Cybersecurity:
The Imperative for Regulation and Compliance

U. MBANASO

PhD Communications and Information Security

Agenda

- Background
- Threat Landscape and Perceptions
- Cybersecurity and Regulation
- Cybersecurity and Critical National Infrastructure
- Understanding Regulatory Compliance
- Strategy for Regulation and Compliance
- Conclusion

Background

- The Internet has a created new Virtual world.
- A virtual World that has dismantled national boundaries and controls.
- A virtual world now popularly known as Cyberspace
  - —a global domain within the information environment consisting of the interdependent network of information technology infrastructures.
- Cyberspace has become an important and strategic environment.
- It is ubiquitous, borderless, global and ambient.

Background

- The Internet has changed our way of life and will continue to do so.
- Increasing dependence on ICTs, impacts on individuals, organisations and governments.
- It is a defining feature of a modern, interconnected and knowledge-based society and economy.
- It is now a primary conduit for socio-economic activities that are vital to every facet of modern life.
- It has become an open space for the ‘good’, ‘bad’ and ‘ugly’.

Why is security an issue in the Cyberspace?

- A level playing ground for both legal, illegal and hostile activities.
- It is transnational in scope, cheap to operate, and yet complex and sophisticated.
- Every traditional illegal activity, or crime has its equivalence in the cyberspace.
- Every traditional hostility is now extended to the cyberspace.
- Its negative impart can have cascaded effect that transcend boundaries.
- The illegal and hostile activities have raised a wide range of Conflicts and Cybercrimes.

Cybercrime

- Cybercrime: All crimes performed or resorted to, by abuse of electronic media or otherwise, with the intent of influencing the functioning of a computer or network system.
- It is a crime where:
  - Computer and/or network is a **target**
  - Computer and/or network is a **tool** of crime
  - Computer and/or network is **incidental** to crime
- All these adversely affects us in varying degrees.

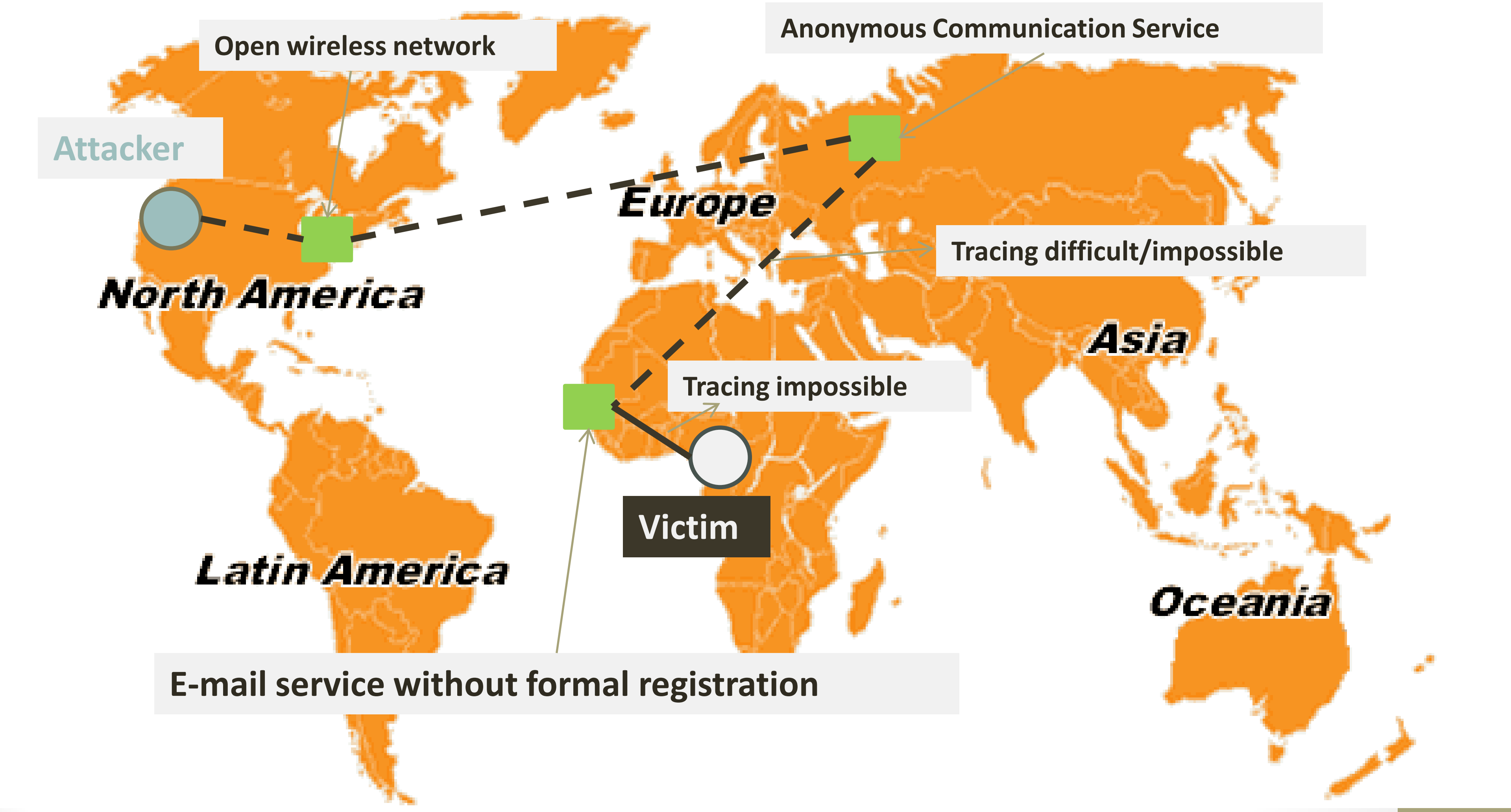
Threat Landscape and Perceptions

- Cyber threat to public and private organizations are becoming increasingly significant
- Exceptional growth of cases of cybercrimes in the financial sector
- Espionage (Proprietary and Intellectual Property)
- Cyber warfare (Cyber conflicts)
- Growing worry about Nigeria, perceived as a nation with massive online criminal activities
- Use of National cyberspace as cyber attack Launchpad
- Mounting Pressure from global community to legislate relevant cyber laws

Examples of Notable Attacks

- In 1989, WANK worm infiltrated NASA's network in protest of nuclear weapons and NASA's use of radioactive probe's booster system
- Strano Network's one-hour "netstrike" against French government websites in 1995 was to protest French government policies on nuclear and social issues
- In 1998, the Electronic Disturbance Theatre's "Web sit-ins" against websites in the US, Mexico to support the Mexican Zapatistas
- The Internet Black Tiger's "suicide email bombings" against Sri Lankan embassies to counter government electronic propaganda
- In 2007, there was a large-scale cyber-attack on Estonia's government telecommunications infrastructure, banks and online media
- Stuxnet 2010 (a worm targeting the Iranian nuclear programme)
- the WikiLeaks saga in 2010 was significant cyberspace event with global impact

Global Picture of Cyber Attack



Open wireless network

Anonymous Communication Service

Attacker

Tracing difficult/impossible

Tracing impossible

Victim

E-mail service without formal registration

Cybersecurity and Regulation

- Cybersceurity is coordinated actions pertaining to the prevention, detection, response, and recovery from incidents on the part of government authorities, the private sector and citizens
- The development and support of cybersecurity strategies are a vital element in the fight against Illegal cyber activities
- Cybersecurity strives to ensure the attainment and maintenance of the security properties of a national cyberspace against security risks.

Cybersecurity and Regulation

- Cybersecurity is a global concern and far-reaching
- Can only be addressed through a coherent strategy taking into account the role of different stakeholders and any existing initiatives.
- There is the need to recognize the real and significant risks posed by inadequate cybersecurity framework.
- Requires we set out a plan for multi-stakeholder Strategy.
- Has three main components - Legal, Technical and Institutional.

Cybersecurity and Regulation

- **Cybersecurity Regulation** encompasses ***directives*** sanctioned by the Executive Branch and ***legislation*** from the legislative arm that ensures cybersecurity safeguards
- The goal of Regulation is to force private and public sectors, especially those that fall within Critical National Infrastructure (CNI) category to protect the information systems and networks from cyberattacks
- the Federal government's full responsibility to guarantee and improve cybersecurity through ***regulation*** and ***legislation***.

Cybersecurity and Regulation Objectives

- Security objectives comprise the following:
  - Confidentiality
    - Access to particular segment of the cyberspace and its resources is restricted only to duly authorised entities.
  - Availability
    - Cyberspace and its resources are always available to the legitimate users.
  - Integrity
    - Cyberspace and its resources are always in the form presented by the originating entity i.e. devoid of tampering or modifications, and ensures non-repudiation.

Cyberspace Regulation & Governance

- Taking full control of nation’s cyberspace for protecting and ensuring its continuity.
- It is essential to national security, safety, and economic vitality of the nation.
- The need to identify and prioritise the nations cyberspace assets: both critical and/or sensitive.
  - systems, networks and resources, whether physical or virtual.
  - So vital to the nation that their incapacitation or destruction would have a devastating effect on security, national economic security, safety, or any combination thereof.

Why is Cyberspace Governance Important?

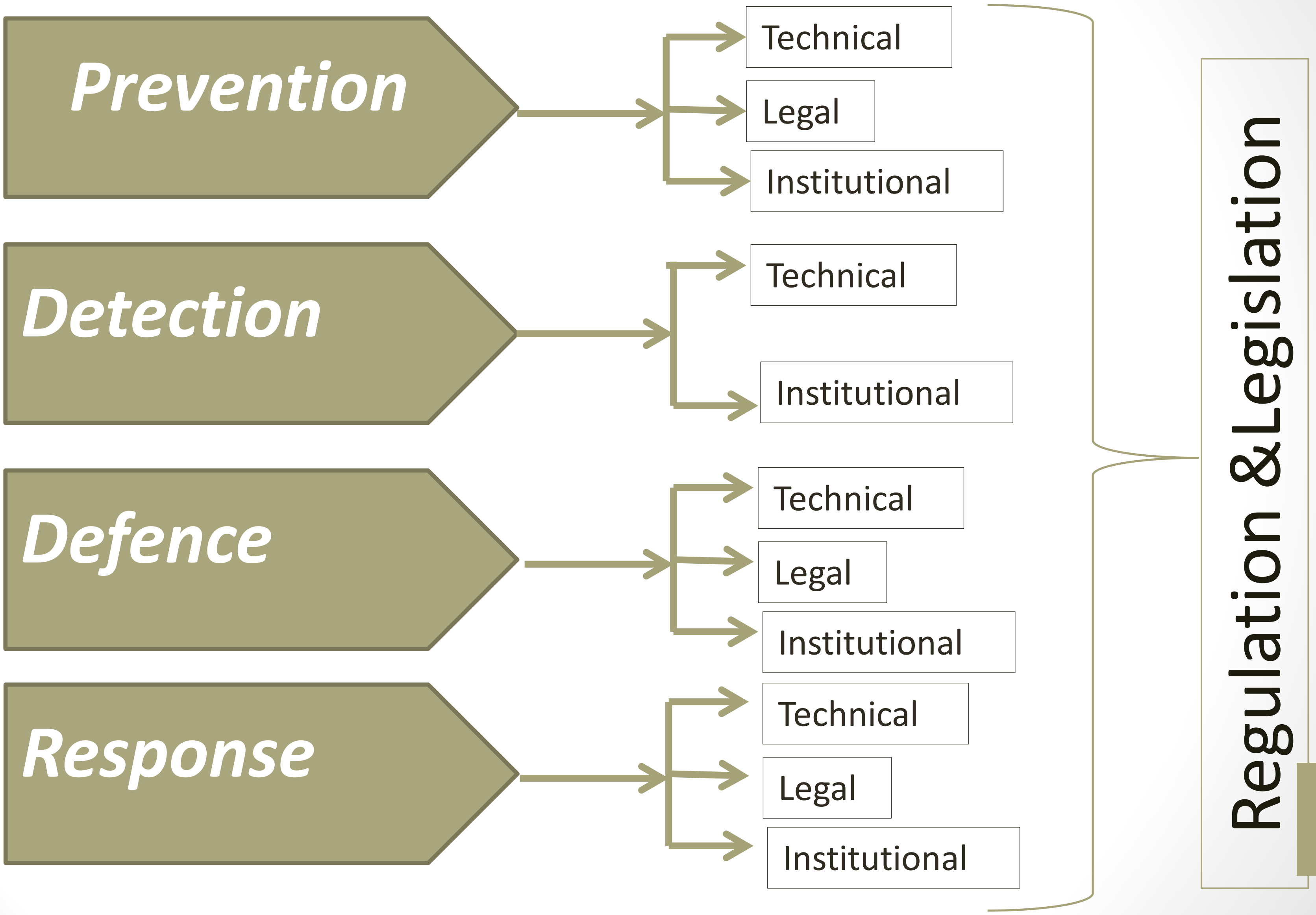
- Attacks on the nation’s cyberspace could significantly disrupt the functioning of government and business alike and produce cascading effects far beyond the targeted sector and physical location of the incident.
- Direct terrorist attacks and natural, manmade, or technological hazards could produce catastrophic losses in terms of human casualties, property destruction, and economic effects, as well as profound damage to public morale and confidence.
- Attacks using components of the nation's cyberspace as weapons of mass destruction could have even more debilitating physical and psychological consequences.

Developing National Cybersecurity Strategy

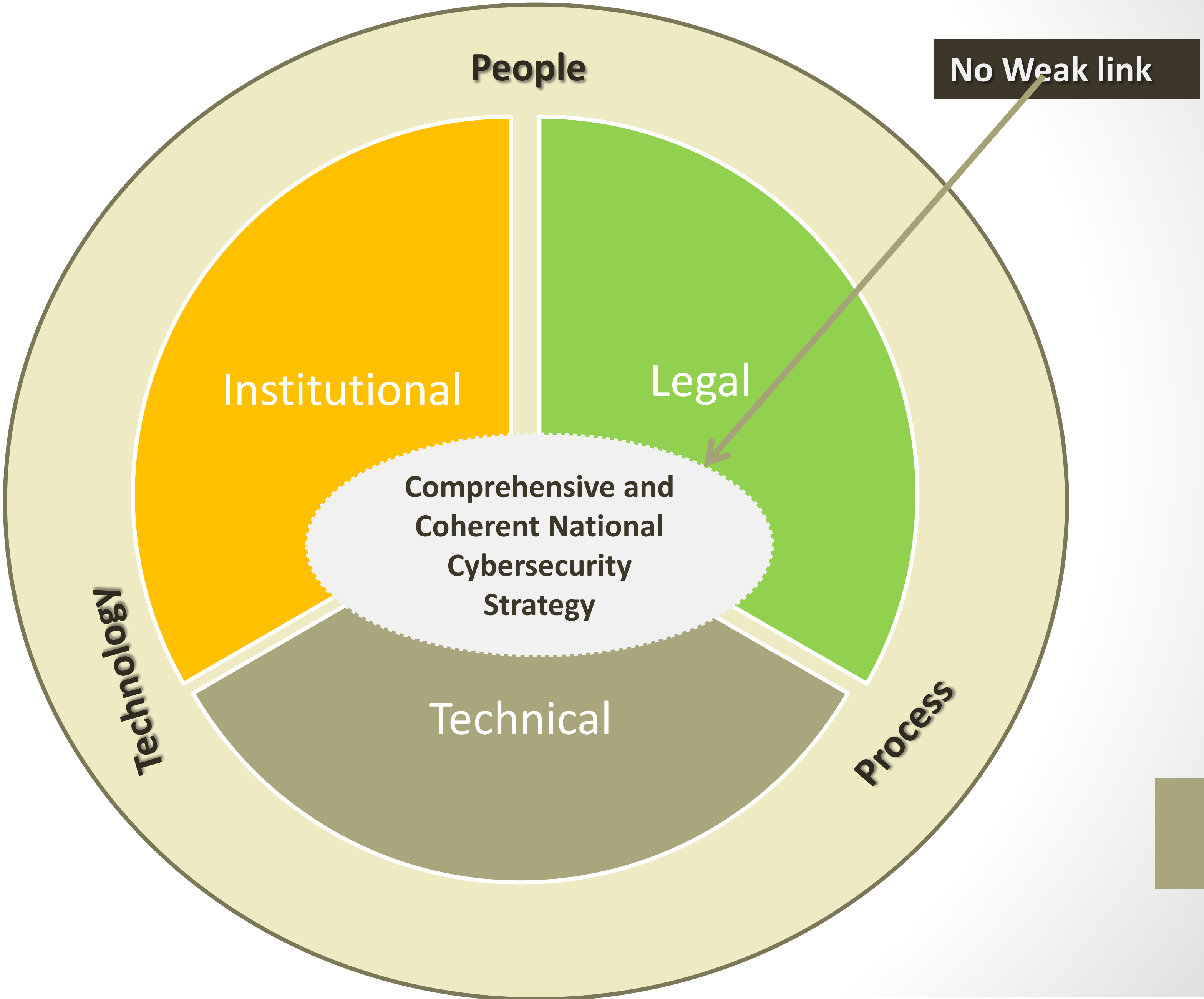
- Comprehensive national cybersecurity framework involves the nation’s capacity, skills, and capability in protecting her National Cyberspace.
- The motivating factors for cyberspace security include among others:
  - To ensure the respect of important rights (lawful use of the cyberspace by citizens);
  - To build confidence in global networks that ensures the nation’s cyberspace is safe (or seen to be safe);
  - To prevent unnecessary restrictions on trans-border flow of data.

Developing National Cybersecurity Strategy

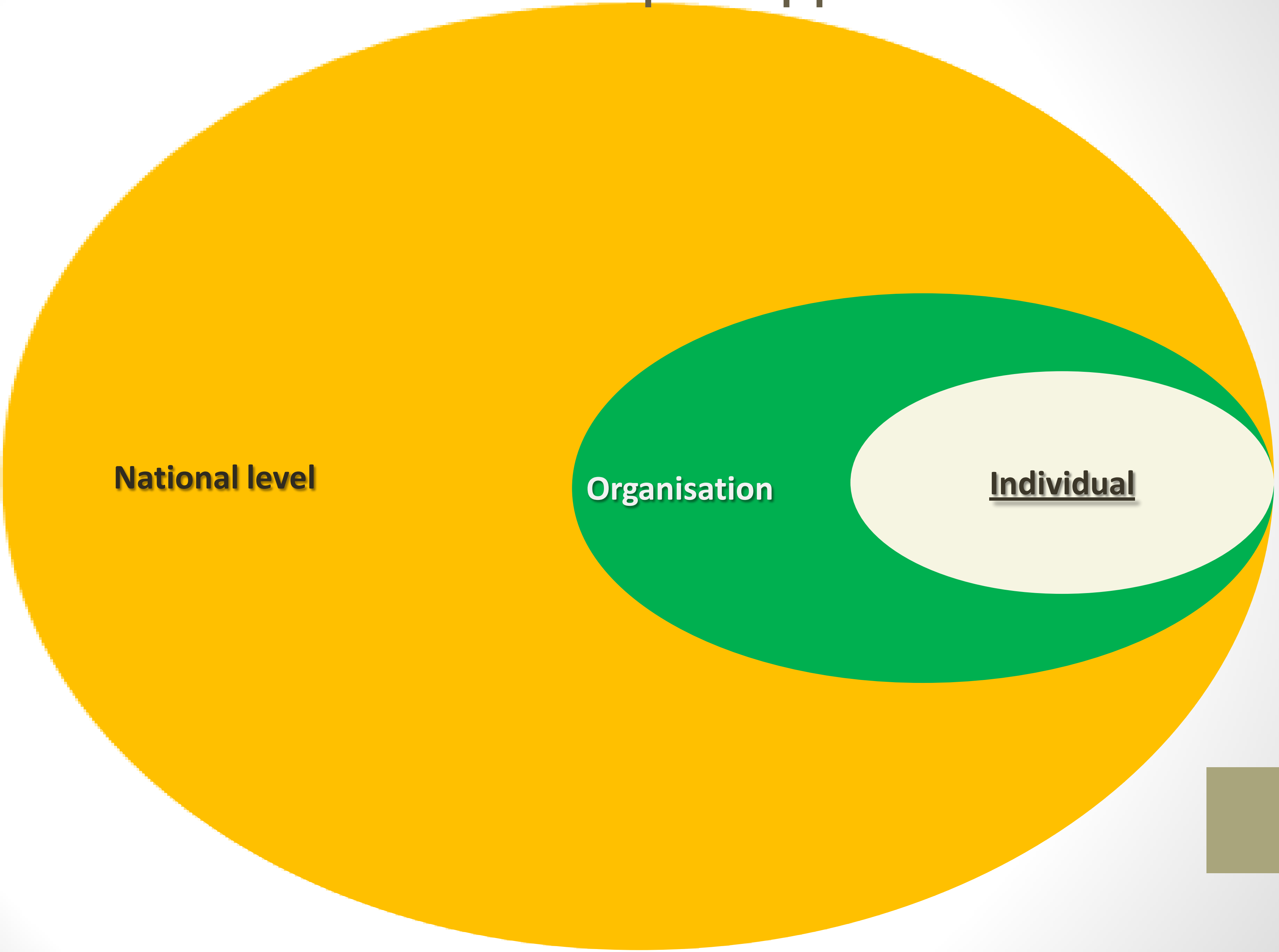
- Focus on four main actions:



Cybersecurity Defence Chain



Defence in- Depth Approach



Understanding Regulatory Compliance Challenges

- Today businesses are under constant pressure to grow rapidly, generate more revenues, reduce costs, and increase profits
- ICT applications, such as e-Government, e-Commerce, e-Education, e-Health and e-Environment
- Achievement of millennium development targets, which can reduce poverty while boasting health and environmental conditions
- Continuous dependent on ICTs and these growing threats have now raised cybersecurity as a business requirement. Cyberspace has become a modern business enabler

Understanding Regulatory Compliance Challenges

- Thus, Regulation and Compliance as part of a National Cybersecurity Strategy
- Require a comprehensive approach that would enable stakeholders to see compliance issues as a business requirement
- Regulation and Compliance must be recognized as vital elements in the fight against illegal cyber activities
- Enforceable Polices, Standards, Baselines, Procedures and Audits
- Compliance is key to achieving cybersecurity
- Organizations may see it as extra cost

Understanding Regulatory Compliance Challenges

- But the cost of noncompliance can be far greater expensive
- Noncompliance may include legal, probationary, notification, and response and recovery costs
- Impacts Organizational reputation and market valuation and future business.
- Organizations may face bad publicity as an outcome of security breaches resulting to lost customers and can ruin the firm
- Reputation is a vital part of corporate posture and image requiring that organizations would rather prefer to protect their integrity than evade compliance.

Strategy for Regulation and Compliance

- NCC to recognize the need to play leadership role in cybersecurity Regulation and Compliance by taking ownership and control;
- Critical assessment of the sector to identify and classify the CNIs within the sector. Identify which Regulations matter most in this sector and sponsor relevant legislation to that effect;
- Creation of awareness to woo stakeholders into partnership of cybersecurity Regulation and Compliance Program;
- Develop Policies, Standards, Guidelines, Procedures and Audits to benchmark implementation of the regulations and compliance specific to this sector;
- Assembly the right team of experts with strong experience and cross-functional management skills in all domains of importance as regards cybersecurity Regulation and Compliance.

Conclusion

- Activities in Cyberspace is changing every aspects of our life.
- The need arises to recognize the dynamics of this changing virtual world.
- National Cybersecurity Strategy must be comprehensive and coherent.
- Critical and sensitive infrastructures must be identified and prioritized.
- Regulation and Compliance as part of National Cybersecurity Strategy
- Legislation as an instrument of the nation’s preparedness to protect Nigerian cyberspace must reflect international dimension.
- Technical, legal and institutional frameworks are non-negotiable ingredients of the legislation.
- Cybersecurity - Defence in-depth approach, key to national cybersecurity.
- National Strategy MUST include capacity, capability and skills acquisition.