ADENAUER STIFTUNG

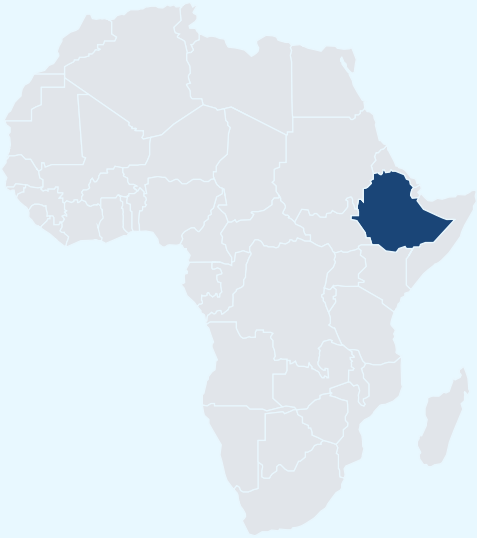
Artificial Intelligence and Cybersecurity in Ethiopia: Mapping the Interface

A Policy Brief

By

Kinfe Yilma (PhD)
Senior Lecturer, School of Law
University of Leeds

May 2026



KAS Office Ethiopia/African Union

Konrad Adenauer Stiftung e.V.
Yeka Sub-City, #165
Diaspora Street

Tel: +251-115-577-644
E-Mail: info.ethiopia@kas.de
P.O.Box 110337
Addis Ababa, Ethiopia

https://www.kas.de/en/web/aethiopien/

Table of Contents

About this Brief

Ethiopia stands at a pivotal moment in its digital transformation. As the country embraces artificial intelligence to advance development ambitions, it is simultaneously entering a more complex and fragile cybersecurity environment. This policy brief responds to that emerging reality. It examines how current Ethiopian policy frameworks engage, with notable gaps and some promise, the growing intersection between AI and cybersecurity.

While recent initiatives, including the 2024 National AI Policy and the revised cybersecurity policy, signal important political commitment, this brief finds that they do not yet fully reckon with the dual nature of AI as both a tool for strengthening and a source of vulnerability for digital security. Key policy instruments tend to address cybersecurity and AI in isolation, leaving their rapidly evolving interface underexplored and insufficiently governed.

This brief is grounded in the recognition that cybersecurity is not merely a technical concern but a matter of public trust, institutional resilience, and human rights protection. It situates Ethiopia's policy trajectory within broader global developments, while remaining attentive to local institutional realities, capacity constraints, and the risks of adopting global technological narratives without adequate contextualisation. In doing so, it offers a balanced perspective, acknowledging the country's progress, while critically engaging with its blind spots, including fragmented policy approaches, overreliance on future strategies, and a tendency toward techno-optimism.

Above all, this brief seeks to contribute constructively to ongoing policy processes. It is intended as a practical resource for policymakers, regulators, and stakeholders working to ensure that Ethiopia's digital future is not only innovative, but also secure, rights-respecting, and resilient.

Happy Reading!

Sincerely,
Alemnew Gebeyehu
Project Manager/Ethiopia
KAS Office Ethiopia/African union

Executive Summary

Recent years have seen widespread enthusiasm around the potential of new and emerging technologies in fueling development globally. Unprecedented advances in generative Artificial Intelligence (AI) and machine learning (ML) appear to have taken this to new heights. Governments are investing considerable resources to harness the potential benefits of AI to advance national development and geopolitical priorities. However, AI presents not only opportunities but also risks that require robust governance arrangements. Cybersecurity is one of the domains where the risks as well as the opportunities of AI are emerging more clearly. In the past few years, AI tools have been deployed to launch sophisticated attacks in various jurisdictions. With further investments in AI research and development, the risks of complex, subtle and increasingly adaptable attacks against digital infrastructures, including critical infrastructures, are bound to steadily increase. Ethiopia has taken a series of steps to harness the potential benefits of AI to its fledgling economy. From creating an AI institute with a wide-ranging mandate to a plan to open a public 'AI university', the country has slowly jumped to the AI hype bandwagon. This policy brief examines Ethiopia's policy readiness to the cybersecurity challenges as well as opportunities that AI presents. Ethiopia has recently issued a series of policy initiatives, including a national AI policy. Nevertheless, the serious risks that AI poses, including risks to cybersecurity, are yet to receive adequate policy attention. The policy brief further finds that other sectoral policies, particularly the national cybersecurity policies, offer little guidance. Ethiopia has recently broached a policy process to develop strategies that seek to implement both the AI and cybersecurity policies. If approached judiciously, these strategic policy instruments may go a long way in filling the void left by the policies. The policy brief closes with a series of recommendations to relevant Ethiopian policymakers and other stakeholders.

Acknowledgment

The author gratefully thanks Konrad-Adenauer-Stiftung, particularly Alemnew Gebeyehu, Project Manager/Ethiopia, for providing all forms of support in developing this policy brief. This policy brief was conceived as part of the workshop on AI and cybersecurity convened by KAS in collaboration with the Ethiopian Cybersecurity Association in Addis Ababa on 20 December 2025. The author thanks the Association, particularly Dr Berhanu Beyene and Ms Seble Girma, for enthusiastically supporting the initiative. Finally, Mr Mnyichil T. Manaye provided various forms of support during the course of this initiative for which the author gratefully expresses gratitude.

Acronyms

AI	Artificial Intelligence
CoE	Council of Europe
EAII	Ethiopian Artificial Intelligence Institute
EU	European Union
ICT	Information and Communication Technologies
INSA	Information Network Security Administration
LLMs	Large Language Models
ML	Machine Learning

01

Introduction

The advent of artificial intelligence (AI) has brought forward a range of opportunities, disruptions and risks in almost every domain of human activity. From agriculture, healthcare to education and climate mitigation, recent policy initiatives tend to put AI at the center of discussion. Cybersecurity has been no exception. AI brings both opportunities and risks to the protection of digital infrastructures. Emerging AI capabilities may enhance the ability to quickly detect exploits, enhance cyber defences and even make response to cyberattacks effective. But risks also exist, including the sophistication and scalability of cybersecurity threats. Recent years have seen several AI-enable cyberattacks around the world. A more recent example is the attack against British engineering firm Arup who lost $25 million to a scam involving an AI generated deepfake image and voice of the company's CEO (CNN, 2024). Lingo, an American telecom company, was fined $1 million by the US Federal Communications Commission for a fraudulent AI-generated robocall with the fake voice of former President Biden to voters in New Hampshire (TechDirt, 2024).

To overcome such challenges as well as to embrace opportunities, a number of governance measures are being taken across jurisdictions. Governance measures often take either of two forms. One relates to tailored updates to national and regional cybersecurity policies and laws. Instead of a distinct AI-centred legislative or policy response, this form of governance initiative introduces patches to gaps in existing rules and procedures in manner that attend to not only the risks but also to harness AI for robustly securing digital infrastructures. The second approach tends to respond to AI benefits and risks as part of the broader AI governance initiatives. Such initiatives can be either broader national AI policies or strategies in which cybersecurity is addressed as one area of policy intervention. In jurisdictions where dedicated AI legislation is introduced or proposed, cybersecurity risks are treated merely as parts of broader AI risks that such legislation seeks to mitigate .

> This policy brief seeks to explore the extent to which Ethiopia's relevant policies attend to the risks as well as opportunities that AI presents to cybersecurity.

Ethiopia has a number of digital policy and legal instruments dealing with the security of digital infrastructures, including a National cybersecurity Policy (2024). The cybercrime law, adopted in 2016, is currently the only operative piece of legislation on cybersecurity. Ethiopian policymakers have introduced AI focused policies and legislation in recent years, namely the National AI Policy (2024) and the draft AI law. The policy brief explores whether or the extent to which these policy instruments deal with the opportunities and risks that AI presents to cybersecurity. The analysis demonstrates that while recent AI governance initiatives appear to deal with cybersecurity broadly, little attention is given in other policy instruments—including in the cybersecurity policy. The draft National Cybersecurity Policy Implementation Roadmap recently unveiled by the Information Network Security Administration (INSA) appears to fill this gap, to a degree. Further policy attention is, however, desirable to fully address the interface between AI and cybersecurity.

The rest of the policy brief moves in four sections.

Section 2 offers a brief account of how the advent of AI transforms cybersecurity. It discusses the ways in which AI offers opportunities but also poses further risks to the security of digital infrastructures. Section 3 explores the extent to which Ethiopian policy instruments—both existing and emerging— address the opportunities and risks to cybersecurity discussed in the preceding section. It shows the shortcomings in existing and emergent cybersecurity policies as well as AI governance initiatives that have emerged in recent years.

Section 4 offers a series of recommendations to Ethiopian policymakers towards making the cybersecurity legal and policy frameworks fit for purpose in the age of AI. Section 5 closes the policy brief with some final remarks.

For purposes of this policy brief, cybersecurity represents the series of rules, procedures and technical systems that are deployed to protect and defend data, critical digital infrastructures, networks and individual rights from malicious attacks, breaches or vulnerabilities. While cybersecurity is often portrayed as the security of the technical infrastructure, the ultimate subject of protection are individual citizens as well as broader public interests. AI, on the other hand, refers to the suite of technologies with the potential to perform complex tasks such as problem-solving, perception reasoning, learning and language cognition that would normally require human intelligence.

The AI Factor in Cybersecurity

The advent of AI is poised to transform cybersecurity. A recent survey finds that AI has already begun to transform the cybersecurity landscape (Boston Consulting Group, 2025).

AI systems, including machine learning (ML) and deep learning, can be a means of enhancing cybersecurity but can also be a source of harm if they remain unchecked (Katina Michael et al, 2023: 107). This may mean the rise of novel and sophisticated cybersecurity threats thereby undercutting the ability of organisations and governments in ensuring public safety. It may also mean new and better ways of preventing or responding to cyberattacks against the security of digital infrastructures and protecting citizens. By way of background, this section discusses the ways in which AI transforms cybersecurity. We first consider how AI reshapes the nature and scope of cybersecurity challenges. We then proceed to briefly discuss the opportunities that AI may present towards enhancing cybersecurity.

02

2.1. Challenges

The novel challenges that AI poses to cybersecurity may take various forms. In this section,

we flag only some of the major challenges to illustrate the dynamic and rapidly evolving digital ecosystem. Threats to cybersecurity evolve with technological developments. New and emerging technologies often provide new ways of undermining the security of digital systems, including critical infrastructures. Attackers are constantly adaptive to rapid technological advances that may allow identifying vulnerabilities and launching attacks at a larger and sophisticated manner. With the rise of AI, the challenges of defending digital systems from such attackers becomes even more pronounced (Blessing Guembe et al, 2022).

AI makes threats more 'intelligent'. As AI enables automated and autonomous ways of decision-making, it may be deployed by attackers to easily plan and perpetrate attacks with little human input. Attacks may, for instance, deploy AI tools to 'hunt' for vulnerabilities at a scale that was not imaginable a few years ago. By blurring the line from what is real and fake, AI tools may further complicate phishing attacks. The concern with the AI factor is that it could effortlessly undermine the resilience of cyber defences and complicate possible responses.

Scalability of threats is the second challenge that AI poses to cybersecurity (Miles Brundagee et al, 2018). As threats become automated, the scale of the attacks is bound to increase considerably. Automated machines enable not only more attacks but that the reach of these will be significant. Once vulnerabilities are identified at a large scale, a single attacker may launch attacks of various forms at various entities at once. Such large-scale, automated attacks would cause significant disruption but also restoring services and planning potential responses would be resource intensive, and require more time than before.

> AI also offers the possibilities of making cybersecurity threats, including actors behind such actors, subtle (Masike Malatji and Alaa Tolah, 2025: 894).

That is the third unique challenge. While technologies offer ways of making attribution harder, AI is likely to make this even harder. AI-enabled attacks such as malware may remain hidden for quite some time undiscovered. Subtleties of AI-enabled cyberattacks are yet to fully emerge but the advent of deepfakes signals as to what is yet to come.

AI may also further 'democratise' cyberattacks. The proliferation of large language models (LLMs) which can be accessed with little, or no fees are likely to enable cyberattacks by anyone with malicious intent. By providing easy access to the means, cyberattacks may no longer be the exclusive preserve of attackers with sophisticated knowledge of computers or organised criminal groups. That makes cybersecurity non-niche and ubiquitous, thereby expanding the scale and breadth of cyberattacks (Masike Malatji and Alaa Tolah, 2025).

2.2. Opportunities

> Beyond the challenges highlighted above, AI may also offer opportunities to strengthen cybersecurity readiness, defenses and responses. That may take at least three forms. One is that AI can enable governments and organisations to preemptively predict and detect emerging threats.

AI's predictive capacity, albeit imperfect, can allow it to identify sources and forms of cyberattacks before they are even launched. AI tools, particularly generative AI, may provide a fertile ground to enhance cyberthreat intelligence that allow to preemptively identify vulnerabilities, anomalous network access, hidden attack patterns (Maanak Gupta et al, 2023: 80220). This might involve email content examination, historical malicious activity recognition, and threat classification for enhanced investigation (Selcuk Okdem and Sema Okdem, 2024: 4, 8). Automated identification of exploits can help countries to quickly fix bugs and hence prevent future attacks.

AI tools may also be deployed post cyberattacks. For complex attacks such as ransomware that might modify its internal structure, AI tools would be useful in undertaking dynamic analysis solutions that are crucial to expedite feature extraction (Selcuk Okdem and Sema Okdem, 2024: 10). That would be central to timely detect specifics of offensive tactics employed (Katina Michael et al, 2023: 104). By further integrating such details with other insights drawn from LLMs, it may contribute towards identifying actors behind cyberattacks. Where the attacks are ongoing, AI tools may also provide the means to take instant defensive measures.

AI may also offer new techniques that modernise cybercrime investigation. For example, AI tools may contribute towards the collection of digital evidence through analysis of digital fragments left by attackers a lot quicker (Suguna Balusamy et al, 2025). Drawing on analysis of huge volumes of data extracted from computers, investigators may be able to perform rapid forensic examinations and possibly identify perpetrators of cyberattacks as quickly as possible. AI tools such as ML may therefore contribute greatly to evidence collection and analysis with more speed, accuracy and efficiency. This, of course, requires considerable investment not only in AI tools by police forces but also training investigators on the basics of deploying AI for investigative purposes.

AI may also be deployed to respond to cyberattacks. Once cyberattacks occur, AI tools might also help in synthesizing huge volumes of data such log files and network traffic. This would enable one to quickly respond to cyberattacks (Maanak Gupta et al, 2023: 80220). Strike-backs, cyber-attacks taken in response to prior attacks, are likely to be launched in a more sophisticated, effective and timely manner than before. While the legality of such attacks in international law is less clear, AI may enable countries to deploy AI as part of their response to large-scale attacks against state and non-state actor attackers.

03

The Ethiopian Policy Landscape

In the past decade or so, Ethiopia has seen considerable investment towards harnessing new and emerging technologies for national development.

The government has long recognised the role of information and communication technologies (ICTs) in fuelling developmental ambitions. Starting with the first national ICT policy of 2002, succeeding digital policies—the most recent being Digital Ethiopia 2030—highlight the need to marshal technologies in alleviating the nation's longstanding socio-economic challenges. This drive to digitise the nation has faced, from time to time, cybersecurity challenges. INSA officials routinely report successes in defending nations against cyberattacks. A more recent report, for instance, documents 13, 494 cyberattacks that the agency managed to prevent (INSA, 2025). Although only defensive successes are officially reported, the country has no doubt been a victim to many attacks that had penetrated whatever defences in place over the past decade or so (Yilma, 2014).

As the nation moves to enthusiastically embrace AI, threats to its critical digital infrastructure are bound to grow exponentially. But it is not clear the extent to which Ethiopia has in place a robust policy regime that not only recognizes the benefits but also the threats that AI poses to digital security. This section discusses the extent to which or whether relevant policy instruments in Ethiopia address the interface between AI and cybersecurity. The analysis focuses on the national cybersecurity and AI policies that have been rolled out in the past few years. As shall be shown below, existing policies do not directly or sufficiently deal with the cybersecurity implications of new and emerging technologies such as AI. We consider further whether this gap would be addressed by policy instruments that are currently being developed under the auspices of INSA and Ethiopian Artificial Intelligence Institute (EAII).

3.1. Cybersecurity Policies

Cybersecurity, including cybercrime, has been one aspect of digital governance that received considerable attention by Ethiopian policymakers. From the first set of cybercrimes codified in the 2004 Criminal Code to the 2011 Information Security Policy and the 2016 computer crime proclamation, cybersecurity has received relatively better policy attention. Ethiopia introduced the first cybersecurity policy in 2011 with the adoption of the National Information Security Policy.

Albeit abbreviated, the Information Security Policy offered high-level direction in dealing with the threats to the nation's fledgling digital infrastructure. As the name readily suggests, the Information Security Policy's focus revolves around protection of 'information' rather than security of digital infrastructures more broadly. Moreover, the stated 'object' of the policy were information structures operated by the government, thereby excluding infrastructure operated by non-state actors (National Information Security Policy of Ethiopia, 2011: 2). That constricted its normative remit considerably. The policy has recently been replaced by the national cybersecurity policy, adopted by the Council of Ministers in June 2024. While the 2024 Policy offers a relatively better policy direction, it remains truncated. This has also limited the extent to which it considers the interface between new and emerging technologies such as AI and cybersecurity.

The cybersecurity policy does not fully address, or consider, the implications of emerging technologies to cybersecurity. It does not go beyond highlighting the inherent technological dynamism and the threats to cybersecurity that comes with it (National Cybersecurity Policy, 2024: 22). That also means the policy does not see new and emerging technologies as a means of strengthening the security of digital infrastructures. That is a significant gap, especially given that the Policy was adopted at the time of incredible AI hype at the national and global levels. Most national cybersecurity policies adopted in recent years clearly recognise both the promises and challenges that AI presents to cybersecurity.

The United Kingdom's cybersecurity policy, adopted in 2022, recognises the value of AI in threat detection as well as a means of automated response to cybersecurity threats (Government Cybersecurity Policy of the United Kingdom, 2022: 48). As discussed in Section 3, AI promises ways of furthering the objective of the policy in strengthening cybersecurity in theface of rapidly changing threats.

INSA has recently launched a process to develop a national cybersecurity roadmap (Draft National Cybersecurity Policy Implementation Roadmap, 2025). The aim of the roadmap is to provide for mechanisms of giving effect to the cybersecurity policy. A central part of this effort is to define the respective role of various stakeholders in the implementation of the policy. A cursory review of the draft roadmap reveals that considerable attention is given to the ways in which AI and ML tools may be marshalled towards cybersecurity purposes. Examples include deploying AI tools in modernising digital forensics, threat detection as well as in raising public awareness (Draft National Cybersecurity Policy Implementation Roadmap, 2025: 20-23). To that degree, the draft roadmap addresses some of the void left in the cybersecurity policy.

But there remain at least two shortcomings in the approach taken in the roadmap with respect to emerging technologies broadly and AI in particular. One is that parts of the roadmap dealing with AI are tucked away in tables appended to the text. That makes them read as incidental, as opposed to crucial, elements of the proposed policy instrument. The second concern relates to the lack of focus on challenges that such technologies pose. The focus in the draft appears to be exclusively on the opportunities that emerging technologies such as AI provide in building robust national cybersecurity posture. This also departs from the approach of the national cybersecurity policy which speaks of both opportunities and threats that come with technological dynamism. No doubt, this approach flows from the overall hype around AI in the country that remains blindsided to AI risks (Yilma, 2026).

Commenting on other concerns goes beyond the scope of this policy brief, but they are worth flagging. Among such concerns is the compulsory tone with which the draft roadmap is formulated. At places, the draft roadmap reads like legislation while it is not. The approach taken with respect to international cooperation would need to be revisited to avoid joining doomed treaty regimes such as the Malabo Convention that are unlikely to bear any fruit. But a core concern relates to the desirability of the roadmap as a whole. While the text lays out the rationales for the roadmap, one might question the need to add yet another policy document instead of either revising the cybersecurity policy or launching a legislative process that would give better effect to the policy. Readers should also be reminded that INSA has already in place a document that provides a methodology on developing internal cybersecurity strategies (National Cyber Security Framework Development Methodology, 2022). By providing a template for best cybersecurity best practices, the Methodology essentially sets out a means of fulfilling national cybersecurity policy aspirations.

3.2. AI Policies

National AI policies and strategies have been the principal means of AI governance in Africa in the past few years (Yilma, 2025). Over a dozen countries have introduced or proposed such policy instruments at the time of writing. The adoption of the Ethiopian AI Policy in June 2024 is part of this approach to AI governance in Africa. Of course, the government had partnered with the Tony Blair Institute for Global Change and the AI Good Foundation to develop an AI policy as early as 2020 (Draft National AI Policy of Ethiopia, 2020). The policy adopted by the Council of Ministers in June 2024 was developed through a disparate process overseen by the EAII. The AI policy offers a broad direction that the government will take in harnessing the benefits of AI while at the same time mitigating the risks.

Cybersecurity is among the AI risks that finds some attention in the AI policy. In the section dealing with AI risks, the Policy underlines the importance of robust cybersecurity to build public trust in AI systems (Ethiopian AI Policy, 2024: 12). It discusses the risks of data breaches that may occur as the nation marches towards embracing AI. The policy further emphasises the need to enact data protection legislation, raise public awareness about data privacy and build a 'strong cybersecurity infrastructure' to protect confidential information (Ethiopian AI Policy, 2024: 12). As such, the policy does not directly address the unique and broader threats that AI poses to cybersecurity. Nor does it recognise the opportunity that it may offer in bolstering cybersecurity capabilities in the nation, including in threat detection, investigation and even in effective response to cyberattacks. That means the AI policy does not recognise the interface between AI and cybersecurity fully.

The AI policy outlines the respective role of various government agencies that may have a role in helping realise its goals. In the context of cybersecurity, it briefly considers the role of INSA, albeit vaguely. The policy provides that INSA shall be involved in developing 'systems to adapt and implement AI technologies that enhance service reliability and efficiency' (Ethiopian AI Policy, 2024: 17). It is not clear whether the proposed 'system' is technological or otherwise. For example, it is not entirely straightforward whether this role would involve developing cybersecurity solutions or standards that would need to be embedded into AI systems developed or imported into the country. That further undermines the value of the AI policy in clearly addressing the interface between AI and cybersecurity.

Unlike other African countries, Ethiopian policymakers have not stopped at developing an AI policy. The EAII is, for instance, reportedly developing an AI strategy. Foreshadowed already in the AI policy, the forthcoming AI strategy is aimed at implementing or giving effect to the policy (Ethiopian AI Policy, 2024: 1). That offers another opportunity to further specify and revisit the approach to cybersecurity merely flagged in the AI policy. In particular, the future AI strategy would need to recognise, and deal at some length, the double-edged aspects of AI with respect to cybersecurity.

Policy Recommendations

In light of the foregoing analysis, this section of the policy brief turns to provide a series of recommendations to stakeholders in the Ethiopian cybersecurity landscape.

Safeguarding national digital infrastructures requires the effort, expertise and collaboration of various stakeholders. Among such stakeholders include lawmakers, regulators, policymakers, the technical community, academics and civil society organisations. While the recommendations are targeted primarily at policymakers, other non-state actor stakeholders are also addressed. For purposes of this section, the term “policymakers” refers to all state actors, including legislators, regulatory, policy initiatives and even state-owned operators who may have a mandate or stake in the protection of the integrity of the Ethiopian digital infrastructure, including critical infrastructures.

04

4.1. Policymakers

We call upon Ethiopian policymakers to:

- Revisit relevant policy instruments in a manner that recognises clearly and fully the risks as well as opportunities that new and emerging technologies such as AI poses to cybersecurity. While both the national cybersecurity and AI policies are adopted as recently as 2024, it is vital to provide due attention to the 'AI factor' in cybersecurity. One way of addressing the gap in the policy instruments is through forthcoming implementation documents. The Ethiopian AI Institute is reportedly developing a strategy envisioned in the AI policy with a view to provide specific strategies to give effect to the national AI policy. Likewise, the Information Network Security Administration is reportedly developing a cybersecurity roadmap which seeks to implement the national cybersecurity policy. These ongoing policy initiatives offer an opportunity to fully address the interface between cybersecurity and emerging technologies such as AI.

- Move past the global hype around AI and recognise its multifarious risks, including on the nation's cybersecurity. While the nation has seen considerable digital transformation in the past decade, recent years have seen unchecked techno-enthusiasm that tend to cloud recognition of the attendant risks of emerging technologies—including AI. It is vital to blend the drive towards digitisation with prudent approaches to digital security. That requires a balanced, nuanced approach that goes beyond hype and is informed by local and global realities as well as sound empirical evidence.

- Establish a transparent approach to policymaking that engages relevant stakeholders meaningfully in the process of only developing policy instruments but also enforcing them. Policy makers such as INSA and EAII should engage directly and in earnest with academia, the technical community and civil society groups in planning, designing and implementing policies and laws, including cybersecurity. Moving past the hitherto opaque process would be key in drawing insights, expertise and of course important input from stakeholders who advocate for the public interest in policymaking and regulation.

- Equip relevant government departments with personnel with appropriate training, experience or experience in cybersecurity in particular and the governance of new and emerging technology more generally. As a purely technical domain, cybersecurity requires technical and policy expertise. Ethiopian policymakers should prize meritocracy in recruitment and explore other mechanisms of enhancing the human resource capabilities of the relevant departments. Part of this effort should be sustained and principled cooperation with development partners and jurisdictions such as the European Union (EU), Council of Europe (CoE) and United Nations Office on Drugs and Crime.

- Establish credible, robust and sustained international cooperation with other states, intergovernmental organisations and international organisations working in the field of cybersecurity. As cybersecurity threats are inherently transnational, little could be accomplished with localised capabilities as well as policies. Building bilateral and multilateral cooperation arrangements would be key to meaningfully protect Ethiopia's budding digital infrastructures as well as the rights of citizens from the multidimensional and complex cybersecurity threats. Part of such transnational cooperation might require joining treaty systems such as the CoE's rather advanced regime of cybercrime. Attention should also turn towards sources of credible threats such as certain jurisdictions in Africa and Asia.

- Put the protection of human rights and fundamental freedoms at the heart of cybersecurity efforts. Not only would steps taken to defend and protect digital infrastructures carry risks of undermining individual rights and freedoms but also AI brings forth unique threats to human rights of citizens. The approach to cybersecurity in the age of AI should seek to respect, protect and uphold human rights in line with the nation's international human rights commitments.

4.2. Other stakeholders

We call upon non-state stakeholders, namely academia, private sector and civil society organisations

➤Academia: Academics, researchers and students hold an important role in advancing the nation's effort at developing a robust regime of cybersecurity in the face of complex and evolving threats. Through reasoned, independent and critical research-based insights, members of the academic community are indispensable sources of technical expertise and empirical evidence on cybersecurity. Be it technological or policy/legal, academia should recognise this role and take reasonable steps to move past bureaucratic hurdles and opacities, and share expertise with policymakers.

➤ Private Sector: Local technology companies involved in the development and deployment of AI are key stakeholders in enhancing digital security. In the absence of clear policy guidance or regulatory requirements, the private sector should take a role in advancing best practices in the development of secure AI systems. Part of this effort should be to establish working relations with other relevant stakeholders to collectively attain the aim of making the nation's digital infrastructure secure from AI-enabled attacks.

➤ Civil Society Organisations: Civil society groups that advocate for the public interest are instrumental in making a regulatory regime in line with pertinent laws, including human rights standards. There are barely any civil society organisations working on digital governance in Ethiopia. Much of the advocacy thus far has largely been carried out by global and regional civil society groups. However, it is vital for existing groups with broader mandate to pay attention to policy initiatives and practices in the digital realm. As the country digitalises more, concerns for human rights and fundamental freedoms expand. This would, of course, require working in close collaboration with academia and other relevant stakeholders to gather the raw materials for effective advocacy.

Final Remarks

Ethiopia is taking a series of steps to harness AI towards the goal of achieving its developmental ambitions.

Part of this effort has been the adoption of national policy instruments, primarily the national AI policy. While instruments put forward thus far provide a sound basis for the development of a governance arrangement, little attention is paid to the implications of the AI to cybersecurity. This policy brief showed that the AI policy does not fully recognise the interface between AI and cybersecurity, including opportunities and challenges. Nor has this omission been addressed in the rather niche policy, i.e. the national cybersecurity policy.

In late 2025, a report released by the Ethiopian government decried the fragmentation of national cybersecurity efforts that undermines the ability to effectively respond to cybersecurity threats, including to digital payment systems. To overcome this challenge, the government tasked INSA and the National Bank of Ethiopia to create a joint cybersecurity center (The Reporter, 13 December 2025). Released in the wake of considerable effort around AI in the country, this initiative has the potential to enhance the country's cybersecurity readiness. Offering further glimmers of hope are ongoing initiatives to develop a national cybersecurity roadmap and AI strategy. Envisioned as means of giving effect to or implementing the respective policies, the strategy and the roadmap should be fashioned in a way that views AI both as a source of challenges as well as opportunities for cybersecurity.

05

Corollary to or perhaps the culmination of policy instruments are the introduction of or revisiting appropriate pieces of legislation. The EAII has already begun drafting legislation, the draft of which exhibits clear influence of the EU's AI Act. As the Institute finalises the bill, it will be important to adopt a balanced approach to AI where benefits and risks are addressed meaningfully.

Ethiopia has a largely modern cybercrime legislation, computer crime proclamation No 958/2016. A decade after its adoption, it is advisable to revisit the law to make it fit for purpose in the age of AI. The policy brief hopefully provides the starting point in reimagining the Ethiopian cybersecurity policy and legal landscape in light of the new realities presented by AI.

References.

1. AI Is Raising the Stakes in Cybersecurity (Boston Consulting Group, 18 December 2025) <https://tinyurl.com/3ajsurk8>.
2. AI Proclamation (Draft, 2o25).
3. Blessing Guembe et al. (2022) 'The Emerging Threat of AI-driven Cyber Attacks: A Review', 36 Applied Artificial Intelligence, 1.
4. British engineering giant Arup revealed as $25 million deepfake scam victim (CNN, 17 May 2024) <https://tinyurl.com/ye7kx84v>.
5. Computer Crime Proclamation No 958/2016, Federal Negarit Gazeta.
6. FCC Fines Lingo Telecom $1 Million Over Sloppy Biden AI Deepfake That Targeted New Hampshire Voters (TechDirt, 23 August 2024) <https://tinyurl.com/y2j6r52a>.
7. Fragmented Cybersecurity Approach Threatens Ethiopia's Digital Payment System (The Reporter, 13 December 2025) <https://www.thereporterethiopia.com/48148/>.
8. Government Cybersecurity Strategy of the United Kingdom: 2022-2030 (2022).
9. INSA Director General Highlights Key Achievements in National Cybersecurity (INSA, 19 August 2019) <https://tinyurl.com/3fhuwkrh>.
10. Katina Michael et al. (2023) 'AI in Cybersecurity: The Paradox', 4 IEEE Transactions on Technology and Society, 104.
11. Kinfe Yilma (2024) 'Developments in Cybercrime Law and Practice in Ethiopia', 30 Computer Law and Security Review, 720.
12. Kinfe Yilma (2025) 'Ethics of AI in Ethics: The Role of Ubuntu and AI Governance Initiatives', 27 Ethics and Information Technology, 1.
13. Kinfe Yilma, AI Fever No Substitute for Sound Governance, Fortune, Vol. 16, No 1347, (22 February 2026) <https://addisfortune.news/ai-fever-no-substitute-for-sound-governance>.
14. Maanak Gupta et al. (2023) 'From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and Privacy', 11 IEEE Access, 80218.
15. Masike Malatji and Alaa Tolah (2025) Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI, 5 AI and Ethics, 883.
16. Miles Brundage et al, The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation, ox.ac.uk Future of Humanity Institute, University of Oxford and others (2018).
17. National Cyber Security Framework Development Methodology (INSA, 2022).
18. National Cybersecurity Policy Implementation Roadmap (Draft, 2025).
19. Selcuk Okdem and Sema Okdem (2024) 'Artificial Intelligence in Cybersecurity: A Review and a Case Study', 14 Applied Sciences 1.
20. Suguna Balusamy et al. (2025) 'Cybercrime Investigations in the Era of Artificial Intelligence: Automated Evidence Collection and Analysis through the Use of Machine Learning', 2025 Global Conference in Emerging Technology (GINOTECH), PUNE, India, 1-16.
21. The National Artificial Intelligence Policy of Ethiopia (Draft, 2020).
22. The National Artificial Intelligence Policy of Ethiopia (June 2024).
23. The National Cybersecurity Policy of Ethiopia (June 2024).
24. The National Cybersecurity Roadmap of Ethiopia (Draft, 2025).
25. The National Information Security Policy of Ethiopia (September 2011).

The views expressed and any potential errors or omissions in this policy brief are solely the responsibility of the author and do not necessarily reflect the official policy or position of Konrad-Adenauer-Stiftung (KAS) Office Ethiopia/African Union. KAS Office Ethiopia/African Union does not endorse or guarantee the accuracy, completeness, or applicability of the information and analysis presented.

KAS Office Ethiopia/African Union

Konrad Adenauer Stiftung e.V.
Yeka Sub-City, #165
Diaspora Street

Tel: +251-115-577-644
E-Mail: info.ethiopia@kas.de
P.O.Box 110337
Addis Ababa, Ethiopia

https://www.kas.de/en/web/aethiopien/

UNIVERSITY OF LEEDS
School of Law

KONRAD ADENAUER STIFTUNG