REPUBLIC OF BULGARIA
Ministry of Transport, Information Technology and Communications

Being Strategic about Cybersecurity

Regional Cybersecurity Forum, 29-30 Nov 2016, Grand Hotel Sofia, Bulgaria

Mr. Joaquín Castellón, Operational Director
Spanish National Security Department

Ms. Anita TIKOS, Desk Officer for International Affairs,
National Cyber Security Center, Republic of Bulgaria

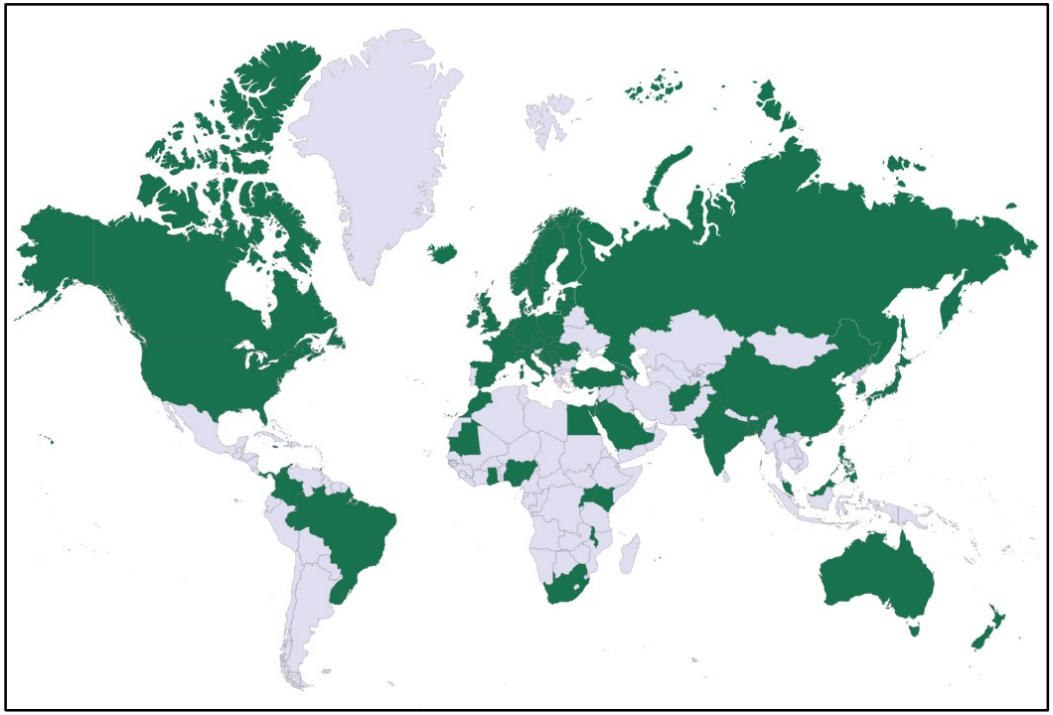
Mr. Yavor Todorov, Head of Section in Cybersecurity Department,
Special Directorate on Information Security, State Agency for National Security, Republic of Bulgaria

Mr. Luc Dandurand, Head of ICT Applications and Cybersecurity,
International Telecommunications Union

How Many Countries Have a Public National Cybersecurity Strategy?

- Only 73 out of the ITU's 193 Member States have a National Cybersecurity Strategy

- New guide being developed in collaboration with other organizations to help Member States develop, publish and implement their National Cybersecurity Strategies



Committed to connecting the world

#ICT4SDG

What would you like to search for?

ITU | General Secretariat | Radiocommunication | Standardization | Development | ITU Telecom | Members' Zone | Join ITU

About | Accessibility | Join ITU-D | Partners | Projects | Publications | Regional Presence | TDAG | WTDC | Study Groups

National Strategies Repository

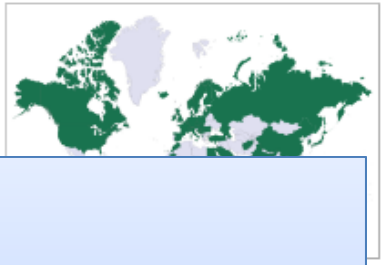
YOU ARE HERE HOME > ITU-D > CYBERSECURITY > NATIONAL STRATEGIES REPOSITORY

SHARE

About

National Strategies

This Repository includes the National Cybersecurity Strategies, be it in a form of a single or multiple documents or as an integral part of a broader ICT or national security strategies.



Please note that not all of the documents are available in English.

Repositories for National Cybersecurity Strategies:

- ITU *http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx*
- ENISA *https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world*
- NATO CCDCOE *https://ccdcoe.org/strategies-policies.html*

Austria

Azerbaijan

Lithuania

Luxembourg

Saudi Arabia

Serbia

National Cyber Security Guide
- A Joint Effort by 15 Partners -

All partners contribute their knowledge and expertise in the area of National Cybersecurity Strategies

Overview of the NCS Guide

- Overarching Principles for a strategy
  - Cross-cutting, fundamental guidance applicable to the strategy's development process and its content
- Good Practice, organized in Strategic Areas
  - Key elements to be considered for inclusion
- Process to develop an NCS
  - Key phases and steps to publish a strategy
- Supporting reference materials
  - Relevant literature

Overarching Principles

- 8 cross-cutting aspects to be considered as part of the NCS development process, as well as kept in mind when it comes to its implementation.
- Together they enable a more efficient development of a forward-looking, holistic, and sustainable NCS
- Applicable to all 7 strategic areas
- Order reflects a logical narrative rather than an order of importance.

Overarching Principles

- Vision
  - The strategy should set a clear whole-of-government and whole-of-society vision.
- Economic and Social Prosperity
  - The strategy should foster economic and social prosperity and maximize the contribution of ICTs to sustainable development and social inclusiveness.

Overarching Principles

- Comprehensive Approach, 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
- Inclusive Process
  - The strategy should be developed with an active participation of all the relevant stakeholders, and it should address their needs and responsibilities

Overarching Principles

- Human Rights and Fundamental Values
  - The National Cybersecurity Strategy should be drafted and implemented in a manner that is consistent with the fundamental values of the sovereign as well as the internationally recognised human rights.
- Risk Management and Resilience
  - The strategy should aim to manage cybersecurity risk in order to foster the resilience of the digital infrastructures and of the economic and social activities that rely on them.

Overarching Principles

- Clear Leadership, Roles and Resource Allocation
  - The NCS should be set at highest level of government, which should also assign the required roles and responsibilities, as well as allocate resources, including funding and human capacity.
- Appropriate Mix of Policy Instruments
  - The NSC should seek to utilize the best tools available for achieving a particular objective. The local context will therefore dictate whether procurement, policy or regulatory measures are used.

Strategic Areas and Good Practice

- Strategic Areas are logical groupings that put a set of related aspects together
  - Helps break down and structure the analysis work
- Good Practice identifies the elements that should be considered for inclusion in an NCS.
  - No mandatory elements! Countries are free to choose which to include, and to adapt them to their specific needs and circumstances.
  - Other aspects can of course be included

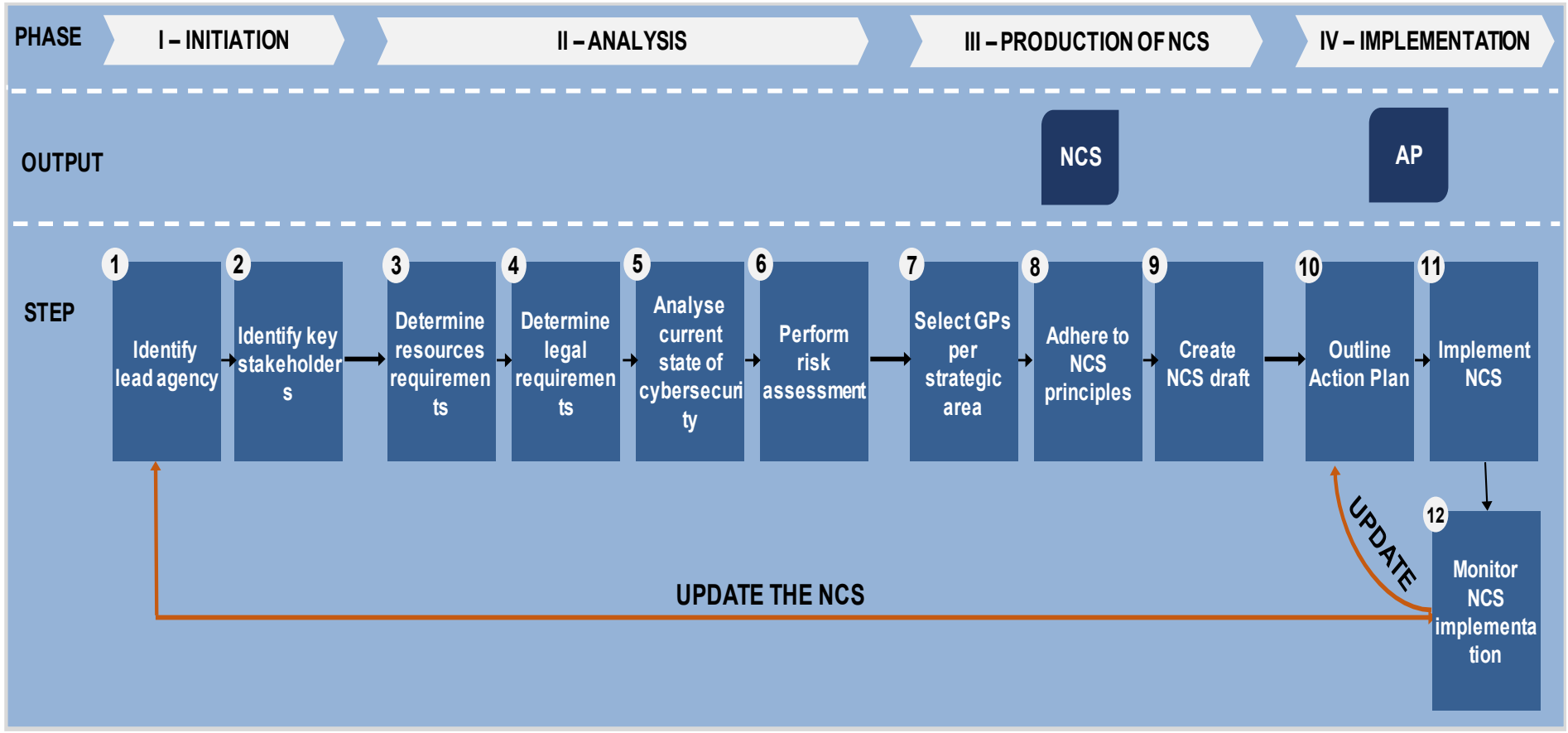
Strategic Areas

- Governance
- Risk Management Framework
- Preparedness and Resilience
- Critical Infrastructure Services
- Capability Development and Awareness
- Criminal Justice
- International Collaboration

Developing an NCS

- Phase 1 – Initiation
- Phase 2 – Analysis
- Phase 3 – Development of the text
- Phase 4 – Implementation
- Guide leads to having an NCS; but after that you need an AP, programs and projects to implement the strategy.
- Need to monitor the environment and update the strategy

Process for the Development of an NCS



The NCS Guide: a Structured Index Into Existing Publications

NCS Guide