Protecting critical infrastructure in the digital age: Analysing cybersecurity threats and countermeasures

Seyi Stephen

UNIVERSITY OF JOHANNESBURG

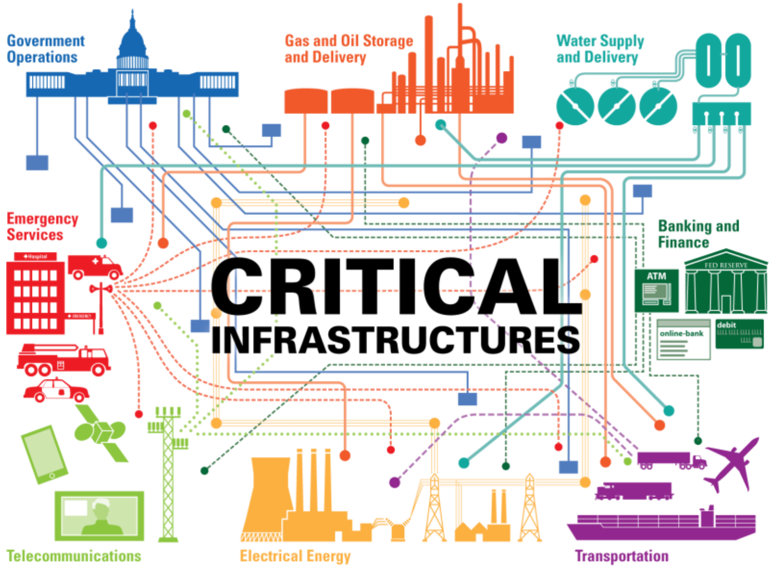
Content

1. Navigating critical infrastructure
2. Cybersecurity in critical infrastructure
3. Research method
4. Findings
5. Conclusions and recommendations

UNIVERSITY
OF
JOHANNESBURG

Navigating critical infrastructure

Critical infrastructure

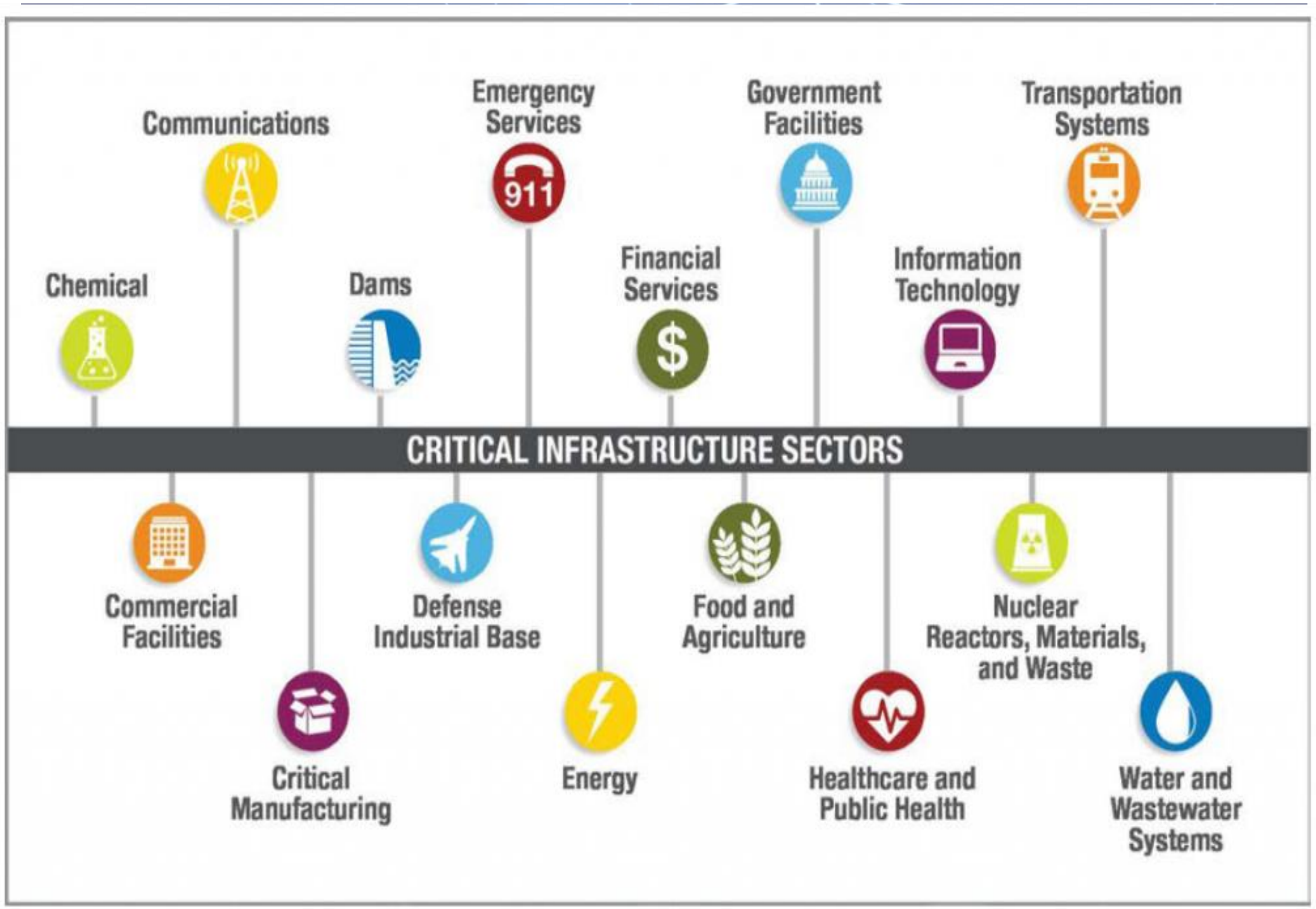


Assess mitigating measures towards cyber threats in safeguarding critical infrastructure

What are critical infrastructures?

Critical infrastructure refers to the essential systems, services, and assets that are vital for the functioning of a society, economy, and national security.

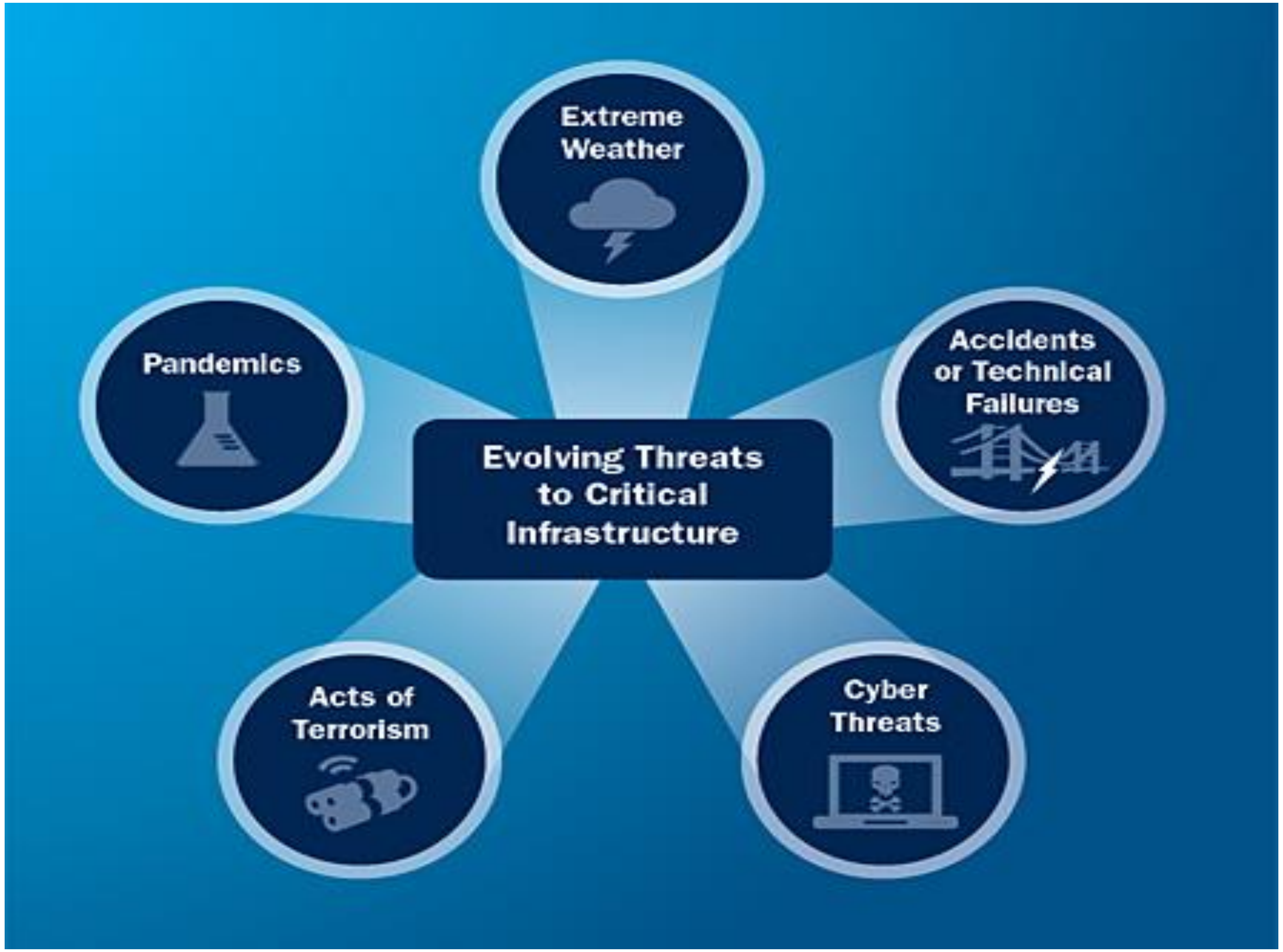
Critical infrastructure cuts across energy, transportation, water, communications, healthcare, financial services, emergency services, etc.



Threats to Critical Infrastructure

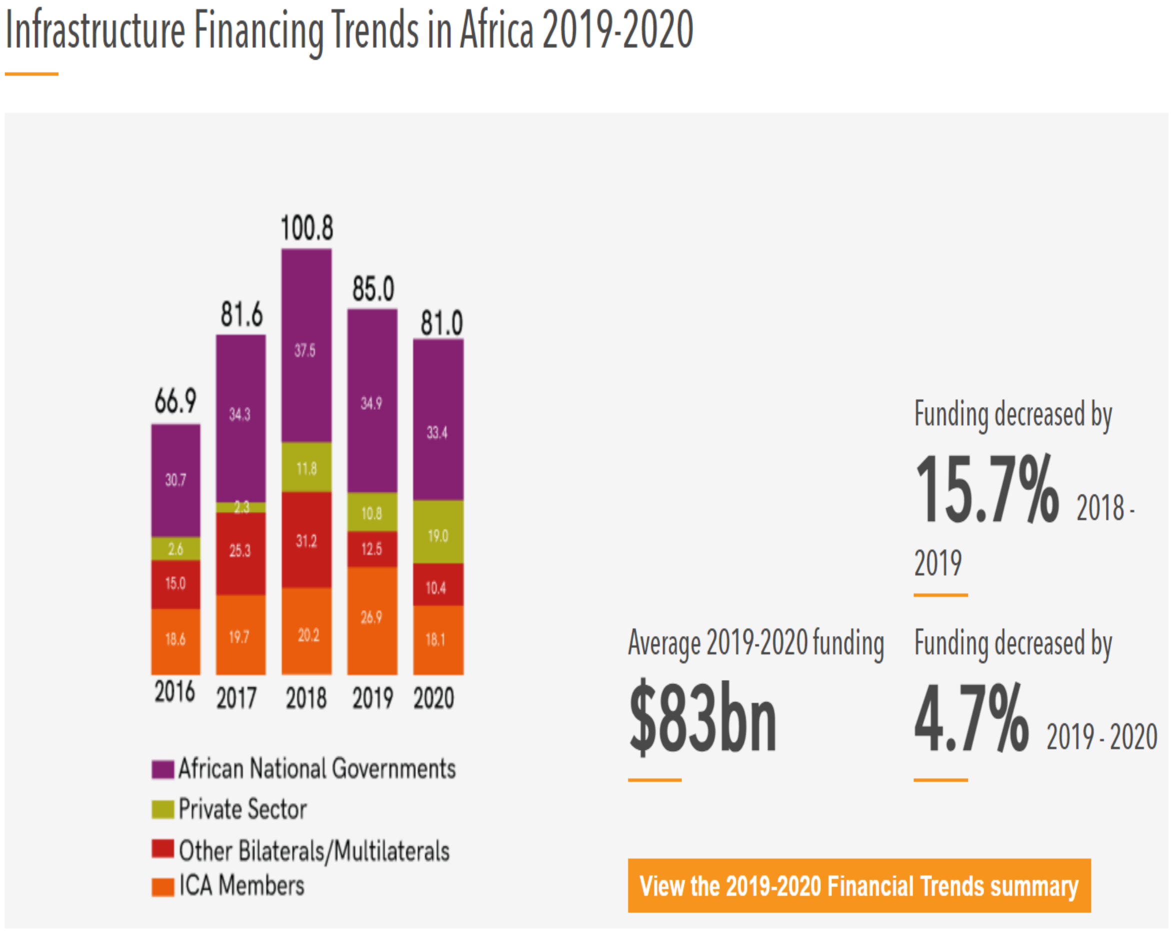
Digital reliance elevates utility vulnerability to cyber threats, as evidenced by Kaspersky's recent findings of the SystemBC variant targeting South Africa's critical infrastructure. Africa leads in industrial systems attacks, with 40.3% of ICS computers affected, notably in the energy sector.

IT-Online


Extreme Weather
Pandemics
Accidents or Technical Failures
Evolving Threats to Critical Infrastructure
Acts of Terrorism
Cyber Threats

Source: emilms.fema.gov and https://it-online.co.za/2023/10/09/threats-to-critical-infrastructure-on-the-rise/

Infrastructure Projection in Africa: From where?



Infrastructure Financing Trends in Africa 2019-2020

Funding decreased by

15.7% 2018 - 2019

Average 2019-2020 funding

$83bn

Funding decreased by

4.7% 2019 - 2020

View the 2019-2020 Financial Trends summary

"Government financing of critical infrastructure in Africa involves various methods, including cost-sharing grants, budgetary allocations, and the support of National Development Banks (NDBs).

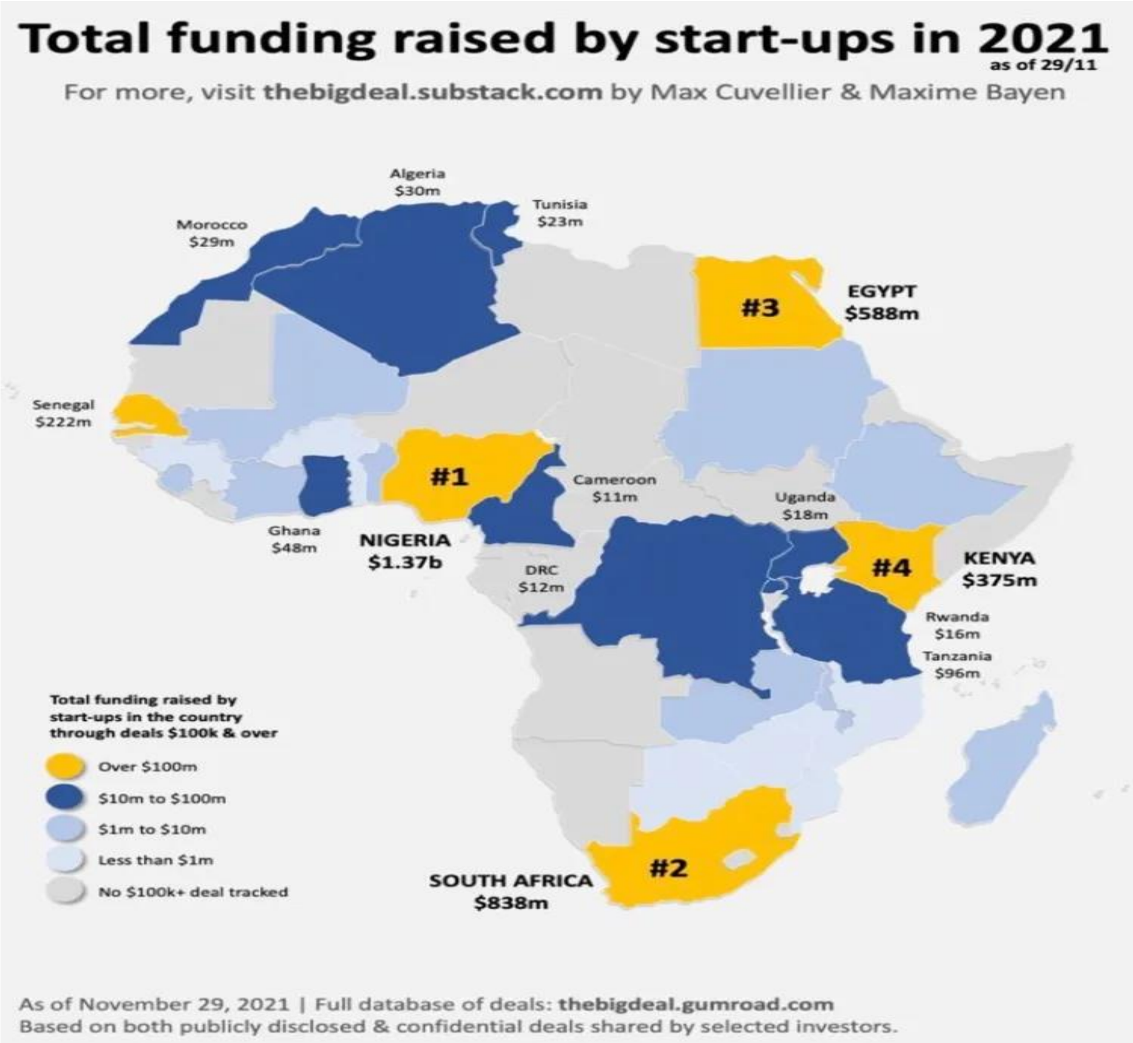
— Critical Infrastructure Programme (CIP)

"Economic diversification is essential for addressing Africa's challenges, particularly given its demographic structure. African governments must prioritise shifting towards labour-intensive growth paths and investing in youth entrepreneurial skills to transition to higher-productivity sectors."

—Akinwumi A. Adesina, President, African Development Bank Group

Sources: The Infrastructure Consortium for Africa (ICA) and South Africa Government at gov.za

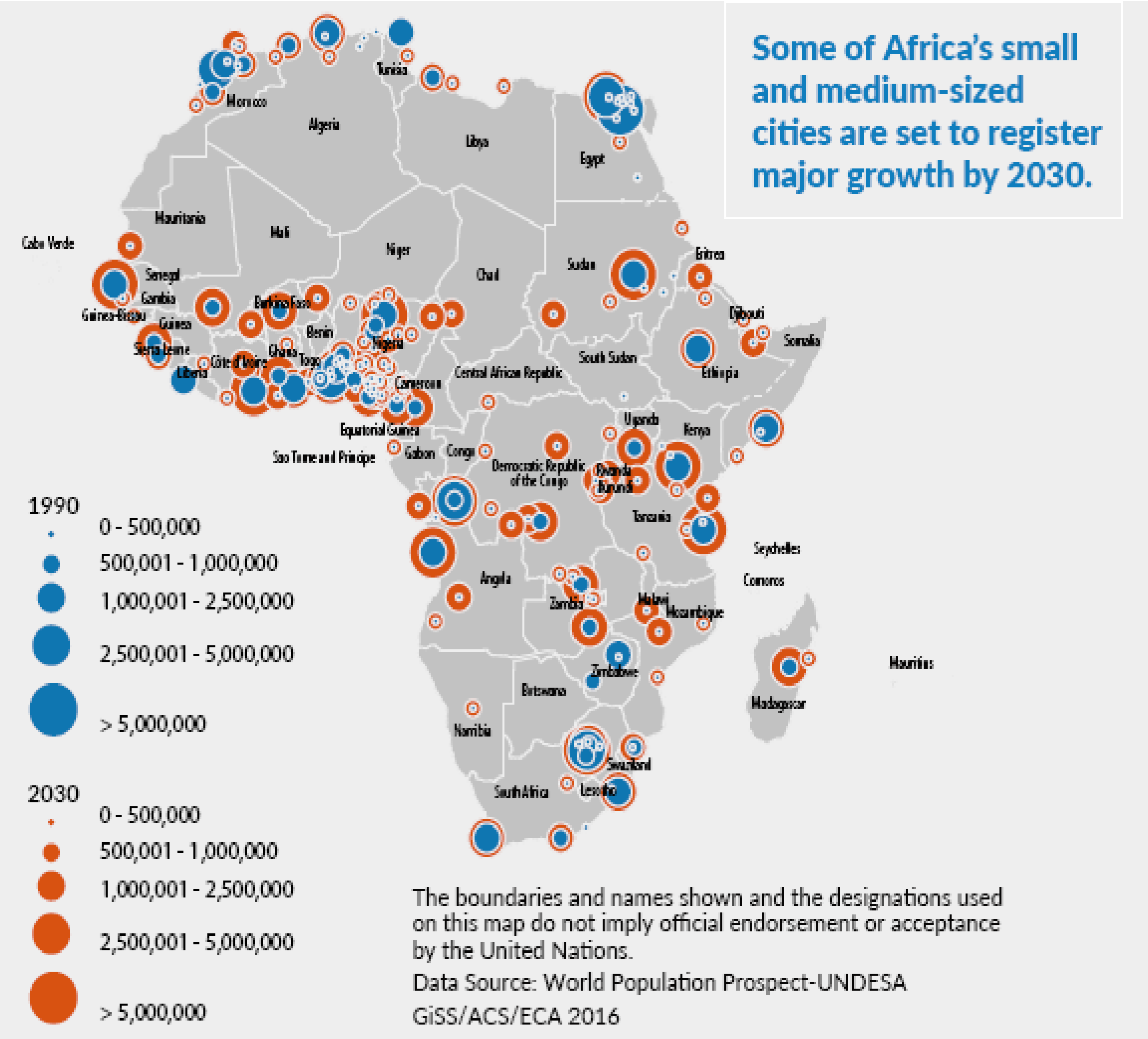
Infrastructure Projection in Africa: To where?



Total funding raised by start-ups in 2021
as of 29/11

For more, visit thebigdeal.substack.com by Max Cuvellier & Maxime Bayen

As of November 29, 2021 | Full database of deals: thebigdeal.gumroad.com
Based on both publicly disclosed & confidential deals shared by selected investors.



Some of Africa's small and medium-sized cities are set to register major growth by 2030.

The boundaries and names shown and the designations used on this map do not imply official endorsement or acceptance by the United Nations.

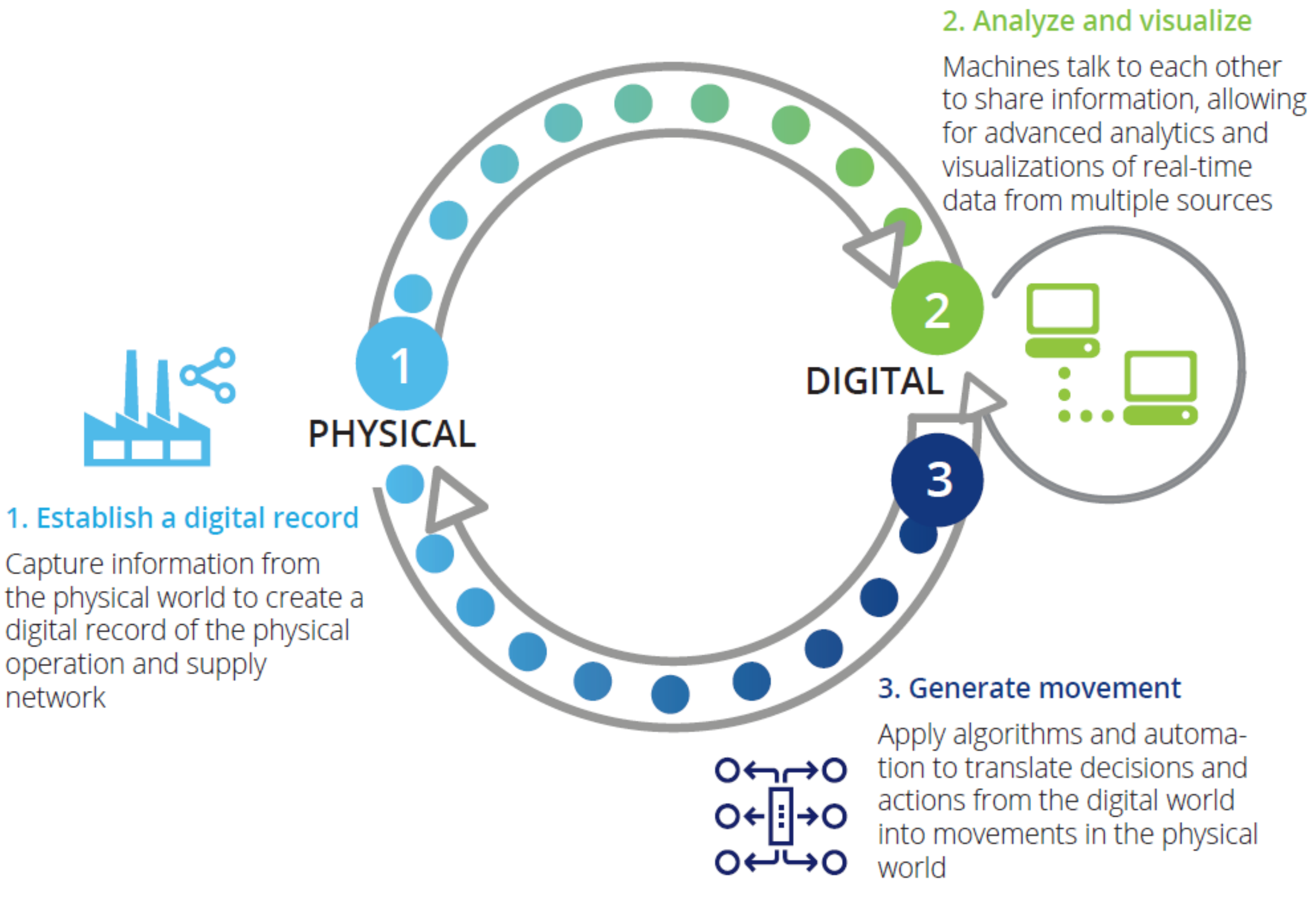
Data Source: World Population Prospect-UNDESA
GiSS/ACS/ECA 2016

Transformation and Integration of digital information

- **Shifting to real-time access to data and intelligence** will fundamentally transform how critical infrastructures are protected.

- **This shift is driven by the continuous and cyclical flow of information and actions** between physical and digital worlds called '**The Physical-to-Digital-to-Physical (PDP) loop.**'

Source: Forces of change: Industry 4.0
A Deloitte series on Industry 4.0



2. Analyze and visualize

Machines talk to each other to share information, allowing for advanced analytics and visualizations of real-time data from multiple sources

1. Establish a digital record

Capture information from the physical world to create a digital record of the physical operation and supply network

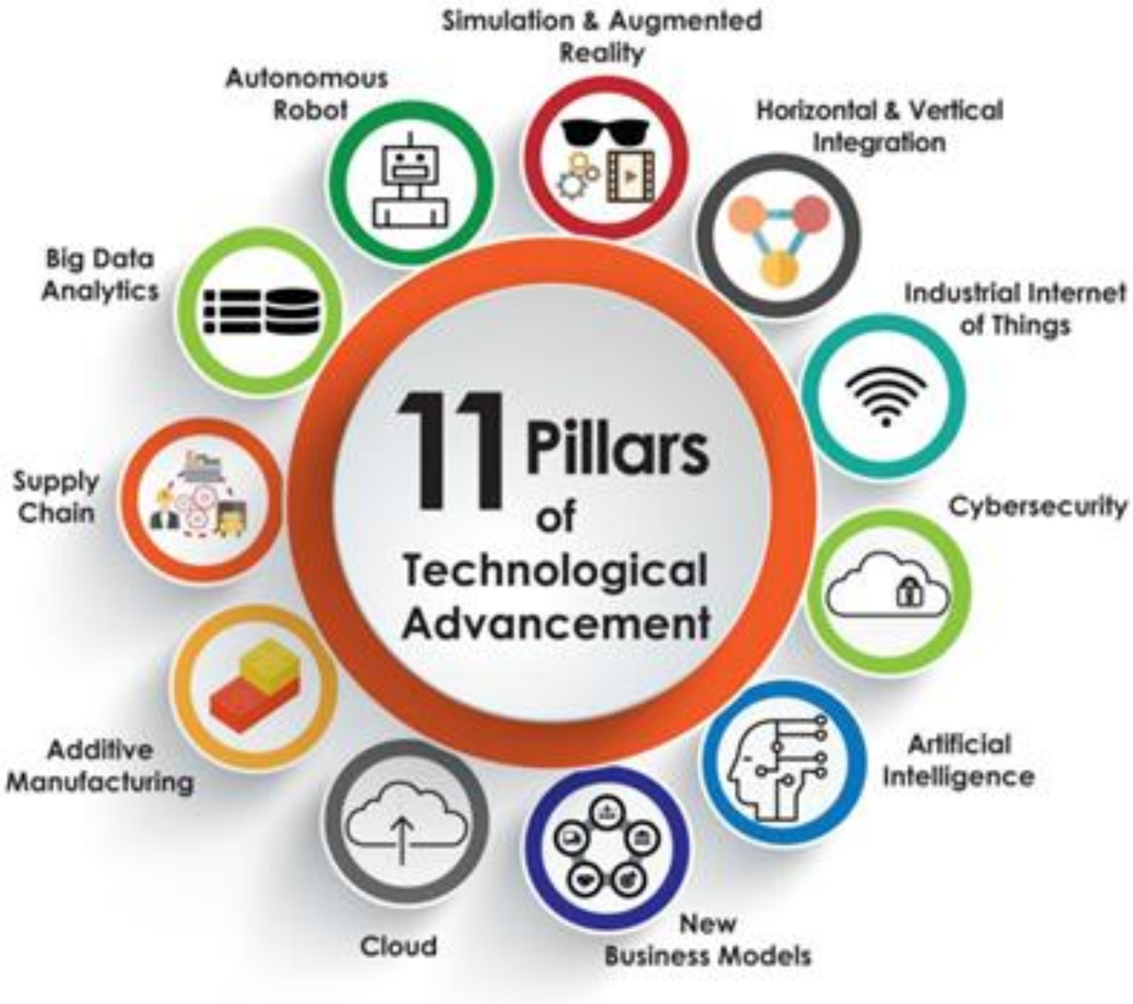
3. Generate movement

Apply algorithms and automation to translate decisions and actions from the digital world into movements in the physical world

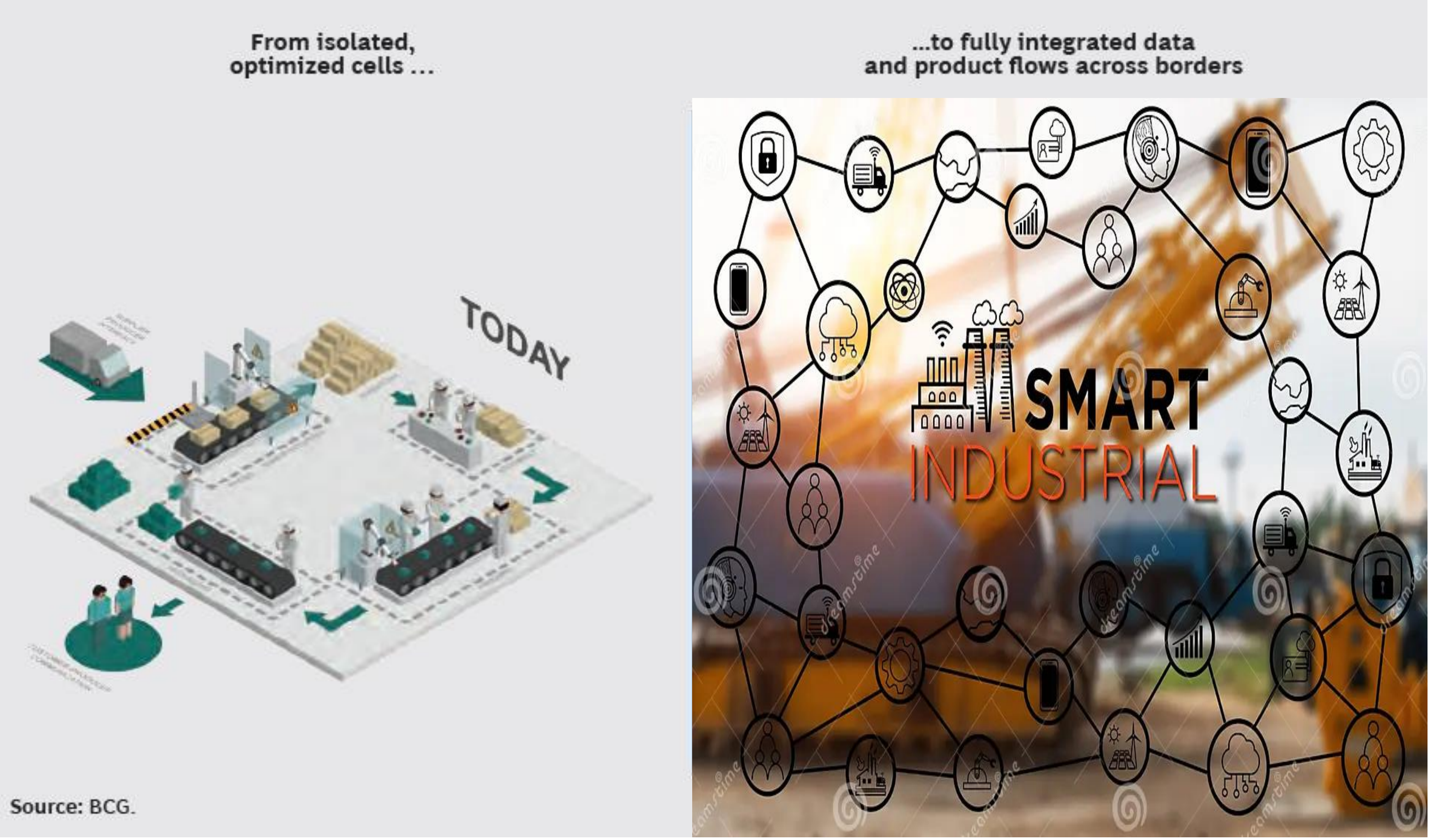
Source: Center for Integrated Research.

Deloitte Insights | deloitte.com/insights

The 11 Pillars of Technological Advancement of Industry 4.0


Simulation & Augmented Reality
Horizontal & Vertical Integration
Industrial Internet of Things
Cybersecurity
Artificial Intelligence
New Business Models
Cloud
Additive Manufacturing
Supply Chain
Big Data Analytics
Autonomous Robot
11 Pillars of Technological Advancement

Changing Traditional Infrastructure to Smart Industry


From isolated, optimized cells ...
...to fully integrated data and product flows across borders
TODAY
SMART
INDUSTRIAL

Source: BCG.

- *With a digital industry 4.0, the 11 pillars of technological advancement will transform production, as well as infrastructures needed for the projection ahead – from planning to conceptualisation, involving the government, individuals, bodies, consumers etc., goals can be achieved within the available resources and personnel.*

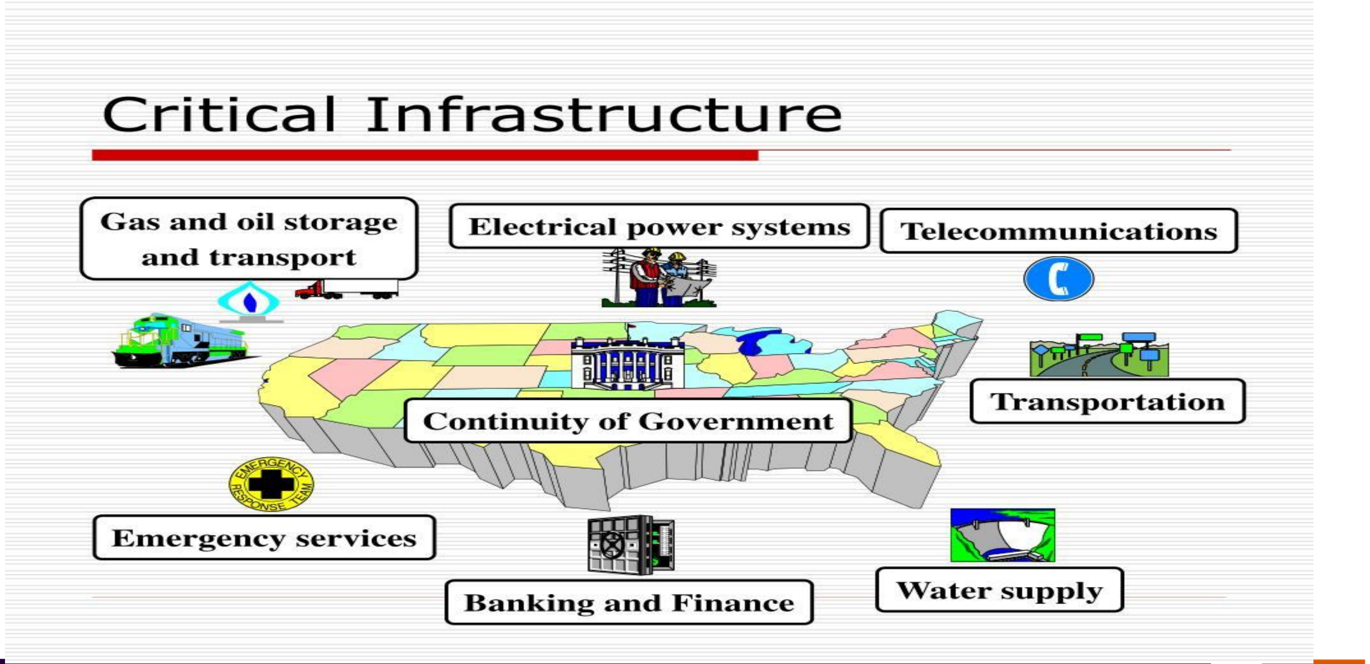
Cybersecurity in critical infrastructure

UNIVERSITY
OF
JOHANNESBURG

Cybersecurity and Critical Infrastructure

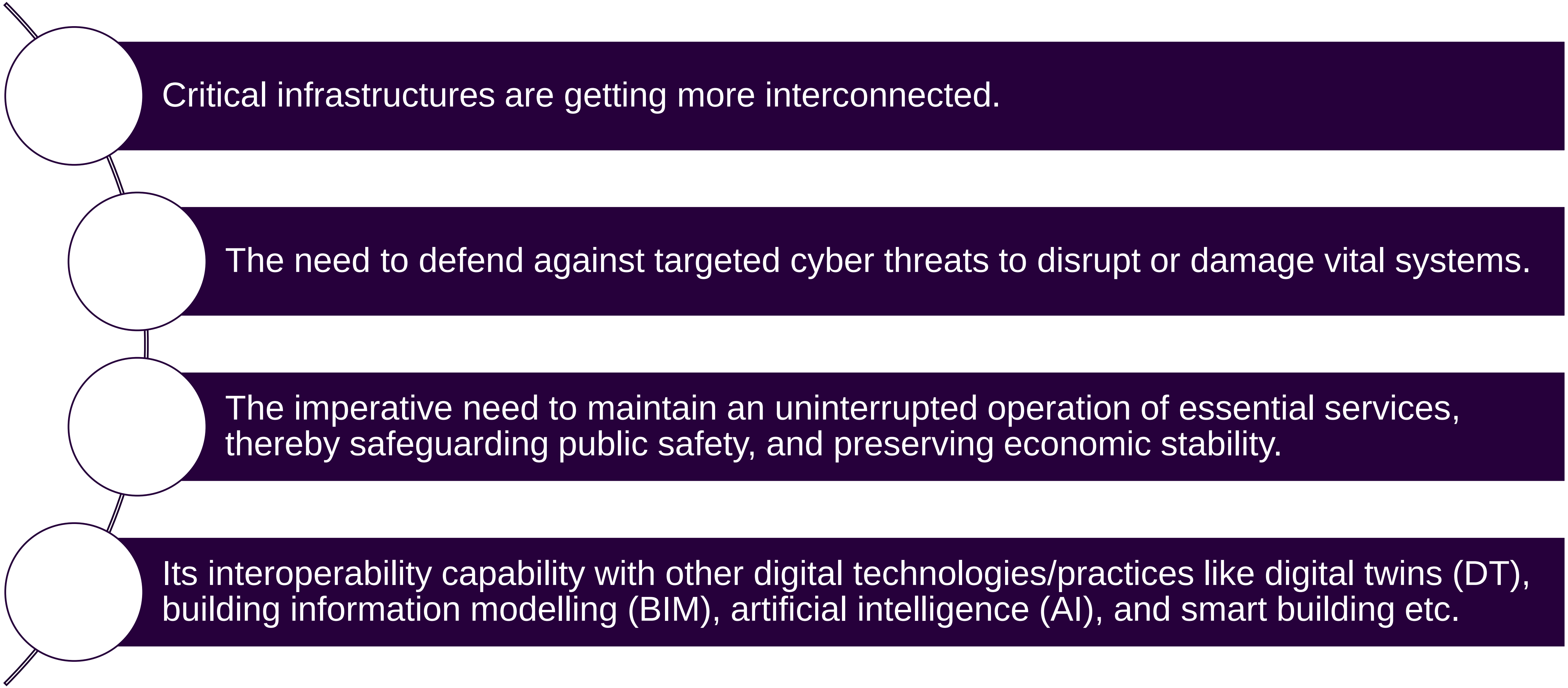
Cybersecurity in critical infrastructure is paramount due to the significant impact that cyberattacks can have on essential services and systems that society relies on.

With the interconnectivity in critical infrastructure, cybersecurity acts as a catalyst that combines the ‘why’, ‘need’, and ‘reason’ for implementing strategies (technology and practice) against vulnerabilities in the connected infrastructure system.



Why does cybersecurity matter in critical infrastructure?

Why Cybersecurity?



Critical infrastructures are getting more interconnected.

The need to defend against targeted cyber threats to disrupt or damage vital systems.

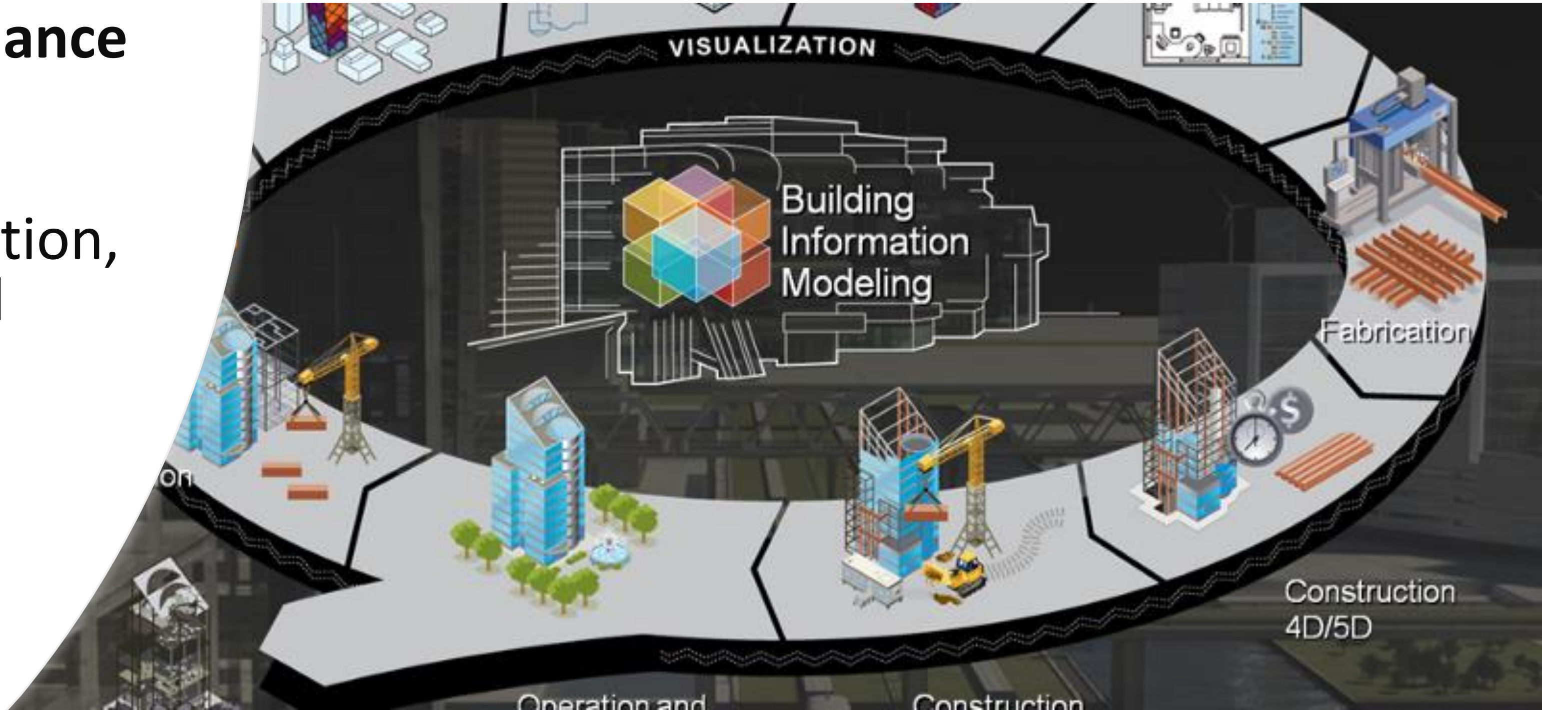
The imperative need to maintain an uninterrupted operation of essential services, thereby safeguarding public safety, and preserving economic stability.

Its interoperability capability with other digital technologies/practices like digital twins (DT), building information modelling (BIM), artificial intelligence (AI), and smart building etc.

Building Information Modelling (BIM)

- **Integrating Building Information Modeling (BIM) enhances critical infrastructure projects by streamlining design, construction, and maintenance processes.**

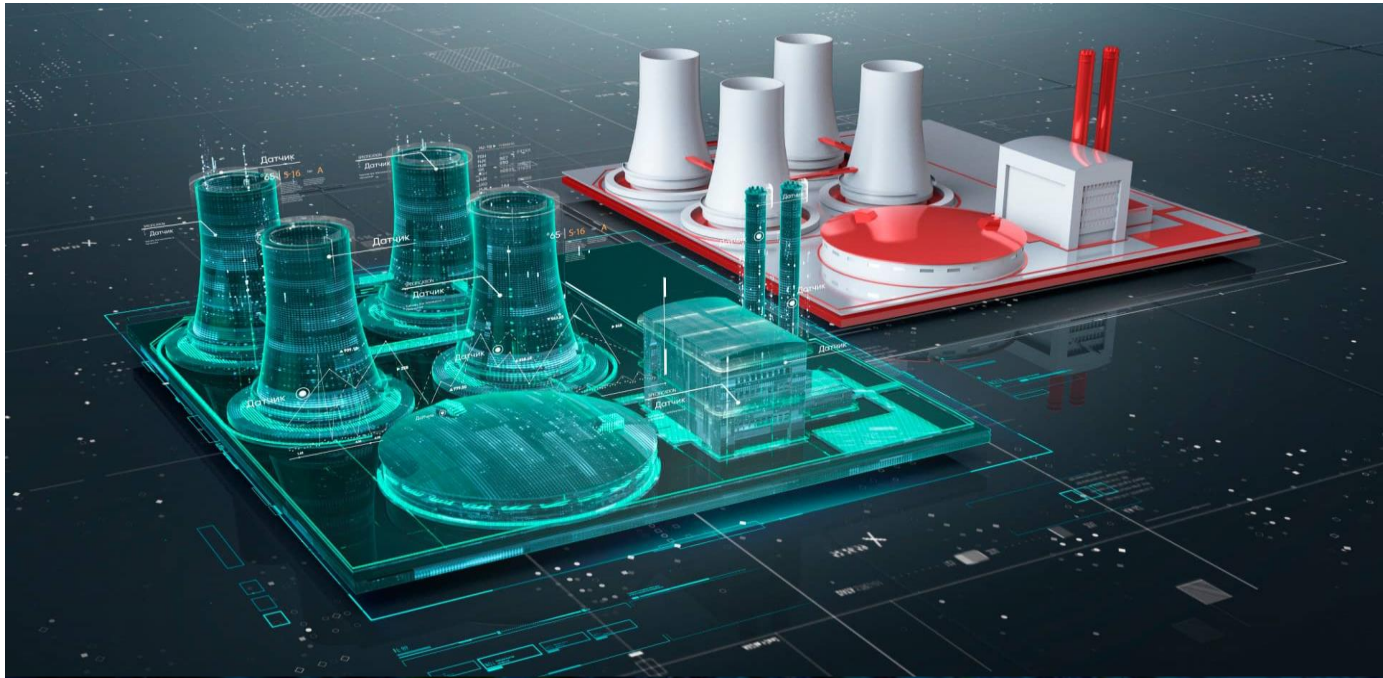
- It ensures efficient resource allocation, reduces risks, and improves overall project coordination for critical infrastructure developments

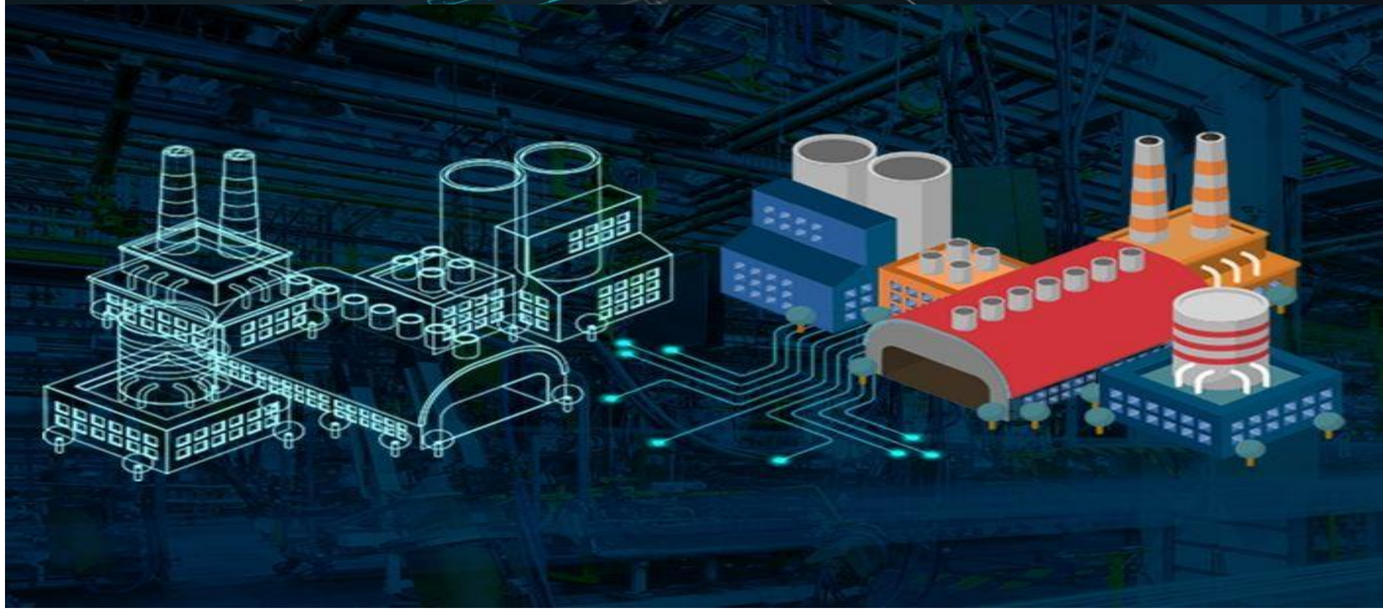


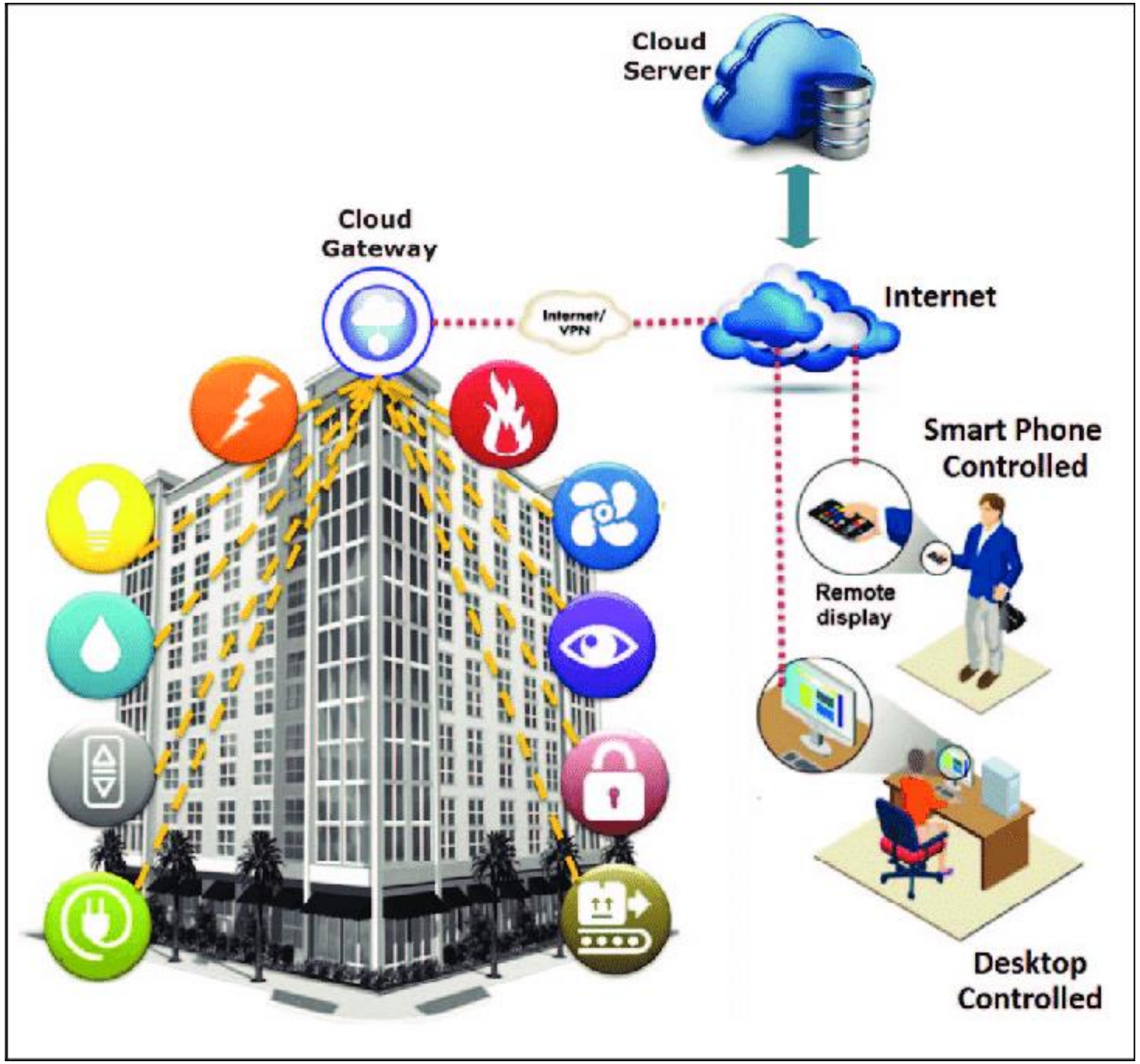
Digital Twins

- **Incorporating digital twins into critical infrastructure enhances real-time monitoring, predictive maintenance, and operational efficiency.**

- Digital twins enable stakeholders to simulate scenarios, optimise performance, and swiftly respond to disruptions, bolstering resilience in critical infrastructure systems.







Smart Building & Infrastructure

- Integration of IoT devices and sensors into buildings and infrastructure to create smart systems that can collect and analyze data in real-time.
- The role of IoT in smart building automation and control systems
- Integrating smart buildings into the smart city framework

Augmented / Virtual Reality

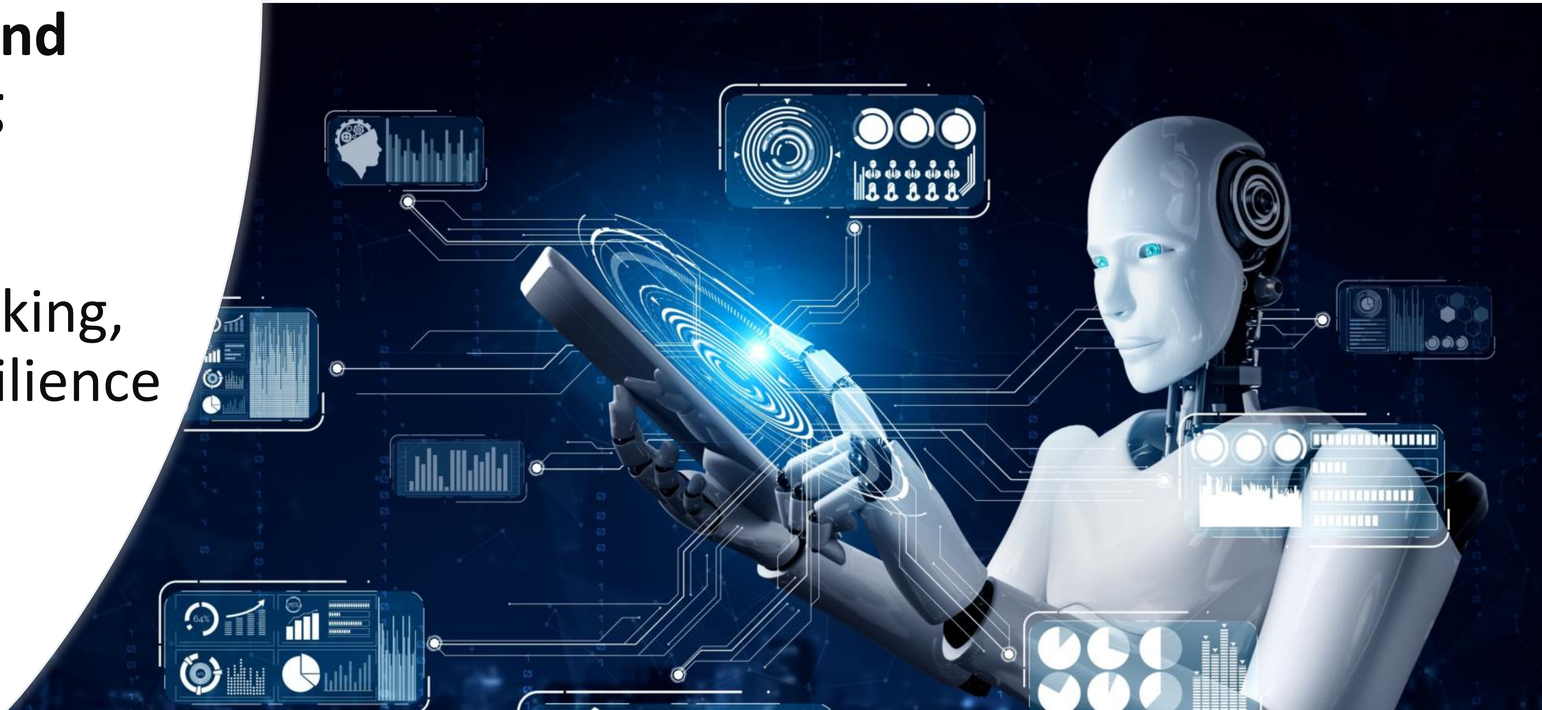
- **AR / VR technologies facilitate immersive training, remote inspections, and enhanced stakeholder collaboration.**

- In visualising complex infrastructure designs, detecting errors early, and improving decision-making processes, ultimately enhancing safety and efficiency.

Artificial Intelligence and Machine Learning

- **Leveraging AI and machine learning in critical infrastructure enables predictive maintenance, anomaly detection, and operations optimisation, enhancing reliability and reducing downtime.**

- Their roles in proactive decision-making, risk mitigation, and ensuring the resilience of critical infrastructure networks.



Cyber-physical system

- **In critical infrastructure, digital technologies are integrated with physical assets, enabling real-time monitoring, control, and automation for improved efficiency and responsiveness.**
- Enhancing resilience against cyber threats through robust security measures, ensuring critical infrastructure operations' integrity, availability, and reliability.

Research Method

UNIVERSITY
OF
JOHANNESBURG

Methods

Method

Quantitative (86 questionnaires retrieved)

Sampling

Random technique

Respondents

Architects, Builders, Engineers, Quantity surveyors, and Cybersecurity experts in Gauteng, South Africa

Tools

Mean item score (MIS), Standard deviation (SD), and Exploratory factor analysis (structure matrix)

Findings

UNIVERSITY
OF
JOHANNESBURG

DEMOGRAPHIC

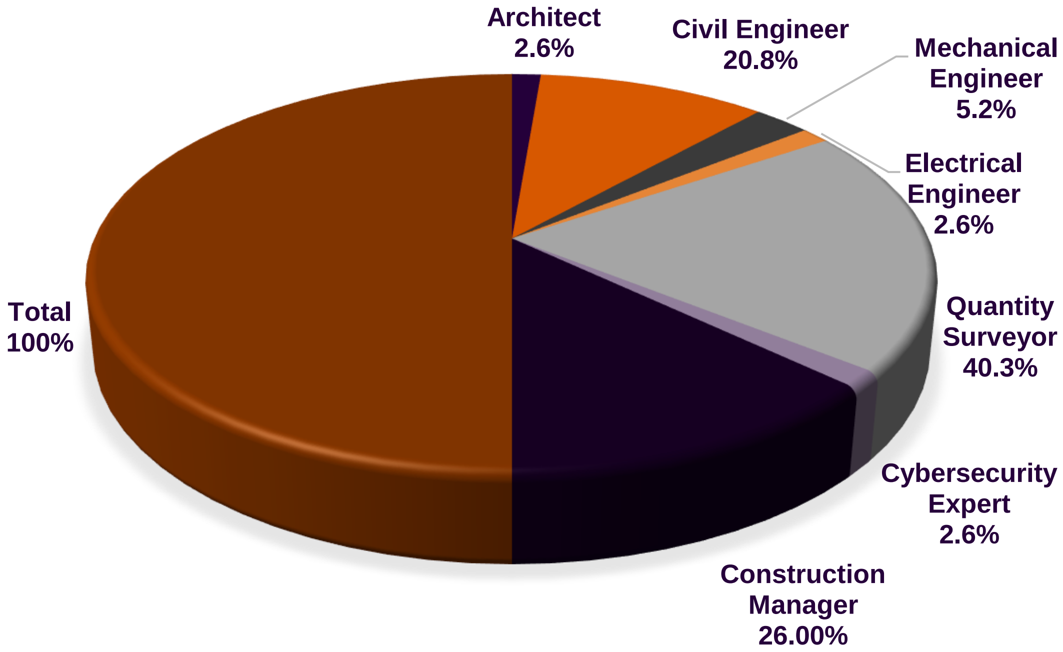


Figure 1: Respondents' professions

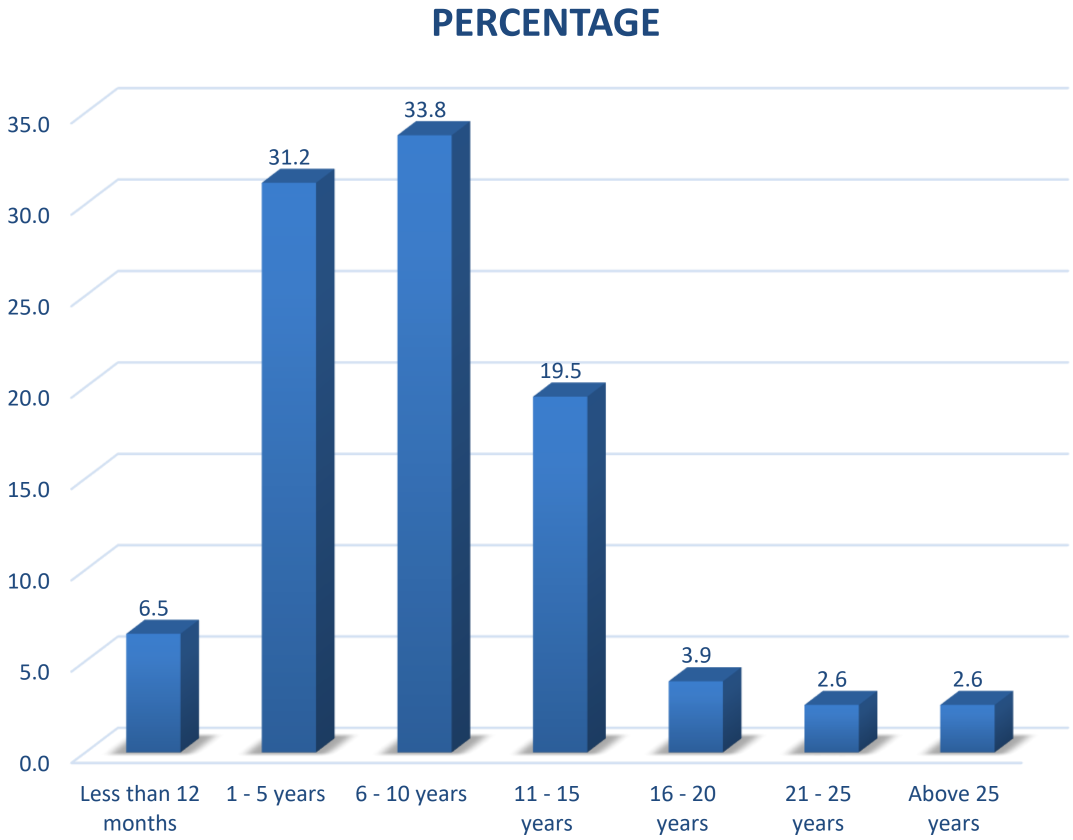


Figure 2: Respondents' years of experience

DEMOGRAPHIC

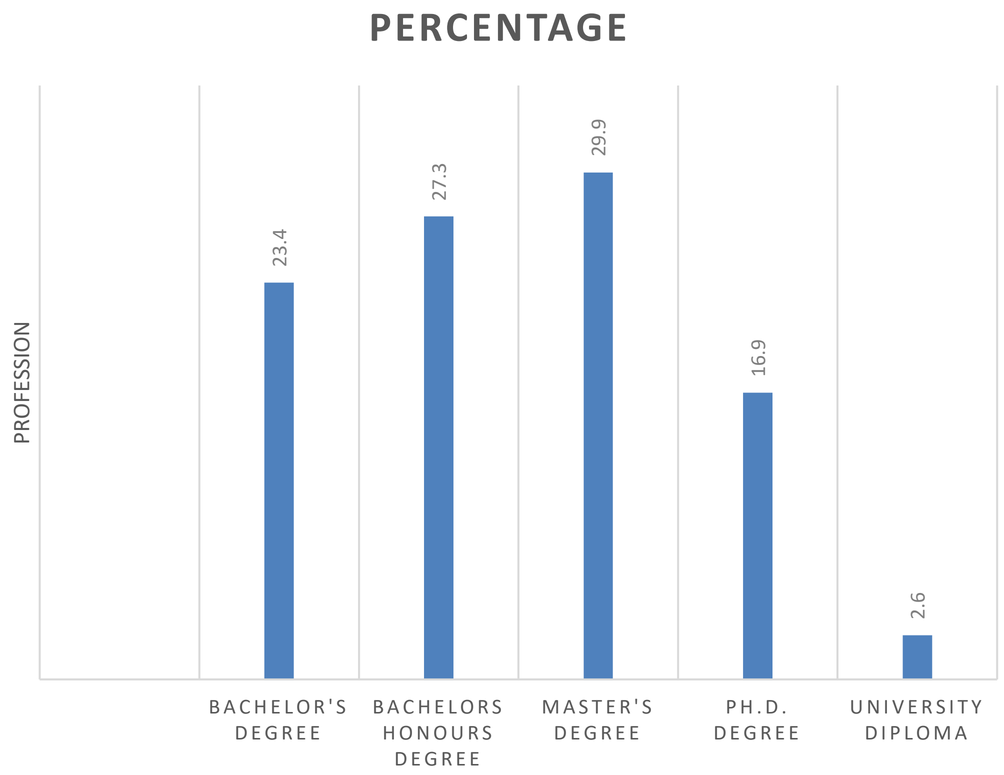
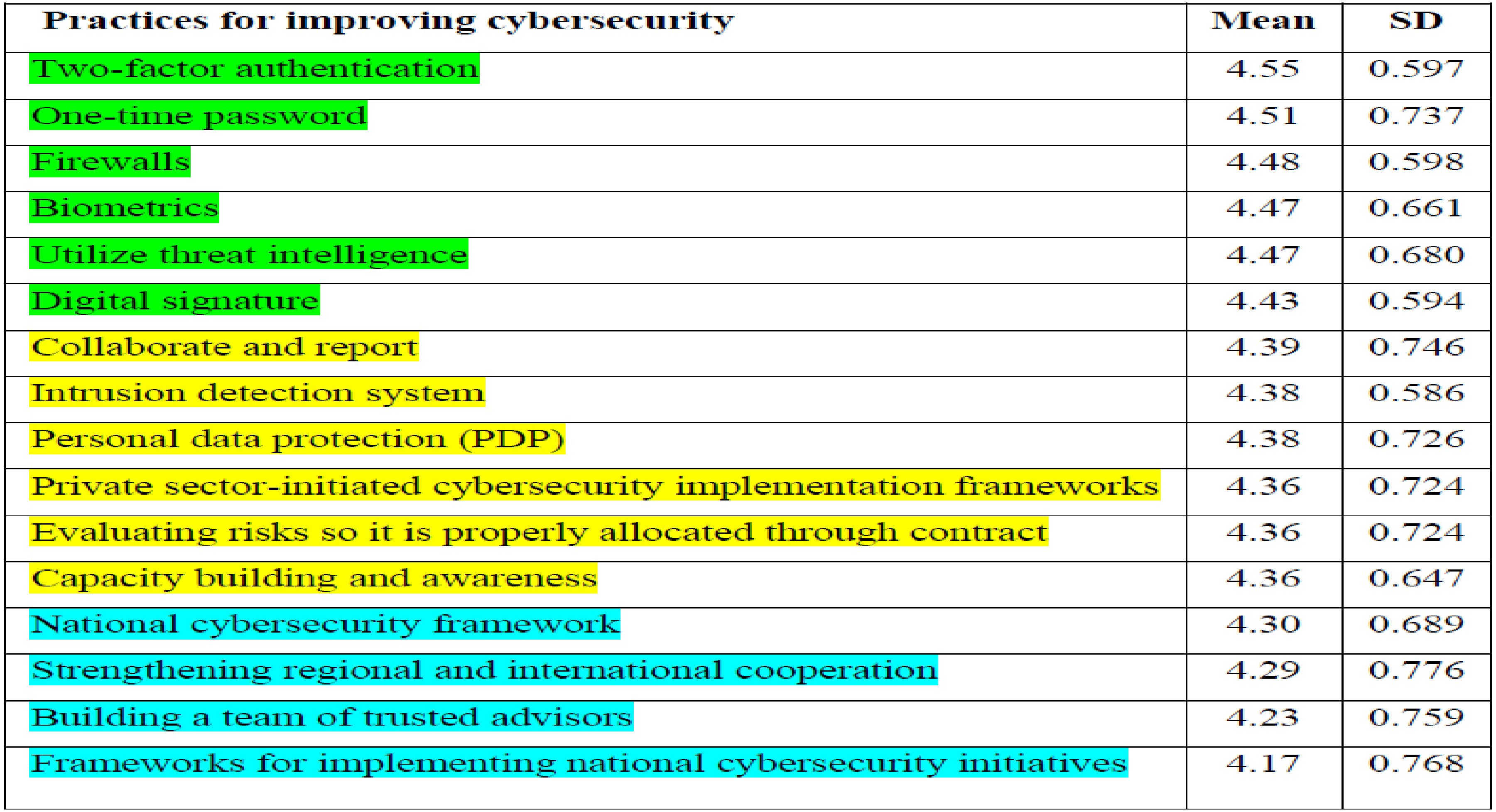


Figure 3: Respondents' qualifications

The respondents' demographic information shows that they possess adequate experience, handle many projects, and are distributed across professions; **there is confidence in their response**.

Cybersecurity measures for critical infrastructure



Practices for improving cybersecurity	Mean	SD
Two-factor authentication	4.55	0.597
One-time password	4.51	0.737
Firewalls	4.48	0.598
Biometrics	4.47	0.661
Utilize threat intelligence	4.47	0.680
Digital signature	4.43	0.594
Collaborate and report	4.39	0.746
Intrusion detection system	4.38	0.586
Personal data protection (PDP)	4.38	0.726
Private sector-initiated cybersecurity implementation frameworks	4.36	0.724
Evaluating risks so it is properly allocated through contract	4.36	0.724
Capacity building and awareness	4.36	0.647
National cybersecurity framework	4.30	0.689
Strengthening regional and international cooperation	4.29	0.776
Building a team of trusted advisors	4.23	0.759
Frameworks for implementing national cybersecurity initiatives	4.17	0.768

Table 1: Respondents' professions

🟩 Dominant 🟨 Average dominance 🟦 Less dominant

The measures outlined contribute to protecting critical infrastructure by establishing robust security layers and protocols.

They mitigate cyber threats through advanced authentication methods like two-factor authentication and biometrics while implementing proactive measures such as intrusion detection systems and threat intelligence utilisation.

Collaborative efforts and adherence to national cybersecurity frameworks and private sector standards bolster resilience and ensure a cohesive approach to safeguarding critical infrastructure from cyber-attacks.

Cluster 1

National Cybersecurity Framework

National cybersecurity frameworks such as National Cybersecurity Policy Framework (NCPF) and NIST Cybersecurity Framework (CSF) 2.0 provide standardised guidelines to enhance critical infrastructure resilience against cyber threats through comprehensive risk management and regulatory compliance.

Cluster 2

Technological Security Measures:

Technological security measures safeguard critical infrastructure by deploying advanced systems and protocols to detect, prevent, and mitigate cyber threats, ensuring operational continuity and resilience.

Cluster 3

Risk Management and Preparedness:

Risk management and preparedness strategies bolster critical infrastructure resilience by identifying potential threats, implementing mitigation measures, ensuring swift response protocols, minimizing disruptions and safeguarding vital services.

Cluster 4

Organisational and Cultural Practices:

This foster a security-conscious environment within critical infrastructure sectors, promoting awareness, adherence to protocols, and a proactive approach to mitigating risks, thereby fortifying defenses against cyber threats and ensuring operational continuity.

Cluster 5

Privacy and Regulatory Compliance:

Privacy and regulatory compliance measures ensure that critical infrastructure entities adhere to legal requirements, safeguarding sensitive data and mitigating potential vulnerabilities, enhancing overall security and resilience against cyber threats.

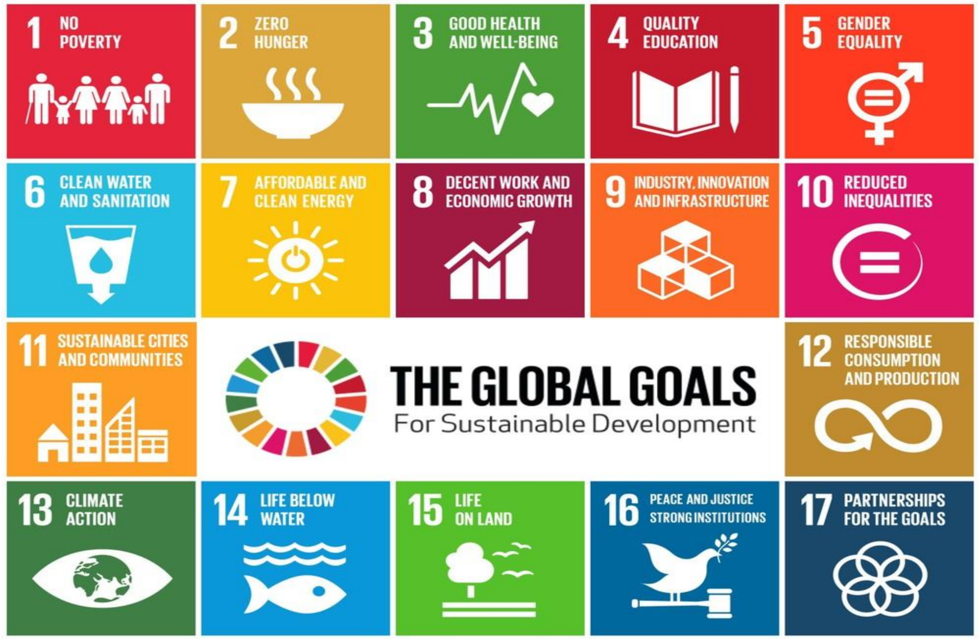
CLUSTER SUMMARY

Conclusions and Recommendations

UNIVERSITY
OF
JOHANNESBURG

Conclusions

- **Need for further studies -** Critical infrastructure forms the backbone of modern society, supporting essential services and economic activities, driving the 17 sustainable development goals (SDG).
- **Understanding digital vulnerability-** There is an increased reliance on digital technologies, which also heightens the vulnerability of these systems to cyber threats.
- **Cybersecurity priority -** Prioritising cybersecurity measures is paramount to safeguarding critical infrastructure, ensuring its resilience, and mitigating potential disruptions to society and national security.


1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
THE GLOBAL GOALS
For Sustainable Development
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
16 PEACE AND JUSTICE STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS

Recommendations

- **Invest in resilience:** Allocate resources towards building resilient infrastructure that can withstand and recover from cyber incidents, ensuring the continuity of essential services and safeguarding national security.

- **Implement continuous monitoring:** Establish mechanisms for continuous monitoring and threat intelligence gathering to detect and mitigate real-time cybersecurity risks, enhancing critical infrastructure systems' proactive defence posture.

- **Implement Continuous Monitoring:** Establish mechanisms for continuous monitoring and threat intelligence gathering to detect and mitigate real-time cybersecurity risks, enhancing critical infrastructure systems' proactive defence posture.

African Leadership Magazine
...Innovation, Entrepreneurship and Development

“Those who fear the sun will not become chief”

African Proverb

http://africanleadership.co.uk

If love is a sickness, patience is the remedy.

- African Proverb

For
Listening

Any questions?

Seyi Stephen, PhD candidate
Construction Management, University of Johannesburg
Email: seyistephen.ss@gmail.com