KM 5: Critical Information Infrastructure and Critical Information Infrastructure Protection

Content

Module Objective

Welcome to the knowledge module on **Critical Information Infrastructure and Critical Information Infrastructure Protection** as part of the GFCE-Africa project.

This knowledge module will address the needs of AU member states with regard to protection of Critical Infrastructure (CI) and Critical Information Infrastructure (CII).

The module is intended (mainly) for policy-makers and decision-makers involved in various areas (foreign affairs, economic development, security and crime, telecommunications, finances, etc.), and those who wish to get acquainted with the concepts related to the risks, actors, and protection of critical infrastructure and critical information information infrastructure.

Upon finishing the module, you will be able to respond to, and find additional resources for the following focus areas:

- Defining Critical Infrastructure (CI) and Critical Information Infrastructure (CII)
- Identifying, classifying CI and CII
- Designating critical information infrastructure sectors
- Policy, legislative and regulatory guidelines
- Governance Framework
- Stakeholder involvement in the CI and CII
- Funding and Capacity development

1. Introduction

Every country has critical infrastructure that makes it function. These critical infrastructures vary between countries as they are identified based on a country's national risk assessment. They include: energy and water supply, telecommunications, financial systems, and government services. In Africa these infrastructures are increasingly monitored and controlled through networks and systems connected to the Internet. Cybersecurity threats exploit the increased complexity and connectivity of such infrastructure, placing a country's security, economy, and public safety and health at risk.

These interconnected information and communication infrastructures are referred to as Critical Infrastructures (CIs) and Critical Information Infrastructures (CIIs). A cybersecurity incident impacting the CI and CII can disrupt social order, the delivery of essential services, and the economic wellbeing of a country. It is therefore imperative that a nation puts in place strategies, policies and activities that provide for the identification, security, and protection of the CI and CII using a risk-management approach.

2. What is Critical Infrastructure (CI) and Critical Information Infrastructure (CII)?

There are no universally recognised definitions for Critical Infrastructure (CI) and Critical Information Infrastructure (CII). There are varying national, regional, and

international definitions for the CII available on CIpedia. A standard definition is provided by the IETF Request for Comments (RFC): 4949 as *those systems that are so vital to a nation that their incapacity or destruction would have a debilitating effect on national security, the economy, or public health and safety*.' Defining the CI and CII is important for classification, registration, and resourcing.

Good Practice: Grasp Definitions of CI Sectors and Services from other Nations

When defining a nation's critical infrastructure, it is a good practice to understand definitions of the CII sectors and services from other nations.…'*one may be inspired by the sets of CI sectors and services defined by other nations*''

The African Union Convention on Cybersecurity and Personal Data Protection defines
Critical Cyber/ICT Infrastructure as 'the cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international stability, and for the sustainability and restoration of critical cyberspace.'

The GFCE-MERIDIAN good practice guide on Critical Information Infrastructure Protection for governmental policy-makers defines Critical Information Infrastructure (CII) as 'those interconnected information and communication infrastructures which are essential for the maintenance of vital societal functions, (health, safety, security, economic or social well-being of people) - the disruption or destruction of which would have serious consequence.'

The United States (U.S.), Cybersecurity and Infrastructure Security Agency (CISA) define critical sectors of the economy as infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

OECD Recommendation of the Council on the Protection of Critical Information Infrastructures (English, French) defines critical information infrastructures (CII) as '*interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy.'*

The UK definition of Critical National Infrastructure is: '*Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which*

could result in: a) Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or b) Significant impact on national security, national defence, or the functioning of the state.'

Case Studies: African Countries Definitions for CI and CII

Ghana's Cybersecurity Act, 2020 (Act 1038) defines critical information infrastructure as a '*computer or computer system designated as essential for national security, or the economic and social well-being of citizens.'*

In Kenya reference to Computer Misuse and Cybercrimes Act, 2018 a system is *'designated as critical infrastructure if a disruption of the system would result in:*

- *The interruption of a life sustaining service including the supply of water, health services, and energy*
- *An adverse effect on the economy of the Republic*
- *An event that would result in massive casualties or fatalities*
- *Failure or substantial disruption of the money market of the Republic; and*
- *Adverse and severe effect of the security of the Republic including intelligent and military services'*

The National Cybersecurity Framework for South Africa defines National Critical Information Infrastructure as 'a*ll ICT systems, data systems, databases, networks (including people, buildings, facilities and processes), that are fundamental to the effective operation of the Republic.'*

The Botswana National Cybersecurity Strategy defines Critical Information Infrastructure as '*the digital infrastructure whose disruption or damage negatively affects the well-functioning of the economy.'*

3. What are the threats to critical infrastructure in Africa?

Today, many African countries face challenges in protecting their critical infrastructure. These include: lack of policy and legislation, lack of an information sharing and coordination framework for government and private sector owned or managed infrastructure, inadequate capacity and resources, acts of terror and vandalism.

Resource: *Examples of Attacks Against Critical Infrastructure In Africa*

Liberia: In 2016, an overzealous hacker employed by one major telecommunications company sabotaged the network of a rival resulting in half the country being cut off from bank transactions. Cut off from internet access, Liberia's information minister, ostensibly in charge of the country's response, was left asking for help on French radio. Despite Liberia's appeals abroad for assistance, authorities did not make arrests until after the software employed in the attack was used to disable Deutsche Telekom.

Nigeria: In August 2012, Boko Haram reportedly hacked the personnel records databases of Nigeria's secret service, revealing the names, addresses, bank information, and family members of current and former personnel of the spy agency. The breach was executed in the name of Boko Haram as a response to Nigeria's handling of interactions with the group. The attack was significant as it represented a substantial shift in tactics of the group which has an anti-Western stance.

South Africa: In June 2020, Life Healthcare, the second largest private hospital operator in South Africa was hit by a cyberattack. This attack, which happened during the COVID-19 pandemic, believed to have cost the organisation more than a month in downtime, affected its admission systems, business processing systems, and email servers, with some systems being forced offline.

The state-owned enterprise Transnet, operating rail, port, and pipeline in South Africa, faced a cyberattack in July 2021. The attack caused Transnet to declare force majeure at several key container terminals, including Port of Durban, Ngqura, Port Elizabeth, and Cape Town. The impact of the attack was 'unprecedented' according to the Institute for Security Studies (ISS) because it was that the 'operational integrity of the country's critical maritime infrastructure has suffered a severe disruption' for the first time, resulting in the shut down of a critical trade route and disruption of vital trade services in the middle of a global pandemic.

The African Union Convention on Cybersecurity and Personal Data Protection requires states to develop a national cybersecurity policy and a strategy that sets out the objectives and timeframes for successful implementation of the policy. Developed in collaboration with stakeholders and based on an all hazards approach, the policy should identify the risks facing the nation and recognise the importance of Critical Information Infrastructure (CII). The convention requires countries to adopt legislative and/or regulatory measures necessary to identify and protect the sectors and supporting ICT systems that are critical to national security and well-being of the economy.

The protection of critical infrastructure requires the national commitment set out in relevant strategy, policy, and legislation.

"Protecting critical infrastructure and critical information infrastructure is like predicting an earthquake. In Geology, we know where an earthquake will strike and at what magnitude, but, what we do not know is when…It is managing this uncertainty that will test our fortitude as businesspeople, technologists, policymakers and scholars of CII in the days and years ahead"
Source: Ensuring (and Insuring?) Critical Information Infrastructure Protection

Reflection: Cyberattacks on infrastructure

1. Identify cyberattacks to infrastructure that have happened in your country.
2. What was the economic and social impact of the disruption caused by the attack?
3. What measures have been put in place by the Government to prevent and mitigate similar attacks?

4. How to identify, classify and register the CI

Identification of critical infrastructure and the sectors and subsectors associated with it, is different and unique to each country.

4.1. Methodologies for identification and classification of critical infrastructure

There are various methodologies for identification of the CII including the use of a service-based approach, application of sectorial or functional criteria, as well as an assessment of stakeholders. The Guide to Developing a National Cybersecurity Strategy recommends cyber risk assessment and threat modelling to identify, designate, and protect the CI,the CII, or essential services.

- **Dependencies and interdependencies**: The examination of dependencies and interdependencies with other infrastructure and services is a good practice in the identification of a CI(I). A dependency is defined as 'the relationship between two products or services in which one product or service is required for the generation of the other product or service'

Good Practice: (National And Cross-Border) Dependency Analysis

Dependencies can be recognised during the process of CI identification and risk assessments. These are CI dependencies within a nation and those of

neighbouring nations and regions. Dependencies may influence the criticality of a particular national infrastructure and can be determined through stakeholder consultations.

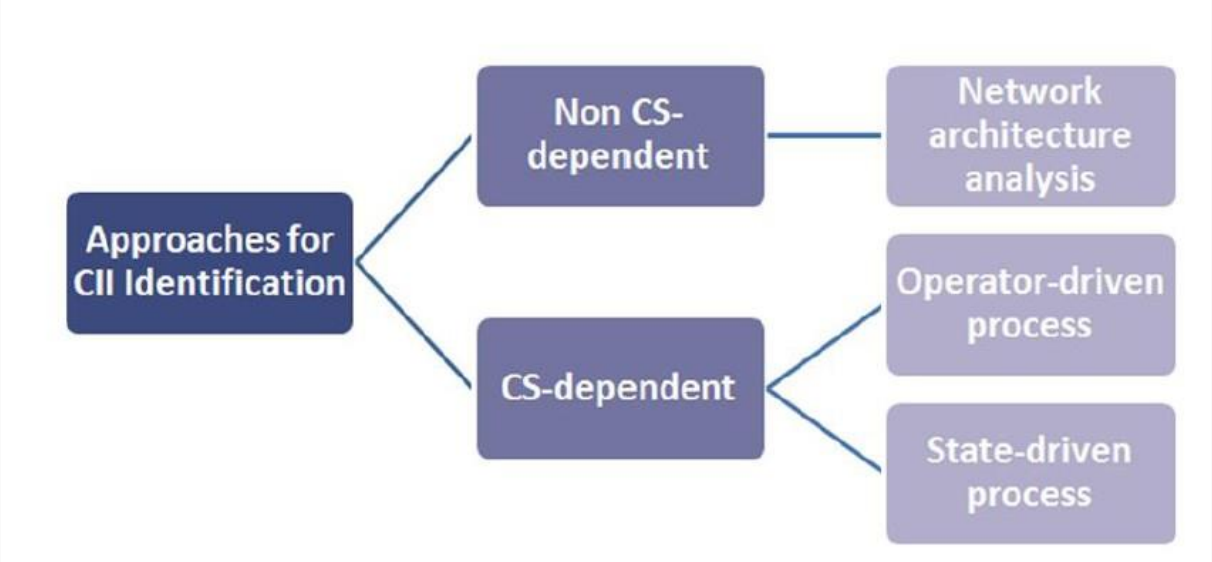

Figure 1: *Methodological approaches for Critical Information Infrastructure identification* Source: ENISA

- **Risk Assessment**: The identification of national CIIs should be guided by a risk assessment. A risk-based approach based on international standards is required to identify and prioritise the implementation of common baseline programmes, policies, and practises for security and resilience of the CI(I) as well as ensure their integration and interoperability.

Good Practice: Develop A National Risk Profile

In developing a National Risk Profile, a country's stakeholders would gain a common understanding of the risks, consequences, and their relative priority. The use of the EU Risk Management Capability Assessment Guidelines may be used by countries in carrying out a risk assessment.

The assessment based on a set of 51 questions on coordination, expertise, methodology, stakeholders, information and communication, equipment, and financing helps with risk identification and prioritisation, and presents the basis for the:

- risk assessment,
- risk management planning,
- implementing risk prevention and preparedness measures.

The National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity helps owners and operators of critical infrastructure to identify, assess, and manage cybersecurity risks using a prioritised, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls.

- **Threat modelling:** This is a structured approach to threat scenarios; an engineering technique to identify possible threats, attacks, vulnerable areas, and countermeasures that could affect the product or the related environment (network, architecture, etc.). Using threat modelling methods profiles of potential attackers, including their goals and methods, a catalogue of threats can be created and the information used to inform defensive measures.

Good Practice: Adopt a methodology to identify CI sectors and services systematically

A structured four-step approach to identification of CI sectors and services is recommended in ENISA's Methodologies for the identification of Critical Information Infrastructure assets and services for the evaluation of a sector or service that could potentially be critical:
1. Apply sector-specific criteria
2. Assess criticality
3. Assess dependencies
4. Apply cross-cutting criteria.

The most useful order of these steps depends on the information available to national policy-makers.

Resource: *How to identify and classify the CI and CII*

ITU 2021 Global CyberDrill Training Video: How to identify and classify critical information infrastructure assets and services

4.2. Designating critical information infrastructure sectors

4.2.1. How critical infrastructure is designated?

The criteria and process of designation of infrastructure as 'critical' is guided by the provisions of the national strategy, policy or law. The role of designation differs between countries and ranges from the President, Minister or head of institution responsible for the protection of critical infrastructure.

Case Study: *How Critical Infrastructure is designated?*

In South Africa, the Critical Infrastructure Protection Act 8 of 2019 provides that the Cabinet Minister responsible for policing may declare infrastructure as 'critical' based on the recommendation of the Critical Infrastructure Council, the application for declaration of infrastructure as critical infrastructure, and any other relevant information.

In Tanzania's Cybercrime Act of 2015, the Minister may designate a computer system as critical information infrastructure, by order published in the Gazette. The order may prescribe guidelines or procedures for the registration, protection, management of critical information infrastructure, management and storage of associated data, disaster recovery plans, and audit.

In Kenya's Computer Misuse and Cybercrimes Act, 2018, the Director, who is the secretary to the National Computer and Cybercrimes Coordination Committee (NC4),shall designate a system as a critical infrastructure if it meets the definition of critical infrastructure and in line with a critical infrastructure framework.

In Nigeria's, the Cybercrimes (Prohibition, Prevention, etc) Act, 2015, the President may, on the recommendation of the National Security Adviser, by order published in the Federal Gazette, designate certain computer systems, and/or networks as constituting Critical National Information Infrastructure if they would, when incapacitated or destroyed, debilitate national or economic security, public health, and safety.

4.2.2. What are the designated CII sectors?

In reference to the definition, designation, and classification of the CII, a country may develop a National Critical Information Infrastructure Register. An accurate and up-to-date register of all assets and locations declared as critical infrastructure should be maintained by the entity charged with the management and protection of critical infrastructure.

Countries may consider implementing an Infrastructure Visualization Platform (IVP) similar to that of the US. The IVP is a data collection and presentation medium that enhances planning, protection and response of critical infrastructure using a combination of immersive imagery, geospatial information, and hypermedia data of critical facilities and surrounding areas to enhance planning, protection, and response efforts.

Case Study: Designated CII sectors

Ghana's Cybersecurity Act, 2020 (Sections 35) has designated 13 CII sectors: National Security and Intelligence, Information and Communications Technology (ICT), Banking and Finance, Energy, Water, Transportation, Health, Emergency Services, Government, Food and Agriculture, Manufacturing, Mining, and Education.

The Botswana National Cybersecurity Strategy has identified the following sectors as national critical infrastructure sectors with regard to the cybersecurity: finance, communications, energy, water, emergency services, food, public safety, health, public services, and e-government.

Kenya's Director, National Computer and Cybercrimes Coordination Committee (NC4), in a Gazette Notice (effective 20th January, 2022), designated as Critical Infrastructure the following sectors: Telecommunications, Electoral, Judicial, Education, Health, Food, Water, Land, Energy, Transport and Industry, Banking, Finance, Defence, Security, and Public safety

The Mauritius National Cybersecurity Strategy, identifies the critical sectors as financial services, Tourism, electricity, water, ICT and Broadcasting, Health, Government Services, Manufacturing, Transport and Logistics, Sugar and Customs.

Resource: Video *Cybersecurity and Critical Infrastructure Protection*

The University of Fairfax Webinar discusses:

- The US National Infrastructure Protection Plan (NIPP),
- Critical infrastructure sectors,
- The common cyber risks shared by all elements of the critical infrastructure,
- How Presidential Policy Directive/PPD 21 - Critical Infrastructure Security and Resilience supports the need for cyber risk resilience,
- An overview of the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity,
- How it supports critical infrastructure protection and suggestions to enhance cyber risk resilience.

Resource: CII Sectors in other countries

The United States of America has 16 CI sectors: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Material, and Waste; Transportation Systems; and Water and Wastewater Systems.

The European Union (EU) Directive on Security of Network and Information Systems (NIS Directive) mandates that member State adopt a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures covering at least the seven CI sectors: Energy, Transport, Banking, Financial Market, Health, Drinking Water Supply and Distribution, and Digital Infrastructure.

The Report from the Commission to the European Parliament and the Council assesses the consistency of the approaches taken by Member States in the identification of operators of essential services (OES) in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems.

The CIIP law in France adopted in December 2013 and the framework for the 'security of activities of vital importance' established in 1998 identifies more than 200 critical operators (called 'operators of vital importance') in 12 sectors including: Food, Health, Water, Telecom and Broadcasting, Space and Research, Industry, Energy, Transport, Finance, Civilian administration, Military activities and Justice. By law, these operators are required to identify their 'critical information systems' that is, those systems 'whose unavailability could strongly threaten the economic or military potential, the security or the resilience of the Nation'.

The UK's Centre for the Protection of National Infrastructure (CPNI) has designated 13 national infrastructure sectors: Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport, and Water. Several sectors have defined 'sub-sectors'; Emergency Services, for example, can be split into Police, Ambulance, Fire Services, and Coast Guard.

***Reflection**:*

Based on the national, regional, and international examples of definition, identification and classification of critical infrastructure discussed, using your country as an example:

- Define Critical Infrastructure and Critical Information Infrastructure CI(I)
- Identify the CI(I)
- Classify the CI(I)

- What principles/criteria did you use?

5. Policy, legislative and regulatory guidelines

In developing national policy, legislation and guidelines for the protection of CI and CII, a review of provisions of existing international conventions, legislation, and structures should be considered.

Resource Video: Kenya's Critical Information Infrastructure: Exploring the Effectiveness and Impact of Existing Legal and Institutional Framework

Source: Strathmore University Business School Webinar

UN General Assembly resolution 58/199 (2003) 'Creation of a global culture of cybersecurity and the protection of critical information infrastructure recognizes that each country will determine its own critical information infrastructures and invites Member States to consider, the elements for protecting critical information infrastructures in developing strategies for reducing risks to critical information infrastructures, in accordance with national laws and regulations;

UN Global Counter-Terrorism Strategy under Pillar II 'Measures to combating and Preventing Terrorism', member states resolved 'to step up all efforts to improve the security and protection of particularly vulnerable targets, such as infrastructure and public places, as well as the response to terrorist attacks and other disa sters, in particular in the area of civil protection'

United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015 report (paragraph 13g) recommends for consideration voluntary, non binding norms for responsible state behaviour in cyberspace which include taking appropriate measures to protect their critical infrastructure from ICT threats taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.

African Union Convention on cybersecurity and Personal Data Protection Article 24 of requires signatories to develop, in collaboration with stakeholders, a national *cybersecurity* policy which recognises the importance of Critical Information Infrastructure (CII) for the nation to identify the risks facing the nation in using the all-hazards approach and outline how the objectives of such policy are to be achieved.

Under Article 25 of the convention, states are required to adopt such legislative and/or regulatory measures as they deem necessary to identify the sectors regarded as sensitive for their national security and well-being of the economy, as well as the information and communication technologies systems designed to function in these sectors as elements of critical information infrastructure; and, in this regard, proposing more severe sanctions for criminal activities on ICT systems in these sectors, as well as measures to improve vigilance, security and management.

In addition, there are requirements in agreements signed under Regional Economic Communities in Africa such as SADC, Protocol on Politics, Defence and Security Co-operation, 2001 which seek to establish an institutional framework by which member states could coordinate policies and activities in areas of policy, defence, and security.
The Organ for Politics, Defence and Security established under this protocol supports the achievement and maintenance of security and the rule of law in the SADC region. The Organ's objectives are in the areas of Military/Defence, Crime Prevention, Intelligence, Peace-making & Peacekeeping Enforcement, Foreign policy, Conflict Management, Prevention & Resolution, and Human Rights. Specific activities to achieve these objectives are spelt out in the Strategic Indicative Plan for the Organ on Politics, Defense and Security Cooperation (SIPO I). These include regular assessments of regional public security situation and building capacity to combat cybercrime and terrorism.

Reflection point:
Which international, regional conventions, and national legislative and regulatory requirements has your country used to implement Critical Infrastructure Protection policies, strategies, and structures?

6. How to develop a critical infrastructure and critical information infrastructure protection policy

The GFCE-MERIDIAN good practice guide reference to EC 2008 defines Critical Information Infrastructure Protection (CIIP) as: "All activities aimed at ensuring the functionality, continuity and integrity of CII in order to deter, mitigate and neutralise a threat, risk or vulnerability or minimise the impact of an incident".

CIIP is a vital element of cyber security and included as a component of the national cyber security strategy. A country may consider developing a CIIP policy to establish

coherence and coordination of the activities, resources and initiatives necessary to secure critical infrastructure from natural disasters and cyber related incidents.

A national policy for the protection of the CI and CII is guided by a set of principles determined by the government and influenced by international and regional conventions, standards, and best practises. The objective of the policy is to establish a national framework for the harmonisation and coordination of critical infrastructure protection.

The Internet Infrastructure Guidelines for Africa recommend that policy makers use four essential principles as a guide in developing strategies and policies for Internet infrastructure security. These principles are

1. Awareness: An understanding of security risks, their impact on the Internet infrastructure ecosystem.
2. Responsibility: Stakeholder accountability and understanding of potential impacts of one's actions, or inactions.
3. Cooperation: Dialogue to encourage cooperation and collective responsibility among all stakeholders.
4. Fundamental rights and Internet properties: Adherence to transparency and non-infringement on the fundamental properties of the internet: voluntary collaboration, open standards, reusable technological building blocks, integrity, permission-free innovation, and global reach.

Good Practice: G8 Principles for Protecting Critical Information Infrastructures

G8 Principles for Protecting Critical Information Infrastructures include national, regional, and international coordination and collaboration, information sharing, identification of interdependencies, determination of stakeholders' roles and responsibilities, enhancement of capabilities, adequate legal provision, research and development, and application of internationally certified standards.

The basic steps of developing and maintaining a current CIIP policy are:

Step 1. Make the CIIP a national priority: The effectiveness of a CIIP policy is improved if embedded in the National Risk Profile (NRP) and National Cybersecurity Strategy and implemented by a committee with high ranking multisectoral stakeholder representation.

Step 2. Identification of critical information infrastructure: Critical infrastructure can be identified by using the four methodological stepping stones inspired by the European Critical Infrastructure Directive (EC2008). The four stepping stones are:

1. apply sector-specific criteria
2. assess criticality
3. assess dependencies
4. apply cross-cutting criteria.

Step 3. Development of a critical information infrastructure protection policy including:

3a. a risk-based approach (in comparison to an ad-hoc approach)
See section 4

3b. embedding of a CII(P) in national crisis management
See Section 7

3c. support for networking and information sharing
Protection of critical infrastructure relies on reliable, secure, and efficient communication among various stakeholders.

Good Practice: Adopt a multi-agency approach and start information sharing

Governments should adopt a multi-agency approach to address the risk and complexity associated with the CIIP at strategic, tactical and operational and technical levels.

Regular meeting of stakeholders selected based on their legal mandate, ownership and operation of critical infrastructure should be considered. These stakeholders include government ministries and agencies, national security, defence and police, the national Computer Security Emergency Response Team and private sector owners and operators of critical infrastructure.

Other networking and information sharing good practices are:
1. Stimulate the sharing of cyber security related information
2. Establish clear roles in CIIP in sharing initiatives
3. Be informed about information sharing standards
4. Take note of the guide to cyber threat information sharing
5. The buddying system
6. Various organisational forms of public-private partnerships for CIP/CIIP
7. Cyber security council at the national level
8. Traffic Light Protocol (TLP)

Source: Chapter 7 GFCE-MERIDIAN good practice guide on Critical Information Infrastructure Protection for governmental policy-makers

Step 4. Monitoring and continuous improvement

The successful implementation of the policy depends on periodic monitoring and evaluation (M&E). Monitoring involves the tracking of the proposed interventions, initiatives, and resources against the expected policy outcomes while evaluation involves the determination of the value of the policy implementation and achievements. The M&E results are shared with stakeholders and feedback provided to enhance future initiatives.

7. National cyber crisis management plan

The Guide to developing a National Cybersecurity Strategy recommends that countries should consider developing a national cybersecurity contingency plan as part of, or aligned with, the overall national contingency or crisis management plan. This plan should consider the findings of the national risk assessments, provide for disaster-recovery and incident-response mechanisms. The cybersecurity contingency plan should determine the cross-sector dependencies that could affect critical infrastructures and categorise cyber incidents based on their impact on critical assets and services.

Several African countries have Disaster Management Plans or Policies that deal with the management of natural disasters. Based on a systematic approach, these plans which may reference the Tampere convention, provide guidelines, principles, and code of conduct for stakeholders, as well as the enactment of legislation which supports the establishment of an institutional framework. Disaster Management Plans also set out various means for resource mobilisation as well as a framework for monitoring and evaluation. These plans need to be updated to include the management of cyber incidents and protection of critical infrastructure.

A National cyber crisis management plan can be defined as a strategic framework which articulates the roles and responsibilities, capabilities, and coordinating structures that support how a Nation responds to, and recovers from, significant cyber incidents posing risks to critical infrastructure.

It can also be defined as a strategic plan which recommends and elaborates on the actions and responsibilities for a coordinated and multidisciplinary approach to respond and recover from cybersecurity incidents of national significance impacting critical systems and the economy.

The objective of the National cyber crisis management plan are:

- To recommend and elaborate on the actions and responsibilities for a coordinated and multidisciplinary approach to respond and recover from cybersecurity incidents of national significance impacting critical systems and the economy.

- To minimise disruption of services or loss/theft of information caused by incidents.
- To use the information gained for better preparation for future handling of incidents.

Resources: National cyber crisis management plans

The National Cyber Incident Response Plan (NCIRP), USA provides guidance to enable a coordinated whole-of-Nation approach to response activities and coordination with stakeholders during a significant cyber incident impacting critical infrastructure.

Canada Cyber Security Event Management Plan provides an operational framework for the management of cybersecurity events that impact or threaten to impact the Canadian government's ability to deliver programs and services to citizens. The plan outlines stakeholders and actions required to ensure that cybersecurity events are addressed in a consistent, coordinated, and timely fashion.

Cyber Incident Management Arrangements for Australian Government outlines the interjurisdictional coordination arrangements, roles and responsibilities, and principles for Australian governments' cooperation in response to national cyber incidents.

.

Reflection Point:

Based on examples given, should your country consider developing a national cyber crisis management plan?

Prepare a justification or concept note referencing relevant strategy, policy and legislative provisions for presentation to the President or relevant government minister.

8. Infrastructure security audits and vulnerability assessments

Infrastructure audits and vulnerability assessments, carried out periodically against minimum standards, are critical for the protection of national security. They are an essential component of the national cybersecurity strategy and contribute to formulation of the National Risk Profile (NRP).

The national cybersecurity strategy should outline the minimum outcome-focussed cybersecurity baselines that are relevant across the CI and CII operators based on international standards and best practises. In determining compliance to national priorities and consistent interoperable practises, audits and assessments make reference to security baselines.

Resource: Cybersecurity Audit Baseline Requirements India

The Cybersecurity Audit Baseline Requirements for Cyber Information Infrastructure provide a minimum, common, and harmonised baseline criterion for cyber security audits. It provides guidance to auditors and auditees and mandatorily applicable to owners and regulators of Critical Information Infrastructure.

Cyber Security audit baseline is defined as the minimum controls to be audited for cybersecurity of an organisation which are grouped into six categories:
(a) Management
(b) Protection
(c) Detection
(d) Response
(e) Recovery
(f) Lessons Learnt and Improvements

The outcome of the risk assessment is the classification of the organisation as high, medium or low risk information infrastructure.

Source: National Critical Information Infrastructure Protection Centre (NCIIPC)

Good Practice: *Defining minimum security baselines*

The **Guide to Developing a National Cybersecurity Strategy** recommends that countries identify and follow good practice elements that support the vision and objectives of the National Cybersecurity Strategy. Defining minimum cybersecurity strategy is one of these good practice elements.

Legislation or regulations should outline the minimum cybersecurity baselines for CI and CII operators. To ensure consistency, better outcomes, greater efficiency and interoperability, security baselines should be outcome-focused and should reference internationally recognized standards and best practises.

The security baselines address:

- High Level risk-management priorities
- Specific cybersecurity practises
- Identification of cyber risks
- Establishment of risk management governance structures

- Measures for protection of data and systems
- Monitoring of the digital environment and detection of anomalies/events
- Response and recovery from incidents
- Procurement requirements

Case study: Country audits of the CII

Ghana's Directive for the Protection of Critical Information Infrastructure (CII) establishes audit measures and procedures to ensure compliance pursuant to Section 38 of the Cybersecurity Act, 2020. The audit of a designated CII is carried out by the Cyber Security Authority (CSA) or its authorised auditor reference to submit reports, risk register, and any cybersecurity activities conducted. Planned significant changes in design, configuration, security, or operation of the CII must be approved by the Authority.

The baseline security requirements for designated CII owners are:

- Policy
- Technical and organisational measures
- Incident reporting

Resource: Agence nationale de la sécurité des systèmes d'information (ANSSI) cross-sectoral, security rules for CII and CI operators

The French Network and Information Security Agency, Agence nationale de la sécurité des systèmes d'information (ANSSI) has defined cross-sectoral, security rules for CII and CI operators, based on operational experience and existing international standards which mostly include cyber hygiene measures and fall within 20 categories:

- Information assurance policies
- Security accreditation
- Network mapping
- Security maintenance
- Logging good practice
- Logs correlation and analysis
- Detection
- Security incidents handling
- Security alerts handling
- Crisis management

- Identification
- Authentication
- Access control and privileges management
- Administration access control
- Administration Systems
- Segregation in systems and networks
- Traffic monitoring and filtering
- Remote access
- Systems set up
- Indicators

9. Governance Framework

The governance framework describes the roles, responsibilities for protection of CI/CII owners, and operators at a national level. The governance framework is guided by cybersecurity strategy, policy, legislation, directive, regulations, good practises, and/or guidelines.

As the CI/CII is not often owned or controlled by the government and the CIIP generally exceeds the capabilities and mandate of a single entity, the establishment of an interagency governance structure such as a committee or agency is of importance.

The governance model should include:

- Identification of public and private entities in charge of specific verticals
- Responsibilities and accountability of CI and CII operators
- Cross-sector and sector-specific cybersecurity baselines
- Information-sharing processes and protocols
- Communication channels and cooperation mechanisms
- Coordination structures and alignment across government entities with overlapping mandates

Case Study: CI and CII Governance

Ghana' Cyber Security Authority (CSA) provides support and guidance to a designated CII in accordance with the provisions of the Cybersecurity Act, 2020 (Act 1038).

National Computer and Cybercrimes Coordination Committee (NC4) is the central point-of-contact for cybersecurity matters in Kenya and coordinates cyber activities

reference to the provisions of the Computer Misuse and Cybercrimes Act 2018.

10. Stakeholder involvement in the CI and CII

Involving a diverse mix of stakeholders from the beginning of the development of a national risk profile is important, as their acceptance of the identification, classification, and protection of critical infrastructure is vital. Various tools and methods can be used for stakeholder analysis. However, a simple categorisation of stakeholders as public, semi-public or private, and as regionally, nationally or internationally operating, would suffice.

While taking advantage of their complementarity perspectives, responsibilities, and expertise, collaboration between public and private sector stakeholders is the cornerstone of effectively protecting critical infrastructure and services.

11. Funding

Critical infrastructure requires financial, human and physical resources that should be identified in the strategy or policy. The resources can be derived from government, development partners or Private Public Partnership (PPP).

Critical infrastructure owners and operators need to make significant investment in their security and adopt cybersecurity best practises. As these measures may not immediately yield measurable benefits, the private sector may be justifiably concerned about the return on security investments. The government may therefore implement standards and practises to incentivise private sector owners and operators to fulfil their individual cybersecurity responsibilities, commensurate with the risk they face and that justify the costs of investment in cybersecurity.

Resource: Incentives for the CI owners and operators

The US Executive Order 13636: Improving Critical Infrastructure Cybersecurity, Incentives Study Analytic Report defines an incentive as a cost or benefit that motivates a decision or action by critical infrastructure asset owners and operators to adopt the Cybersecurity Framework under development by NIST. These include market-based incentives such as insurance. However, to hasten the pace of the necessary improvement in cybersecurity, government action can provide additional

impetus to the market. In the US, incentives contained in legislation, policy, and other sources include expedited grants, information sharing, insurance, new regulation/legislation, prioritised technical assistance, procurement considerations, public recognition, subsidies, and tax incentives.

12. Capacity development

The Cybersecurity and Infrastructure Security Agency's (CISA) Infrastructure Security Division offers free training programs to government and private sector partners.

Training programs include National Infrastructure Protection Foundational Courses such as Introduction to the National Infrastructure Protection Plan, Achieving Results through Critical Infrastructure Partnership and Collaboration and Security Awareness Training Courses such as Workplace Security Awareness, Active Shooter: What You Can Do and Protecting Critical Infrastructure against Insider Threat. Sector specific training is offered for the Chemical , Commercial Facilities , Dams Sector Emergency Services , Nuclear Reactors, Materials, and Waste Sectors

13. (Geo)political and social factors

Critical infrastructure usually sits astride country and jurisdictional boundaries. The safety and security of such infrastructures requires collaboration between partners in the public and private sectors on a regional and global level. International cooperation, in particular, the willingness and ability to share information, a legal framework against cyber crime, and a strong culture of security in the face of rapid technological growth and consequential social changes, enhances national operational infrastructure security capabilities.

The US collaborates with international partners to enhance and promote cross-border and global critical infrastructure security and resilience through information sharing. In 2012, the Critical Five (Australia, Canada, New Zealand, the United Kingdom, and the United States) was established to enhance information sharing and work on issues of mutual interest. Collaboration among regional economic communities should therefore be considered to enhance the protection of critical infrastructure in Africa.

Communication infrastructure is considered a CI. Consequently, 5G is critical national infrastructure and will manage other critical infrastructure sectors. With growing concern over China’s technological dominance globally and particularly in

Africa, the decisions of operators to partner with particular vendors will depend on a country's risk appetite.

Standards enable interoperability of systems and networks and are therefore an integral part of protection of critical infrastructure. Consequently, proposals made by China at the International Telecommunications Union (ITU) for standards development in a new Internet Protocol ('New IP') and facial recognition systems in visual surveillance could have a significant impact on the security and protection of critical infrastructure, especially the consideration of smart cities and communities in Africa.

14. Conclusion

Congratulations, you have reached the end of the module. In the concluding part, we will reflect on the key takeaways from this module, leaving some additional space for you to write down the points which seem important to you and are not included above.

As more government and private sector run infrastructure goes online to improve efficiency and integration, security considerations for the protection of these infrastructures, embedded in strategy, policy and legislation is imperative.

In this module, through the exploration of definitions and methodologies of identification of critical critical Infrastructure (CI) and Critical Information Infrastructure (CII), we have appreciated differences between international, regional and national perspectives. We have considered the policy, legislative, and regulatory guidelines are necessary for the identification of resources and the creation of governance frameworks for CI and CII protection. Finally, we have briefly discussed the geopolitical issues that African countries need to keep in mind when drawing up and implementing CI and CII protection policies.

Reflection: Important Points

Write down 5 important points that are important to you and are not included in this module.