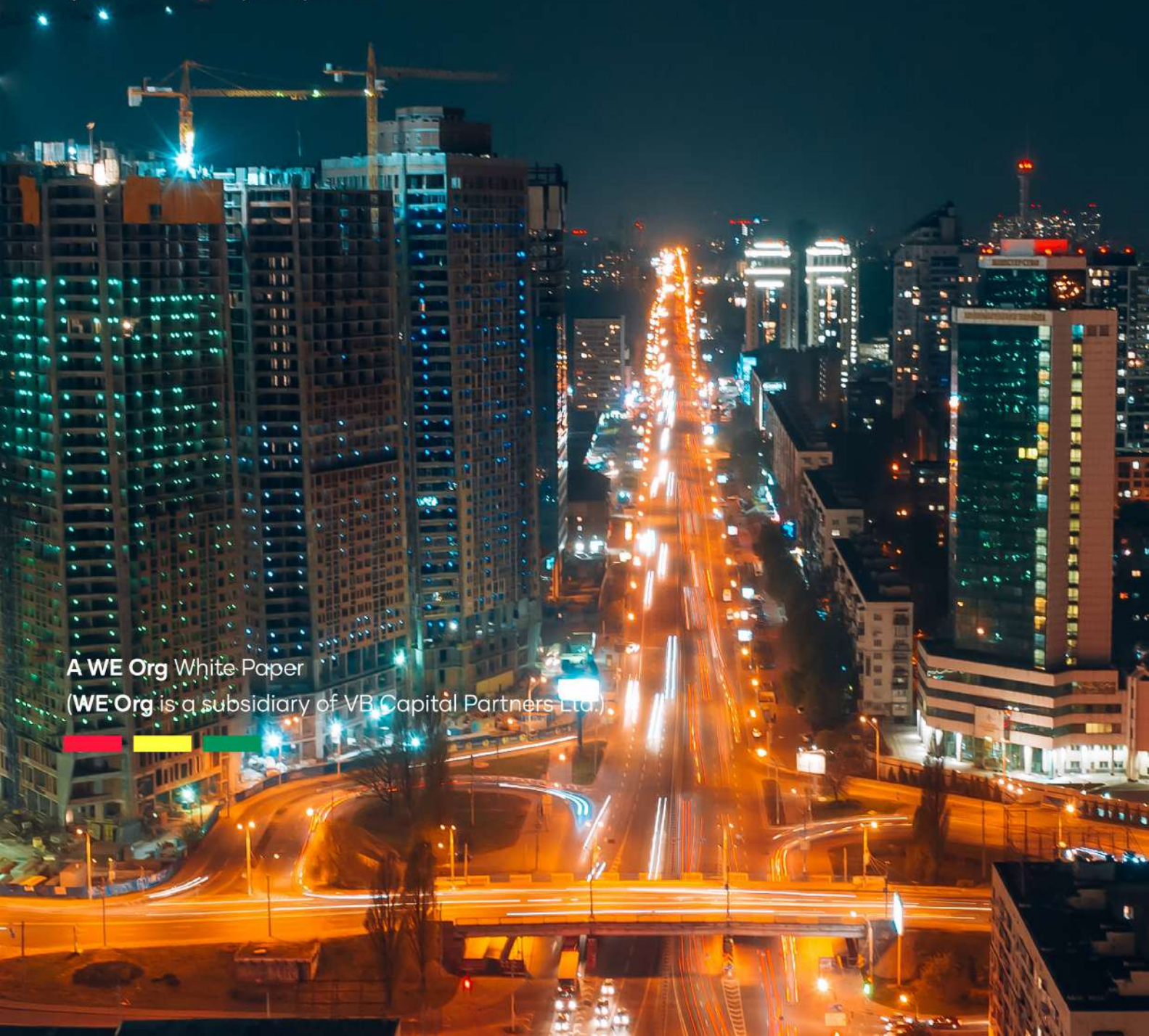
Strengthening Ghana's Cyber Resilience:

Operationalizing the Cybersecurity (Amendment) Act, 2025



A WE Org White Paper

(**WE Org** is a subsidiary of VB Capital Partners Ltd.)

Executive Summary

GHANA STANDS AT A PIVOTAL MOMENT IN ITS DIGITAL TRANSFORMATION JOURNEY.

The Cybersecurity (Amendment) Bill, 2025 reinforces the nation's leadership in Africa's cybersecurity landscape, strengthening the Cyber Security Authority (CSA) and expanding its scope to include emerging technologies such as Artificial Intelligence (AI), cloud computing, Internet of Things (IoT), blockchain, and quantum computing.

This legislative milestone builds upon the Cybersecurity Act, 2020 (Act 1038) and the National Cybersecurity Policy and Strategy (NCPS), providing a robust foundation forgovernance, protection, and accountability. Yet, as Ghana's digital economy expands, cyber threats are evolving faster than regulatory mechanisms. The challenge ahead lies not in creating more rules, but in translating policy into practical, preventive capability across public and private sectors.

This white paper explores how Ghana can leverage the 2025 Amendment to deepen national cyber resilience moving from compliance and Digitalisation (MoCD), and strategic partners to operationalize the Amendment through enhanced governance, intelligence-sharing, simulation, and innovation.

Ghana's Cybersecurity Evolution

The Cybersecurity Act, 2020 (Act 1038) created the Cyber Security Authority (CSA) and provided them legal basis for regulating critical information infrastructure (CII), licensing service providers,and protecting citizens online.

Subsequent policy milestones such as the National Cybersecurity Policy and Strategy (NCPS) and the Safer Digital Ghana initiative laid the groundwork for public awareness, coordination, and institutional strengthening.

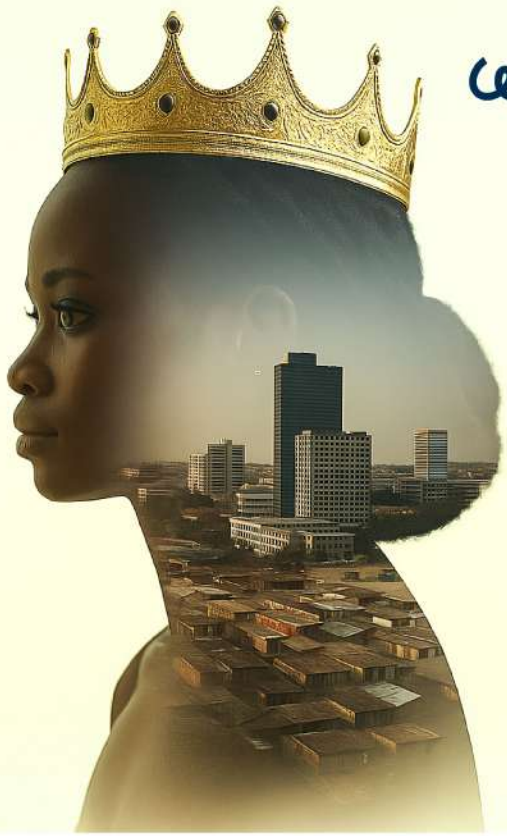
Over the past decade, Ghana has established itself as a regional model for cybersecurity governance.

The Cybersecurity (Amendment) Bill, 2025 represents the next evolution of that journey. It introduces:

- Expanded CSA authority to investigate, prosecute, and sanction cybercrime.
- Formal recognition of emerging technologies within the cybersecurity regulatory perimeter.
- Enhanced mechanisms for professional accreditation and certification.
- Provisions that strengthen digital rights and child online protection.

The Amendment signals a nation ready to secure its digital future. However, next phase of progress requires translating these legal provisions into measurable operational resilience where agencies, enterprises, and citizens alike can anticipate, mitigate, and respond to cyber risks effectively.

The New Digital Risk Landscape



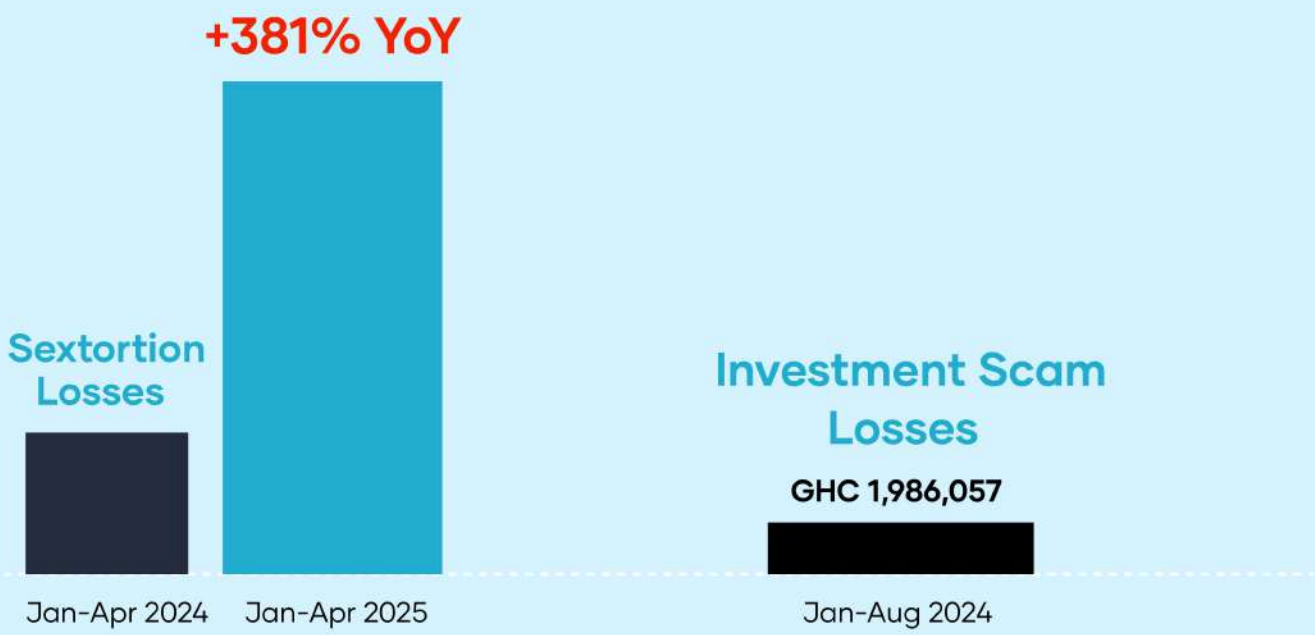
Ghana's digital economy is expanding at unprecedented speed. Financial inclusion through mobile money, digital government platforms, smart agriculture, e-commerce, and fintech innovations are transforming how citizens interact and how businesses compete.

With digital adoption comes exposure. The attack surface now extends beyond government systems to private networks, cloud environments, and connected devices. Threat actors are more organized, leveraging artificial intelligence, automation, and global collaboration.

Recent global trends, ransomware-as-a-service, data breaches targeting supply chains, and the exploitation of AI-driven systems illustrate a world where cyber incidents are no longer isolated events but systemic risks.

For Ghana, this means the national conversation must evolve from response to readiness. Prevention, detection, and resilience must become embedded features of national governance not post-incident reactions.

GHANA'S CURRENT THREAT POSTURE



What does this mean for Ghana

Ghana's cyber exposure is no longer theoretical. Current national reporting shows rapid monetization of cybercrime primarily through social engineering, online fraud, and criminal marketplaces exploiting the country's expanding digital adoption.

Key Facts

(Source: Cyber Security Authority, Ghana)

- **Jan - Apr 2024:**
  155 sextortion cases = GH₵103,663 losses (CSA)
- **Jan - Apr 2025:**
  sextortion losses escalated to GH₵499,044 (CSA). (increase = 381% YoY).
- **Jan - Aug 2024:**
  149 investment scam reports = GH₵1,986,057 losses (CSA).
- **H1 2024:**
  CSA recorded 226 sextortion cases and GH₵112,209 in losses.

Other Evidence

- Ghana Police (Oct 23, 2025) intercepte 57 people coerced into "romance scam" production in Accra (AP).
- INTERPOL continues to list phishing / online scams / BEC / ransomware as Africa's most reported threats.
- ITU Global Cybersecurity Index baseline (2020) placed Ghana 3rd in Africa (86.69%) This shows capability potential, but threat pressure has since intensified faster that policy has operationalized.

Strengths of the 2025 Amendment

The 2025 Amendment Bill introduces several enhancements that align with global best practices:

01

Empowerment of the Cyber Security Authority

The CSA's expanded authority to conduct investigations and prosecutions enhance deterrence and streamline the response to cybercrime.

02

Inclusion of Emerging Technologies

By covering AI, IoT, blockchain, quantum computing, and cloud infrastructure, the Amendment ensures legal oversight of rapidly evolving technologies.

03

Strengthened Institutional Coordination

The Bill formalizes cross-agency collaboration through committees and working groups, promoting whole-of-government cybersecurity governance.

04

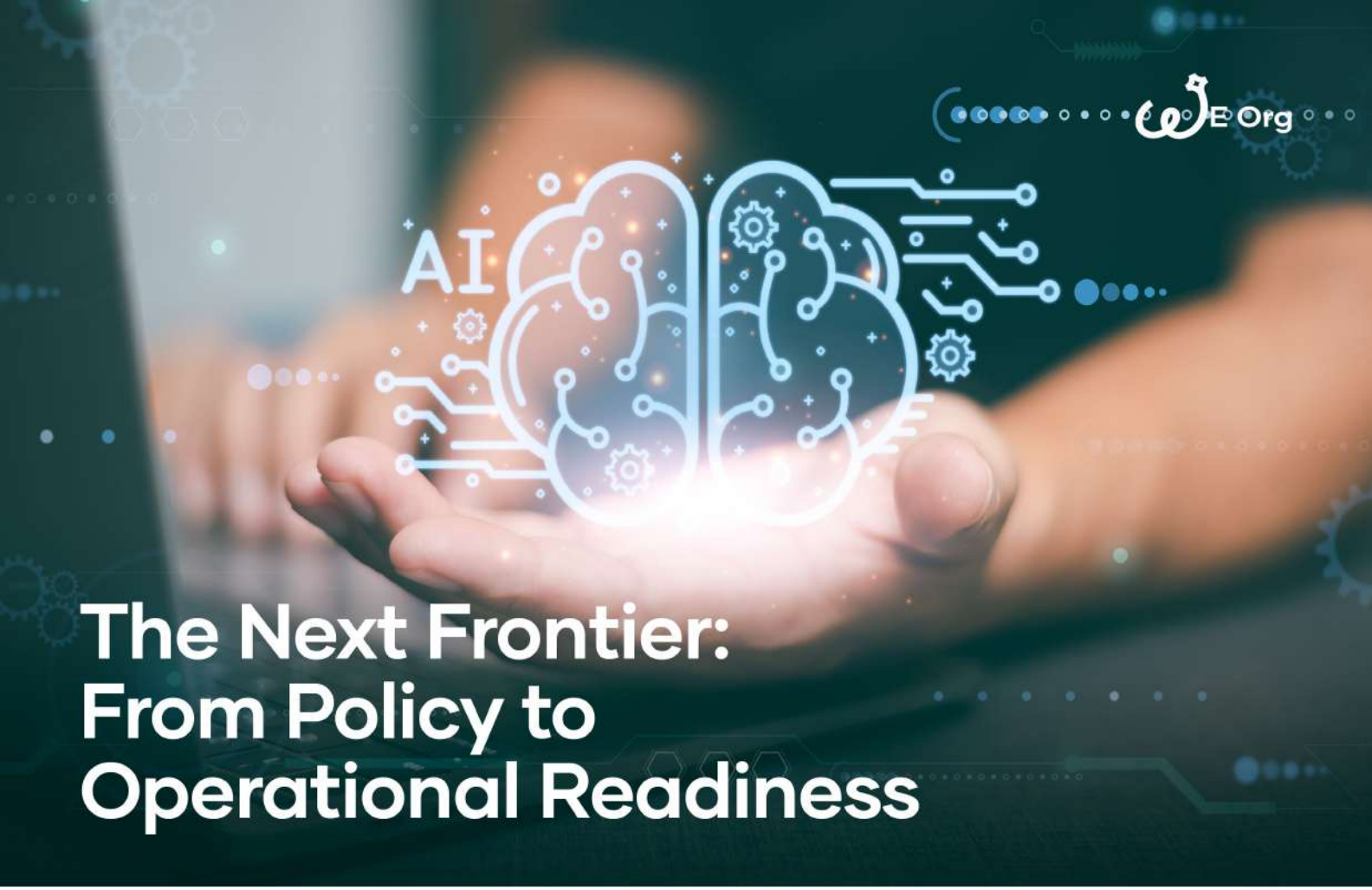
Enhanced Citizen Protection

Provisions addressing online harassment, fraud, and child exploitation demonstrate a commitment to protecting digital citizens.

05

Resource Mobilization

The Cybersecurity Fund expansion enables the CSA to mobilize domestic and external resources to sustain national efforts.



The Next Frontier: From Policy to Operational Readiness

The next stage of Ghana's cybersecurity maturity is operationalization; translating laws and policies into action across all levels of society.

That shift requires structured collaboration between the CSA, MoCD, and strategic partners with technical expertise, innovation capacity, and risk management experience.

The following framework outlines seven national initiatives that would strengthen the Amendment's impact and embed preventive resilience across Ghana's digital ecosystem

Strategic Focus Area	Purpose and Outcomes	Proposed Collaboration
01 National Cyber Risk Framework	Establish a unified, risk-based governance model aligned tonNIST CSF 2.0 and ISO 27001. Define minimum control baselines and sector-specific maturity targets.	Technical design and implementation support under CSA's supervision to harmonize sectoral directives.
02 Continuous Threat Intelligenc Exchange	Develop a national cyber intelligence and early-warning system connecting public - and private-sector SOCs.	Integrate CSA's incident reporting with automated data exchange and shared analytics infrastructure
03 Cyber Hygiene & SME Security Program	Expand national awareness programs into structured SME security certification and training	Design modular training and digital hygiene standards endorsed by CSA and MoCD
04 National Simulation Exercises (Red/Blue Team)	Conduct annual resilience tests for government agencies and critical infrastructure operators.	Facilitate joint exercises and readiness audits coordinated by CSA and Sectoral CERTs.
05 AI & Cloud Assurance Lab	Establish a national facility to test and validate the security of AI models, smart systems, and cloud environments.	Operate under CSA governance to ensure emerging technologies meet national assurance standards.
06 Preventive Funding Mechanism	Dedicate a portion of the Cybersecurity Fund to proactive resilience initiatives, training, R&D, infrastructure	Implement Performance based funding tied to measurable risk reduction outcomes.
07 National Cyber Resilience Index	Introduce an annual readiness index benchmarking public and private sector preparedness.	Manage through CSA to promote transparency, accountability, and continuous improvement.

Together, these initiatives transform Ghana's cybersecurity ecosystem from legislative strength to preventive excellence, reinforcing digital trust and economic competitiveness.

WE Org: Standards Aligned Methods and Proof Points

WE Org brings the operational frameworks, the technical tools and the AI-first engineering capability to convert policy into measurable cyber resilience.

Governance and Risk Frameworks Implemented

- ✓ NIST Cybersecurity Framework 2.0 (Feb 2024); including the new GOVERN function.
- ✓ NIST AI Risk Management Framework for safe, risk aware AI adoption across government services.
- ✓ ISO/IEC 42001 (AI Management System Standard); for AI assurance and auditability.

Threat Informed Defense for AI and IT

- ✓ MITRE ATT&CK + MITRE ATLAS (for both traditional threat actors and adversarial ML attack paths).
- ✓ OWASP Top 10 for LLM Applications; controls for prompt injection, insecure output handling, data poisoning, excessive agency, etc. AI-Driven Innovations deployable in Ghana
- ✓ SOC Copilot for Ghana; LLM-assisted SOC workflows with retrieval-only guardrails.
- ✓ UEBA models for mobile money + PSP fraud anomaly detection tuned to Ghana's empirical fraud typologies.
- ✓ Automated phishing/BEC triage aligned to INTERPOL rated top threats.
- ✓ Adversarial AI testing; red team playbooks aligned to MITRE ATLAS.
- ✓ Deepfake detection for CSA campaigns; detecting AI-generated scam content.

Regulatory Alignment Note

The following matrix demonstrates how these proposed initiatives align with existing national mandates, ensuring full policy continuity and avoiding duplication.

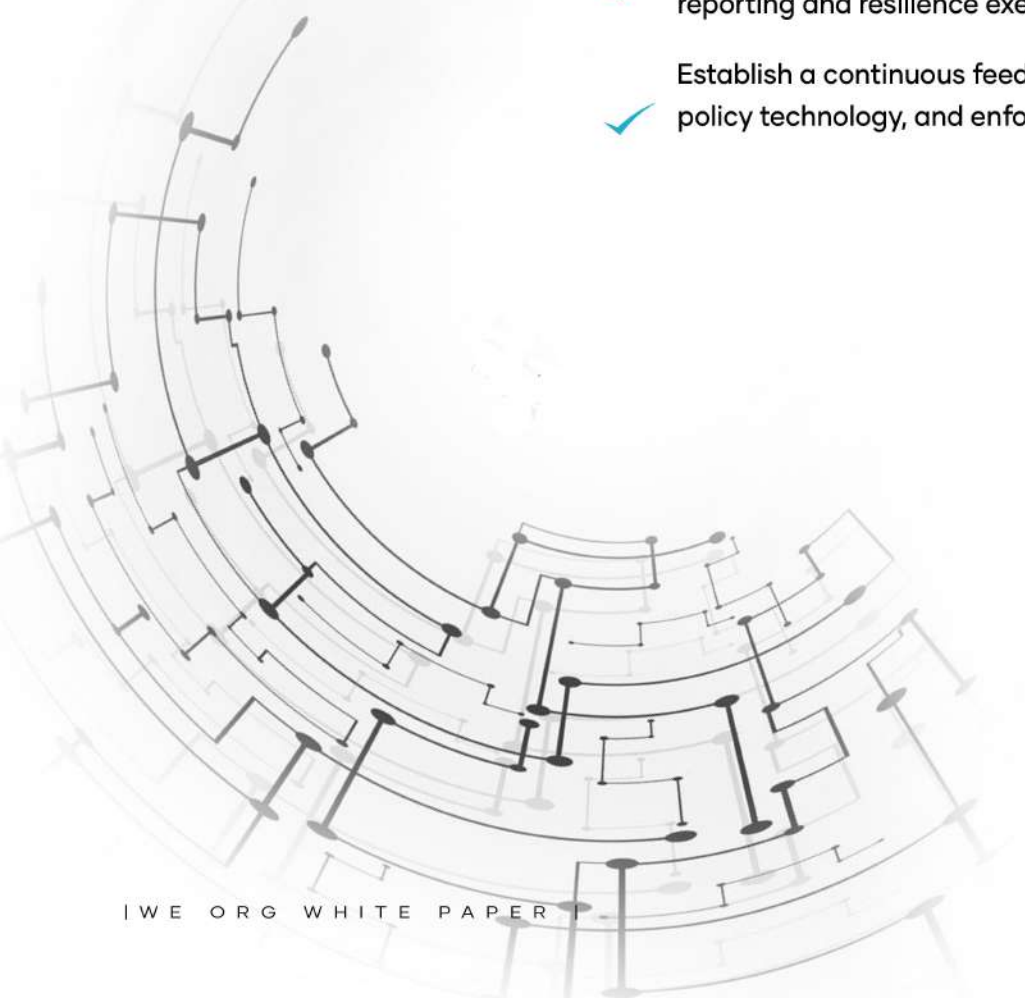
Strategic Focus Area	Existing Ghana Framework(s)	Complementarity and Added Value
National Cyber Risk Framework	Cyber Security Authority under Act 1038: National Cybersecurity Policy & Strategy (2024).	Extends CSA's regulatory powers into a nationwide preventive control baseline
Continuous Threat Intelligence Exchange	CII Directive (2021): 24-hour incident reporting, 72-hour vulnerability disclosure; BoG Cybersecurity Directive (2019).	Expands sector-specific reporting into a unified cross -sector early-warning system.
Cyber Hygiene & SME Security Program	NCPS 2024: national capacity building emphasis; BoG directive on enterprise security governance.	Scales digital hygiene to SMEs and public institutions outside regulated sectors.
National Simulation Exercises	CII Directive: annual audit and incident response requirements.	Converts audits into full-scale simulation exercises testing national readiness.
AI & Cloud Assurance Lab	Cybersecurity Amendment Bill 2025: inclusion of AI, IoT, blockchain, cloud; CSA licensing of cybersecurity service providers.	Creates a technical assurance facility for these new domains, ensuring compliance is verifiable.
Preventive Funding Mechanism	Cybersecurity Fund (Act 1038).	Allocates funding proactively for prevention, innovation, and workforce development.
National Cyber Resilience Index	Sectoral directives (BoG, CII): audit metrics and compliance reporting.	Introduces a transparent, national-level benchmark for resilience and continuous improvement.

Pathways for National Collaboration

Operationalizing preventive resilience will require structured collaboration between the Cyber Security Authority, Ministry of Communications and Digitalisation, and implementation partners across academia, industry, and civil society.

Policy Implementation and Technical Support

- Translate the 2025 Amendment's provisions on AI, cloud, and IoT into operational guidelines and standards.
- Develop sectoral playbooks for risk management, reporting and resilience exercises.
- Establish a continuous feedback mechanism between policy technology, and enforcement teams.



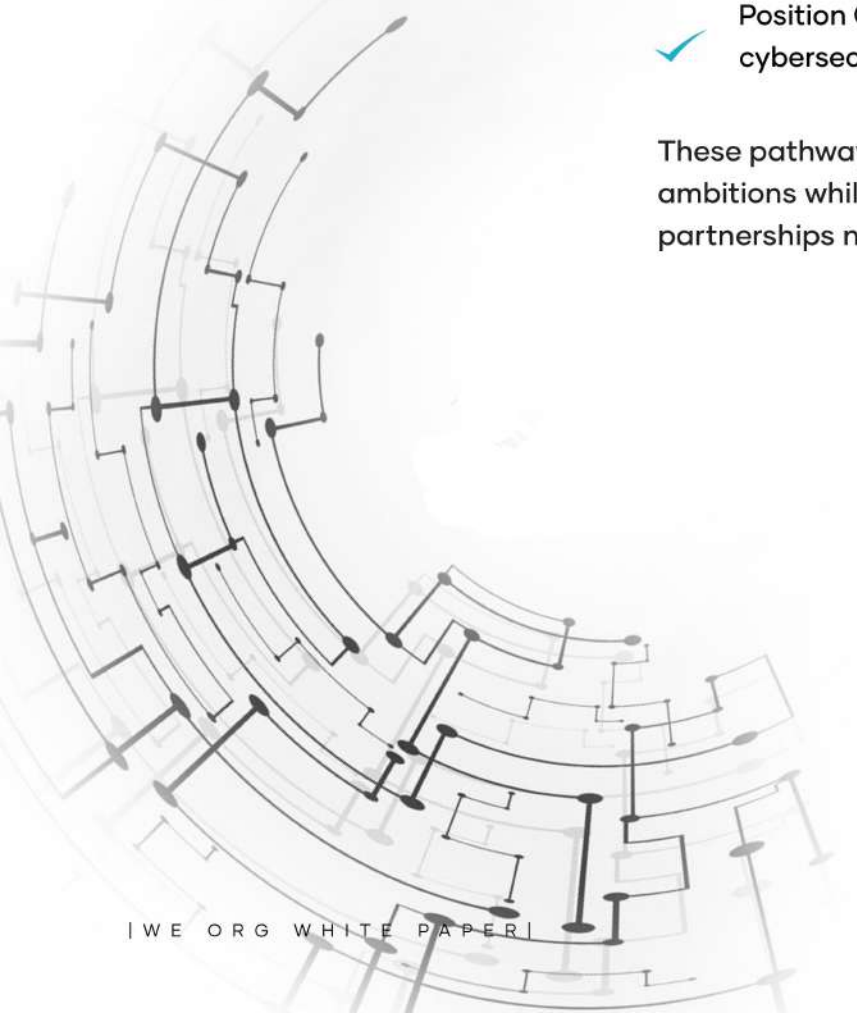
Capacity Building and Workforce Development

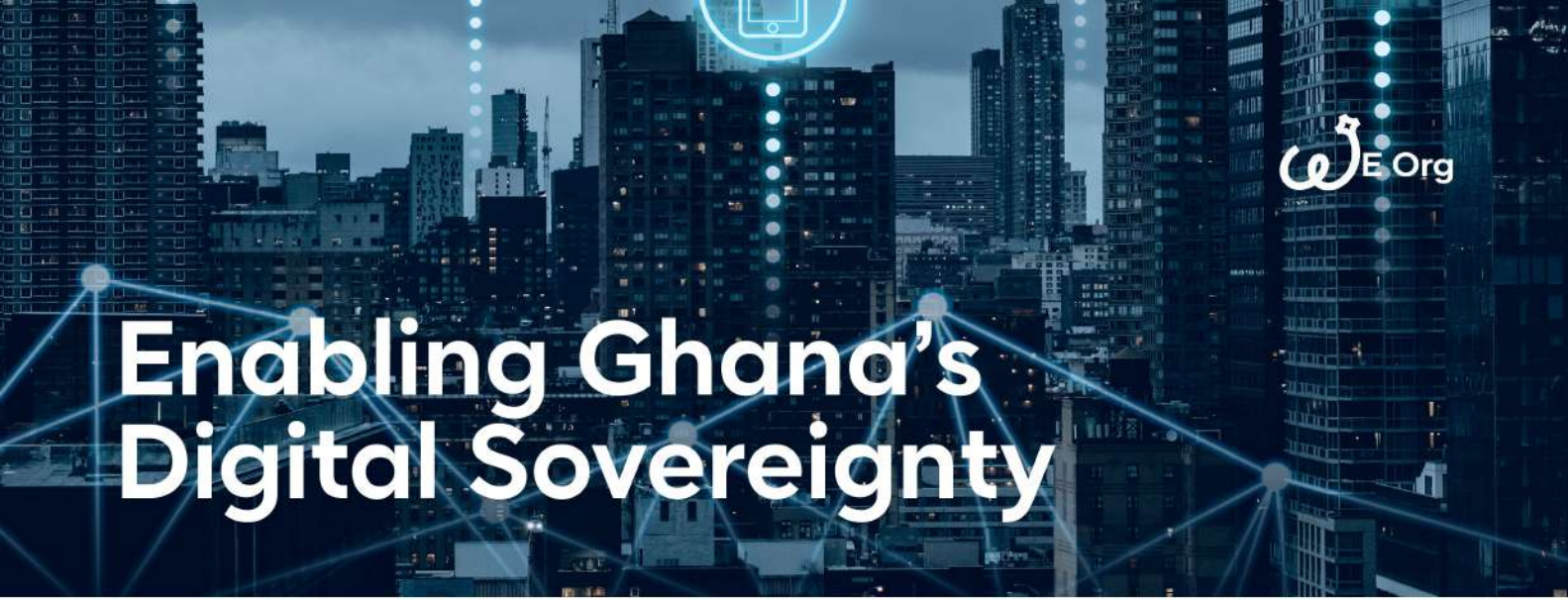
- Create a National Cyber Resilience Academy to consolidate training, certification, and knowledge exchange.
- Integrate cybersecurity modules into tertiary and professional curricula.
- Support women and youth inclusion in the cybersecurity workforce through targeted initiatives.

Innovation and Research Collaboration

- Establish a National Cyber Innovation Lab to pilot AI-assisted detection, digital forensics, and data analytics.
- Promote joint R&D between universities and private innovators under CSA oversight.
- Position Ghana as a West African center for cybersecurity research and technology export.

These pathways mirror Ghana's existing policy ambitions while providing the structure and partnerships needed to achieve them sustainably.





Enabling Ghana's Digital Sovereignty

As Ghana integrates AI, data analytics, and digital services across public administration and commerce, cybersecurity becomes an element of national sovereignty.

Protecting data, ensuring digital trust, and maintaining the integrity of national infrastructure are now as critical as securing borders or managing currency.

The Amendment provides the legal authority; the task ahead is to institutionalize cybersecurity as a culture within ministries, enterprises,and individual behavior.

Embedding preventive controls at scale will:

- Safeguard national infrastructure from systemic cyber incidents.
- Protect citizens' data and privacy across digital platforms.
- Enhance investor confidence in Ghana's digital economy.
- Strengthen the nation's role as a regional cybersecurity leader.

CONCLUSION: Turning Vision into Capability

Ghana's Cybersecurity Evolution is a story of foresight and leadership.

From the establishment of the Cyber Security Authority in 2020 to the 2025 Amendment, the country has demonstrated its commitment to protecting its digital frontier.

The opportunity ahead lies in implementation. By embedding preventive resilience mechanisms, intelligence sharing, simulation exercises, workforce development, and innovation. The nation can turn legal authority into operational readiness.

Cyber resilience is no longer a technical aspiration; it is a national development priority that underpins economic growth, social protection, and digital trust.

Through strategic collaboration among government institutions, regulators, private partners, and citizens, Ghana can move confidently into a future where cybersecurity is both a national strength and a competitive advantage.

About Us

Africa's First Applied AI Research Company

We Org is a technology and innovation company accelerating Africa's digital transformation through human-centered design, ethical AI, and strategic governance. We work with governments, institutions, and private partners to build secure, scalable, and inclusive systems that redefine national progress. We Org is a subsidiary of VB Capital Partners Ltd, a global consulting and technology firm dedicated to advancing resilient, data-driven economies.