Harnessing Artificial Intelligence For National Cyber Resilience

Abimbola O'larred Turner
@Clan_Clueless

The future of technology. I bet you never saw it from this angle.

@SwickTV

eVTOLs (electric vertical takeoff and landing) human passenger drones

The Reality: Showing Nigeria's critical infrastructure under pressure

NIGERIA'S CRITICAL INFRASTRUCTURE ALREADY UNDER PRESSURE

Powering lives. Connecting communities. Enabling the economy. **Under constant threat.**

POWER SECTOR

- Aging infrastructure and equipment
- Gas supply constraints and vandalism
- Grid losses of 30–40%
- Limited SCADA security

IMPACT: Blackouts, economic losses, disrupted services, public safety risks

BANKING & FINANCIAL SERVICES

- Rising cyberattacks and phishing
- Account takeover and fraud
- Third-party/vendor risks
- High volume of digital transactions

IMPACT: Financial losses, erosion of trust, service disruptions, economic instability

Disruption in one sector triggers impact across all.

TELECOMMUNICATIONS

- Fibre cuts and theft
- Vandalism of towers and equipment
- SIM-swap fraud and identity theft
- High dependency on imported technology

IMPACT: Call drops, internet outages, financial fraud, loss of productivity

GOVERNMENT SERVICES

- Legacy systems and outdated software
- Data breaches and ransomware attacks
- Limited cybersecurity budgets and skills
- Fragmented systems and data silos

IMPACT: Disrupted public services, data loss, loss of citizen trust, national security risks

CROSS-CUTTING PRESSURES AFFECTING ALL SECTORS

CYBER THREATS
AI-powered attacks, ransomware, phishing, and insider threats are increasing.

ECONOMIC PRESSURE
Inflation, currency fluctuations, and high cost of technology importation.

SKILLS GAP
Shortage of cybersecurity and ICT professionals across sectors.

POLICY & REGULATION
Fragmented policies, slow adoption, and weak enforcement of standards.

INFRASTRUCTURE GAPS
Poor maintenance, inadequate funding, and poor physical security.

PUBLIC AWARENESS
Low cybersecurity awareness increases vulnerability to social engineering.

CLIMATE & ENVIRONMENT
Flooding, erosion, and extreme weather events damage critical infrastructure.

WHY IT MATTERS

- A cyberattack on the power grid can shut down hospitals, banks, and airports.
- A telecom outage stops businesses, payments, and emergency communications.
- A breach in government systems exposes citizens' data and weakens national security.

RESILIENT INFRASTRUCTURE. SECURE NIGERIA. PROTECTED FUTURE.

THE TIME TO STRENGTHEN RESILIENCE IS NOW.

Building secure, resilient, and sustainable systems is essential to protect Nigeria's future and ensure national stability.

Sources: NERC, NCC, Central Bank of Nigeria, NIMC, NDPC, FGN Reports, Industry Reports (2023–2024)

What must Nigeria do to secure its critical infrastructure against AI-driven cyber threats? Page 1

Focus on the fundamentals first, then scale AI intelligently.

1. Protect identities and privileged access.
2. Segment critical networks.
3. Deploy AI for detection, response, and prediction.
4. Build robust backup and recovery capabilities.
5. Share threat intelligence across sectors.
6. Strengthen regulation, reporting, and workforce capacity.

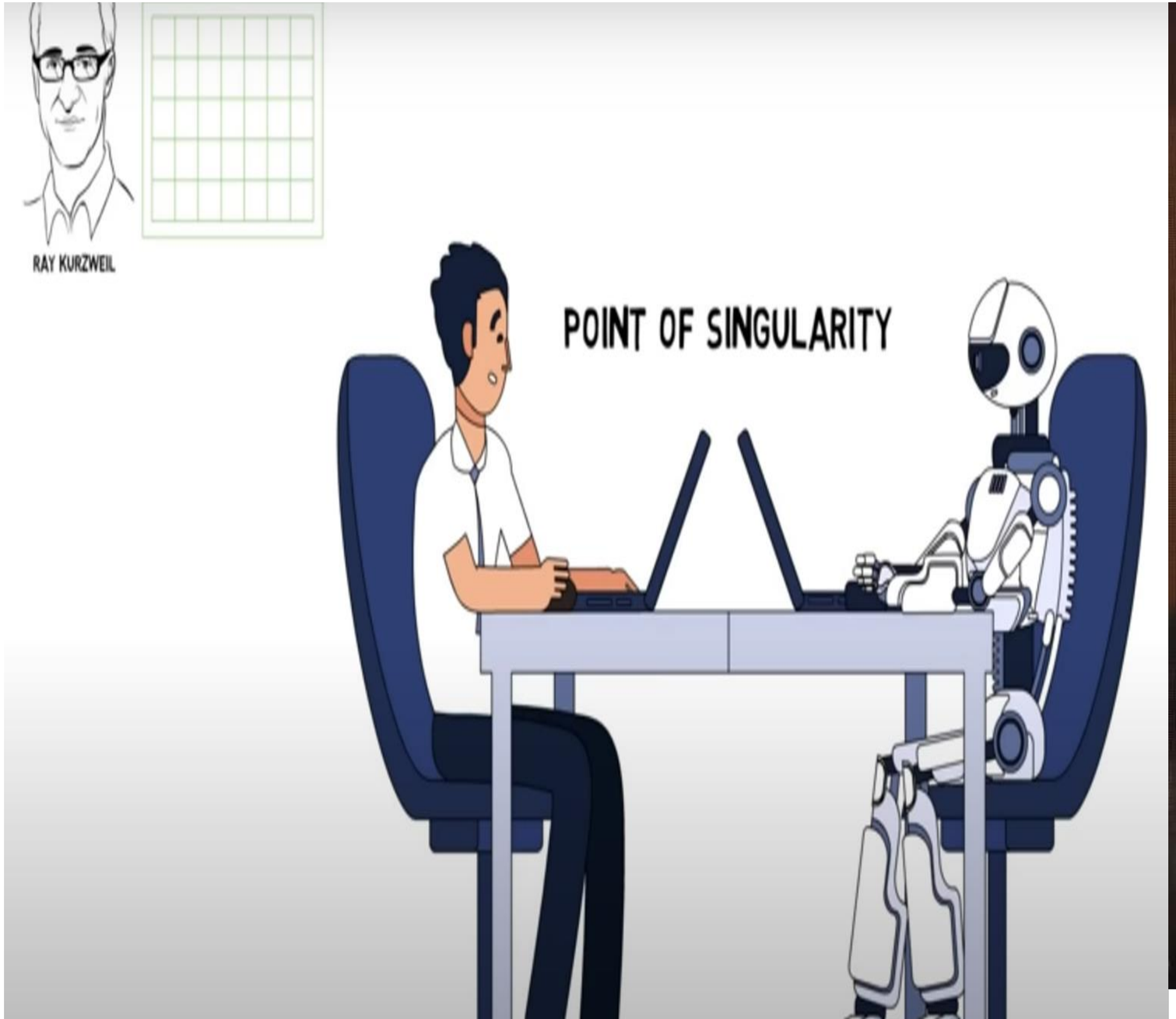
What must Nigeria do to secure its critical infrastructure against AI-driven cyber threats? page 2

Answer: The common denominator is identity compromise
1. Government systems:
Identity databases, tax systems, immigration systems, procurement platforms, and public service portals.
2. Power sector:
Grid control systems, distribution management systems, smart meters, and operational technology (OT) networks.
3. Telecommunications:
Mobile networks, fibre backbones, internet gateways, cloud infrastructure, and data centres(SOC).
4. Banking and fintech:
Core banking systems, payment switches, mobile banking, ATMs, and digital wallets.
Key message: AI is changing both the attack and defence landscape.
Attackers now use AI for phishing, credential theft,
malware development, and social engineering at scale.

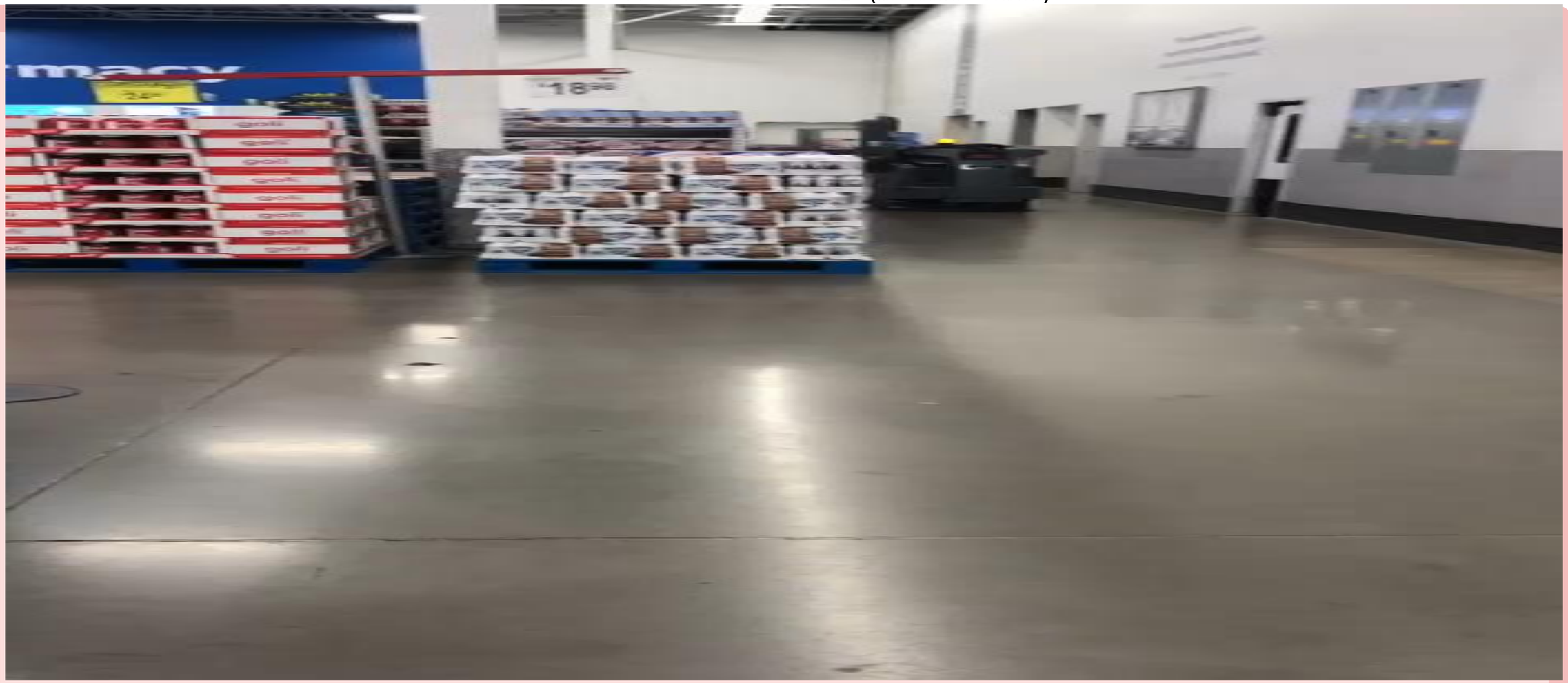
The New Threat — AI-Driven Cyber Attacks

Threat	Practical Example
AI-generated **phishing (very common in Nigeria now)**	Perfect emails targeting bank staff or government officials
Deepfake voice calls	Fake CEO or minister instructing urgent transfers
AI-assisted malware	Malware that adapts to evade detection
Automated reconnaissance	AI scans internet-facing systems for weaknesses
Disinformation attacks	Fake announcements during crises/ elections, fake farms, shopping gone wrong.

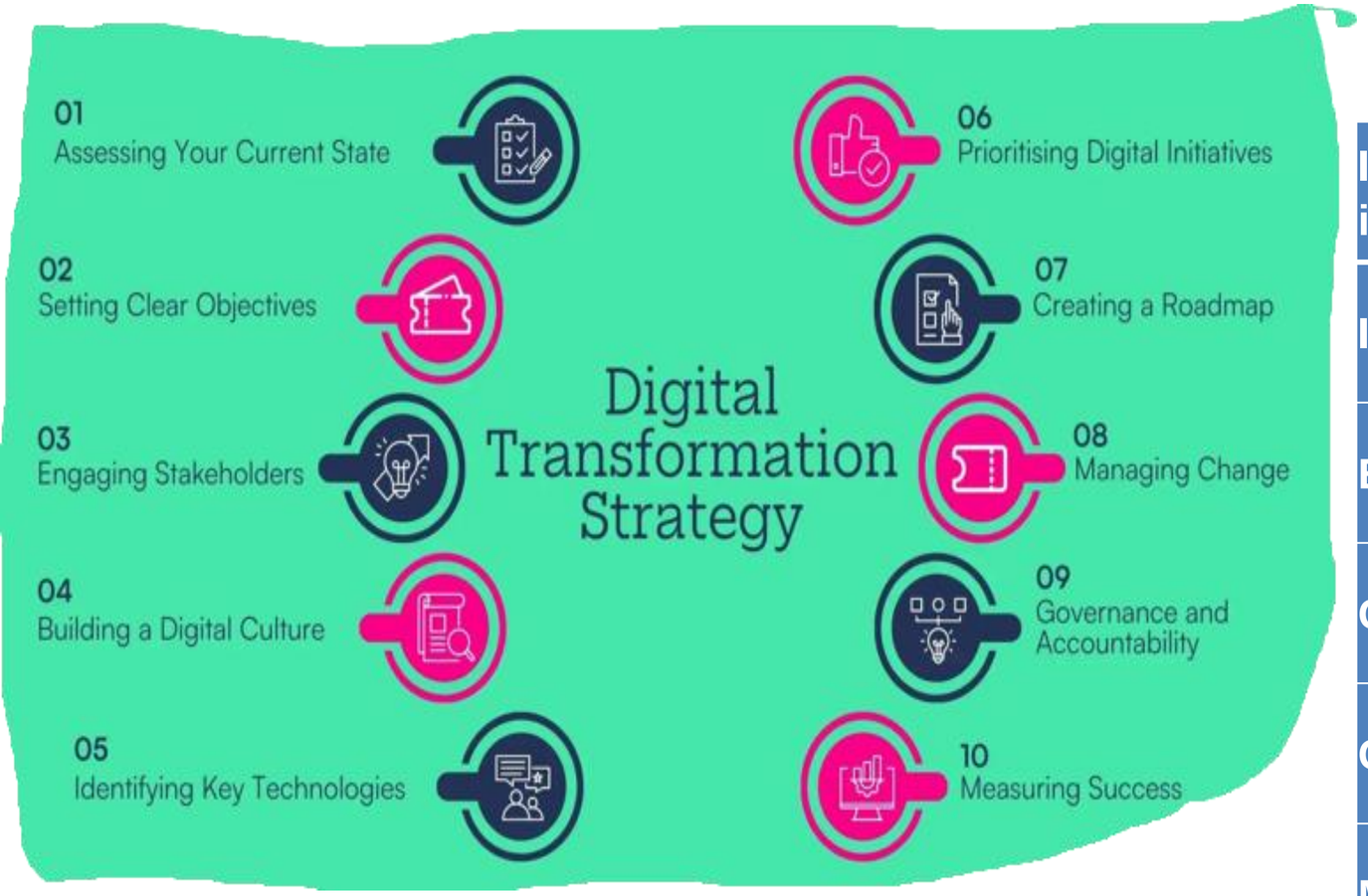
Will AI Replace Jobs (e.g CYBORGS by Elon Musk)?



Store Data Collection AI (amateur video)



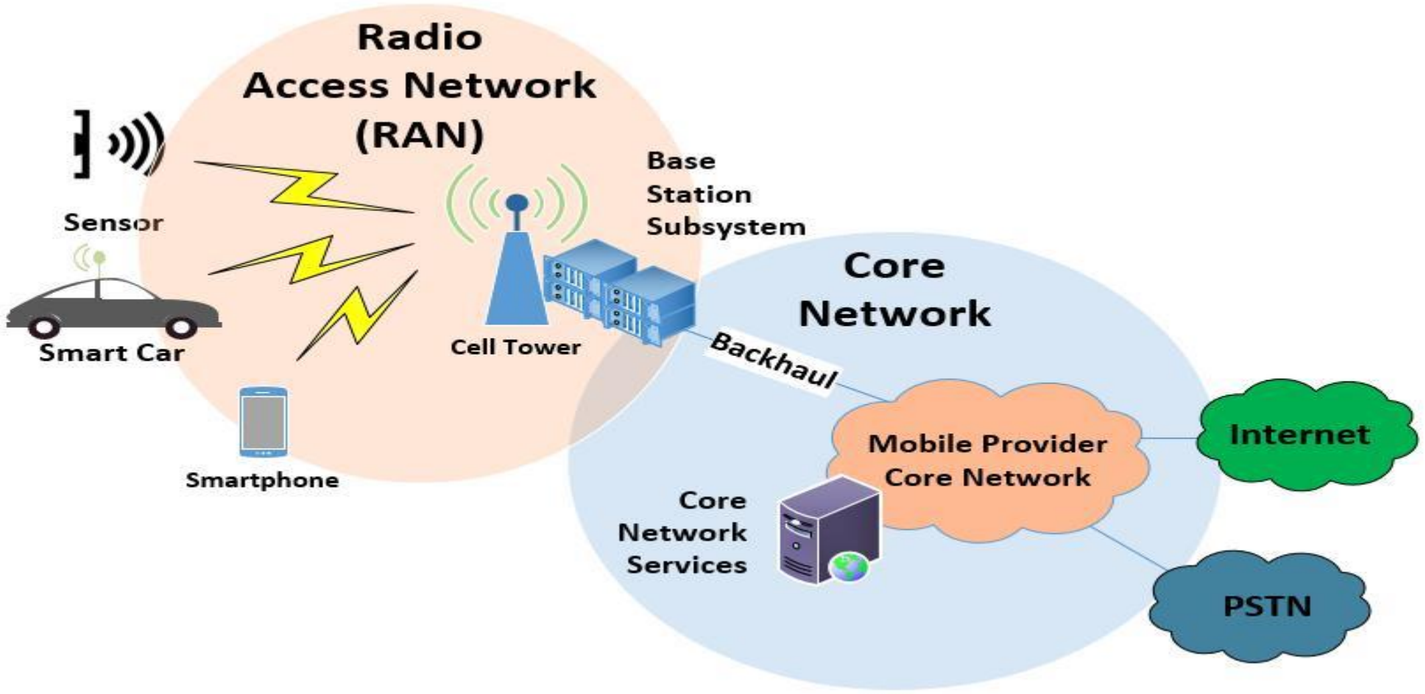
What Nigeria Must Do (12-Month Action Plan)



Top Priorities

Identify and classify all critical digital assets (Asset inventory).
Implement MFA across government and critical sectors.
Establish sectoral AI-enabled SOCs.
Conduct national cyber resilience exercises.
Create a unified incident reporting platform.
Mandate offline backup and recovery testing.
Invest in cybersecurity workforce development.
Deploy AI-based fraud and deepfake detection capabilities.

Cyber attacks: The common denominator is identity compromise

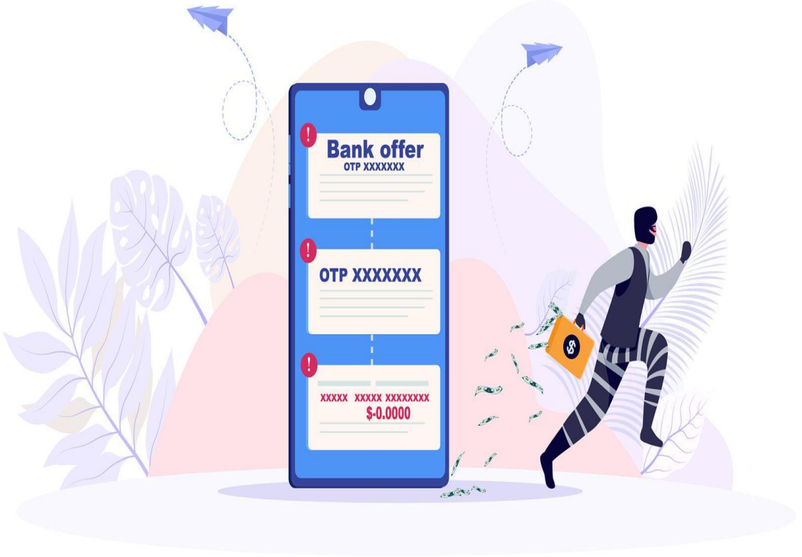


Telecom, Government and Banks:

Network intrusion,

SIM-swap fraud, AI-assisted phishing,

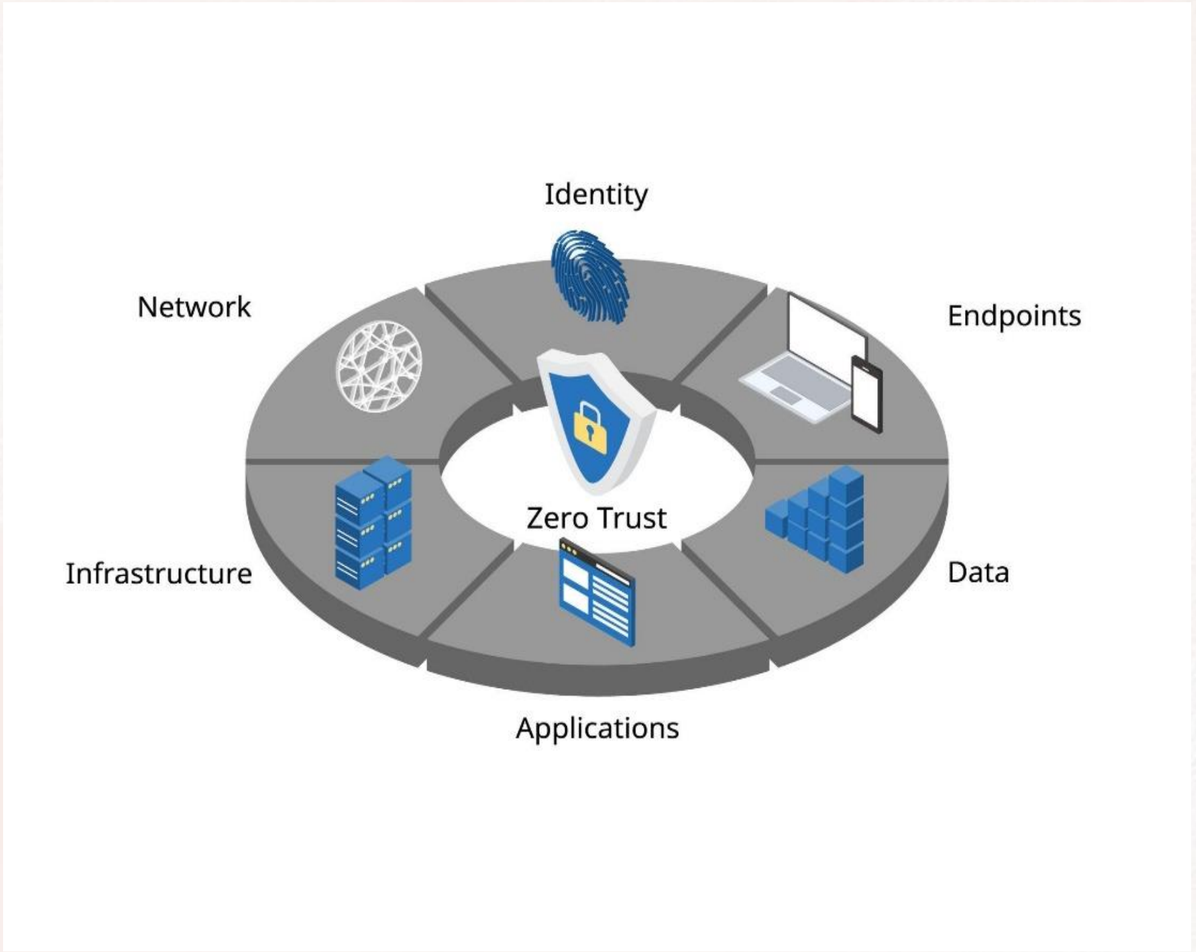
DDoS attacks (Distributed Denial-of-Service)



What Artificial Intelligence Should Actually Do

Four-Layer Defence Model

Layer	What to Implement
1. Prevent:	Zero Trust access, MFA, network segmentation, asset inventory
2. Detect:	AI-enabled SOC, endpoint detection, network analytics
3. Respond:	24/7 incident response team, automated containment, crisis communication
4. Recover:	Offline backups, disaster recovery sites, regular recovery testing.



Note: Resilience means assuming a breach will occur and preparing to recover quickly.

Five layers every critical infrastructure operator should implement pg1.

Layer 1. Identity Protection

- Multi-factor authentication for all privileged accounts
- Privileged access management for administrators
- Continuous monitoring for stolen credentials

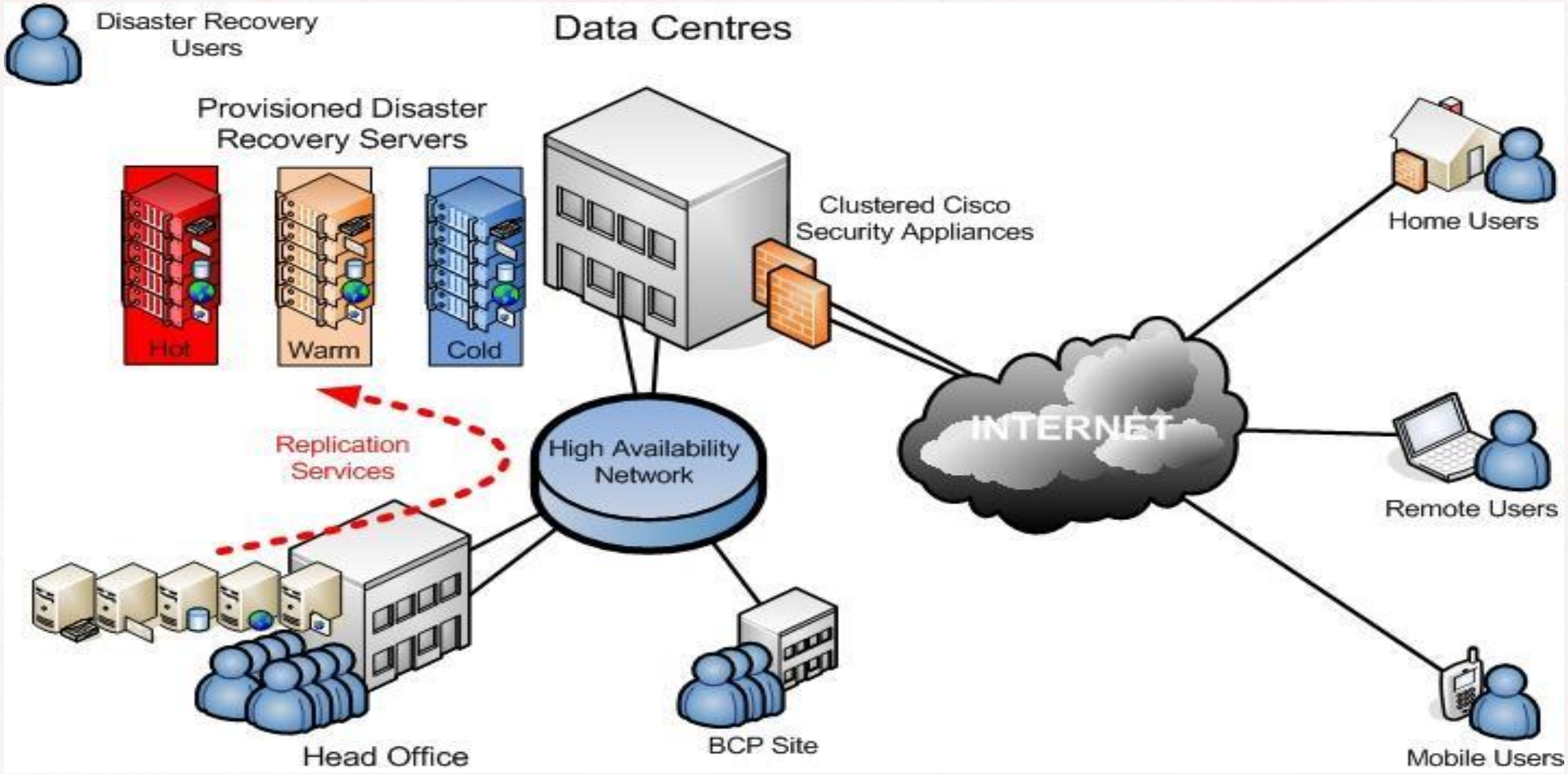
Layer 2. Network Segmentation

- Separate IT networks from operational technology (OT) networks
- Strict access controls between business systems and industrial control systems

Layer 3. Threat Intelligence Sharing

- Share indicators of compromise across sectors
- Coordinate through national CERT(Computer Emergency Response Team) structures

Five layers every critical infrastructure operator should implement pg2

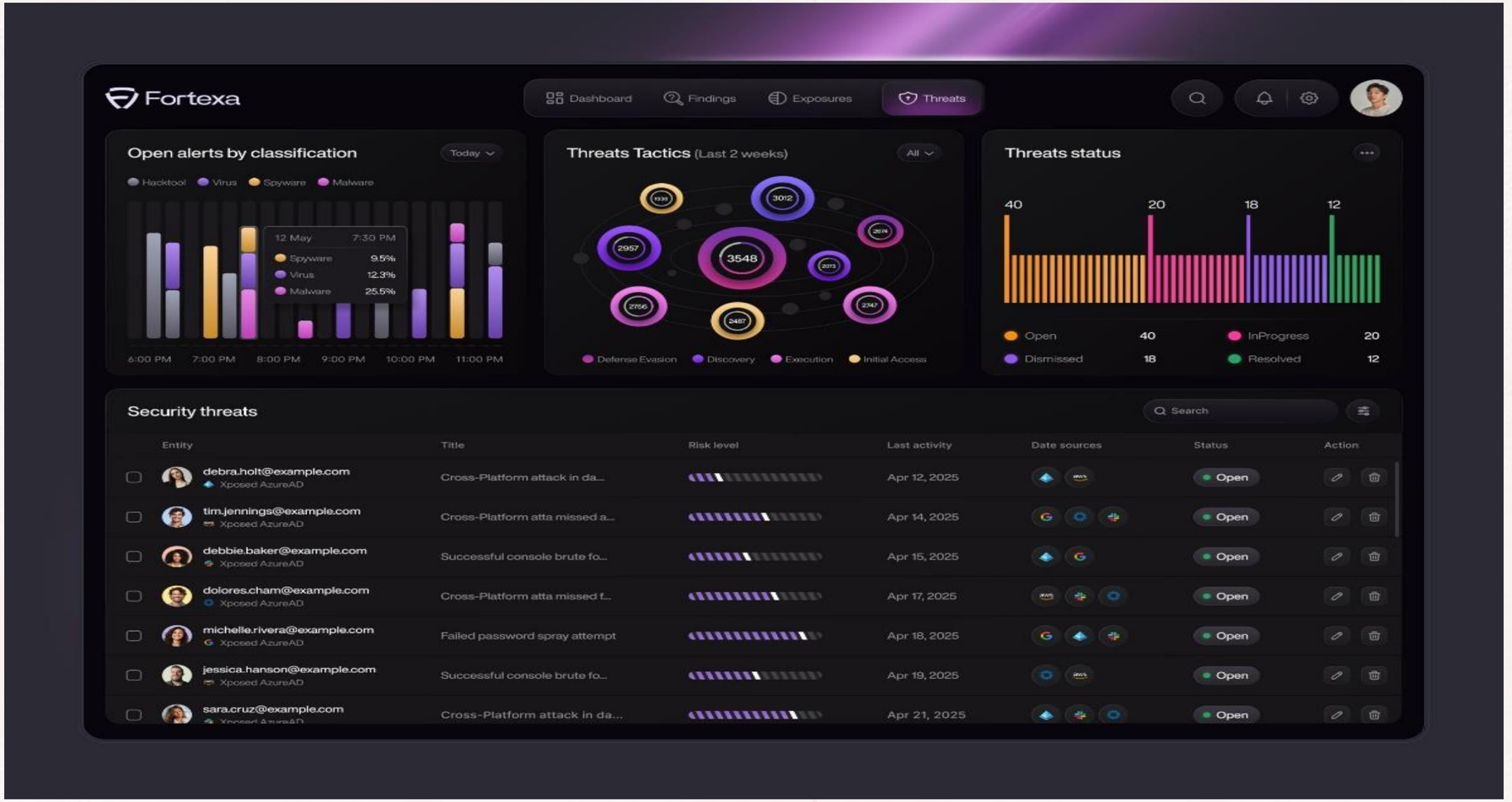


- Offline backups
- Disaster recovery sites
- Regular recovery drills

Layer 4. Picture of disaster recovery site

Five layers every critical infrastructure operator should implement pg3

Layer 5. AI-Enabled Monitoring



- Use machine learning to detect abnormal behaviour
- Monitor unusual login locations, transaction patterns, and network traffic
- Deploy Security Information and Event Management (SIEM) with AI analytics

Examples:

•SIM-Swap Fraud CBN-NCC launched TIRMS (Telecoms Industry Risk Management System) to combat rising SIM-swap fraud, Bank account takeover and financial loss

•Network Disruption MTN recorded over 9,200 fibre cuts in 2025 Internet, voice, and payment service outages

•Core Network Attack MTN Group cyber incident exposed customer information, Potential large-scale service disruption and data compromise.

Critical rule

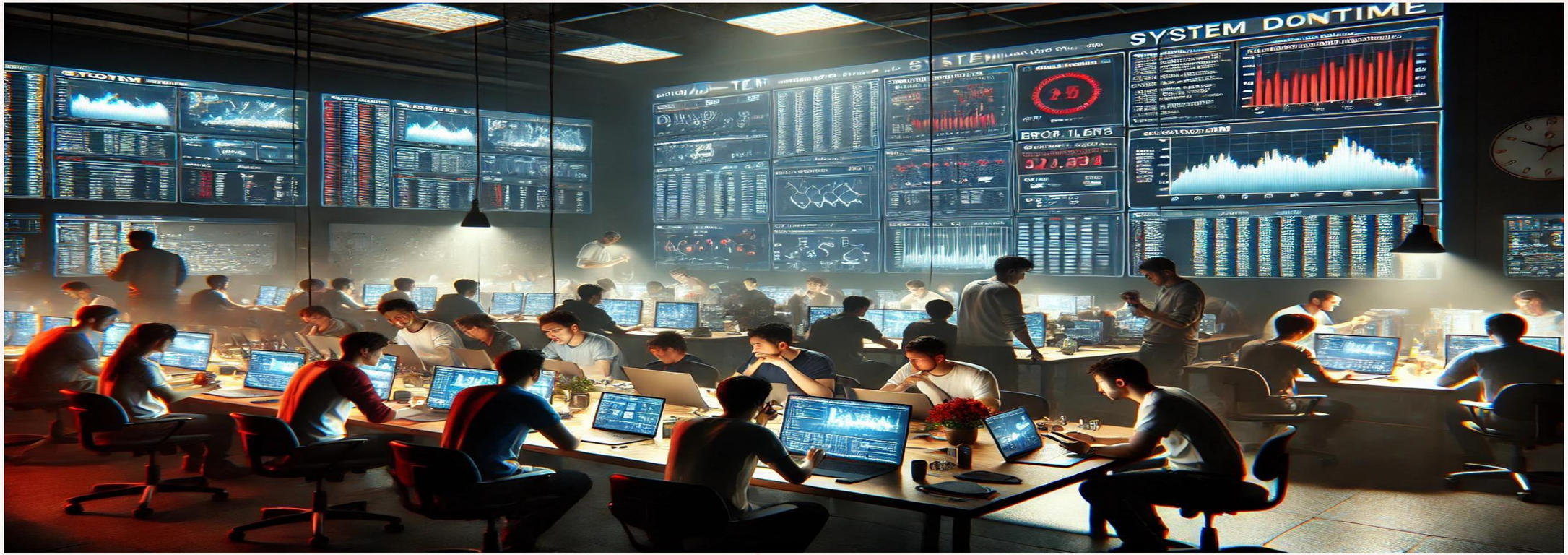
Do not negotiate operational decisions through email during an active attack.
Use pre-approved secure communication channels.

Internet of Everything:

encompasses the interconnection of not just devices, but also people, processes, and data, creating a network where everything communicates, collaborates, and shares information in real-time.

Final Note: One of the things Nigeria should do is to set up:

National war room Management/cyber crisis room



Teams working together in one room: SOC, Legal, Communications, Executives
AI should become a force multiplier for cyber defenders and national resilience.
The objective is not to buy more technology but to build systems that can continue operating, recover quickly, and maintain public trust even when under attack.


Thank You