GUIDE TO DEVELOPING A NATIONAL CYBERSECURITY STRATEGY

STRATEGIC ENGAGEMENT IN CYBERSECURITY

ITU

CCDCOE

The Commonwealth Cybercrime Initiative

CTO

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

Deloitte.

Global Cyber Security Capacity Centre

GCSP
Geneva Centre for Security Policy
Where knowledge meets experience

Microsoft

POTOMAC INSTITUTE FOR POLICY STUDIES

Some Rights Reserved

Rights & Permission

Acknowledgments

This Guide was developed by twelve partners from Intergovernmental and International Organisations, private sector, as well as academia and civil society and included the following organisations: Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organisation (CTO), Deloitte, the Geneva Centre for Security Policy (GCSP), the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford, the International Telecommunication Union (ITU), Microsoft, the NATO Cooperative Cyber Defence Centre Of Excellence (NATO CCD COE), the Potomac Institute for Policy Studies, RAND Europe, The World Bank and the United Nations Conference on Trade and Development (UNCTAD).

The team included Katalaina Sapolu (ComSec), Shadrach Haruna (ComSec), Martin Koyabe (CTO), Fargani Tambeayuk (CTO), Andrea Rigoni (Deloitte), Carolin Weisser (GCSCC), Marco Obiso (ITU), Kaja Ciglic (Microsoft), Kadri Kaska (NATO CCD COE), Francesca Spidalieri and Melissa Hathaway (the Potomac Institute for Policy Studies), Erik Silfversten (RAND Europe), David Satola and Sandra Sergeant (The World Bank), and Cecile Barayre (UNCTAD).

The European Union Agency for Network and Information Security (ENISA) provided a significant contribution to the Guide.

The contributions of the following people are also recognised: Grace Acayo, Rosheen Awotar-Mauree, Ben Baseley-Walker, Paul Cornish, Luc Dandurand, Michael Goldsmith, Kemal Huseinovic, Andraz Andy Kastelic, Maxim Kushtuev, Lena Lattion, Gustav Lindstrom, Damien Maddalena, Emily Munro, Lara Pace, Sarah Puello Alfonso, Valeria Risuglia, Taylor Roberts, Monica M. Ruiz, Irene Rubio, Ann Valjataga, Julienne Wright.

Foreword

It is a pleasure to present – on behalf of the partners involved – the National Cybersecurity Strategy Guide, aimed at providing an aggregated and harmonised set of principles and good practices on the development, establishment and implementation of national cybersecurity strategies.

Facilitated by ITU, twelve partners from the public and private sectors, academia and civil society agreed to share their experience, knowledge and expertise, producing a Guide that gathers existing know-how from the participating organisations as well as providing references to complementary publications, in order to ease access to available resources.

Over the last two decades, billions of people around the world have benefited from the exponential growth and rapid adoption of information and communications technologies, and the associated economic and social opportunities. We are witnessing a digital revolution that is profoundly transforming our societies.

Cybersecurity is a fundamental factor in achieving socio-economic development. Yet, only seventy-six[1] countries around the world have, publicly available, national cybersecurity strategies. It is therefore imperative to boost efforts to produce them. As the title suggests, the objective of the Guide is to instigate strategic thinking and help national leaders and policy-makers to develop, establish and implement national cybersecurity strategies.

I am confident that the National Cybersecurity Strategy Guide will serve as a useful tool for all stakeholders with cybersecurity responsibilities. I would personally like to express my gratitude to the partners, for their continuous, invaluable support and commitment in making this project a great success as a concrete example of a successful multistakeholder collaboration.

Brahima Sanou
Director, ITU Telecommunication Development Bureau

[1] From the ITU Global Cybersecurity Index (GCI) 2017

Table of contents

Preface

This National Cybersecurity Strategy Guide 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, which taps into the knowledge, experience and expertise of many organisations in the field of national cybersecurity strategies and policies. Specifically, this Guide has been produced by twelve partners from public and private sectors, as well as and academia and civil society.

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 policy-makers in the development of defensive responses to cyber-threats, in the form of a National Cybersecurity Strategy, and in thinking strategically about cybersecurity, cyber-preparedness, response and resilience, building confidence and security in the use of information and communications technologies (ICTs).

The National Cybersecurity Strategy 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 the resulting National Cybersecurity Strategy Guide can serve as a useful tool to all stakeholders, including national policy-makers, 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.

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 the 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, who provide assistance in cybersecurity.

2 Introduction

Over the last two decades, billions of people around the world have benefited from the exponential growth and rapid adoption of information and communications technologies, and the associated economic and social opportunities.

Since its creation, the Internet has evolved from an information-exchange platform 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 cyber-threats, 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.

By developing and implementing a National Cybersecurity Strategy, a nation can improve the security of its digital infrastructure and ultimately contribute to its broader socio-economic aspirations. National leaders need to be strategic about the opportunities offered and the risks posed to their countries by the digital environment; they also need to establish a clear vision of the digital future they wish to create.

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, services, telecommunications systems, and data in the cyber-environment.[2]

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.

[2] Definition adapted from https://www.bcmpedia.org/wiki/Cyber_Security

Setting out the vision, objectives and priorities 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.

3 Lifecycle of a National Cybersecurity Strategy

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

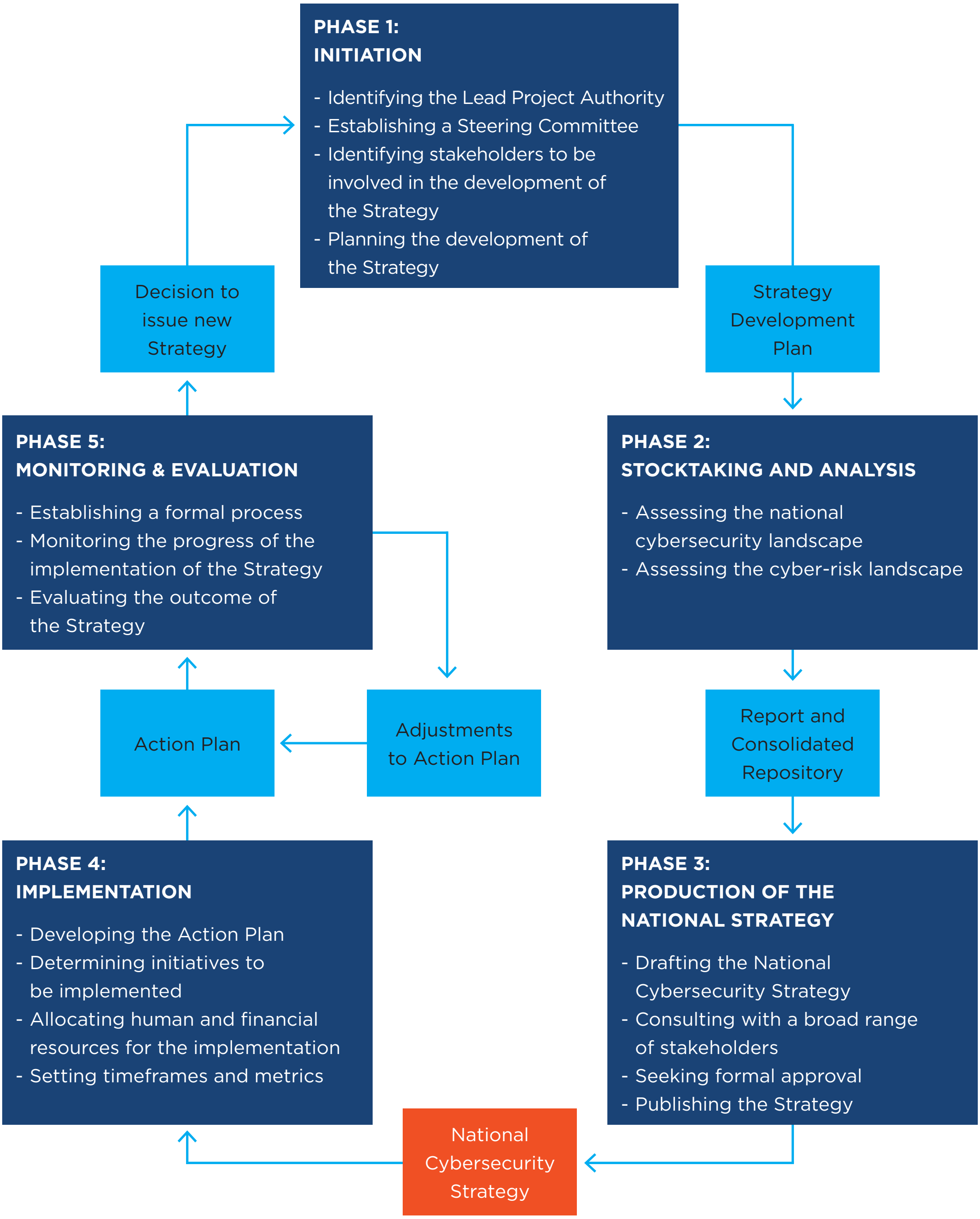
- Phase I – Initiation
- Phase II – Stocktaking and analysis
- Phase III – Production
- Phase IV – Implementation
- Phase V – Monitoring and evaluation

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.

Figure 1 *- Lifecycle of a National Cybersecurity Strategy*



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]

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 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 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.

[3] The individual or entity in charge of the decision-making process at the national level.

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 ensure all pertinent knowledge and expertise is utilised. 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.

Such cooperation mechanism could take the form of an Advisory Committee, that would contribute in providing members to the Steering Committee, as well as be consulted on the various phases.

3.1.4 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. It should specify how and when relevant stakeholders will be expected to participate in the development process to contribute input and feedback.

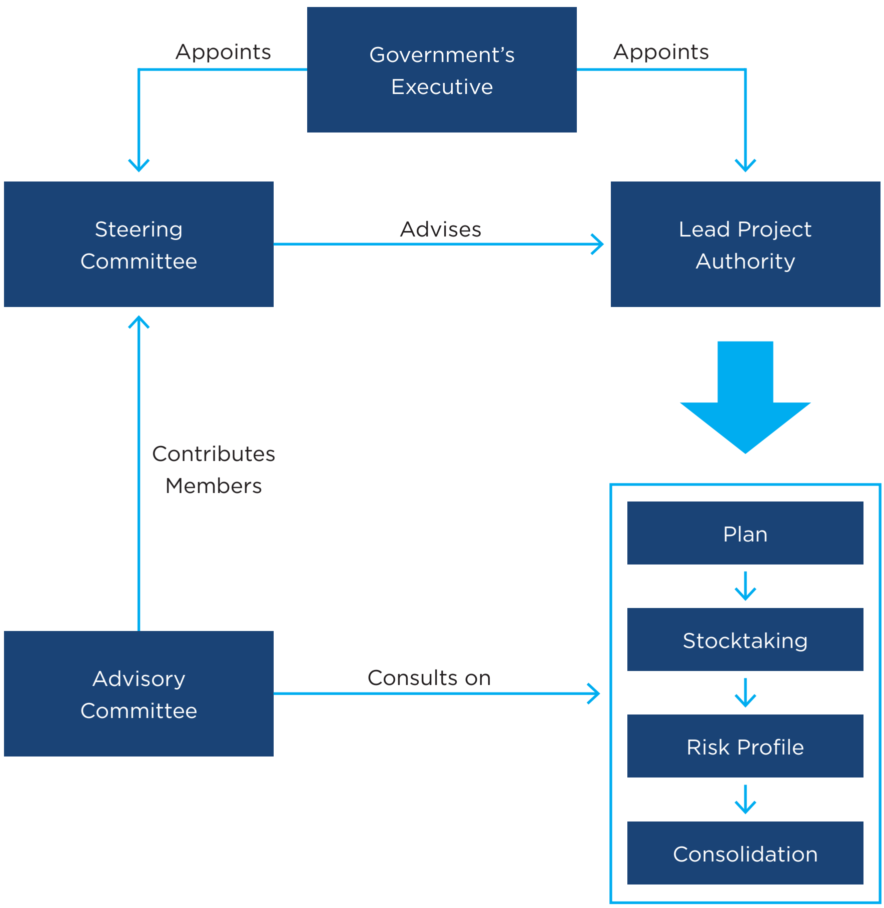
It should also identify the human and financial resources needed, and where these could be procured. For example, required expertise could be solicited from intergovernmental organisations, the private sector, academia, or development agencies. Similarly, funding requirements might be addressed through 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).

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

Further references available on page 55.

Figure 2 *- Stakeholders*



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-risk landscape to inform the drafting and development of the National Cybersecurity Strategy. The output of this exercise 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 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 stated objectives of the Strategy 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 potential effects and outcomes of means chosen.

Further references available on page 55.

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).

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 (CERTs). 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, private sector projects, ICT and cyber-education and skill-development programmes, cyber-R&D initiatives; data on Internet penetration and infection rates, ICT uptake, 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).

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) should be considered 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.

Similarly 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 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 responsible for initiating and developing cybersecurity policies and regulations within the country. In addition, it should define the responsibilities and tasks of the entities responsible for collecting threat and vulnerability information, responding to cyber-incidents (e.g., national CERTs), 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 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. 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 the Strategy

The Strategy should be a public document and should be made readily available. Its broad availability 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 and the private sector.

Further references available on page 55.

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 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 could include organising cybersecurity exercises, establishing security baselines for critical infrastructures, or 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 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 key performance indicators should be developed by the Lead Project Authority in partnership with the respective owners. 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 55.

3.5 Phase V: Monitoring and evaluation

During this phase, 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 its competent authority should assess whether the Strategy is still relevant 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 key performance indicators (KPI) by near-term, mid-term and long-term objectives helps reinforce the governance and management mechanisms. Key performance indicators or metrics should be:

- ***Specific*** *– target a specific area for improvement.*
- ***Measurable*** *– quantify or at least suggest an indicator of progress.*
- ***Achievable*** *– state what results can realistically be achieved, given available resources.*
- ***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.

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 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 55.

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 it 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 56.

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 prioritised.

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, sustainable development, etc.

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 56.

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 government, businesses and individuals. These groups face cybersecurity risks and share a level of responsibility in managing them, depending on their role. While it may be a difficult task, identifying and 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, the Strategy should be a public document.

Further references available on pages 56 and 57.

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 57.

4.5 Fundamental human rights

The Strategy should respect and be consistent with fundamental values.

The Strategy should recognise the fact that rights that people have offline must also be protected online. It should respect universally agreed fundamental 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 balancing the needs of the State with those of the individuals, 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 pages 57 and 58.

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, 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, ensuring the resilience of economic and societal activity in the country. With that in mind, the Strategy should encourage the adoption of business-continuity measures, which include incident and crisis management, as well as recovery plans.

Further references available on page 58.

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, incentive and 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 59.

4.8 Clear leadership, roles, and resource allocation

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 59.

4.9 Trust environment

The Strategy should help build a digital environment that citizens and businesses 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 and digital financial transactions, among others) supported by ICTs and utilised by the 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 59.

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 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 be considered for inclusion in the text of the Strategy when addressing the governance structure for national cybersecurity. The Strategy should clearly state the objectives and ambitions the government has in mind for cybersecurity, as well as outline the roles and accountabilities required to ensure its implementation.

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 include 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 how significant the country finds cybersecurity.

5.1.2 Establish a competent cybersecurity authority

The Strategy should identify a dedicated national-competent cybersecurity authority – 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.

Such a national competent cybersecurity 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. This approach may require additional policy or legal structures to empower them to perform their 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.

5.1.3 Ensure intra-government 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 (i.e. rules) and resources yield the desired outcomes of the Strategy.

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.

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 stakeholders (and vice-versa) in ensuring cybersecurity. To this end, it should articulate how the government will engage these 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.

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, material, as well as the relationships and partnerships and continued political commitment and leadership required for successful execution. Resourcing the objectives and tasks within the Strategy should not be viewed as a one-time initiative. Resources can be allocated by task or objective, or by a governmental entity.

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 pages 60 and 61.

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 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 result in the identification of key assets and services critical to the proper functioning of the society and economy, threats, and the risks associated with them.

The approach should aim to 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.

5.2.2 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 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 infrastructure or services, the risk-management methodology should furthermore provide guidance on minimising risk through secure architecture and design, recognising that security is best achieved where it is an integral part of the design process of a product, process or service (*security by design*).

5.2.3 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 critical to its society and economy.

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.

5.2.4 Establishing 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 cyber-incidents.

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 61.

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 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 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 organisational 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 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

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, 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 decision-making 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 under pressure, and help understand any cross-sector dependencies.

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

Further references available on pages 62 and 63.

5.4 Focus area 4 - Critical Infrastructure services and essential services

This focus area investigates good practice relating to protecting Critical Infrastructures (CIs), and in particular Critical Information Infrastructures (CIIs). While there are no universally recognised definitions for the two terms and the 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)* is a term used to describe 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.

Alternatively, the concept of essential services may be applied, referring to services, which are essential for the maintenance of critical societal or economic activities.

In either case, a few non-exhaustive examples of these 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 and private clinics), drinking-water 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, among others).

5.4.1 Establish a risk-management approach to protecting critical infrastructures and services

The Strategy should address the protection of CIs and CIIs from a risk-management perspective, in accordance with Principle of Risk Management and Resilience (Section 4.6). A detailed risk assessment should guide the identification of national CIs and CIIs and critical 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.

Furthermore, a risk-based approach should also be adopted in identifying and prioritising implementation of programmes and policies designed to protect CIs and CIIs. To facilitate engagement with the private sector, a risk-management approach based on 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.

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. When developing such baselines, internationally recognised standards and best practices should be considered to ensure better security outcomes and greater efficiencies.

Security baselines should be outcomes-focused, 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”), which in turn can allow government and industry to benefit from continuous security improvements. In addition, an outcomes-based approach to the development of these baselines leaves room for sector-specific implementation or "how to" guidance, which allows enterprises the flexibility to regularly update their own guidance to reflect the changing technology and threat environments.

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 the 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: coming to an agreement on common 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 pages 63 and 64.

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 and awareness-raising among government entities, citizens, businesses and other organisations – crucial to enabling a country's digital economy.

Good practices considered in this section include, 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 Develop cybersecurity curricula

The Strategy should facilitate the development of school curricula with the aim of accelerating cybersecurity skills development and awareness throughout the formal education system. This should include developing dedicated cybersecurity curricula across primary and secondary schools, integrating cybersecurity courses in all computer science and IT programmes in higher education, and creating dedicated cybersecurity degrees and government apprenticeships.

Additionally, the school 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.

5.5.2 Stimulate skills development and workforce training

The Strategy should address 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. Technical training should be complemented with initiatives focused on risk management.

The Strategy should also foster initiatives, which aim to develop dedicated cybersecurity career paths, in particular for the public sector, and incentives to increase the supply of qualified cybersecurity professionals. 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.

5.5.3 Implement a coordinated cybersecurity awareness-raising programme

The Strategy should assign responsibility to coordinate cybersecurity awareness campaigns and activities at the national level to a competent authority to ensure resources are streamlined and accountability established. The authority 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.

5.5.4 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 dissemination of new findings, baseline technologies, techniques, processes and tools. 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 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.

Further references available on pages 64 and 65.

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 and on Trust Environment (Sections 4.3 and 4.9, respectively). Such a framework could include: the adoption of legislation that defines what constitutes illegal cyber-activity; legal recognition of individual rights and civil liberties; establishment of compliance mechanisms; the building of capacity to enforce the framework; institutionalisation of critical entities; and international cooperation to fight cybercrime.

5.6.1 Establish cybercrime legislation

The Strategy should promote the development of a domestic legal framework that clearly defines what constitutes prohibited cyber-activity, and that aims to reduce online crime. 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).

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).

5.6.2 Recognise and safeguard individual rights and liberties

The Strategy should safeguard essential due process rights (in the case of criminal investigations and prosecutions), as well as rights of data protection, including protecting the privacy of personal data (possibly through the development of a data-protection and privacy framework) and freedom of expression, in accordance with the Principle of Fundamental Human Rights (Section 4.5).

5.6.3 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 digital investigation, lawful interception of communications and use of electronic evidence.

5.6.4 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 and other investigators). 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; and to effectively collaborate with industry and international law-enforcement entities (e.g., INTERPOL, Europol) to tackle cybercrime and to boost cybersecurity. This element should take into consideration focus area 5 on Capability and Capacity Building and Awareness Raising (Section 5.5).

5.6.5 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, those responsible for protecting critical 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).

In some legal systems, legislation might be required for the establishment of institutions involved in cybersecurity, such as national CERTs/CIRTs/CSIRTs, or in clarifying the authority of a single agency to coordinate cyber-policy in a country.

5.6.6 Support international cooperation to combat 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. This element should take into consideration focus area 7 on international cooperation (Section 5.7).

Further references available on pages 65 and 66.

5.7 Focus area 7 - International cooperation

This focus area emphasises the elements that the Strategy should cover in terms of cybersecurity engagements outside the particular country, both at regional and international levels. Cybersecurity increasingly plays a role in many different areas of international relations, including human rights, economic development, trade, commerce, arms control, security, stability, peace and conflict resolution.

The Strategy should therefore recognise the borderless nature of cybersecurity, and highlight the need to cooperate with not only national, but also international stakeholders. International engagements with public and private stakeholders are key to facilitating a constructive dialogue, developing trust and cooperation mechanisms, finding mutually acceptable solutions to common challenges, and creating a global culture of cybersecurity.

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, as well as its foreign-policy priorities.

5.7.1 Recognise the importance of cybersecurity as a priority of foreign policy

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. To this end, it is important to encourage the development and use of competencies and skills focused on cyber-issues (cyber-diplomacy) to complement the traditional methods and processes of diplomacy. 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.

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

This may also require better harmonisation among different governmental players (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 player at a negotiating table in the international cybersecurity arena is properly coordinated and aligned with other governmental bodies.

5.7.2 Engage in international discussions

The Strategy should identify specific international fora and cooperation mechanisms that the country wishes to join to effectively engage diplomatically on cyber-related issues. These could include regional or global organisations, intergovernmental discussions, public and/or private-sector alliances, as well as established traditional cooperation and collaboration mechanisms that include cybersecurity issues.

As the country begins to undertake such engagements, these will likely require the government to develop additional competencies and skills focused on cyber-issues and increase its overall cybersecurity capacity. It is therefore important to effectively prioritise these efforts and allocate adequate resources (personnel and money) to ensure that they deliver concrete results.

5.7.3 Promote formal and informal cooperation in cyberspace

The Strategy should indicate the operational international-cooperation mechanisms that the country wishes to commit to. The country may wish to engage in formal and informal international endeavours advancing cooperation on, for example, policy and legislative development, law enforcement, incident-response, information- and threat-sharing. Participation in such initiatives could, for example, support better cooperation and exchange of information between relevant authorities on potential threats and vulnerabilities.

5.7.4 Align domestic and international cybersecurity efforts

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

To this end, the Strategy should show the country's commitment to ensuring consistency between its 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.

Notable examples of existing international efforts that could be considered as part of the Strategy include, but are not limited to: the work of the United Nations Governmental Group of Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), the Organisation of Security and Cooperation in Europe (OSCE) on confidence building measures (CBMs) and international norms applicable in cyberspace, the work of the G7 Group's High-Tech Crime Subgroup, the Council of Europe's Budapest Convention on Cybercrime, the African Union's Convention on Cybersecurity, the agreement between the governments of state members of the Shanghai Cooperation Organization on cooperation in the field of ensuring international information security, the Arab Convention on Combating Information Technology Offences, the ECOWAS Directive on fighting cybercrime, as well as the support of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) for the Tallinn Manuals 1.0 and 2.0.

Further references available on page 66.

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.

CCI (2017), *Harare Scheme on Mutual Legal Assistance in Criminal Matters*

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

Commonwealth (2018), *Commonwealth Cyber Declaration*

CTO (2015), *Commonwealth Approach for Developing National Cyber Security Strategies*

Council of Europe (2001), *Budapest Convention on Cybercrime*

Council of the European Union (2017), *Cyber Diplomacy toolbox*

ENISA (2014), *An Evaluation Framework For National Cyber Security Strategies*

ENISA (2011), *CERT Operational Gaps and Overlaps*

ENISA (2011), *Good Practice Guide for Incident Management*

ENISA (2015), *Methodologies for the Identification of Critical Information Infrastructure Assets and Services*

ENISA (2016), *National Cyber Security Strategy Good Practice Guide – Designing and Implementing National Cyber Security Strategies*

ENISA (2012), *National Cyber Security Strategies: Practical Guide on Development and Execution*

ENISA (2012), *National Cyber Security Strategy, Setting the Course for National Efforts to Strengthen Security in Cyberspace*

ENISA (2016), *National Cyber Security Strategies: Training Tool*

ENISA (2016), *Stocktaking, Analysis and Recommendations on the Protection of CIIs*

ENISA (2016), *Strategies for Incident Response and Cyber Crisis Cooperation*

Global Cyber Security Capacity Centre, University of Oxford (2016), *Cybersecurity Capacity Maturity Model for Nations*

ITU (2017), *Securing Information and Communication Networks. Best Practices for Developing a Culture of Cybersecurity*

ITU (2017), *Global Cybersecurity Index*

ITU (2011), *National Cybersecurity Strategy Guide*

ITU (2010), *UNDERSTANDING CYBERCRIME: Phenomena, Challenges and Legal Response*

ITU (2009), *Cybersecurity Guide for Developing Countries*

Microsoft (2013), *Developing a National Strategy for Cybersecurity*

Microsoft (2014), *Critical Infrastructure Protection: Concepts and Continuum*

Microsoft (2014), *Critical Connections: Protecting Infrastructures*

Microsoft (2014), *Hierarchy of Cybersecurity Needs*

Microsoft (2018), *Building an effective national cybersecurity agency*

Microsoft (2018), *Cybersecurity Policy Framework*

Microsoft (2015), *Information Sharing Framework for Cybersecurity*

Microsoft (2017), *Risk Management for Cybersecurity: Security Baselines*

NATO CCD COE (2012), *National Cyber Security Framework Manual*

NATO CCD COE (2013), *National Cyber Security Strategy Guidelines*

NIST (2014), *Framework for Improving Critical Infrastructure Cybersecurity*

OAS (2015), *Best Practice for Establishing a National CSIRT*

OAS (2004), *Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity*

OAS (2015), *Cyber Security Awareness Campaign Toolkit*

OAS (2015), *Report Cybersecurity and Critical Infrastructure in the Americas*

OECD (2015), *Companion Document to the Recommendation on Digital Security Risk Management for Economic and Social Prosperity*

OECD (2012), *Cybersecurity Policy Making at a Turning Point*

OECD (2015), *Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity*

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

OECD (2008), *Recommendation of the Council on the Protection of Critical Information Infrastructures*

OECD (2007), *Report on the Development of Policies for the Protection of Critical Information Infrastructures*

Potomac Institute for Policy Studies (2015), *Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and An Index*

United Nations (2015), *Sustainable Development Goals*

United Nations (1976), *International Covenant on Economic, Social and Cultural Rights, International Covenant on Civil and Political Rights and Optional Protocol to the International Covenant on Civil and Political Rights, Resolution 2200 (XXI)*

United Nations (2014), *The Right to Privacy in the Digital Age, Res A/RES/68/167*

United Nations (1948), *Universal Declaration of Human Rights*

UNCTAD (2014), *A Framework for Information and Communications Technology Policy Reviews*

UNCTAD, *Developing E-Commerce Legislation*

UNCTAD (2016), *Study on Data Protection Regulations and International Data Flows*

UNHR (1976), *International Covenant on Civil and Political Rights*

World Bank et al (2017), *Combatting Cybercrime: Tools and Capacity Building for Emerging Economies*

A detailed breakdown of references to the individual principles and good practice can be found below.

National Cybersecurity Strategy Lifecycle

Sub-topic	Reference
Initiation	ENISA (2016), National Cyber Security Strategies: Training Tool NATO CCD COE (2013): National Cyber Security Strategy Guidelines, section: 1.3
Stocktaking and analysis	ENISA (2016), National Cyber Security Strategies: Training Tool NATO CCD COE (2013): National Cyber Security Strategy Guidelines, sections: 2.1, 2.2, 3.2.1, 3.3.1 NATO CCD COE (2012): National Cyber Security Framework Manual, sections: 3.4, 4
Production of the National Strategy	ENISA (2016), National Cyber Security Strategies: Training Tool
Implementation	ENISA (2016), National Cyber Security Strategies: Training Tool
Monitoring and evaluation	ENISA (2016), National Cyber Security Strategies: Training Tool NATO CCD COE (2013): National Cyber Security Strategy Guidelines, section: 3.9 NATO CCD COE (2012): National Cyber Security Framework Manual, section: 2.4

Overarching principles

Sub-topic	Reference
Vision	Microsoft (2013), Developing a National Cybersecurity Strategy, p.4 NATO CCD COE (2013): National Cyber Security Strategy Guidelines, section: 1.3.1 OECD (2015), Recommendation on Digital Security Risk Management for Economic and Social Prosperity Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index, p.1-3
Comprehensive approach and tailored priorities	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.1, p.14 Microsoft (2013), Developing a National Cybersecurity Strategy, p.5
Inclusiveness	CCI (2013), Checklist p2 CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies 4.5 and 4.6.6 ENISA (2015), Methodologies for the Identification of Critical Information Infrastructure Assets and Services, chapter 3 ENISA (2016), An Evaluation Framework for National Cyber Security Strategies 3.2 ENISA (2016), National Cyber Security Strategies: Setting the Course for National Efforts to Strengthen Security in Cyberspace, p.9 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.1, p.14 ITU (2011), National Cybersecurity Strategy Guide, chapter 5.3 NATO CCD COE (2013): National Cyber Security Strategy Guidelines, section: 1.1.3

Sub-topic	Reference
Inclusiveness (continued)	NATO CCD COE (2012): National Cyber Security Framework Manual, sections: 3.4, 3.5, 4.3 OAS (2015), Cyber Security Awareness Campaign Toolkit, p.20 OAS (2015), Report on Cybersecurity and Critical Infrastructure in the Americas, p.2 OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, p.14-15 OECD (2013), Recommendation of the Council Con-cerning Guidelines for the Protection of Privacy and Transborder flows of Personal Data (Privacy Guidelines); Supplementary Explanatory Memoran-dum to the Revised OECD Privacy Guidelines, p.31 Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index, p.3-6 UNCTAD (2016), Data Protection Regulations and International Data Flows: Implications for Trade and Development UNCTAD (2014), A Framework for Information and Communications Technology Policy Reviews
Economic and social prosperity	Microsoft (2014), Hierarchy of Cybersecurity Needs, chapter 1 NATO CCD COE (2012): National Cyber Security Framework Manual, sections: 1.5.1, 2.2.1 Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index, p.1-3
Fundamental human rights	CCI (2013), Checklist 2.6.5. CTO (2015), Commonwealth Approach for Develop-ing National Cyber Security Strategies, Principle 4 ENISA (2014), An Evaluation Framework for Cyber Security Strategies, 3.1.1 Objectives Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 4.1, p.39

Sub-topic	Reference
Fundamental human rights (continued)	ITU (2011), National Cybersecurity Strategy Guide, chapter 7.4 Microsoft (2013), Developing a National Cybersecurity Strategy, p.5 NATO CCD COE (2013): National Cyber Security Strategy Guidelines, sections: 1.3.1, 1.3.3 NATO CCD COE (2012): National Cyber Security Framework Manual, sections: 1.5.4, 1.5.5, 5.2.6 OECD (2015), Companion Document to the Recommendation on Digital Security Risk Management for Economic and Social Prosperity, principle 9 and principle 3 UNCTAD (2016), Data Protection Regulations and International Data Flows: Implications for Trade and Development United Nations (1948), Universal Declaration of Human Rights United Nations (1976), International Covenant on Economic, Social and Cultural Rights, International Covenant on Civil and Political Rights and Option-al Protocol to the International Covenant on Civil and Political Rights United Nations (2014), The Right to Privacy in the Digital Age
Risk management and resilience	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.3, p.15 Microsoft (2013), Developing a National Cybersecurity Strategy, p.6 Microsoft (2017), Risk Management for Cybersecurity: Security Baselines OECD (2015), Recommendation on Digital Security Risk Management Economic and Social Prosperity and Companion Document

Sub-topic	Reference
Appropriate set of policy instruments	ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies NATO CCD COE (2013): National Cyber Security Strategy Guidelines, section: 3.1 NATO CCD COE (2012): National Cyber Security Framework Manual, section: 1.4
Clear leadership, roles and resource allocation	ENISA (2016), NCSS Good Practice Guide – Designing and Implementing National Cyber Security Strategies NATO CCD COE (2012): National Cyber Security Framework Manual, section: 4 Microsoft (2018):Building an effective national cybersecurity agency Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0 – A Plan for Cyber Readiness: A Baseline and an Index, sections: 1-7
Trust environment	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 2.2, p.25 NATO CCD COE (2013): National Cyber Security Strategy Guidelines, section: 1.3.1 Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, sections: 4, 6

National Cybersecurity Strategy Good Practice

Sub-topic	Reference
Focus area 1 – Governance	CCI (2013), Checklist.
	CTO (2015), 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
	ENISA (2016), 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
	ENISA (2016), An Evaluation Framework for National Cyber Security Strategies, sections: 2.2.1, 3.1.1, 3.1.2, 3.1.3
	ENISA (2016), National Cyber Security Strategies: Setting the course for National Efforts to Strengthen Security in Cyberspace, sections: 4, 6
	Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.1, 1.5, 1.6, p.14-15
	ITU (2011): National Cybersecurity Strategy Guide, sections: 5.2.1, 5.3, 7.2, 7.3, 11.1, 11.2, 20, 20.2
	Microsoft (2013), Developing a National Cybersecurity Strategy, sections: A Principled Approach to Cybersecurity, Establishing Clear Priorities and Security Baseline
	Microsoft (2018) Building an effective national cybersecurity agency
	NATO CCD COE (2013), National Cyber Security Strategy Guidelines, sections: 1.1, 3.3, 3.8
	NATO CCD COE (2012), 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
	OECD (2012), Cybersecurity Policy Making at a Turning Point, Annex IV
	OECD (2013), Recommendation of the Council Concerning Guidelines for the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines)
	OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2-A, Companion Document

Sub-topic	Reference
Focus area 1 – Governance (continued)	OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, 2-A, Companion Document OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, section 1
Focus area 2 - Risk management in National Cybersecurity	CTO (2015), 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 ENISA (2016), National Cyber Security Strategy Good Practice Guide – Designing and Implementing National Cyber Security Strategies, section: 3.3 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.3, p.14 ITU (2011), National Cybersecurity Strategy Guide, section 10.1.2 Microsoft (2017), Risk Management for Cybersecurity: Security Baselines Microsoft (2013), Developing a National Cybersecurity Strategy, chapter on Building a Risk Approach NATO CCD COE (2013), National Cyber Security Strategy Guidelines, section: 3.5 NATO CCD COE (2012): National Cyber Security Framework Manual, sections: 2.1.2, 5.3.2 NIST (2015), Framework for Improving Critical Infrastructure Cybersecurity OAS (2018), Managing National Cyber Risk OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, section: 1

Sub-topic	Reference
Focus area 3 – Preparedness and resilience	Carnegie Mellon (2003), Handbook for Computer Security Incident Response Teams (CSIRTs) CCI (2013), Checklist CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, section: 4.4.3, 4.4.20, 4.4.21, 4.4.22, 4.4.27, 4.4.31 ENISA (2016), 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 ENISA (2016), Strategies for Incident Response and Cyber Crisis Cooperation, p ENISA (2011), CERT Operational Gaps and Overlaps, p. ENISA (2011), Good Practice Guide for Incident Management, p. Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.2, p.14 ITU (2011), National Cybersecurity Strategy Guide: 11.3, 17.3 Microsoft (2017), Risk Management for Cybersecurity: Security Baselines Microsoft (2015), Information Sharing Framework for Cybersecurity Microsoft (2013), Developing a National Strategy for Cybersecurity, section: Building Incident Response Capabilities NATO CCD COE (2013): National Cyber Security Strategy Guidelines, Section: 3.5 NATO CCD COE (2012): National Cyber Security Framework Manual, sections: 3.2, 4.2.2 OAS (2016), Best Practice for Establishing a National CSIRT, p.35 OAS (2004), Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity, pp.3-4

Sub-topic	Reference
Focus area 3 – Preparedness and resilience (continued)	OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, section: 2-B Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, sections: 2, 4
Focus area 4 - Critical infrastructure services/essential services	CTO (2015), 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 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.3, 1.4, p.14; Dimension 5.2, p.49 ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, section: 3.6 ENISA (2015), Methodologies for the Identification of Critical Information Infrastructure Assets and Services ENISA (2016), An Evaluation Framework for National Cyber Security Strategies, section: 4.2 ITU (2011), National Cybersecurity Strategy Guide, sections: 5.1.1, 5.3.3, 11.4 Microsoft (2017), Risk Management for Cybersecurity: Security Baselines Microsoft (2014), Critical Infrastructure Protection: Concepts and Continuum, all sections Microsoft (2014), Critical Connections: Protecting Infrastructures, all sections NATO CCD COE (2013): National Cyber Security Strategy Guidelines, sections: 3.4, 3.5 NATO CCD COE (2012), National Cyber Security Framework Manual, section: 4.5.4 OAS (2015), Report Cybersecurity and Critical Infrastructure in the Americas OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity

Sub-topic	Reference
Focus area 4 - Critical infrastructure services/essential services (continued)	OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures: Part I, Part II Potomac Institute for Policy Studies (2015): Cyber Readiness Index 2.0, sections: 2, 4
Focus area 5 – Capability and capacity building and awareness raising	CCI (2013), Checklist; CCI (2005, 2017), Commonwealth Network of Contact Persons Framework; CCI (2011), Harare Scheme on Mutual Legal Assistance in Criminal Matters; CTO (2015), 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 ENISA (2016), 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 ENISA (2016), Strategies for Incident Response and Cyber Crisis Cooperation, section: 2.1 ENISA (2011), CERT Operational Gaps and Overlaps, p.6, 16, 19, 21, 27, 29, 31, 32, 50, 57 ENISA (2010), Good Practice Guide for Incident Management, p.19, 23, 26, 32, 46, 56, 58, 64, 69 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 1.5, p.15; Dimension 2.1, 2.2., 2.3, p.25; Dimension 3-1, 3-2, 3-3, p. 32; Dimension 5.6, p.49 ITU (2011), National Cybersecurity Strategy Guide, sections: 5.3.7, 5.3.8, 12.4, 12.1, 12.3, 18 Microsoft (2013), Developing a National Strategy for Cybersecurity, section: Driving Research and Technology Investment, Public Awareness, Workforce Training and Education; NATO CCD COE (2013, National Cyber Security Strategy Guidelines, section: 3.5

Sub-topic	Reference
Focus area 5 – Capability and capacity building and awareness raising (continued)	NATO CCD COE (2012), National Cyber Security Strategy Framework Manual, sections: 4.5.5, 4.6.3; OAS (2015), Cyber Security Awareness Campaign Toolkit, all sections; OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, section: 2-B Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, sections: 2, 5 UNCTAD (2015), Prgramme on E-Commerce and Law Reform
Focus area 6 – Legislation and regulation	CCI (2013), Checklist CTO (2015), 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 Council of Europe (2001), Budapest Convention on Cybercrime, article 15 ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.15, 3.184.9, 4.12 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 4.1, 4.2, 4.3, p.39-40; Dimension 5.7, p.50 UNHR (1976), International Covenant on Civil and Political Rights, article 19 ITU (2011), National Cybersecurity Strategy Guide, sections: 5.3.4, 5.3.5, 9, 11.5, 12.2, 15 ITU (2010), ITU Toolkit for Cybercrime Legislation NATO CCD COE (2013), National Cyber Security Strategy Guidelines, section: 3.2 NATO CCD COE (2012), National Cyber Security Strategy Framework Manual, section: 5 OAS: Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, section: 3

Sub-topic	Reference
Focus area 6 – Legislation and regulation (continued)	UN (2015), Sustainable Development Goals, article 16.3 UNCTAD, Global Cyberlaw Tracker World Bank et al., Combatting Cybercrime: Tools and Capacity Building for Emerging Economies
Focus area 7 – International cooperation	CTO (2015), Commonwealth Approach for Developing National Cyber Security Strategies, sections: 4.4.20, 4.4.21 ENISA (2016), National Cyber Security Strategies Good Practice Guide – Designing and Implementing National Cyber Security Strategies, sections: 3.16 and 4.10 ENISA (2016), Guidebook on National Cyber Security Strategies, section: 3.16 Global Cyber Security Capacity Centre, University of Oxford (2016), Cybersecurity Capacity Maturity Model for Nations (CMM), Dimension 4.3, p.40 ITU (2011), National Cybersecurity Strategy Guide, sections: 5.3.9, 10.2.2, 13, 19 Microsoft (2013), Developing a National Strategy for Cybersecurity, section on structuring international engagement NATO CCD COE (2013), National Cyber Security Strategy Guidelines, sections: 1.3, 3.2.1, 3.3.2 NATO CCD COE (2012), National Cyber Security Strategy Framework Manual, sections: 4.7, 5.4.2, 5.4.3 OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures, chapters: 4, 5 OECD (2015), Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, p. 13, 48, 58 Potomac Institute for Policy Studies (2015), Cyber Readiness Index 2.0, sections: 4, 6

7 Acronyms

Acronym	Definition
CCI	Commonwealth Cybercrime Initiative
CERT	Computer Emergency Response Team
CBM	Confidence Building Measures
CII	Critical Information Infrastructure
CTO	Commonwealth Telecommunications Organisation
ENISA	European Union Agency for Network and Information Security
ICT	Information & Communication Technology
ITU	International Telecommunication Union
NATO CCD COE	NATO Cooperative Cyber Defence Centre of Excellence
NIST	National Institute of Standards and Technology
OAS	Organization of American States
OECD	Organization for Economic Co-operation and Development
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development