The African Cybersecurity Threat Landscape

AiCE Africanism & Pan-African Studies — How serious is the threat?

How Serious Is the Threat?

The cybersecurity threat to African countries, organisations, and individuals is serious, growing, and systematically underestimated. Interpol's African Cyberthreat Assessment reports consistently identify Africa as one of the world's most targeted regions for cybercrime — partly because African digital systems are often less well-defended than their equivalents in Europe or North America, making them easier targets, and partly because the rapid digitalisation of African economies has created valuable new targets without corresponding investment in security.

The African Development Bank estimates that cybercrime costs African economies approximately $4 billion per year in direct losses — and the indirect costs, including lost productivity, damaged reputation, regulatory penalties, and the deterrence of digital investment, are likely several times higher. For context, $4 billion represents approximately the entire annual health budget of Nigeria, Africa's largest economy.

Threat Type	African Examples & Impact
Financial Fraud & Scams	Nigeria's Business Email Compromise fraud causes an estimated $1.5 billion in annual losses; mobile money fraud across East Africa erodes trust in digital finance.
Ransomware	Hospitals in South Africa and Kenya hit by ransomware; government systems locked, disrupting service delivery, with payment typically demanded in cryptocurrency.
State-Sponsored Attacks	Foreign state actors targeting African government ministries and stealing sensitive diplomatic data; suspected election interference in several countries.
Disinformation Campaigns	Foreign-funded disinformation during African elections and health misinformation causing preventable deaths; difficult to counter without suppressing legitimate speech.

Threat Type	African Examples & Impact
Surveillance Technology	Pegasus spyware used against journalists and activists in Rwanda, Morocco, and Togo; demonstrates that cybersecurity is fundamentally a human rights issue.
Cryptocurrency Fraud	South Africa's Mirror Trading International Ponzi scheme lost investors an estimated $1.7 billion; regulatory frameworks lag rapid adoption.
Data Breaches	South African credit bureau Experian breach exposed 24 million records (2020); multiple government database breaches have exposed millions of citizens' personal data.

The Most Dangerous Threat: Surveillance Technology and Political Repression

Among all the cybersecurity threats facing Africa, none is more insidious — or more directly relevant to the democratic values examined in an earlier unit — than the use of surveillance technology by African governments against their own citizens. The Pegasus spyware scandal, which broke globally in 2021, revealed that the Israeli NSO Group's military-grade surveillance software had been used to target journalists, human rights activists, lawyers, and opposition politicians across Africa, with documented use in Rwanda, Morocco, Togo, and several other countries.

Pegasus is a 'zero-click' spyware, meaning it can infect a target's smartphone without the target taking any action, such as clicking a link. Once installed, it gives the operator complete access to the phone's contents: messages, emails, photos, contacts, location data, and even the microphone and camera. A journalist who believes their communications are private is in fact being monitored in real time. A human rights defender whose sources trust them with their identity is exposing those sources to the government they are trying to hold accountable.

The use of Pegasus and similar tools — FinFisher, Candiru, RCS — against African civil society figures is a direct attack on the democratic values this course has defended throughout. A free press that cannot communicate securely is not free. A civil society that cannot organise without government surveillance is not independent. The

cybersecurity of journalists, activists, and opposition figures is not a marginal concern — it is central to the health of African democracy.

> *"When a government uses spyware to read a journalist's messages, it is not committing a cybercrime. It is committing a crime against democracy. The security of the journalist's phone is the security of the public's right to know."*
>
> **— Adesina Olagunju, Founder, AiCE**

Key Takeaways

Cybercrime costs African economies an estimated $4 billion annually across financial fraud, ransomware, state-sponsored attacks, disinformation, and cryptocurrency fraud — but the most dangerous threat is the weaponisation of surveillance technology like Pegasus against journalists and activists, which is a direct attack on democratic institutions, not merely a technical security incident. The next lesson examines how prepared African countries currently are to defend against these threats.