CYBER CRIME

Cyber cracks beneath Uganda's digital rise

Attackers are increasingly exploiting ordinary internet functions that many institutions barely monitor.

Cybersecurity.|

BETTY M. NDAGIRE

At a district headquarters in Uganda, an official logs into a government system using a national Identity Card instead of piles of paperwork. A health worker uploads records from a rural clinic onto a shared platform, while a bank clerk verifies customer details within seconds. To many citizens, it feels like long-awaited digital progress is finally taking shape.

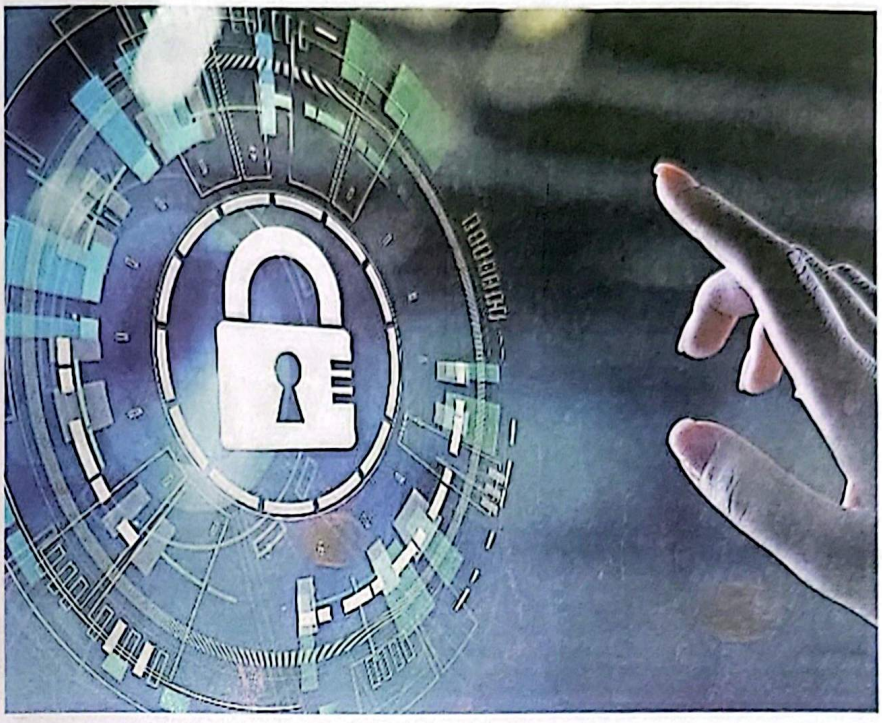
But beneath Uganda's rapid digital transformation lies a growing vulnerability that often only becomes visible when systems fail, money disappears or services suddenly freeze. As more public services move online, government institutions are becoming bigger targets for cyber attacks, despite many still operating with weak or outdated protections.

That contrast, fast digitisation alongside fragile cyber preparedness, is now pushing Uganda to rethink how it secures public systems. It is also increasing interest in "Firewall as a Service (FWaaS)", a model where institutions access cloud-based cybersecurity protection instead of buying costly hardware infrastructure.

Richard Obita, the director of technical services at the National Information Technology Authority Uganda (NITA-U), says the country's digital growth has made cybersecurity impossible to ignore.

He says the National Backbone Infrastructure, which connects ministries, departments, agencies and local governments, is expanding together with government digital services.

"One of the things that NITA-U does is the provision of e-government services to ministries, departments and agencies," Obita says. "As government continues digitising services for the benefit of citizens, there is need to enhance the security of the network so that government operates in a secure environment."



Artificial Intelligence, cloud systems and future quantum computing technologies are reshaping the cybersecurity landscape. PHOTO/FILE

No cyber protection

Obita says many government institutions are still operating without proper cyber protection despite handling sensitive citizen data and financial systems. During engagements with district local governments, several openly admitted they had no firewall protection at all.

"Some of them were saying no, they do not have firewalls," he explains. "They can now leverage on the government firewall. It cuts costs because government already adopted a strategy to rationalise resources. We do not have to duplicate efforts."

The economic logic behind the model is significant for Uganda, where many district administrations struggle with constrained budgets, aging ICT equipment and limited technical staff. Traditional hardware firewalls often require importation, installation space, cooling systems and constant maintenance, costs that many institutions cannot sustain.

The new system allows agencies to access cybersecurity protection through software hosted within government infrastructure. Obita describes it as a shared service model similar to how government already provides internet and centralised data hosting.

"The beauty with it is that it is a cloud-based cybersecurity solution," he says. "Entities do not have to buy hardware. We simply give them a firewall, more or less a software firewall."

For Uganda, the stakes go far beyond technical jargon. Government systems are increasingly interconnected with banks, health systems, tourism databases and financial platforms. Obita says NITA-U has already begun integrating systems across sectors so institutions can share information digitally instead of relying on paperwork.

"When an organisation goes to a bank, what they normally ask you for is your basic information, national ID, and that data is with NITA-U," he says. "By just showing your national ID, systems can pull the information instead of filling forms and lining up for services."

But integration also creates a larger attack surface. A breach in one vulnerable institution can potentially expose multiple connected systems.

Elizabeth Namanya, a network engineer at Spidd Africa, says reality is why cybersecurity is becoming inseparable from digital transformation itself.

"Cybersecurity is no longer optional," Namanya says. "With digital transformation, firewall as a service gives enterprise-grade protection for government services without the burden of managing complex infrastructure."

Namanya explains that the initiative was designed to create awareness among ministries, departments and agencies as Uganda rolls out the firewall service nationally. Spidd Africa worked alongside NITA-U and Palo Alto Networks to implement the solution.

"It is cost-effective and it protects their networks," she says, adding that many institutions previously lacked the capacity to deploy advanced cybersecurity tools independently.

Uganda's challenge reflects a wider African paradox. Governments are digitising faster than they are securing. Cybercrime continues costing African economies billions of dollars annually, yet many public institutions still rely on outdated defenses or fragmented security systems.

In Uganda, this vulnerability is intensified by rising internet penetration, mobile money expansion and growing use of digital public services. Every new online platform, from tax systems to health records, creates another possible entry point for attackers.

Titus Gateri, a Palo Alto Systems engineer and cyber security architect, warns that attackers are increasingly exploiting ordinary internet functions that many institutions barely monitor.

"What atackers know is that Domain Name System (DNS) is running in every organisation and nobody is inspecting it," Gateri says. "Someone can be sitting in Russia, Kenya or anywhere issuing instructions to your machines through DNS traffic."

He recounts an incident in Kenya where an organisation unknowingly lost large amounts of sensitive data through manipulated DNS traffic over a weekend.

"About 20 to 30 gigabytes of DNS traffic were moving from an email server," he explains.

"On inspection, it turned out attackers were breaking down email databases into small pieces and sending them out disguised as DNS requests." Such attacks are especially dangerous for developing countries where institutions often lack advanced monitoring systems and trained cyber personnel.

Gateri says traditional security systems are also becoming too slow and expensive for modern threats. Hardware firewalls can take weeks or months to procure because of shipping delays, customs processes and global supply chain disruptions.

"With physical appliances, you have to worry about shipping, customs, cooling and cabling," he says. "Now you go to the data portal, click and have your firewall in about 20 minutes."

For governments operating under budget pressure, that speed could become transformational. Instead of waiting months for hardware procurement, districts can activate protection almost instantly.

Emerging cyber risks

Yet the emerging cyber risks are evolving faster than many policymakers anticipated. Gateri warns that Artificial Intelligence, cloud systems and future quantum computing technologies are reshaping the cybersecurity landscape.

"What is considered secure today may become unsafe in the next few years," he says, warning that attackers are already harvesting encrypted data now in anticipation of future quantum computing capabilities that could crack current encryption methods.

He says this has created a "harvest and wait" strategy where cybercriminals steal encrypted information, store it and wait for more powerful computing systems to unlock it later.

Firewall as a service; therefore, goes beyond software. It reflects a deeper struggle over whether digital transformation in a low-income economy can happen securely enough to sustain public trust.

Key data

300%

The National Information Technology Authority reports a 300 percent spike in automated attacks.

27%

East Africa recorded the highest rejection rate for identity verification in Africa in 2024, at 27 percent, according to the 2025 Digital Identity Fraud report.

Data

'Attackers are already harvesting encrypted data now in anticipation of future quantum computing capabilities that could crack current encryption methods.'