FIKIR INSTITUTE
Somalia & Horn of Africa

RESEARCH REPORT

From Law to Practice: Building Somalia's National Cybersecurity Strategy

Somalia passed a Cybersecurity Law, named a lead authority and released a national risk framework within six months. This report assesses what remains before that architecture functions as a strategy, with a focus on the public-private partnership gap.

Hodan Farah · 18 August 2026 · FIKIR Institute

Abstract: Between January and July 2026, Somalia built more national cybersecurity architecture than in the preceding decade combined: a Cybersecurity Law passed by parliament in January, a lead regulatory authority formally designated, a national Computer Incident Response Team (SOM-CIRT) launched in March, and a National Cybersecurity Risk Management Framework released in July, built on ISO/IEC 27000 and 27005 standards. This report assesses that architecture against the four elements a functioning national strategy requires, a centralised strategic direction, a resourced and empowered authority, a complete legal and regulatory framework, and structured public-private partnership, and finds the fourth element the least developed. A proposed Joint Cyber Defense Collaborative linking telecom operators, banks, regulators and government agencies remains at the proposal stage, even as incidents including a November 2025 breach of the e-visa platform affecting roughly 35,000 applicants, and an October 2024 business email compromise that cost a Somali solar energy company $350,000, demonstrate that private-sector systems are already live targets. The report recommends specific next steps across all four pillars, with priority on converting the proposed collaborative into an operating body with a legal mandate.

What has been built

Somalia's cybersecurity architecture has moved unusually fast by the standard of the country's other institution-building efforts. Parliament approved the Cybersecurity Law on 26 January 2026, establishing a national framework that defines the policy role of the Ministry of Communications, designates the National Communications Authority (NCA) as the country's lead cybersecurity authority, sets obligations for operators of critical infrastructure, and creates a formal system for incident prevention, reporting and response, including the Somalia Computer Incident Response Team, SOM-CIRT, which the NCA launched on 7 March. In July, the NCA released a National Cybersecurity Risk Management Framework, developed through consultation with government institutions, universities, private technology firms and civil society groups in Mogadishu, and aligned to the ISO/IEC 27000 and 27005 international standards. Within the law's structure, a Cybersecurity Department carries responsibility for designating Critical Information Infrastructure, sectors including telecommunications, financial services, energy, water, transport and

government digital systems, whose operators face specific obligations under the framework.

This sequence, law, authority, incident response capability, risk framework, in under seven months, represents genuine progress against a starting point the Somali Institute for Development Research and Analysis (SIDRA) described, in a policy brief issued before the framework's release, as a country with substantial gains in digital connectivity and mobile finance but no functional national cybersecurity framework and no operational incident response capability. Two of those three gaps are now formally closed on paper. The question this report addresses is how much of that architecture is operating in practice, and where the remaining gaps sit.

Why the gap matters now, not eventually

Somalia is not building this architecture against a hypothetical threat. In November 2025, Somalia's e-visa platform was breached, exposing personal data, names, photographs, dates and places of birth, email addresses, marital status and home addresses, belonging to an estimated 35,000 applicants. A year earlier, in October 2024, a Somali solar energy company lost $350,000 after attackers compromised its email system, impersonated senior staff, and diverted funds intended for the International Solar Alliance to a fraudulent account, a business email compromise scheme that required no exploitation of government systems at all, only of ordinary corporate email hygiene. Independent assessments have placed Somalia among the top twenty countries globally for the share of computers infected with malware. None of these incidents required a sophisticated state-level adversary; they exploited the same categories of weakness, unpatched systems, weak authentication and untrained staff, that structured national frameworks exist to close. The law and the framework are the architecture. Whether they close gaps like these depends on implementation choices that have not yet been made.

The partnership gap

Of the four elements a functioning national cybersecurity strategy requires, centralised direction, a resourced authority, a complete legal framework, and structured public-private partnership, the fourth is the least developed in Somalia's current architecture. The NCA's consultation process for the July risk framework did bring government officials, universities, private technology firms and civic groups into the same room, and a Joint Cyber Defense Collaborative, intended to link telecom operators, banks, regulators and government agencies for threat-information sharing and coordinated incident response, has been proposed. But a proposed collaborative is not an operating one. Somalia's most consequential digital infrastructure, mobile money platforms, commercial bank systems, telecom networks, is privately or jointly operated, and a national strategy that treats private operators as consultees rather than formal partners with reporting obligations and shared visibility into threat data will struggle to protect infrastructure it does not have operational insight into. This is compounded by a capacity constraint documented across both government and industry: most public institutions and many private companies still lack trained cybersecurity professionals, a gap that structured recruitment, regular training and sustained awareness programmes are only beginning to address.

Recommendations

Centralise strategic direction. The Cybersecurity Law, the risk management framework and SOM-CIRT's operational mandate should be consolidated into a single published national cybersecurity strategy document with time-bound targets and a named lead for each target, so that implementation can be tracked against specific commitments rather than treated as complete once the underlying documents exist.

Resource the designated authority. The National Communications Authority's cybersecurity mandate should be matched with a dedicated, ring-fenced budget line and a published staffing plan for the Cybersecurity Department, distinct from the NCA's existing telecommunications regulatory functions, to ensure Critical Information Infrastructure designation and oversight does not compete for resources with the authority's other responsibilities.

Complete the legal framework. Parliament and the Ministry of Communications should prioritise implementing regulations that the Cybersecurity Law's framework structure anticipates but does not yet fully specify, particularly mandatory breach notification timelines and penalties, sector-specific rules for financial services and telecommunications, and a formal published list of designated Critical Information Infrastructure operators and their specific obligations.

Formalise public-private partnership. The proposed Joint Cyber Defense Collaborative should be converted from a proposal into an operating body with a legal charter, defined membership obligations for telecom operators and banks, and a standing threat-information-sharing mechanism, modelled on functioning information-sharing and analysis centres elsewhere, rather than left as an informal consultative forum. Mandatory incident reporting from designated CII operators to SOM-CIRT should be a condition of continued operation in Somalia's telecommunications and financial sectors, not a voluntary best practice.

Somalia has, in under a year, built more of the formal architecture for a national cybersecurity strategy than most observers would have predicted. The test that now matters is whether the fourth pillar, structured partnership with the private operators who run most of the infrastructure this architecture exists to protect, closes as quickly as the first three did, or whether it remains the gap that incidents like the e-visa breach and the solar company fraud continue to exploit while consultation continues.

References

- Hiiraan Online, "Somalia approves cybersecurity law to protect digital systems and critical infrastructure," January 2026.
- National Communications Authority of Somalia, "Somalia's Parliament Approves the Cybersecurity Law."
- TechAfrica News, "Somalia Establishes National Cybersecurity System with Parliamentary Approval," 29 January 2026.
- TechAfrica News, "Somalia Launches National Cybersecurity Risk Management Framework," 21 July 2026.
- Dawan Africa, "Somalia's Telecom Regulator Eyes National Cybersecurity System."
- Ecofin Agency, "Somalia Expands Public Sector Cyber Skills Amid Rising Threats."
- SIDRA Institute, "Cybersecurity in Somalia: Current Landscape, Risks, and Opportunities."
- ID Tech, "Somalia's E-Visa Platform Hit By Cyber Incident, Exposing Traveller Data."

- Powers of Africa, "Cyberattacks: Somalia Moves to Strengthen Its Cybersecurity Framework."
- Global Cyber Security Capacity Centre, University of Oxford, Somalia country profile.