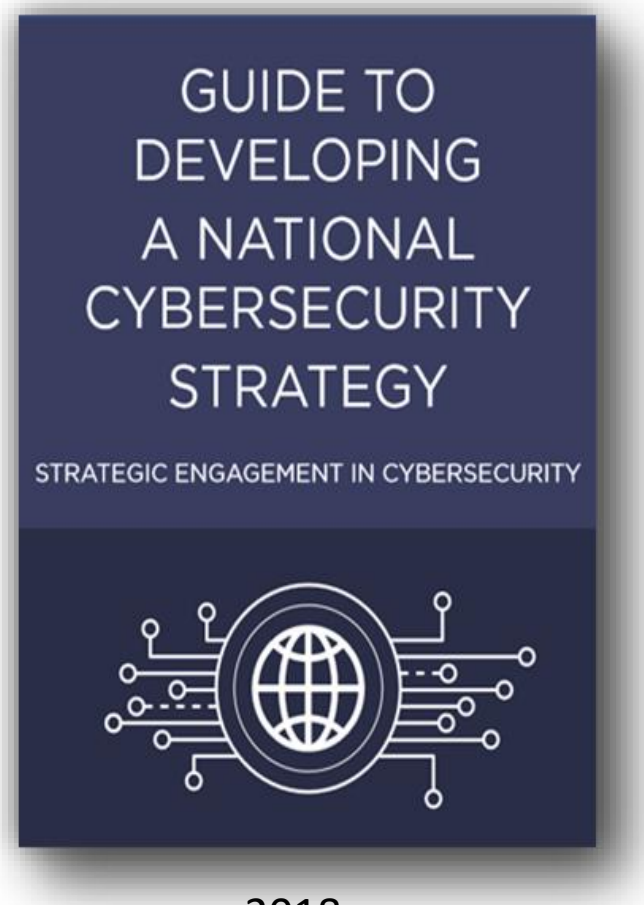
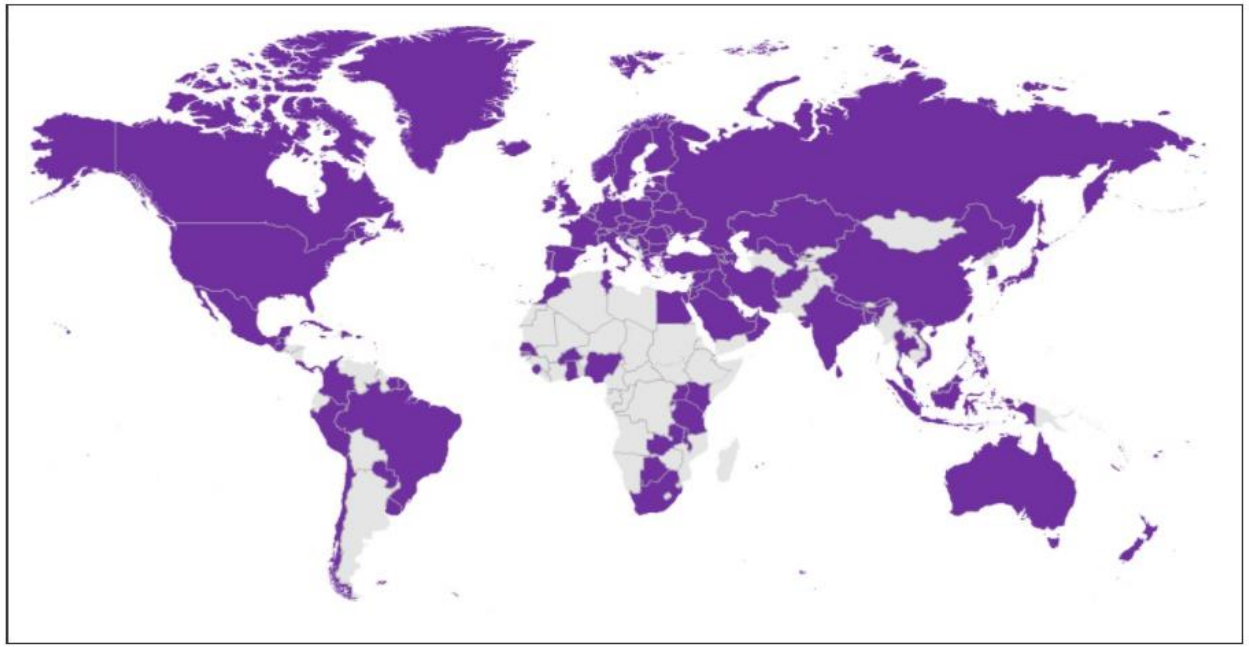
National Cybersecurity Strategy Development and Implementation

www.NCSguide.org

Proliferation of Strategies



2018



In 2018 only **76** countries had adopted an NCS, today more than **127** countries have these strategies in place, and many have used the Guide as a reference.

ITU National Cybersecurity Strategy repository (https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx)

Challenges remain

- Fast-changing nature of cyberspace
- Increased dependency on ICT
- Evolving cyber-risk/cyber-threat landscape
- Acceleration of digital transformation
- Challenges in implementing the NCS
- Challenges in adapting the NCS
- 60% of Least Developed Countries do not have an NCS in place

Guide to Developing a National Cybersecurity Strategy 2nd Edition

One of the most comprehensive overviews of what constitute successful cybersecurity strategies, to guide national leaders and policy-makers in thinking strategically about cybersecurity, preparedness and resilience at the national level.

Evolving landscape

The complex nature of cyberspace calls for continuous improvements to NCSs:

- Evolving cybersecurity landscape
- Increased dependency on ICTs
- Rapidly growing cyber risks.

Collaborative effort

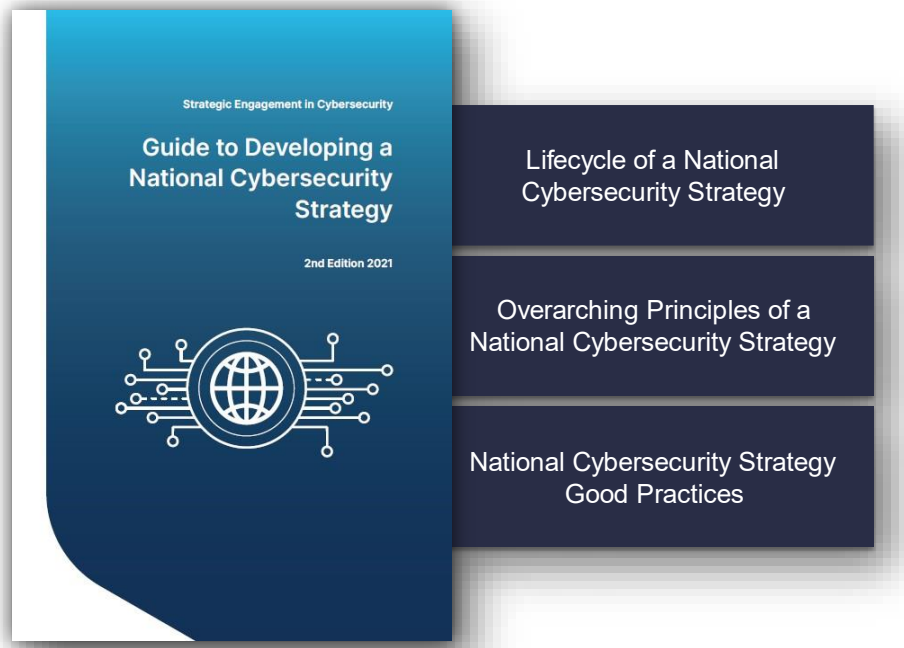
The Guide is the result of a multistakeholder cooperation effort. It merges the expertise of 19 partners from:

- Public and private sectors
- International organisations and NGOs
- Civil society
- Academia

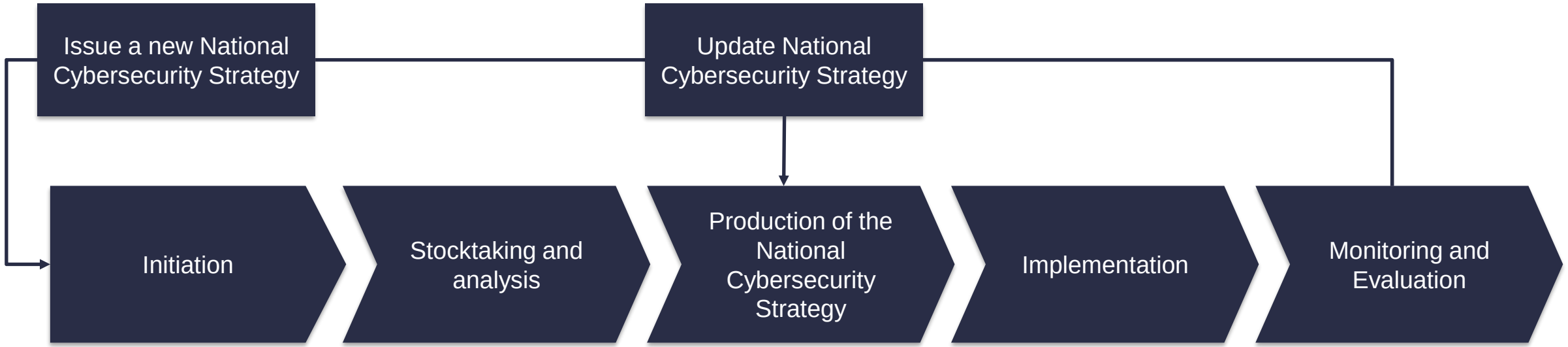
NCS Methodology

It provides reference framework to support countries' ongoing efforts to embrace digitalisation within a comprehensive NCS:

- Lifecycle of a strategy
- 9 Overarching principles
- 37 Best Practices



The Lifecycle of a National Cybersecurity Strategy



- Identifying the Lead Project Authority
- Establishing Steering Committee
- Identifying stakeholders to be involved in the NCS development
- Identifying human and financial resources
- Planning the development

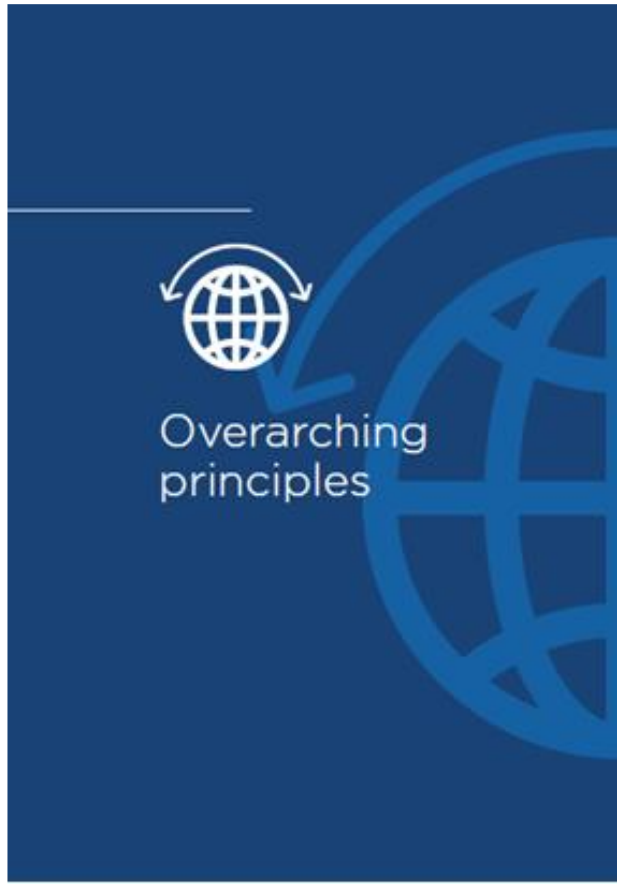
- Assessing the national cybersecurity landscape
- Assessing the cyber-risk landscape

- Drafting the NCS
- Consulting with a broad range of national, regional and international stakeholders
- Seeking formal approval
- Publishing and promoting the NCS

- Developing the action plan
- Determining initiatives to be implemented
- Allocating human and financial resources for the implementation
- Setting timeframes and metrics

- Establishing a formal process
- Monitoring the progress of the implementation of the Strategy
- Evaluating the outcome of the Strategy

The *nine* overarching principles



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

Good Practice and Focus Areas

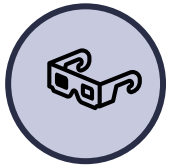
The good practice elements framework

Governance	Risk management in national cybersecurity	Preparedness and resilience	Critical infrastructure services and essential services	Capability and capacity building and awareness raising	Legislation and regulation	International cooperation
Ensure the highest level of support	Conduct a cyber-threat assessment	Establish cyber-incident response capabilities	Establish a risk-management approach	Strategically plan capacity building and awareness raising	Establish a domestic legal framework for cybersecurity	Recognise cybersecurity as a priority of foreign policy
Establish a competent cybersecurity authority	Define a risk-management approach	Establish contingency plans for cybersecurity crisis management	Adopt a governance model with clear responsibilities	Develop cybersecurity curricula	Establish a legal framework on cybercrime	Engage in international discussions
Ensure intra-governmental cooperation	Identify a methodology for managing cybersecurity risk	Promote information-sharing	Define minimum cybersecurity baselines	Stimulate capacity development and workforce training	Recognise and safeguard individual rights and liberties	Promote formal and informal cooperation in cyberspace
Ensure inter-sectoral cooperation	Develop sectoral cybersecurity risk profiles	Conduct cybersecurity exercises	Utilise a wide range of market levers	Implement cybersecurity awareness-raising programme	Create compliance mechanisms	Promote capacity building for international cooperation
Allocate dedicated budget and resources	Establish cybersecurity policies	Establish impact assessment of cybersecurity incidents	Establish public-private partnerships	Foster cybersecurity innovation and R&D	Promote capacity-building for law enforcement	
Develop an implementation plan				Tailor programmes for vulnerable sectors and groups	Establish inter-organisational processes	
					Support international cooperation to combat cybercrime	

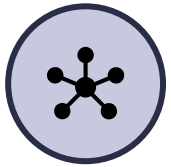
Focus on implementation

National Cybersecurity Strategy (NCS) is more than a document, it includes two levels:

- **Policy level**: what a country wants to do, what interest to pursue
- **Strategy level**: how orchestrate resources to protect national interests in cyberspace



Informed decision making



Stakeholders involvement

Governance

Human/economic resources

International cooperation

Contributors

To learn more, schedule trainings, or get in touch:

itu.int/cyb

cybersecurity@itu.int