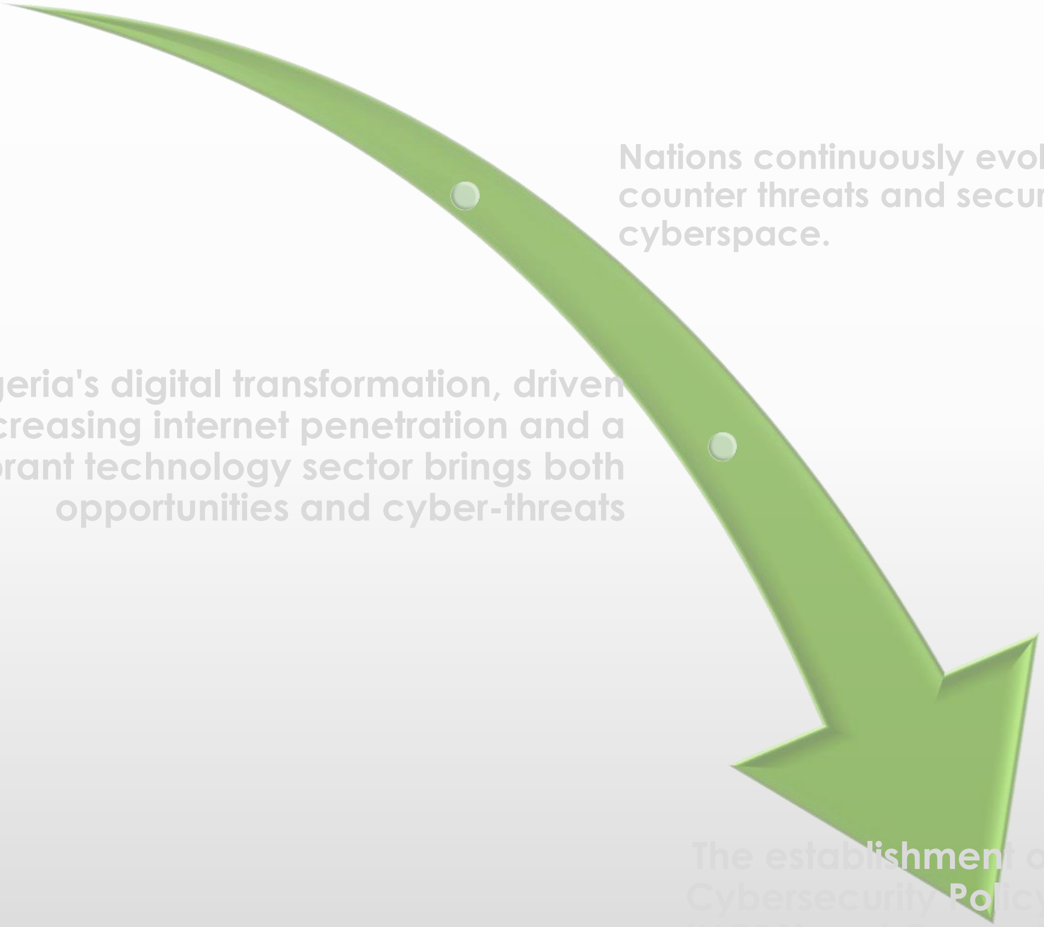
# EMERGING CYBERTHREATS AND COUNTER STRATEGIES IN NIGERIA

BY

Dr PETER AFUNANYA, fsi, mnipr

# INTRODUCTION



The surge in cyber threats due to technological advancements and increased digital activities makes cybersecurity essential for everyone.

Nations continuously evolve strategies to counter threats and secure their cyberspace.

Nigeria's digital transformation, driven by increasing internet penetration and a vibrant technology sector brings both opportunities and cyber-threats

The establishment of the National Cybersecurity Policy and Strategy (NCPS) and Computer Emergency Response Team (CERT) underscores Nigeria's commitment to respond to cyber incidents effectively

# AIM

This paper will examine strategies for countering threats in Nigeria’s Cyber landscape.

# SCOPE

To achieve this aim, the paper will cover the following:

✓ Conceptual Clarifications
- Cyberspace
- Cyberthreats
- Cybersecurity
- Strategies

✓ Overview of the Nigeria's Cyber Space

✓ Understanding Emerging Threats in Nigeria's Cyber Domain

✓ Impact of Cyber threats on National Security

✓ Efforts of Government in Cyber Security in Nigeria

✓ Role of DSS in curtailing the Menace of Cyber threats

✓ Challenges in Addressing Cyber Attacks

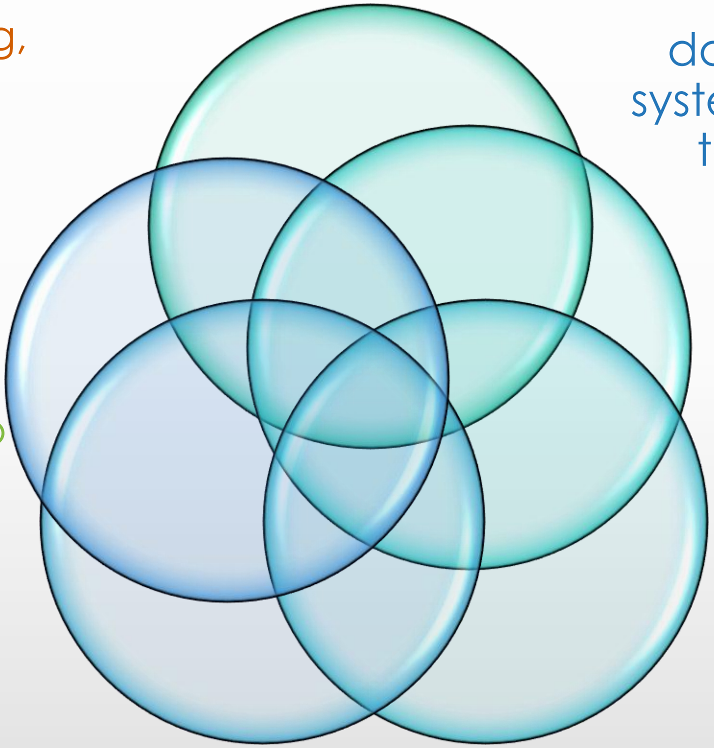
✓ Conclusion

✓ Recommendations

# CONCEPTUAL CLARIFICATIONS

**Cyberspace** is a borderless domain where interconnected computers enable information processing, manipulation, and interaction globally (Choucri, 2013)

‘John (2016) defines **cyber-threats** as malicious actions aimed at disrupting or damaging computer systems in critical sectors to access sensitive information.



**Cybersecurity** aims to reduce malicious attacks on software, computers, and networks through tools like intrusion detection, virus prevention, and encryption (Amoroso, 2006).

Mintzberg (1994) indicated that **strategy** is a plan, a pattern, a position, a perspective, a ploy, a maneuver intended to outwit a competitor.

# OVERVIEW OF THE NIGERIAN CYBERSPACE

Nigeria boasts a rapidly growing digital landscape characterized by the following:

i. Increasing Internet Penetration (With over 100 million internet users Nigeria represents one of Africa's largest internet markets)

ii. Evolving Infrastructure (Limited fixed broadband access and reliance on mobile data networks create vulnerabilities)

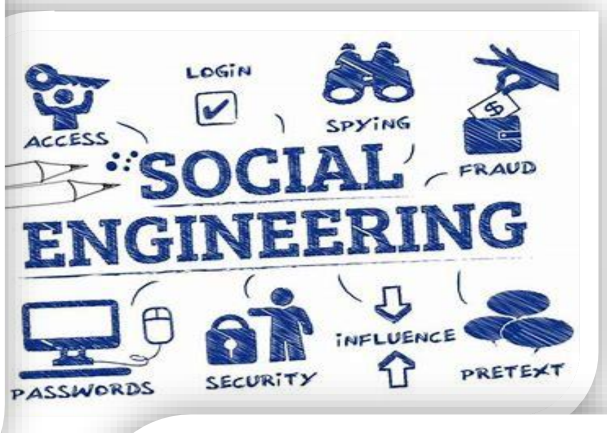
iii. Thriving Fintech Sector (widespread adoption of mobile money platforms and online banking services)

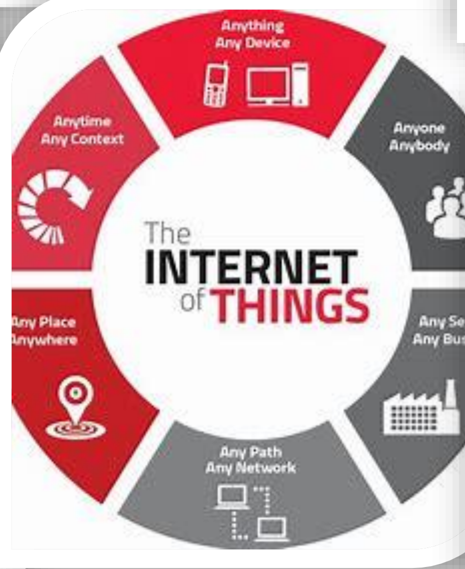
iv. Active Social Media Presence (Social media platforms like Facebook, WhatsApp, and Twitter are widely used for communication etc)

v. E-Government Initiatives (strides towards e-governance by implementing online services for citizens and businesses)

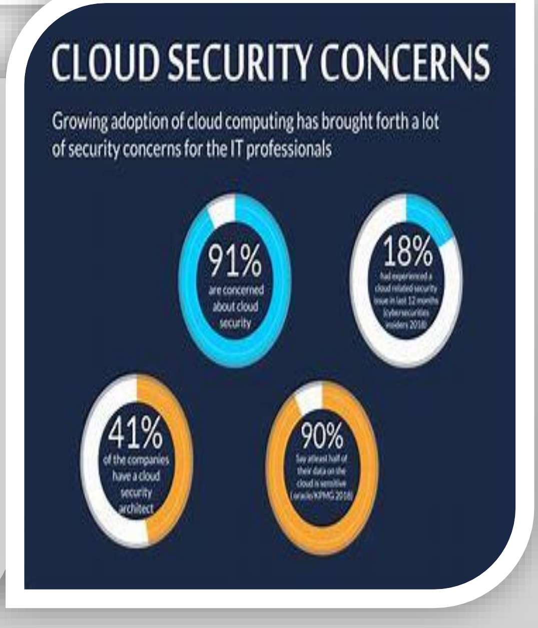
# UNDERSTANDING EMERGING THREATS IN NIGERIA'S CYBER DOMAIN

Nigeria's evolving digital landscape presents fertile ground for a diverse range of cyber threats such as:





COMMON IoT DEVICE VULNERABILITIES
TO WATCH OUT FOR
Insecure components
Unnecessary open ports
Insufficient logging mechanisms



# UNDERSTANDING EMERGING THREATS IN NIGERIA'S CYBER DOMAIN ...

Other identified emerging threats include:

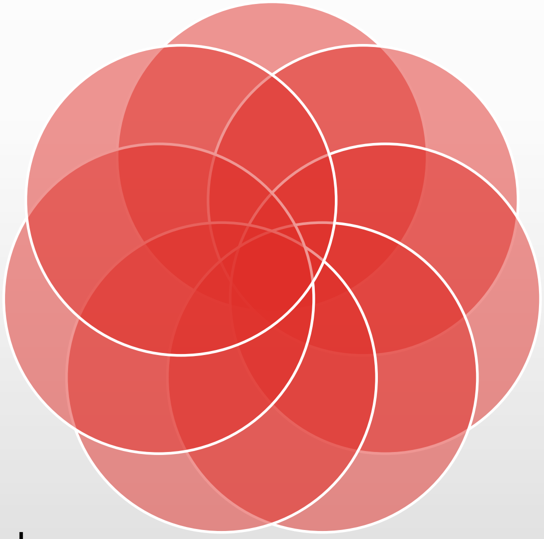
Trolling and Harassment Campaigns

Amplification through Algorithms

Exploitation of Weak Cybersecurity Practices

# IMPACT OF CYBER-THREATS ON NATIONAL SECURITY

The interconnected nature of cyberspace means that cyber-threats can have a ripple effect, impacting not just national security but also economic prosperity, social stability and international relations. Impact include:



Data Breaches and Espionage

Economic impact:

Political instability

Erosion of Public Trust

Social division and conflict

Undermining public health and safety

Damage to reputations and careers

International Relations

Disruption of Critical Infrastructure

# EFFORTS OF GOVERNMENT IN CYBER SECURITY IN NIGERIA

Legal frameworks and some agencies were created by government to secure Nigeria’s cyberspace. These include:

i. Establishment of the Nigerian Computer Emergency Response Team (ngCERT) which functions as the national focal point for cyber security incidents

ii. National Information Technology Development Agency (NITDA): is the primary agency responsible for developing Nigeria's IT sector and implementing cybersecurity policies.

iii. Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024 is a legal framework for addressing cybercrime;

iv. Advanced Fee Fraud And Other Related Offences Act punishes certain offences pertaining to Advance Fee Fraud;

# EFFORTS OF GOVERNMENT IN CYBER SECURITY IN NIGERIA…

v. **The Economic And Financial Crime Commission (amended) Act 2004:** investigates all financial crimes, including advance fee fraud, money laundering, counterfeiting, illegal charge transfers etc

**vi. Sectoral Computer Security Incident Response Teams (CSIRTs):** These are specialized teams established by critical sectors like banking, telecommunications, and government to handle cyber incidents specific to their industries.

**vii. Collaboration with International Partners:** Nigeria actively collaborates with international organizations and other countries on cybersecurity issues. This includes information sharing, capacity building, and joint efforts to combat cybercrime.

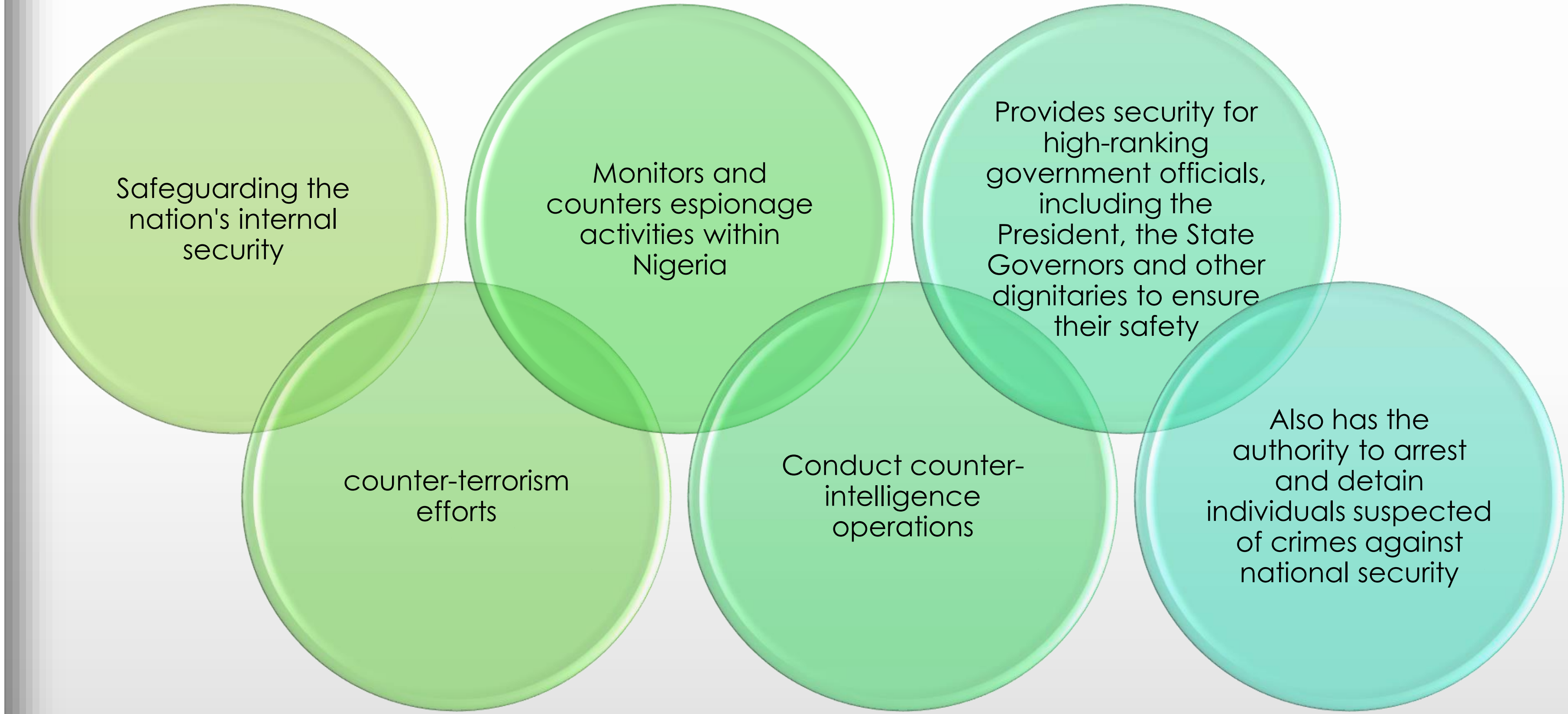
# ROLE OF DSS IN CURTAILING THE MENACE OF CYBER-THREATS

The Department of State Services is constitutionally charged with the primary responsibility of maintaining the internal security of Nigeria. Pursuant to section 2(3) of the National Security Agencies (NSA) Act Cap. 74 LFN, 2004 and Instrument SSS No. 1 of 1999, made pursuant to the same NSA Act, the primary responsibilities of the Service include:

STATE SECURITY SERVICE

LOYALTY • VIGILANCE • VERITY

# ROLE OF DSS IN CURTAILING THE MENACE OF CYBER-THREATS…



- Safeguarding the nation's internal security
- counter-terrorism efforts
- Monitors and counters espionage activities within Nigeria
- Conduct counter-intelligence operations
- Provides security for high-ranking government officials, including the President, the State Governors and other dignitaries to ensure their safety
- Also has the authority to arrest and detain individuals suspected of crimes against national security

STATE SECURITY SERVICE

LOYALTY • VIGILANCE • VERITY

# ROLE OF DSS IN CURTAILING THE MENACE OF CYBER-THREATS

The DSS has undertaken several key initiatives to address and mitigate the growing threat of cybercrime.

i. **Threat Intelligence**. The Service monitors cybercriminal activities, identify emerging trends and assess potential risks to national security. By staying ahead of the curve, the DSS provide timely and actionable intelligence to the government on necessary preventive measures

ii. **Investigations**. The DSS investigates cybercrimes, including hacking activities, online fraud and cyber espionage. It gathers evidence, identify perpetrators and work towards bringing them to justice. This investigative role deters cybercriminals and disrupts their operations.

iii. **Collaboration**. The DSS collaborates with other government agencies, law enforcement bodies and international partners on cybercrime issues. This collaboration allows for information sharing, coordinated responses to cyberattacks and joint efforts to dismantle cybercriminal networks.

STATE SECURITY SERVICE

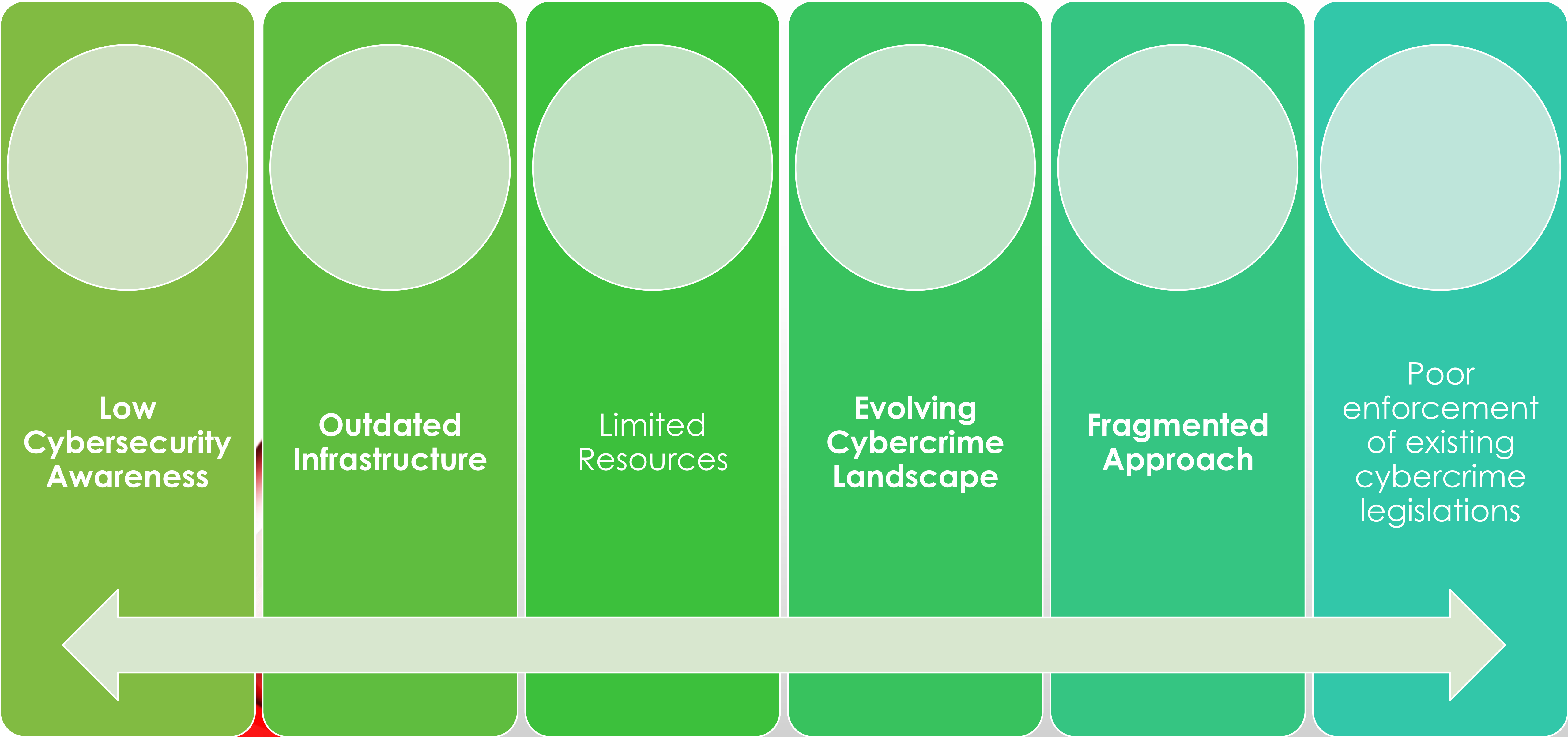
LOYALTY • VIGILANCE • VERITY

# ROLE OF DSS IN CURTAILING THE MENACE OF CYBER-THREATS

vi. **Establishment of a Cybersecurity Department.** To bolster its efforts in combating cybercrime, the DSS has established a dedicated Cybersecurity Department. This specialized unit focuses on developing and implementing comprehensive cybersecurity strategies, policies and initiatives.

vii. **Acquisition of Modern Facilities to Track Criminal Activities in Cyberspace**. The DSS has invested in acquiring state-of-the-art facilities and technologies to track and combat criminal activities in cyberspace. These advanced tools and systems enable the DSS to conduct sophisticated cyber surveillance, track digital footprints and analyse cyber incidents with high precision. Modern facilities empowers the DSS to effectively trace and disrupt cybercriminal operations.

# CHALLENGES IN ADDRESSING CYBER ATTACKS



**Low Cybersecurity Awareness**

**Outdated Infrastructure**

Limited Resources

**Evolving Cybercrime Landscape**

**Fragmented Approach**

Poor enforcement of existing cybercrime legislations

# CONCLUSION

# RECOMMENDATIONS

1. NITDA should partner with universities and private partners, to create specialized training and certification courses to address the shortage of skilled cybersecurity professionals

2. The NCC and Ministry of Communications and Digital Economy to sustain public awareness of citizens and businesses on online safety and common cyber threats through nationwide campaigns.

3. The Ministry of Communications and Digital Economy and NITDA should upgrade outdated IT systems and enforce strong security protocols.

# RECOMMENDATIONS

4. Security agencies should collaborate to establish Cybersecurity Threat Intelligence Center for continuous monitoring and intelligence sharing to counter evolving cyber threats.

5. National Assembly to strengthen legislations to enhance law enforcement capabilities and ensure effective prosecution of cybercrime cases.

# THANK YOU