STRATEGIC ENGAGEMENT IN CYBERSECURITY

Guide to Developing a National Cybersecurity Strategy

THIRD EDITION 2025

SOME RIGHTS RESERVED

ISBN 978-92-61-42081-9 (PDF English Edition)

This Guide was developed by thirty-seven Contributors from Intergovernmental and International Organizations, private sector, as well as academia and civil society and included the following organizations:

Accenture, African Union (AU), Arab League, Axon Partners Group, Commonwealth Telecommunications Organisation (CTO), Council of Europe (CoE), Cybercrime Research Institute (CRI), Cybersecurity Capacity Centre for Southern Africa (C3SA), Deloitte, DiploFoundation (Diplo), European Bank for Reconstruction and Development (EBRD), e-Governance Academy (eGA), European Union CyberNet (EU CyberNet), Experirē Strategy & Advisory, Forum of Incident Response and Security Teams (FIRST), Geneva Centre for Security Sector Governance (DCAF), Global Cyber Security Capacity Centre (GCSCC), Global Forum on Cyber Expertise (GFCE), Global Partners Digital (GPD), Hathaway Global Strategies LLC, Inter-American Development Bank (IADB), International Criminal Police Organization (INTERPOL), International Monetary Fund (IMF), International Telecommunication Union (ITU), KPMG, Microsoft, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), NRD Cyber Security, Organization of American States (OAS), United Nations Development Programme (UNDP), United Nations Interregional Crime and Justice Research Institute (UNICRI), United Nations Institute for Disarmament Research (UNIDIR), United Nations Office of Counter-Terrorism (UNOCT), United Nations Office for Disarmament Affairs (UNODA), United Nations Office on Drugs and Crime (UNODC), United Nations University (UNU), World Bank (WB), World Economic Forum (WEF), and the European Union Agency for Cybersecurity (ENISA) contributed to the Guide as observer. All the above-mentioned entities are hereinafter collectively referred to as "Contributors".

RIGHTS & PERMISSION

GENERAL DISCLAIMERS

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the International Telecommunication Union, the World Bank or any of the Contributors concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

The ideas and opinions expressed in this publication are those of the authors; they do not necessarily reflect the views of the International Telecommunication Union, the World Bank, its Board of Executive Directors, or the governments they represent, or those of the Contributors. The mention of specific companies, products or services does not imply that they are endorsed or recommended in preference to others of a similar nature that are not mentioned. Errors and omissions excepted; the names of proprietary products are distinguished by initial capital letters.

All reasonable precautions have been taken by the International Telecommunication Union, the World Bank and Contributors to verify the information contained in this publication. However, the published material is being distributed without warranty of any kind, either expressed or implied. The responsibility for the interpretation and use of the material lies with the reader. In no event shall the International Telecommunication Union, the World Bank or any of the Contributors be liable for damages arising from its use.

CONTRIBUTORS

accenture

جامعة الدول العربية

AXON

CTO

COMMONWEALTH
TELECOMMUNICATIONS
ORGANISATION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

C3SA
Cybersecurity Capacity Centre for Southern Africa

DiPLO

European Bank
for Reconstruction and Development

eGA
e-governance academy

EU CyberNet

Funded by
the European Union

Experire
strategy & advisory

FIRST

DCAF
Geneva Centre
for Security Sector
Governance

Global
Cyber Security
Capacity Centre

GFCE
Global Forum on Cyber Expertise

GLOBAL
PARTNERS
DIGITAL

HGS

IDB

IMF

INTERPOL

ITU

Microsoft

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

NRD Cyber Security

OAS | CICTE

UN
DP

unicri
United Nations
Interregional Crime and Justice
Research Institute

UNIDIR

UNITED NATIONS
OFFICE OF COUNTER-TERRORISM

United Nations Office
for Disarmament Affairs

United Nations
Office on Drugs and Crime

UNU
Macau

WORLD BANK GROUP

World
Economic
Forum

OBSERVER

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

Joint Foreword

Technology and connectivity are powerful enablers of inclusive and sustainable development. Technological growth, however, brings persistent and evolving cybersecurity challenges. Experience shows that the full potential of digitalization remains out of reach unless its underlying infrastructure and services are secure, resilient, and reliable.

One of the most important steps governments can take as they seek to promote digital transformation while addressing cybersecurity risks is to invest in long-term strategic planning to guide resource allocation, set priorities, and build capacities. Cybersecurity should be integrated into a country's broader vision and approached strategically and systemically, through iterative cycles of implementation, monitoring, and evaluation. To this end, many countries have gained valuable experience through the development and successive revisions of their national cybersecurity strategies. This accumulated knowledge provides a solid foundation for drawing conclusions and formulating recommendations that can guide countries with less experience or resources in navigating this ever-evolving domain.

In 2018, to empower and equip national leaders and policymakers with the analytical and conceptual tools needed to craft national cybersecurity strategies, a group of Contributors co-authored the *Guide to Developing a National Cybersecurity Strategy* (the "Guide"). Building on the positive reception of the first edition, a broader coalition convened to update the Guide and publish its second edition in 2021.

Both editions of the Guide coincided with a significant rise in the adoption of national cybersecurity strategies worldwide. In 2018, only 76 countries had adopted a formal strategy; by 2021, that number had increased to approximately 127. Today, 136 countries have a national cybersecurity strategy in place, with many now on their second or even third iteration. Throughout this process, the Guide has become a widely recognized resource, an authoritative reference, and a blueprint for national leaders and policymakers.

This third edition sharpens the focus on practical measures to safeguard the national cybersecurity posture, addressing the latest cybersecurity risks, including those driven by emerging technologies, the proliferation of connected devices, and complex supply chains and threats, while offering actionable protections to strengthen resilience in an increasingly dynamic landscape. It places greater emphasis on implementation roadmaps, measurement, and continuous improvement, as well as cross-border cooperation. The objective of the Guide remains to inform strategic thinking and support national leaders and policymakers in the development, implementation, and revision of national cybersecurity strategies and policies, anchored in appropriate legal and operational frameworks. We are confident that this new edition will serve as a valuable tool for all stakeholders with cybersecurity responsibilities.

As with previous editions, this Guide is the result of a unique, collaborative, and inclusive multistakeholder effort, bringing together organizations working in the field of national cybersecurity strategies, policies, and cyber capacity-building. In 2021, twenty organizations contributed to the second edition. For this third edition, the group has nearly doubled in size: thirty-seven organizations from the public and private sectors, academia, and civil society contributed their knowledge and experience. This edition draws on their collective expertise and references complementary publications and additional resources.

We express our sincere gratitude to the Contributors involved for their invaluable support and commitment, which have made this project a concrete example of effective multistakeholder collaboration. We encourage continued partnership and look forward to deepening our engagement with governments, regional and international bodies, law enforcement, academia, the private sector, civil society, and United Nations entities to accelerate implementation, and foster strategic dialogue on cybersecurity, cyber capacity-building, and cyber resilience.

Jointly signed by:

Mr. Holger Zwingmann
Security Transformation Associate Director,
Head of Cyber at Technology Strategy & Advisory
IX EMEA, Accenture

Mr. Álvaro Neira
Partner, Axon Partners Group

Ms. Bernadette Lewis
Secretary General, Commonwealth
Telecommunication Organisation

Mr. Virgil Spiridon
Head of Operations, Cybercrime Programme Office
of the Council of Europe

Prof. Wallace Chigona
Director, Cybersecurity Capacity Centre for Southern
Africa, University of Cape Town, South Africa

Dr. Jovan Kurbalija
Executive Director, DiploFoundation

Mr. Hannes Astok
Chairman of the Management Board,
e-Governance Academy

Ms. Liina Areng
Project Director, EU CyberNet

Mr. Roi Yarom
Associate Director, Cybersecurity Policy Specialist,
Digital Hub, European Bank for Reconstruction and
Development (EBRD)

Mr. Alessandro Ortalda
Founder and Managing Director, Experirē
Strategy & Advisory

Mr. Chris Gibson
Executive Director, FIRST

Ambassador Nathalie Chuard
Director, Geneva Centre for Security Sector
Governance (DCAF)

Prof. Sadie Creese
Director, Global Cyber Security Capacity Centre

Mr. David van Duren
Director, Global Forum on Cyber Expertise
(GFCE) Secretariat

Ms. Lea Kaspar
Executive Director, Global Partners Digital

Ms. Melissa Hathaway
President, Hathaway Global Strategies, LLC

Ms. Paula Acosta
Institutional Capacity of the State Division Chief, IADB

Mr. Tobias Adrian
Financial Counsellor and Director of the IMF's Monetary and Capital Markets Department.

Dr. Cosmas Luckyson Zavazava
Director of the Telecommunication Development Bureau (BDT), International Telecommunication Union

Mr. Cyril Gout
Acting Executive Director of Police Services, INTERPOL

Mr. Khaled Wali
Minister Plenipotentiary, Director ICT Department, League of Arab States

Ms. Kaja Ciglic
Senior Director, Cybersecurity Policy and Diplomacy, Customer Security and Trust, Microsoft

Mr Tõnis Saar
Director, NATO Cooperative Cyber Defence Centre of Exellence

Dr. Vilius Benetis
Director, NRD Cyber Security

Mr. Guillermo Moncayo
Deputy Executive Secretary in charge, Inter-American Committee against Terrorism (CICTE), Organization of American States (OAS).

Mr. Mauro Miedico
Director, United Nations Counter-Terrorism Centre

Mr. Robert Opp
Chief Digital Officer, United Nations Development Programme

Dr. Robin Geiss
Director, United Nations Institute for Disarmament Research

Mr. Leif Villadsen
Acting Director, United Nations Interregional Crime and Justice Research Institute

Dr. Jingbo Huang
Director, United Nations University Institute in Macau

Ms. Izumi Nakamitsu
Under-Secretary-General and High Representative for Disarmament Affairs, UNODA

Ms. Brigitte Strobel-Shaw
Officer in Charge of the Division of Treaty Affairs, UNODC

Ms. Christine Zhenwei Qiang
Global Director, Digital Transformation, World Bank

Mr. Tal Goldstein
Head of Strategy and Growth, Centre for Cybersecurity, World Economic Forum

Contents

PREFACE

The *Guide to Developing a National Cybersecurity Strategy* is one of the most comprehensive overviews of what constitutes a successful cybersecurity strategy. It is the result of a unique, collaborative, and equitable multistakeholder effort.

The Contributors came together with an appreciation of the need to strengthen cooperation and coordination across the international community on cyber capacity-building. The objective of this effort is to support national leaders and policymakers in the development of defensive and proactive responses to cybersecurity risks, in the form of a National Cybersecurity Strategy (NCS), and in thinking strategically about cybersecurity, cyber preparedness, response, and resilience, while building confidence and security in the use of digital technologies.

The Guide was developed through an iterative approach that sought to reach agreement through consensus-building. It is based on existing authoritative resources and aims to facilitate their use by national stakeholders. Wherever possible, the relevant sources and tools used in developing each section of this Guide are listed in the Reference section (available on www.ncsguide.org) to encourage their broader use.

Cybersecurity is a foundational element underpinning the achievement of socio-economic objectives of modern economies. The hope is that this third edition of the *Guide to Developing a National Cybersecurity Strategy* can continue to serve as a useful tool for all stakeholders involved in the development, implementation, and revision of this type of official document, including national leaders, policymakers, legislators, and regulators with cybersecurity responsibilities. In addition, it might have broader applicability, as the concepts introduced can be applied at the regional or municipal levels, and can also be adapted for industry or used for academic research.

NOTE TO READERS ON THE UPDATE

Version 3 of the *Guide to Developing a National Cybersecurity Strategy* (NCS) updates, refines, and expands upon Version 2, which was published in 2021. Since then, the cybersecurity risk environment, technologies, and policy practices have continued to evolve and grow in complexity. This edition captures key developments in cybersecurity as well as emerging and disruptive technologies that governments should consider in their national strategic planning, while preserving compatibility with prior versions and the Guide's process-plus-content approach.

This new Version focuses on practical recommendations and ease of use, and includes new material where practice has advanced. However, Version 3 remains fully compatible with Version 2 and preserves the Guide's balance between process (Lifecycle) and content (Overarching Principles and Focus Areas). Countries that adopted earlier versions can use Version 3 to review and update their national cybersecurity strategies or make incremental improvements, particularly in financing, governance, requirements for critical infrastructure, critical information infrastructure, and essential services (CI/CII/ES), risk management, incident response, legislation, and international engagement.

Major updates and additions include:

- **Lifecycle financing and long-term sustainment**: More detailed language emphasizes strategic resource planning and sustainable funding across the full NCS lifecycle (development, implementation, monitoring, review, and renewal). This includes alignment with national budget and public investment cycles, the use of dedicated funding lines, optimization of existing government resources, and external financing (e.g., multilateral development banks (MDBs), international financial institutions (IFIs), donors, technical assistance). Multi-year sustainment, attention to out-year costs and forward-looking budget projections, and fully funded initiatives are stressed. Resources should be defined in terms of money, people, and material.

- **Monitoring, evaluation, and cyclical reviews**: Governments are encouraged to incorporate SMART KPIs (Specific, Measurable, Achievable, Relevant, Time-related) into their strategies and action plans, establish clear governance of monitoring and evaluation, and define baseline metrics with scheduled reviews (e.g., mid-term check-ins, 3–5-year renewals) to ensure the strategy remains current with threats, technologies, and national priorities.

- **Technological foresight and adaptability (new principle)**: This principle underscores horizon scanning and policy agility to anticipate evolving digital risks and adapt to emerging technologies (artificial intelligence (AI), automation, quantum computing, Internet of Things (IoT), 5G/6G, distributed ledger technologies), with mechanisms to translate foresight into strategy and regulation.

- **Governance and accountability**: Guidance is strengthened on lead authority roles, whole-of-government and whole-of-society coordination, stakeholder engagement, and advisory mechanisms. It emphasizes intra-governmental and cross-sector coordination, clear assignment of responsibilities and mandates, and integration of governance into action plans.

- **Critical infrastructure, critical information infrastructure, and essential services (CI/CII/ES)**: Expanded guidance addresses identification, designation, governance, and risk-based requirements for operators. It introduces outcome-focused baselines, tiered expectations, oversight mechanisms, and considerations for cross-border interdependencies and systemic cybersecurity risks (e.g., an incident involving a widely used software provider that leads to the disruption of thousands of its customers, or a failure of a critical financial institution that disrupts an entire financial system, causing broader economic impact).

- **Risk management framework**: The updated Guide stresses the importance of having a national approach to assessing and managing cybersecurity risk, including dynamic national and sectoral assessments; a continuously updated national risk register covering critical sectors, services, functions, operators, and assets; adoption of common methodologies aligned with international standards; and feedback loops linking risk insights to policy, investment, and crisis management.

- **Incident response and resilience**: This version expands guidance on the role of national response teams (Computer Emergency Response Teams (CERTs), Computer Security Incident Response Teams

(CSIRTs), Computer Incident Response Teams (CIRTs)) with sectoral counterparts, Security Operations Centers (SOCs), and Product Security Incident Response Teams (PSIRTs) in national cybersecurity architectures. It also reinforces contingency planning, information-sharing mechanisms (including ISACs/ISAOs), national and international exercises, and severity/impact assessments.

- **Capability, capacity, and awareness**: Deeper guidance is provided on national cybersecurity workforce frameworks, education-to-workforce pathways (from early education to advanced programs and apprenticeships), and inclusive strategies to attract and retain talent, including women and underrepresented groups. The Guide also highlights executive and operational training, certification, dedicated career pipelines, and coordinated national awareness campaigns tailored to diverse audiences.

- **Legislation and regulation**: The updated Guide presents a holistic approach by mapping policy goals to legal and regulatory instruments. It clarifies mandates and oversight, embeds safeguards in cybercrime and electronic-evidence provisions, and emphasizes proportionality, human rights, due process, and data protection. It also supports legal harmonization and cross-border cooperation.

- **International cooperation**: This version strengthens links between domestic priorities and foreign policy. It encourages participation in international law and norms processes, confidence-building measures (CBMs), and standards bodies; promotes practical cooperation through formal and informal networks (including CERT/CSIRT/CIRT communities, law enforcement channels, and multistakeholder platforms); and expands on capacity-building for cyber diplomacy and international engagement.

- **Reference section** (available at www.ncsguide.org): This version of the Guide will provide a dynamic Reference Section on its website, enabling simplified access and maintenance to keep references up to date.

This updated Guide is designed as a practical reference for national leaders, policymakers, regulators, industry representatives, civil society, and other parties involved in the development of an NCS. Recognizing the importance of multistakeholder engagement, the Guide's emphasis on government entities in some sections seeks to highlight where a government entity's leadership is pivotal to the sustainability of the process. It aims to help countries develop, implement, and sustain an effective NCS in alignment with evolving risks, emerging technologies, and international good practices.

SECTION 1

Document Overview

1.1 PURPOSE

The purpose of this document is to guide national leaders and policymakers in the development, implementation, and revision of a National Cybersecurity Strategy (NCS), and in thinking strategically about cybersecurity, cyber preparedness, and resilience.

This Guide aims to provide a useful, flexible, and user-friendly framework to set the context of a country's socio-economic vision and current national cybersecurity posture and to assist national leaders and policymakers in the development or revision of a Strategy that takes into consideration a country's specific situation, cultural norms, and societal values, while encouraging the pursuit of secure, resilient, digitally empowered, and connected societies.

The Guide is a unique resource, as it provides a framework developed and endorsed by organizations with demonstrated and diverse experience in this topic area and builds on their prior work in this space. As such, it offers the most comprehensive overview to date of what constitutes a successful National Cybersecurity Strategy.

1.2 SCOPE

Cybersecurity is a complex challenge that encompasses multiple governance, policy, operational, technical, and legal aspects. This Guide addresses, organizes, and prioritizes many of these areas based on existing and well-recognized models, frameworks, and references. The Guide focuses on protecting civilian aspects of cyberspace and, as such, highlights overarching principles and good practices that need to be considered in the drafting, development, implementation, and revision of a National Cybersecurity Strategy.

To this end, the Guide makes a clear distinction between the "process" adopted by countries during the lifecycle of a National Cybersecurity Strategy (initiation, stocktaking and analysis, production, implementation, reviews) and the "content" (i.e., the actual text that would appear in a National Cybersecurity Strategy document). The Guide does not cover aspects such as the development of defensive or offensive cybersecurity capabilities by a country's military, defense forces, or intelligence agencies, even though a number of countries have been developing such capabilities.

This Guide addresses (i) "what" should be included in a National Cybersecurity Strategy, and (ii) "how" to build, implement, and review it. The Guide also provides an overview of the core components of what it takes for a country to become cyber-prepared, highlighting the critical aspects that governments should consider when developing their national strategies and action plans. Finally, this Guide offers national leaders and policymakers a holistic, high-level overview of existing approaches and applications, as well as an online Reference Section with additional and complementary resources that can inform specific national cybersecurity efforts.

1.3 OVERALL STRUCTURE AND USAGE OF THE GUIDE

This Guide is primarily structured as a resource to help national leaders and policymakers prepare, draft, and manage their National Cybersecurity Strategy. The content is organized to follow the process and order of Strategy development:

- **Section 2 – Introduction**: provides an overview of the subject of the Guide with related definitions;
- **Section 3 – Strategy Development Lifecycle**: details the steps in the development of a Strategy and its management during its full lifecycle;
- **Section 4 – Overarching Principles for a Strategy:** outlines the cross-cutting, fundamental considerations to be taken into account during the Strategy development;
- **Section 5 – Focus Areas and Good Practices**: identifies the key elements and topics that should be considered during the Strategy development; and
- **Supporting Reference Materials** (available online at www.ncsguide.org): provides relevant literature that stakeholders can review as part of their drafting and reviewing efforts.

In particular, Section 3 addresses the process and aspects related to the development of a National Cybersecurity Strategy (such as preparation, drafting, implementation, and long-term sustainability), while Sections 4 and 5 are more focused on the content of a National Cybersecurity Strategy, as they highlight concepts and elements that the document should contain.

1.4 TARGET AUDIENCE

This Guide is first and foremost targeted at national leaders and policymakers[1] responsible for developing a National Cybersecurity Strategy. The secondary audience includes other public and private stakeholders involved in the development and implementation of a Strategy, such as responsible government staff, regulatory authorities, law enforcement, providers of digital services, critical infrastructure owners and operators, civil society, academia, and research institutions. The Guide may also prove useful to stakeholders in the international development community that provide assistance in cybersecurity.

[1] The Guide uses "policymakers" as a broad term that refers to all government entities or functions involved in the development, implementation, and revision of an NCS.

SECTION 2

Introduction

Since their emergence, information and communication technologies (ICTs) and digital services have evolved to become the backbone of modern business, critical services and infrastructure, social networks, and the global economy as a whole.

As a result, national leaders have launched digital strategies and funded projects to increase internet connectivity and leverage the benefits of digital technologies to stimulate economic growth, enhance productivity and efficiency, improve service delivery and capacity, provide access to business and information, enable e-learning, strengthen workforce skills, and promote good governance. Countries cannot ignore the opportunities associated with greater connectivity and participation in the digital economy.

While the reliance on digital infrastructure is growing, the technology remains inherently vulnerable. The confidentiality, integrity, and availability of data, information systems, and digital infrastructure are challenged by rapidly evolving cybersecurity risks, including electronic fraud, theft of intellectual property and personally identifiable information, disruption of services, and damage or destruction of physical and digital assets. The transformational power of digital technologies and the internet as catalysts for economic growth and social development is at a critical point, as citizens' and nations' trust and confidence in the use of these technologies are increasingly undermined by cyber insecurity and the exploitation of vulnerabilities.

To fully realize the potential of technology, countries must align their national economic visions with their national security priorities. If the security risks associated with the proliferation of digitally-enabled infrastructure and internet applications are not appropriately balanced with comprehensive national cybersecurity strategies and resilience plans, countries will be unable to achieve the economic growth and national security goals they seek. In response, governments are developing both offensive and defensive capabilities to defend themselves from illicit and illegal activities in cyberspace and to pre-empt incidents before they can cause harm. This document focuses specifically on defensive and proactive responses, particularly in the form of national cybersecurity strategies.

2.1 WHAT IS CYBERSECURITY

Several national and international definitions of the term "cybersecurity" exist. For the purpose of this document, the term "cybersecurity" refers to the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurance measures, and technologies that can be used to protect the availability, integrity, and confidentiality of assets in the connected infrastructures of government, private organizations, and citizens. These assets include connected computing devices, personnel, infrastructure, applications, digital services, telecommunications systems, and data within the digital environment.

2.2 BENEFITS OF A NATIONAL CYBERSECURITY STRATEGY AND STRATEGY DEVELOPMENT PROCESS

National cybersecurity strategies can take many forms and can go into varying levels of detail, depending on a country's objectives and cybersecurity maturity. Therefore, there is no established or universally agreed definition of what constitutes a National Cybersecurity Strategy.

Relying on existing research in this area, this document encourages stakeholders to think of a National Cybersecurity Strategy as:

- an expression of the vision, high-level objectives, principles, and priorities that guide a country in addressing cybersecurity;
- an overview of the stakeholders responsible for strengthening national cybersecurity and their respective roles and responsibilities; and
- a description of the steps, programs, and initiatives that a country will undertake to protect its national digital infrastructure, and in the process, increase its security and resilience.

Setting the vision, objectives, and priorities upfront enables governments to look at cybersecurity holistically across their national digital ecosystem, rather than focusing narrowly on one sector, responding only to particular risks, or reacting to specific incidents – it allows them to be strategic. Priorities for national cybersecurity strategies vary by country: while some may focus on protecting critical infrastructure, others may prioritize intellectual property protection, promoting trust in the digital environment, or improving cybersecurity awareness of the general public – or a combination of these objectives.

The need to identify and prioritize investments and resources for the strategy development and implementation, as well as for related programs and initiatives, is critical to successfully managing risks in an area as all-encompassing as cybersecurity.

A National Cybersecurity Strategy also provides the opportunity to align cybersecurity priorities with broader ICT-related objectives. Cybersecurity is central to achieving the socio-economic objectives of modern economies, and the Strategy should reflect how those are supported. This can be achieved by referencing existing policies that implement a country's digital or developmental agendas, or by incorporating cybersecurity into them.

Finally, a National Cybersecurity Strategy development process should translate a government's vision into coherent and implementable policies that will help achieve its objectives. This includes not only the steps, programs, and initiatives to be implemented, but also the resources allocated for those efforts and how they should be used. Similarly, the process should identify the metrics and performance indicators to ensure that desired outcomes are achieved within set budgets and timelines.

SECTION 3

Lifecycle

This Section provides an overview of the phases in the development of a National Cybersecurity Strategy, which include:

- **Phase I – Initiation**
- **Phase II – Stocktaking and Analysis**
- **Phase III – Sustainable Funding and Resource Planning**
- **Phase IV – Production**
- **Phase V – Implementation**
- **Phase VI – Monitoring and Evaluation**

It also introduces the key entities that should be involved in the development of the Strategy and highlights other relevant stakeholders that can contribute to the process.

Ultimately, this section aims to help the reader understand the steps a country should take to draft or update a National Cybersecurity Strategy and the possible mechanisms for its implementation, tailored to the country's specific needs and requirements, integrating the overarching principles (Section 4) and good practice elements (Section 5).

This Lifecycle, as illustrated in Figure 1, guides users of this document in focusing on strategic thinking about cybersecurity and cyber resilience at the national level. This strategic thinking, as explained in Section 2 should take into account and align with the country's priorities across national security, economic prosperity, and digital resilience, recognizing cybersecurity as an enabler of effective national governance and sustainable development.

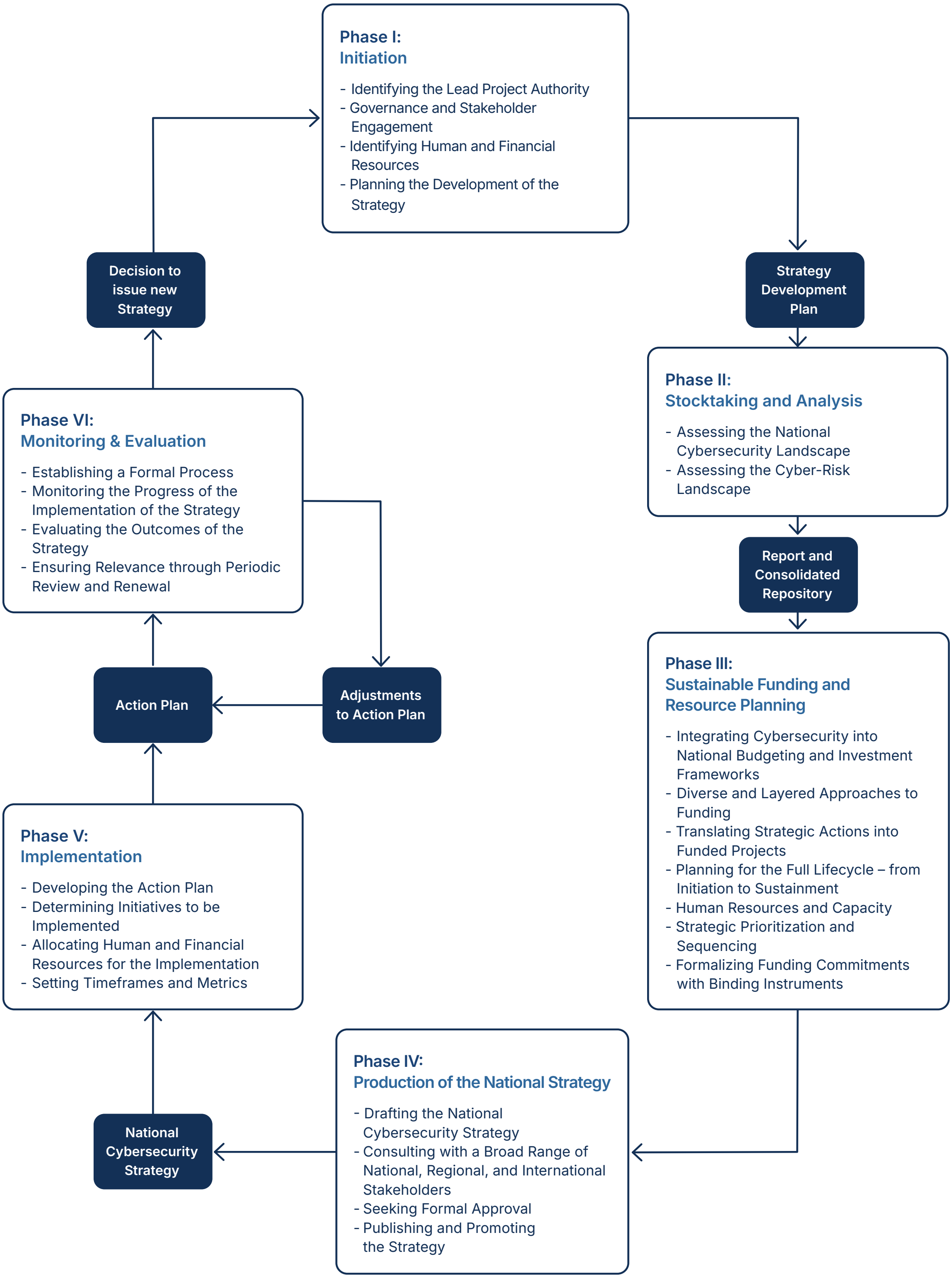
3.1 PHASE I - INITIATION

The Initiation Phase provides the foundations for effective Strategy development. During this phase, relevant stakeholders in key government entities should establish clear roles and responsibilities, define project management processes and timelines, and identify additional stakeholders who should be involved in the production of the Strategy. It should also be decided whether the document will be a whole-of-nation Strategy or focused primarily on government entities and national critical assets. The outcome of this phase is a development plan for the Strategy, which, where required by national governance processes, may need approval by the country's Executive.

3.1.1 Identifying the Lead Project Authority

In line with the principle of clear leadership, roles, and resource allocation (Section 4.8), the Strategy development should be coordinated by a single, competent authority. The Executive should appoint a pre-existing or newly created public entity, such as a ministry, agency, or department, to lead the development of the Strategy. This entity, referred to here as the Lead Project Authority, should appoint an individual or team responsible and accountable for leading and coordinating the development process. The designation of a Lead Project Authority does not imply that the entity must oversee a new specific project; it may equally be a ministry, agency, or body with an existing initiative, or simply a political mandate, provided it is formally empowered to coordinate the Strategy's development.

Figure 1 - Lifecycle of a National Cybersecurity Strategy



Phase I:
Initiation

- Identifying the Lead Project Authority
- Governance and Stakeholder Engagement
- Identifying Human and Financial Resources
- Planning the Development of the Strategy

Strategy Development Plan

Phase II:
Stocktaking and Analysis

- Assessing the National Cybersecurity Landscape
- Assessing the Cyber-Risk Landscape

Report and Consolidated Repository

Phase III:
Sustainable Funding and Resource Planning

- Integrating Cybersecurity into National Budgeting and Investment Frameworks
- Diverse and Layered Approaches to Funding
- Translating Strategic Actions into Funded Projects
- Planning for the Full Lifecycle – from Initiation to Sustainment
- Human Resources and Capacity
- Strategic Prioritization and Sequencing
- Formalizing Funding Commitments with Binding Instruments

Phase IV:
Production of the National Strategy

- Drafting the National Cybersecurity Strategy
- Consulting with a Broad Range of National, Regional, and International Stakeholders
- Seeking Formal Approval
- Publishing and Promoting the Strategy

National Cybersecurity Strategy

Phase V:
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 VI:
Monitoring & Evaluation

- Establishing a Formal Process
- Monitoring the Progress of the Implementation of the Strategy
- Evaluating the Outcomes of the Strategy
- Ensuring Relevance through Periodic Review and Renewal

Decision to issue new Strategy

Where feasible, the Lead Project Authority should be distinct from the entity(ies) responsible for implementation and should be empowered to work impartially with all stakeholders. It should be provided with the tools, resources, and authorities necessary to fulfill its mandate (e.g., authority to convene inter-agency meetings and request information across government) and the capacity to use them effectively.

3.1.2 Governance and Stakeholder Engagement

To support the Lead Project Authority in developing the Strategy, the Executive should establish one or more governance mechanisms, such as a Steering Committee for strategic direction and quality assurance, an expert Advisory Group drawing from the public and private sectors and civil society, and formal consultation channels, to ensure transparency and inclusion across the Strategy's Lifecycle.

The mandate, composition, and operating procedures of these mechanisms should be clearly defined from the outset, with appropriate authorizations for participants who may handle sensitive materials, and membership that reflects assigned responsibilities and seniority where appropriate.

In parallel, the Lead Project Authority should identify an initial set of stakeholders, clarify their roles, and set expectations for collaboration. Priority should be given to: (1) entities with formal policymaking mandates (e.g., ministries, departments, agencies); (2) strategically significant actors (e.g., critical infrastructure owners and operators); and (3) organizations or individuals with demonstrated expertise that can inform the process (e.g., technology and digital service providers, specialized advisers, academic specialists).

As the work progresses, the Lead Project Authority may review and expand the list of relevant stakeholders to incorporate emerging needs and insights from government, the private sector, and civil society, in line with the principle of inclusiveness (Section 4.3).

To enable effective cooperation among stakeholders, the Lead Project Authority should consider regular inter-agency meetings (in-person or virtual), structured engagements with academia and civil society, milestone reviews across the NCS Lifecycle, and periodic progress reports.

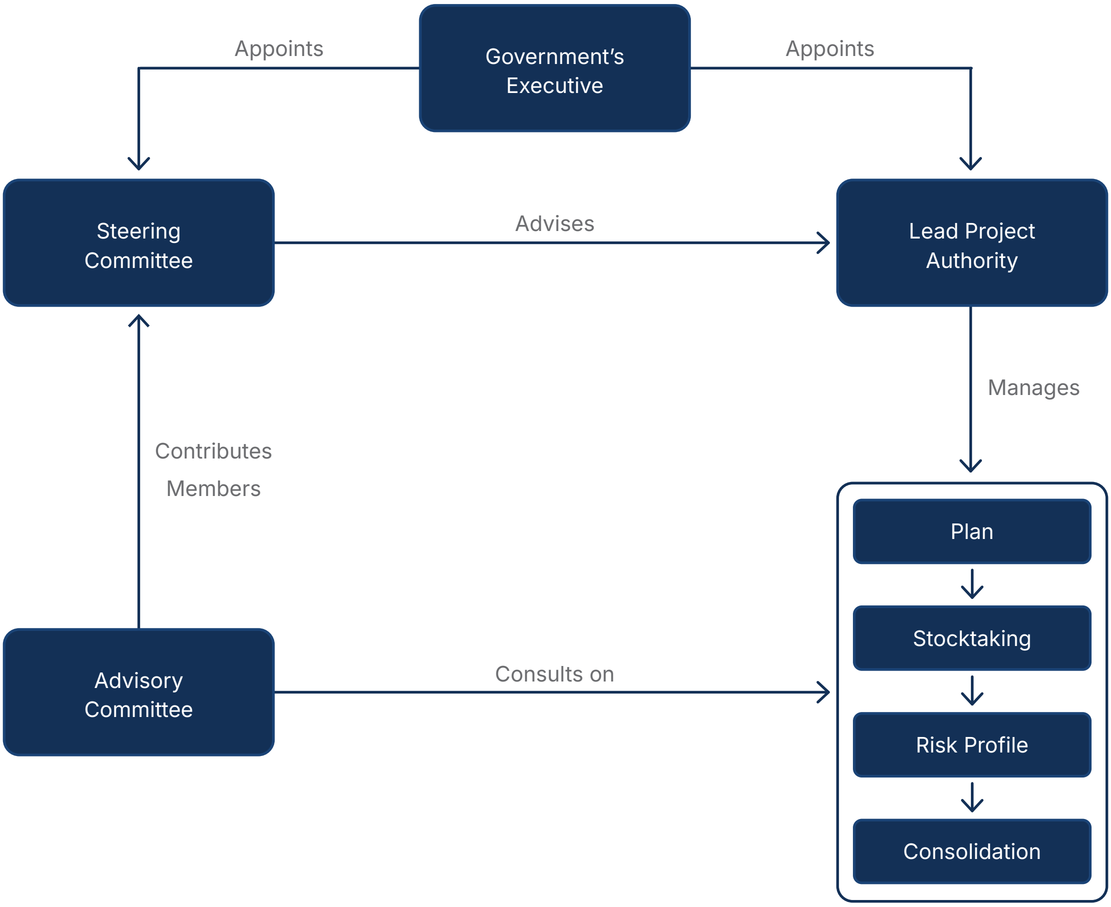
Where appropriate, international partners, including international organizations, development agencies, regional bodies, and private entities, can be engaged through expert exchanges and focused working sessions to provide additional support and specialized expertise on the NCS.

3.1.3 Identifying Human and Financial Resources

The Lead Project Authority should identify the human and financial resources needed to develop the Strategy, determine their sources, and outline how they will be procured and allocated. For example, required expertise may be solicited from across government, intergovernmental organizations, the private sector, civil society, or academia.

Funding should draw on a mix of sources, including dedicated national budget lines tied to specific NCS objectives, reallocation or optimization of existing government resources, new budget authorizations, and external investments (e.g., international organizations, multilateral development banks (MDBs), international

Figure 2 - Stakeholders' Roles and Responsibilities



financial institutions (IFIs), bilateral donors, and philanthropic or technical assistance programs). External actors may provide targeted investments aligned with NCS goals, particularly for cyber capacity-building, infrastructure development, legal and institutional reform, and cybersecurity workforce development.

Depending on national practice, this step may focus exclusively on resourcing Strategy development (with implementation budgeting addressed later in Section 3.3), or the two may be merged. Either way, strategic planning and sustainable resourcing help ensure the NCS is drafted within the planned timeframe, actionable in the near term, and durable over the long term.

3.1.4 Planning the Development of the Strategy

In the final step of the Initiation Phase, the Lead Project Authority should prepare a Strategy development plan. Once drafted, it should be submitted to relevant stakeholders (e.g., Steering Committee) for review and to the Executive for approval, in accordance with the national governance processes.

When drafting the development plan, the Lead Project Authority should consider whether the NCS will take the form of legislation or policy, as this may affect the formal processes required and the timeframe for adoption.

The Strategy development plan should clearly identify major steps and activities, key stakeholders, timelines, and resource requirements (human and financial). It should specify how and when relevant stakeholders are expected to participate and provide input and feedback.

Figure 2 illustrates example interactions and role distributions among stakeholders and committees.

3.2 PHASE II - STOCKTAKING AND ANALYSIS

The purpose of this phase is to collect information to assess the national cybersecurity landscape and current and emerging cybersecurity risks, to inform drafting and development of the Strategy. The output should be a report providing an overview of the current strategic national cybersecurity posture, risk landscapes, and pressing concerns, to be submitted to key decision-makers.

Before beginning production (or updating) of the Strategy, the Lead Project Authority should carefully analyze and assess the stocktaking results to identify gaps in cybersecurity capacity and present options to address them. The analysis should assess the extent to which existing policy, regulatory, and operational environments meet the national needs, and highlight where they fall short. It should also identify specific issues (e.g., educational and workforce gaps) and define desired outcomes for the Strategy, along with the means available and required to achieve them.

KEY ELEMENTS TO BE MAPPED

- Stakeholders
- Roles and Responsibilities
- Critical Assets and Services
- Existing Laws,Regulation, Policies, etc.
- Soft-regulatory Mechanisms Incident Response Capabilities
- National and International Cybersecurity Initiative
- Multilateral and Bilateral Agreements
- Private Sector Projects
- Education and R&D Programs
- Indicators on National Digital Development
- Threats Information
- Active or Planned Technical Assistance and Investments

3.2.1 Assessing the National Cybersecurity Landscape

For the Strategy to be effective, it must reflect the country's cybersecurity posture. An analysis of the existing strengths and weaknesses should therefore be conducted in collaboration with stakeholders across government, the private sector, and civil society. This step follows the principle of a comprehensive approach and tailored priorities (Section 4.2).

The Lead Project Authority should also map stakeholder roles and responsibilities in national cybersecurity to leverage good practices and reduce overlaps.

As part of this effort, the Lead Project Authority should identify assets and services critical to the proper functioning of society and the economy; map existing national laws, regulations, policies, programs, and capacities related to cybersecurity; catalog soft-regulatory mechanisms such as private-public partnerships; and take stock of existing capabilities to address cybersecurity challenges and respond to cyber incidents (e.g., national and sectoral CERTs/CSIRTs/CIRTs and SOCs). The roles and responsibilities of relevant public bodies with cybersecurity responsibilities, such as regulators or data-protection authorities, should also be mapped.

Additionally, data that can inform the national cybersecurity posture should be collected, such as: existing national cybersecurity programs and international initiatives; multilateral and bilateral agreements; private sector projects; digital and cybersecurity-education and skill development programs; cyber-R&D initiatives; indicators on internet penetration, connectivity, and digitalization; and insights on emerging threats and broader cybersecurity trends. Relevant inputs from the private sector, research institutions, and other stakeholder groups should be included in this analysis as well.

For developing countries, mapping collaborative initiatives with development partners is crucial to coordinate technical assistance and investments. The Lead Project Authority should also review relevant information at the regional and international levels, as well as sector-specific strategies and initiatives.

3.2.2 Assessing the Cyber-Risk Landscape

Building on the stocktaking results, the Lead Project Authority should assess risks associated with national digital dependence. This is foundational for prioritizing activities and allocating resources toward the greatest risk-reduction opportunities while avoiding duplication and uneven distribution.

This assessment should begin by identifying national digital assets (public and private), their interdependencies, vulnerabilities, and threats, and estimating the likelihood and potential impact of cyber incidents or disruptions.

This effort aligns with the principle of risk management and resilience (Section 4.6), which recognizes that risk management is critical to fully realizing the benefits of the digital environment for socio-economic development.

This initial risk assessment can serve as the basis for more specific risk assessments in the future (more information on the Principle of Risk Management and Resilience and how to conduct risk assessments can be found in Sections 4.6, 5.2, and 5.3).

3.3 PHASE III - SUSTAINABLE FUNDING AND RESOURCE PLANNING

Effective cybersecurity requires sustained commitment, not only in policy and political will, but also in financing. From inception through implementation, evaluation, and renewal, each phase of the Strategy lifecycle demands dedicated, predictable, and long-term funding. Without adequate and continuous financial support, even well-designed strategies risk remaining unrealized. This subsection outlines key considerations for identifying, securing, and managing sustainable funding to support the full lifecycle of the Strategy. All steps should be captured in an Action Plan.

3.3.1 Integrating Cybersecurity into National Budgeting and Investment Frameworks

Ideally, the development and implementation of a Strategy should be resourced through established national budgeting and public investment planning processes. Cybersecurity should not be treated as a siloed or one-time initiative, but as a cross-cutting national priority, integrated and aligned with other strategic investments such as infrastructure development, digital connectivity, public service modernization, and national security.

Cybersecurity-specific funding lines should be reflected in annual budget cycles, medium-term expenditure frameworks, and national development plans, as appropriate. To maximize impact and cost-efficiency, governments should actively seek synergies between the Strategy and other priority sectors. Major national programs in health, education, transportation, or critical infrastructure modernization often have embedded digital and cybersecurity components. Building cybersecurity protections into these programs at the design stage, rather than retrofitting later, can reduce costs, strengthen operational alignment, and improve public trust and mission resilience.

3.3.2 Diverse and Layered Approaches to Funding

Funding a Strategy can and should involve a mix of sources, including:

- Dedicated national budget allocations tied to specific objectives, line-ministry activities, or other key entities with national cybersecurity roles and responsibilities.
- Reallocation or optimization of existing resources, especially where current programs can be enhanced through cybersecurity improvements.
- New budget authorizations or legislation enabling multi-year commitments or authorizing funding for strategic initiatives requiring longer planning horizons than a single budget cycle or administration allows.
- External funding (e.g., international organizations, MDBs/IFIs, bilateral donors, philanthropic or technical assistance programs). These actors may offer targeted financing instruments aligned with strategic goals, particularly for capacity-building, infrastructure development, legal and institutional reform, and cyber/digital workforce development.

Coordination with development partners and inclusion of the Strategy within national development cooperation strategies can ensure that cybersecurity receives appropriate attention within foreign assistance portfolios. Establishing a central coordination mechanism for donor and partner engagement, linked to national cybersecurity priorities, can help avoid duplication, improve absorptive capacity, and align funding with strategic needs.

3.3.3 Translating Strategic Actions into Funded Projects

An additional consideration is the translation of strategic action plans into formal public investment projects using nationally recognized planning and budgeting methodologies. Aligning strategic actions with the country’s public investment management system allows cybersecurity initiatives to be structured as formal projects with clear objectives, indicators, timelines, responsible institutions, and resource requirements.

Governments are encouraged to apply tools such as the Logical Framework Approach (LFA), Cost-Benefit Analysis (CBA), Theory of Change (ToC), or similar approaches to assess feasibility, effectiveness, and alignment with national priorities. Embedding these initiatives within national planning and budgeting cycles, such as medium-term expenditure frameworks, helps ensure that cybersecurity efforts are not treated as ad hoc activities, but are sustained, accountable, and integrated into the broader public policy agenda.

3.3.4 Planning for the Full Lifecycle – from Initiation to Sustainment

Sustainable funding must account not only for launching new initiatives, but also for their ongoing operation, maintenance, and renewal. Strategic initiatives often span multiple years and may outlast a particular administration. Budgeting efforts must therefore factor in the full lifecycle costs, including recurring expenditures such as licensing, training, infrastructure maintenance, and staffing. Insufficient planning for sustainment can have serious negative consequences. For instance, deploying a security tool but failing to renew licences or provide ongoing training can create vulnerabilities or degrade trust in digital public services. Similarly, cybersecurity initiatives launched with one-time external funding may not be viable without parallel domestic commitments. The Strategy should therefore:

- Prioritize fewer, fully funded initiatives over many under-resourced ones;
- Build out-year costs into forward-looking budget projections;
- Identify opportunities for cost-sharing or co-financing with development partners, the private sector, or regional initiatives;
- Maintain budget flexibility to address unforeseen costs and emergent needs.

3.3.5 Human Resources and Capacity

A critical, and often underfunded, component of the Strategy is the human element. No strategy can succeed without a capable, well-resourced, and retained cybersecurity workforce. The Strategy should consider human resource needs as a fundamental and recurring line item, not a one-off cost.

Governments should identify common skills needs across ministries and sectors and develop shared training pipelines, career pathways, and professional development programs to maximize efficiency. Investment in workforce development should be treated as a strategic investment, a foundational enabler for nearly every other initiative. Joint investments with regional or international partners in education, training, and certification can help achieve scale, sustainability, and improved outcomes (more information on skills development can be found in Section 5.5).

3.3.6 Strategic Prioritization and Sequencing

Resource planning should be guided by strategic prioritization. Some NCS activities may be high-cost and long-term but deliver outsized benefits; these should be viewed as “strategic investments” and be funded accordingly. The longer an initiative takes to mature, and the more objectives it supports, the more critical it becomes to fully fund it from the outset.

Only a limited number of such initiatives will likely be feasible within available national and partner resources. Governments should therefore carefully sequence implementation based on available funding, political momentum, and institutional readiness, securing early wins that build momentum for subsequent phases.

3.3.7 Formalizing Funding Commitments with Binding Instruments

To ensure the continuity and sustainability of cybersecurity investments, funding and responsibilities for the Strategy implementation should be formalized through binding instruments (e.g., executive mandates, inter-ministerial agreements, cabinet-level resolutions, or legally enacted budgetary provisions). Such instruments establish a formal basis for resource allocation, clarify institutional responsibilities, and protect cybersecurity funding from discretionary budget shifts. Codifying these commitments reinforces political will, strengthens inter-agency coordination, and provides a durable foundation for long-term capacity development and implementation of strategic priorities.

Ultimately, sustained and predictable financing is the backbone of the entire NCS Lifecycle; without it, strategies risk becoming aspirational documents rather than operational drivers of national resilience. Embedding cybersecurity in long-term resource planning ensures that every subsequent phase, from implementation to monitoring, review, and renewal, can deliver tangible, lasting impact.

3.4 PHASE IV - PRODUCTION OF THE NATIONAL CYBERSECURITY STRATEGY

The purpose of this phase is to develop the text of the Strategy by engaging key stakeholders from the public sector, private sector, academia and civil society through a series of public consultations and working groups. This broader group of stakeholders, coordinated by the Lead Project Authority, will be responsible for defining the overall vision and scope of the Strategy, setting high-level objectives, taking stock of the current situation (detailed in Phase II), prioritizing objectives in terms of impact on society, citizens, and the economy, and available resources (detailed in Phase III). As part of this phase, all cross-cutting principles (Section 4) and good practice elements (Section 5) detailed in this Guide should be considered.

3.4.1 Drafting the National Cybersecurity Strategy

Once the Sustainable Funding and Resource Planning phase is complete, the Lead Project Authority, in collaboration with the Steering Committee, should initiate the drafting of the NCS. While the process can be driven directly by the Lead Project Authority, it is advisable to involve relevant stakeholders to ensure diverse and important perspectives are captured. Dedicated working groups, where feasible and within available resources, may be created to focus on specific topics or draft different sections of the Strategy. These groups should follow the processes established in the Initiation Phase, adjusting them as necessary.

The Strategy should provide the overall cybersecurity direction for the country; express a clear vision and scope; set objectives to be accomplished within a specific timeframe; and prioritize them in terms of impact on society, the economy, and infrastructure. Moreover, it should identify possible courses of action, incentivize implementation efforts, and guide the allocation of required resources to support all these activities. The Strategy may also include findings developed during the Stocktaking and Analysis Phase.

Similar to the step on planning the development of the Strategy, the final document should put forward a clear governance framework (Section 5.1) defining the roles and responsibilities of key stakeholders. This includes identifying the entity responsible and accountable for managing and evaluating the Strategy, as well as the body responsible for its overall management and implementation, such as a central authority or a national cybersecurity council.

The Strategy should also identify the different entities that make up the national cybersecurity architecture of the country, including those responsible for developing cybersecurity policies and regulations; collecting threat and vulnerability information; responding to cyber incidents (e.g., national CERTs/CSIRTs/CIRTs); and strengthening preparedness and crisis management. It should clearly describe how these entities interact with each other and with the central authority.

3.4.2 Consulting with a Broad Range of National, Regional, and International Stakeholders

As mentioned above, stakeholder engagement is crucial for the success of a Strategy. To ensure that the final document is based on a shared vision and minimizes the risk of inconsistent or conflicting requirements with other national ones, the draft should be disseminated widely, including stakeholders beyond those directly involved in the Strategy development process. This can be done through a variety of engagements, including online consultations, validation workshops, and additional working groups. International and regional organizations and other external stakeholders can also play a role by providing advice and expertise. Feedback and comments from this process should be incorporated into the final Strategy.

3.4.3 Seeking Formal Approval

In the final step, the Lead Project Authority should ensure that the Strategy is formally adopted by the Executive. This adoption process will vary by country and depend on the legislative framework. For example, adoption could take place through a parliamentary procedure or a high-level administrative document of the government, such as a decree or a resolution.

Furthermore, it is essential that the Strategy is not only approved at the highest levels of government, but that this commitment carries through into the implementation phase. The relevant entities and officials should be held accountable and supported with both political capital and resources, ensuring that cybersecurity efforts remain strong and sustainable over time, beyond the initial publication of the Strategy.

3.4.4 Publishing and Promoting the Strategy

The Strategy should be a public document and made readily available. The launch of the Strategy should ideally be accompanied by internal and external promotional activities. Broad dissemination of the

Strategy will ensure that the public is aware of the government's cybersecurity priorities and objectives and will support national awareness-raising efforts.

The accompanying Action Plan, whether annexed to the Strategy or published separately, should also highlight opportunities for further engagement and cooperation with all relevant stakeholders.

3.5 PHASE V - IMPLEMENTATION

A structured approach to implementation, supported by adequate human and financial resources (see also Section 3.3), is critical to the success of the Strategy and should be considered as part of its development. In this context, adequate human resources refers to the availability of sufficient staff and professionals with expertise in governance, policy, cybersecurity, technology, and regulatory matters. The implementation phase is often centered on an Action Plan, which guides the activities envisioned.

3.5.1 Developing the Action Plan

As with the development of the Strategy, its implementation cannot be the sole responsibility of a single body or authority. Instead, it requires engagement and coordination of a range of stakeholders across government, with additional support from critical infrastructure owners and operators, civil society, and the private sector. The Action Plan, developed in line with the principle of clear leadership, roles, and resource allocation (Section 4.8), provides the framework for effective implementation.

The process of developing the Action Plan is nearly as important as the document itself. Orchestrated by the Lead Project Authority, it should serve as a mechanism to bring relevant stakeholders together to agree on objectives and outcomes, coordinate efforts, and pool resources.

3.5.2 Determining Initiatives to be Implemented

The Strategy defines the government's objectives and the outcomes it seeks across different focus areas. In the Action Plan, the Lead Project Authority, in coordination with relevant stakeholders, should identify the specific initiatives that will achieve these objectives. Examples include organizing cybersecurity exercises and drills, establishing security baselines for critical infrastructure sectors, and setting an incident reporting framework, among others.

The timeline and effort needed for the implementation of these initiatives should be prioritized according to criticality, ensuring that limited resources are leveraged effectively. To this end, results from Phase II (Stocktaking and Analysis), especially the assessment of the cybersecurity risk landscape (Section 3.2.2), should inform prioritization.

3.5.3 Allocating Human and Financial Resources for the Implementation

Once initiatives are prioritized, they should be formalized within the Strategy and/or the Action Plan, which should identify the specific entities responsible and accountable for each initiative (e.g., ministries, departments, agencies). These entities are then accountable for the implementation of each specific initiative assigned to them and are expected to coordinate their efforts with other relevant stakeholders as part of the implementation process.

The Lead Project Authority should ensure these entities have the appropriate legal or institutional mandate to carry out their tasks. It should also work with them to determine the human, technical, and financial resources required to accomplish the work (e.g., expertise, staffing, funding needs). The Lead Project Authority should help identify and secure the required resources in line with Phase III (Section 3.3).

3.5.4 Setting Timeframes and Metrics

A critical element of the Action Plan is the development of specific metrics and key performance indicators (KPIs) to track implementation and assess progress of each initiative laid out in the Action Plan (see also Section 3.6). These may include the percentage of actions completed, budget disbursement to date, or identification of entities falling behind on delivery, etc. Specific timelines for the implementation of each initiative should also be clearly set.

The Lead Project Authority, in partnership with the implementing entities, should develop these metrics and KPIs. Implementing entities should also maintain a more detailed set of metrics to support evaluations of efficiency and effectiveness during and after their completion.

3.6 PHASE VI - MONITORING AND EVALUATION

Developing and implementing the Strategy is an ongoing process. A competent authority should devise a formal process to monitor and evaluate the Strategy. During the monitoring phase, the government should ensure that the Strategy is implemented in accordance with its Action Plan. During the evaluation phase, the government and the national competent authority should assess whether the Strategy remains relevant in light of the evolving risk environment, whether it continues to reflect government objectives, and what adjustments may be necessary.

3.6.1 Establishing a Formal Process

To ensure effective monitoring and evaluation of the Strategy implementation, the government should identify an independent entity responsible for monitoring progress and assessing efficacy. This entity should ideally be involved in defining appropriate monitoring and evaluation metrics for the Strategy and its Action Plan during the Production and Initiation phases.

Monitoring and measuring the performance and execution of the Action Plan should be embedded in the governance mechanisms the country establishes for the Strategy. Continuous assessment of implementation progress (i.e., what is working and what is not) helps inform adjustments. Good governance mechanisms should also clearly delineate accountability and responsibility for successful execution. Establishing metrics or KPIs by near-term, mid-term, and long-term objectives helps reinforce governance and management structures.

Key performance indicators or metrics should be SMART.

SPECIFIC: Target a defined area for improvement and focus on the change expected.

MEASURABLE: Quantify or suggest clear indicators of progress.

ACHIEVABLE: State what results can realistically be achieved with available resources.

RELEVANT: Focus on significant indicators of progress and specify who is responsible.

TIME-RELATED: Specify when the result(s) are expected.

KPIs should always be tailored to specific goals and linked to specific initiatives to facilitate corrective actions. The more detailed a KPI is, the more difficult it will be to measure reliably, so balance is required. Baseline metrics are essential for effective monitoring and for identifying areas of improvement. Budget allocation should also reflect the ambition and complexity of the intended impact.

3.6.2 Monitoring the Progress of the Implementation of the Strategy

The entity responsible for monitoring the progress of implementation of the Strategy should do so according to an agreed timeline across the entire lifecycle of the Strategy. Monitoring outputs (e.g., reports) should highlight deviations from the agreed evaluation parameters (e.g., deadlines, quality standards, expenditures, etc.) and provide explanations for delays, such as shifting priorities, insufficient staffing or resources, etc.

This should complement periodic updates from initiative owners to the Lead Project Authority. All relevant stakeholders should be actively involved in monitoring the implementation and progress of the Strategy. This approach ensures accountability for commitments, facilitates early identification of challenges, and enables the government to take corrective action or adapt Action Plans based on lessons learned during the implementation process.

3.6.3 Evaluating the Outcomes of the Strategy

Beyond tracking progress, it is also essential to periodically evaluate outcomes against the objectives originally set. This evaluation determines whether the objectives of the Strategy are being achieved or whether adjustments are needed.

As part of this process, the broader digital and cybersecurity risk environment must also be regularly re-evaluated to determine whether external changes are affecting the outcomes of the Strategy. Effectively, this process acts as a light-touch revision of a country’s risk assessment profile.

The assessment, together with associated recommendations, should be compiled into a report for the Lead Project Authority. This report should include proposals to update the Action Plan and ensure that it remains current and responsive to evolving policies, national cybersecurity architecture, and the risk landscape.

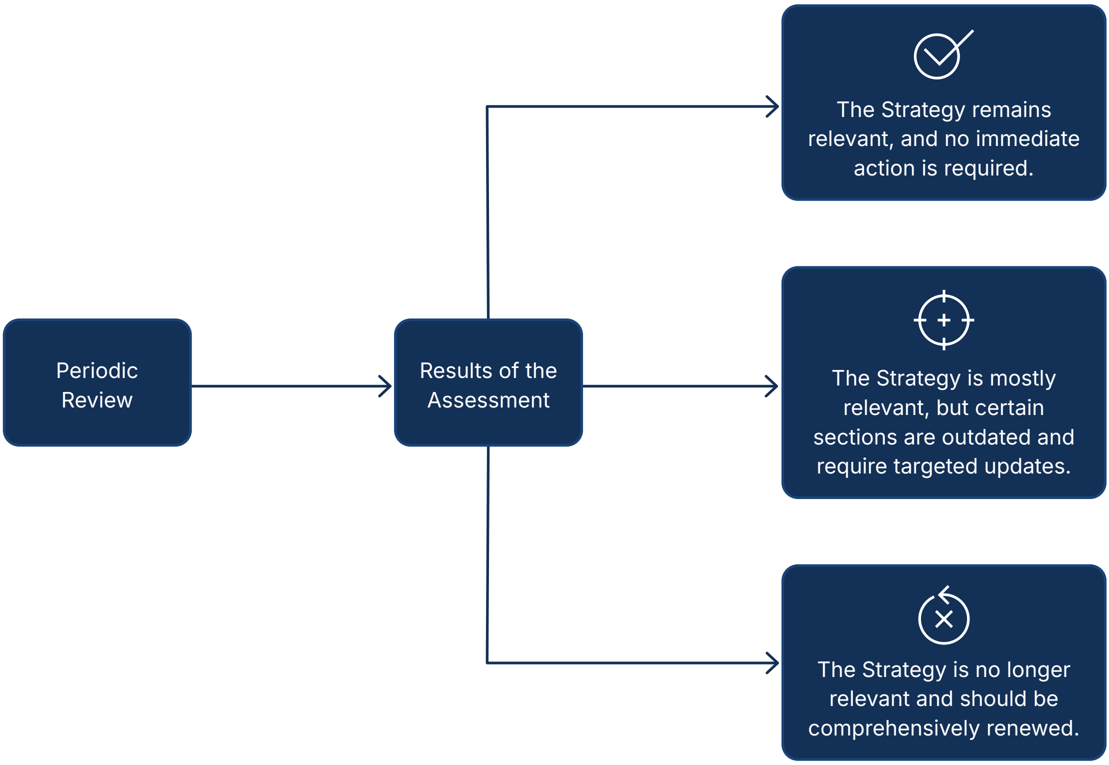
Ultimately, reports produced throughout the NCS lifecycle should serve as the basis for the overall review of the Strategy, in line with the timeline set during the Initiation phase. This overarching review should assess not only progress and external developments, but also shifts in government priorities and objectives.

3.6.4 Ensuring Relevance through Periodic Review and Renewal

The Strategy should be subject to regular review to ensure it remains aligned with evolving threats, technological changes, and shifting national priorities. Reviews should be institutionalized in the governance framework, include (where possible) the involvement of external stakeholders who can provide alternative viewpoints, and be scheduled at regular intervals (e.g., every 3 to 5 years), with at least one mid-term review conducted halfway through the Strategy's expected lifespan. In addition, reviews should be triggered by major events such as significant cyber incidents, legislative or regulatory changes, or shifts in the geopolitical landscape.

The review process should assess the continued relevance of the Strategy and produce recommendations for how to move forward. For instance, this may include:

Figure 3 - Periodic Review of a Strategy



Periodic Review

Results of the Assessment

The Strategy remains relevant, and no immediate action is required.

The Strategy is mostly relevant, but certain sections are outdated and require targeted updates.

The Strategy is no longer relevant and should be comprehensively renewed.

Ultimately, regular and mid-term reviews ensure that the Strategy remains a living document, responsive to changing conditions. These reviews should feed directly into the next cycle of NCS development, beginning again with initiation and stocktaking.

SECTION 4

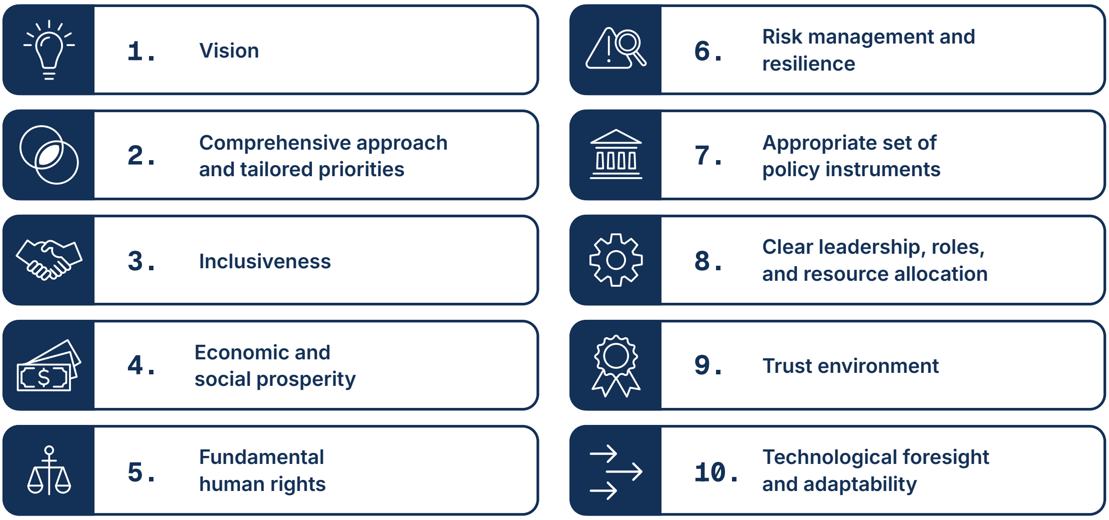
Overarching Principles

This section presents ten cross-cutting principles, which, when taken together, can help in the development of a forward-looking and holistic National Cybersecurity Strategy.

These principles are applicable to all key focus areas identified in this document. They should be considered in all steps of the Strategy development process, from the drafting of the Strategy document to its implementation.

The order of these principles reflects a logical narrative rather than an order of importance.

Figure 4 - Overarching Principles



1. Vision
2. Comprehensive approach and tailored priorities
3. Inclusiveness
4. Economic and social prosperity
5. Fundamental human rights
6. Risk management and resilience
7. Appropriate set of policy instruments
8. Clear leadership, roles, and resource allocation
9. Trust environment
10. Technological foresight and adaptability

4.1 VISION

The Strategy should set a clear whole-of-government and whole-of-society vision.

A Strategy is more likely to succeed when it sets a vision that helps all stakeholders understand what is at stake and why the Strategy is needed (context), what is to be accomplished (objectives), and whom it impacts (scope).

The clearer the vision, the easier it will be for leaders and key stakeholders to ensure a comprehensive, consistent, and coherent approach. A clear vision also facilitates coordination, cooperation, assistance, and implementation across relevant stakeholders. It should be formulated at a sufficiently high level and consider the dynamic nature of the digital environment. The objectives and implementation timeline of the Strategy should be aligned with this vision.

4.2 COMPREHENSIVE APPROACH AND TAILORED PRIORITIES

The Strategy should result from an all-encompassing understanding and analysis of the overall digital environment, yet be tailored to the country's circumstances and priorities.

Cybersecurity is not only a technical challenge but also a multifaceted issue extending beyond economic and social prosperity into areas such as law enforcement, national and international security, international relations, trade negotiations, and sustainable development.

Priorities should be based on the country's specific context, aligned with national objectives and the Strategy implementation timeline, and supported with appropriate resources. Some cybersecurity issues may be addressed in separate strategic documents (e.g., digital aspects of national security and defense within a national security or defense strategy).

The Strategy should also be clearly aligned with broader digital governance frameworks, such as those for data governance, AI, and digital trust, to ensure policy coherence and institutional resilience. Such integration reinforces the Strategy's comprehensive approach and helps embed cybersecurity within the secure and responsible use of data and emerging technologies, fostering a trusted and sustainable digital environment.

4.3 INCLUSIVENESS

The Strategy should be developed with the active participation of all relevant stakeholders and should address their needs and responsibilities throughout the entire process.

The digital environment is critical to governments, organizations, and individuals. These groups face cybersecurity risks and share responsibility for managing them, depending on their role. Governments should establish partnerships and collaboration mechanisms that include all relevant stakeholders in NCS development and implementation.

While difficult, identifying and meaningfully engaging stakeholders is essential to ensure the Strategy reflects diverse needs and expertise and is successfully implemented. To foster inclusiveness and transparency, the Strategy should be a public document.

4.4 ECONOMIC AND SOCIAL PROSPERITY

The Strategy should foster economic and social prosperity and maximize the contribution of digital technologies to sustainable development and inclusiveness.

Greater connectivity, digitalization, and participation in the digital economy can expedite growth and social progress, advance key societal values, improve public-service delivery and capacity, facilitate international trade, and promote good governance.

The increasing reliance on digital infrastructure for the functioning of societies demands increased attention to cybersecurity. However, cybersecurity is not a goal in itself; the Strategy should be aligned with the country's broader socio-economic objectives, building trust and confidence so that societies can realize these objectives while protecting themselves from cybersecurity risks.

4.5 FUNDAMENTAL HUMAN RIGHTS

The Strategy should respect and be consistent with fundamental human rights.

It should recognize the fact that rights that people have offline must also be protected online. The Strategy should respect universally recognized human rights, including, but not limited to, those enshrined in the United Nations Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, as well as relevant multilateral or regional legal frameworks. Particular attention should be paid to freedom of expression, privacy of communications, and personal data protection. In particular, the Strategy should avoid facilitating arbitrary, unjustified, or otherwise unlawful surveillance, interception of communications, or collection of personal data.

In ensuring that the country is able to take action to meet its legitimate interests while still respecting individuals' human rights, the Strategy should ensure that, where applicable, surveillance, interception, and collection of data only occur within the context of a specific investigation or legal case, under lawful authority, on the basis of a public, precise, comprehensive, and non-discriminatory legal framework, and with effective oversight, procedural safeguards, and remedies in line with international obligations.

4.6 RISK MANAGEMENT AND RESILIENCE

The Strategy should enable efficient management of cybersecurity risks and strengthen the resilience of economic and social activities.

As with other types of risk, cybersecurity risk cannot be entirely eliminated but can be managed and mitigated. The Strategy should encourage entities to prioritize cybersecurity investments, balance risk against opportunities, adopt continuous risk management, and facilitate a coherent approach across interdependent entities and sectors.

Resilience requires preparation for incidents, crisis management, and recovery. The Strategy should encourage the adoption of business continuity and disaster recovery measures to ensure essential services and functions can withstand and recover from disruptions to digital infrastructure.

4.7 APPROPRIATE SET OF POLICY INSTRUMENTS

The Strategy should use the most appropriate policy instruments available to achieve its objectives, considering specific national circumstances.

Governments have different levers and policy instruments at their disposal to achieve their outcomes. These include legislation, regulation, standardization, certifications, incentives, information-sharing mechanisms, education, good practice sharing, norms of behavior, and building communities of trust, among others. Each of these levers has its strengths and weaknesses, comes at a differing cost, and brings different results.

The most effective outcomes are achieved by selecting and balancing these policy instruments and tools according to the intended objective.

4.8 CLEAR LEADERSHIP, ROLES, AND RESOURCE ALLOCATION

The Strategy should be set at the highest level of government, with clear leadership and accountability for its execution. Relevant roles and responsibilities must be assigned, and sufficient human and financial resources allocated.

Cybersecurity should be promoted and sustained at the highest levels of government. Moreover, to ensure accountability and progress, focal points of individual workstreams must be identified, and all parties should have a clear understanding of their respective roles and responsibilities.

The Strategy should also allocate the appropriate human, financial, and material resources necessary for its implementation. This principle needs to guide both the Strategy development process and the elaboration of its Action Plan and related initiatives.

4.9 TRUST ENVIRONMENT

The Strategy should help build a digital environment that citizens and organizations can trust.

Building trust in the national digital ecosystem, in which users' rights and interests are protected, and the security of data and information systems is assured, is essential for realizing the full potential of the social, political, and economic opportunities of digital transformation. The Strategy must enable policies, processes, and actions to secure critical services such as e-governance, e-commerce, digital finance, and telemedicine. By protecting rights and assuring system security, the Strategy fosters trust among both the general population and public- and private-sector organizations delivering digital services.

4.10 TECHNOLOGICAL FORESIGHT AND ADAPTABILITY

Cybersecurity priorities, objectives, and actions must adapt to the evolving digital and risk environment.

Emerging and disruptive technologies (e.g., AI, automation, IoT, quantum computing, 5G/6G, distributed-ledger technologies) bring both opportunities and risks that may reshape the national strategic thinking.

Governments should institutionalize technological foresight, horizon scanning, and regular reviews to anticipate disruptive trends, assess their impact, and adapt policies accordingly. This requires structured engagement with government, industry, academia, and research to integrate innovation insights and international good practices.

The Strategy must be treated as a living framework, capable of evolving alongside technological change while supporting resilience, security, and digital innovation. Reviews and mid-term updates (see Section 3 - Lifecycle) are critical to ensure adaptability is built into the NCS lifecycle.

SECTION 5

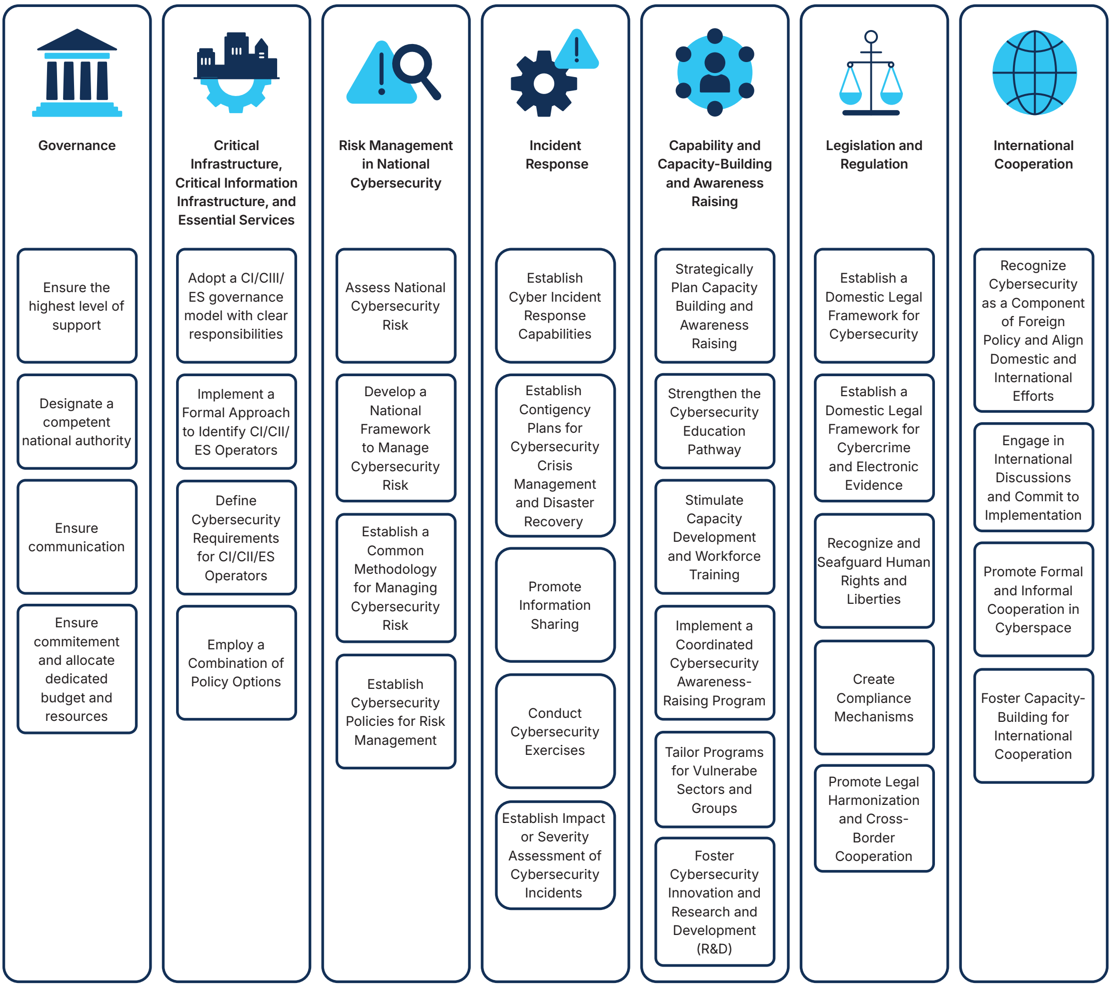
National Cybersecurity Strategy Good Practice

Cybersecurity affects many areas of socio-economic development and is influenced by several factors within the national context.

Therefore, this Section introduces a set of good-practice elements that can make the Strategy comprehensive and effective, while allowing for tailoring to the national context.

These good-practice elements are grouped into distinct focus areas, overarching themes for a comprehensive NCS. While both the focus areas and the good-practice elements have been put forward here as examples of good practice, it is particularly important that the latter are viewed in the national context, as some may not be relevant to a country's specific situation. Countries should identify and follow the good-practice elements that support their own objectives and priorities in line with the vision defined in their Strategy (Section 4.1). The order of the individual elements or focus areas below should not be seen as indicating a level of importance or priority.

Figure 5 - Focus Areas



Governance
- Ensure the highest level of support
- Designate a competent national authority
- Ensure communication
- Ensure commitement and allocate dedicated budget and resources

Critical Infrastructure, Critical Information Infrastructure, and Essential Services
- Adopt a CI/CIII/ES governance model with clear responsibilities
- Implement a Formal Approach to Identify CI/CII/ES Operators
- Define Cybersecurity Requirements for CI/CII/ES Operators
- Employ a Combination of Policy Options

Risk Management in National Cybersecurity
- Assess National Cybersecurity Risk
- Develop a National Framework to Manage Cybersecurity Risk
- Establish a Common Methodology for Managing Cybersecurity Risk
- Establish Cybersecurity Policies for Risk Management

Incident Response
- Establish Cyber Incident Response Capabilities
- Establish Contigency Plans for Cybersecurity Crisis Management and Disaster Recovery
- Promote Information Sharing
- Conduct Cybersecurity Exercises
- Establish Impact or Severity Assessment of Cybersecurity Incidents

Capability and Capacity-Building and Awareness Raising
- Strategically Plan Capacity Building and Awareness Raising
- Strengthen the Cybersecurity Education Pathway
- Stimulate Capacity Development and Workforce Training
- Implement a Coordinated Cybersecurity Awareness-Raising Program
- Tailor Programs for Vulnerabe Sectors and Groups
- Foster Cybersecurity Innovation and Research and Development (R&D)

Legislation and Regulation
- Establish a Domestic Legal Framework for Cybersecurity
- Establish a Domestic Legal Framework for Cybercrime and Electronic Evidence
- Recognize and Seafguard Human Rights and Liberties
- Create Compliance Mechanisms
- Promote Legal Harmonization and Cross-Border Cooperation

International Cooperation
- Recognize Cybersecurity as a Component of Foreign Policy and Align Domestic and International Efforts
- Engage in International Discussions and Commit to Implementation
- Promote Formal and Informal Cooperation in Cyberspace
- Foster Capacity-Building for International Cooperation

5.1 FOCUS AREA 1 - GOVERNANCE

This focus area introduces good-practice elements for governance structures, models, and frameworks for national cybersecurity that can be included in the Strategy. This includes clearly stating the strategic objectives and outcomes the government intends to pursue at the political, operational, and technical levels to increase national resilience and reduce risks to people, companies, critical infrastructures, services, and assets. The Strategy should also identify the roles, responsibilities, authority, powers, and accountability mechanisms of the stakeholders tasked with implementing the Strategy, such as the competent national authority (where applicable).

5.1.1 Ensure the Highest Level of Support

The Strategy should have the formal endorsement of the highest level of government. This endorsement serves two important purposes. First, it improves the likelihood that sufficient resources will be allocated and that coordination efforts will be successful. Second, it signals to the broader national ecosystem that the country's cybersecurity is intertwined with its digital economy and other social and political aspects that depend on digital systems, and therefore must be treated as a national priority.

The Strategy may also need to be codified in the domestic legal framework to obtain national relevance and prioritization.

5.1.2 Designate a Competent National Authority

Effective national cybersecurity governance requires the designation of one or more competent national cybersecurity authorities, depending on the country's size and constitutional structure. In federal or decentralized systems, multiple authorities may be necessary. These authorities should be explicitly identified in the Strategy as responsible for leading and coordinating cybersecurity governance, providing guidance and support for its implementation. To ensure authority and effectiveness, they should be anchored in, or closely connected to, the highest level of government or national leadership, enabling them to provide strategic direction, coordinate action, and monitor implementation.

Tasks of the competent authority may include preparing draft laws and policies on cybersecurity governance, defining and clarifying roles, responsibilities, processes, and decision rights, and ensuring effective implementation of the Strategy. Given that cybersecurity is a cross-cutting domain, it is important that the competent national authority can involve and direct relevant stakeholders. This includes identifying and overseeing the stakeholders responsible for operational tasks or initiatives and establishing related performance targets.

The competent authority should also be responsible for reporting on the progress and outcomes of cybersecurity activities. To facilitate reporting, responsible stakeholders and government entities should be mandated to report back to the competent national authority in measurable terms. Using key performance indicators (KPIs) is an effective way to assess progress and promote accountability by enabling oversight (see Section 3.6 for a description of SMART KPIs).

To enable the competent authority to carry out its tasks, it should be given a clear mandate over all relevant stakeholders. This mandate may have to be formalized in policy or law to empower the authority to perform its functions.

5.1.3 Ensure Communication, Coordination, and Collaboration

Cybersecurity requires a whole-of-nation approach, drawing on the efforts of all of society, and must be built on successful cooperation between different stakeholders, including public and private actors. A national cybersecurity governance system should define the roles, responsibilities, processes, and relationships among various stakeholders to ensure effective, efficient, and accountable delivery of cybersecurity.

The allocation of roles and responsibilities should align with each stakeholder's mandate within the country's constitutional and legal framework. For example, government bodies may deliver public services, civil society may provide oversight and advisory support, and the legislature may be responsible for lawmaking.

Governance must therefore address actors across multiple dimensions, such aslaw and policy, strategy, operations, and technology, and operate across organizational, local, national, regional, and international levels.

5.1.3.1 Ensure Intra-government Cooperation

The Strategy should identify and include the government entities affected by or responsible for its implementation. Intra-governmental commitment, coordination, and cooperation are core functions of governmental institutions and are essential to ensure that governance mechanisms (e.g., standards, regulations, market incentives) and resources yield the desired outcomes of the Strategy. Having a well-established and high-level national cybersecurity competent authority will also help enhance intra-government coordination and cooperation.

Effective communication, coordination, and collaboration ensure that all ministries and government agencies are aware of each other's respective powers, missions, and tasks. Examples include periodic meetings involving relevant stakeholders and the creation of an intra-government task force to address a particular issue.

Intra-government coordination mechanisms should also ensure that cybersecurity policies and actions are consistent across ministries and government agencies, avoiding duplication and promoting coherence with the country's broader digital transformation agenda.

5.1.3.2 Ensure Sectoral Cooperation

The national cybersecurity governance structure should reflect an understanding of the dependencies that the government has on the private sector and other non-governmental stakeholders (and vice-versa) so they can work together on achieving a more secure, safe, and resilient ecosystem in line with the principle of inclusiveness (Section 4.3). To this end, the Strategy should articulate how the government will engage these non-governmental stakeholders and clearly define their roles and responsibilities within the governance framework.

It is good practice for the Strategy to call for the identification of a network of authoritative national contact points for industries essential to the operation and recovery of critical services and infrastructures. Roles assigned to each stakeholder should be consistent with their overall mandate within the national legal and institutional framework.

The Strategy should also be aligned with other national priorities, such as ensuring connectivity is affordable, available, and inclusive; advancing data protection and privacy while promoting innovation; strengthening infrastructure resilience and service availability in the face of disasters, climate change, and pandemics; responsibly exploring and adopting emerging technologies such as AI, blockchain, quantum computing, and distributed ledger technologies. Such alignment ensures that sectoral cooperation on cybersecurity is not siloed, but embedded in broader national objectives for digital transformation, resilience, and sustainable development.

5.1.4 Ensure Commitment and Allocate Dedicated Budget and Resources

Successful national cybersecurity efforts require political commitment and leadership, underpinned by trusted partnerships. Commitment in this context means supporting consistent policies over time to ensure national cybersecurity priorities are delivered. A good practice is to establish safeguards ensuring consistency between the country’s domestic and foreign policy agendas, so one ministry does not undermine another by presenting conflicting positions on the same policy issue (e.g., trade flow vs. export control of dual-use technologies).

This long-term perspective should also apply to cybersecurity governance with respect to emerging technologies: while remaining technologically neutral, it should establish resilient mechanisms to anticipate and manage technological change as the landscape evolves.

Another critical element of national cybersecurity that requires commitment is resourcing. Sufficient, consistent, and continuous funding is foundational to an effective national cybersecurity posture. Governance structures must be designed with dedicated budgets that provide relevant stakeholders with the resources required to carry out their tasks. Resources should be defined in terms of money (i.e., dedicated budget), people, and materials.

The objectives and tasks within the Strategy should not be viewed as a one-time allocation of resources. Resource requirements should be revisited regularly based on progress or shortfalls in implementing tasks or objectives within the Strategy. The government may also consider establishing a central cybersecurity budget managed by a national governance mechanism. Whether consolidating disparate funding sources into a coherent, integrated program or creating a unified intra-governmental budget, the overall program should be managed and tracked through milestones to ensure successful implementation.
Further references are available at www.ncsguide.org.

5.2 FOCUS AREA 2 - CRITICAL INFRASTRUCTURE, CRITICAL INFORMATION INFRASTRUCTURE, AND ESSENTIAL SERVICES

This focus area examines good practices for identifying and protecting Critical Infrastructure (CI), Critical Information Infrastructure (CII), and Essential Services (ES), as well as for strengthening their reliability and resilience.

The potential consequences of an incident impacting CI/CII/ES can be severe, disrupting social order, interrupting the delivery of services, and undermining the economic well-being of a country. The Strategy should therefore emphasize the importance of risk management and resilience efforts aimed at reducing the likelihood and impact of such disruptive or destructive incidents.

There are no universally recognized definitions for CI/CII/ES, which may ultimately depend on geopolitical, socio-economic, and cultural characteristics of the national context. Governments should therefore define these terms based on their national cybersecurity risk assessments, circumstances, and priorities.

This Guide recognizes the lack of common terminology and adopts a flexible approach that allows for different interpretations of the concepts of CI/CII/ES and related operators. These infrastructures and services are highly interdependent, with the functioning of one often relying on others, and disruptions in one area can cascade across multiple systems. Examples include:

- **Critical Infrastructures (CI):** assets essential to the functioning and security of society and the economy (e.g., power plants, water treatment facilities, rail networks).
- **Critical Information Infrastructures (CII):** ICT and operational technology systems (IT and OT) that support key functions of critical infrastructure (e.g., Internet Exchange Points (IXPs), submarine cables, Supervisory Control and Data Acquisition (SCADA) systems, and national data centers).
- **Essential Services (ES):** services necessary to sustain critical societal or economic activities (e.g., electricity supply, digital and mobile communications, public transportation, healthcare services).
- **CI/CII/ES Operators:** public or private entities that own or operate CI and/or CII and provide ES (e.g., Internet Service Providers (ISPs), Domain Name Service providers (DNSs), telecom operators, major hospitals, central banks, water and energy utilities, etc.)
- **Service Level Agreements (SLA):** formal contracts or agreements between CI/CII/ES operators that define expected service levels, performance metrics, responsibilities, and response mechanisms required to maintain operational continuity and resilience across interdependent systems.

5.2.1 Adopt a CI/CII/ES Governance Model with Clear Responsibilities

The Strategy should, at a high level, define the governance structure, roles, responsibilities, and coordination mechanisms of the various stakeholders involved in CI/CII protection, in accordance with the principle of clear leadership, roles, and resource allocation (Section 4.8).

Because CI/CII/ES protection often exceeds the capacity of any single government agency, appointing an overall coordinator for CI/CII/ES cybersecurity, such as an interagency committee, can significantly strengthen coordination and protection efforts.

The governance model for CI/CII/ES protection should include: the identification of government entities in charge of specific sectors; the responsibilities and accountability of operators; the establishment of communication channels and cooperation mechanisms between public and private actors to ensure the continuity and recovery of critical services; mechanisms to promote coordination and alignment among government entities with overlapping mandates; and ways to ensure that sectoral regulators create clear, consistent security requirements that avoid duplication, prevent waste of resources, and streamline compliance efforts across both public and private sectors.

Given the cross-border nature of CI/CII/ES, the governance model should also include mechanisms for regional and international coordination and collaboration.

5.2.2 Implement a Formal Approach to Identify CI/CII/ES

The Strategy should promote the identification of CI/CII/ES through a formal, repeatable, and criteria-based approach. This process should be centrally coordinated, periodically reviewed, and used to inform national risk management, resource allocation, and incident response planning. Outputs typically include a national register of critical sectors, services, functions, operators, and assets, with associated levels of criticality and risk profiles.

While a variety of methodologies exist to identify CI/CII/ES, countries might consider applying sectoral, functional, and impact criteria, such as dependencies and interdependencies with other infrastructure, relevance of the infrastructure for maintaining minimum service levels, redundancies, market share, and geographic location.

Reviews should occur at regular intervals (e.g., every two years) or after major incidents or technological changes to ensure the registry remains accurate and relevant. Early and continuous involvement of relevant stakeholders, including public authorities, regulators, and private infrastructure operators, is essential. The Strategy should also encourage or incentivize private operators to conduct regular Business Impact Analyses (BIAs) and Risk Assessments. These assessments should evaluate the potential effects of disruptions on critical assets, operations, and functions, and their outputs should be shared with relevant authorities to inform national-level identification, business continuity, and disaster recovery planning (Sections 3.2.2, 5.3.1, and 5.4.2).

The Strategy should establish feedback loops to integrate lessons learned from incidents, exercises, and audits into future identification cycles, and promote convergence with regional and international frameworks to support cross-border consistency.

5.2.3 Define Cybersecurity Requirements for CI/CII/ES Operators

The Strategy should either highlight the existing or promote the development of new legislative and regulatory frameworks outlining cybersecurity requirements for CI/CII/ES operators and other relevant stakeholders (in accordance with Section 5.6.1 on Legislation and Regulation). These requirements should be structured so that the targeted operators meet a minimum baseline of cybersecurity practices, while also maintaining flexibility to align with their own risk management priorities.

Baselines should leverage internationally recognized standards and good practices, enabling better integration within global supply chains and avoiding interoperability issues across national borders. Requirements should address a range of cybersecurity practices, such as adopting a risk-oriented approach (in accordance with Sections 4.6 on risk management and resilience and 5.3.2 on national risk assessment); protecting data and systems; securing procurement processes and supply chain; monitoring digital environments and detecting potential anomalies or events; and responding to and recovering from incidents, supported by well-defined incident and crisis management processes, business continuity measures, and disaster recovery plans.

Operators may also be required to maintain Security Operations Centers (SOCs) for real-time monitoring and incident response. Cybersecurity baselines should be proportionate to the risk profile and criticality of the operators involved. A tiered approach can be applied to differentiate between high-impact and lower-impact entities, ensuring efficient allocation of compliance efforts without undercutting core protections.

Cross-sectoral baselines should be developed first, enabling greater interoperability and consistency of sector-specific practices and streamlined compliance for cross-sector functions and subsectors. These can be complemented by sector-specific “how to” guidance, offering options to inform and integrate enterprise practices. These guidelines should also be supported by a set of oversight mechanisms (e.g., performance-based audits, self-assessments, mandatory reporting) to ensure that baseline requirements are not only adopted but also actively maintained.

Cybersecurity baselines should be outcome-focused to ensure greater agility over time as the risk landscape and technology continue to evolve. Articulating what operators should aim to achieve (e.g., “control logical access to critical resources”), rather than prescribing how they should implement security (e.g., “use two-factor authentication”), allows government and industry to benefit from continuous security improvements.

Framing requirements in outcome terms also enables flexibility in implementation, encourages innovation, and reduces the regulatory burden of constant updates. This approach is particularly valuable for adapting to emerging technologies and changing threat environments, as it avoids prematurely locking operators into specific technical solutions.

5.2.4 Employ a Combination of Policy Options

The Strategy should envisage the deployment of a wide range of policy tools to ensure that cybersecurity responsibilities are both enforceable and achievable, in accordance with the principle of a comprehensive approach and tailored priorities (Section 4.2).

To encourage operators across CI/CII/ES to adopt cybersecurity practices commensurate with the risks they face, governments should deploy a balanced mix of incentives and disincentives. Policy options may include: conducting audits and other compliance monitoring efforts; defining liability and accountability measures; developing certification and accreditation schemes; providing financial incentives and subsidies; delivering cyber capacity-building initiatives; and promoting structured public-private partnerships (PPP), such as sectoral Information Sharing and Analysis Centers (ISACs) or Information Sharing and Analysis

Organizations (ISAOs), to facilitate cross-sector intelligence sharing and collective defense (Section 4.7 on using an appropriate set of policy instruments and Section 5.4.3 on promoting information-sharing).

Since operators may not fully internalize the broader societal impacts of cybersecurity incidents, policy interventions are often necessary to ensure that safeguards are adopted not only for corporate benefits but also for the broader public interest. Policy tools should therefore be carefully calibrated to address the gaps between what the markets can and should drive and what the evolving risk environment requires.

Where voluntary or market-based solutions prove insufficient, the Strategy should recognize the role of targeted regulation or direct public intervention, particularly in high-risk or low-competition sectors. At the same time, effective policy frameworks should avoid overregulation that could stifle innovation or duplicate existing efforts, instead streamlining requirements across public and private entities.

Finally, the Strategy should promote regular evaluation of these policy tools, using metrics to assess behavior change, resilience outcomes, and market responsiveness. Adjustments should be made over time based on emerging risks, new technological developments, and lessons learned from implementation. Embedding this review cycle reinforces accountability, ensures sustained alignment with national priorities, and supports long-term resilience across CI/CII/ES (Lifecycle Section).

5.3 FOCUS AREA 3 - RISK MANAGEMENT IN NATIONAL CYBERSECURITY

This focus area introduces good practices for addressing cybersecurity through risk management. As stipulated in the principle of risk management and resilience (Section 4.6), a risk management approach should be adopted, since cybersecurity risks cannot be fully eliminated. Ensuring that a country has a clear understanding of the risks that it faces allows it to prioritize resources, reduce vulnerabilities, and improve overall preparedness. Moreover, the risk management approach should align with national priorities and consider the digital environment in its entirety, in accordance with the principle of comprehensive approach and tailored priorities (Section 4.2). It should focus on identifying interdependencies within and across sectors, as well as risks arising from cross-border dependencies.

The Strategy should ensure that risk management is not treated as a one-time exercise, but as a continuous, data-driven process that integrates strategic foresight, sectoral intelligence, and evolving threat landscapes. Given that cybersecurity threats and the digital environment are extremely dynamic and unpredictable, any risk management approach should be reviewed regularly and designed to address unknown risks. As such, the Strategy should plan for monitoring and evaluation of risk management activities to strengthen resilience and ensure continuous improvement. This includes establishing institutional responsibilities for oversight, evaluation, and refinement of risk management frameworks at national, sectoral, and organizational levels.

5.3.1 Assess National Cybersecurity Risk

The Strategy should promote regular identification, analysis, and assessment of cybersecurity risk at the national level, guided by a formal and repeatable approach. This typically entails estimating the likelihood and potential impact of cybersecurity incidents based on threats, vulnerabilities, and interdependencies of societal functions. Assessments should be dynamic, incorporating threat intelligence, cross-border and geopolitical considerations, and emerging technological risks such as those posed by advances in AI or quantum computing.

The assessment could include sectoral risk profiles for those sectors deemed most critical to society and the economy. Sectoral risk profiles provide a basis for more specific risk assessments and help introduce coherence within and across all sectors nationally. In addition, the assessment should consider CI/CII/ES (Section 5.2.2) and their interdependencies within and across sectors (e.g., between energy, telecommunications, water, and healthcare). It should identify systemic cybersecurity risks whose impacts may cascade across interconnected systems and disrupt the continuity of essential services.

The Strategy should define governance mechanisms for conducting and updating national and sectoral risk assessments, specifying the roles of national cybersecurity authorities, sectoral regulators, intelligence agencies, and key private stakeholders in contributing to and validating the assessment. Such efforts will inform and help align cyber risk management strategies with the country's crisis management plan, while also mobilizing the necessary capabilities, capacities, expertise, funding, and policies to strengthen the overall national cybersecurity posture.

5.3.2 Develop a National Framework to Manage Cybersecurity Risk

The Strategy should promote the development and implementation of a national framework for the consistent and coordinated management of cybersecurity risk across interdependent sectors and assets. The framework should establish a national risk register, securely stored and communicated, to provide government visibility and oversight of risks and approaches taken to manage them. The framework should prioritize risks based on the probability of occurrence and their potential impact. The risk register should consider the nation's risk appetite and tolerance levels across different sectors and functions and guide risk classification accordingly. The national risk register should be dynamic and updated at regular intervals (e.g., annually or after major incidents) based on evolving threats and technology.

The framework should also include mechanisms for aggregating sectoral and organizational risk data, while respecting confidentiality and data protection requirements, to ensure strategic-level visibility without exposing sensitive operational details. It should specify the responsibilities of key entities in each sector for the assessment, acceptance, and treatment of national-level cybersecurity risks, ensuring accountability and clear reporting lines, and supporting coordinated decision-making, such as escalation protocols and decision-making pathways, related to systemic cybersecurity risks.

Additionally, the Strategy should encourage the definition of national-level risk metrics to assess the effectiveness of cybersecurity measures, along with feedback mechanisms to support continuous policy improvement and inform future strategic and operational decisions.

5.3.3 Establish a Common Methodology for Managing Cybersecurity Risk

The Strategy should promote the establishment of a common methodology for managing cybersecurity risks. This will ensure efficiency and consistency across organizations and facilitate the exchange of threat and risk information across interdependent systems. A methodology based on international standards should be favored, as it may reduce costs and improve interaction with the private sector. This common methodology should be adaptable to sector-specific needs and flexible enough to incorporate future changes in technology and threat actors.

The methodology should provide guidance on the full risk management lifecycle, from assessing threats to valuing assets, defining risk appetite and tolerance levels, implementing and maintaining mitigating measures, and accepting residual risk. It should also include a certification program to assess and improve compliance. This certification should be scalable and tiered, offering different levels of controls for organizations of varying sizes and criticality, and aligned with national compliance frameworks as well as relevant international obligations.

Importantly, for the procurement of digital infrastructures or services, the risk management methodology should provide guidance on mechanisms for enhancing the reliability of the supply chain. It should also promote secure-by-design and secure-by-default principles.

5.3.4 Establish Cybersecurity Policies for Risk Management

The Strategy should encourage the establishment of national cybersecurity policies, adopted in accordance with the principle of an appropriate set of policy instruments (Section 4.7) and the principle of comprehensive approach and tailored priorities (Section 4.2). These policies should cover governance, operational, and technical requirements; clarify stakeholder roles and responsibilities; and mandate specific approaches to these issues. To ensure coherence, the Strategy should promote the development of a national cybersecurity policy framework that aligns sectoral efforts, eliminates redundancy, and defines minimum expectations across critical sectors.

Examples of such policies could include requirements for cybersecurity in secure procurement, information-sharing programs, coordinated vulnerability disclosure, minimum security baselines and standards of care, certification programs for compliance, and mandatory reporting to competent authorities. These policies should also define procedures for timely, secure, and standardized incident notification, ensuring compatibility with sector-specific and cross-border reporting obligations.

A coordinated national policy framework would lead to more efficient and effective cybersecurity management, as it would harmonize practices, reduce redundancy, and ensure consistency and interoperability across sectors. To this end, the Strategy should establish mechanisms for policy coordination among regulators, agencies, and private sector stakeholders, such as national working groups, interagency task forces, or advisory councils, with clearly defined mandates and reporting responsibilities to ensure that cybersecurity policies are consistently applied and remain fit for purpose.

5.4 FOCUS AREA 4 - INCIDENT RESPONSE

This focus area provides an overview of good practices that support the establishment and sustainability of national capabilities to prepare for, prevent, detect, mitigate, respond to, and recover from cybersecurity incidents, while improving a country’s overall cyber resilience.

5.4.1 Establish Cyber Incident Response Capabilities

The Strategy should call for the establishment of a national body that serves as a central point of contact to facilitate and coordinate national incident response capabilities across the country. Often, this involves the establishment of Computer Emergency Response Teams (CERTs), Computer Security Incident Response Teams (CSIRTs), or Computer Incident Response Teams (CIRTs)[2] with national responsibility.

The national CERT/CSIRT/CIRT may be complemented by sectoral or organizational teams (e.g., finance, health, energy, transport), which provide sector-specific services and act as intermediaries between organizations and the national CERT/CSIRT/CIRT.

The specific organizational model of a CERT/CSIRT/CIRT may vary (e.g., national, governmental, sectoral), and while not every country has the same needs and resources, these specialized and dedicated teams should provide both proactive and reactive functions, as well as preventive and educational services. These entities can increase a country's ability to respond quickly and recover from incidents, while also reducing adverse impacts and strengthening resilience.

The core service areas that CERTs/CSIRTs/CIRTs typically offer include cyber incident response and coordination, vulnerability management, situational awareness (including threat intelligence and information sharing), and knowledge transfer. The national CERT/CSIRT/CIRT may also host the government Security Operation Center (SOC), providing services such as monitoring, detection, and management of information security events to public agencies.

The Strategy may also encourage the establishment of Security Operations Centers (SOCs) and Product Security Incident Response Teams (PSIRTs) by private-sector entities to enhance their ability to detect threats, manage events, and handle ICT product vulnerabilities. Ultimately, these entities serve as the first line of defense for the management and containment of incidents, feeding into the national response system.

The Strategy should also define and formalize cooperation mechanisms and communication procedures between national, sectoral, and private incident response teams, as well as with regional and/or international counterparts.

5.4.2 Establish Contingency Plans for Cybersecurity Crisis Management and Disaster Recovery

The Strategy should call for the development of a national contingency plan for cybersecurity emergencies and crises. The plan should be integrated into or aligned with the broader national contingency framework. Sector-specific plans for critical information infrastructures and essential services should also be considered.

[2] While there are subtle distinctions in origin and usage, the terms CERT, CSIRT, and CIRT are widely used interchangeably within the incident response community. This guide references the CSIRT Services Framework developed by the Forum of Incident Response and Security Teams (FIRST) to describe the typical range of services offered by response teams https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2-1.

This national cybersecurity contingency plan should integrate inputs from all stakeholders (Principle 4.3 on inclusiveness), as well as findings from national risk assessments and analysis of cross-sector dependencies that may affect the continuity of operations of CI/CII/ES. It should also define escalation procedures, incident categorization criteria, and disaster recovery mechanisms, ensuring clarity on how incidents are prioritized, communicated, and managed.

5.4.3 Promote Information Sharing

The Strategy should call for the establishment of information-sharing mechanisms to facilitate the exchange of actionable intelligence and threat information between and among the public and private sectors.

Formal and informal information-sharing programs can help improve coordination, foster timely and accurate communications during incident response and recovery, and enable the rapid dissemination of threat intelligence among affected parties and other stakeholders. These mechanisms help improve the understanding of how and which sectors have been targeted, identify measures that can be used to mitigate damage to affected assets, and ultimately reduce vulnerabilities and cascading impacts.

The Strategy should designate one or more institutional structures (e.g., CERT/CSIRT/CIRT) responsible for transmitting accurate and actionable information among national stakeholders, including both public and private actors. It may also encourage participation in structured information-sharing mechanisms, such as Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), and other forms of Public-Private Partnerships (PPPs) and cooperative arrangements.

Importantly, information-sharing should be a two-way process. Government entities must contribute relevant information to demonstrate partnership and build trust, thereby encouraging private-sector entities to share their own insights in return. This reciprocal exchange ensures that incident responders remain focused on priority threats and are better prepared to respond effectively.

5.4.4 Conduct Cybersecurity Exercises

The Strategy should encourage the organization and coordination of domestic and international cybersecurity and incident response exercises at the strategic and operational levels. These exercises may take the form of simulations, tabletop exercises, or live operational drills, and should engage both technical and non-technical audiences.

Cybersecurity exercises and related crisis-planning mechanisms can help countries test response procedures, validate communication channels, develop required skills (see Section 5.5 on Capacity-Building), and evaluate the operational readiness of CERTs/CSIRTs/CIRTs to respond to cybersecurity incidents and service disruptions under pressure. They also enhance understanding of cross-sector dependencies and foster institutional capacity for incident response.

Similarly, regional and international cybersecurity exercises can strengthen cyber incident response capabilities across borders, improve understanding of interdependencies, build confidence and trust between governments, stimulate information sharing and collaboration for investigative and judicial cooperation, and enhance collective resilience and preparedness.

5.4.5 Establish Impact or Severity Assessment of Cybersecurity Incidents

The Strategy should encourage the establishment of standardized mechanisms to assess and categorize cybersecurity incidents based on their severity and impact. These assessments aim to evaluate the broader context of cyber-related incidents, including potential and actual impacts on critical sectors, infrastructures, services, and population groups, as well as cascading effects across interdependent systems.

Assessments should be conducted transparently and collaboratively, engaging a wide range of stakeholders. They should be integrated into national disaster recovery and contingency plans, with outcomes feeding directly into the national cyber incident response framework and informing future policy refinements.

5.5 FOCUS AREA 5 - CAPABILITY AND CAPACITY-BUILDING, AND AWARENESS RAISING

Technology and policy frameworks often dominate cybersecurity discourse, yet it is the human element, skills, awareness, and institutional capacity, that ultimately determines the effectiveness of a country’s cyber resilience. This focus area addresses the challenges related to advancing cybersecurity capacity across all levels of society by advancing cyber safety, addressing behaviors, awareness, and cyber hygiene in the digital environment. It focuses on both human and institutional development, aiming to raise awareness among key stakeholders, including government entities, citizens, academia, and the private sector, which are crucial to enabling a country’s digital economy.

Good practices considered in this section include the strategic planning and coordination of capacity-building activities, workforce development programs, the integration of cybersecurity curricula into formal education, and the implementation of targeted awareness-raising campaigns. Furthermore, the section highlights how fostering research, innovation, and cross-sector collaboration between the government, private sector, and academia can enhance national capabilities and support long-term sustainability of cybersecurity efforts.

5.5.1 Strategically Plan Capacity Building and Awareness Raising

Strategic planning is the foundation of effective cyber capacity-building and awareness raising. This process should distinguish between long-term human capital development, which aims to strengthen national expertise and workforce pipelines over a Strategy’s lifecycle, and shorter-term capacity-building efforts, such as targeted training and public awareness campaigns. A well-articulated plan allows for coordination, resource optimization, and accountability across different actors and levels of government.

Long-term human capital planning requires a whole-of-governmental approach, convening relevant ministries, such as education, foreign affairs, justice, labor, economy, and digital affairs, alongside national cybersecurity authorities. This planning process should be evidence-based, identifying future cyber-skills needs, developing national cybersecurity workforce frameworks, and defining measurable KPIs linked to clear implementation pathways from early education through university, postgraduate programs, and advanced research. It should also include timelines, funding models, and mechanisms for periodic review and adjustment.

Importantly, planning the expansion of the cybersecurity workforce presents an opportunity to promote inclusion and gender equality by cultivating expertise across underrepresented communities, rural and economically disadvantaged populations, and women, thereby addressing national-level skills gaps through equitable access to capacity-development opportunities.

The planning process should also guide shorter-term capacity-building initiatives, including executive and operational training, drills, simulations, awareness-raising, and other public outreach activities, such as engagement in events linked to Cybersecurity Awareness Month. While less resource-intensive, these activities require strategic oversight to remain relevant, inclusive, and responsive to changing threat landscapes, communication channels, and public behaviors. These activities should be coordinated and overseen by the competent national cybersecurity agency and embedded throughout the Strategy's implementation period.

A tripartite partnership among government, academia, and the private sector is essential to this planning process, balancing workforce supply and national cyber skills demand. In this collaboration, governments provide direction and incentives, academic institutions and training providers deliver education and skills, and the private sector contributes hands-on experience, innovation, and funding support. This partnership also plays a strategic role in cultivating innovation and entrepreneurship, strengthening the national ecosystem, and supporting the development of a sustainable, forward-looking cybersecurity workforce.

Finally, given national differences in priorities, maturity, and resource level, there is no one-size-fits-all approach to cyber capacity-building. The information gathered should therefore be used to design approaches tailored to each country's specific political, economic, and social context.

5.5.2 Strengthen the Cybersecurity Education Pathway

The Strategy should facilitate the development or expansion of dedicated cybersecurity education pathways aimed at accelerating cybersecurity skills development and awareness throughout the entire formal education system, from early education to higher education and professional training. Curricula should be interdisciplinary and multidisciplinary, covering not only technical but also non-technical cybersecurity skills and topics such as digital literacy, public policy, law, governance, economics, risk management, ethics, social sciences, and international relations.

At the primary and secondary levels, the focus should be on building foundational digital literacy and promoting safe online behavior. In tertiary education, more specialized and advanced programs should be developed, including the integration of cybersecurity courses in all computer science and IT programs, as well as the creation of dedicated cybersecurity degrees and apprenticeships. Apprenticeship programs should be developed through collaborative efforts between government, industry, and educational institutions to ensure that the knowledge and skills acquired through formal education are directly applicable in practice and aligned with industry needs, creating a continuous learning loop that supports both workforce readiness and long-term career development. Adult learners and professionals may require flexible, short-term programs focused on reskilling or upskilling to address evolving workforce demands.

Given the multi-disciplinary nature of cybersecurity education, universities, colleges, training centers, and other educational institutions should be encouraged to work across departments and in partnership with academic and private sector stakeholders to optimize resources and efforts when developing or updating their programs. These institutions can play a critical role in educating the workforce on the unique tenets of cybersecurity and can serve as incubators for the future workforce by combining theory, methodology, tools, and implementation, and by leveraging campus-wide resources to merge knowledge with practical skills.

Strategies could also include the development of cybersecurity workforce frameworks. These frameworks provide a structured approach to identifying, developing, and aligning cybersecurity roles, competencies, and training opportunities across sectors. They support strategic workforce planning and help align educational initiatives with current and emerging industry needs. For example, existing SOCs and PSIRTs could be leveraged as practical training environments or internship opportunities for students wishing to enter operational and product-security roles.

Additionally, curricula should foster awareness of and stimulate interest in cybersecurity career opportunities. To further the efforts, the government and the private sector should consider establishing various incentive schemes, such as scholarships, grants, and private-public partnerships, to support learners and trainees at all levels, particularly in underrepresented communities.

5.5.3 Stimulate Capacity Development and Workforce Training

The Strategy should encourage the development of cybersecurity training and skills development schemes for experts and non-experts in both public and private sectors. This effort could include the provision of executive and operational training, formal internships, traineeships, mentorships, and national or international certifications for security professionals, based on needs identified by industry and government. The Strategy should also encourage targeted training for national-level actors involved in domestic and foreign policy, including regulators and legislators. Trainings should be complemented with initiatives focused on cyber risk management, and with practical exercises within and among government entities and other stakeholders, such as drills and simulations.

These initiatives should target a wide range of beneficiaries, including professionals seeking to enter or advance in the cybersecurity field, public officials, and non-experts whose work intersects with cybersecurity. Government, academia, the private sector, and civil society should act as key implementers and enablers, collaborating to design and deliver training that meets the evolving needs of the cybersecurity ecosystem.

The Strategy should also foster initiatives that aim to develop dedicated cybersecurity career paths and an effective pipeline of future employees, particularly for the public sector, and promote incentives to increase the supply of qualified cybersecurity professionals and help retain talent. These should be created in partnership with academia, the private sector, and civil society.

To address the ongoing gender gap in cybersecurity, a gender-balanced approach that motivates, encourages, and facilitates greater engagement from women should be considered across all efforts aimed at skills development and training. The Strategy should also promote inclusive approaches that reach other underrepresented groups, such as individuals from geographically remote or economically disadvantaged areas, minority communities, and those with disabilities and neurodivergent profiles, many of whom hold significant untapped potential. To attract and retain diverse talent, the Strategy should therefore address accessibility and inclusion at every stage of the talent pipeline.

5.5.4 Implement a Coordinated Cybersecurity Awareness-Raising Program

Entities responsible for cybersecurity awareness campaigns and activities at the national level should collaborate with relevant stakeholders to develop and implement coordinated, data-driven programs focusing on disseminating information about cybersecurity risks and threats, as well as best practices for countering them.

Such efforts could include partnerships with private sector actors, such as banks, telecommunications providers, and digital and social media platforms, that are often best positioned to deliver targeted awareness campaigns on specific cybersecurity risks relevant to their user base, such as financial scams, phishing, and data privacy threats.

5.5.5 Tailor Programs for Vulnerable Sectors and Groups

The Strategy should identify groups in society that require particular attention regarding cyber capacity-building and awareness-raising. Cybersecurity awareness programs could include a variety of initiatives tailored to different audiences: the general public, children, the elderly, individuals with disabilities, digitally challenged populations, schoolteachers, social workers, and executives across the public and private sectors. These programs should explicitly address issues such as cyberbullying, sexual harassment, and online safety. They should promote a culture of cyber hygiene, the responsible use of technology, and critical thinking skills to help individuals identify and respond to online risks.

Tailored programs should be developed for sectors identified as being particularly at risk or in need of empowerment to protect themselves, such as small- and medium-sized enterprises (SMEs), community-based organizations (CBOs), underserved communities or low-income communities.

5.5.6 Foster Cybersecurity Innovation and Research and Development (R&D)

The Strategy should foster an environment that stimulates basic and applied research in cybersecurity across sectors and stakeholder groups. Such initiatives include, for example, ensuring that national research efforts support the objectives of the Strategy, developing cybersecurity-focused R&D programs in public research organizations, effectively developing and disseminating new findings, baseline technologies, techniques, processes, and tools. The Strategy should also aim to develop an efficient, competitive, and sustainable local market for cybersecurity services.

In addition, the Strategy should also promote continuous research into evolving cyber risks affecting diverse population groups, such as youth, the elderly, small businesses, or rural communities, to inform the design of targeted training programs and awareness campaigns that are both relevant and effective.

To this end, governments should promote close collaboration with academia and the private sector to support a dynamic cybersecurity ecosystem. Targeted support for startups and SMEs, including access to funding and incubation programs, can help build a competitive domestic market and ensure the broad availability of cybersecurity products and services.

To promote the development of such solutions, the Strategy could explore incentive mechanisms, including grants, procurement programs, tax credits, competitions, and other initiatives that encourage the development of innovative cybersecurity solutions, products, and services.

Moreover, countries should seek to establish ties with the international research community in the scientific fields related to cybersecurity, such as computer science, electrical engineering, applied mathematics, and cryptography, as well as in non-technical fields such as social and political sciences, business and management studies, criminology, law, and psychology.

5.6 FOCUS AREA 6 - LEGISLATION AND REGULATION

This focus area covers legal and regulatory aspects that should be addressed as part of a national cybersecurity strategy. The Strategy should call for a legal framework to establish cybersecurity mandates and responsibilities, protect society against cybercrime and the misuse of technology, and foster a digital environment in line with the principles of inclusiveness, fundamental human rights, and a trust environment (Sections 4.3, 4.5, and 4.9, respectively). The legal framework should, at a minimum, align with the country's obligations under international, regional, and national human rights law, and should include:

- Establishing or clarifying the roles and responsibilities of national cybersecurity authorities, sector-specific regulators, and coordination mechanisms.
- Granting legal authority to designate critical information infrastructure, together with risk management obligations, security controls, mandatory incident reporting requirements, and national incident reporting platforms.
- Defining substantive cybercrime offenses in criminal law and providing procedural powers and safeguards for investigation, prosecution, and international cooperation.
- Providing compliance, enforcement, and oversight mechanisms, including audit authority, corrective measures, sanctions, and review procedures.
- Enabling international cooperation through cross-border information sharing, mutual legal assistance, and participation in multilateral cybersecurity coordination frameworks.

- Embedding provisions for sustained legal capacity development, regulatory institutionalization, and adaptation of the framework over time in line with international developments.

The Strategy should map the relationship between policy objectives and the legal and regulatory framework, including operational aspects, and should identify gaps, and signal areas where legislative or regulatory adjustment may be needed. It should also recognize the breadth of the legal framework, covering primary legislation, secondary instruments, technical standards, industry codes of practice, and guidelines, and define a process for regular review to ensure proportionality, rights protection, technological responsiveness, and coherence with both domestic and international standards.

5.6.1 Establish a Domestic Legal Framework for Cybersecurity

The Strategy should promote the development of a domestic legal framework that grants clear statutory authority to assign institutional roles, define regulatory mandates, and coordinate the responsibilities of government agencies, sector regulators, and other relevant stakeholders.

The legal framework should set out clear competences to designate CI, CII, and ES, and impose cybersecurity obligations on operators. A statutory designation mechanism should ensure precision, predictability, and proportionality in assigning such obligations (e.g., a tiered obligation structure based on impact criteria; see Sections 5.2.2 and 5.2.3). Transparent designation criteria should guarantee consistent application of rules, while administrative and judicial review procedures should allow operators to appeal designations, dispute regulators' decisions, or challenge sanctions through clearly defined legal channels.

A well-defined legal foundation ensures that limited regulatory resources prioritize entities whose compromise would have national-level impacts. It should also be adaptable to technological developments, in line with the principle of technological foresight and adaptability (Section 4.10), and clearly define the relationship between overarching cybersecurity law and sectoral regulatory regimes, ensuring coherence and avoiding both overlap and regulatory gaps.

5.6.2 Establish a Domestic Legal Framework on Cybercrime and Electronic Evidence

The Strategy should promote the development of a domestic legal framework that clearly defines cybercrime and related criminal offences, and provides adequate procedural powers for effective investigation, prosecution, and adjudication based on admissible electronic evidence.

The framework should define aspects such as substantive criminal offences, procedural powers for the collection of electronic evidence, and evidentiary rules addressing collection, authentication, integrity, chain of custody, and admissibility. Jurisdictional provisions should specify the application of national law to offences committed domestically, against domestic systems, by nationals abroad, or with extraterritorial effects, applying territorial, nationality, or effects-based principles as appropriate.

It should also establish the legal authority for international cooperation (Section 5.7.2), including mutual legal assistance, joint investigative teams, extradition, and participation in international cooperation mechanisms, and should seek alignment with international and regional instruments to ensure effective cross-border enforcement.

In addition, operational aspects of cybercrime investigation and prosecution may be addressed in secondary instruments, such as establishing specialized units, building digital forensic capabilities, developing standard operating procedures (SOPs), and setting up structured crime-reporting mechanisms.

5.6.3 Recognize and Safeguard Human Rights and Liberties

The Strategy should pay particular attention to technology-related legal issues that can affect the level of cybersecurity and have impacts on human rights (e.g., encryption, anonymity, responsible vulnerability disclosure, ethical hacking, and others). In doing so, the Strategy should ensure that both technical security measures and criminal justice responses are consistent with constitutional principles and applicable international human rights obligations (Section 4.5). Differences between cybersecurity (technical and preventive measures) and cybercrime (criminal justice responses) should be recognized and addressed in a manner that maintains the appropriate balance between security and rights protection.

One aspect that may be addressed in the legal framework design considerations as part of the NCS is the definition of how personal data may be processed for legitimate cybersecurity and cybercrime purposes, while embedding safeguards that uphold data protection principles. Data protection rules should be integrated into cybersecurity and law enforcement frameworks to ensure protection from unlawful access and use, and proper handling of personal data during investigations and incident response.

Safeguards for investigatory powers should require judicial or independent authorization, be grounded in the principles of necessity and proportionality, and provide effective legal remedies for individuals affected by state surveillance or investigative measures. Strategic considerations regarding cybercrime legislation should establish lawful tools for authorities to investigate and prosecute serious offences, while embedding procedural protections to prevent overbroad surveillance, politically motivated prosecutions, or violations of privacy rights. The Strategy's legal considerations should also consider how to prevent the criminalization of legitimate cybersecurity activities, such as ethical hacking, penetration testing, coordinated vulnerability disclosure, or security research, which contribute to a safer digital environment.

5.6.4 Create Compliance Mechanisms

The Strategy should promote the establishment of compliance, enforcement, and oversight mechanisms to ensure that the legal framework for cybersecurity and cybercrime is effectively implemented and enforced. Legislation should convert statutory obligations into clear, auditable requirements, preserve legal certainty for regulated entities, maintain institutional accountability, and provide defined legal avenues to contest enforcement actions.

The framework should grant competent authorities supervisory powers to conduct audits, inspections, compliance monitoring, and reviews of incident response, as well as to issue corrective orders with remediation deadlines and impose proportionate administrative, financial, or operational sanctions.

Oversight mandates should be clearly allocated among national cybersecurity authorities, sector-specific regulators, and coordination bodies to prevent duplication, fragmentation, or conflicting requirements.

Given the potential legal and economic consequences of enforcement decisions, procedural safeguards should ensure transparency, proportionality, and fairness. These include defined administrative appeal procedures, judicial review options, and legal standards for assessing the justification and reasonableness of sanctions.

Enforcement should be balanced with incentives that promote voluntary reporting and cross-sector information sharing. Safe harbor provisions for timely, good-faith incident disclosure, confidentiality protections for shared threat intelligence, and explicit separation between enforcement functions and cooperative information-sharing functions (e.g., CERTs/CIRTs/CSIRTs, SOCs, ISACs/ISAOs, or PSIRTs) can help maintain trust and encourage collaboration, while ensuring accountability.

5.6.5 Promote Legal Harmonization and Cross-Border Cooperation

The Strategy should recognize the cross-border dimension of cybersecurity, consider the ratification of international cooperation agreements, and encourage the alignment of the national legal framework with international cooperation standards. Shared standards support legal certainty and the protection of national interests and priorities in cross-border data sharing and cybersecurity efforts spanning multiple jurisdictions.

The legal framework should grant national authorities clear powers to engage in structured international cooperation while safeguarding domestic mandates and national security priorities. These provisions should enable timely information sharing and ensure consistent handling of shared data under confidentiality and data protection rules. They should also facilitate mutual legal assistance and cross-border investigations, support coordinated responses to cybersecurity incidents, and provide mechanisms for resolving jurisdictional conflicts.

Additionally, the Strategy should promote harmonization of national legislation with regional and international instruments, such as the Council of Europe Convention on Cybercrime (Budapest Convention), the UN Convention against Cybercrime (2024), OECD recommendations, Mutual Legal Assistance Treaties (MLATs), and other relevant frameworks. Such integration should follow careful institutional tailoring to ensure legal and operational coherence and to avoid fragmented legislation, overlapping obligations across regulations, or mandates that exceed the administrative or technical capacity of national institutions and regulated entities.

5.7 FOCUS AREA 7 - INTERNATIONAL COOPERATION

This focus area emphasizes the elements that the Strategy should cover regarding the external cybersecurity engagements of a country at the bilateral, regional, and international levels. At the bilateral level, this could involve establishing cyber cooperation agreements with key partner countries, for instance, on information sharing, incident response, or cyber capacity-building. Regionally, the country should consider active participation in relevant regional organizations and frameworks that address cybersecurity-related matters. At the international level, engagement with global organizations, particularly the United Nations, standardization bodies, and intergovernmental or multistakeholder platforms, is essential. These efforts could also include public-private partnerships. Cooperation with private sector actors (e.g., antivirus companies, SOCs, PSIRTs, ISACs/ISAOs, the threat intelligence community, social media providers, and global digital platforms) should be recognized as an essential component of international cooperation.

With digitalization impacting all areas of international relations, including human rights, economic and social development, trade negotiations, commercial relations, the development and use of emerging and disruptive technologies, supply chain security, and broader issues of stability, peace, and conflict resolution, cybersecurity has become an indispensable part of a country's foreign policy. The Strategy should therefore recognize the borderless nature and international dimension of cybersecurity, highlighting the need to engage in international discussions and to cooperate with national, regional, and international stakeholders, as well as civil society, industry, non-governmental organizations, and academia.

In doing so, the Strategy should consider existing regional and international frameworks to prevent fragmentation, leverage good practices, and facilitate cross-border collaboration. Engagement with international public and private stakeholders is key to fostering constructive dialogue, developing trust and cooperation mechanisms, finding mutually acceptable solutions, and addressing common challenges, while building a global understanding of the importance of cybersecurity and resilience. Regional and international cooperation should be fostered in harmony with the political, social, cultural, and economic priorities of the country, in line with the principle of a comprehensive approach and tailored priorities (Section 4.2).

5.7.1 Recognize Cybersecurity as a Component of Foreign Policy and Align Domestic and International Efforts

The Strategy should clearly articulate the government's priority areas and indicate long-term objectives for international cooperation, including which stakeholders (e.g., public, private, regional, global) should be engaged.

The Strategy should express a commitment to international cooperation on cybersecurity and recognize cybersecurity issues as an integral component of the country's foreign policy across all relevant areas, including international peace and security, trade negotiations, cybercrime, and cyber capacity-building (CCB).

Moreover, the Strategy should ensure consistency between the country's domestic and foreign policy agendas and align national cybersecurity approaches with its international efforts. This includes adopting policies and harmonizing the national legal framework to reflect the country's obligations and commitments under international law. Such areas might include, for instance, support for international cybersecurity norms and confidence-building measures (CBMs); commitment to CCB; participation in the development of international cybersecurity standards; and joining existing regional and international processes.

This may also require harmonization among different governmental entities (a whole-of-government approach), including the Head of State and Cabinet, Ministry of Foreign Affairs, Ministry of Digitalization (or Digital Transformation), Ministry of Industry and Trade, Ministry of Justice, Ministry of Defense, national CERT/CSIRT/CIRT, and other institutions with national security, cyber, or digital responsibilities. This ensures that positions expressed by one domestic entity at a negotiating table in the international arena are properly coordinated and aligned across government.

5.7.2 Engage in International Discussions and Commit to Implementation

The Strategy should identify specific international fora and cooperation mechanisms that the country will join or cooperate with at the bilateral, regional, and international levels to effectively engage on cyber-related issues. It should reaffirm the country's commitment to the application of international law to cyberspace, including the Charter of the United Nations and international humanitarian and human rights law, and may also outline a national position on how international law applies to this domain.

The Strategy should commit to joining and implementing existing regional and international instruments aimed at combating cybercrime and addressing other cyber threats, such as the Council of Europe Convention on Cybercrime (Budapest Convention), the UN Convention against Cybercrime, or relevant regional conventions (Section 5.6.5). The Strategy should also acknowledge that many international trade agreements include digital or cyber provisions (e.g., cross-border data flows, dual-use technologies).

Commitments may include the implementation of the UN framework for responsible state behavior in the use of ICTs, endorsed by the General Assembly, encompassing norms, CBMs, and CCB. The Strategy may also emphasize participation in other relevant regional and international processes, such as the UN Global Mechanism on ICTs in the context of international security. The Global Mechanism is a state-led, permanent mechanism with the aim of promoting an open, secure, stable, accessible, and peaceful ICT environment.

To ensure credibility, the Strategy should stress measurable objectives, allocate adequate resources (human and financial), define mandates for international engagement, and establish accountability mechanisms for evaluating results.

5.7.3 Promote Formal and Informal Cooperation in Cyberspace

The Strategy should emphasize both formal and informal international cooperation mechanisms across the public and private sectors that the country intends to engage in. Formal cooperation refers to structured, often legally binding arrangements such as treaties, conventions, and institutional partnerships that promote collaboration on policy, legislation, and law enforcement (e.g., INTERPOL, WIPO). Informal cooperation involves more flexible, trust-based networks that enable the voluntary exchange of information and expertise, without legally binding commitments, such as multistakeholder forums (e.g., GFCE, IGF); incident response and threat-sharing mechanisms (e.g., FIRST, ISACs, ISAOs, SOC-CSIRT networks, the Global Intergovernmental Points of Contact Directory on the Use of ICTs in the Context of International Security); and regional trust-building initiatives. Participation in these efforts facilitates improved coordination, timely exchange of information among relevant authorities, and collaborative responses to threats and vulnerabilities. The Strategy should also support strengthening legal frameworks to facilitate international cooperation (Section 5.6.5).

5.7.4 Foster Capacity-Building for International Cooperation

As the country undertakes international engagements related to cyberspace, it will need to develop or expand competencies and skills across all relevant government bodies, including expertise on cyber diplomacy, international law, data protection and privacy, trade, emerging and disruptive technologies, supply chain security, and other digital matters.

In order to effectively engage in international discussions and cooperation, the Strategy should encourage the development of dedicated cyber diplomacy capacity within government, for example by establishing a specialized office, appointing cyber diplomats, or designating trained personnel as focal points within existing government portfolios or ministries. These officials should be equipped to engage in international fora, negotiate cyber-related issues, and coordinate cross-border cybersecurity cooperation.

Other capacity-building priorities may include strengthening the ability of the national CERT/CSIRT/CIRT to cooperate internationally; enhancing law enforcement and judicial cooperation; building skills to apply international law and norms in cyberspace; and participating in international cyber exercises. Governments should leverage existing international capacity-building programs (e.g., GLACY+, Global Forum on Cyber Expertise (GFCE), INTERPOL, etc.) to develop these competencies. For instance, law enforcement capacity-building efforts can help local and national law enforcement agencies enhance their skills, knowledge, and technical capabilities to leverage high-tech tools and systems for cross-border cybercrime prevention, detection, investigation, and prosecution. They can also allow law enforcement to keep abreast of cybercrime trends and the ever-evolving threat landscape to stay ahead of crime.

The Strategy should also encourage peer learning, knowledge, and skills transfer with international partners, and emphasize participation in international cybersecurity exercises and cross-border incident response drills as both capacity-building and trust-building measures.

SECTION 6

Reference Materials

To prepare this Guide, we reviewed existing guides, frameworks, and good practices from around the world. This process allowed us to identify a wide range of resources that can support countries in designing, implementing, and sustaining their national cybersecurity strategies.

This section brings together these references in a comprehensive catalogue, so readers can explore the principles, concepts, and approaches discussed throughout the Guide in greater depth and apply them to their own national context. While not exhaustive, this collection offers a strong foundation for policymakers, practitioners, and researchers to build upon, and encourages continued exploration of newly available resources.

In this version of the Guide the Reference Section is available on its website (www.ncsguide.org), enabling simplified access and maintenance to keep references up to date.

Reference section available at www.ncsguide.org.

SECTION 7

Acronyms

Acronym	Definition
AI	Artificial Intelligence
AU	African Union
BIAs	Business Impact Analyses
C3SA	Cybersecurity Capacity Centre for Southern Africa
CBA	Cost-Benefit Analysis
CBMs	Confidence-Building Measures
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CCB	Cyber Capacity-Building
CBOs	Community-Based Organizations
CERTs	Computer Emergency Response Teams
CII	Critical Information Infrastructure
CIRTs	Computer Incident Response Teams
CISRTs	Computer Security Incident Response Teams
CI	Critical Infrastructure
CoE	Council of Europe
CRI	Cybercrime Research Institute
CTO	Commonwealth Telecommunications Organisation
DCAF	Geneva Centre for Security Sector Governance
Diplo	DiploFoundation
EBRD	European Bank for Reconstruction and Development
eGA	e-Governance Academy
ENISA	European Union Agency for Cybersecurity
ES	Essential Services
EU CyberNet	European Union CyberNet
FIRST	Forum of Incident Response and Security Teams
GCSCC	Global Cyber Security Capacity Centre
GFCE	Global Forum on Cyber Expertise
GLACY+	Global Action on Cybercrime Extended
GPD	Global Partners Digital
ICCs	International Coordinating Committees
ICT	Information and Communication Technology
IADB	Inter-American Development Bank
IFIs	International Financial Institutions
IGO	Intergovernmental Organization
IGF	Internet Governance Forum
IMF	International Monetary Fund
INTERPOL	International Criminal Police Organization
IoT	Internet of Things
ISACs	Information Sharing and Analysis Centers
ISAOs	Information Sharing and Analysis Organizations
IT	Information Technology

ITU	International Telecommunication Union
IXPs	Internet Exchange Points
KPIs	Key Performance Indicators
LFA	Logical Framework Approach
MDBs	Multilateral Development Banks
MLATs	Mutual Legal Assistance Treaties
NCS	National Cybersecurity Strategy
OAS	Organization of American States
OECD	Organisation for Economic Co-operation and Development
PPP	Public–Private Partnerships
PSIRTs	Product Security Incident Response Teams
R&D	Research & Development
SCADA	Supervisory Control and Data Acquisition
SLA	Service Level Agreement
SMART	Specific, Measurable, Achievable, Relevant, Time-related
SMEs	Small- and Medium-Sized Enterprises
SOCs	Security Operations Centers
ToC	Theory of Change
UNDP	United Nations Development Programme
UNICRI	United Nations Interregional Crime and Justice Research Institute
UNIDIR	United Nations Institute for Disarmament Research
UNOCT	United Nations Office of Counter-Terrorism
UNODA	United Nations Office for Disarmament Affairs
UNODC	United Nations Office on Drugs and Crime
UNU	United Nations University
WB	World Bank
WEF	World Economic Forum
WIPO	World Intellectual Property Organization