KICTANet
The Power of Communities

MEMORANDUM ON:

Draft Kenya Cybersecurity Strategy 2025-2029

Submitted to:
The National Computer and Cybercrime Coordination Committee

Submitted By:

Kenya ICT Action Network (KICTANet)

25 April 2025

25th April 2025

The National Computer and Cybercrime Coordination Committee
Herufi House 2nd Floor Lt. Tumbo Lane
P.O. Box:30091 – 00100,
Nairobi
Tel: +254 716 148 341

Submitted via email to strategy@nc4.go.ke

Dear Sir/Madam,

Re: Memorandum on the Draft Kenya Cybersecurity Strategy 2025-2029

Greetings from KICTANet!

KICTANet is a non-profit multi stakeholder think tank for ICT policy and regulation based in Kenya whose guiding philosophy encourages synergies for ICT policy-related activities and initiatives. Our mission is to promote an enabling digital ecosystem that is open, inclusive, secure, and rights-based through multi-stakeholder approaches.

We submit this memorandum with expertise on human rights and Information and Communication Technology (ICTs) and in response to the call for input on Draft Kenya Cybersecurity Strategy 2025-2029. We have included herein a matrix presentation that captures the key issues and concerns, and highlights our proposals on relevant sections of the strategic plan for your review and consideration.

We are available to provide further input and perspectives on the strategic plan, as and when required.

We look forward to your response.

Regards,
Dr. Grace Githaiga,
CEO, Kenya ICT Action Network (KICTANet

Section/ Sub-section/	Issue/Concern	Proposal/Recommendation
3.1 Cybersecurity Policies, Laws, Regulations and Standards	**a) Focus on criminalisation:** Kenya's legislative framework is heavily tilted toward criminalisation (e.g., the Computer Misuse and Cybercrimes Act, 2018) without enough focus on prevention, resilience, and rights-protective measures. Additionally, digital transformation efforts in ministries, departments and agencies (MDAs) at national and county government levels lead to varied and sometimes inconsistent procurement practices that expose vulnerabilities. **b) Lack of international and regional alignment:** Kenya's legal framework is not aligned with regional and global cybersecurity standards. These include the EAC Cyberlaws Framework, AU Convention on Cybersecurity and Personal Data Protection, AU Data Governance Framework, the Budapest Convention, and the proposed Draft Cybercrime Convention. c) **Risk of Complexity for SMEs** Depending on the approach, guidelines risk being too generic for large enterprises and too complex for SMEs. It is also unclear as to whether compliance will be voluntary, mandatory, or linked to industry standards. Also, if the guidelines introduce strict, one-size-fits-all regulations, SMEs and startups may struggle with high compliance costs, stifling innovation and growth. Further, there is no clear plan for industry collaboration or how SMEs and individuals, who often lack technical expertise,	a) Shift focus of the CMCA from criminalisation and focus on a balanced approach that also strengthens aspects such as cybercrime prevention, cybersecurity resilience, capacity building, risk management alongside criminalisation. b) Harmonize Kenya's cybersecurity laws and strategy with international frameworks, including the UN Cybercrime Convention, Budapest Convention and the AU Convention on Cyber Security and Personal Data Protection. c) Develop flexible, sector-based, risk-based guidelines, ensuring large enterprises follow compliance frameworks, while SMEs get practical, low-cost cybersecurity measures. d) Encourage self-regulation with industry-led best practices. e) Introduce incentives (e.g., tax breaks, grants) for SMEs to adopt cybersecurity best practices instead of imposing strict mandates. f) Develop procurement guidelines that mandate transparent, digital tender processes to ensure that ICT acquisitions at national and county

Section/ Sub-section/	Issue/Concern	Proposal/Recommendation
	will be supported in implementing these guidelines.	government level meet rigorous cybersecurity standards.
3.2 Cybersecurity Governance	**Cybersecurity Governance and Institutional Coordination** Kenya's current institutional landscape is fragmented. There are multiple institutions handling cybersecurity, including the National KE-CIRT/CC (Kenya Computer Incident Response Team), National Cybersecurity Coordination Committee (NC4), the ICT Authority, the Communications Authority (CA), the National Security Advisory Committee (NSAC), the Ministry of Information and Digital Economy, the Ministry of Interior, and the Ministry of Defence. Also, the predominant focus on criminalisation limits proactive resilience and effectiveness of institutions in promoting cybersecurity. This fragmentation hinders effective coordination and establishing a new National Cybersecurity Agency without clarifying its role and relationships with existing entities may increase fragmentation and amplify the duplication of mandates, inefficiencies, and bureaucratic bottlenecks.	a) Strengthen the existing cybersecurity coordination framework by improving inter-agency collaboration, multi stakeholder participation and the clarification of roles, responsibilities and mandates. b) Shift focus from criminalisation and focus on strengthening aspects such as cybercrime prevention, cybersecurity resilience, capacity building, and risk management. c) Develop inter-agency MoUs, a centralized threat intelligence platform, and entrench regular multi stakeholder engagement to inform decision-making.
3.3 Critical Information Infrastructure Protection (CIIP)	a) **CII Protection:** With increasing digitalization, CIIs—including telecommunications, mobile money, and government service portals (e.g., eCitizen)—are growing targets. Current CIIP measures lack robust sector-specific risk assessments, continuous monitoring, and standards that address the	a) Mandate regular, sector-specific vulnerability assessments and establish baseline cybersecurity standards for all CIIs. b) Integrate continuous monitoring and rapid incident detection technologies, along with

Section/ Sub-section/	**Issue/Concern**	**Proposal/Recommendation**
	procurement risks inherent in decentralized digital services at both national and county levels. b) A centralized national asset inventory could become a high-value target for cyberattacks if not properly secured. It is unclear how the inventory will be protected from unauthorized access or misuse.	automated patch management systems. c) Develop coordinated procurement standards to mitigate risks associated with acquiring ICT goods and services across all government levels. d) Implement robust security measures, including encryption, multi-layer access controls, and regular security audits to protect the inventory.
3.4 Cyber Incident Response and Management	a) **Fragmentation of Incident Reporting:** The current incident response mechanisms are fragmented across various agencies and not well coordinated at national and county government level, and across the diverse sectors. The effective coordination of threat intelligence and incident reporting could further be undermined by disjointed systems, limited collaboration and information sharing. b) Kenya already has the National KE-CIRT/CC (Kenya Computer Incident Response Team – Coordination Centre) under the Communications Authority (CA). Creating new response teams may cause confusion, redundancy, and bureaucratic delays. c) The strategy does not specify who will manage the centralized system, how it will integrate existing frameworks, or how it will handle sensitive information from different sectors.	a) Review, strengthen & streamline existing cybersecurity structures and institutions under a robust governance and coordination framework instead of creating parallel institutions. Define clear mandates to prevent redundancies and overlaps, ensure institutional independence by establishing a clear governance structure that prevents political interference in cybersecurity. b) Establish an integrated /centralised coordination framework or incident reporting platform to facilitate seamless reporting and information-sharing between KE-CIRT/CC, NC4, regulators (CA), ICTA, sector-specific CSIRTs, and law enforcement, ensuring real-time data sharing while maintaining confidentiality. c) Strengthen international cooperation for

Section/ Sub-section/	Issue/Concern	Proposal/Recommendation
	d) Kenya already has established think tanks like KICTANet actively engaging in cybersecurity policy advocacy, stakeholder engagement, and impact assessments. Creating a new institute without leveraging existing expertise risks redundancy and unnecessary resource allocation. The strategy does not define whether this think tank will be government-led, independent, or multi-stakeholder-driven, nor does it outline how it will be funded and sustained in the long term. The proposed agency could have a research department to perform these tasks.	real-time threat intelligence sharing, aligning with regional and global initiatives. d) Mandate regular simulation exercises and coordinated drills at both national and county levels. e) Provide capacity-building support for already existing sector-specific CSIRTs to enhance technical expertise and incident response capabilities. f) Develop National Cybersecurity Incident Reporting guidelines to define clear incident escalation procedures, reporting structures, and the roles of various institutions to avoid overlap. g) Leverage existing think tanks (e.g., KICTANet) instead of creating a new entity to avoid duplication and ensure continuity of cybersecurity policy research and advocacy. h) Adopt a multi-stakeholder model where government agencies, academia, industry, and civil society collaborate to enhance cybersecurity policy discourse and impact assessments.
3.5 Cybersecurity Capability and Capacity Building	There is a significant cybersecurity skills gap and low public cyber hygiene awareness. Despite expanding digital services (e.g., e-commerce, mobile payments), many users and	Investing in cybersecurity capacity building at all levels is critical for reducing cyber risks and promoting resilience

Section/ Sub-section/	Issue/Concern	Proposal/Recommendation
	organizations lack the training to detect and respond to cyber threats, leading to a high incidence of fraud and social engineering attacks.	and trust. Skills and awareness are not only essential for improving incident response, but also promote proactive cybersecurity culture and maturity especially as the digital economy expands. a) Launch nationwide capacity building and awareness programmes. b) Roll out accredited training programs for cybersecurity professionals across national and county government and critical sectors and industries. c) Partner with academic institutions to integrate cybersecurity into educational curricula from primary to tertiary level. d) Initiate extensive public awareness campaigns on cybersecurity best practices, tailored to diverse audiences, including vulnerable groups. Lessons can be learnt from KICTANet's cyber hygiene awareness programmes that have leveraged a robust curriculum developed in partnership with ICTA and leveraged social media and specific

Section/ Sub-section/	Issue/Concern	Proposal/Recommendation
		training to raise awareness.
3.6 New and Emerging Technologies	Emerging technologies are rapidly reshaping the cybersecurity landscape, offering both powerful defensive tools and novel threat vectors. Key trends include the maturation of AI and machine learning for threat detection, the advent of agentic and generative AI that can automate attacks, the expansion of IoT and edge computing which increases the attack surface, the rollout of 5G/6G networking enabling new services and risks, breakthroughs in quantum computing that threaten current cryptography, advances in blockchain and distributed ledger for secure transactions, and the rise of extended reality (AR/VR) systems with unique security challenges.	a) Link initiatives with Kenya's National Artificial Intelligence Strategy and Cloud Policy, including strengthening AI cybersecurity ethics to guide AI use in cybersecurity. b) Develop certification standards for IoT hardware. c) Develop policies and guidelines on the procurement, use and deployment of new and emerging technologies in the public sector.
3.7 Cyber Risks and Cybercrimes Management	a) Online cybercrime reporting portals already exist (such as the one under NC4 portal); but the challenge is that there is no unified system where reports are centralized, tracked, and escalated efficiently. Citizens and businesses often don't receive feedback on reported cases, leading to low public trust in these platforms. b) Many citizens and SMEs are also unaware of where or how to report cybercrimes, and existing platforms may not be user-friendly or widely accessible (e.g., mobile apps, USSD for non-internet users).	a) Enhance the effectiveness of existing platforms rather than creating new ones. This includes integrating KE-CIRT/CC, NC4, DCI, and sectoral CSIRTs into a unified reporting system that allows seamless sharing of reports. b) Expand reporting channels to include mobile apps, USSD codes, and AI-driven chatbots to ensure accessibility across diverse demographics.

Section/ Sub-section/	Issue/Concern	Proposal/Recommendation
3.8 Public Private Partnership	The section on PPP is disjointed and is not linked to the section 4.2 on multi stakeholder engagement.	Integrate section on PPP with the section on multi stakeholder engagement.
3.9 International Cooperation and Collaboration	Kenya's cybersecurity work is influenced by various global and regional frameworks, such as the AU Convention, AU Data Governance Framework, AU Continental Free Trade Agreement (AfCFTA), and the UN Cybercrime Convention. However, these international aspects are not adequately integrated into the national strategy.	a) Align national cybersecurity policies with the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention) and the AU Data Governance Framework to promote consistency across the continent. b) Leverage the AU Continental Free Trade Agreement (AfCFTA) to create a framework for digital trade that includes cybersecurity standards. c) Ensure compliance with the regional and international standards to facilitate international cooperation and mutual legal assistance. d) Promote bilateral and multilateral dialogues to update and harmonize norms and practices, thereby reducing the sole focus on criminalisation and shifting toward a more balanced, comprehensive approach.
4. Engagement with Stakeholders for Sustainability	**a) Gaps in Stakeholder Engagement Approaches:** Kenya's cybersecurity efforts have been top–down, government-leaning with a heavy focus on criminalisation. This approach limits the involvement of the private sector, academia, and civil society, which are critical for developing	A multistakeholder approach leverages diverse expertise from academia, civil society, government, media, private sector, and the technical community which is critical to enhance transparency, and to foster innovation. Kenya should ensure inclusive approaches to policy- and

Section/ Sub-section/	Issue/Concern	Proposal/Recommendation
	innovative, resilient solutions and ensuring broader public trust. b) While the strategy outlines various forms of stakeholder engagement (e.g., forums, surveys, hearings), it lacks a clear institutional structure and accountability mechanism to ensure that engagement is continuous, inclusive, and meaningfully integrated into cybersecurity policymaking. Without such structures, these efforts risk becoming fragmented, inconsistent, or symbolic.	decision-making. A multistakeholder approach promotes a culture of collective responsibility, ensuring that cybersecurity is viewed as a shared public good. a) Embed multi stakeholders (academia, civil society, government, media, private sector, and the technical community) within the national cybersecurity governance structures, with clear mandates, rotating representation, and ensure engagement in policy development, monitoring and implementation of the national strategy. b) Create incentives (such as tax breaks, grants, or recognition awards) for the private sector, civil society, and academic institutions that contribute to national cybersecurity objectives and initiatives. c) Ensure that the regular multi stakeholder consultations provided for, are embedded in practices of the existing institutions, as opposed to them not being integrated across the various sections of the strategy.