CYBER4Dev

NATIONAL **CYBERSECURITY** STRATEGY TOOLKIT

NI·CO

Republic of Estonia
Information System Authority

Foreign, Commonwealth & Development Office

Ministry of Foreign Affairs of the Netherlands

Funded by the European Union

This document was produced with the financial assistance of the European Union. The view expressed herein can in no way be taken to reflect the official opinion of the European Union

Designed by **HUMAN Design Studios**

Kadri Kaska

Liis Rebane

Kadri Kaska is a Senior Cybersecurity Expert at the e-Governance Academy (eGA), with her main areas of expertise in national cybersecurity strategy and governance frameworks, and domestic and international law. Prior to joining the eGA in 2022, she served for over a decade at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) as a cybersecurity legal and policy researcher and Head of the Law Branch. During her time there, she was seconded to the Estonian Information System Authority, where she contributed to the agency's activities in cyber threat assessment, policy analysis and legal drafting. Kadri has been the lead author and editor of annual Estonian Cybersecurity Assessments, one of the authors of Estonia's Cybersecurity Act and the 2018 Cybersecurity Strategy, and has worked with several international and regional organisations in cybersecurity capacity building. Kadri holds a master's degree in law from the University of Tartu and is currently pursuing studies in behavioral science at the same university.

Liis Rebane is an IT and information security professional with more than four years of hands-on experience in IT and security Risk Management and Risk Control in financial sector. Prior to that, she served as the National Cyber Policy Coordinator for Estonia, being responsible for the National Cybersecurity Strategy planning and execution, as well as contributing to the adoption of the NIS directive . During recent years, Liis has worked with several countries both in developing national cybersecurity strategies, conducting cybersecurity assessments, and providing trainings and workshops. Liis holds a PhD degree in physics with more than 10 years of experience in academic research and application of quantitative methods.

Table of Contents

Overview

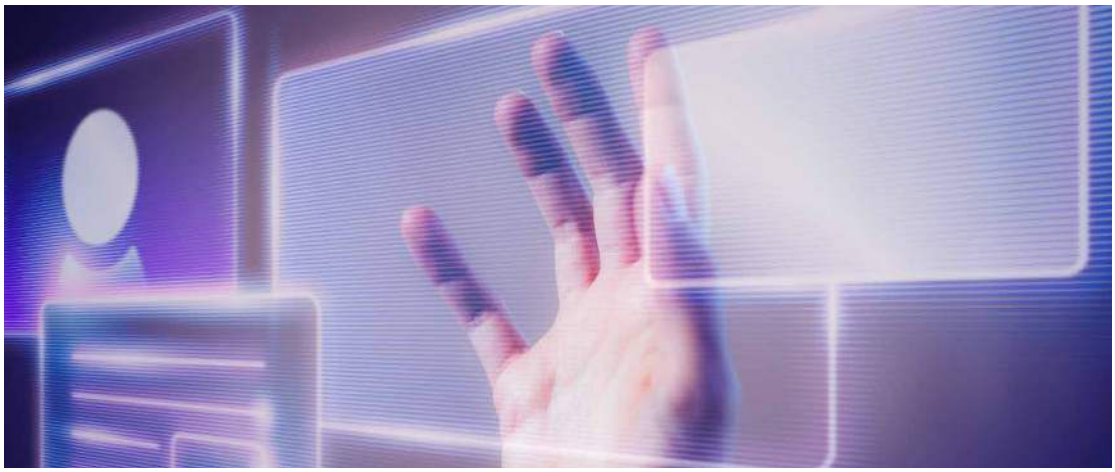
The purpose of this Toolkit is to offer a concise, practical guide for creating or updating a National Cybersecurity Strategy (NCS). It aims to assist national authorities in executing the NCS process by incorporating practical lessons, success factors, and common pitfalls to ensure the timely delivery of a comprehensive, tailored NCS document, with robust governance and broad stakeholder engagement.

Drawing from the authors' experience in the Cyber4Dev project implementation, as well as their roles in national authorities and as consultants supporting NCS processes in a number of countries, the Toolkit provides practical, real-world guidance for NCS development. It does not replace academic and policy literature offering comprehensive guidance on NCS theory, but presents an honest approach based on the authors' experiences, focusing on a pragmatic NCS process that, while striving for the ideal, has proven effective in practice.

The Toolkit comprises two main parts:

1. Part I, the **NCS Process,** outlines the essential practical steps and considerations for developing a new NCS.
2. Part II, **NCS Subject Areas,** presents a collection of NCS 'building blocks' to consider when developing an NCS, with a focus on baseline cybersecurity and resilience.

The Toolkit concludes with general tips and observations based on the authors' experiences, accompanied by a curated list of international best-practice NCS Guidelines and Tools, which are considered valuable and practical resources for detailed guidance and insight into both overall NCS setup and specific strategic areas.



How to use this document

Users of the Toolkit are recommended to follow the stages outlined in the NCS Process, referring to the NCS Subject Areas for objective-setting, prioritisation, and mapping stakeholder needs and commitments.

Chapter 1, the NCS Process, identifies six essential stages for a successful NCS design:

1. Establish NCS process ownership: Designate a lead agency and advisory board to govern the NCS.
2. Create a NCS Project Plan: Develop a timeline with clear milestones, deliverables, and responsibilities.
3. Assess the strategic context: Evaluate the threat landscape, determine current maturity, and conduct a SWOT analysis.
4. Identify vision and guiding principles.
5. Develop strategic objectives and lines of action.
6. Identify and engage stakeholders: Engage government and private sector stakeholders and establish a clear approach for stakeholder involvement during the drafting, validation, and finalisation phases.
7. **Outlook for next steps: NCS action plan and implementation.**

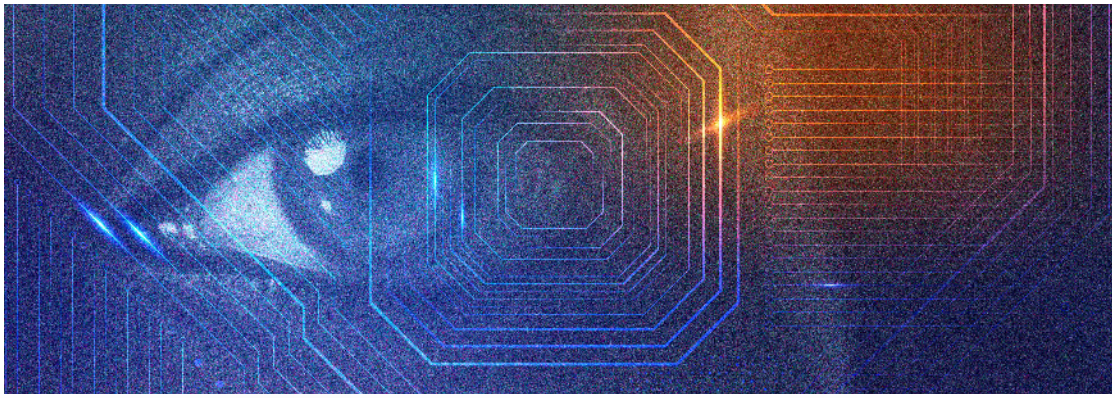
These stages form an interconnected sequence for the foundation of the NCS document and process. However, the stages should be iteratively revisited as stakeholder involvement increases, comprehension deepens, and strategic vision becomes clear.

Chapter 2, the **NCS Subject Areas**, outlines key "building blocks" for shaping the NCS content and structure, encompassing cybersecurity governance, risk management, incident management capacities, and cybersecurity awareness and skills. The NCS focus and structure will differ country by country, depending on national needs, priorities, and maturity. Nonetheless, common practices can guide the initial process. The Toolkit's distinction between baselines and advanced capacities helps to set realistic priorities and maintain a manageable scope.

NCS Process

Establishing NCS process ownership

The first step for a successful NCS process involves assigning both personal and institutional ownership and establishing a dedicated oversight and advisory board as a mechanism to connect to the necessary stakeholders. Below is a detailed guide for executing this step, including the purpose, role and tasks, resource considerations, and recommendations.



An NCS Process should start with appointing a competent organisation and individual responsible for the NCS process, ideally at the government level. The NCS owner is responsible for developing a project plan and leading the execution of the strategy development process. Both the organisation and the individual should have adequate subject matter competence, mandate, and resources to complete the process successfully.

In practice, the optimal choice for this role tends to be the organisation responsible for the country's cybersecurity or digitalisation agenda – the area holding this responsibility varies widely country-by country, ranging from the economy or education, to military defence or internal security. While there are both more and less successful examples across the whole spectrum, it is relevant that the responsible organisation is capable for broad engagement of stakeholders and understands the value of open information sharing and communication – this might pose a need for additional conscious effort if the NCS responsibility is assigned to an organisation with military or internal security culture. An NCS with substantial content needs to be a public document in order to establish the necessary level of engagement across the society. A more detailed non-public or classified complementary appendix may be established to cover more sensitive content, if a necessity for this is identified. Finally, it is important that the organisation with NCS ownership needs to have an authority to hold other organisations (at least in the government sector) accountable for their actions in the area. If such authority is lacking, a higher-level entity, such as the ministry for ICT, should assume process ownership. Whilst this organisation will have responsibility for producing the NCS, it is essential they engage a broad range of government and non-government stakeholders at each stage of the process.

External consultancy may be beneficial to provide support to the organisation responsible for the NCS process. However, it is important to keep in mind that the ownership itself cannot be outsourced. Assistance from experienced penholders, facilitators, and advisors can be invaluable, especially for countries at the early stages of a mature NCS journey. They can provide additional experience and capacity, but the ultimate responsibility remains with the designated organisation.

Then, establish an oversight and advisory board for strategy development to ensure engagement and appropriate input from organisations within their governance areas. The board should comprise representatives from all subject matter areas of the strategy, with members possessing both subject matter competence and a mandate to represent their organisations' needs and priorities. In addition to comprehensive representation of government organisation, it adds value to consider representation of private sector, NGOs, and academia to ensure direct multi-stakeholder engagement. Alternatively the input from non-government stakeholders can be incorporated via workshops, interviews, and feedback rounds.

The advisory board acts as the primary sounding board for major decisions regarding the strategy. It should be regularly updated about the work status, needs, and outcomes. Importantly, all members of this board are expected to engage organisations, including private sector, civil society, and academia within their governance areas to provide necessary input and feedback to the strategy.

Creating a NCS Project plan

Once ownership of the process has been established, the first essential step for the process owner is to draft a project plan for the strategy development process and coordinate it with the advisory board. A formal approval by the board may be beneficial, depending on the country's administrative tradition and culture, but is not essential. However, the project plan should at least have their support, adequately considering their needs and securing their commitment to deliver. Otherwise, there is a risk they are caught by surprise and fail to sufficiently commit to the process.

An NCS should have a specified duration, after which a review and development of the new NCS should be initiated. Even the best-crafted strategy will be affected by developments in the external threat and risk landscape, new technologies, geopolitical changes, and other factors. Between five to eight years is a reasonable timeline for a strategy; enough time to set strategic direction, but not too long for it to become redundant.

The project plan might consider the elements listed in the example project plan provided below. The tasks will be further detailed in subsequent sections of the document.

Note that the indicative timeline proposed in the table should be assumed as the minimum possible: it is informed by real-life practice but reflects the process in close-to-ideal circumstances (committed team, small number of stakeholders, and effective communication). Depending on the scope of organisations involved and complexity of the situation, the process might take considerably longer.

Task	Responsibility	Deliverable(s)	Timeline
Project initiation			
Establishing the project owner and lead		Project owner and lead appointed	Month 1
Project validation with Advisory Board	Project owner/lead	Project kick-off meeting	Month 1
	Advisory Board members	POCs assigned from the Advisory Board organisations	Month 1
Initial assessment (report and structure)	Project owner/lead	Assessment delivered and introduced to Advisory Board	Months 1-2
Stakeholder engagement			
Kick-off workshop with stakeholders	Project owner/lead (external support recommended for facilitation and documentation)	Kick-off workshop with stakeholders: establish stakeholder commitment for the NCS process and timeline, and documentation of initial feedback	Month 2
Stakeholder interviews/ consultations	Project owner with team members or external support	Documented input to strategy process from all primary stakeholder groups.	Months 2-3
Draft strategy			
First draft of the strategy and consultation with advisory board (1-2 cycles)	Drafting by project owner (external support may be considered for supportive penholder in drafting process) Stakeholder engagement supported by Advisory Board members	Initial draft-strategy, incorporating input from stakeholder consultations. 3-week review period for national stakeholders, resulting in comprehensive round of initial feedback and input.	Month 3

Task	Responsibility	Deliverable(s)	Timeline
Incorporate feedback into the draft strategy.	Project owner	Second draft of the strategy	Month 4
Consultation			
Validation workshop with stakeholders	Project owner (external support recommended for facilitation)	Common review and alignment with core stakeholders	Month 4
National review period	Project owner with the support of advisory board	Validation and written feedback to the strategy by all relevant national stakeholders (provide about 1 month)	
Review and alignment	Project owner (possibly with external support)	Conclude final draft	Month 5
Finalisation			
Finalisation and approval	Project owner with the support of advisory board	Final alignment of the draft among core stakeholders. Initiate national adoption process	Month 6
Presentation for adoption	Project owner	Presentation of the final NCS	Month 7

Assessment of the strategic context

Improving national cyber resilience requires understanding the current state and strategic perspective of cybersecurity, encompassing external (cyber threat landscape) and internal (national capacity) factors. A SWOT analysis, consultations with stakeholders, and reference to international best practices can guide this. However, to be successful as a means to deliver change, a strategy must consider the national context. A 'one-size-fits-all' approach which does not account for factors specific to your country will not be as effective.

The national context is determined by several things, not all of which directly relate to cybersecurity:

- What is the existing administrative structure, tradition, constitutional boundaries? Where would cybersecurity responsibility most naturally fall? How is decision-making authority assigned and at what level?
- What is the predominant decision-making culture in the country? The balance point between subordination and collaboration may vary widely between countries. In a top-down culture, policy initiatives may be required to improve public-private cooperation horizontally, for example.
- What are the national objectives related to digitalisation? What are the objectives in other areas that the cyber strategy will connect to - law enforcement, economic development, national defence, foreign affairs?

Cybersecurity SWOT analysis

The purpose of this exercise is to identify existing opportunities and challenges that inform the strategy process. The analysis does not necessarily become a part of the strategy document, but stocktaking is crucial to determine where the country stands and inform the definition of where it would like to go.

- **Opportunities:** Benefits that the country expects from digital transformation and cybersecurity; recent dynamics highlighting pressing issues and trends (e.g., COVID-induced work pattern changes).
- **Threats:** Regional and national cyber threat picture, key threat actors, significant recent incidents; general and specific ICT dependency (e.g., overreliance on single providers, legacy or untrusted technology); high-risk sectors due to their societal and economic significance where service disruption would bring severe or large-scale consequences.
- **Strengths:** Existing structures, organisations, mandates, legislation, supply of/access to talent.
- **Weaknesses:** Organisational capacities and resources; cybersecurity awareness among target groups and general population; level of involvement in international cooperation.

Identification of vision and guiding principle

A consistent vision and fundamental principles support long-term strategic alignment: they are anchor points to help guide both where (vision) and how (values) the country would like to move. For the vision and guiding principles to serve this aim, they should be: a) organic to the country's context and stakeholders, b) easy to remember, and c) offer inspiration and clarity when navigating between decisions.

Developing a vision and guiding principles are as much a part of the NCS process as the definition of strategic objectives and agreeing on lines of action. They should be designed in collaboration and consultation with stakeholders. We suggest using the NCS vision and principles to link cybersecurity into the broader national value system (e.g., inclusivity, openness, competitiveness, trust and reliability) and avoid too vague, lengthy or implausible vision statements.[1]

While international references offer guiding principles for the NCS process,[2] the following have had most traction in our project experience:

- **Cybersecurity is a whole-of-society matter and an integral element of public security,** with joint and shared responsibilities of public and private partners.
- **Leadership and collaboration:** actively involving stakeholders in improving conditions in cyberspace; committing to active participation in regional and international cooperation.
- **Safeguarding and promoting human rights and fundamental freedoms** online as well as offline, such as privacy, freedom of expression, and free movement of information.
- **Values-driven approach:** adhering to fundamental societal values: democracy, rule of law, transparency and public trust when designing cybersecurity measures; using appropriate policy instruments that are adequate, effective, and proportionate; encouraging (gender and other) diversity to benefit from full talent potential.
- **Treating cybersecurity as an enabler and amplifier of digital development and socioeconomic prosperity,** supporting innovation, competitiveness, sustainable development, and social inclusiveness.
- **Risk-based approach,** recognising that absolute security is not achievable and promoting resilience that avoids cyber risks from having significant adverse effects on the society and economy.

Definition of strategic objectives and lines of action

Defining the strategic objectives and respective lines of action for reaching those constitutes the core of the NCS document and process that defines the envisioned scope and prioritisation of efforts during the strategy period. The explicit guidance for building up the content and draft subject areas to frame objectives and lines of action

1 For recommendations concerning a vision for the NCS, see https://ncsguide.org/the-guide/principles/. For recommendations on the hallmarks of a good vision, see https://www.sitra.fi/en/blogs/seven-tips-for-vision-creators/

2 https://ncsguide.org/the-guide/principles/.

is detailed under "NCS subject areas" section.

The largest challenges for successful choice and design of a set of strategic objectives along with actions that are necessary to fulfil them is universal in nature, irrespective of the country or sector:

- **Concluding mismatched strategic objectives and lines of action** such that completing the actions fails to deliver the envisioned strategic value.
- **Strategy process being disconnected from resource planning** – this challenge is intensified for countries with a decentralised national cybersecurity governance model.
- **Insufficient connection and integration between NCS and other national strategic planning documents** – this can lead to stand-alone efforts in cybersecurity domain, which are not supported by wider development efforts and national priorities, leading to weak results and insufficient engagement at national level. With cybersecurity becoming an integral part of all fields of governance and policy planning at national level, the need for close integration only intensifies in time.
- **Failure to acknowledge always present limitations set by available human and financial resources.** The challenge is intensified by the observation that an NCS planning process tends to always start with a strong initial intuition that everything is important and the step of taking a difficult discussion what *not* to do and prioritise during the next strategy period may be skipped, leading to vague strategy and arbitrary prioritisation.

Failure to overcome these challenges during NCS design phase – in particular ensuring sufficient prioritisation, realistic resource allocation, and securing stakeholder buy-in – may limit the relevance of the NCS.

Stakeholder engagement and consultations

To ensure that the NCS is relevant in substance and establishes ownership and accountability, close consultation with a broad range of stakeholders is crucial. Such engagements help to collect informed input to the draft strategy, its planned priorities and actions, verify its calibration and relevance during feedback rounds, and help secure broad-based legitimacy and commitment from stakeholders, which is essential for the subsequent execution of strategic initiatives.

The typical core stakeholder list might include:

- Government digital policy and cybersecurity leads
- Other government ministries (including those with less obvious or less direct cybersecurity roles such as Justice, Education, Finance, Business, Defence, or Foreign Affairs)
- Public agencies with digitalisation and cybersecurity responsibilities; sectoral regulators; law enforcement, national security and defence authorities; key ICT-dependent service providers in the government and public sector
- Private sector entities: telecoms and internet service providers, other critical national infrastructure entities and industry organisations
- Educational and research institutions
- Civil society representatives and NGOs promoting IT literacy
- Individual ICT and cyber experts

Additionally, international and regional organisations and consultants may be engaged for ensuring alignment with general best practices and trends.

The following guiding principles have proven helpful for planning stakeholder consultations:

- Engage based on necessary functions, not just institutions.
- Ideally, strive to have high-level representatives, who are knowledgeable about substantive issues in their area
- Balance formal representation with decision-makers and experts passionate about the subject and able to drive change.
- Include visionaries from government, private sector, and academia.
- Distinguish between stakeholders and spectators: while broad feedback is beneficial, not all opinions carry the same weight.

Importantly, ensure that engagement is genuine: allow for sufficient time to provide input and feedback, and demonstrate that it is being considered. Be transparent and provide justification if proposals are not accepted. Failure to engage stakeholders with respect and transparency may lead to loss of credibility over time.

We advise several rounds of stakeholder consultations to be carried out, utilising both in-person and online meeting and workshop formats. Experience says that it is best to aim for a medium-size group (10-20 participants) per consultation event. Ideal participants are those who are high-level enough to represent their agencies' position, but at the same time hands-on enough to be knowledgeable about substantive issues.

The final draft of the NCS should be subjected to national consultation for review and feedback. Expect the final national consultation to bring substantial feedback: the NCS process owner, supported by internal or external resources, should prepare to review numerous comments. A coordination table can be helpful to keep track of all feedback and provide assurance to all stakeholders, indicating reasons for omitting any comments from the final strategy. Often, there might be feedback that is too detailed for the strategy document but provides valuable input for subsequent development of the action plan for strategy implementation.

Next steps: NCS Action Plan and Implementation

Once NCS strategy document is concluded, a full NCS lifecycle needs to be established and followed, comprising four phases, as detailed in Figure below:

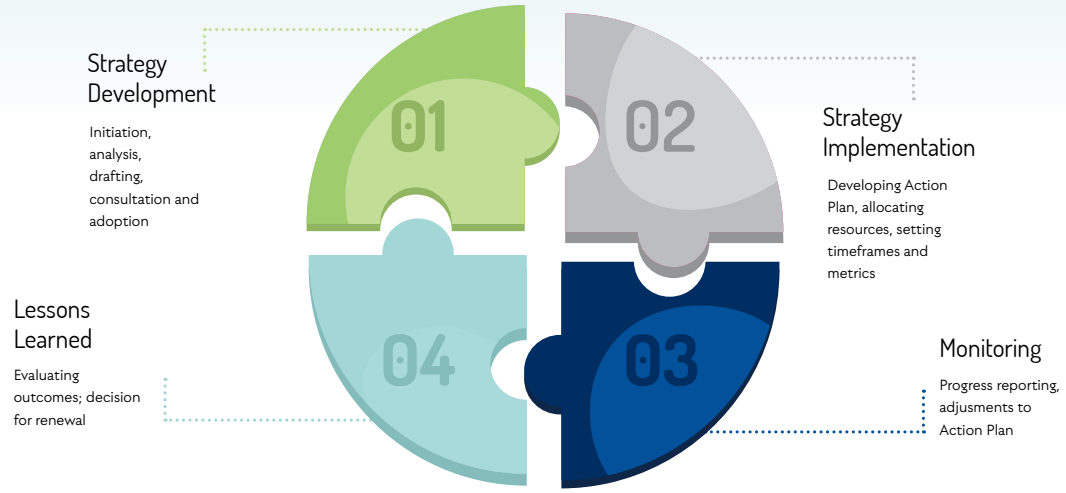
- Strategy development
- Strategy implementation
- Monitoring
- Post-implementation review and lessons learned.

Current Toolkit focuses on strategy development phase, while detailed guidance on concluding the implementation plan, monitoring, and post-implementation review remain out of scope of this guidance.

Brief summary of the stages following the NCS development:

After concluding the NCS, a complementing Action Plan needs to be developed. Strategies are worthless unless they are acted upon, so the Action Plan is there to ensure tasks are completed on time and the NCS is implemented effectively. An Action Plan should contain specific tasks, clarify owners and contributors, establish deadlines and performance metrics for the responsible entities, and outline a roadmap for the strategic tasks outlined in the NCS. Successful implementation of an Action Plan also requires a reporting structure to follow up on the implementation of the Action Plan, on the progress achieved and any obstacles. Such reporting provides guidance for necessary adjustments to the Strategy implementation, based on the evolving threat and risk landscape and taking into account relevant administrative or other changes and alignment with other strategic areas.

A post-implementation review and lessons learned exercise should be scheduled after completion of the strategy period. This will review the progress against the strategy's objectives, identify any gaps, and draw valuable conclusions for design and implementation of the next strategy. This review process should ideally involve some independent scrutiny. This can be individuals from inside or outside of government, but to ensure impartiality they should not have been directly involved in implementation of the strategy.



NCS subject areas

This part of the Toolkit provides a sample checklist of topics and measures to consider for developing the NCS objectives and lines of action, based on the Cyber4Dev project experience.

The NCS aims to bring about a consistent improvement in national cybersecurity capacity by addressing both cross-cutting and sector-specific issues. To help organise the NCS development, this Toolkit adopts a baseline-oriented approach, focusing on fundamental national capacities that precede more advanced objectives and maturity.[3] Such a baseline approach is in no way intended to limit the inclusion of further focus areas, and various international references linked at the end of this document provide helpful resources and insight for that.

We have structured the fundamental NCS objectives and lines of action around horizontal (cross-cutting) and vertical (sector-oriented) blocks. This approach helps to develop and synchronise the NCS contents and ensure that objectives remain manageable and consistent. These basic blocks include:

1. Cybersecurity governance framework
2. Cyber risk management framework
3. National cyber incident management
4. Cybersecurity awareness and education

The depth and ambition of the objectives within each block should align with national needs, priorities, and maturity, as well as resource availability. Blocks can thus be rearranged and further areas included as per national circumstances. Still, for manageability, we recommend limiting the NCS to a few (up to 5) areas with 3-5 objectives each, totalling no more than 12-15 objectives for the strategy period.

When substantiating each of these blocks with objectives and lines of action through the NCS process and document, we have used a three-step approach:

3 These align with the European Union baselines for national cybersecurity as laid out in the Directive on Network and Information Security (NIS Directive). Recognising the relevance of advanced capacities to future-proofing the national digital ecosystem, such as investing in research and development to advance cybersecurity technologies and techniques; facilitating cybersecurity industry, and developing capacity to participate in international norms-building, these will not be elaborated further in this document.

1. **Presenting the context:** This includes a brief description of the current environment relevant to the particular area. It highlights key national and international trends, existing organisational mechanisms, legal/normative frameworks, and main perceived challenges based on the strategic assessment.

2. **Defining a clear problem statement:** This involves articulating specific challenges and opportunities, which provide a common understanding of the question, "what problem are we solving?". The identified problems should be directly addressed by the Objectives and Lines of Action. This ensures that all major issues are linked to a planned action, and no activities are pursued without a clear underlying justification.

3. **Outlining strategic objectives:** This step includes the main lines of action and priority activities, reflecting achievable ambitions and commitments by the end of the strategy period.

The structure of an NCS's most basic building blocks is illustrated in the Table below.

CYBERSECURITY GOVERNANCE	
Cybersecurity governance framework Stakeholder cooperation mechanisms Legal framework International cooperation	
CYBER RISK MANAGEMENT	**NATIONAL CYBER INCIDENT MANAGEMENT AND FIGHT AGAINST CYBERCRIME**
Identifying critical national cyber-dependent functions and operators Cyber risk assessment and resilience framework Crisis preparedness at entity/operator and national levels	National capacities for cyber incident prevention and response Threat assessment and situational awareness Combatting cybercrime
CYBERSECURITY EDUCATION AND AWARENESS	
Enhance cybersecurity awareness Cybersecurity at all levels of education Skilled cybersecurity workforce	

The following sections provide a short and consolidated outline of aspects considered by Cyber4Dev during NCS consulting projects, which can serve as a starting point for NCS development.

Cybersecurity governance

In establishing or refining the national cybersecurity governance framework, there are certain core aspects that should be considered: establishing or strengthening national competent authorities for cybersecurity; allocating clear roles and responsibilities for cybersecurity across government and other stakeholders; ensuring adequate mandates for oversight and accountability; and setting up frameworks and fora for effective coordination and collaboration. Depending on the national needs, state of maturity, and ambition, different policy tools may be needed, so oftentimes a broad legislative review might also be appropriate to address under this block.

Cybersecurity governance framework

- Assign high-level executive responsibility for cybersecurity.
- Designate and resource competent national authority(/ies) for cybersecurity.
- Form an intragovernmental strategic coordination or decision-making body.
- Define roles and responsibilities for other government actors in cybersecurity.
- Establish oversight for NCS implementation and implement regular monitoring and reporting mechanisms for cybersecurity indicators.

Stakeholder cooperation

- Develop a public-private partnership mechanism involving relevant stakeholders.
- Create participation platforms for policy consultation, activity coordination, and operational cooperation.

Legal framework

- Conduct an assessment of the current legal framework; identify and implement legislative changes required for NCS objectives.
- Define national cybersecurity functions and responsibilities in the legal and regulatory framework.

International cooperation

- Identify key international and regional cyber diplomacy platforms; establish a plan to build capacity to participate and represent the nation in these platforms.
- Identify regional and international cybersecurity policy, information sharing, and operational cooperation formats and plan for connecting to them.

Cyber risk management framework

The national strategic approach to manage cyber risks should at the minimum encompass all functions that are critical to the functioning of the state and society. This block includes actions related to assessing cybersecurity risks, identifying digital-dependent assets determining the functioning of both state powers and critical private sector services, and implementing appropriate security controls to mitigate those risks, as well as integration with crisis planning. Again, legislative changes might need to be planned and implemented to properly enforce risk management activities.

Identifying critical cyber-dependent functions and operators

- Develop criteria and a legal framework to identify critical information infrastructure (CII) operators and create a comprehensive catalogue of all CII operators, maintained and updated regularly.
- Establish a common cybersecurity standard mandatory for government institutions and CII operators, following a risk-based approach and prioritising continuity of essential services.

Cyber risk assessment and resilience framework

- Establish national reference standards, guidelines, and auditing strategies to support the implementation of cybersecurity measures by CII operators and to hold them accountable for compliance. Prioritise measures and investments based on the national risk profile.
- Promote continuous risk monitoring at the national level and encourage the adoption of cybersecurity best practices among government and private sector entities.
- Set up a mechanism for periodic vulnerability disclosure and information exchange between critical information infrastructure (CII) operators and competent cybersecurity authorities.
- Establish a systematic practice of identifying and developing cyber risk scenarios at the operator and national level that can provide input to crisis planning, stress-testing and exercise-design, and business continuity management efforts.

National cyber incident management and fight against cybercrime

The core components addressed in this NCS building block are a functional national-level incident prevention and response capacity across the whole spectrum of cyber threats, considering also law enforcement capabilities to better fight cybercrime. In a typical NCS, incident response and law enforcement will likely be addressed in different chapters, but both share several similarities: the need to invest into both preventive and reactive capacities, the need for a clear and adequate legal basis for the execution of state powers, and a strong and fundamentally important international cooperation dimension. This outline might also be useful for considering in the context of developing national cyber defence capacities, i.e. to prevent and respond to cyber threats relevant to national security and defence.

National capacities for cyber incident prevention and response

- Establish a Computer Security Incident Response Team/Computer Emergency Response Team (CSIRT/CERT) with a national responsibility to manage cybersecurity threats and incidents. Establish its role as the main point of contact for reporting cyber incidents.
- Establish a portfolio of CSIRT/CERT's fundamental services, both proactive and reactive, for cyber incident prevention and response.
- Set up CSIRT's/CERT's trusted and secure communication channels for communication and cooperation, as well as policies for information handling. Establish, encourage and safeguard the practice of information sharing on vulnerabilities, threats and incidents.
- Develop criteria to assess cyber incidents based on their impact on critical assets, services, and population.

Crisis preparedness

- Develop crisis management plans for government institutions and the private sector to handle cyber crises. Organise national cybersecurity exercises to test the effectiveness of these plans.
- Develop a national contingency plan to prepare for large-scale cyber incidents or threats, defining escalation criteria, emergency management roles, and communication plans.
- Regularly test the cyber contingency plan through operational-level exercises to refine crisis management processes and decision-making.

Threat assessment and situational awareness

- Regularly assess threat and risk landscape to inform risk-based decision-making and establish cybersecurity awareness and training activities.
- Develop a knowledge management system for capturing lessons from incidents and responses, respecting business confidentiality.

Combatting cybercrime

- Adopt a legal framework to define cybercrime in harmony with international instruments.
- Establish legal mandates and authority for law enforcement, executive authorities, and digital service providers in cybercrime prevention; define law enforcement and prosecution powers for cybercrime investigation, including electronic evidence collection and international cooperation mechanisms.
- Strengthen judicial and law enforcement capacities with necessary resources for effective cybercrime investigation, including appropriate digital forensic capabilities, standard operating procedures, and publicised crime reporting mechanisms.
- Provide training to criminal justice professionals on cybercrime, technology tools, and electronic evidence management.

Cybersecurity awareness and education

The final fundamental NCS building block focuses on establishing a comprehensive approach to cybersecurity awareness and education to ensure that all stakeholders, including government employees, contractors, and the public have an adequate understanding of cyber risks and have the capability, opportunities and motivation for secure behaviour.

Enhance cybersecurity awareness

- Create a coordinated national programme of awareness and culture on cybersecurity, including a coordinating body for implementation and management. Allocate resources for the long-term implementation of the program and define metrics and routines for monitoring cybersecurity awareness.
- Develop targeted cybersecurity awareness programmes for different groups, such as businesses, government, civil society, the broader population and the youth.
- Provide easily accessible baseline cybersecurity guidelines to assist organisations with limited resources; create training resources on cyber hygiene and risk management for key groups, based on nationally relevant objectives.

Cybersecurity at all levels of education

- Develop a national cybersecurity education plan defining the roles and responsibilities at all levels of the education system.
- Develop resources and tools to offer basic cyber hygiene proficiency into all school levels.
- Integrate cybersecurity courses into IT programmes in higher education.
- Create dedicated undergraduate and graduate degree programmes in cybersecurity to ensure a sufficient supply of talent.

Skilled cybersecurity workforce

- Prepare a competency development program for professionals from public organisations.
- Conduct a national assessment of the cybersecurity skills gap.
- Develop a strategic action plan for long-term development of necessary cybersecurity skills.

Lessons and General Observations

This section summarises the authors' main overall observations and recommendations to ensure the success of the NCS.

Ownership and coherent leadership of the NCS are essential to a successful outcome. We have seen time and again how important committed national leadership, dedicated to the process and with a sufficient mandate to engage parties across domains, is to the success of the NCS project. Without it, a NCS tends to result in a sum of individual agencies' activities according to their own priorities rather than a concerted whole, and leads to a fragmented, uneven and wasteful cybersecurity management, exacerbating similar problems in the future. The launch of a new NCS is a critical moment to set out its national importance and secure broad buy-in from all stakeholders. A Presidential/Prime Ministerial announcement, or at least one from the minister responsible for the strategy, will give it increased weight and awareness.

Defining a successful governance model is one of the core deliveries of a successful NCS. Successful governance and NCS execution can be delivered both by centralised and decentralised approach to governance - both with their strengths and weaknesses. While organisations' broad autonomy that is characteristic to the decentralised governance model stimulates creative partnerships and informal efficient cooperation, the consistency of actions and coordinated allocation of resources may be more straightforward with the centralised cybersecurity governance model, while decentralised governance setup needs to carefully consider establishing comprehensive understanding on division of responsibilities, coordination, responsibilities, and mechanisms for decision-making.

Providing a well-anchored long-term vision and fundamental principles are a powerful means to guide value-driven strategic development that remains consistent across strategy periods, yet is open to revision and adjustment where justified.

The Strategy and its Action Plan are complementing tools. Taken together, they ensure consistency and stability while remaining agile in a fast-evolving environment. The national cybersecurity strategy establishes a common ground for actors and actions, ensuring coherence between the various aims and activities, and providing predictability and stability for all actors for the strategy period. The Action Plan, with its focused planning period and regular review, is to ensure agility and responsiveness to the current situation within the boundaries of the strategy. To realise the objectives set out in the NCS, any subsequent policies, legislation, or sectoral strategies addressing cybersecurity should be aligned with the vision, principles, objectives, and commitments agreed in the NCS.

The solid stakeholder engagement gives quality and legitimacy to the strategy, but it must be accompanied by mutual accountability. Throughout the strategy process, public and private stakeholders are invited to engage in the strategy process, demonstrating their ambition and contributing their expertise to building national level cyber resilience. Yet ownership means not only the right to voice opinions, but also participation in burden-bearing. We call for all those involved in the strategy process to remain as committed to the strategy implementation as they have been to its development, and to hold each other accountable for delivering results.

Committed leadership is essential to the successful implementation of the national cybersecurity strategy. The continuation of strong ownership and engagement of stakeholders via an oversight and advisory board is essential for a successful realisation of the strategy. A NCS contributes to continuous improvement of cybersecurity if it is implemented; a strategy that remains on the shelf without implementation is a waste of resources and harms the trust and good will of stakeholders invested into the process. Committed implementation over time will also give insight of what works and what should be adjusted, where the ambition level could be raised and where targets might have been too optimistic due to unforeseen complexities.

Finally, a NCS is a process with a lifecycle, rather than a document. Periodic review, analysis and lessons learnt during and at the end of the strategy period should be part of the strategic approach to further developing and strengthening national cybersecurity.

Tools and references

1. Catalogue of national cybersecurity measures (legal, technical, organisational, capacity development, cooperation):
    - International Telecommunication Union: Global Cybersecurity Index. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
2. NCS lifecycle, principles and good practice:
    - Process and Guide to developing a National Cybersecurity Strategy. https://ncsguide.org/
3. Strategic, preventive and responsive capacity areas and indicators for national cybersecurity
    - e-Governance Academy: National Cybersecurity Index (NCSI). https://ncsi.ega.ee/ (12)
4. European Union elements of a national strategy
    - NIS 2016: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148
    - NIS2 for more advanced digital society https://www.nis-2-directive.com/

www.cyber4dev.eu