KM2: CYBERSECURITY STRATEGY, POLICY AND REGULATION

KNOWLEDGE MODULE OBJECTIVE

Welcome to the knowledge module on cybersecurity strategy, policy and regulation. This module provides a guide to developing national strategies in cybersecurity to support national goals. In this module you will also learn about two of the key levers for implementing strategies: legislation and regulation. The module is delivered using case studies and available best practices in the area.

Upon finishing this module, you should be able to address and find additional resources to the following issues:

- Does a country need a national cybersecurity strategy and what should it contain?
- What sources of information and support are able to assist with national strategy development?
- What levers does a government have to make sure the strategy is implemented?
- What is the role of legislation and regulation and how is it developed?
- What sources of information and support are able to assist with legislation and regulation?
- How have some African countries approached the development of strategies and what are the lessons available from these approaches?
- How to monitor and evaluate the implementation of strategies?
- When do you start another strategy lifecycle?

INTRODUCTION

The increased reliance on digital technology globally comes with risks and threats. A cybersecurity strategy is a high level document designed to address the risks and issues associated with the use of digital technologies. Developing a national cybersecurity strategy has the benefit of providing certainty in cybersecurity governance, which will in turn increase trust for those using digital technologies and provide tools, policies and guidelines to manage risks.

Once the strategy has been developed, the responsibility for coordinating its implementation lies with the government. Successful implementation of strategies depends on application of various levers available to governments and understanding how the levers can best be used to bring about the desired outcomes.These levers and how governments can use them are usually described in the strategy.

Legislation and regulations are two of the most effective levers governments and their agencies can adopt in implementing functional strategies. These levers can create institutions, establish relationships and assign responsibilities necessary for the successful implementation of the strategies. The focus and manner of developing use of the legislations and regulations may vary between countries based on priorities and other existing legal frameworks. This module will provide a guide as to how to think through the options a government has and consider how legislation or regulation could be developed to achieve the goals in its strategy.

WHAT IS A NATIONAL CYBERSECURITY STRATEGY

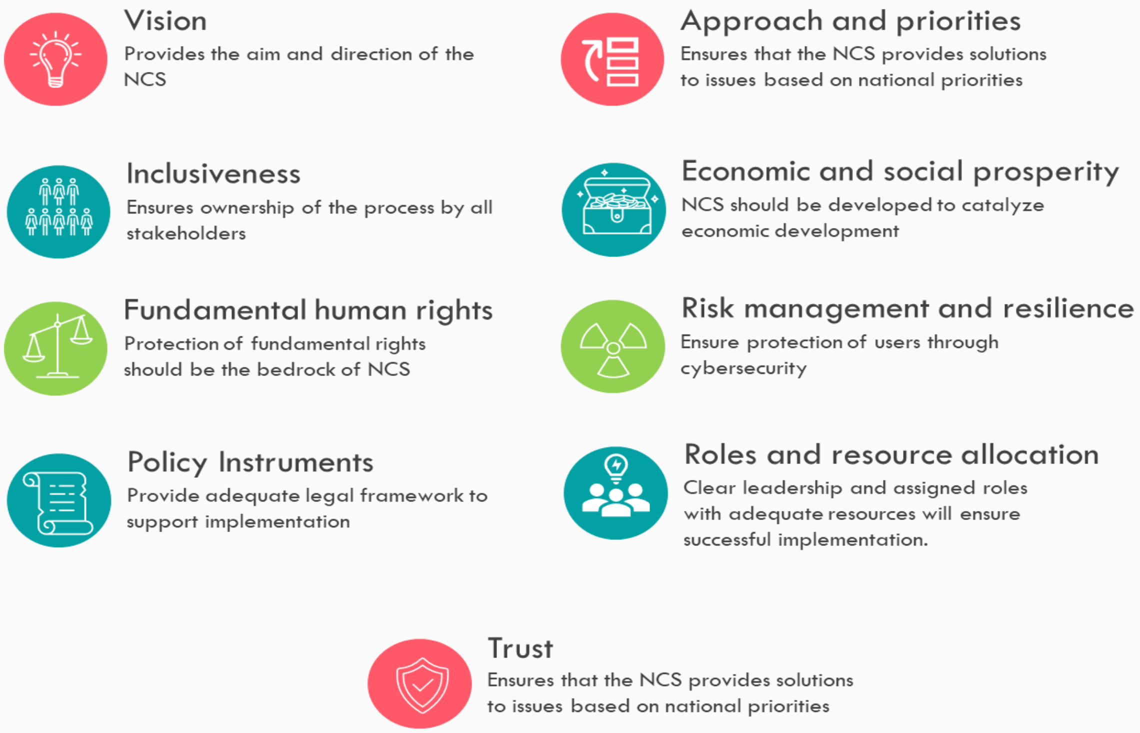
The European Union Agency for Cybersecurity (ENISA) defines a National Cybersecurity Strategy as ‘a plan of actions designed to improve the security and resilience of national infrastructures and services’. It is a high-level top-down approach to cybersecurity that establishes a range of national objectives and priorities that should be achieved in a specific timeframe. It can also be described as a careful plan or method of protection for both informational and non-informational assets through the ICT infrastructure for achieving particular national goals usually over a long period of time (Azmi et al.).

Usually, National cybersecurity strategies are high-level, stakeholder-oriented country-owned plans that governments use to describe issues such as:

- The vision, high-level objectives, principles and priorities that will guide the country in addressing cybersecurity;
- An overview of the stakeholders tasked with improving the cybersecurity of the nation and their respective roles and responsibilities; and
- The steps, programmes and initiatives that a country will undertake to protect its national cyber-infrastructure and, in the process, increase its security and resilience.

[Source: *Guide to developing a national cybersecurity strategy* - (International Telecommunication Union (ITU) et al. 2018, 13)]

The aim of developing the NCS is not strictly for cybersecurity only. It can also serve as a tool for economic development. There are various phases and activities that would form part of developing and implementing a national cybersecurity strategy. These activities and outcomes are usually referred to as the lifecycle of the strategy. We will discuss this later in the text. The International Telecommunications Union (ITU) Guide to developing national cybersecurity strategies, identifies nine guiding principles that should help officials and stakeholders throughout the strategy development lifecycle. These principles are not limited to any phase of the cycle and should be taken together as a whole because they apply to all key focus areas of the NCS. These principles are depicted in the diagram below.



Vision
Provides the aim and direction of the NCS

Approach and priorities
Ensures that the NCS provides solutions to issues based on national priorities

Inclusiveness
Ensures ownership of the process by all stakeholders

Economic and social prosperity
NCS should be developed to catalyze economic development

Fundamental human rights
Protection of fundamental rights should be the bedrock of NCS

Risk management and resilience
Ensure protection of users through cybersecurity

Policy Instruments
Provide adequate legal framework to support implementation

Roles and resource allocation
Clear leadership and assigned roles with adequate resources will ensure successful implementation.

Trust
Ensures that the NCS provides solutions to issues based on national priorities

Figure 1. A graphic outline of the Guiding Principles of the NCS process.

Reflection Point
Do you know any National Strategy from your country in area or subject matter? If yes, kindly look at its structure.

CYBERSECURITY STRATEGIES IN AFRICA

Generally, African countries have made little progress in developing and implementing national cybersecurity strategies. Recent information indicates that only 17 of Africa's 54 countries have completed a national cybersecurity strategy, which is less than half the global average as the map below indicates.

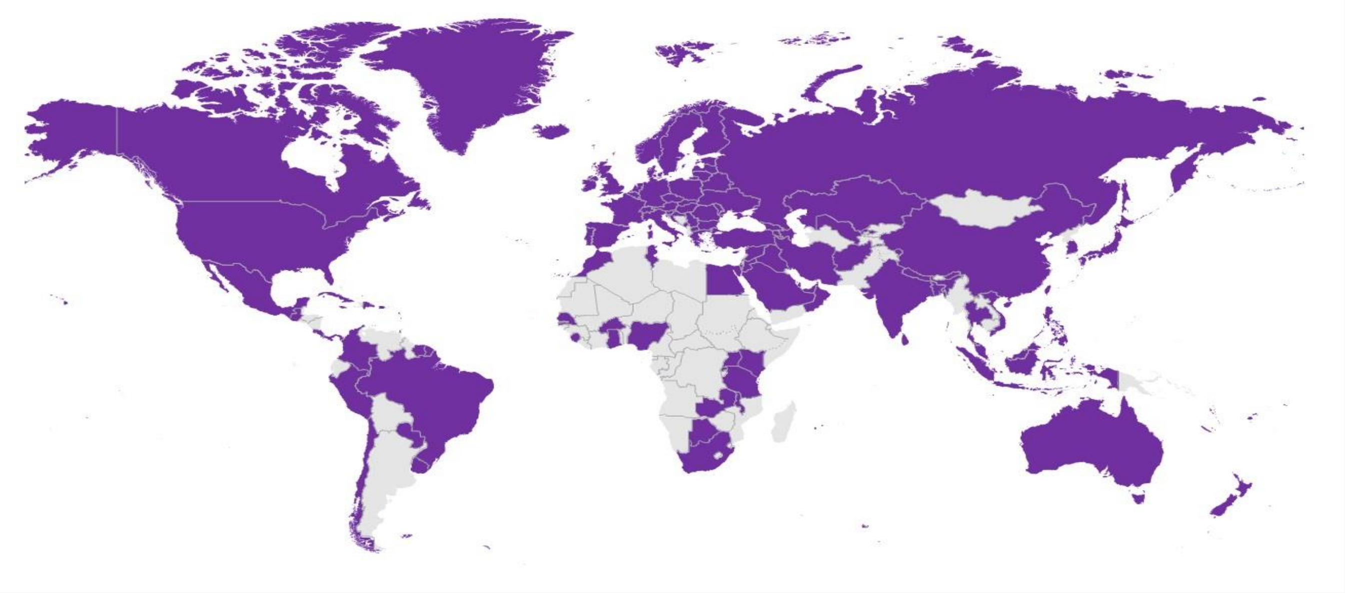
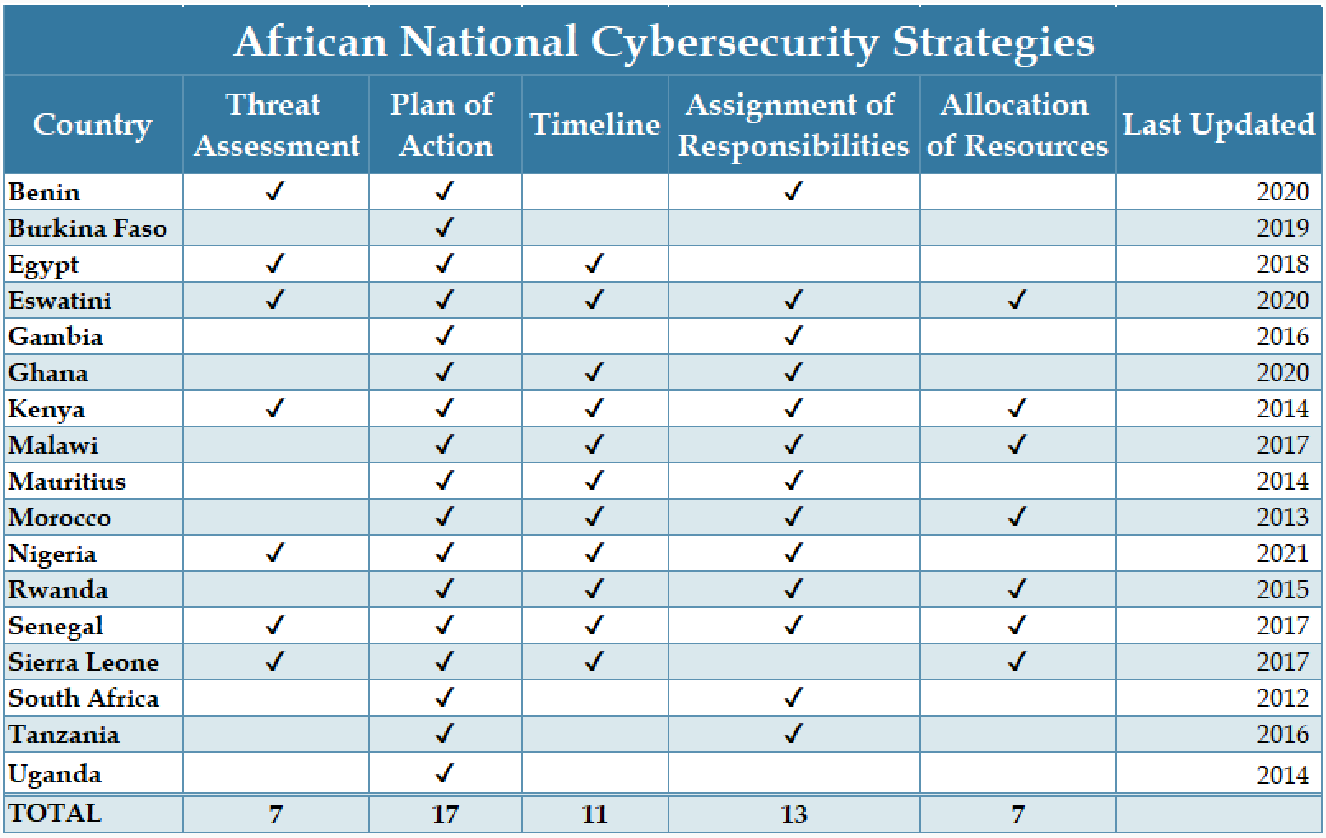


Fig. 2 A depiction of countries with NCS
Source: ITU National Cybersecurity Strategies Repository

The countries in Africa with cybersecurity strategies are at various levels of development and implementation. The table below indicates the status of these strategies.



African National Cybersecurity Strategies

Country	Threat Assessment	Plan of Action	Timeline	Assignment of Responsibilities	Allocation of Resources	Last Updated
Benin	✓	✓		✓		2020
Burkina Faso		✓				2019
Egypt	✓	✓	✓			2018
Eswatini	✓	✓	✓	✓	✓	2020
Gambia		✓		✓		2016
Ghana		✓	✓	✓		2020
Kenya	✓	✓	✓	✓	✓	2014
Malawi		✓	✓	✓	✓	2017
Mauritius		✓	✓	✓		2014
Morocco		✓	✓	✓	✓	2013
Nigeria	✓	✓	✓	✓		2021
Rwanda		✓	✓	✓	✓	2015
Senegal	✓	✓	✓	✓	✓	2017
Sierra Leone	✓	✓	✓		✓	2017
South Africa		✓		✓		2012
Tanzania		✓		✓		2016
Uganda		✓				2014
TOTAL	7	17	11	13	7	

Fig. 3. Africa Cybersecurity Strategies
Source: Africa Centre for Strategic Studies, Article on 'Africa Lessons on Cyber Strategy'

Unfortunately, the existence of a document called a national cybersecurity strategy is not sufficient to address cybersecurity issues on a national scale. The relevant issue is its implementation and impact on the country. The article on Africa's lessons on cyber strategy (Ajijola and Allen), identifies the strategies of three countries it considers to have met the minimum essential criteria in Africa. They are Eswatini, Kenya and Senegal. The criteria include:

- A threat assessment that identifies the scope and scale of a country's cyber threats
- A plan of action that contains concrete goals and activities intended to address the threats
- A timeline
- An assignment of responsibilities across key stakeholders
- Clear provisions that allocate resources

The Eswatini Cybersecurity Strategy clearly defines the scope of the strategy which would cover all sectors of the country and provide guidelines to all relevant stakeholders on their expected roles and responsibilities. The strategic context identified the threats and vulnerabilities, while the capacity review provided the current status of cybersecurity in the country.

The strategy also described its alignment with the national goal of the country and sets out its own goals to include; enhance security and resilience; strengthen the cybersecurity governance, policy, regulatory and legislative frameworks; build Eswatini's capacity and expertise in cybersecurity; foster a safe and secure information society for Eswatini; and strengthen cooperation, collaboration and partnerships on cybersecurity. The strategy also assigns roles and responsibilities for implementation, including a monitoring and evaluation framework.

The same model is adopted for Kenya and Senegal. One of the strategic success factors in developing and implementing a national cybersecurity strategy is the need for inclusiveness, which would provide the necessary resources for crafting and implementation.

Reflection Point
Why do you think most African countries are yet to develop national NCSS?

BENEFITS AND USES OF CYBERSECURITY STRATEGY

There are various benefits a country may gain when developing a cybersecurity strategy. The primary benefit would be that a country is likely to achieve better cybersecurity outcomes with a strategy than without one. Because the cybersecurity strategy provides measures and plans for addressing threats arising from the use of digital technologies, it serves as a confidence building measure that supports the use of digital technologies to attain economic development. It also provides a framework for international cooperation in addressing global issues regarding cybersecurity.

Other benefits of a cybersecurity strategy are that it can help:

- Decide how cybersecurity can support higher level national goals, such as economic growth, defence, education, safety for its citizens etc.
- Prioritise cybersecurity effort and investment.
- Create a roadmap or action plan to get from the current state to the country's desired cybersecurity readiness and capability.
- Ensure that the national approach to cybersecurity reflects its national values.
- Improve communication and cooperation among the wide number of ministries and agencies involved in cybersecurity.
- Clarify or change the responsibilities of those ministries and agencies.
- Direct that new institutions or agencies be created.
- Set targets for ministries and agencies, with a reporting process so that ministers and officials can monitor progress and identify problems early.
- Improve cooperation between government ministries and key organisations from the outside government in the private sector and civil society needed to implement the NCSS and improve national cybersecurity.
- Encourage support for the national cybersecurity effort by involving companies, civil society and even citizens in deciding the strategy priorities and how its goals are to be achieved.

The categories for using NCSS can be divided into three major areas (Azmi et al.). The first major area is for National Security. Under this, strategies are used primarily as tools to reduce cyber threats to critical national infrastructure by strengthening national resilience for CNI and protecting state secrets. In some instances, it could also serve as a tool to promote economic security and prosperity. Secondly, the strategy could serve a jurisprudential purpose as it may be a requirement of other policy documents or laws. It could also be a mandate of the government agency required by law. Thus the creation of the NCSS meets the requirement as required by law or other policies. Thirdly, it can be used to achieve political needs. Sometimes it becomes imperative as part of the political drive to create NCS. In the modern era of digital diplomacy, NCS could serve as a diplomatic tool for engaging resources for further development and promoting a country's image.

Case Study: Ghana

- 2008 establish the National Information Technology Agency
- 2015 publish NCSS. The strategy directed that four new institutions be created: National Cyber Security Council; National Cyber Security Center; National CSIRT; and the National Cyber Security Policy Working Group.
- 2018 establish National Cyber Security Center
- Enacted the Cybersecurity Act, 2020 (Act 1038) to regulate cybersecurity activities in Ghana

PHASES OF DEVELOPING AND IMPLEMENTING A NATIONAL STRATEGY

There are various phases and activities that would form part of developing and implementing a national cybersecurity policy and strategy. We refer to this as the lifecycle of the policy and strategy. The NCS guide recommends the following model for policy and strategy lifecycle stages:

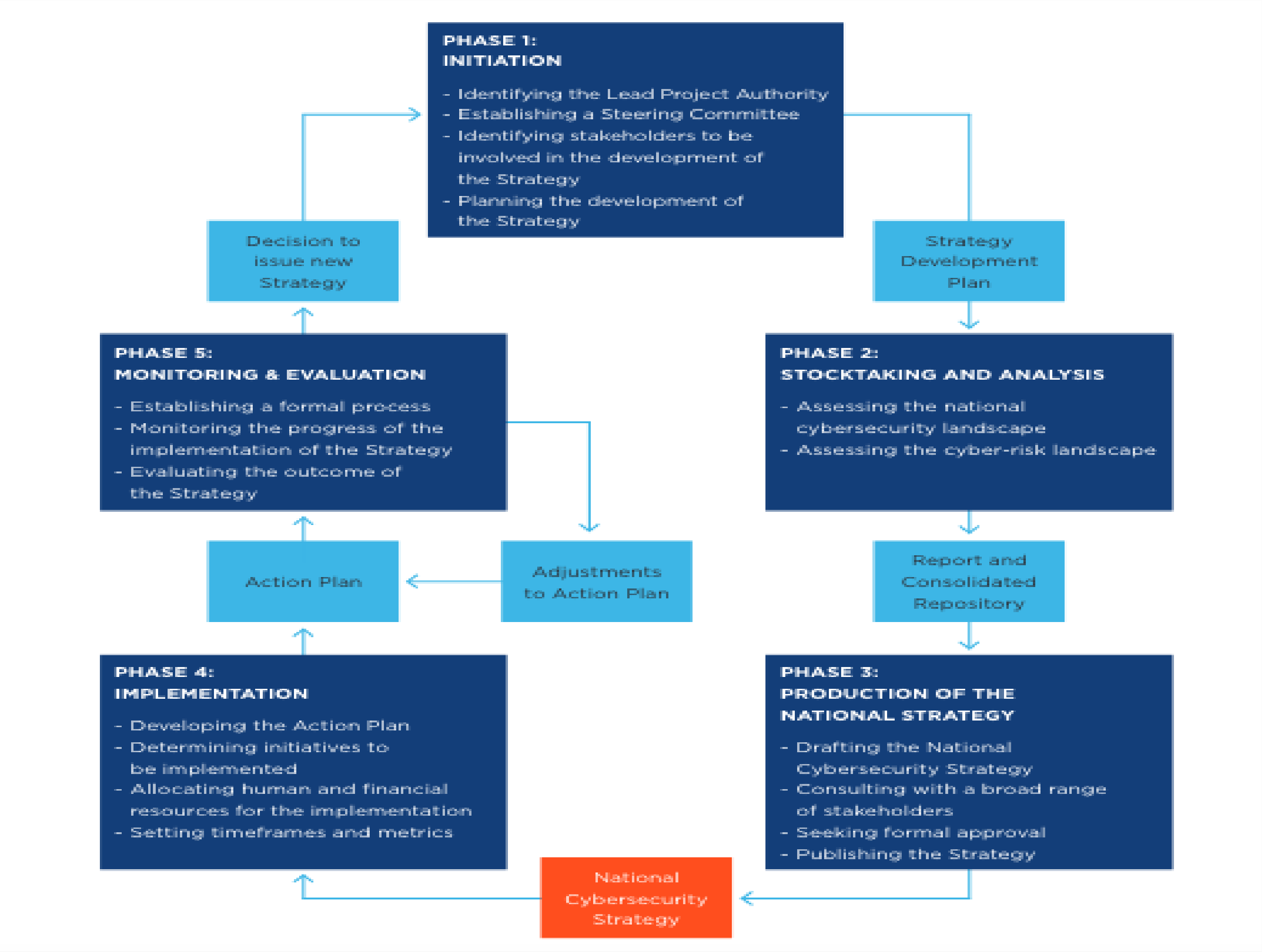
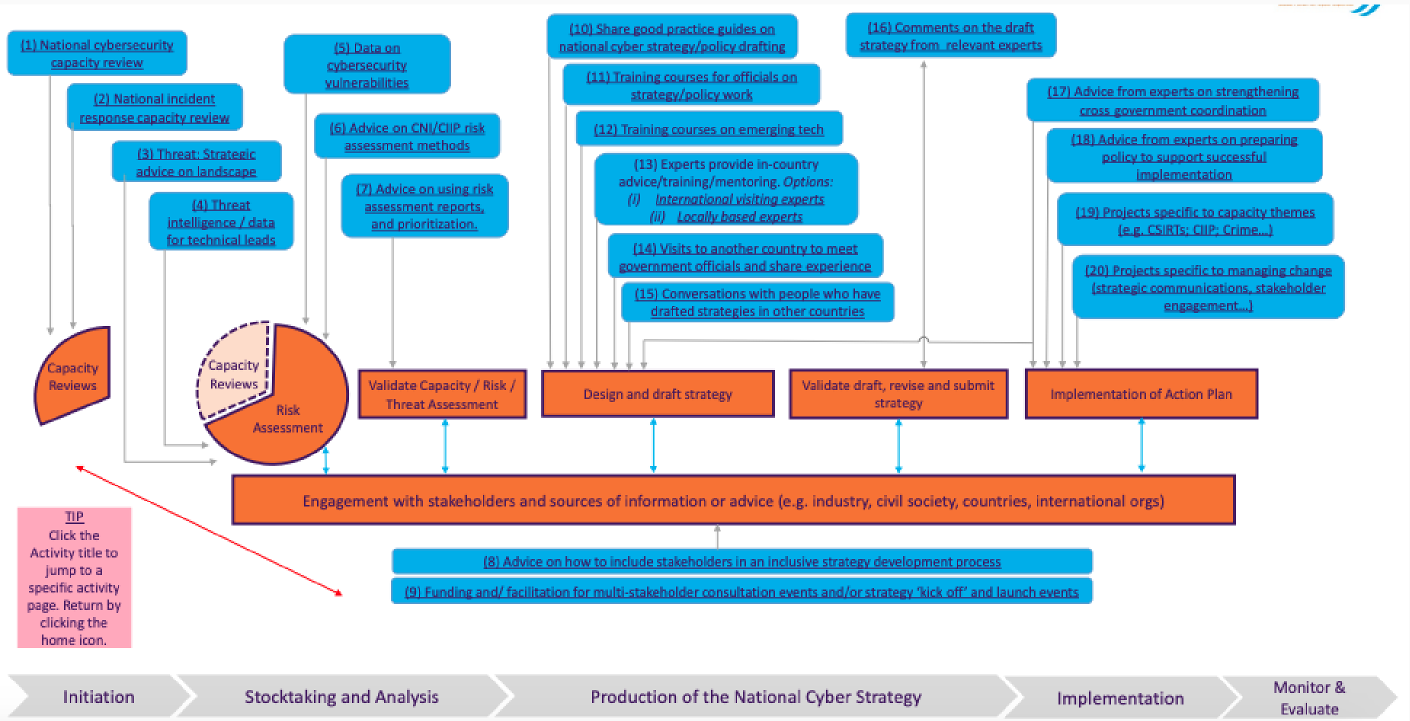

PHASE 1: INITIATION
- Identifying the Lead Project Authority
- Establishing a Steering Committee
- Identifying stakeholders to be involved in the development of the Strategy
- Planning the development of the Strategy
Strategy Development Plan
PHASE 2: STOCKTAKING AND ANALYSIS
- Assessing the national cybersecurity landscape
- Assessing the cyber-risk landscape
Report and Consolidated Repository
PHASE 3: PRODUCTION OF THE NATIONAL STRATEGY
- Drafting the National Cybersecurity Strategy
- Consulting with a broad range of stakeholders
- Seeking formal approval
- Publishing the Strategy
National Cybersecurity Strategy
PHASE 4: IMPLEMENTATION
- Developing the Action Plan
- Determining initiatives to be implemented
- Allocating human and financial resources for the implementation
- Setting timeframes and metrics
Action Plan
Adjustments to Action Plan
PHASE 5: MONITORING & EVALUATION
- Establishing a formal process
- Monitoring the progress of the implementation of the Strategy
- Evaluating the outcome of the Strategy
Decision to issue new Strategy

Figure 4. A depiction of the entire NCS process and life cycle.

When a country considers developing NCSS, there are various opportunities for international assistance throughout the strategy lifecycle. The GFCE has illustrated the types of assistance that a country can call upon in its *Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle* This Catalogue offers examples of 20 activities that could go into a project supporting a country's NCS cycle. We advise that the catalogue should be used as a reference document to understand the support that is available to countries with examples provided through case studies.


(1) National cybersecurity capacity review
(2) National incident response capacity review
(3) Threat: Strategic advice on landscape
(4) Threat intelligence / data for technical leads
(5) Data on cybersecurity vulnerabilities
(6) Advice on CNI/CIIP risk assessment methods
(7) Advice on using risk assessment reports, and prioritization.
(10) Share good practice guides on national cyber strategy/policy drafting
(11) Training courses for officials on strategy/policy work
(12) Training courses on emerging tech
(13) Experts provide in-country advice/training/mentoring. Options:
(i) International visiting experts
(ii) Locally based experts
(14) Visits to another country to meet government officials and share experience
(15) Conversations with people who have drafted strategies in other countries
(16) Comments on the draft strategy from relevant experts
(17) Advice from experts on strengthening cross government coordination
(18) Advice from experts on preparing policy to support successful implementation
(19) Projects specific to capacity themes (e.g. CSIRTs; CIIP; Crime...)
(20) Projects specific to managing change (strategic communications, stakeholder engagement...)
Capacity Reviews
Capacity Reviews
Risk Assessment
Validate Capacity / Risk / Threat Assessment
Design and draft strategy
Validate draft, revise and submit strategy
Implementation of Action Plan
Engagement with stakeholders and sources of information or advice (e.g. industry, civil society, countries, international orgs)
(8) Advice on how to include stakeholders in an inclusive strategy development process
(9) Funding and/ facilitation for multi-stakeholder consultation events and/or strategy 'kick off' and launch events
TIP
Click the Activity title to jump to a specific activity page. Return by clicking the home icon.
Initiation
Stocktaking and Analysis
Production of the National Cyber Strategy
Implementation
Monitor & Evaluate

Before or during the **Initiation** of a national strategy, a country can benefit from capacity/capability reviews covering the overall national situation and/or focusing on specific capabilities such as national incident response.

Once the strategy development process has been initiated - often through political direction from a minister – the phase of **Stocktaking and Analysis** begins. One of the most important things for a country to explore in this phase is its cyber risks and the threats and vulnerabilities that feed into those risks. The assistance of international partners can be requested to help understand these risks. Projects might provide advice on, among other things, the strategic risk landscape, threat intelligence data, data on national cybersecurity vulnerabilities or methodologies for assessing the cyber risk to Critical National Infrastructure. This stocktaking can gather a lot of data and assessments, so countries can also request assistance with bringing all this information together, prioritising it and using it to draw out some insights that will inform the strategy drafting.

If it hasn't already begun, the Stocktaking and Analysis phase is a good time for governments to begin or increase their communication and collaboration with external stakeholders in the NCSS. These stakeholders typically include the private sector, universities, think tanks, NGOs, the media and ultimately, the country's public. International assistance can provide advice on involving these stakeholders in the strategy lifecycle and facilitate events with stakeholders to discuss the strategy.

Having gathered and analysed information and begun consulting stakeholders, a country can move to the Producing the National Strategy phase. One of the quickest ways to benefit from international assistance when entering this phase is to read the good practice and lessons learned guides on national strategy/policy drafting. The *Guide to developing a national cybersecurity strategy* is one source that has already been mentioned, but there are others, such as the *National Cybersecurity Strategies: Lessons Learned and Reflections from The Americas and Other Regions* by the Organization of American States. The Cybil Portal contains a repository of such guides.

Besides reading good practice guides, it can also help to converse with officials in other countries who have produced national strategies. An additional benefit is that it can create or strengthen working-level networks between countries that can be useful when implementing the strategy. These conversations can happen remotely, but they can also be conducted in person during visits to other countries.

There are options for more intense learning and knowledge sharing on strategy development that go beyond conversations and visits. One option is to send officials to training courses related to cybersecurity strategy and policy or key issues within the strategy, such as emerging technology. Another is to bring in international or local experts to provide independent advice and support to the strategy production. While asking such experts to write the strategy is not good practice, it is common to invite experts outside the government to assist. Such experts can also help strengthen the coordination and collaboration across government on strategy development, for example, by facilitating inter-ministry workshops.

Once officials have prepared a draft of the strategy or chapters within it, they can invite independent experts to provide feedback confidently. Having considered feedback from experts and the stakeholder consultations, officials will amend the draft so that it is ready for consideration by ministers, and their approval and adoption.

It is a good practice for an NCSS to be accompanied by an action plan to guide its implementation. An Action Plan describes in greater detail what actions are required by the strategy, who is responsible for them, when they will be done and what indicators will be used to monitor that the action was successfully completed.

The lifecycle of a strategy does not finish when it is adopted. The next phases are to **Implement** the strategy and to **Monitor and Evaluate** it. After a few years, this will usually be followed by a strategy refresh being initiated and the cycle starts again.

During the strategy implementation, international assistance is available to support cyber capacity building in many different areas, including: incident response; CNI and Critical Information Infrastructure Protection; tackling cybercrime; public awareness; workforce skills; standards; and cyber diplomacy. Officials can also assist in developing national cybersecurity policies and cybercrime that sit under the strategy.

THE LEVERS TO DRIVE STRATEGY IMPLEMENTATION

A government has a range of levers to drive the implementation of its NCSS. As we will discuss later in the module, two of these are legislation and regulation, but they are not the only ones. Which levers a government chooses to use, and how, will depend upon its national circumstances and approach to policy.

The levers available to a government include:

- Create standards and tools related to cybersecurity to enable certainty and ease in cybersecurity activities. Examples: establishing a certification scheme to make it easier for companies to choose secure or capable suppliers; creating an online tool that any company, organisation or agency can use to check the security of its website; creating information sharing mechanisms and communities of trust.

- Provide knowledge and education to organisations and citizens. Examples: public awareness campaigns; education curricula; giving cybersecurity guides/toolkits to small businesses; circulating vulnerability and threat alerts from a National CSIRT or Cybersecurity Centre.

- Provide rewards or incentives for good cybersecurity. Examples: using government procurement policy to buy IT services from companies with cybersecurity certificates, which incentivise them to complete certification.

- The government leads by example by practising cybersecurity. Examples: the government can begin to roll out better cybersecurity approaches (e.g. two-factor authentication logins or email authentication) by adopting them first in ministries and publicising this to the industry.

- Applying pressure without criminalising. Example: producing 'worst performers' lists for implementing a particular recommended cybersecurity practice that they should be implementing – these might be published or shared just with the companies concerned.

- Government investment and Public Private Partnerships. For example where governments and the private sector share information on vulnerabilities in CNI to adequately address the vulnerabilities through collaboration.

- Funding academic research.

In addition to the above levers, a government has legislation and regulation, which has many uses including:

- Give new roles, powers or authorities to a government agency or an external body that the government has tasked with fulfilling a national cybersecurity role;

- Create a new agency or organisation;

- Make companies, other organisations or citizens responsible for taking certain actions the government wants to promote (e.g. protecting data in a defined way or reporting breaches); and

- Making it an offence to commit acts that the government wants to deter.

The levers available to a government can be viewed on a scale from strong encouragement (the 'carrot') at one end to strong deterrence (the 'stick') at the other.

Case Study for Encouragement Lever:

1. The SME Toolkit in Nigeria
2. Cybersecurity awareness in Ghana
3. Africa CERT is a good example of governments and private sector collaborating across the African Continent.

ROLE OF LEGISLATION AND REGULATION

Every country has a unique approach to legislation and regulation. From a procedural perspective, legislation is produced by a legislature (e.g. the parliament), while regulation (aka secondary legislation, delegated legislation or subordinate legislation) is issued by the bureaucracy. However, whether a particular cybersecurity direction needs to be issued in the form of legislation or regulation depends upon each country's political and legal tradition.

Furthermore, countries are not the only source of cybersecurity regulation: it can also come from higher level international bodies. For example, the World Forum for Harmonization of Vehicle Regulations adopted UN Regulations on software cybersecurity in vehicles in 2020. In the African context, the African Union (AU) adopted the Convention on Cyber Security and Personal Data Protection—also known as the Malabo Convention, in 2014. This was followed by the release of the Personal Data Protection Guidelines for Africa, a collaborative measure between the Internet Society and the AU in 2018.

In many cases, national governments are free to choose whether they adopt internationally negotiated regulations into their domestic law and regulations. However, governments may have already agreed to adopt all the regulations issued by a particular international body. There are also strong economic incentives to adopt international industry standards: for example, if a country wants to export cars, its companies must follow international standards for car safety.

One way to simplify the approach to legislation and regulation is to start with the national strategy. The strategy should set the national vision and goals for cybersecurity. When producing the strategy, officials consider what legislation and regulation will be needed to achieve these goals and whether there are any gaps or weaknesses in the legal and regulatory framework that already exists. Where there are large gaps or big changes needed, then the strategy can direct that these be addressed, for example, by tasking a ministry with preparing and presenting to parliament a draft law by a certain date.

The *Guide to developing a national cybersecurity strategy* describes several elements of the legal and regulatory framework that an NCSS might give direction on:

- defining what constitutes illegal cyber-activity;
- legal recognition of individual rights and civil liberties;
- institutionalising critical entities and agencies;
- establishing compliance mechanisms that prevent, combat and mitigate actions directed against the confidentiality, integrity and availability of ICT systems, infrastructures and data – these mechanisms may include, among other things, procurement rules, information-sharing programmes, vulnerability disclosure, minimum standards of care, security baselines and certification programs; and
- international cooperation on cybercrime and cybersecurity matters.

(Source: *Guide to developing a national cybersecurity strategy*, p.40,46)

PROCESS FOR DEVELOPING LEGISLATION AND REGULATION PART 1 (STRATEGY TO POLICY)

Having identified legislation and regulation as some of the levers a government may deploy to implement a national strategy, it is necessary to discuss the process of converting the objectives into legislation. The process for developing legislation and regulation varies a lot between countries. This section will outline a generic approach that can be applied in most countries.

As mentioned earlier in the text, NCSS is a document containing the vision, high-level objectives, principles and priorities that will guide the country in addressing cybersecurity. In most instances, the subject that requires leveraging through legislation has been identified in the NCSS. Thus the strategy development process should have produced a prioritised list of cybersecurity issues that need to be addressed by the government.

Based on these priority areas, and objectives, the standard practice is to break down the objectives and priority areas into policy directions that would form the basis of legislation or regulations. This can be done either in the strategy development process, or during the years between strategy drafting and implementation. Some countries appoint a Cybersecurity Policy Group that consists of experts from within (and sometimes outside) the government to advise what the areas of policy should be and the policies' content. In Ghana, it was the National Cyber Security Working Group, while in Nigeria, it was called the Nigerian Cybercrime Working Group.

Some possible policy areas would include cybercrime prohibition, Data protection, cybersecurity in key sectors (e.g. energy; finance; e-government; health), technology assurance, education, workforce and awareness. The ‘Double Decision Diamond’ described in *National Cybersecurity Strategies: Lessons Learned and Reflections from The Americas and Other Regions* is a tool that can help move from strategic objectives to policy initiatives (and thereby policy areas). Some of the typical cybersecurity issues that would need to be addressed would include cybercrime, personal data protection, protection of critical networks, sector-specific regulations; for example, finance; energy; health, product-specific regulation for example, devices, aeroplanes, cars, electronic transactions, digital signatures, cybersecurity standards certification of companies/organisations among others.

The next step after identifying a key policy area, a government will typically decide to develop a corresponding policy. It is in this policy that the government will decide which levers to use to implement the policy and whether legislation or regulation should be among them. Policy development typically begins with ministerial direction, to set the framework and timeline, and then consultation, which can be informal or formal.

Informal consultation can occur before ‘pen is put to paper’. A good time to begin informal consultation is when the NCSS is being produced, but consultation should not be put off simply because there isn’t a strategy being drafted. The informal consultation helps officials produce the framework of ideas on the problem and policy solutions that can be discussed with ministers and put into a formal consultation process.

Formal consultation will typically involve the publishing of documents upon which stakeholders can provide feedback. In South Africa, for example, policy development follows a common approach to consultation, using two rounds of documents known as papers. The first round is based on a discussion document called a Green Paper. The Green Paper expresses the position of the government on a particular issue. It is published with a request for public comments. Sometimes, the Green Paper is followed by a more refined discussion document, called a White Paper. The white paper is a broad government policy statement and may invite additional public comments on the issue. The relevant parliamentary Committees may propose amendments or other proposals and then send the policy paper back to the Ministry for further discussion and final decisions.

The consultation process will break stakeholders into groups based on characteristics or interest levels and engage with each differently. One of the most important groups will be the technical experts with deep knowledge and experience in policy. Some of these experts may already be within the government, but they often work outside it in universities, companies or civil society organisations. Advice for consulting and working with stakeholders in cybersecurity can be found in '*A Short Guide to Stakeholder Engagement on National Cybersecurity Strategy Development*' *(Weisser Harris et al. 2022).*

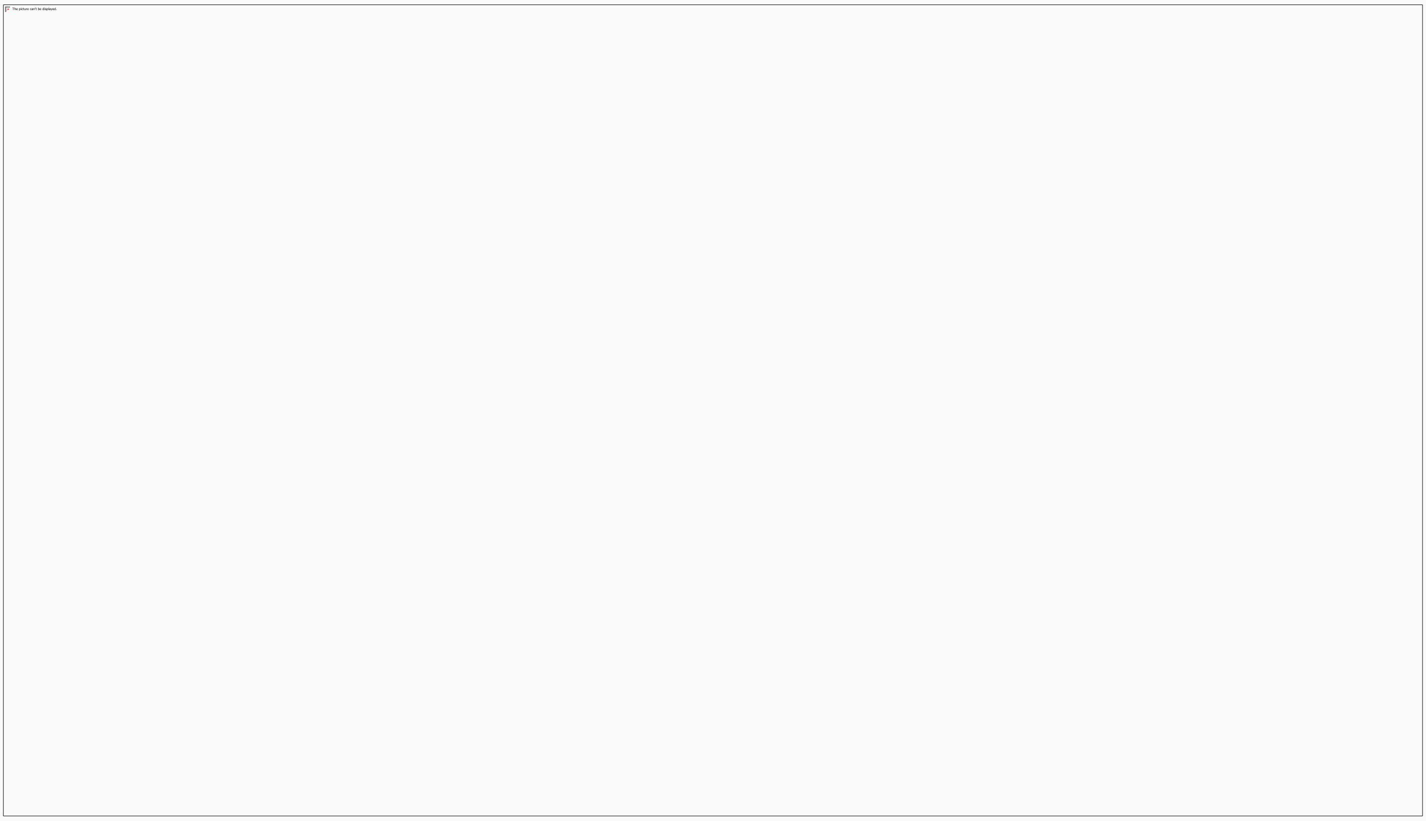


Figure 6. Various ways for stakeholder consultation and engagement.

A Minister or the Cabinet will approve a final policy position at the end of the policy development process. It is good practice to publish this, as South Africa does with its White Papers (referenced above). In Nigeria, such policies are approved by the Federal Executive Council, a council of all Ministers of the Federal Government chaired by the President.

Many policies require legislation or formal regulation to support or drive their implementation. Sometimes the nature of a policy issue determines the type of lever to apply in its implementation. For example, it would be more suitable to use legislation to address cybercrime issues, typically activities that need to be prohibited and treated like crimes as distinct from policies that aim to regulate specific sectors or cybersecurity-related activities such as data handling and digital security measures.

A policy to tackle cybercrime will always require primary legislation to define rights and responsibilities in civil law, and crimes and punishments in criminal law (substantive law). It will also require primary legislation to define how cybercrimes are processed through the judicial system (procedural law). More information on this is contained in the Cybercrime Knowledge Module.

In contrast, policies that seek to regulate a sector or a type of cybersecurity-related activity, such as data handling, will require regulation, which may or may not require new primary legislation. Please note that sometimes, legislation and regulations may be related. There are three main ways in which regulation can relate to primary legislation:

1. The regulation is issued via primary legislation. Example: South Africa's Protection of Personal Information Act (POPIA) No. 4 of 2013.

2. The regulation is issued by a ministry/agency/organisation that already has the authority to do so. No new primary legislation is needed. Example: The Nigerian Data Protection Regulation, 2019 ('NDPR') was issued by the National Information Technology Development Agency ('NITDA').

3. Primary legislation is needed to give an existing body a new authority to issue regulations or to create a new body with this authority. Example: Kenya's Data Protection Act (DPA) 2019 established the Office of the Data Protection Commissioner (ODPC), which, together with a regulatory Task Force, had the mandate to create regulation under the DPA, which it subsequently did in the Data Protection Regulations 2021.

The process for developing cybercrime legislation is described in the Cybercrime Knowledge Module. The process for developing regulation is described in the next section.

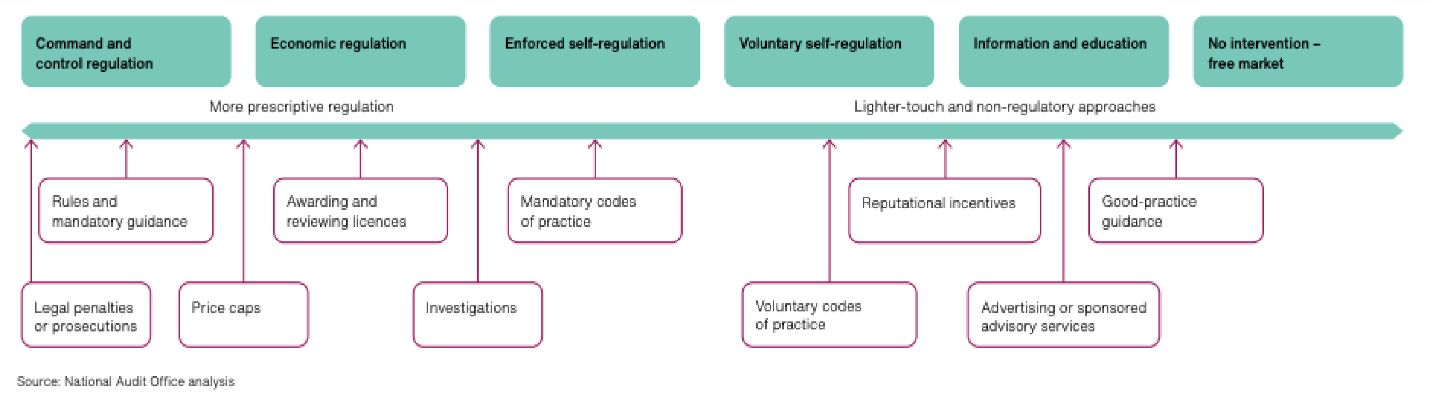
PROCESS FOR DEVELOPING LEGISLATION AND REGULATION PART 2 (POLICY TO REGULATION)

In the previous sections, we discussed the transition from strategy objectives to policy. We also mentioned various areas that would be best addressed by legislation and others that the use of regulation may be better leveraged to address implementation. This section will provide an overview of how policy directions can be transformed into regulations.

The technical task for officials producing regulation is to convert policy aims and ideas into a detailed set of rules and processes. These rules and processes should be geared to achieve the goals that the policy direction has proposed. The primary issue at the beginning is determining the kind of regulatory approach that best addresses the policy objective. This is because there is a need to strike a balance between the use of regulation to control and restrict unacceptable activities in cyberspace, while not preventing the vast advantages derived from it.

When considering regulation, an early decision is the type of regulatory approach that will be followed. There is a range of options from heavy-touch to light-touch. The heavy-touch approach is best suited for issues that require restrictions in order to prevent damage or destruction. The light touch approach can be used where guidance is needed to attain a particular objective. Below is a diagram that depicts the spectrum of regulatory options from heavy-touch to light-touch.

.


Command and control regulation
Economic regulation
Enforced self-regulation
Voluntary self-regulation
Information and education
No intervention – free market
More prescriptive regulation
Lighter-touch and non-regulatory approaches
Rules and mandatory guidance
Awarding and reviewing licences
Mandatory codes of practice
Reputational incentives
Good-practice guidance
Legal penalties or prosecutions
Price caps
Investigations
Voluntary codes of practice
Advertising or sponsored advisory services

Source: National Audit Office analysis

Source: (National Audit Office of United Kingdom 2021, 8)

While there are no specific regulatory processes designed for cybersecurity regulations, there are various generic regulatory processes that can be adapted for use in cybersecurity regulations. A good example is the *UK NAO's 'Good practice guidance: Principles of effective regulation'.* This practice guidance recommends that the following regulation development lifecycle be applied to cybersecurity regulation.

Design • Defining the overall purpose of regulation • Setting regulatory objectives • Ensuring accountability • Determining the degree of regulatory independence • Deciding on powers • Determining a funding model • Designing organisational structure and culture	Analyse • Using information and data • Embedding the citizen perspective • Monitoring service provider compliance and incentives • Engaging with stakeholders • Ensuring capacity and capability • Adopting a forward-looking approach
Intervene • Developing a theory of change • Prioritising interventions • Drawing on a range of regulatory tools • Embedding consistency and predictability • Ensuring interventions are proportionate • Being responsive	Learn • Establishing governance processes • Measuring performance • Evaluating impact and outcomes • Engendering cooperation and coordination • Ensuring transparency

When developing regulation the government will consider what architecture is needed to oversee, maintain and enforce the regulation. Sometimes, primary legislation may make provisions on how the regulations made by a particular body should be implemented, thus recommending the architecture for such regulations. Typical levels in the architecture may include:

- Body(ies) to oversee the regulatory framework and monitor its implementation;
- Body(ies) to develop regulations on particular or several issues;
- Body(ies) to enforce or administer the regulation;
- The entities that are being regulated and need to follow the regulation; and
- The consumer or citizen or beneficiary who is protected by the regulation.

Sometimes, new entities may need to be created to implement and enforce a regulation or assign new enforcement power to an existing legal entity.

We should note that considerations for developing regulations should not be restricted to only domestic issues. Officials developing regulations will need to understand the international regulatory landscape for the relevant policy area. Within Africa, the AU Convention on Cyber Security and the Protection of Personal Data (aka Malabo Convention) has provisions relevant to regulating data protection and electronic transactions.

At the international level, there are good practice frameworks for cybersecurity that regulation can make use of, such as NIST and ISO. There are also a large number of national and sectoral regulations that companies must comply with, and governments should take account of when developing their regulation. For example, the EU's General Data Protection Regulation (GDPR) regulates the protection of data of the EU citizens and applies to organisations that handle that data even if they are outside the EU.

Governments can use regulations in other jurisdictions for ideas in their national regulation. For example, Egypt's Data Protection Law (Law No. 151 of 2020) contains many provisions similar to the EU's GDPR. (PWC 2020, 16) When companies have to follow a single process to comply with the regulations of multiple markets, it reduces their compliance costs and workload.

Case study
In 2016, the UK decided to use less interventionist policy levers. For example, focusing on educating the boards of companies rather than regulating them. When the UK reviewed their approach in 2022, it concluded that companies were improving their cyber risk management but not quickly enough to meet the changing threat, so it decided to shift towards "a more interventionist approach to utilising market incentives and regulations to quickly establish better practices". This illustrates how governments can keep their use of policy levers under regular review and change the balance of levers they use. [Source for this case study: (UK Department for Digital, Culture, Media and Sport 2022, section 4)]

SUPPORT FOR PRODUCING REGULATION

There are various sources to learn good practices for developing regulations which countries can draw from. The Organization for Economic Cooperation and Development (OECD) has produced over twenty years of guidance on the features of good regulation. It encourages countries to have their principles for good regulation, which many do and should be a reference point for those developing national cybersecurity regulations.

Researchers assessing the quality of regulation in the Digital Markets Act produced a framework of principles of good regulation – drawing on OECD and WEF guidance – that could be helpful to officials in a cybersecurity context. (Bauer et al. 2022, 6) The headline principles are:

1. Clear policy objectives based on solving a factual well-identified issue with proven intervention mechanisms
2. Clarity of compliance regulations
3. Proportionality and adaptability

Sources of cybersecurity-specific guidance and support for regulation development include:

- Capacity building training and advisory projects on regulations (e.g. Commonwealth Secretariat; ITU; Cyber4Dev).
- Some capacity building programs, especially the World Bank's, include support for sectoral regulation alongside investments in infrastructure (e.g. the Bank's Digital Malawi project).
- Regional workshops are held to discuss the harmonisation of regulation, such as the 2015 UNCTAD-ECOWAS West African seminar as part of E-Commerce Week.

MONITORING AND EVALUATION

The monitoring and evaluation phase should determine if the action plans are being implemented based on the agreed timelines and, where they are implemented, if they have the desired results. At this stage, there should be a formal process to determine if the implementation has met the goals of the NCS and to assess if there is a need to review it for the next cycle of the process. The activities under this are as follows:

1. Creating a formal process

To ensure that targets are met, there is a need to create a formal process for the monitoring of the implementation of the NCS and evaluating the outcomes to determine if the goals have been achieved. Most countries identify, or establish, an independent government entity which will monitor and evaluate the implementation process. In some instances, the entity coordinating the implementation of the NCS creates a monitoring and evaluation role to ensure that goals are met. The monitoring framework should have performance indicators which are specific, measurable, achievable, responsible, and time related.

2. Monitoring the implementation of the Strategy

Once the formal process for the monitoring and evaluation is created, the entity responsible for this should measure the implementation based on the agreed parameters. If there are any deviations from agreed timelines or reasons for failure to adhere to the goals set, this should be noted as it would serve as valuable input to future iterations of the strategy when the NCS is reviewed for another cycle. This approach will ensure that relevant stakeholders are held accountable for the responsibilities assigned to them for implementation.

3. Evaluating the outcomes of the Strategy

In addition to assessing the progress in implementation based on the agreed matrix, it is also necessary to evaluate the outcomes and compare them with the objectives set in the NCS. This will help determine if the objectives of the NCS are taking the country in the right direction. The assessment and associated recommendations should be compiled into a report for the Lead Project Authority, and include ways to update the Implementation Action Plan and ensure that it is current and responsive to the changing policy and the risk landscape.

FUNDING

Funding is another fundamental aspect of the implementation process. The traditional way of funding the implementation process is the allocation of funds from the government budget. This approach has its difficulties. Apart from the financial resources of most governments being low with competing interests, taking ownership of the process by the stakeholders should include innovative funding arrangements. This must be specifically addressed under the strategies and action plan. For example, in Nigeria, the Cybercrimes Act of 2015 provides that a certain percentage of fees should be charged on electronic funds transfers, and such fees are reserved to fund cybersecurity activities. Similarly, the National Cybersecurity Policy also suggests that a certain percentage of government agencies' budgets should be dedicated to cybersecurity activities.

Works Cited

Ajijola, Abdulhakeem, and Nate Allen. *African Lessons in Cyber Strategy*. 8 March 2022. *Africa Centre for Strategic Studies*, https://africacenter.org/spotlight/african-lessons-in-cyber-strategy/.

Azmi, Riza, et al. "Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy." *www.researchgate.com*, Research Gate, December 2016, https://www.researchgate.net/publication/308470260_Motives_behind_Cyber_Security_Strategy_Development_A_Literature_Review_of_National_Cyber_Security_Strategy. Accessed 25 November 2022.

International Telecommunications Union. *Guide to developing a national cybersecurity strategy*. ITU Geneva, 2018. *Guide to developing a national cybersecurity strategy*, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

Bauer, Matthias, Fredrik Erixon, Oscar Guinea, Erik van der Marel, and Vanika Sharma. 2022. "The EU Digital Markets Act: Assessing the Quality of Regulation." ECIPE. https://www.researchgate.net/publication/362092853_The_EU_Digital_Markets_Act_Assessing_the_Quality_of_Regulation.

International Telecommunication Union (ITU), The World Bank, Commonwealth Telecommunications Organisation (CTO), NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), and Commonwealth Secretariat. 2018. "Guide to Developing a National Cybersecurity Strategy." https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

National Audit Office of United Kingdom. 2021. "Good Practice Guidance: Principles of Effective Regulation." https://www.nao.org.uk/wp-content/uploads/2021/05/Principles-of-effective-regulation-SOff-interactive-accessible.pdf.

Organization of American States (OAS) and Global Partners Digital. 2022. "National Cybersecurity Strategies: Lessons Learned and Reflections from The Americas and Other Regions." https://cybilportal.org/wp-content/uploads/2022/08/National-Cybersecurity-Strategies.-Lessons-learned-and-reflections-ENG.pdf.

PWC. 2020. "Data Privacy in Egypt: What You Need to Know." https://www.pwc.com/m1/en/services/assurance/risk-assurance/documents/webcast-data-privacy-egypt-what-you-need-know.pdf.

UK Department for Digital, Culture, Media and Sport. 2022. "2022 Cyber Security Incentives and Regulation Review." UK Department for Digital, Culture, Media and Sport. https://www.gov.uk/government/publications/2022-cyber-security-incentives-and-regulation-review/2022-cyber-security-incentives-and-regulation-review.

Weisser Harris, Carolin, Daniela Schnidrig, Elizabeth Orembo, James Boorman, and Kerry-Ann Barrett. 2022. “A Short Guide to Stakeholder Engagement on National Cybersecurity Strategy Development.” Global Forum on Cyber Expertise. https://cybilportal.org/wp-content/uploads/2022/08/GFCE-NCS-Development-Stakeholder-Engagement-Paper.pdf.