Joint Submission for Call for Public Comments to Draft Kenya Cybersecurity Strategy, 2025 - 2029
Comments By:
Organisation 1: Pollicy (www.pollicy.org)
Organisation 2: Article 19 Eastern Africa (https://www.article19.org/regional-office/eastern-africa/)
Organisation 3: Association for Progressive Communications (APC) (https://www.apc.org/en)
Organisation 4: International Press Institute (https://ipi.media/)

Joint Submission for Call for Public Comments to Draft Kenya Cybersecurity Strategy, 2025 - 2029

Overview

A cybersecurity strategy presents powerful opportunities to enhance national cybersecurity capabilities. As technologies and data become more accessible, actors are increasingly harnessing them to execute complex, adaptive cyberattacks, with artificial intelligence introducing threats that challenge conventional cybersecurity approaches. Proactively, the Kenyan government, in its strategic pillars to advance the digitisation of government services for better public service delivery, has ensured that preventative measures and evolving tactics are minimised. Safeguarding the integrity, reliability, and accountability of civic technologies and digital public infrastructures is therefore essential to ensure trust in their deployment across critical sectors.

Notably, three key priority areas emerge in the draft strategy: **the need for proactive data and AI governance within cybersecurity, strengthened constitutional oversight over weaponised digital surveillance** and **enforcement tools, and the integration of gender- responsive, intersectional approaches into cybersecurity frameworks**. Recognising that cybersecurity is no longer a purely technical issue, the strategy embeds a rights-based perspective, aligning with global best practices that call for inclusive, equitable digital safety policies. AI's dual impact—amplifying financial crimes and intensifying threats, such as the distribution of non-consensual intimate imagery (NCII) through synthetic media—demands deliberate safeguards rooted in both technological excellence and social accountability. Importantly, the cyber environment is understood not only as a technical ecosystem but as an interconnected socio-technical space where Kenyan culture, privacy, dignity, economic security, and constitutional freedoms are at stake. We note that that the strategy aims to reinforce a common standard for cyber risk management across all sectors, while ensuring that oversight mechanisms empower citizens and civil society to hold cyber governance structures accountable in a rapidly digitising Kenya.

1. **Detailed Comments and Key Recommendations**

Section	Comments	Recommendation	Justification (include reference to relevant national, regional and international frameworks and best practices)
SECTION 1: Introduction and Background			
1.1 Background	We encourage the government to consider the nuances of the false news taxonomy when identifying potential threat factors to critical information infrastructure. Misinformation is the unintentional sharing of false information with no intention to cause harm. Disinformation is the intentional dissemination of false or misleading information to cause harm. Both mis and disinformation can pose a threat to critical information infrastructure, and	Expressly identify disinformation as a cyber threat priority and the need to adopt a human rights-based approach to addressing it.	The Paris Call for Trust and Security in Cyberspace urges 'states, the private sector, and organisations in civil society to work together to promote peace and security in cyberspace, fight disinformation and address new threats that put citizens and infrastructure in danger.' The Freedom Online Coalition (FOC), of which Kenya is a member, adopted in 2016 a statement on a human rights-based approach to cybersecurity, which affirms that human rights and cybersecurity are complementary, interdependent and mutually reinforcing and that cybersecurity policies and practices should be rights-respecting by design. See more:

	rights-respecting approaches to combating mis and disinformation can help mitigate cybersecurity risks and combat cybercrimes.		FOC statement of support for the cybersecurity and human rights recommendations https://freeandsecure.online/resources/foc-statement-support-cybersecurity-human-rights-recommendations/ "APC policy explainer: A human rights-based approach to cybersecurity APC", November 2020 https://www.apc.org/en/pubs/apc-policy-explainer-human-rights-based-approach-cybersecurity
SECTION 2: Strategic Foundations			
Section	**Comments**	**Recommendation**	**Justification (include reference to relevant national, regional and international frameworks and best practices)**
2.1. Guiding Principles	We welcome the inclusion of "Upholding Constitutional Rights" and the need to safeguard the rights to privacy, freedom of expression, and access to information as guaranteed under the Constitution as guiding principles. However, the draft strategy contains few references to rights (and some of them appear only in the messages at the beginning of the document and in the executive summary).	We recommend strengthening the language and including references to the need for a human rights-based approach to cybersecurity in the guiding principles. Such an approach means putting people at the centre and ensuring that there is trust and security in networks and devices that reinforce, rather than threaten, human security. Such an approach is systematic, meaning that it addresses the technological, social and legal aspects together, and does not differentiate between national security	The eleven UN norms for responsible state behaviour in cyberspace, agreed by the UN Group of Governmental Experts (GGE), welcomed by the UN General Assembly in 2015, and further developed in the subsequent multilateral processes on state use of ICTs, set out an international consensus on appropriate state behaviour in cyberspace. In particular, *Norm e* reminds States to respect and protect human rights and fundamental freedoms, both online and offline, in accordance with their respective obligations and UN resolutions. See more: United Nations, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (New York: United Nations, 2015), https://documents.un.org/doc/undoc/gen/n15/457/57/pdf/n1545757.pdf

		interests and the security of the global internet. A human rights-based and human-centric approach to cybersecurity should not be limited to high-level principles; the cybersecurity strategy should also set out concrete actions, indicators, and budget allocations aligned with this approach.	The Freedom Online Coalition (FOC), of which Kenya is a member, adopted in 2016 a statement on a human rights based approach to cybersecurity, which affirms that human rights and cybersecurity are complementary, interdependent and mutually reinforcing and that cybersecurity policies and practices should be rights respecting by design. See more: FOC statement of support for the cybersecurity and human rights recommendations https://freeandsecure.online/resources/foc-statement-support-cybersecurity-human-rights-recommendations/ "APC policy explainer: A human rights-based approach to cybersecurity APC", November 2020 https://www.apc.org/en/pubs/apc-policy-explainer-human-rights-based-approach-cybersecurity
2.1. Guiding Principles	We also encourage the strategy to include gender equality in its Guiding Principles. A gender approach to cybersecurity directly builds upon a human rights and human-centric approach to cybersecurity. Effective cybersecurity, gender equality, and human rights are mutually reinforcing.	Gender mainstream the national cybersecurity strategy and its action plan, including concrete and measurable goals and indicators. Key recommendations towards this objective could include: To understand national cybersecurity risks and threats from a gender perspective (collect evidence, case	Gender equality is enshrined in the Charter of the United Nations, the Universal Declaration of Human Rights, and affirmed in the Convention on the Elimination of all Forms of Discrimination Against Women (CEDAW 1979); the Beijing Declaration and Platform for Action (1995); the Women, Peace, and Security Agenda (2000); the 2030 Sustainable Development Goals; and regional instruments such the Constitutive Act of the African Union and Protocol to the African Charter on Human and People's Rights on the Rights of Women in Africa (2003). Both the UN Group of Governmental Experts (GGE) and the first UN Open-Ended Working Group (OEWG) in security of and in the use of information and communications technologies 2019-2021 in its Final

	A gender approach seeks to amend gender-unaware projects, measures, or policies that do not recognize gender and exclusion issues and therefore risk contributing to gender inequalities. It is a perspective that addresses the differentiated risks and impacts of cyber threats to make cybersecurity responsive to complex and differentiated needs, priorities, and perceptions based on gender and other factors.	studies, reports, and draw on the expertise of organizations already working on this) To analyse legal frameworks and policies that can respond to the gender needs and challenges, even if only partially. To map the government's knowledge and engagement with international debates on gender and cybersecurity or related subjects, such as internet governance, and cybercrime. To conduct a national risk assessment to collect information and evidence on the gender and intersectional risks faced by people in the context of cybersecurity. *See more at:* *A framework for developing gender-responsive cybersecurity policy: An assessment tool*, APC. https://www.apc.org/en/pubs/framework-developing-gender-responsive-cybersecurity-policy#norms	Substantive Report, emphasised the importance of gender balance and the need to promote effective and meaningful participation and leadership of women in decision-making processes related to the use of ICTs in the context of international security. The first OEWG 2019-2021 final report also noted the prominence of gender perspectives in its discussions and underscored the importance of narrowing the "gender digital divide". The final report of the Group also acknowledged that cyber threats may also have a different impact on different groups and entities, including women. It stated that capacity-building should respect human rights, be gender sensitive and inclusive, universal and non-discriminatory. The second OEWG (2021-2025) continues to draw attention to the need for a gender perspective in addressing threats, stressed the need to promote gender-responsive capacity-building efforts, including through the integration of a gender perspective into national ICT and capacity-building policies as well as the development of checklists or questionnaires to identify needs and gaps in this area. Several UN resolutions pertain directly to human rights, gender equality, and ICTs. For example, HRC resolutions 32/13 (2016) and 38/7 (2018) condemn tech-facilitated gender-based violence, reiterate the importance of digital privacy, and call on states to close the gender digital divide. The 2018 HRC resolution (38/5) on "Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts" likewise reiterates state responsibilities to address TFGBV and calls for the integration of a gender perspective into all digital policy and implementation. HRC resolutions 47/23 (2021) and 53/29 (2023) recognise the importance of new and emerging technologies to gender equality as well as their potential to contribute to gender discrimination and sexual and gender-based violence. The 2021 iteration of the HRC resolution on human rights on the internet (A/HRC/47/L.22) specifically recognizes that digital divides undermine women's full enjoyment of their human rights. The 2018 UN General Assembly (UNGA) resolution on privacy in the digital age (73/179) calls on states to develop and strengthen

			gender-responsive policies to protect the right to privacy. The 2023 UNGA resolution (78/213) on the protection and promotion of human rights in the context of digital technologies calls on states to close the gender digital divide; mainstream a disability, gender, and racial perspective into digital policy; stresses the importance of women and girls' access to technology; and recognises the importance of combating technology-related sexual and gender-based violence. Outcome documents of the World Summit on the Information Society (WSIS) in 2003 and 2005 recognised the gender gap in decision making processes and the need for the international community to pay special attention to marginalised and vulnerable groups' unique needs in society. The International Telecommunication Union (ITU) Resolution 70 on "Mainstreaming a gender perspective in ITU and promotion of gender equality" calls, among other issues, for the empowerment of women through telecommunications/information and communication technologies. *References:* *APC policy explainer: What is a gender approach to cybersecurity?*, APC, 2023. https://www.apc.org/en/pubs/apc-policy-explainer-what-gender-approach-cybersecurity *A framework for developing gender-responsive cybersecurity policy: Norms, standards and guidelines.* APC https://www.apc.org/sites/default/files/gender-cybersecurity-policy-norms.pdf *Forthcoming report on guidelines for gendered implementation of the 11 Un cybernorms for responsible state behaviour*
2.2 Guiding Principles	We encourage the establishment of a clear use of data to harness information integrity through 1. Power mapping and establishing the role of the	To establish access to data frameworks through Resolution On Promoting And Harnessing Data Access As A Tool For Advancing Human Rights And	Access to data is *References:* *Digitising Kenya: An assessment of the citizen centricity of Kenya's digital governance." Report, focusing on citizen-centric digital*

	government in standardising access to data through a data sharing framework that promotes openness, security and privacy respecting in all contexts	Sustainable Development In The Digital Age. Achpr/Res.620 (Lxxxi) 2024 https://www.stephensonharwood.com/insights/the-eu-data-act-rights-of-access-to-data#:~:text=What%20are%20the%20access%20rights,to%20users%20(Article%203).	*governance, addressing the digital divide, and exploring pathways to more inclusive policies.* Pollicy, 2025 https://pollicy.org/resource/digitising-kenya/ *Data deficits and democratic processes: The under-explored role of data in African elections,* Research ICT Africa 2025 *https://researchictafrica.net/research/data-deficits-and-democratic-processes-the-under-explored-role-of-data-in-african-elections/*
SECTION 3: Areas of Strategic Focus			
Section	**Comments**	**Recommendation**	**Justification (include reference to relevant national, regional and international frameworks and best practices)**
3.1 Cybersecurity Policies, Laws, Regulations and Standards	Rather than balancing rights against security, cybersecurity-related policies must provide security in a way that reinforces human rights.	In the context of the cybersecurity strategy, Kenya could: Amend regulatory provisions, including in the Official Secrets Act, Preservation of Public Security Act, Data Protection Act, Prevention of Terrorism Act, and the National Intelligence Service Act, which permit state surveillance of online content without adequate safeguards. Guarantee adequate and independent oversight mechanisms which operate on principles of transparency and accountability, provide redress mechanisms to victims, and control state surveillance practices to ensure they are limited and proportional in	See more at: *Universal Periodic Review 49th Session – Joint stakeholder report: Human rights in the digital context in Kenya,* Association for Progressive Communications (APC) and Kenya ICT Action Network (KICTANet) https://www.apc.org/en/pubs/universal-periodic-review-49th-session-joint-stakeholder-report-human-rights-digital-context

		accordance with International human rights standards. Advancing legal and policy frameworks that give legal protection against gender-based cyber threats for women, including journalists and human rights defenders	
Section 3:1 Cybersecurity Policies, Laws, Regulations and Standards. (a) Amend the CMCA, 2018 to establish National Cybersecurity Agency and the National Cybersecurity Academy.	The proposal to amend the CMCA, 2018 is narrowly aimed at establishing the National Cybersecurity Agency and the National Cybersecurity Academy. However, inherent human rights concerns with the law and the threats to freedom of expression persist. Sections 22 and 23, in particular, are vaguely worded given the failure to define key terms such as 'false, misleading or fictitious' as well as setting broad standards open to subjective interpretation, including 'results in panic, chaos'. The sections offend the legality principle of limitations on human rights. Sections 22 and 23 also disproportionately criminalise expression, including defamation contrary to Kenya's international human rights obligations and case law.	Amend the CMCA to align with international laws and standards on free expression and remove criminal sanctions on expression.	The proposed amendment will reflect a more human rights-based approach to disinformation as a cybersecurity threat factor. Section 3.4.2. of the strategy on developing cyber capacity towards increased cybersecurity expertise, education, research and awareness across the nation can serve to confront disinformation in a more rights-respecting and less punitive manner. The Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda, provides that, 'General prohibitions on the dissemination of information based on vague and ambiguous ideas, including "false news" or "non-objective information", are incompatible with international standards for restrictions on freedom of expression, as set out in paragraph 1(a), and should be abolished.' It further states that criminal defamation laws are unduly restrictive and should be abolished. Principle 22 of the 2019 Declaration of Principles on Freedom of Expression and Access to Information in Africa calls on States to repeal laws that criminalise sedition, insult and publication of false news, and amend criminal laws on defamation and libel with necessary and proportionate civil sanctions. General Comment 34 of the International Covenant on Civil and Political Rights provides that criminal law should be a last resort for the most serious cases, and imprisonment sanctions are inappropriate.

3.1 Section 3:1 Cybersecurity Policies, Laws, Regulations and Standards. d. Ratify and adopt regional, international cybersecurity conventions, treaties, laws and norms.	We welcome interventions that aim to align national laws with international frameworks, reinforce legal protections in cyberspace, enhance accountability and promote international cooperation. We urge the government to include a non-exhaustive list of regional and international instruments that will shape the country's responses to cybersecurity and protect citizens. The State should pay due consideration to shortcomings in international cybersecurity instruments, such as the United Nations Convention against Cybercrime, that may compromise the achievement of these goals.	Provide a non-exhaustive list of regional and international instruments that the State aims to ratify or adopt. Refrain from signing or ratifying the UN Convention against Cybercrime, or entering reservations on contentious clauses.	The proposed examples will provide a more specific indication of the government's normative priorities at the regional and international levels. Additionally, the ratification and adoption of regional and international instruments should be followed by a critical examination of their normative strengths and weaknesses, aimed at enhancing the protection of citizens' rights and cyberspace. See the joint statement by over 100 international human rights organisations on the weaknesses of the United Nations Convention against Cybercrime, including overbroad formulation, weak data protection and human rights safeguards, and inadequate gender mainstreaming measures. Also see, Urgent Appeal to Address Critical Flaws in the Latest Draft of the UN Cybercrime Convention https://ipi.media/wp-content/uploads/2024/07/Cybercrime-Open-Letter-to-EU-and-MS.pdf
3.3 Critical Information Infrastructure Protection (CIIP)	The cybersecurity strategy and its action plan for building "cyber resilience" can be broad according to national needs, but the government can consider expanding the definition of "critical infrastructure" to include services and supports that are particularly vital to the lives and wellbeing of women, girls, people of diverse gender identities, expressions, and sexualities, and/or people belonging to marginalised and/or minority groups.	Among the measures that could be contemplated are: The commitment that the government's critical infrastructure risk models incorporate a gender and intersectional approach to protecting the rights of people given their diverse needs. For this, the government can organise regular consultation with	See more at: *A framework for developing gender-responsive cybersecurity policy: An assessment tool*, APC.

		multistakeholder partners to expand the definition of critical infrastructure. The government can consider coordinating training sessions with stakeholders on how the gender approach can contribute to developing these models and creating a plan for timely responses to incidents.	
3.4 Cyber Incident Response and Management	Cyber incidents must have responses that conform to the principles of legality and proportionality. The definitions of security and threats could be aligned with gender-responsive, human-centric, and intersectional approaches to cybersecurity.	To advance progress in this area, among other measures, it is possible to propose the following: In consultation with civil society, the government could aim for gender parity, and the increased participation of people of diverse gender identities, expressions and sexualities, as well as other marginalised groups in cyber incident response. The government and multistakeholder community could collect and produce intersectional, gender-disaggregated data on cyber incidents. Special contingency plans that, based on a gender and intersectionality analysis, seek to protect people most vulnerable to specific types of cyber attacks. Ensure regular training and inclusive	See more at: *A framework for developing gender-responsive cybersecurity policy: An assessment tool*, APC.

		participation in gender-responsive emergency planning. Provide resources to support the infrastructure of groups that have experienced gendered and human rights impacts of cyber attacks due to their work.	
3.5 Cybersecurity Capability and Capacity Building		Promote inclusive and gender-responsive cybersecurity capacity-building by aligning efforts with the Sustainable Development Goals and the Global Digital Compact (GDC) commitments. This includes addressing systemic barriers to digital inclusion, supporting the participation of women and girls in STEM and cyber careers, and ensuring safe and affordable connectivity. Sustain and fund initiatives that empower women, LGBTQI+ people, and marginalised communities to actively engage in cybersecurity governance.	The UN OEWG stated that cyber capacity-building should respect human rights and fundamental freedoms and be universal, non-discriminatory, gender-sensitive, and inclusive. United Nations Office for Digital and Emerging Technologies, “Global Digital Compact”, 2024, https://www.un.org/techenvoy/global-digital-compact
3.6 New and Emerging Technologies		The strategy must consider the potential, unintended, and gender-differentiated effects of emerging technologies, including	

		generative AI, as well as hidden or malicious technical features in licit products. Additionally, it should conduct a gender audit of widely used existing cybersecurity products and practices.	
SECTION 4: Sustainability Considerations			
Section	**Comments**	**Recommendation**	**Justification (include reference to relevant national, regional and international frameworks and best practices)**
4.2 Engagement with Stakeholders for Sustainability	Welcome language on the Consulting, involving and collaborating with stakeholders.	Proposals for an inclusive process design to bring human rights and gender considerations: Meaningfully engage and consult multistakeholder partners, with a focus on civil society organisations involved in advocacy relating to women's, LGBTQI+ people, and marginalised and minority communities, to collaboratively and transparently develop cybersecurity policies and practices. To enable inclusive consultation mechanisms, design participation processes carefully, paying attention to power dynamics and ensuring equitable representation. Continuously evaluate and review the implementation of the gender approach to cybersecurity policy, with meaningful participation from civil society.	

		GPD, *Inclusive Cyber Norms Toolkit*, 2023. https://www.gp-digital.org/news/gpd-unveils-new-guide-to-fostering-inclusive-cyber-norm-processes/ A framework for developing gender-responsive cybersecurity policy: Norms, standards and guidelines. APC https://www.apc.org/sites/default/files/gender-cybersecurity-policy-norms.pdf	
4.3 Monitoring and Evaluation	Monitoring and evaluation of the policy should be underway based on compliance with the action plan. A review of the policy should clearly identify gaps in the policy text or in its implementation and provide a concrete action plan for addressing these gaps. A continuous cycle of monitoring and review should be built into the implementation plan.		
SECTION 5: Implementation Framework			
Section	**Comments**	**Recommendation**	**Justification (include reference to relevant national, regional and international frameworks and best practices)**
Implementation	The current NC4 Committee	Include a clear framework for	

Framework	constitution includes high-ranking departments without a clearly spelt-out implementation strategy among its members.	inclusivity in the implementation process.	