SIDRA INSTITUTE

Policy Brief 26

December 2025

Cybersecurity in Somalia: Current Landscape, Risks, and Opportunities

Abdi Omar Bile

Key Messages

- Somalia's rapid expansion in digital technologies has reshaped communication, commerce, and service delivery, yet the country remains highly vulnerable due to the absence of a comprehensive national cybersecurity framework capable of protecting its growing digital ecosystem.
- Cyberattacks targeting Somalia have increased in scale and sophistication, affecting government systems, private companies, and individuals, and exposing sensitive data as seen in recent breaches involving major institutions, including the national e-visa platform.
- Weak legal enforcement, limited technical infrastructure, and insufficient skilled personnel continue to undermine Somalia's ability to detect, manage, and respond to cyber threats, leaving the country's digital systems exposed to significant operational and financial risks.
- The National Communications Authority and its Computer Emergency Response Team remain under-resourced and not fully operational, preventing the establishment of a coordinated national mechanism for monitoring threats and guiding incident response across public and private sectors.
- Digital financial services and mobile-money networks have become central to Somalia's economy, but their heavy reliance on telecommunications infrastructure makes them highly susceptible to cyberattacks that could disrupt financial stability and public trust.
- Somalia's integration into the East African Community and its partnerships with technologically advanced countries offer critical opportunities to strengthen institutional capacity, modernize cybersecurity governance, and align with regional and global best practices.
- The country's youthful and increasingly tech-savvy population provides a strategic advantage for future digital resilience, making investments in digital literacy, cybersecurity education, and innovation ecosystems essential for building a secure digital future.
- Sustained investment in cybersecurity, including adequate budget allocation, specialized personnel, and clear regulatory frameworks, is urgently required to safeguard Somalia's digital transformation and ensure long-term national security and economic stability.

Introduction

Digital technologies and internet connectivity continue to reshape social and economic systems worldwide. For households, improved access to timely information and reduced transaction costs help strengthen learning outcomes, support more active labor-market participation, and raise income and overall welfare. For businesses, digital tools are becoming integral to decision-making, operational efficiency, innovation, and the ability to reach a broader market (World Bank, 2024).

Africa is experiencing a rapid digital transformation. Despite ongoing challenges related to infrastructure, connectivity, and service reliability, Internet adoption continues to rise across the continent. Between 2019 and 2022, more than 160 million people became regular users of cyberspace, highlighting the growing dependence on digital platforms for communication, commerce, education, and governance (World Bank, 2024). This expansion is reshaping how communities connect and access opportunities, even as digital inclusion remains uneven across regions.

Despite the rapid expansion of the digital age, this transformation has also introduced significant risks, most notably the rising threat of cybercrime. As technological innovation accelerates, cybercriminals have adapted in parallel, using increasingly sophisticated methods to exploit digital vulnerabilities. These developments pose serious risks to individuals, organizations, and national security. The impacts extend well beyond financial losses, often resulting in considerable psychological and emotional distress for victims (Interpol, 2024).

In 2024, the cybersecurity landscape was shaped by rising geopolitical tensions, rapid AI adoption, and increasing vulnerabilities across global supply chains, according to the Global Cybersecurity Outlook 2025 (World Economic Forum, 2025). Organizations faced mounting pressure as regulatory environments became more fragmented and cybercrime, particularly AI enhanced ransomware, grew more sophisticated. More than 15 million cybercrime incidents were recorded globally in 2024, a slight decrease from the previous year. The highest level was in 2021, with 19.23 million incidents (Statista, 2025).

In 2023, nearly 10 million devices were infected with data-stealing malware, each exposing an average of 51 login credentials. Cybercriminals used these stolen credentials to enable further attacks or traded them across dark-web forums and private Telegram channels (Kaspersky, 2024).

Africa is among the regions that have faced the highest number of cyberattacks in recent years. The 2023 assessment points to a sharp rise in such incidents, underscoring the continent's growing exposure to digital threats (Interpol, 2024). According to the report, the average number of weekly cyberattacks per organization increased by 23% from the previous year, marking the highest global growth rate. Although the report does not provide a consolidated total of incidents, it highlights that both the frequency and impact of cybercrime continue to escalate. Importantly, cyber-dependent and cyber-enabled crimes are now classified as medium to high-risk threats in more than two-thirds of surveyed countries, revealing widespread vulnerability across Africa's digital landscape.

While the global community has witnessed significant technological advancements over the past three decades, Somalia has also grappled with prolonged conflict and instability, conditions that have constrained its ability to benefit from digital progress fully. Even so, notable gains have been made, particularly in telecommunications and digital financial services (World Bank, 2024). Somalia's cybersecurity vulnerabilities stem from weak legal enforcement, limited technical infrastructure, a shortage of skilled personnel, and the absence of coordinated national mechanisms for threat detection and response. Together, these factors create a fragile digital environment highly susceptible to cyber risks, underscoring the urgent need for sustained capacity-building and strategic planning.

Somalia currently faces a significant gap in its cybersecurity architecture, as there is no clearly defined national strategy to prevent or respond to large-scale cyberattacks. Although the cabinet has approved a new cybersecurity bill, it has not yet been ratified by parliament (SONNA, 2025). The country ranks among the top 20 globally in terms of the number of computers infected with malware, underscoring the severity of the threat.

The absence of a coordinated cybersecurity system also means there is no reliable mechanism for tracing the origin of attacks. Over the past decade, cyber incidents in Somalia have frequently involved the hacking of email accounts, personal computers, and web applications, exposing both individuals and institutions to persistent digital vulnerabilities (Nur, Abas Osman, 2021).

This policy brief examines Somalia's digital development, the emerging cybersecurity challenges, the current response efforts, and future opportunities, and concludes with actionable policy recommendations.

Methodology

This policy brief employed a desk-based review of secondary data drawn from published research, government documents, credible media sources, and policy reports. Given the scarcity of peer-reviewed studies on cybersecurity in Somalia, the analysis relied heavily on grey literature, including institutional reports, regulatory documents, and expert commentaries. All sources were carefully assessed for credibility, relevance, and consistency with the study's objectives before being incorporated.

Key Research Findings

Digital Growth in Somalia

Somalia's digital development has expanded considerably over the past two decades, supported by increasing mobile connectivity and rising internet penetration in major urban centers. As of early 2025, the country recorded approximately 11.3 million active mobile connections, around 58.3 percent of the total population. However, many of these subscriptions may be limited to basic services such as voice and SMS and may not necessarily include internet access (Datareportal, 2025). Social media usage has also grown, with an estimated 3.05 million user profiles recorded in January 2025, representing roughly 15.8 percent of the population (Datareportal, 2025).

Digital financial services operated by telecommunications companies have expanded rapidly, becoming a central driver of Somalia's informal economy and daily transactions (Peter Chonka, Gayatri Sahgal, & Mahad Wasuge, 2025). Remittances have also remained Somalia's primary source of foreign exchange since the early 2000s. In 2021, cross-border transfers from the Somali diaspora were estimated at more than US$1.4 billion. According to the Central Bank of Somalia, remittances account for 50 percent of total inflows and roughly 25 percent of the country's GDP, underscoring their importance to household resilience and national economic stability (World Bank , 2024).

Somali financial institutions heavily rely on digital technology. The country's financial sector currently consists of thirteen (13) domestic commercial banks, one (1) foreign bank branch, fifteen (15) money transfer businesses, and five (5) mobile money operators (Central Bank of Somalia, 2015). In 2015, the sector made another significant advancement when Premier Bank partnered with MasterCard Inc. to issue debit cards, marking an important milestone in Somalia's integration into global financial services (Bloomberg, 2015).

Despite digital money systems being the fastest-growing component of Somalia's technological advancement, progress in other sectors has been limited. Industries that support online business operations, instant payments, and digital advertising remain underdeveloped. Nevertheless, Information and Communication Technology (ICT) has improved access to international trade, making it easier for businesses to import products from global suppliers. In recent years, several digital media companies have emerged, and the government has launched various digitalization initiatives to shift from paper-based processes to digitized, automated systems (Heritage Institute, 2023).

However, over the past decade, Somalia has made substantial progress in its digital transformation. Despite these gains, significant challenges persist, including limited digital skills, underdeveloped digital infrastructure, inaccessible connectivity, a digital gender gap, inadequate regulatory frameworks, and weak cybersecurity capacity—leaving the digital ecosystem vulnerable to cyberattacks.

Cybersecurity Threats and Incidents in Somalia

Cybersecurity analysis in Somalia remains underdeveloped, with no quantitative data currently available to assess the scope or impact of cyber threats. The National Communications Authority (NCA) serves as the primary institution responsible for national cybersecurity oversight. Its mandate includes preventing, mitigating, and responding to cybercrimes across the country. Within the NCA, the Somalia Computer Emergency Response Team/Coordination Center (SomCERT/CC) plays a central role in managing cybersecurity incidents affecting both public and private sectors. SomCERT/CC is tasked with detecting and reporting information security events; however, its effectiveness is limited by the absence of a centralized database for systematic incident tracking and analysis.

The Governance Statistics Report published by the Somalia National Bureau of Statistics (SNBS, 2024) provides a qualitative assessment of cybersecurity trends in Somalia. According to the report, cybercriminals frequently target individuals through widely used social media platforms, with fraud and financial scams remaining among the most common forms of cybercrime. Common tactics include phishing emails, fake investment opportunities, and fraudulent websites designed to mislead both individuals and businesses. The rapid expansion of mobile money services has further contributed to an increase in mobile-based fraud, particularly unauthorized transactions and SIM-card swapping (SNBS, 2024).

Cyber incidents have continued to rise as government agencies, businesses, and individuals become frequent targets for unauthorized access to sensitive information. Weak cybersecurity measures across many organizations create an environment that enables hackers to exploit system vulnerabilities, infiltrate critical networks, and carry out malicious activities. Theft and data breaches have become a growing concern, especially as increasing volumes of personal information are stored and shared online (SNBS, 2024).

Online harassment and cyberbullying remain major cybersecurity issues in Somalia, especially on social media platforms. These crimes often target individuals like journalists, activists, and women, involving the spread of false information, online threats, and defamation. According to SNBS, ransomware and malware attacks are also increasing. These attacks encrypt vital data, with cybercriminals demanding payments for its release. Malware is similarly used to breach systems, steal information, or disrupt operations, often leading to substantial financial losses and operational downtime.

The most common cyberattacks faced by Somali telecommunications companies, one of the country's most digitally dependent sectors, are phishing, virus and malware infections, denial of service (DoS) attacks, and advanced persistent threats (APTs). Limited cybersecurity awareness and training have left many employees vulnerable to social engineering tactics, increasing the risk of system breaches and unauthorized access (Nur, Abas Osman, 2021).

A notable example of Somalia's growing exposure to cyber threats is the October 2024 incident involving a Somali solar energy company that lost USD 350,000 in a sophisticated cyberattack. According to media reports, hackers infiltrated the company's email system and impersonated its executives to redirect payments meant for India's International Solar Alliance (ISA). The attackers used forged documents and deceptive communication to manipulate financial transactions, ultimately transferring the funds into a fraudulent account (Hiiraan Online, 2024).

The recent cyberattack on Somalia's e-visa system in November 2025 highlights the country's increasing cybersecurity threats and ongoing vulnerabilities in government agencies. During this attack, personal data of about 35,000 people, including applicants' names, photos, birth dates and locations, email addresses, marital statuses, and home addresses, was leaked (Al Jazeera, 2025).

Current Responses

Somalia currently lacks effective and institutionalized mechanisms to respond to cybersecurity threats and attacks. The Computer Emergency Response Team (CERT), established under the National Communications Authority (NCA), remains non-operational in detecting or mitigating cybersecurity risks (World Bank, 2024).

In addition, the country faces foundational gaps in both data protection and cybersecurity capacity. Although the recent enactment of the Public Data Protection Act and the creation of the Somali Data Protection Authority represent important legal milestones, the operational capacity of these frameworks remains limited and under-resourced.

Most government institutions and private companies in Somalia lack dedicated and trained cybersecurity teams. Key security practices are not widely implemented; only a limited number of organizations use Intrusion Detection Systems (IDS), data encryption, or routine information backups. Instead, many institutions rely almost exclusively on basic antivirus tools and firewall software as their primary line of defense. Additionally, formal or written cybersecurity procedures are largely absent (Nur, Abas Osman, 2021).

However, Somalia's cybersecurity capacity remains at an early stage of development. Key supporting institutions, including the Data Protection Authority and the national Computer Emergency Response Team (CERT), are not yet fully operational, and a comprehensive law addressing cybersecurity and cybercrime is still pending.

Opportunities

Despite Somalia's cybersecurity system being in a period of rapid development, the country can benefit from the experiences of neighboring states that have already implemented national cybersecurity strategies. Somalia's accession to the East African Community (EAC) in 2024 presents an opportunity to align with regional best practices and strengthen its digital resilience (EAC, 2024). Collaboration with technologically advanced nations is also essential for expanding national cybersecurity capacity. The Memorandum of Understanding signed in May 2025 between the Somalia National Communications Authority (NCA) and the Malaysian Communications and Multimedia Commission (MCMC) marked an important step toward improving cooperation on digital regulation, technical capacity-building, and cybersecurity (SONNA , 2025).

Somalia's private sector offers another promising avenue for strengthening national cybersecurity, particularly through the Information and Communications Technology (ICT) industry. As one of the most dynamic segments of the economy, the ICT sector now contributes approximately 11 percent of GDP, with telecommunications driving much of this growth (World Bank, 2024). The rapid expansion of digital businesses further underscores both the urgency and the opportunity to establish resilient cybersecurity systems that can support Somalia's evolving digital landscape.

Somalia's National Communications Authority (NCA) has faced challenges due to inconsistent budget allocations, which undermine financial planning and operational continuity (NCA, 2024). However, there are notable opportunities to strengthen the sector—particularly through the World Bank Group's continued engagement in Somalia. The Somalia Capacity Advancement, Livelihoods and Entrepreneurship through Digital Uplift Project (SCALEDUP) (P168115), launched in 2019 and funded by the World Bank, supports the development of a vibrant digital ecosystem. This includes investments in digital ID systems, government digital service capabilities, data protection, and cybersecurity, as well as institutional capacity-building for both the Ministry of Communications and Technology (MoCT) and the NCA (World Bank, 2024).

Somalia's final opportunity lies in its human capital, one of the world's youngest populations. Urban youth are increasingly tech-savvy, supported by expanding mobile phone usage and growing internet access. This demographic advantage offers a strategic pathway for investment in youth-centered digital policies, including cybersecurity training, digital literacy, and the development of innovation ecosystems.

Conclusion

Somalia has made progress in digital transformation over the past few years. However, its cybersecurity systems and data protection safeguards are still in the early stages of development, even as global cyber threats continue to grow rapidly.

As a result, these sectors and the broader digital landscape in the country remain vulnerable to cybersecurity threats due to the absence of a strong, functional national cybersecurity framework.

Addressing cybersecurity is essential not only for the sectors mentioned above but also for the country as a whole. Somalia urgently needs foundational cybersecurity systems to protect its developing digital infrastructure, financial sector, and public institutions, and to build resilient security frameworks that can operate effectively.

Policy Recommendations

- The Federal Government of Somalia, particularly the National Communications Authority (NCA), should swiftly strengthen and equip all necessary infrastructure with a National Computer Emergency Response Team (SomCERT) that will serve as the primary point of contact for cyber incidents at the national level and ensure the effective fulfillment of its responsibilities.
- Somalia's NCA should provide regular, mandatory, and effective cybersecurity training programs for public and private sector institutions to raise awareness of the importance of cybersecurity and to help operators better understand risks and the best practices for managing them
- The NCA should establish a Joint Cyber Defense Collaborative to improve coordination between government and private actors, unify national cybersecurity efforts, share information, and coordinate responses to major threats affecting critical infrastructure.
- The Federal Parliament of Somalia should approve the cybersecurity bill to provide a clear legal framework for protecting national digital systems, institutions, and citizens from cyber threats.
- Public and private institutions in Somalia should hire dedicated cybersecurity professionals and conduct regular training to strengthen employees' digital security skills and awareness.
- The NCA should convene an annual national cybersecurity conference to enhance public awareness of digital risks, promote best practices, and strengthen collaboration across government, private sector, and civil society.
- Somalia should collaborate with technologically advanced countries to benefit from their technical expertise, secure digital tools, and effective policy models that support national cybersecurity development, protect critical sectors such as mobile money and telecommunications, and promote digital literacy.
- The Federal Government should increase national budget allocations for cybersecurity to build institutional capacity, enable SomCERT/CC to become fully operational, and ensure effective enforcement of the national cybersecurity framework.

References

Al Jazeera. (2025, November 16). Somalia confirms major data breach in electronic visa system. https://www.aljazeera.com/news/2025/11/16/somalia-confirms-major-data-breach-in-electronic-visa-system

Bloomberg. (2015, June 3). Mastercard crosses final African frontier as it enters Somalia. https://www.bloomberg.com/news/articles/2015-06-03/mastercard-crosses-final-african-frontier-as-it-enters-somalia

Central Bank of Somalia (CBS). (2015). Annual report 2024. https://centralbank.gov.so/annual-report-2024/

DataReportal. (2025, March). Digital 2025: Somalia. https://datareportal.com/reports/digital-2025-somalia

East African Community (EAC). (2024, March). Somalia finally joins EAC as the bloc's 8th partner state. https://www.eac.int/press-releases/3049-somalia-finally-joins-eac-as-the-bloc-s-8th-partner-state

Heritage Institute. (2023, May). Digital ID: Prospects and challenges for Somalia. https://heritageinstitute.org/digital-id-prospects-and-challenges-for-somalia/

Hiiraan Online. (2024, October). Hackers steal $350k from Somali solar firm in bold cyberattack on India's ISA. https://hiiraan.com/news4/2024/Oct/198464/hackers_steal_350k_from_somali_solar_firm_in_bold_cyberattack_on_india_s_isa.aspx

Interpol. (2024). Africa cyberthreat assessment report 2024. https://www.interpol.int/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf

Kaspersky. (2024, April). Data-stealing malware infections increased sevenfold since 2020, Kaspersky experts say. https://www.kaspersky.com/about/press-releases/data-stealing-malware-infections-increased-sevenfold-since-2020-kaspersky-experts-say

National Communications Authority (NCA). (2024). Annual report 2022–2023. https://nca.gov.so/wp-content/uploads/2025/01/NCA-Annual-Report-2022-2023_.pdf

Nur, A. O. (2021). Cybersecurity awareness in Somalia. https://www.theseus.fi/handle/10024/501168

Chonka, P., Sahgal, G., & Wasuge, M. (2025). Mobile money, (dis)empowerment and state reconstruction in Somalia's conflicted digital economy. https://doi.org/10.1093/ia/iiae273

Somalia National Bureau of Statistics (SNBS). (2024). Governance statistics report (2nd version). https://nbs.gov.so/wp-content/uploads/2025/03/Governance-Statistics-Report-2nd-Version.pdf

SONNA. (2025, May). Somalia signs MoUs with Malaysia on digital regulation and cybersecurity. https://sonna.so/en/somalia-signs-mous-with-malaysia-on-digital-regulation-and-cybersecurity/

SONNA. (2025, August). Somali cabinet approves landmark cybersecurity bill to boost digital security. https://sonna.so/en/somali-cabinet-approves-landmark-cybersecurity-bill-to-boost-digital-security/

Statista. (2025). Cyberattacks: Annual worldwide forecast. https://www.statista.com/forecasts/1485031/cyberattacks-annual-worldwide

World Bank. (2024). Digital progress and trends report 2023. https://www.worldbank.org/en/publication/digital-progress-and-trends-report

World Bank. (2024). Digital transformation drives development in AFE/AFW Africa. https://www.worldbank.org/en/results/2024/01/18/digital-transformation-drives-development-in-afe-afw-africa

World Bank. (2024). https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099045403212411797

World Economic Forum. (2025). Global cybersecurity outlook 2025. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

About the Author

Abdi Omar Bile holds a Bachelor's degree in Computer Science and a Master's degree in Journalism and Mass Communication. He has nearly 15 years of experience in digital media and currently serves as a researcher at SIDRA Institute. His research interests include media, technology, politics, and broader social issues.

SIDRA INSTITUTE

Ministerial Hill, Behind the Immigration Building, Garowe, Puntland, Somalia

Tel: +252 5 846044

Email: info@sidrainstitute.org

Website: https://sidrainstitute.org/