Strategic Engagement in Cybersecurity

Guide to Developing a National Cybersecurity Strategy

2nd Edition 2021

Partners


COUNCIL OF EUROPE
CONSEIL DE L'EUROPE


The Commonwealth


CTO
COMMONWEALTH
TELECOMMUNICATIONS
ORGANISATION


DCAF
Geneva Centre
for Security Sector
Governance


Deloitte.


FIRST
Improving Security Together


Global
Cyber Security
Capacity Centre


GCSP
Geneva Centre for
Security Policy


GLOBAL
PARTNERS
DIGITAL


INTERPOL


ITU


Microsoft


CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE


POTOMAC INSTITUTE
FOR POLICY STUDIES


THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP


UNIDIR
UNITED NATIONS INSTITUTE
FOR DISARMAMENT RESEARCH


UNITED NATIONS
OFFICE OF COUNTER-TERRORISM


UNITED NATIONS
UNIVERSITY
Institute in Macau

Observers


AXON


CYBER READINESS
INSTITUTE


GFCE


OAS
More rights
for more people

Some Rights Reserved

Place des Nations
1211, Geneva 20
Switzerland

This Guide was developed by twenty partners from Intergovernmental and International Organisations, private sector, as well as academia and civil society and included the following organisations: Council of Europe (CoE), Commonwealth Secretariat (ComSec), Commonwealth Telecommunications Organisation (CTO), Geneva Centre for Security Sector Governance (DCAF), Deloitte, Forum of Incident Response and Security Teams (FIRST), Global Cyber Security Capacity Centre (GCSCC), Geneva Centre for Security Policy (GCSP), Global Partners Digital (GPD), International Criminal Police Organization (INTERPOL), International Telecommunication Union (ITU), Microsoft, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Potomac Institute for Policy Studies (PIPS), RAND Europe, World Bank, United Nations Institute for Disarmament Research (UNIDIR), United Nations Office of Counter-Terrorism (UNOCT), United Nations University (UNU). Axon Partners Group (Axon), the Cyber Readiness Institute (CRI), the Global Forum on Cyber Expertise (GFCE), the Organization of American States (OAS), and the World Economic Forum (WEF) contributed to the Guide as observers. All the above-mentioned entities are hereinafter collectively referred to as "Contributors".

Rights & Permissions

Telecommunication Union (ITU), Microsoft, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Potomac Institute for Policy Studies (PIPS), RAND Europe, World Bank, United Nations Institute for Disarmament Research (UNIDIR), United Nations Office of Counter-Terrorism (UNOCT), United Nations University (UNU). The above-mentioned organizations shall not be liable for any content or error in this translation.

Adaptations — If you create an adaptation of this work, please add the following disclaimer along with the attribution: *This is an adaptation of an original work* by Council of Europe (CoE), Commonwealth Secretariat (ComSec), Commonwealth Telecommunications Organisation (CTO), Geneva Centre for Security Sector Governance (DCAF), Deloitte, Forum of Incident Response and Security Teams (FIRST), Global Cyber Security Capacity Centre (GCSCC), Geneva Centre for Security Policy (GCSP), Global Partners Digital (GPD), International Criminal Police Organization (INTERPOL), International Telecommunication Union (ITU), Microsoft, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Potomac Institute for Policy Studies (PIPS), RAND Europe, World Bank, United Nations Institute for Disarmament Research (UNIDIR), United Nations Office of Counter-Terrorism (UNOCT), United Nations Office on Drugs and Crime (UNODC), United Nations University (UNU). *Views and opinions expressed in the adaptation are the sole responsibility of the author or authors of the adaptation and are not endorsed by above mentioned organizations.*

Third-Party Content — The Contributors do not necessarily own each component of the content contained within the work. They therefore do not warrant that the use of any third-party-owned individual component or part contained in the work will not infringe on the rights of those third parties. The risk of claims resulting from such infringement rests solely with you. If you wish to re-use a component of the work, it is your responsibility to determine whether permission is needed for that re-use and to obtain permission from the copyright owner. Examples of components can include but are not limited to, tables, figures, or images.

Any requests for use exceeding the scope of the aforementioned license (CC BY-NC 3.0 IGO) should be addressed to the International Telecommunication Union (ITU), Place des Nations, 1211 Geneva 20, Switzerland; email: itumail@itu.int

Disclaimers; privileges and immunities

The findings, interpretations, and conclusions expressed in this publication do not necessarily reflect the views of the Contributors, their secretariats or their governing bodies. The Contributors do not guarantee the accuracy of the data included in this work. The boundaries, colours, denominations, and other information shown on any graphic or chart in this work do not imply any judgment on the part of the IGOs concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

Nothing herein shall constitute or be considered to be a limitation upon or waiver of the privileges and immunities to which certain Contributors are entitled under national laws and international agreements, all of which are specifically reserved.

Joint foreword

Over the last two decades, people worldwide have benefitted from the growth and adoption of information and communication technologies (ICTs) and associated socio-economic and political opportunities. Digital transformation can be a powerful enabler of inclusive and sustainable development, but only if the underlying infrastructure and services that depend on it are safe, secure, and resilient. To reap the benefits and manage the challenges of digitalization, countries need to frame the proliferation of ICT-enabled infrastructures and services within a comprehensive national cybersecurity strategy.

To help governments in this endeavour, a consortium of partner organisations jointly developed and published the first Guide to Developing a National Cybersecurity Strategy (NCS) in 2018. Since then, the number of national cybersecurity strategies or frameworks worldwide has increased significantly. In 2018, only 76 countries had adopted a strategy while today more than 127 countries have such strategies in place, and many have used the Guide as a reference and blueprint.[1]

However, the fast-changing nature of cyberspace, the increased dependency on ICT, and the proliferation of digital risks all call for continuous improvements to national cybersecurity strategies. Most countries have both accelerated their digital transformation and become increasingly concerned about the immediate and future threats to their critical services, infrastructures, sectors, institutions, and businesses, as well as to international peace and security, that could result from the misuse of digital technologies and inadequate resilience. This second edition of the Guide could not come at a more critical time. The updated content reflects the complex and evolving nature of cyberspace, as well as the main trends that can impact cybersecurity and should, therefore, be included into national strategic planning. The objective of the Guide is to instigate strategic thinking and continue supporting national leaders and policy-makers in the ongoing development, establishment, and implementation of such national cybersecurity strategies and policies. We are confident that this new Guide will serve as a useful tool for all stakeholders with cybersecurity responsibilities.

As in the previous edition, this Guide is the result of a unique, collaborative, and equitable multi-stakeholder cooperation effort among partners working in the field of national cybersecurity strategies, policies, and cyber capacity-building. Twenty expert organisations from the public and private sectors, as well as academia and civil society, shared their experience, knowledge, and expertise to produce this updated Guide, which draws from existing know-how from the participating organisations, as well as references to complementary publications and other available resources.

We would like to express our gratitude to the partners involved for their invaluable support and commitment in making this project a great achievement as a concrete example of a successful multistakeholder collaboration. We want to encourage this partnership to continue to collaborate and we look forward to working even more closely with governments, regional and international

[1] Global Cybersecurity Index reports 2018 and 2020 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

bodies, law enforcement, academia, the private sector, civil society, and the United Nations entities to promote strategic reflections on cybersecurity, cyber capacity-building, and cyber resilience.

Jointly signed by:

Mr. Jorge Martínez Morando
Partner, Axon Partners Group Consulting

Mr. Alexander Seger
Head of Cybercrime Division, Council of Europe

Ms. Lessie Longstreet
Global Director, Outreach and Partner Engagement, Cyber Readiness Institute

Dr. Luis Franceschi
Senior Director, Governance and Peace Directorate, Commonwealth Secretariat

Ms. Bernadette Lewis
Secretary General, Commonwealth Telecommunication Organisation

Ambassador Thomas Guerber
Director, Geneva Centre for Security Sector Governance

Mr. Andrea Rigoni
Partner and Global Governments & Public Services Cyber Leader, Deloitte

Mr. Chris Gibson
Executive Director, Forum of Incident Response and Security Teams

Prof. Sadie Creese
Director, Global Cyber Security Capacity Centre

Ambassador Thomas Greminger
Director, Geneva Centre for Security Policy

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

Ms. Lea Kaspar
Executive Director, Global Partners Digital

Mr. Craig Jones
Director of Cybercrime, INTERPOL

Ms. Doreen Bogdan-Martin
Director, Telecommunication Development Bureau, International Telecommunication Union

Ms. Amanda Craig
Senior Director, Cybersecurity Policy, Microsoft

Col. Jaak Tarien
Director, NATO Cooperative Cyber Defence Centre of Excellence

Ms. Melissa Hathaway
President, Hathaway Global Strategies LLC, and Senior Fellow at the Potomac Institute for Policy Studies

Ms. Nicole Klingen
Acting Director, Digital Development, The World Bank

Dr. Robin Geiss
Director, United Nationas Institute for Disarmament Reasearch

Dr. Jehangir Khan
Director, United Nations Counter-Terrorism Centre, United Nations Office of Counter-Terrorism

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

Mr. Georges de Moura
Head of Industry Solution, Center for Cybersecurity, World Economic Forum

Contents

Preface

The Guide to Developing a National Cybersecurity Strategy is one of the most comprehensive overviews of what constitute successful cybersecurity strategies. It is the result of a unique, collaborative, and equitable multi-stakeholder effort.

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

The Guide was developed through an iterative approach, which sought to reach agreement through consensus-building. It is based on existing resources and aims to facilitate its use by national stakeholders. Wherever possible, the relevant sources and tools used to develop each set of recommendations are listed in the Reference section 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 second 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 and implementation of this type of official document, including national 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, as well as adapted for industry or used for academic research.

Note to readers on the update

Version 2 of the Guide to Developing a National Cybersecurity Strategy updates, refines, clarifies, and expands on Version 1, which was published in 2018. Since then, the cyber risk landscape has evolved and become increasingly more complex, and this iteration attempts to capture the main cybersecurity trends that should be taken into consideration in the national strategic planning. While Version 2 expands and enhances the content of version 1, it does not change the structure of the Guide nor the level of detail. Compatibility with version 1 has been an explicit objective of this revision. The updates made can be summarized as follows:

- Importance of funding with intent and investing in necessary resources: more detailed language has been incorporated to emphasize the need to invest in the necessary economic, human, and organisational resources for the full lifecycle of the Strategy (development, implementation, and revision);

- Stakeholders involvement: this version reiterates the crucial role of the private sector and civil society in the processes of incident response and management, information sharing, and awareness raising both domestically and abroad. Also, more emphasis is given to the role that international stakeholders can play in the development and implementation of a national cybersecurity strategy. There are a wide variety of international

organisations, non-governmental organisations, and multilateral organisations that specialise in supporting national governments;

- Resilience and interdependencies: the updated content stresses the importance of considering a country's internet-infrastructure entanglements and the resulting dependencies and vulnerabilities, the interconnections and interdependencies across sectors, and other supply chain risks. It provides more detailed good practices to encourage cooperation among different stakeholders to address increasing risks and improve resilience in the face of the expanding threat landscape;

- Multidisciplinary approach to cyber capacity building: this version of the Guide recognises that cybersecurity applies to all verticals of society, and provides more detailed recommendations to develop capacity building activities that are inclusive and multidisciplinary, including policy, law enforcement, education, awareness, and diplomacy efforts;

- Legislation, regulation, and human rights: this version has significantly expanded the coverage of good practices relating to the development of domestic cybersecurity and cybercrime legislation and regulation, and on the safeguarding of human rights and liberties.

- International cooperation: the updated Guide further emphasises the areas that a Strategy could cover in terms of cybersecurity cooperation and engagement at the regional and international levels, including on international trade agreements, regional economic partnerships, and voluntary norms of responsible state behaviour in cyberspace. It stresses the importance of international law enforcement cooperation and formal or informal mechanisms to share information, build trust, and support cross-border cooperation in combating cybercrime and other cyber-enabled crimes.

Section 1

Document Overview

1.1 Purpose

The purpose of this document is to guide national leaders and policy-makers in the development of a National Cybersecurity Strategy, 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 security posture and to assist policy-makers in the development of a Strategy that takes into consideration a country's specific situation, cultural and societal values, and that encourages the pursuit of secure, resilient, ICT-enhanced and connected societies.

The Guide is a unique resource, as it provides a framework that has been agreed on by organisations 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 successful national cybersecurity strategies.

1.2 Scope

Cybersecurity is a complex challenge that encompasses multiple different governance, policy, operational, technical and legal aspects. This Guide attempts to address, organise, and prioritise many of these areas based on existing and well-recognised models, frameworks and other references. The Guide focuses on protecting civilian aspects of cyberspace and as such, it highlights the overarching principles and good practice that need to be considered in the process of drafting, developing and managing a National Cybersecurity Strategy.

To this end, the Guide makes a clear distinction between the "process" that will be adopted by countries during the lifecycle of a National Cybersecurity Strategy (initiation, stocktaking and analysis, production, implementation, reviews) and the "content", 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 cyber-capabilities by a country's military, defence forces, or intelligence agencies, even though a number of countries have been developing such capabilities.

In order to provide direction and good practice on "what" should be included in a National Cybersecurity Strategy, as well as on "how" to build, implement and review it, this Guide addresses both elements.

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 implementation plans.

Finally, this Guide offers policy-makers a holistic, high-level overview of existing approaches and applications, and a reference to additional and complementary resources that can inform specific national cybersecurity efforts.

1.3 Overall structure and usage of the Guide

This Guide has primarily been structured as a resource to help government stakeholders in preparing, drafting and managing their National Cybersecurity Strategy. As such, the content is organised to follow the process and order of a 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 considered during the development of a Strategy;
- **Section 5** – Focus areas and good practices: identifies the key elements and topics that should be considered during the development of a Strategy; and
- **Section 6** – Supporting reference materials: provides further pointers to relevant literature that stakeholders can review as part of their drafting effort.

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 policy-makers responsible for developing a National Cybersecurity Strategy. The secondary audience are all other public and private stakeholders involved in the development and implementation of a Strategy, such as responsible government staff, regulatory authorities, law enforcement, ICT providers, critical infrastructure operators, civil society, academia, and research institutions. The Guide could also prove useful to the different stakeholders in the international development community that provide assistance in cybersecurity.

Section 2

Introduction

Since its creation, Information and Communication Technology has 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 started to launch digital strategies and to fund projects that increase Internet connectivity and leverage the benefits stemming from the use of ICTs, to stimulate economic growth, to increase productivity and efficiency, to improve service delivery and capacity, to provide access to business and information, to enable e-learning, to enhance workforce skills and to promote good governance. Countries cannot ignore the opportunities associated with becoming connected and participating in the Internet economy.

While the reliance of our societies on the digital infrastructure is growing, technology remains inherently vulnerable. The confidentiality, integrity and availability of ICT infrastructure are challenged by rapidly evolving risks, including electronic fraud, theft of intellectual property and personal identifiable information, disruption of service, and damage or destruction of property. The transformational power of ICTs and the Internet as catalysts for economic growth and social development are at a critical point where citizens' and national trust and confidence in the use of ICTs are being eroded by cyber-insecurity.

To fully realise the potential of technology, states must align their national economic visions with their national security priorities. If the security risks associated with the proliferation of ICT-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 the national security goals they are seeking. In response, nations 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 to their nations. This document will look specifically at defensive 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" is meant to describe the collection of tools, policies, guidelines, risk management approaches, actions, trainings, best practices, assurance, and technologies that can be used to protect the availability, integrity, and confidentiality of assets in the connected infrastructures pertaining to government, private organisations, and citizens; these assets include connected computing devices, personnel, infrastructure, applications, digital services, telecommunications systems, and data in 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 the particular country's objectives and levels of cyber-readiness. Therefore, there is no established and commonly 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 tasked with improving cybersecurity of the nation and their respective roles and responsibilities; and;
- a description of the steps, programmes and initiatives that a country will undertake to protect its national cyber-infrastructure and, in the process, increase its security and resilience.

Setting the vision, objectives, and priorities upfront enables governments to look at cybersecurity holistically across their national digital ecosystem, instead of at a particular sector, objective, or in response to a specific risk – it allows them to be strategic. Priorities for national cybersecurity strategies vary by country, so while the focus for one country may be addressing critical infrastructure-related risks, for others it may be protecting intellectual property, promoting trust in the online environment, or improving cybersecurity awareness of the general public or a combination of these issues.

The need to identify and subsequently prioritise investments and resources 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 other ICT-related objectives. Cybersecurity is central to achieving socio-economic objectives of modern economies and the Strategy should reflect how those are supported. This can be done by referencing existing policies that seek to implement a country's digital or developmental agendas or by assessing how cybersecurity can be incorporated into them.

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

Section 3

Lifecycle of a National Cybersecurity Strategy

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

- Phase I – Initiation
- Phase II – Stocktaking and analysis
- Phase III – Production
- Phase IV – Implementation
- Phase V – Monitoring and evaluation

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

This Section ultimately aims to provide the reader with an understanding of the steps to be taken by a nation in order to draft a National Strategy and the possible mechanisms for its implementation according to the nation's specific needs and requirements, integrating the overarching principles (described in Section 4) and good practice (described in Section 5).

This lifecycle, as illustrated in Figure 1, guides users of this document in focusing on strategic thinking about cybersecurity at the national level.

3.1 Phase I: Initiation

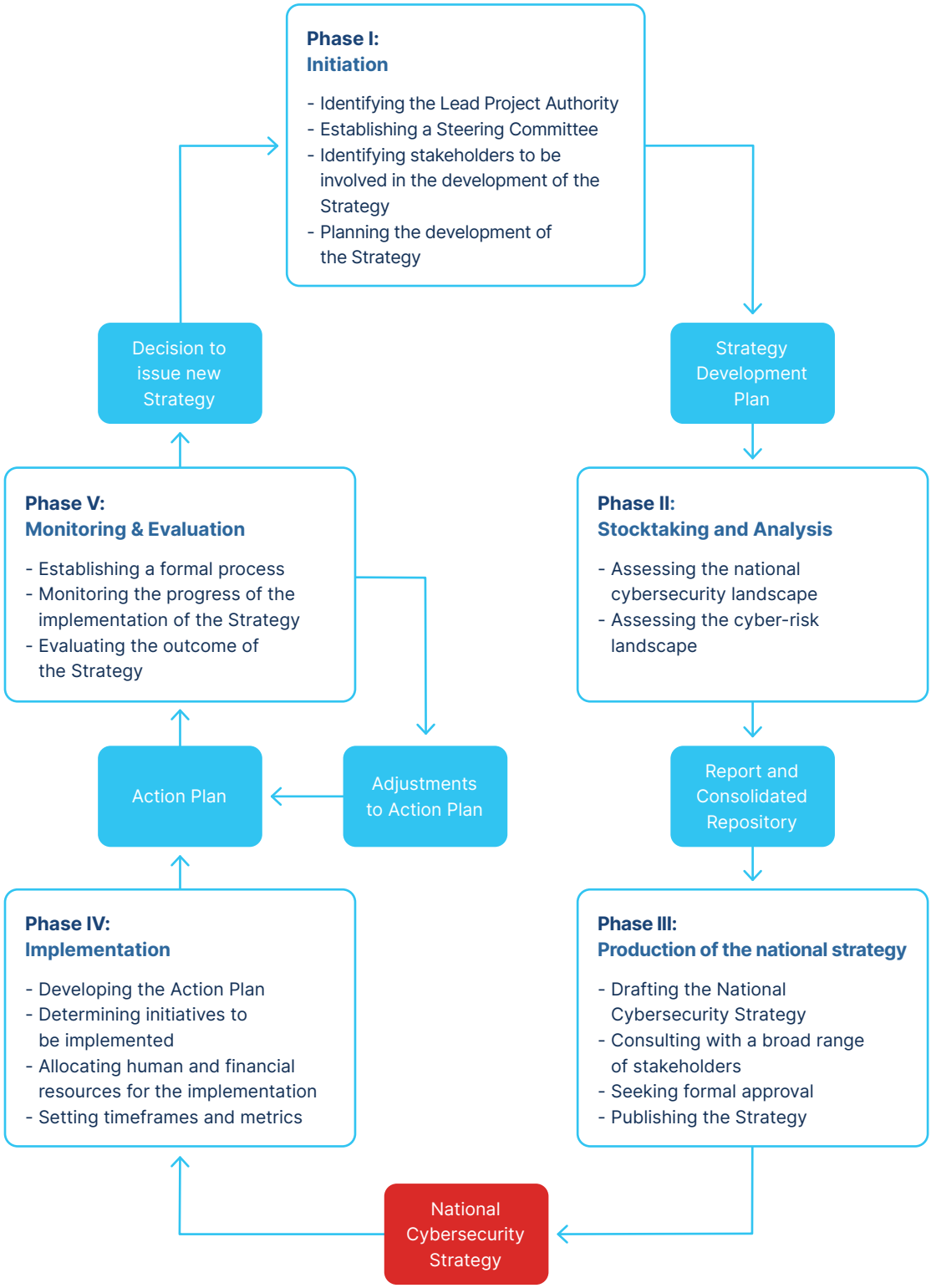
In accordance with Sections 4 and 5 of this document, the initiation phase of a National Cybersecurity Strategy provides the foundations for its efficient development. This phase is expected to focus on processes, timelines, and identification of key stakeholders who should be involved in the production of the Strategy. The outcome of this phase is the elaboration of a plan for the development of the Strategy. When foreseen by the country's governance process, the plan may require the approval of the country's Executive.

3.1.1 Identifying the Lead Project Authority

In line with the principle of defining clear leadership, roles, and resource allocation (Section 4.8), the Strategy development process should be coordinated by a single, competent authority. The Executive should appoint an either pre-existing or newly created public entity, such as a ministry, agency, or a department, to lead the development of the Strategy. This entity, referred to in this document as the Lead Project Authority, should in turn, appoint an individual or team responsible and accountable for leading the Strategy development process.

The Lead Project Authority should be neutral throughout the development process. To this end, it is recommended that this entity be different from the one(s) that will be responsible for the implementation of the Strategy. This or

Figure 1 - Lifecycle of a National Cybersecurity Strategy



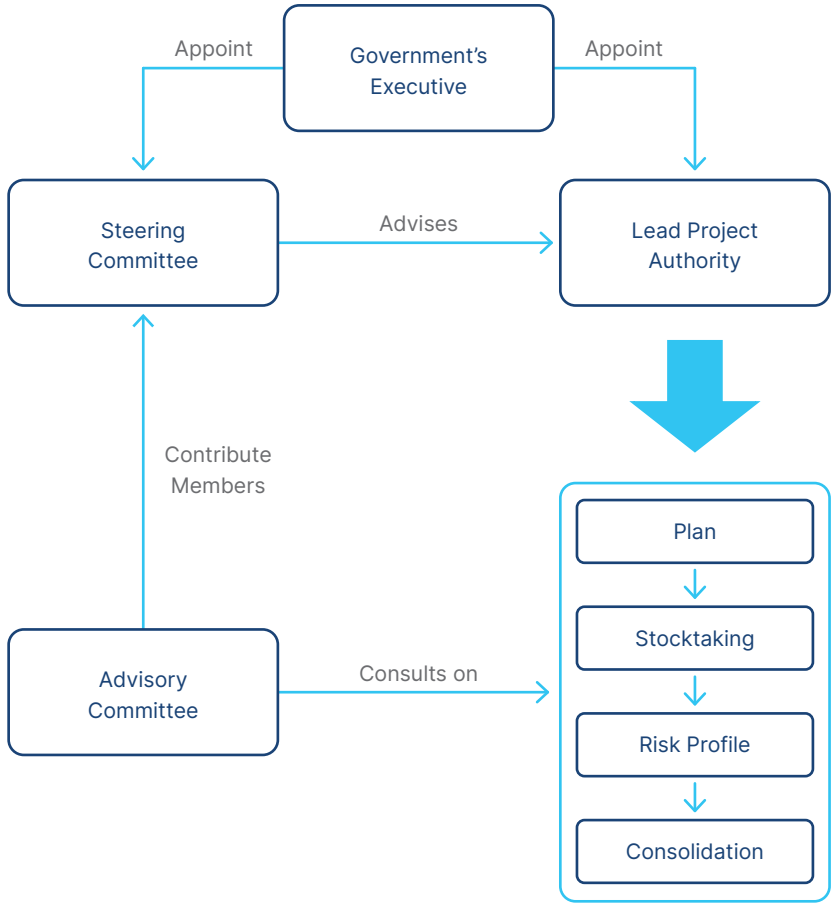
other mechanisms should be adopted to overcome any inherent bias and help avoid intra-governmental competition for resources.

3.1.2 Establishing a Steering Committee

The Executive should also establish a Steering Committee to work with the Lead Project Authority in developing the Strategy. It should be empowered to provide guidance, as well as play a role in quality assurance. In addition, it should guarantee the transparency and inclusiveness of the process, in accordance with the principle on clear leadership, roles, and resource allocation (Section 4.8). The Steering Committee's role, set-up, and membership should be clearly defined from the outset.

As the Steering Committee may need to review sensitive documents, it should be constituted accordingly. It is also important that its membership reflects the various responsibilities given to this body, for instance through seniority of appointments.

Figure 2 - Stakeholders



3.1.3 Identifying stakeholders to be involved in the development of the Strategy

In this step, the Lead Project Authority should identify an initial set of stakeholders to be involved in the development of the Strategy. It should also clarify the roles of the different stakeholders and outline how they will collaborate in order to manage expectations throughout the process.

Throughout the process, the Lead Project Authority may need to reach out to additional stakeholders to leverage all pertinent knowledge and expertise. This would embrace the principle of inclusiveness (Section 4.3), which highlights the importance of cooperation with a range of stakeholders across government, the private sector, and civil society. For example, the Lead Project Authority could consider including ICT companies, critical-infrastructure operators, academic experts, and non-governmental organisations working on raising cybersecurity awareness and preparedness, amongst others.

For such cooperation mechanism, the Lead Project Authority could establish an Advisory Committee, that would contribute in designating members to serve on the Steering Committee, as well as consulting on the various phases of the Strategy development. Whenever possible its composition should be wide enough to include representation from all the sectors of the society that are going to be impacted by the Strategy.

In addition, the Lead Project Authority, with advice from the Steering Committee, could consider involving international stakeholders to get extra support or expertise. There are a wide variety of international organisations, non-governmental organisations, and private entities that specialise in supporting national governments in their NCS activities.

3.1.4 identifying human and financial resources

In this step, the Lead Project Authority should identify the human and financial resources needed to develop and implement the strategy, and where these could be procured. For example, required expertise could be solicited from intergovernmental organisations, the private sector, civil society, academia, or development agencies. Similarly, funding requirements might be addressed through reallocation of dedicated funding streams in existing budgets, or through new funding available from third parties (e.g., international organisations).

Particular attention should be placed on securing long-term funding for the full lifecycle of the National Cybersecurity Strategy, including its development, implementation, and refinement. For further details on the allocation of resources for the implementation, please see “Allocating human and financial resources for the implementation” (Section 3.4.3), and for further details on long-term funding, please see “Allocate dedicated budget and resources” (Section 5.1.5).

3.1.5 Planning the development of the Strategy

In the final step of the Initiation phase, the Lead Project Authority should prepare a plan for developing the National Cybersecurity Strategy. Once the plan has been drafted, it should be submitted, as applicable, to the Steering

Committee and the Executive, for approval, in accordance with the national governance processes.

In drafting the plan, the Lead Project Authority should also consider whether the National Cybersecurity Strategy will take the form of legislation or policy, as different options might influence the formal processes that would need to be followed, as well as the timeframe for adoption.

The Strategy development plan should identify the major steps and activities, key stakeholders, timelines, and resource requirements including human and financial. It should specify how and when relevant stakeholders will be expected to participate in the development process to contribute input and feedback.

Figure 2 shows possible interactions and distribution of roles between different stakeholders and committees.

Further references available on page 56.

3.2 Phase II: Stocktaking and analysis

The purpose of this phase is to collect data to assess the national cybersecurity landscape and the current and future cyber-related risks to inform the drafting and development of the National Cybersecurity Strategy. The output of this exercise, conducted by or with the consult of the Advisory Committee, should be a report that provides an overview of the strategic national cybersecurity posture and risk landscapes to be submitted to the Steering Committee.

Before beginning the actual production (or updating) of the text of the Strategy, the Lead Project Authority should carefully analyse and assess the information gathered during the stocktaking phase to ensure that any gaps in cybersecurity capacity are identified and options for addressing them presented. The analysis should result in an assessment of how far the existing policy, regulatory, and operational environments meet the identified needs of the country and highlight where they fall short.

Similarly, it should be used to identify specific key issues, such as educational and training gaps.

Lastly, the analysis should result in an assessment of all relevant and desirable outcomes for the Strategy, as well as the necessary and available means that can be employed to reach the desired goals.

3.2.1 Assessing the national cybersecurity landscape

For the National Cybersecurity Strategy to be effective, it needs to reflect the cybersecurity posture of the country. To this end, an analysis of the country's existing cybersecurity strengths and weaknesses should be conducted, and relevant materials and documents should be consulted in collaboration with relevant stakeholders across government, private sector, and civil society. This step should embrace the principle of comprehensive approach and tailored

priorities (described in Section 4.2). The Lead Project Authority, with support from the Advisory Committee, should also take stock of different stakeholders' roles and responsibilities in the cybersecurity of the country in order to share effective practices and reduce overlaps.

As part of this effort, the Lead Project Authority should identify assets and services critical to the proper functioning of the society and economy, and map existing national laws, regulations, policies, programmes, and capacity as they relate to cybersecurity. The Lead Project Authority should also identify existing soft regulatory mechanisms, such as private-public partnerships, and take stock of capabilities that have been developed to address cybersecurity challenges, such as national Computer Emergency Response Teams, Computer Incident Response Teams or Computer Security Incident Response Teams (CERTs/CIRTs/CSIRTs). Moreover, the roles and responsibilities of existing public agencies with a cybersecurity mandate, such as regulators or data-protection agencies, should be identified and mapped.

Additionally, related data that can inform the country's cybersecurity posture should be collected. This could include: information on existing national cybersecurity programmes; international initiatives; multilateral and bilateral agreements; private sector projects; ICT and cyber-education and skill-development programmes; cyber-R&D initiatives; data on Internet penetration and infection rates, ICT uptake, and technology developments; and insights on future ICT and cybersecurity trends and threats.

Relevant information provided by the private sector, research institutions, and other stakeholder groups should be included in this analysis as well. For developing countries, it is also crucial to map out the collaborative initiatives with development partners to coordinate technical assistance and investments.

Finally, the Lead Project Authority should also investigate similar information at the regional and international levels, and examine sector-specific strategies and initiatives.

3.2.2 Assessing the cyber-risk landscape

Building on the information collected in the previous step, the Lead Project Authority should assess the risks the nation faces due to digital dependence. This can be achieved through the identification of national digital assets, both public and private, their interdependencies, vulnerabilities and threats, and an estimation of the likelihood and potential impact of a cyber-incident.

This effort embraces the principle of risk management and resilience (Section 4.6), which recognises that risk management is critical to fully realising the benefits of the digital environment for socio-economic development. Furthermore, this initial risk assessment can form the basis for future, more specific risk assessments (further information on the Principle of Risk Management and Resilience and how to conduct risk assessments can be found in Section 5.2).

Further references available on page 56.

3.3 Phase III: 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, 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), prioritising objectives in terms of impact on society, citizens and the economy, and ensuring the necessary financial resources. As part of this phase, all the cross-cutting principles (Section 4) and good-practice elements (Section 5) detailed in this Guide should be considered.

3.3.1 Drafting the National Cybersecurity Strategy

Once the stocktaking and analysis phase is complete, the Lead Project Authority, in collaboration with the Steering Committee, should initiate the drafting of the Strategy. Dedicated working groups could be created either to focus on specific topics, or to draft different sections of the Strategy. The working groups should follow the processes established in the Initiation Phase, adjusting these 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 time frame; and prioritise these in terms of impact on society, the economy, and infrastructure. Moreover, it should identify possible courses of actions; incentivise implementation efforts; and drive the allocation of required resources to support all these activities. The Strategy may also include some of the findings developed in the Stocktaking and Analysis Phase.

Similar to the step dealing with planning the development of the Strategy, the actual document needs to put forward a clear governance framework (Section 5.1) that defines the roles and responsibilities of key stakeholders. This includes the identification of the entity responsible and accountable for the management and evaluation of the Strategy, as well as an entity responsible for its overall management and implementation, such as a central authority or a national cybersecurity council.

The Strategy also needs to define or confirm the mandate of the different entities involved in the national cybersecurity architecture of the country, including those responsible for: initiating and developing cybersecurity policies and regulations; collecting threat and vulnerability information; responding to cyber-incidents (e.g., national CERTs/CIRTs/CSIRTs); and strengthening preparedness and performing crisis management. It should also ensure that it is clear how all of these entities interact with each other and with the central authority.

3.3.2 Consulting with a broad range of national, regional and international stakeholders

As mentioned above, engaging stakeholders is crucial for the success of a Strategy. In order to ensure that the final Strategy is based on a shared vision, the draft document should be disseminated across a wide stakeholder group not limited to those who participated in the Strategy development

process. This can happen through a variety of engagements, including online consultation, validation workshops, and additional working groups. International organisations and other external stakeholders can play a role in the consultation step by providing advice and expertise. It is expected that feedback and comments resulting from this process will be used to finalise the Strategy.

3.3.3 Seeking formal approval

In the final step of the Strategy development, the Lead Project Authority should ensure that the Strategy is formally adopted by the Executive. This official adoption process will vary by country and be based on how the Strategy is defined in the legislative framework. For example, it could be adopted through a parliamentary procedure or a government decree.

Furthermore, it is pivotal that the Strategy is not only developed with approval from the highest levels of government, but that this commitment continues in its implementation phase. The relevant officials should be held accountable and be supported by both political capital and resources.

3.3.4 Publishing and promoting the Strategy

The Strategy should be a public document and should be made readily available. The launch of the Strategy should ideally be accompanied by internal and external promotion activities. The broad availability of the strategy will both ensure that the general public is aware of the government's cybersecurity priorities and objectives, and also support any effort to raise cybersecurity awareness. Should the Strategy be accompanied by an Action Plan, the latter should also indicate additional opportunities for further engagement and cooperation with civil society, the private sector, and international partners.

Further references available on page 57.

3.4 Phase IV: Implementation

The Implementation phase is the most important element of the overall National Cybersecurity Strategy lifecycle. A structured approach to implementation, supported by adequate human and financial resources, is critical to the success of the Strategy and needs to be considered as part of its development. The implementation phase is frequently centred on an Action Plan, which guides the various activities envisioned.

3.4.1 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 different stakeholders across the government, as well as support from civil society and the private sector. The Action Plan, developed in accordance with the principle of clear leadership, roles, and resource allocation (Section 4.8), can support the effective implementation of the Strategy.

The development of the Action Plan is almost as important as the Plan itself. The process, orchestrated by the Lead Project Authority, should serve as a mechanism to bring the relevant stakeholders together to agree on objectives and outcomes, as well as coordinate efforts and pool resources.

3.4.2 Determining initiatives to be implemented

The National Cybersecurity Strategy highlights the government's objectives and the outcomes they wish to realise across the different focus areas identified. In the Action Plan, the Lead Project Authority should – in coordination with relevant stakeholders – identify the specific initiatives within each focus area that will help meet those objectives. Examples of such initiatives could include organising cybersecurity exercises, establishing security baselines for critical infrastructures, and setting an incident reporting framework, amongst others.

The timeline and effort needed for the implementation of these initiatives should be prioritised in accordance with their criticality to ensure that limited resources are appropriately leveraged. To this end, results and outcomes of Phase II (Stocktaking and analysis) specifically with regards to "Assessing the cyber-risk landscape" (Section 3.2.2) might be considered.

3.4.3 Allocating human and financial resources for the implementation

Once the priority initiatives have been identified, the Lead Project Authority should identify specific government entities as owners for each of those initiatives. In turn, these government entities would be responsible and accountable for the implementation of each specific initiative assigned to them and be expected to coordinate their efforts with other relevant stakeholders as part of the implementation process.

To ensure these entities can deliver the expected outcomes, the Lead Project Authority should assess whether they have been given an appropriate mandate – legal or otherwise – required for the implementation. The Lead Project Authority should also work with the owners of the specific initiatives to understand what resources are required to accomplish the work. This assessment should incorporate human resources, expertise, and funding needs. The Lead Project Authority should then work with the owners to help them identify and secure the required resources in accordance with administrative financial structures of the country.

3.4.4 Setting timeframes and metrics

The final critical element of the Action Plan is the development of specific metrics and key performance indicators (KPIs) to assess each of the initiatives undertaken, such as whether the country conducted an awareness campaign on the importance of information sharing, organised and executed a cybersecurity exercise with critical infrastructure sector, or passed a security baseline law. Specific timelines for implementation should also be set.

The metrics and KPIs should be developed by the Lead Project Authority in partnership with the respective operators. The latter should be encouraged to

define and maintain a more detailed set of metrics to facilitate evaluations of the efficiency and effectiveness of the initiatives during and following their completion.

Further references available on page 57.

3.5 Phase V: 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. In the monitoring phase, the government should ensure that the Strategy is implemented in accordance with its Action Plan. In the evaluation phase, the government and the national competent authority should assess whether the Strategy is still relevant and current in light of the changing risk environment and whether it still reflects the government's objectives and what adjustments are necessary.

3.5.1 Establishing a formal process

To ensure effective monitoring and evaluation of the implementation of the Strategy, the government will have to identify an independent entity responsible for monitoring and evaluating the implementation progress and efficiency. The entity should ideally be involved in defining appropriate monitoring and evaluation metrics for the implementation of the Strategy and associated Action Plan and initiatives, which should take place during the Production and Initiation phases.

Monitoring and measuring the performance and successful execution of the implementation plan for the Strategy should be part of the governance mechanisms that a country puts in place. Continuous assessment of the implementation plan (i.e., what is going well and what is not) helps inform the Strategy. Good governance mechanisms with regards to the Strategy implementation should also clearly delineate the accountability and responsibility for ensuring successful execution. Establishing metrics or KPIs by near-term, mid-term, and long-term objectives helps reinforce the governance and management mechanisms. Key performance indicators or metrics should be SMARRT:

- **Specific** – target a specific area for improvement and focus on the change that is expected.
- **Measurable** – quantify or at least suggest an indicator of progress.
- **Achievable** – state what results can realistically be achieved, given available resources.
- **Relevant** – focus on significant indicators of progress
- **Responsible** – specify who will do it
- **Time-related** – specify when the result(s) can be achieved.

The establishment of baseline metrics will enable better monitoring of actions and highlight areas of potential improvement. Furthermore, the allocation of budgets should match the levels of ambition and complexity of the desired impact.

3.5.2 Monitoring the progress of the implementation of the Strategy

The entity responsible for monitoring the progress of implementation of the Strategy should do so in accordance with an agreed upon timeline over the course of the entire lifecycle of the Strategy. The outcome of such monitoring activity (e.g., a report), should note any deviations from the agreed upon timelines and the reasons for any delays, such as priorities shifting, insufficient staffing or resources, etc. This should be done in addition to periodic updates by the owners of the different strands of the implementation of the Strategy to the Lead Project Authority. All relevant stakeholders should be actively involved in monitoring the implementation of the Strategy.

This approach will ensure that the relevant stakeholders are held accountable to the commitments set; it will also ensure that any challenges to implementation are identified early on. In turn, this would allow the government to either rectify the situation or adapt its plans accordingly based on the lessons learnt in the implementation process.

3.5.3 Evaluating the outcomes of the Strategy

In addition to assessing the progress across the agreed upon metrics, it is important to also periodically evaluate the outcomes and compare them with the objectives originally set. This is critical for understanding whether the objectives of the Strategy are being realised or whether different actions should be considered.

As part of this process, the broader risk environment also needs to be regularly re-evaluated to understand whether any 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, and include ways to update the Action Plan and ensure that it is current and responsive to the changing policy and the risk landscape.

Ultimately, the reports produced over the lifecycle of the Strategy should also form the basis for the overall review of the National Cybersecurity Strategy, in accordance with the timeline set during the initiation phase. This overarching review should not only consider the progress made and the changes in the external environment, but also re-assess the government's own priorities and objectives.

Further references available on page 57.

Section 4

Overarching Principles

This Section presents nine cross-cutting principles, which 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 a National Strategy development process, from the drafting of the National Strategy document to its implementation.

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

4.1 Vision

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

A Strategy is more likely to be successful 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), as well as what it is about and who it impacts (scope).

The clearer the vision, the easier it will be for leaders and key stakeholders to ensure a more comprehensive, consistent, and coherent approach. A clear vision also facilitates coordination, co-operation, and implementation of the Strategy amongst the 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.

Further references available on page 58.

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 a complex multi-faceted issue, with aspects extending beyond economic and social prosperity into areas such as law enforcement, national and international security, international relations, trade negotiations, and sustainable development.

It is important to understand all the aspects of cybersecurity and how they interrelate, potentially complementing or competing with each other. Based on this understanding and an analysis of the country's specific context, priorities can then be defined in line with the objectives and implementation timeline of the Strategy. Priorities will allow for setting up specific objectives and timelines and to allocate the necessary resources.

The priorities included in a National Cybersecurity Strategy will vary by country. Some of the cybersecurity topics can be addressed in the same or in separate strategic documents (e.g., digital aspects of national security and defence can be addressed within a national security or defence strategy). Further references available on page 58.

4.3 Inclusiveness

The Strategy should be developed with the active participation of all the relevant stakeholders, and it should address their needs and responsibilities.

The digital environment has become critical to governments, organisations, and individuals. These groups face cybersecurity risks and share a level of responsibility in managing them, depending on their role. For this reason, it is advisable for governments to establish partnerships and collaboration mechanisms to include the private sector and civil society in cyber strategy negotiations and implementation.

While it may be a difficult task, identifying and meaningfully engaging all the relevant stakeholders is essential to the development and successful implementation of a National Cybersecurity Strategy. This will help understand stakeholder needs and their unique knowledge and expertise, thus facilitating cooperation towards achieving the objectives of the Strategy.

To foster inclusiveness and transparency, the Strategy should be a public document. Further references available on page 59.

4.4 Economic and Social Prosperity

The Strategy should foster economic and social prosperity and maximise the contribution of ICT to sustainable development and social inclusiveness.

The digital environment has the potential to expedite economic growth and social progress, to advance key societal values, to improve public-service delivery and capacity, to facilitate international trade, and to promote good governance.

The increasing reliance on the digital environment for the functioning of societies demands increased attention on cybersecurity. However, cybersecurity is not a goal in itself; the Strategy should be aligned with the country's broader socio-economic objectives and lead to building the trust and confidence necessary to both help realise these objectives as well as protect the country from cyber-threats.

Further references available on page 59.

4.5 Fundamental human rights

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

The Strategy should recognise the fact that rights that people have offline must also be protected online. It should respect universally agreed fundamental human rights, including, but not limited to, the ones found in the United Nations' Universal Declaration of Human Rights and International

Covenant on Civil and Political Rights, as well as relevant multilateral or regional legal frameworks.

Attention should be paid to freedom of expression, privacy of communications, and personal data protection. In particular, the Strategy should avoid facilitating the practice of arbitrary, unjustified or otherwise unlawful surveillance, interception of communications, or processing of personal data.

In ensuring that the State 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 of communications, and collection of data are conducted within the context of a specific investigation or legal case, authorised by the relevant national authority and on the basis of a public, precise, comprehensive, and non-discriminatory legal framework enabling effective oversight, procedural safeguards, and remedies.

Further references available on page 59.

4.6 Risk management and resilience

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

While the digital environment provides stakeholders with economic and social opportunities, it also exposes them to cybersecurity risk. For example, when organisations use ICT to foster innovation, gain productivity, and improve competitiveness, or when governments deploy their services online, cybersecurity incidents can occur, potentially resulting in financial loss, reputational damage, disruption of operations, physical impacts, undermining of innovation, etc. As with other types of risk, cybersecurity risk cannot be entirely eliminated but they can be managed and minimised.

To address that challenge, the Strategy should encourage entities to prioritise their cybersecurity investments and to proactively manage risk. Depending on an entity's risk appetite, a balance has to be maintained between security measures and potential benefits, considering the dynamic nature of the digital environment. The Strategy should also recognise the need for continuous risk management and facilitate a coherent approach across interdependent entities.

The focus on risk management will also prepare stakeholders for potential security incidents and compromises, ensuring the resilience of economic and societal activity in the country. With that in mind, the Strategy should encourage the adoption of business-continuity and disaster recovery measures, which include incident and crisis management, as well as recovery plans.

Further references available on page 60.

4.7 Appropriate set of policy instruments

The Strategy should utilise the most appropriate policy instruments available to realise each of its objectives, considering the country's specific circumstances.

The government's cybersecurity goals will only be achieved if a change in behaviour occurs across all stakeholders involved. In most cases, governments have different levers and policy instruments at their disposal to achieve that outcome. These include legislation, regulation, standardisation, certifications, incentives, information-sharing programmes and mechanisms, education programmes, sharing best-practice, setting expected norms of behaviour, and building communities of trust among others. Each of these has its own strengths and weaknesses, comes at differing cost, and brings different results.

The best results can be achieved by selecting the most appropriate policy instrument for each individual objective and balancing the use of different tools.

Further references available on page 62.

4.8 Appropriate set of policy instruments

The Strategy should be set at the highest level of the government, which will then be responsible for assigning relevant roles and responsibilities and allocating sufficient human and financial resources.

Cybersecurity should be promoted and sustained at the highest levels of government. Moreover, to ensure accountability and progress, focal points of individual work streams need to be identified, and all parties involved should have a clear understanding of their respective roles and responsibilities. The Strategy should also allocate the human, financial, and material resources necessary for its implementation. This principle needs to guide both the Strategy development process and the elaboration of the action plan for the Strategy.

Further references available on page 62.

4.9 Trust environment

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

Building trust in the national digital ecosystem, in which users' rights and interests are protected and security of data and systems is assured, is essential to realise the full potential of the social, political, and economic opportunities offered by the use of ICTs. The Strategy must enable policies, processes, and actions at the national level in order to render secure critical services (including e-governance, e-commerce, digital financial transactions, tele-medicine, among others) supported by ICTs and utilised by citizens. Such course of actions would inculcate the principle of trust not only among the general population but also within those public and private organisations that will offer their ICT-related services to citizens.

Further references available on page 63.

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 – effectively overarching themes for a National Cybersecurity Strategy. 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). The order of the individual elements or focus areas below should not be seen as indicating a level of importance or priority.

5.1 Focus Area 1 - Governance

This focus area introduces good-practice elements to consider for inclusion in the text of the Strategy when addressing the governance structure for national cybersecurity (including all entities with responsibilities and authorities for advancing the digital economy and reducing risk from cyber insecurity). The Strategy should clearly state the objectives and outcomes the government has for the country to increase its resilience and reduce risks to its companies, critical infrastructures, services, and assets. The Strategy should clearly identify the roles and responsibilities of the stakeholders tasked with its implementation and introduce measures to hold authorities and officials accountable for the implementation, monitoring, evaluation, and outcome of the Strategy (see *Lifecycle of a National Cybersecurity Strategy*).

To that end, the Strategy should identify and empower the competent authority accountable for the execution of the Strategy; establish a mechanism to identify and task the government entities affected by, or responsible for, the implementation of the Strategy; commit to include specific, measurable, attainable, result-based, and time-based objectives in the implementation plan for the Strategy; and recognise the need to commit resources (e.g., political will, funding, time, and people) to achieve the desired outcomes.

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. Firstly, it improves the likelihood that sufficient resources will be allocated and that coordination efforts will be successful. Secondly, 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 must be a national priority.

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

5.1.2 Establish a competent cybersecurity authority

The Strategy should identify a dedicated national competent authority who has the responsibility for executing the Strategy. This authority should be a leader (whether an individual or an entity) who is elevated and strongly anchored at the highest level of government to provide direction, to coordinate action, and to monitor the implementation of the Strategy. The competent authority should also be responsible for reporting on the progress and outcome of the Strategy.

Such a national competent authority should also act as management entity to define and clarify roles, responsibilities, processes, decision rights, and the tasks required to ensure effective implementation of the Strategy. This includes identifying the stakeholders who will oversee the implementation of the Strategy and establishing performance targets for various ministerial or governmental departments, institutions, or individuals responsible for specific aspects of the Strategy and subsequent action plan. In some cases, the position of national competent authority for cybersecurity may have to be formalized in policy or law to empower it to perform its missions.

Given the fact that cybersecurity intersects many different issue areas, it is important to ensure that the national-competent authority has the ability to involve and direct relevant stakeholders. This too may require additional legislation that mandates government entities to report back to the national competent authority about their progress on achieving the Strategy's outcomes in measurable terms. Using key performance indicators (KPIs) is an effective way to assess progress.

5.1.3 Ensure intra-governmental cooperation

The Strategy should establish a mechanism to identify and include the government entities affected by or responsible for its implementation. Intra-governmental commitment, coordination, and cooperation are core functions of those governmental institutions, needed to ensure that the governance mechanisms (e.g., standards, regulations, market incentives, etc.) 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 and coordination ensure that all ministries and government agencies are aware of each other's respective authorities, missions, and tasks. Commitment, however, is about supporting consistent policies over time to ensure that promises in the Strategy are delivered. An example of a coordination mechanism would be conducting periodic meetings that involve all relevant stakeholders in the plans of actions that are to be jointly reviewed. An example of a cooperation mechanism would be the creation of an intra-government task force to address a particular issue. An example of commitment is consistency between the country's domestic and foreign policy agendas, so that one ministry does not undermine the credibility

of another by representing different positions on the same policy issue area (e.g., trade flow vs. export control of dual-use technologies).

5.1.4 Ensure inter-sectoral cooperation

The Strategy should reflect an understanding of the dependencies that the government has on the private sector and other national non-governmental stakeholders (and vice-versa) in achieving a more secure, safe, and resilient ecosystem (Principle of Inclusiveness). To this end, the Strategy should articulate how the government will engage these different stakeholders and define their roles and responsibilities. For example, the Strategy should identify a network of authoritative national contact points for critical industries that are essential for the operation and recovery of critical services and infrastructures.

The Strategy should be aligned with other national priorities, such as ensuring connectivity is affordable, available, and inclusive; advancing data protection and privacy while promoting innovation; strengthening infrastructures resilience and service availability to disasters, climate change, and pandemics; exploring new technologies like AI, blockchain, quantum computing; etc. (Principle 2 on "*Comprehensive Approach and Tailored Priorities*").

5.1.5 Allocate dedicated budget and resources

The Strategy should specify the allocation of dedicated and appropriate resources for its implementation, maintenance, and revision. Sufficient, consistent and continuous funding provides the foundations for an effective national cybersecurity posture.

Resources should be defined in terms of money (i.e., dedicated budget), people, and, materiel. Successful execution also requires political commitment and leadership, underpinned by trusted partnerships. The objectives and tasks within the Strategy should not be viewed as a one-time allocation of resources. Resourcing requirements should be revisited regularly based upon progress or shortfalls in the implementation of tasks or objectives of the Strategy.

The government may also consider the establishment of a central budget for cybersecurity, managed by a central cybersecurity governance mechanism. Whether assembling disparate funding sources into a coherent, integrated programme or creating a unified intra-governmental budget, the overall programme should be managed and tracked by milestones to ensure successful implementation of the Strategy.

5.1.6 Develop an implementation plan

The Strategy should be accompanied by, or reference, an implementation plan that outlines in greater detail how its strategic objectives will be achieved. Effective implementation plans identify the accountable entity responsible for each task and objective, the resources required to execute them over time (near-term, mid-term, long-term), the processes that will be used, and the outcomes that are expected (Section 3.4 on Initiating Implementation).

Further references available on page 63.

5.2 Focus area 2 - 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 4.2), a risk-management approach should be adopted, as cyber-risks cannot be fully eliminated. Rather, ensuring that a country has a good understanding of the risks that it is exposed to allows it to manage these most effectively. In terms of assessing risk, the approach should focus on identifying inter-dependencies and also consider risks arising from dependencies across the national border. The risk-management approach should consider the whole lifecycle, from development or procurement to operation and replacement.

It is also important to note that, as cybersecurity threats are extremely dynamic and unpredictable, any risk-management approach should be reviewed regularly. As such, the Strategy should plan for monitoring and evaluation of risk- management activities to ensure continuous improvement.

5.2.1 Conduct a cyber threat assessment and align policies with the ever-expanding cyber threat landscape

The Strategy should identify and evaluate the evolving cyber threat environment and potential impact and consequences on critical infrastructures and essential services. The Strategy should first identify the country's domestic critical infrastructures and services – those physical and cyber systems and assets that are vital to the proper functioning of society and economy, and whose incapacitation or destruction would have a debilitating impact of the physical or economic security or public health or safety of the country.

A cyber threat landscape assessment should be conducted to identify the specific cyber threats and risks *page* critical infrastructures and services, as well as the individuals who use and rely upon them, and to help prioritize resources to protect them. Such an assessment would also inform and help align cyber risk management strategies with the country's crisis management plan. It can also help harness the necessary capabilities/capacities, people, funding, and strategies to strengthen the overall cybersecurity posture of the Nation.

5.2.2 Define a risk-management approach

The Strategy should define a coherent approach for risk management to be followed by all government entities and critical infrastructure operators identified domestically.

The approach should aim to build upon the cyber threat assessment and develop a national risk register, securely stored and communicated, to allow government oversight of risks and approaches taken to manage these. The approach should moreover develop a method of prioritisation based on a calculation of the probability of realising the risks and their impact. It should furthermore specify the responsibilities of key entities in each sector regarding the assessment, acceptance, and treatment of national-level cybersecurity risks.

5.2.3 Identify a common methodology for managing cybersecurity risk

The Strategy should identify a common methodology for managing cybersecurity risks. This will ensure efficiency and consistency across all organisations and facilitate the exchange of threat and risk information across inter-dependent systems. A methodology based on international standards should be favoured as it may reduce costs and yield better interaction with the private sector.

The methodology should provide guidance on assigning roles and responsibilities for various aspects of managing risk, such as assessing the threats, valuing assets, implementing and maintaining mitigating measures, and accepting the residual risk. The methodology should include a certification programme to help assess and eventually improve compliance.

Importantly, for the procurement and development of infrastructures or services, the risk-management methodology should provide guidance on minimising risk through secure architecture and design and regular assessments/audits, recognising that security is best achieved when it is an integral part of the design, development, and implementation process of a product, process, or service (security by design).

5.2.4 Develop sectoral cybersecurity risk profiles

The Strategy should call for the use of sectoral risk profiles for cybersecurity. A sectoral risk profile is a quantitative analysis of the types of threats faced. The goal of a risk profile is to provide a less-subjective understanding of risk by assigning numerical values to variables representing different types of threats and the danger they pose. The Strategy should recommend risk profiles to be developed for those sectors that the country considers most critical to its society and economy. (These sectoral risk profiles could be part of the cyber threat landscape assessment discussed in section 5.2.1)

The use of sectoral risk profiles provides a basis for more specific risk assessments for individual organisations, introduces coherence within and across all sectors nationally, and reduces the resources needed for organisational risk assessments. They should be regularly updated to ensure that they remain current.

5.2.5 Establish cybersecurity policies

The Strategy should encourage the establishment of cybersecurity policies for critical national entities, such as government authorities and critical infrastructures operators, among others. Such policies, adopted in accordance with the Principle of an Appropriate Set of Policy Instruments (Section 4.7), would cover governance, operational and technical requirements, and instruct stakeholders on their roles and responsibilities, as well as guide or mandate specific approaches to these issues.

For example, this could include policies that address cybersecurity in procurement or development, define information-sharing programmes, coordinate vulnerability disclosure, set minimum standards of care, specify

security baselines, define certification programmes for compliance, and mandate the reporting of cybersecurity –incidents to the competent authorities.

A coordinated approach at the national level would lead to more efficient and effective cybersecurity management, as it would harmonise practices and facilitate coordination and interoperability.

Further references available on page 64.

5.3 Focus area 3 - Preparedness and resilience

This focus area provides an overview of good practices that support the establishment and sustainability of effective national capabilities to prepare for, prevent, detect, mitigate and respond to major cybersecurity incidents, and to improve a country's overall cyber-resilience.

5.3.1 Establish cyber-incident response capabilities

The Strategy should call for the establishment of an appropriate national incident response capabilities to address operational cybersecurity challenges. Often, this capability refers to the establishment of Computer Emergency Response Teams (CERTs), Computer Security Incident Response Teams (CSIRTs) or Computer Incident Response Teams (CIRTs) with national responsibility.

Although the specific organizational form of a CERT/CSIRT/CIRT may vary (e.g., national, government, sectoral, etc.), and not every country may have the same needs and resources, these specialised and dedicated teams should provide a set of both proactive and reactive functions, as well as preventive and educational services. Thus, these entities can increase a country's ability to respond quickly and recover from cyberattacks, as well as improve its resilience against cyber-threats, reducing the possible overall economic and operational impact of nationally significant cyberattacks.

The areas of services that CERT/CSIRT/CIRT can offer include cyber-incident response and coordination, vulnerability management, situational awareness, knowledge transfer, and threat and intelligence information sharing. The Strategy may also encourage the establishment of PSIRT (Product Security Incident Response Teams) by private sectors to enhance their ability to handle ICT product vulnerabilities.

The Strategy should also identify and develop cooperation mechanisms and communication procedures between national and sectorial incident response teams (should they exist in the country), as well as with international counterparts.

5.3.2 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 part of, or aligned with, the overall national contingency plan. A specific plan for critical information infrastructures should also be considered.

This national cybersecurity contingency plan should consider the findings from the national risk assessments and any cross-sector dependencies that could affect the continuity of operations of critical infrastructures, as well as any disaster recovery mechanisms. Moreover, it should provide an overview of the national incident response mechanisms; as well as highlight how cybersecurity incidents are categorised and escalated, based on their impact on critical assets and services.

5.3.3 Promote information-sharing

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

Formal and informal information-sharing programmes can help foster effective coordination and consistent, accurate and appropriate communications during incident response and recovery activities; facilitate rapid sharing of threat and intelligence information among affected parties and other stakeholders; help improve the understanding of how and which sectors have been targeted; disseminate information on the methods that can be used to defend and mitigate damage on the affected assets; and ultimately reduce vulnerabilities and exposure along with their attendant risks.

The Strategy should identify one or more institutional structures (i.e., competent authorities) responsible for transmitting accurate and actionable information among the national cybersecurity community, including the public and private sectors.

Information-sharing should be a two-way process. If governments are willing to share the information they retain, their actions will demonstrate to private sector entities that the government is indeed a partner in threat information sharing, and help ensure that responders are focused on and better prepared to respond to essential threats.

5.3.4 Conduct cybersecurity exercises

The Strategy should encourage the organisation and coordination of domestic and international cybersecurity and incident response exercises. These can follow different formats (e.g., simulations or real-time exercises) and target the technical and non-technical audiences.

Cybersecurity exercises and other crisis planning mechanisms can help countries develop the institutional capacity to perform incident response effectively, test crisis-management procedures and communication mechanisms, verify the operational ability of CERTs/CSIRTs/CIRTs to respond to cybersecurity incidents and service disruptions under pressure, and help understand any cross-sector dependencies.

Similarly, international cybersecurity exercises can help strengthen cyber-incident response capacity among countries, understand cross-border dependencies, build confidence and trust between countries, and improve the overall international resilience and preparedness levels.

5.3.5 Establish impact or severity assessment of cybersecurity incidents

The Strategy should encourage the establishment of impact or severity assessment mechanisms to assess and evaluate cybersecurity incidents based on their impact on critical assets, services, infrastructure, and people. This type of assessments aims to understand the larger context of a cyber-related incident, including its potential and actual impacts on different sectors and/or population groups and its cascading effects.

Such assessments should be conducted in consultation with a wide range of stakeholders in an open, inclusive, and transparent manner. The assessments should be integrated into the national disaster recovery and contingency plans, and the results should inform cyber incident response overall.

Further references available on page 65.

5.4 Focus area 4 - Critical Infrastructure and essential services

This focus area investigates good practice relating to identifying and protecting Critical Infrastructures (CIs) and Critical Information Infrastructures (CIIs), and strengthening their resilience. The Strategy should recognise and promote the importance of advancing the security and continuity of CI and CII. The potential consequences of an incident impacting CI or CII can disrupt social order, the delivery of essential services, and the economic wellbeing of a country, and the Strategy should emphasize the importance of cyber risk management efforts intended to reduce the likelihood of such disruptive or destructive cyber incidents.

While there are no universally recognised definitions for the terms CI and CII, and governments need to consider which entities and services to include based on their own national risk assessment, for the purpose of this Guide, these terms are defined as follows:

- Critical Infrastructures (CI) are assets that are essential to the functioning and security of a society and economy in any given nation; and
- Critical Information Infrastructures (CII) are IT and ICT systems that operate key functions of the critical infrastructure of a nation.

Whereas the concept of essential services may be applied in reference to services that are essential for the maintenance of critical societal or economic activities.

In either case, a few non-exhaustive examples of these CI, CII or essential services include: energy (electricity, oil and gas), transportation (air, rail, water and road), finance and banking (credit institutions, trading venues and central counterparties), healthcare (healthcare organisations, including hospitals, private clinics, and research institutions), utilities (water and sanitation supply and distribution), digital and telecommunications (fixed and mobile telephone services and provision of internet infrastructure, such as internet exchange points (IXPs) and domain name service (DNS), among others). Definitions and designations may ultimately depend on the geopolitical, economic, and cultural characteristics of the national context.

5.4.1 Establish a risk-management approach to identifying and protecting critical infrastructure and essential services

The Strategy should address the importance of protecting CIs and CIIs from cyber-related risks and devising a comprehensive risk-management approach in accordance with the Principle of Risk Management and Resilience (Section 4.6).

A detailed risk assessment should guide the identification of national CIs and CIIs and essential services, whose disruption may have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy. The Strategy should include or be accompanied by a specific list of CIs and/or CIIs and their correlation, which can be periodically reviewed and updated as necessary.

While there exist a variety of different methodologies to identify CI and CII, nations might consider applying sectorial or functional criteria, such as dependencies and interdependencies with other infrastructure, service, and scope of impact, and the relevance of the infrastructure for maintaining a minimum service supply level. In this designation and review process, the Strategy should envisage the early and ongoing involvement of all the relevant stakeholders including public authorities, semi-public, and/or private infrastructure operators.

Furthermore, a risk-based approach should be adopted to identify and prioritise the implementation of programmes, policies, and practices designed to protect and strengthen the security and resiliency of CIs and CIIs. These programmes and policies should be structured so that CI and CII meet a common baseline of security practices, while also maintaining a level of flexibility to be consistent with their own risk assessments and risk management priorities. In order to leverage existing best practices, enable domestic industry to integrate with global ICT supply chains, and avoid CI/CII interoperability issues across national borders, a risk-management approach based on well-established international standards might also be considered.

5.4.2 Adopt a governance model with clear responsibilities

The Strategy should at a high level describe the governance structure, roles, and responsibilities of the different stakeholders for CI and CII protection. As stipulated in the Principle of Clear Leadership, Roles and Resource Allocation (Section 4.8), an effective and efficient CI-protection programme requires that stakeholders have clearly defined roles and responsibilities and establish a coordination mechanism for managing ongoing issues.

CIs and CIIs are often not owned or controlled by the government, and CI and CII protection efforts generally exceed the capabilities and mandate of any single agency in a government. Thus, appointing an overall coordinator for CI and CII (cyber-)security, such as an interagency committee, can greatly assist in efforts to protect critical infrastructure.

The governance model for CI and CII protection should include the identification of government entities in charge of specific verticals, the responsibilities and accountability of operators of CIs and CIIs, as well as the communication

channels and cooperation mechanisms between public and private agencies to ensure the operation and recovery of critical services and infrastructures.

The governance model should include mechanisms that ensure coordination and alignment across government entities with overlapping missions. The governance should also ensure that sectoral regulators create clear and consistent security requirements that avoid duplication of tasks and streamline important compliance efforts across both public and private sector entities.

5.4.3 Define minimum cybersecurity baselines

The Strategy should either highlight the existing or propose the development of new legislative and regulatory frameworks outlining minimum cybersecurity baselines for CI and CII operators, among others. Security baselines should address a range of high-level risk management priorities as well as more specific cybersecurity practices, such as identifying cyber risks and establishing risk management governance structures; protecting data and systems via access management protocols and other measures; monitoring digital environments and detecting potential anomalies or events; and responding to and recovering from incidents. When developing such baselines, internationally-recognised standards and best practices should be considered to ensure better security outcomes and greater efficiencies. Baselines that are relevant across sectors should be developed as a starting point, enabling greater interoperability and consistency of sector-specific practices and streamlined compliance for cross-sector functions.

The Strategy should also highlight that cybersecurity baselines should be outcome-focused to ensure greater agility over time as the risk landscape and technology continue to rapidly evolve. Articulating what organisations should aim to achieve (e.g., "control logical access to critical resources"), rather than how organisations should implement security (e.g., "utilise two-factor authentication"), can allow government and industry to benefit from continuous security improvements. In addition, an outcome-based approach to the development of these baselines can be complemented by sector-specific implementation or "how to" guidance, which provides options to inform and integrate enterprise practices.

In addition to addressing a range of high-level risk management priorities, cybersecurity baselines should also include procurement requirements to ensure that ICT suppliers have adequate and auditable security measure in place.

The Strategy should support the establishment of a resilient CI and CII national environment, and prepare stakeholders to respond, mitigate, and recover from potential cybersecurity incidents. The risk management approach should encourage the adoption of crisis management processes, business continuity measures, and recovery plans.

5.4.4 Utilise a wide range of market levers

The Strategy should consider a wide range of policies to ensure that all organisations and individuals are indeed incentivised to fulfil their individual cybersecurity responsibilities, commensurate with the risks they face, in

accordance with the principle of comprehensive approach and tailored priorities (Section 4.2).

Identifying gaps between what the markets can and should drive and what the risk environment requires is a crucial step towards determining when and how to leverage the range of incentives and disincentives available to improve security. To encourage the uptake of cybersecurity standards and practices across CIs and CIIs, the Strategy should indicate that the government will consider a range of policy options and market levers at its disposal.

5.4.5 Establish public private partnerships

The Strategy should encourage the creation of formal public-private partnerships to increase the security of CIs and CIIs. Public-private partnerships are a cornerstone of effectively protecting critical infrastructure and managing security risks in both the short- and long-term. They are essential for boosting trust amongst and between industry and the government.

However, establishing sustainable partnerships requires that all of the participating stakeholders have a clear understanding of the goals of the partnership and the mutual security benefits that stem from working together. Some of the areas could include: developing cross-sector and sector-specific cybersecurity baselines, establishing effective coordinating structures and information-sharing processes and protocols, building trust, identifying and exchanging ideas, approaches and best practices for improving security, as well as improving international coordination.

Further references available on page 67.

5.5 Focus area 5 - Capability and capacity building and awareness raising

Technology and policy considerations can dominate cybersecurity discussions, overlooking the fundamental human element at its core. This Focus Area addresses the challenges related to advancing cybersecurity capacity building (both human and institutional) and awareness raising among stakeholders, including government entities, citizens, businesses, and other organisations – crucial to enabling a country's digital economy.

Good practices considered in this section include the coordination of capacity building activities, the establishment of dedicated cybersecurity curricula and awareness raising programmes, expansion of training schemes and workforce-development programmes, adoption of international certification schemes, and promotion of innovation and research and development (R&D) clusters.

5.5.1 Strategically plan capability and capacity building and awareness raising

The Strategy should assign clear roles and responsibilities to entities tasked with the coordination of capacity building and awareness raising activities at the national level to ensure resources are streamlined, efforts are not duplicated, and accountability is established. The appointed national authorities should also be responsible for monitoring the implementation and evaluating the outcomes of these activities, as well as recommending changes if necessary.

Cybersecurity capability and capacity building and awareness raising should be evidence-based and strategically planned. A detailed assessment of the national cybersecurity landscape and current capacity building initiatives should guide the identification of existing gaps in capacity needs, skills, and awareness and inform forward-looking solutions. Given differences within and among countries and regions, there is no one-size-fits-all approach to cybersecurity capability and capacity building, so the information gathered should be used to design approaches tailored to the specific political, economic, and social context. The responsible authorities might also produce an action plan that includes budget allocations, timelines, and metrics to monitor the progress of each of these planned actions.

5.5.2 Develop cybersecurity curricula

The Strategy should facilitate the development or expansion of dedicated school curricula aimed at accelerating cybersecurity skills development and awareness throughout the formal education system. Curricula should be inter/multi-disciplinary and cover 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. Dedicated cybersecurity curricula should be developed across primary and secondary schools, integrating cybersecurity courses in all computer science and IT programmes in higher education, and creating dedicated cybersecurity degrees and apprenticeships.

Given the multi-disciplinary nature of cybersecurity education, universities, colleges, and other educational institutions should be encouraged to work across departments and with other academic partners to optimize resources and efforts when developing or updating their programmes. These institutions can play a critical role in educating civilian and military workforces on the unique tenets of cybersecurity and can serve as incubators for future workforce, bringing together theory with methodology, tools, and implementation, and optimizing campus-wide resources to combine knowledge, intellectual capacity, and practical skills.

Additionally, the curricula should foster awareness of and stimulate interest in cybersecurity career opportunities. To further the efforts in this space, the government should also consider establishing various incentive schemes, such as scholarships for private education programmes and grants for relevant apprenticeships.

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. The effort could include the provision of executive and operational training, formal internships and traineeships, and (national and international) certification of security professionals, based on the needs identified by industry and government. The Strategy should also encourage specific 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.

The Strategy should also foster initiatives that aim to develop dedicated cybersecurity career paths and an effective pipeline of future employees, in particular 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 of experts in cybersecurity, a gender-balanced approach that motivates, encourages, and facilitates more engagement from women should be considered across all efforts aimed at skills-development and training, ensuring inclusivity in the future.

5.5.4 Implement a coordinated cybersecurity awareness-raising programme

The entities responsible for cybersecurity awareness campaigns and activities at the national level should collaborate with relevant stakeholders to develop and implement cybersecurity awareness programmes focusing on disseminating information about cybersecurity risks and threats, as well as about best practices for countering them.

A cybersecurity awareness-raising programme could include awareness-raising campaigns aimed at the general public, children, digitally challenged, consumer- focused education programmes, and awareness-raising initiatives among others, targeted at executives across public and private sectors. Awareness programmes should include relevant KPIs and metrics for measuring impact and effectiveness.

5.5.5 Foster cybersecurity innovation and R&D

The Strategy should foster an environment that stimulates basic and applied research in cybersecurity across sectors and various stakeholder groups. Such initiatives include, for example, ensuring that national research efforts support the objectives of the National Cybersecurity Strategy; developing cybersecurity-focused R&D programmes in public research organisations; effective development and dissemination of new findings, baseline technologies, techniques, processes, and tools. The strategy should also envisage developing an efficient and sufficient local market of cybersecurity services.

Moreover, as part of the Strategy, countries should also 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, but also non-technical fields such as social and political sciences, business and management studies, criminology and psychology to name a few.

The Strategy should look at incentive mechanisms available from grants, procurements, tax credits, competitions, and other initiatives that encourage the development of innovative cybersecurity solutions, products, and services.

5.5.6 Tailor programmes for vulnerable sectors and groups

The Strategy should identify those groups of society which require particular attention when it comes to cybersecurity capacity and capability building and awareness raising. These include groups which have been identified as being particularly at risk or which need to be empowered to protect themselves, such as small and medium enterprises (SMEs), community-based organizations (CBOs), underserved communities, and/or low-income communities.

Further references available on page 68.

5.6 Focus area 6 - Legislation and regulation

This focus area covers the development of a legal and regulatory framework to protect society against cybercrime and promote a safe and secure cyber environment, in accordance with the Principles of Inclusiveness, Fundamental Human Rights, and on Trust Environment (Sections 4.3, 4.5 and 4.9, respectively). Such a framework should include: the adoption of legislation that defines what constitutes illegal cyber-activity, as well as the procedural tools that are needed to investigate and prosecute these crimes at the national level and for cooperating cross-border; establishment of compliance mechanisms; the building of capacity to enforce the framework; institutionalization of critical entities; and international cooperation to fight cybercrime. The framework should recognize and be consistent with the country's obligations under international, regional, and national human rights law.

Cybersecurity, cybercrime, and protection of personal data are interrelated concepts. Countries should establish a legal and regulatory framework which covers these three areas in a holistic and coherent way.

The Strategy should inform and guide the development of legislation so that roles and responsibilities of actors involved in applying the law are clear and well-defined, while ensuring compliance with existing legal principles and provisions. The Strategy should map the existing legal and regulatory framework, including operational aspects, and identify areas where new or revised legislation and regulation is required.

5.6.1 Establish a domestic legal framework for cybersecurity

The Strategy should encourage the development of domestic cybersecurity and data protection legal frameworks, which refer to actions relevant to the prevention, monitoring, and handling of cyber-related incidents, and any other action that public and private entities should undertake to foster a secure and resilient national cyberspace.

In the current absence of an international legal instrument defining the aspects of cybersecurity regulations, the country will have to rely on regional and/or national best practices for establishing its domestic legal frameworks for cybersecurity. The Strategy should build upon current acts and regulations tackling such aspects, if any, and establish, update, and reform the legal framework for cybersecurity, including but not limited to: information security rules and their applicability to the security of information systems; identification of national critical information infrastructure; establishment

of national and sectoral agencies dealing with cybersecurity aspects (i.e., national cybersecurity agencies, national and sectoral CERTs/CSIRT/CIRT); certification of cybersecurity organisations, processes, products, and policies; national/state security rules applicable to security of cyberspace; and other relevant matters.

Further, the Strategy should provide guidance on how to deal with common regulatory approaches that concern both cybersecurity and cybercrime (for example, cross-sectoral exchange of information and intelligence sharing mechanisms, reporting and criminal justice statistics, joint response and public-private cooperation, among others).

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 what constitutes cybercrime and related criminal offences, and that provides adequate procedural powers for effective investigation and prosecution, as well as adjudication of related cases on the basis of admissible electronic evidence.

Most often, this capability takes the form of cybercrime legislation, which can be achieved by enacting specific new laws or amending existing ones (e.g., the penal code, laws regulating banking, telecommunications and other sectors). These laws should specify: substantive criminal offences (offences against or by means of computer systems or data); procedural means to collect electronic evidence (ranging from preservation of integrity of data to search and seizure, and from production order to real-time interception of content data); and tools for expedited and effective international cooperation in such cases. In order to establish clear and enforceable cybercrime legislation across borders, countries should try to harmonize their domestic legal framework with existing international and regional legal instruments on this matter.

The Strategy should provide guidance also to operational aspects of cybercrime investigation and prosecution (e.g., establishment of specialized units, proper digital forensics capacities, standard operating procedures, crime reporting, etc.) that may not be set at the level of primary legislation but could be nevertheless provided as secondary regulations, guidelines, or best practices.

The Strategy should also encourage the creation of a process to monitor the implementation and review of legislation and governance mechanisms, identify gaps and overlapping authorities, and clarify and prioritise areas that require modernisation (e.g., existing laws such as old telecommunication laws).

5.6.3 Recognise and safeguard human rights and liberties

The Strategy should promote the development of domestic legal frameworks on cybersecurity, cybercrime and other related areas that respect and protect human rights. In doing so, the differences of context between cybersecurity (technical aspects of security) and cybercrime (criminal justice response) should be properly highlighted and considered.

The Strategy should pay particular attention to technology-related legal issues that can affect the level of cybersecurity and which have impacts on human rights (e.g. encryption, anonymity vulnerability disclosure, ethical hacking and others). In doing so, the Strategy should promote approaches that are consistent with individuals' human rights.

In terms of cybercrime and criminal justice matters overall, the Strategy should safeguard essential due process rights applicable in criminal investigations and prosecutions, as well as rights of privacy and personal data protection, and freedom of expression, in accordance with the Principle of Fundamental Human Rights and Trust (Sections 4.5 and 4.9).

The strategy should also ensure that the rights of those who are victims of – or at risk from – cyber incidents and cybercrime are sufficiently taken into consideration and protected.

5.6.4 Create compliance mechanisms

The Strategy should promote the establishment of domestic compliance mechanisms (both enforcement and incentives). These mechanisms should be set in place to prevent, combat, and mitigate actions directed against the confidentiality, integrity, and availability of ICT systems and infrastructures, and threatening computer data, in accordance with the aforementioned legal framework. They should inter alia cover the particularities of response to cyber incidents, criminal investigations, specialized procedures (such as lawful interception of communications), and use of electronic evidence.

5.6.5 Promote capacity-building for law enforcement

The Strategy should encourage the development of cyber-law-enforcement capacity, including training and education for a range of stakeholders involved in combating cybercrime (e.g., judges, prosecutors, lawyers, law-enforcement officials, forensic specialists, financial investigators, and others). Law enforcement should receive specialised training to interpret and apply domestic cybercrime laws (i.e., translate the law into technical notions and vice versa); to effectively detect, deter, investigate and prosecute cybercrime offenses while respecting human rights; and to effectively collaborate with industry and international law-enforcement entities (e.g., INTERPOL, Europol) to tackle cybercrime and to boost cybersecurity. Such training and education should be continuous and cover all relevant criminal justice and security professionals, and should be kept continuously up-to-date with current cyber-related challenges and threats. This element should take into consideration focus area 5 on Capability and Capacity Building and Awareness Raising (Section 5.5).

5.6.6 Establish inter-organisational processes

The Strategy should identify and recognise the mandates of domestic agencies with the primary authority to ensure compliance with cybercrime legislation (primarily criminal justice authorities and forensic services), those responsible for prevention of and response to cyber incidents that raise to the national level (including protection of critical information infrastructures), and those

responsible for ensuring that all international cybercrime requirements are being met (e.g., ensure that national laws comply with international treaty obligations) and across judicial lines (e.g., cross-border cooperation) (see also Section 5.1.3 and 5.1.4; and Section 5.6.6).

5.6.7 Support international cooperation to combat cyber threats and cybercrime

The Strategy should demonstrate a commitment to protect society against cybercrime globally, through ratification, where possible and in accordance with the overall national agenda, of international cybercrime agreements or equivalent agreements to fight cybercrime, and through the promotion of coordination mechanisms to address international cybercrime. This may include aligning national laws with international treaty obligations and bilateral agreements, for example by establishing mutual legal assistance, enabling cross-border investigations and prosecutions, handling of digital evidence, and extradition.

Also, the Strategy should recognize the importance of building informal mechanisms that enable trusted cooperation and cross-border exchange of information, intelligence, and technical support between cybersecurity actors in both public and private sector.

In particular, international law enforcement cooperation plays a vital role in combating cybercrime through the exchange of information, cross-border investigations, operations, and arrests. For example, INTERPOL provides a secure global police communications system for countries to facilitate police-to-police requests and formal mutual legal assistance requests from one central authority to another. These channels can assist in the investigation and prosecution of cybercrime beyond a nation's borders. Law enforcement cooperation can also help improve cross-jurisdictional interoperability and ensure timely and coordinated joint police actions. Other organizations like AFRIPOL, AMERIPOL, ASEANAPOL, GCCPOL, ECOPOL, and Europol are likewise fostering law enforcement cooperation at the regional level.

These elements should take into consideration focus area 7 on international cooperation (Section 5.7).

Further references available on page 69.

5.7 Focus area 7 - International cooperation

This focus area emphasises the elements that the Strategy should cover in terms of external cybersecurity engagements of a particular country, both at regional and international levels. With digitalisation impacting all areas of international relations, such as human rights; economic and social development; trade negotiations; commerce relations; arms control; the use of new and disruptive technologies; security of supply chains; and security, stability, peace, and conflict resolution, cybersecurity has become an integral part of a country's foreign policy.

The Strategy should therefore recognise the borderless nature and international dimension of cybersecurity, and highlight the need to engage in

international discussions and cooperate with both national and international stakeholders, as well as civil society, industry, and non-governmental organizations. International engagements with public and private stakeholders are key to facilitating a constructive dialogue, developing trust and cooperation mechanisms, finding mutually acceptable solutions and addressing common challenges, and creating a global understanding of the importance of cybersecurity and resilience.

In accordance with the principle of comprehensive approach and tailored priorities (Section 4.2), regional and international cooperation should be fostered in harmony with the political, social, cultural, and economic layout of the country. The country's cybersecurity priorities should inform and be aligned with its foreign policy's goals and vice versa.

5.7.1 Recognise cybersecurity as a component of foreign policy and align domestic and international efforts

The Strategy should express a commitment to international cooperation on cybersecurity and recognise cyber-issues as an integral component of the country's foreign policy across all relevant areas, including international cyber stability and trade negotiation.

The Strategy should clearly articulate the government's focus areas and indicate long-term objectives for international cooperation, including which stakeholders (e.g., public, private, regional, global) would be engaged. Such focus areas might include, for instance, support for the establishment of international cybersecurity norms and confidence-building measures (CBMs), commitment to cybersecurity capacity-building (CCB), participation in the development of international cybersecurity standards, as well as joining existing regional and international processes.

Moreover, the Strategy should ensure consistency between the country's domestic and foreign-policy agendas by harmonising its national legal framework and policies with its international commitments, and aligning its national cybersecurity approaches with its international efforts. This may also require harmonisation among different governmental entities (e.g., head of state and cabinet, Ministry of Foreign Affairs, Ministry of ICT, Ministry of Industry and Trade, Ministry of Justice, Ministry of Defence, etc.) so that the policy position expressed by one domestic entity at a negotiating table in the international arena is properly coordinated and aligned with other governmental bodies.

5.7.2 Engage in international discussions and commit to implementation

The Strategy should identify specific international fora and cooperation mechanisms that the country wishes to join or cooperate with to effectively engage internationally on cyber-related issues. These could include regional or global organisations, standardisation bodies, intergovernmental or multistakeholder discussions, public and/or private-sector alliances, as well as established traditional cooperation and collaboration mechanisms that have a cyber or digital component.

The Strategy should specify the country's commitment to the application of international law, including the Charter of the United Nations and international human rights law. It could also outline a national commitment to join and implement existing regional and international instruments to combat cybercrime and other cyber threats (e.g., the Council of Europe's Budapest Convention on Cybercrime, the African Union's Convention on Cybersecurity, the Arab Convention on Combating Information Technology Offences, the ECOWAS Directive on fighting cybercrime, etc.). The Strategy should recognize that many international trade agreements also have a digital or cyber component (e.g., the Wassenaar Arrangement governs dual-use technologies, and the United States-Mexico-Canada Agreement (USMCA) and the Regional Comprehensive Economic Partnership (RCEP) among Asia-Pacific nations govern cross-border data flows).

The Strategy should also encourage the country's commitment to the furtherance of voluntary norms of responsible State behaviour in cyberspace and of CBMs in cyberspace. Notable examples of international efforts and fora for the elaboration of such norms and CBMs include the UN Open-ended Working Group on security of and in the use of information and communications technologies (OEWG), the Organisation of Security and Cooperation in Europe (OSCE) on confidence building measures and international norms applicable in cyberspace, the work of the G7 Group's High-Tech Crime Subgroup, as well as other regional initiatives and multistakeholder efforts (e.g., Paris Call, industry initiatives, etc.). It is important to prioritise international engagement efforts, allocate adequate resources (personnel and money), and define adequate mandates to ensure that they deliver concrete results.

The Strategy should also express the commitment to the implementation of the agreed norms of voluntary State behaviour in cyberspace such as the ones proposed by the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security in its 2015 report, and further developed by the GGE on Advancing responsible State behaviour in cyberspace in the context of international security, which concluded its work in May 2021.

5.7.3 Promote formal and informal cooperation in cyberspace

The Strategy should indicate the operational (both public and private sector) international cooperation mechanisms that the country wishes to commit to. The country may wish to engage in formal and informal international endeavors advancing cooperation on policy and legislative development, law enforcement (e.g., INTERPOL, EUROPOL, WIPO), incident response, information- and threat-sharing (e.g., FIRST, ISACs), among others. Participation in such initiatives could support better cooperation and exchange of timely and actionable information between relevant authorities on potential threats and vulnerabilities and coordination in defense and response mechanisms.

Cross-border information exchanges with private sector organizations and industry dealing with cybersecurity threats (anti-virus companies, threat intelligence community, global social media providers and other relevant actors) should be considered an important component of international cooperation efforts as well.

5.7.4 Promote capacity building for international cooperation

As the country begins to undertake international engagements, these will likely require the government to develop additional competencies and skills focused on cyber-issues and increase its overall capacity to address an ever-increasing range of cyber issues, including international cyber stability, data protection and privacy, trade, commerce, arms control, the use of new and disruptive technologies, security of supply, and other digital matters.

In order to effectively engage in international discussions and cooperation, it is important to encourage the development and use of competencies and skills focused on cyber-issues (including cyber-diplomacy and trade negotiations) to complement the traditional methods and processes of diplomacy and trade. The Strategy may also include the development of specific organisational structures and the establishment of some dedicated office or trained personnel whose primary focus is diplomatic engagement on cyber-issues relating to trade, diplomacy, and international law.

Other priority areas for capacity building may include CERT/CSIRT cooperation, law enforcement and judicial cooperation, applicable public international law, voluntary norms of responsible State behaviour, etc. Various international capacity building programmes are available to support such efforts (e.g., GLACY+, Global Forum on Cyber Expertise (GFCE), INTERPOL, etc.). 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 ever-evolving threat landscape to stay ahead of crime.

The Strategy should consider existing regional and international cybersecurity initiatives and foster harmonisation and alignment. This would allow the country to leverage existing good practices, as well as to contribute towards cohesion and convergence of cybersecurity approaches.

The Strategy should encourage peer-learning and the transfer of cybersecurity knowledge and skills with international partners. Furthermore, participation in international events and cybersecurity exercises can provide both means for cybersecurity capacity building and for building trust and fostering international cooperation.

Further references available on page 71.

Section 6

Reference Materials

In the process of developing this Guide, a stocktaking of existing guides and best practices was conducted.

This allowed us to identify materials already available to support countries in developing their National Cybersecurity Strategy. The list below provides a comprehensive catalogue of the abovementioned materials, including web links.

NCS Lifecycle

Initiation

CCDCOE. 'National Cyber Security Strategy Guidelines', section 1.3, 2013. https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf.

ENISA. 'National Cyber Security Strategies: Training Tool', 2016.

Global Cyber Security Capacity Centre. 'Cybersecurity Capacity Maturity Model for Nations (CMM)' dimension 1: 1.1, University of Oxford, 2021. (https://gcscc.ox.ac.uk/cmm-2021-edition)

GPD. 'Involving Stakeholders in National Cybersecurity Strategies: A Guide for Policymakers', 2020. https://www.gp-digital.org/publication/involving-stakeholders-in-national-cybersecurity-strategies-a-guide-for-policymakers/.

Stocktaking and Analysis

CCDCOE. 'Cybersecurity Strategy & Governance Repository'. https://ccdcoe.org/library/strategy-and-governance/.

CCDCOE. 'National Cyber Security Framework Manual', sections: 3.4, 4, (2012). https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/.

CCDCOE. 'National Cyber Security Strategy Guidelines', sections: 2.1, 2.2, 3.2.1, 3.3.1, (2013).

ENISA. 'National Cyber Security Strategies: Training Tool', 2016.

GCSCC. 'Cybersecurity Capacity Maturity Model for Nations (CMM)', Dimension 1: 1.1, University of Oxford, 2021. https://gcscc.ox.ac.uk/cmm-2021-edition.

GFCE. 'Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle', sections: 1-7, 2021. https://cybilportal.org/tools/catalog-of-project-options-for-the-national-cybersecurity-strategy-ncs-cycle/.

ITU. 'Global Cybersecurity Index 2020', 2021. https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/.

OAS. 'Managing National Cyber Risk', 2018. https://www.oas.org/es/sms/cicte/ENGcyberrisk.pdf.

Potomac Institute for Policy Studies. 'Cyber Readiness Index 2.0', 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

UNIDIR. 'Cyber Policy Portal', 2021. www.cyberpolicyportal.org

Production

ENISA. 'National Cyber Security Strategies: Training Tool', 2016.

Global Cyber Security Capacity Centre. 'Cybersecurity Capacity Maturity Model for Nations (CMM)', Dimension 1: 1.1, University of Oxford, 2021. (https://gcscc.ox.ac.uk/cmm-2021-edition)

Potomac Institute for Policy Studies. 'Cyber Readiness Index 2.0', 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

Implementation

ENISA. 'National Cyber Security Strategies: An Implementation Guide', 2012.

ENISA. 'National Cyber Security Strategies: Training Tool', 2016.

GCSCC. 'Cybersecurity Capacity Maturity Model for Nations (CMM)', Dimension 1: 1.1, University of Oxford, 2021. https://gcscc.ox.ac.uk/cmm-2021-edition.

GFCE. 'Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle', 2021. https://cybilportal.org/tools/catalog-of-project-options-for-the-national-cybersecurity-strategy-ncs-cycle/.

Potomac Institute for Policy Studies. 'Cyber Readiness Index 2.0', 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

Monitoring and Evaluation

CCDCOE. 'Cybersecurity Strategy & Governance Repository'. https://ccdcoe.org/library/strategy-and-governance/.

CCDCOE. 'National Cyber Security Framework Manual', section 2.4, 2012. https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/.

ENISA. 'National Capabilities Assessment Framework', 2020.

ENISA. 'National Cyber Security Strategies: Training Tool', 2016.

Global Cyber Security Capacity Centre. 'Cybersecurity Capacity Maturity Model for Nations (CMM)', Dimension 1: 1.1, University of Oxford, 2021. (https://gcscc.ox.ac.uk/cmm-2021-edition)

OAS. 'Managing National Cyber Risk', 2018. https://www.oas.org/es/sms/cicte/ENGcyberrisk.pdf.

Potomac Institute for Policy Studies. 'Cyber Readiness Index 2.0', 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

Overarching Principles

Vision

ENISA. 'National Cyber Security Strategies: Training Tool', 2016.

Global Cyber Security Capacity Centre. 'Cybersecurity Capacity Maturity Model for Nations (CMM)', Dimension 1: 1.1, University of Oxford, 2021. (https://gcscc.ox.ac.uk/cmm-2021-edition)

Microsoft. 'Building an Effective National Cybersecurity Agency', 2018.

Microsoft. 'Developing a National Cybersecurity Strategy, Sections: A Principled Approach to Cybersecurity, Establishing Clear Priorities and Security Baseline', 2013.

Potomac Institute for Policy Studies. 'Cyber Readiness Index 2.0', 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

Comprehensive approach and tailored priorities

CCDCOE. 'Cybersecurity Strategy & Governance Repository'. https://ccdcoe.org/library/strategy-and-governance/.

CCDCOE. 'National Cyber Security Framework Manual', sections: 3.4, 4, (2012). https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/.

CCDCOE. 'National Cyber Security Strategy Guidelines', sections: 2.1, 2.2, 3.2.1, 3.3.1, (2013).

ENISA. 'National Cyber Security Strategies: Training Tool', 2016.

GCSCC. 'Cybersecurity Capacity Maturity Model for Nations (CMM)', Dimension 1: 1.1, University of Oxford, 2021. https://gcscc.ox.ac.uk/cmm-2021-edition.

GFCE. 'Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle', sections: 1-7, 2021. https://cybilportal.org/tools/catalog-of-project-options-for-the-national-cybersecurity-strategy-ncs-cycle/.

OAS. 'Managing National Cyber Risk', 2018. https://www.oas.org/es/sms/cicte/ENGcyberrisk.pdf.

Potomac Institute for Policy Studies. 'Cyber Readiness Index 2.0', 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

UNIDIR. 'Cyber Policy Portal', 2021. www.cyberpolicyportal.org.

Inclusiveness

Economic and Social Prosperity

GPD. 'Involving Stakeholders in National Cybersecurity Strategies: A Guide for Policymakers', 2020. https://www.gp-digital.org/publication/involving-stakeholders-in-national-cybersecurity-strategies-a-guide-for-policymakers/.

GPD. 'Toolkit for Inclusive and Value-Based Cybersecurity Policymaking'. https://www.gp-digital.org/publication/toolkit-for-inclusive-and-value-based-cybersecurity-policymaking/.

OECD. 'Recommendation of the Council on Digital Security of Critical Activities', 2019. https://ccdcoe.org/uploads/2020/01/OECD-191211-The-Recommendation-of-the-Council-on-Digital-Security-of-Critical-Activities.pdf.

OECD. 'Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2-A, Companion Document', 2015.

OECD. 'Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2-A, Companion Document', 2015.

Potomac Institute for Policy Studies. 'Cyber Readiness Index 2.0', 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

Fundamental human rights

Council of Europe. 'Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence - Draft as Approved by the Cybercrime Convention Committee', 2021.

Council of Europe. 'Strategic Priorities for Cooperation on Cybercrime and Electronic Evidence in GLACY Countries', sections 1, 2, 6, (2016).

Council of Europe. 'Strategic Priorities for the Cooperation against Cybercrime in the Eastern Partnership Region', sections 1,2,7, (2013).

CTO. 'Commonwealth Approach for Developing National Cyber Security Strategies', sections 4.4.5, 4.4.6, 4.4.7, 4.4.8, 4.4.9, 4.4.18, 4.4.19, 4.4.20, (2015).

ENISA. 'National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies', sections 3.15, 3.184.9, 4.12, (2016).

Europe, Council. 'Budapest Convention on Cybercrime and Its Additional Protocol on Xenophobia and Racism (2001)', 2004.

ITU. 'Guidelines for Policy-Makers on Child Online Protection', sections 3.3, 3.4, (2020). https://www.itu-cop-guidelines.com/policymakers.

Potomac Institute for Policy Studies. 'Cyber Readiness Index 2.0', section 3, 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

UN. 'Sustainable Development Goals, Article 16.3 UNCTAD, Global Cyberlaw Tracker', 2015.

UNHR. 'International Covenant on Civil and Political Rights, Article 19', 1976.

WEF. 'Cybercrime Prevention Principles for Internet Service Providers', 2020. https://www.weforum.org/reports/cybercrime-prevention-principles-for-internet-service-providers.

WEF. 'Partnership against Cybercrime', 2020. https://www.weforum.org/reports/partnership-against-cybercrime.

WEF. 'Recommendations for Public-Private Partnership against Cybercrime', 2016. http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf.

World Bank. 'Combatting Cybercrime: Tools and Capacity Building for Emerging Economies'.

Risk management and resilience

Carnegie Mellon. 'Handbook for Computer Security Incident Response Teams (CSIRTs)', 2003.

CCDCOE. 'National Cyber Security Framework Manual', sections: 3.2, 4.2.2, (2012). https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/.

CCDCOE. 'National Cyber Security Strategy Guidelines', sections 3.5 (2013). https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf.

CCI. 'Checklist', 2013.

CTO. 'Commonwealth Approach for Developing National Cyber Security Strategies', sections 4.4.3, 4.4.20, 4.4.21, 4.4.22, 4.4.27, 4.4.31, (2015).

ENISA. 'CERT Operational Gaps and Overlaps', 2011.

ENISA. 'Good Practice Guide for Incident Management', 2011.

ENISA. 'National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies', sections 3.6, 3.7, 3.10, 3.14, 4.1, 4.5, 4.8, (2016).

ENISA. 'Strategies for Incident Response and Cyber Crisis Cooperation', 2016.

FIRST. 'FIRST CSIRT Services Framework Version 2.1', 2019. https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0.pdf.

FIRST. 'FIRST PSIRT Services Framework Version 1.1', 2020. https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.1.pdf.

Global Cyber Security Capacity Center. 'Cybersecurity Capacity Maturity Model for Nations (CMM)', Dimension 1: 1.2; Dimension 5: 5.6, University Oxford, 2021.

ITU. 'CIRT Framework', 2021.

ITU. 'CyberDrill Framework', 2021.

Microsoft. 'Developing a National Strategy for Cybersecurity, Section: Building Incident Response Capabilities', 2013.

Microsoft. 'Information Sharing Framework for Cybersecurity', 2015.

Microsoft. 'Risk Management for Cybersecurity: Security Baselines', 2017.

OAS. 'Best Practice for Establishing a National CSIRT', p. 35, 2016.

OAS. 'Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity', pp.3-4, 2004.

OECD. 'Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity', section 2-B, 2015.

Potomac Institute for Policy Studies. 'Cyber Readiness Index 2.0', section 2,4, (2015). https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

TNO. 'Getting Started with a National CSIRT Guide', 2021. https://cybilportal.org/tools/getting-started-with-a-national-csirt-guide/.

UNU. 'Report: Cyber Resilience in Asia Pacific – A Review of National Cybersecurity Strategies', 2020. https://collections.unu.edu/view/UNU:7760.

WEF and Carnegie. 'International Strategy to Better Protect the Financial System Against Cyber Threats', 2020. https://carnegieendowment.org/2020/11/18/international-strategy-to-better-protect-financial-system-against-cyber-threats-pub-83105.

WEF. 'Cyber Resilience in the Electricity Ecosystem: Securing the Value Chain', 2020. https://www.weforum.org/whitepapers/cyber-resilience-in-the-electricity-ecosystem-securing-the-value-chain.

WEF. 'Cyber Resilience: Playbook for Public- Private Collaboration', 2018. https://www.weforum.org/reports/cyber-resilience-playbook-for-public-private-collaboration.

WEF. 'Pathways Towards a Cyber Resilient Aviation Industry', 2021. https://www.weforum.org/reports/pathways-towards-a-cyber-resilient-aviation-industry.

Appropriate set of policy instruments

CCDCOE. 'National Cyber Security Strategy Framework Manual', section 5, 2012. https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/.

CCDCOE. 'National Cyber Security Strategy Guidelines', section 3.2, 2013. https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf.

CCI. 'Checklist', 2013.

CTO. 'Commonwealth Approach for Developing National Cyber Security Strategies', sections 4.4.5, 4.4.6, 4.4.7, 4.4.8, 4.4.9, 4.4.18, 4.4.19, 4.4.20, (2015).

ENISA. 'National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies', sections 3.15, 3.184.9, 4.12, (2016).

Europe, Council. 'Budapest Convention on Cybercrime and Its Additional Protocol on Xenophobia and Racism (2001)', 2004.

Global Cyber Security Capacity Center. 'Cybersecurity Capacity Maturity Model for Nations (CMM)'. Dimension 4: 4.1, 4.3, 4.4, University Oxford, 2021.

Clear leadership, roles, and resource allocation

CCDCOE. 'National Cyber Security Framework Manual', sections 1.4.2, 2.1.1 2.1.3, 2.2, 2.3, 2.4, 3.1, 3.5, 4, 5.3.1, (2012). https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/.

CCDCOE. 'National Cyber Security Strategy Guidelines', sections 1.1, 3.3, 3.8, (2013). https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf.

CTO. 'Commonwealth Approach for Developing National Cyber Security Strategies', sections 4.4.1, 4.4.4, 4.4.5, 4.4.8, 4.4.9, 4.4.20, 4.4.21, 4.4.34, 4.5, (2015).

ENISA. 'An Evaluation Framework for National Cyber Security Strategies', sections 2, 2.2.1, 3.1.1, 3.1.2, 3.1.3, (2016).

ENISA. 'National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies', sections: 3.1, 3.2, 3.4, 3.5, 3.17, (2016).

ENISA. 'National Cyber Security Strategies: Setting the Course for National Efforts to Strengthen Security in Cyberspace', sections 4, 6 (2016).

Global Cyber Security Capacity Centre. 'Cybersecurity Capacity Maturity Model for Nations (CMM)', Dimension 1: 1.1, 1.2, University of Oxford (2021). (https://gcscc.ox.ac.uk/cmm-2021-edition)

GPD. 'Toolkit for Inclusive and Value-Based Cybersecurity Policymaking'. https://www.gp-digital.org/publication/toolkit-for-inclusive-and-value-based-cybersecurity-policymaking/.

Microsoft. 'Building an Effective National Cybersecurity Agency', 2018.

Microsoft. 'Developing a National Cybersecurity Strategy, Sections: A Principled Approach to Cybersecurity, Establishing Clear Priorities and Security Baseline', 2013.

Trust environment

ENISA. 'National Cyber Security Strategies: An Implementation Guide', 2012.

ENISA. 'National Cyber Security Strategies: Training Tool', 2016.

GCSCC. 'Cybersecurity Capacity Maturity Model for Nations (CMM)', Dimension 1: 1.1, University of Oxford, 2021. https://gcscc.ox.ac.uk/cmm-2021-edition.

GFCE. 'Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle', 2021. https://cybilportal.org/tools/catalog-of-project-options-for-the-national-cybersecurity-strategy-ncs-cycle/.

Potomac Institute for Policy Studies. 'Cyber Readiness Index 2.0', 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

Focus Areas

FA 1 Governance

CCDCOE. 'National Cyber Security Framework Manual', sections 1.4.2, 2.1.1 2.1.3, 2.2, 2.3, 2.4, 3.1, 3.5, 4, 5.3.1, (2012). https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/.

CCDCOE. 'National Cyber Security Strategy Guidelines', sections 1.1, 3.3, 3.8, (2013). https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf.

CCI. 'Checklist', 2013.

CTO. 'Commonwealth Approach for Developing National Cyber Security Strategies', sections 4.4.1, 4.4.4, 4.4.5, 4.4.8, 4.4.9, 4.4.20, 4.4.21, 4.4.34, 4.5, (2015).

ENISA. 'An Evaluation Framework for National Cyber Security Strategies', sections 2, 2.2.1, 3.1.1, 3.1.2, 3.1.3, (2016).

ENISA. 'National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies', sections: 3.1, 3.2, 3.4, 3.5, 3.17, (2016).

ENISA. 'National Cyber Security Strategies: Setting the Course for National Efforts to Strengthen Security in Cyberspace', sections 4, 6 (2016).

Global Cyber Security Capacity Centre. 'Cybersecurity Capacity Maturity Model for Nations (CMM)', Dimension 1: 1.1, 1.2, University of Oxford (2021). (https://gcscc.ox.ac.uk/cmm-2021-edition)

GPD. 'Toolkit for Inclusive and Value-Based Cybersecurity Policymaking'. https://www.gp-digital.org/publication/toolkit-for-inclusive-and-value-based-cybersecurity-policymaking/.

Microsoft. 'Building an Effective National Cybersecurity Agency', 2018.

Microsoft. 'Developing a National Cybersecurity Strategy, Sections: A Principled Approach to Cybersecurity, Establishing Clear Priorities and Security Baseline', 2013.

OAS. 'Managing National Cyber Risk', 2018. https://www.oas.org/es/sms/cicte/ENGcyberrisk.pdf.

OECD. 'Recommendation of the Council on Digital Security of Critical Activities', 2019. https://ccdcoe.org/uploads/2020/01/OECD-191211-The-Recommendation-of-the-Council-on-Digital-Security-of-Critical-Activities.pdf.

OECD. 'Cybersecurity Policy Making at a Turning Point, Annex IV', 2012.

OECD. 'Recommendation of the Council Concerning Guidelines for the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines', 2013.

OECD. 'Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2-A, Companion Document', 2015.

OECD. 'Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2-A, Companion Document', 2015.

Potomac Institute for Policy Studies. 'Cyber Readiness Index 2.0', 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

FA2 Risk management in national cybersecurity

CCDCOE. 'National Cyber Security Framework Manual', sections: 2.1.2, 5.3.2, (2012). https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/.

CCDCOE. 'National Cyber Security Strategy Guidelines', 2013. https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf.

CTO. 'Commonwealth Approach for Developing National Cyber Security Strategies', sections 4.4.6, 4.4.15, 4.4.24, 4.4.25, 4.4.26, 4.4.27, (2015).

ENISA. 'National Cyber Security Strategy Good Practice Guide – Designing and Implementing National Cyber Security Strategies, 2016.

Global Cyber Security Capacity Centre. 'Cybersecurity Capacity Maturity Model for Nations (CMM)', Dimension 1: 1.1, 1.2, 1.3; Dimension 2: 2.1; Dimension 3: 3.1, 3.2, 3.4; Dimension 4: 4.1, 4.2, 4.3, 4.4; Dimension 5: 5.1, 5.2, 5.4, 5.5, 5.6, University of Oxford, 2021. https://gcscc.ox.ac.uk/cmm-2021-edition.

Microsoft. 'Developing a National Cybersecurity Strategy. Building a Risk Approach', 2013.

Microsoft. 'Risk Management for Cybersecurity: Security Baselines', 2017.

NIST. 'Framework for Improving Critical Infrastructure Cybersecurity', 2015.

OAS. 'Managing National Cyber Risk', 2018. https://www.oas.org/es/sms/cicte/ENGcyberrisk.pdf.

OECD. 'Recommendation of the Council on Digital Security of Critical Activities', 2019. https://ccdcoe.org/uploads/2020/01/OECD-191211-The-Recommendation-of-the-Council-on-Digital-Security-of-Critical-Activities.pdf.

OECD. 'Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity', 2015.

Potomac Institute for Policy Studies. 'Cyber Readiness Index 2.0', section 1, 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

UNIDIR. 'Supply Chain Security in the Cyber Age: Sector Trends, Current Threats and Multi-Stakeholder Responses', 2020. https://unidir.org/publication/supply-chain-security-cyber-age-sector-trends-current-threats-and-multi-stakeholder.

WEF. 'Principles for Board Governance of Cyber Risk', 2021. https://www.weforum.org/reports/principles-for-board-governance-of-cyber-risk.

FA3 Preparedness and resilience

Carnegie Mellon. 'Handbook for Computer Security Incident Response Teams (CSIRTs)', 2003.

CCDCOE. 'National Cyber Security Framework Manual', sections: 3.2, 4.2.2, (2012). https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/.

CCDCOE. 'National Cyber Security Strategy Guidelines', section 3.5 (2013). https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf.

CCI. 'Checklist', 2013.

CTO. 'Commonwealth Approach for Developing National Cyber Security Strategies', sections 4.4.3, 4.4.20, 4.4.21, 4.4.22, 4.4.27, 4.4.31, (2015).

ENISA. 'CERT Operational Gaps and Overlaps', 2011.

ENISA. 'Good Practice Guide for Incident Management', 2011.

ENISA. 'National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies', sections 3.6, 3.7, 3.10, 3.14, 4.1, 4.5, 4.8, (2016).

ENISA. 'Strategies for Incident Response and Cyber Crisis Cooperation', 2016.

FIRST. 'FIRST CSIRT Services Framework Version 2.1', 2019. https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0.pdf.

FIRST. 'FIRST PSIRT Services Framework Version 1.1', 2020. https://www.first.org/standards/frameworks/psirts/FIRST_PSIRT_Services_Framework_v1.1.pdf.

Global Cyber Security Capacity Center. 'Cybersecurity Capacity Maturity Model for Nations (CMM)', Dimension 1: 1.2; Dimension 5: 5.6, University Oxford, 2021.

ITU. 'CIRT Framework', 2021.

ITU. 'CyberDrill Framework', 2021.

Microsoft. 'Developing a National Strategy for Cybersecurity, Section: Building Incident Response Capabilities', 2013.

Microsoft. 'Information Sharing Framework for Cybersecurity', 2015.

Microsoft. 'Risk Management for Cybersecurity: Security Baselines', 2017.

OAS. 'Best Practice for Establishing a National CSIRT', p. 35, 2016.

OAS. 'Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity', pp.3-4, 2004.

OECD. 'Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity', section 2-B, 2015.

Potomac Institute for Policy Studies. 'Cyber Readiness Index 2.0', section 2,4, (2015). https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

TNO. 'Getting Started with a National CSIRT Guide', 2021. https://cybilportal.org/tools/getting-started-with-a-national-csirt-guide/.

UNU. 'Report: Cyber Resilience in Asia Pacific – A Review of National Cybersecurity Strategies', 2020. https://collections.unu.edu/view/UNU:7760.

US "National Cyber Incident Scoring System (NCISS) which includes a Cyber Incident Severity Schema (CISS)". https://us-cert.cisa.gov/CISA-National-Cyber-Incident-Scoring-System.

WEF and Carnegie. 'International Strategy to Better Protect the Financial System Against Cyber Threats', 2020. https://carnegieendowment.org/2020/11/18/international-strategy-to-better-protect-financial-system-against-cyber-threats-pub-83105.

WEF. 'Cyber Resilience in the Electricity Ecosystem: Securing the Value Chain', 2020. https://www.weforum.org/whitepapers/cyber-resilience-in-the-electricity-ecosystem-securing-the-value-chain.

WEF. 'Cyber Resilience: Playbook for Public- Private Collaboration', 2018. https://www.weforum.org/reports/cyber-resilience-playbook-for-public-private-collaboration.

WEF. 'Pathways Towards a Cyber Resilient Aviation Industry', 2021. https://www.weforum.org/reports/pathways-towards-a-cyber-resilient-aviation-industry.

FA4 Critical Infrastructure services and essential services

CCDCOE. 'National Cyber Security Framework Manual', section 4.5.4, 2012. https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/.

CCDCOE. 'National Cyber Security Strategy Guidelines', sections 3.4, 3.5, (2013). https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf.

CTO. 'Commonwealth Approach for Developing National Cyber Security Strategies', sections 4.4.12, 4.4.13, 4.4.20, 4.4.25, 4.4.26, 4.4.28, 4.4.32, (2015).

ENISA. 'An Evaluation Framework for National Cyber Security Strategies', section 4.2, 2016.

ENISA. 'Methodologies for the Identification of Critical Information Infrastructure Assets and Services', 2015.

ENISA. 'National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies', section 3.6, 2016.

Global Cyber Security Capacity Center. 'Cybersecurity Capacity Maturity Model for Nations (CMM)'. Dimension 1: 1.1, 1.3, University Oxford, 2021.

Meridian and GFCE. 'Companion Document to the GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for Governmental Policy-Makers', 2016. https://www.tno.nl/media/10425/companiondocument_gpg_ciip.pdf.

Microsoft. 'Critical Connections: Protecting Infrastructures, All Sections', 2014.

Microsoft. 'Critical Infrastructure Protection: Concepts and Continuum, All Sections', 2014.

Microsoft. 'Risk Management for Cybersecurity: Security Baselines', 2017.

OAS. 'Report Cybersecurity and Critical Infrastructure in the Americas', 2015.

OECD. 'Recommendation of the Council on Digital Security of Critical Activities https://Ccdcoe.Org/Uploads/2020/01/OECD-191211-The-Recommendation-of-the-Council-on-Digital-Security-of-Critical-Activities.Pdf.

Potomac Institute for Policy Studies (2015): Cyber Readiness Index 2.0', 2019. https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

OECD. 'Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity', 2015.

Potomac Institute for Policy Studies. 'Cyber Readiness Index 2.0', section 2.4, 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

UNIDIR. 'International Cooperation to Mitigate Cyber Operations against Critical Infrastructure', 2021. https://unidir.org/criticalinfrastructure.

UNOCT, CTED and INTERPOL. 'Compendium of Good Practices for the Protection of Critical Infrastructure against Terrorist Attack', 2018. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/eng_compendium-cip-final-version-120618.pdf.

FA5 Capability and capacity building and awareness raising

'Council of Europe, Capacity Building Programmes', n.d.

CCDCOE. 'National Cyber Security Strategy Framework Manual', sections 4.5.5, 4.6.3, (2012).

CCDCOE. 'National Cyber Security Strategy Guidelines', 2013. https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf.

CCI. 'Checklist', 2013.

CCI. 'Commonwealth Network of Contact Persons Framework', 2005.

CCI. 'Harare Scheme on Mutual Legal Assistance in Criminal Matters', 2011.

Council of Europe. 'Capacity building programmes'. https://www.coe.int/en/web/cybercrime/capacity-building-programmes.

Council of Europe. 'Cybercrime Octopus Community (Country Resources, Training Materials, Guides and Research'. https://www.coe.int/en/web/octopus/home?desktop=true.

CTO. 'Commonwealth Approach for Developing National Cyber Security Strategies', sections 4.4.11, 4.4.17, 4.4.20, 4.4.34, 4.4.12, 4.4.14, 4.4.16, 4.4.23, (2015).

ENISA. 'CERT Operational Gaps and Overlaps', p. 6, 16, 19, 21, 27, 29, 31, 32, 50, 57 (2011).

ENISA. 'Cybersecurity Skills Development in the EU', 2020.

ENISA. 'Good Practice Guide for Incident Management' p.19, 23, 26, 32, 46, 56, 58, 64, 69, (2010).

ENISA. 'National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies', sections 3.12, 3.8, 3.11, 3.13, 4.3, 4.6, 4.7, 4.14, (2016).

ENISA. 'Strategies for Incident Response and Cyber Crisis Cooperation, Section', section 2.1, (2016).

Global Cyber Security Capacity Center. 'Cybersecurity Capacity Maturity Model for Nations (CMM)'. Dimension 3: 3.1, 3.2, 3.3, 3.4, University Oxford, 2021.

ITU. 'CIRT Framework', 2021.

ITU. 'CyberDrill Framework', 2021.

Microsoft. *Developing a National Strategy for Cybersecurity, Section: Driving Research and Technology Investment, Public Awareness*. Workforce Training and Education, 2013.

NIST. 'Workforce Framework for Cybersecurity NICE Framework', 2020. https://doi.org/10.6028/NIST.SP.800-181r1.

OAS. 'Cyber Security Awareness Campaign Toolkit, All Sections', 2015.

OAS. 'Cybersecurity Education: Planning for the Future Through Workforce Development', 2020.

OECD. 'Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity', section 2-B, 2015.

Potomac Institute for Policy Studies. 'Cyber Readiness Index 2.0', section 2.5, 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

UNCTAD. 'Programme on E-Commerce and Law Reform', 2015.

US "National Cyber Incident Scoring System (NCISS) which includes a Cyber Incident Severity Schema (CISS)".
https://us-cert.cisa.gov/CISA-National-Cyber-Incident-Scoring-System.

FA6 Legislation and Regulation

CCDCOE. 'National Cyber Security Strategy Framework Manual', section 5, 2012. https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/.

CCDCOE. 'National Cyber Security Strategy Guidelines', section 3.2, 2013. https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf.

CCI. 'Checklist', 2013.

Council of Europe. 'Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence - Draft as Approved by the Cybercrime Convention Committee', 2021.

Council of Europe. 'Strategic Priorities for Cooperation on Cybercrime and Electronic Evidence in GLACY Countries', sections 1, 2, 6, (2016).

Council of Europe. 'Strategic Priorities for the Cooperation against Cybercrime in the Eastern Partnership Region', sections 1,2,7, (2013).

CTO. 'Commonwealth Approach for Developing National Cyber Security Strategies', sections 4.4.5, 4.4.6, 4.4.7, 4.4.8, 4.4.9, 4.4.18, 4.4.19, 4.4.20, (2015).

ENISA. 'National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies', sections 3.15, 3.184.9, 4.12, (2016).

Europe, Council. 'Budapest Convention on Cybercrime and Its Additional Protocol on Xenophobia and Racism (2001)', 2004.

Global Cyber Security Capacity Center. 'Cybersecurity Capacity Maturity Model for Nations (CMM)'. Dimension 4: 4.1, 4.3, 4.4, University Oxford, 2021.

ITU. 'Guidelines for Policy-Makers on Child Online Protection', sections 3.3, 3.4, (2020). https://www.itu-cop-guidelines.com/policymakers.

Potomac Institute for Policy Studies. 'Cyber Readiness Index 2.0', section 3, 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

UN. 'Sustainable Development Goals, Article 16.3 UNCTAD, Global Cyberlaw Tracker', 2015.

UNHR. 'International Covenant on Civil and Political Rights, Article 19', 1976.

WEF. 'Cybercrime Prevention Principles for Internet Service Providers', 2020. https://www.weforum.org/reports/cybercrime-prevention-principles-for-internet-service-providers.

WEF. 'Partnership against Cybercrime', 2020. https://www.weforum.org/reports/partnership-against-cybercrime.

WEF. 'Recommendations for Public-Private Partnership against Cybercrime', 2016. http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf.

World Bank. 'Combatting Cybercrime: Tools and Capacity Building for Emerging Economies'.

FA7 International Cooperation

'Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence - Draft as Approved by the Cybercrime Convention Committee', n.d.

CCDCOE. 'National Cyber Security Strategy Framework Manual', sections 4.7, 5.4.2, 5.4.3, (2012). https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/.

CCDCOE. 'National Cyber Security Strategy Guidelines', sections 1.3, 3.2.1, 3.3.2, (2013). https://ccdcoe.org/uploads/2018/10/NCSS-Guidelines_2013.pdf.

CCDCOE. 'The Tallin Manual 2.0', 2017. https://ccdcoe.org/research/tallinn-manual/.

Council of Europe. 'Budapest Convention on Cybercrime and Its Additional Protocol on Xenophobia and Racism (2001)', chapter III, 2004.

Council of Europe. 'Strategic Priorities for Cooperation on Cybercrime and Electronic Evidence in GLACY Countries' Strategic Priority 7, 2016.

Council of Europe. 'Strategic Priorities for the Cooperation against Cybercrime in the Eastern Partnership Region', Strategic Priority 8, 2013.

CTO. 'Commonwealth Approach for Developing National Cyber Security Strategies', sections 4.4.20, 4.4.21 (2015).

ENISA. 'Guidebook on National Cyber Security Strategies, Section', section 3.16, 2016.

ENISA. 'National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies', sections: 3.16. 4.10, (2016).

Global Cyber Security Capacity Center. 'Cybersecurity Capacity Maturity Model for Nations (CMM)', Dimension 1: 1.1, 4: 4.4, University Oxford, 2021.

Microsoft. 'Developing a National Strategy for Cybersecurity, Section on Structuring International Engagement', 2013.

OECD. 'Recommendation of the Council on Digital Security of Critical Activities', 2019. https://ccdcoe.org/uploads/2020/01/OECD-191211-The-Recommendation-of-the-Council-on-Digital-Security-of-Critical-Activities.pdf.

OECD. 'Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity' p. 13, 48, 58, 2015.

Potomac Institute for Policy Studies. 'Cyber Readiness Index 2.0', section 4.6, 2015. https://www.potomacinstitute.org/images/CRIndex2.0.pdf.

UNIDIR. 'Cyber Policy Portal', 2021.

UNIDIR. 'International Cooperation to Mitigate Cyber Operations against Critical Infrastructure', 2021. https://unidir.org/criticalinfrastructure.

Section 7

Acronyms

Acronym	Definition
AFRIPOL	African Union Mechanism for Police Cooperation
AMERIPOL	The Police Community of the Americas
ASEANAPOL	ASEAN Chiefs of Police
Axon	Axon Partners Group
CBMs	Confidence-building measures,
CBOs	Community-based Organizations
CCB	Commitment to cybersecurity capacity-building
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CERTs	Computer Emergency Response Teams
CIIs	Critical Information Infrastructures
CIRTs	Computer Incident Response Teams
CIs	Critical Infrastructures
CoE	Council of Europe
ComSec	Commonwealth Secretariat
CRI	The Cyber Readiness Institute
CSIRTs	Computer Security Incident Response Teams
CTO	Commonwealth Telecommunications Organisation
DCAF	Geneva Centre for Security Sector Governance
DNS	Domain Name Service
ECOPOL	ECO Police
ECOWAS	Economic Community of West African States
Europol	European Police Office
FIRST	Forum of Incident Response and Security Teams
GCCPOL	Gulf Cooperation Council Police
GCSCC	Global Cyber Security Capacity Centre
GCSP	Geneva Centre for Security Policy
GFCE	The Global Forum on Cyber Expertise
GGE	UN Group of Governmental Experts
GLACY+	Global Action on Cybercrime Extended
GPD	Global Partners Digital
ICT	Information & Communication Technology
INTERPOL	International Criminal Police Organization
ISACs	Information Sharing and Analysis Centers
ITU	International Telecommunication Union ITU
IXPs	Internet Exchange Points
KPIs	Key Performance Indicators
NCS	National Cybersecurity Strategy
OAS	The Organization of American States
OEWG	UN Open-ended Working Group
OSCE	Organisation of Security and Cooperation in Europe
PIPS	Potomac Institute for Policy Studies
R&D	Research and Development
RCEP	Regional Comprehensive Economic Partnership
SMEs	Small and Medium Enterprises
UNIDIR	United Nations Institute for Disarmament Research
UNOCT	United Nations Office of Counter-Terrorism
UNU	United Nations University
USMCA	United States-Mexico-Canada Agreement
WEF	The World Economic Forum
WIPO	World Intellectual Property Organization