CONSORTIUM OF GLOBAL EXPERT ORGANIZATIONS LAUNCHES THE SECOND EDITION OF THE GUIDE TO DEVELOPING A NATIONAL CYBERSECURITY STRATEGY

Written by: Giacomo Assenza, Cybersecurity Research Officer, International Telecommunication Union (ITU), Francesca Spidalieri, Cybersecurity Consultant, Hathaway Global Strategies and Carolin Weisser Harris, Lead International Operations, Global Cyber Security Capacity Centre (GCSCC)

As of 2021, more than 127 countries have adopted a National Cybersecurity Strategy (NCS) - an increase of 40% in the last three years.[1] However, challenges remain in the adoption and implementation, as well as the adaptation of NCS documents to the ever-changing cyber threat landscape. To help governments in this endeavor, a consortium of leading organizations from the cyber capacity building community jointly published a second edition of the Guide to Developing a National Cybersecurity Strategy. The new edition of this good practice guidance reflects the evolving cybersecurity landscape, emerging security trends and threats, and the growing need for strategic thinking in the development and implementation of the NCS.

National cybersecurity strategies - a global achievement

Over the last two decades, people worldwide have benefitted from the growth and adoption of information and communication technologies (ICTs) and associated socioeconomic and political opportunities. Digital transformation can be a powerful enabler of inclusive and sustainable development, but only if the underlying infrastructure and services that depend on it are safe, secure, and resilient. To reap the benefits and manage the challenges of digitalization, it has become common understanding that countries need to frame the proliferation of ICT-enabled infrastructures and services within a comprehensive national cybersecurity strategy. As a result of this heightened awareness, in 2021, more than 127 countries have adopted an NCS, almost 40% more than three years ago.

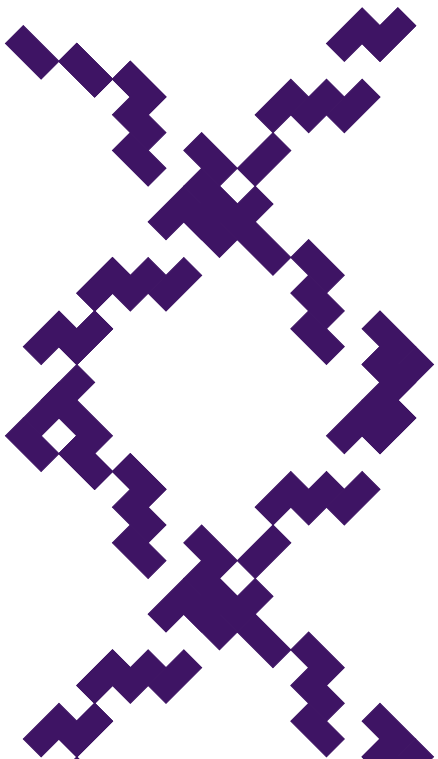
NCS in their ever-changing context

In the last decade, most countries have both accelerated their digital transformation and become increasingly concerned about the immediate and future threats to their critical services, infrastructures, sectors, institutions, and businesses, as well as to international peace and security that could result from the misuse of digital technologies and inadequate resilience. This fast-changing nature of cyberspace, the increased dependency on ICTs, and the proliferation of digital risks call for continuous improvements to national cybersecurity strategies and policies.

To help governments improve their existing or future NCS, a consortium of nineteen expert organizations (figure 1) working in the field of national cybersecurity strategies and policies came together to contribute their experience, knowledge, and expertise to update the original Guide to Developing a National Cybersecurity Strategy (NCS), v.1. Over the last three years, the first edition of Guide has served governments as an important resource in their NCS journey and it is our hope that the second edition will serve an even growing number of governments and international stakeholders. As in the previous edition, the 2021 edition of the Guide is the result of a unique, collaborative, and equitable multi-stakeholder cooperation effort among partners from the public and private sectors, as well as academia and civil society.

Good practice to prepare an NCS for new risks and challenges

The new edition of the Guide reflects the complex and evolving nature of cyberspace, the requirements for increased cybersecurity preparedness that arise from a growing number of digital risks, as well as other key trends that can impact the cybersecurity posture of a country and should, therefore, be included into national strategic planning. Focus was also given to how to develop, acquire, and prioritize financial and human resources. As in the first version, the objective of the Guide is to instigate strategic thinking and support national leaders and policy-makers in the ongoing development, establishment, and implementation of their national cybersecurity strategies and policies.



"Cybersecurity is essential to ensure effective and inclusive digital transformation. That is why comprehensive National Cybersecurity Strategies are so important, to reap the benefits and manage the challenges of digitalization, countries need to frame the proliferation of ICT-enabled infrastructure within a comprehensive National Cybersecurity Strategy."

- Ms Doreen Bogdan-Martin, Director of the Telecommunication Development Bureau (BDT) of the International Telecommunication Union (ITU).

"A Strategy is not only a document [...] it is how a government is going to play its fundamental role in orchestrating the protection of its national interest in cyberspace."

- Andrea Rigoni, Global Government and Public Services Cyber Leader, Deloitte.

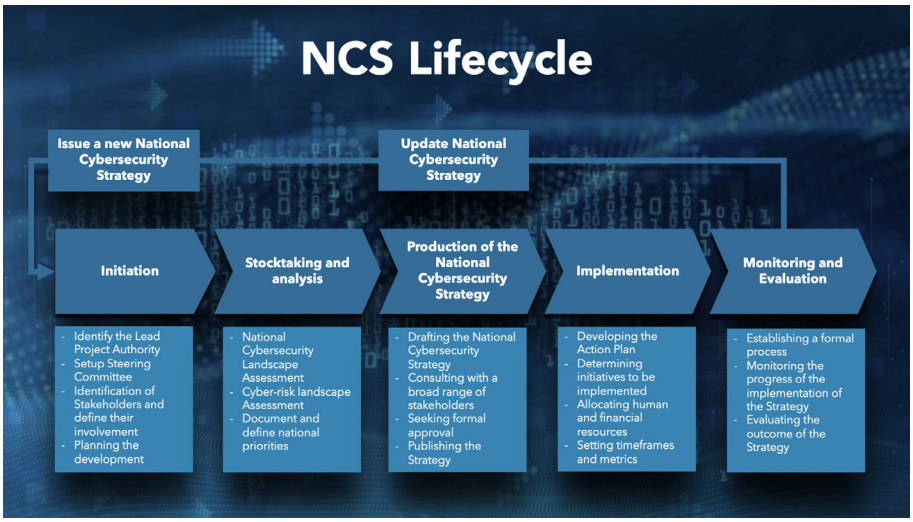


Figure 1. NCS Lifecycle.

Figure 2. Overarching principles.

The Guide remains structured in three core areas: 1. NCS Lifecycle (figure 1), 2. Overarching Principles (figure 2), and 3. Focus Areas that should be included in a NCS (figure 3). A reference list of complementary publications and other publicly available resources to support governments on their NCS journey is also provided.

To complement the Guide, a website was launched to further disseminate these good practices included and provide a space for sharing information and experience, provide updates, and contribute to knowledge sharing among governments, as well as implementers and funders of cybersecurity capacity building activities.

Visit: WWW.NCS.GUIDE

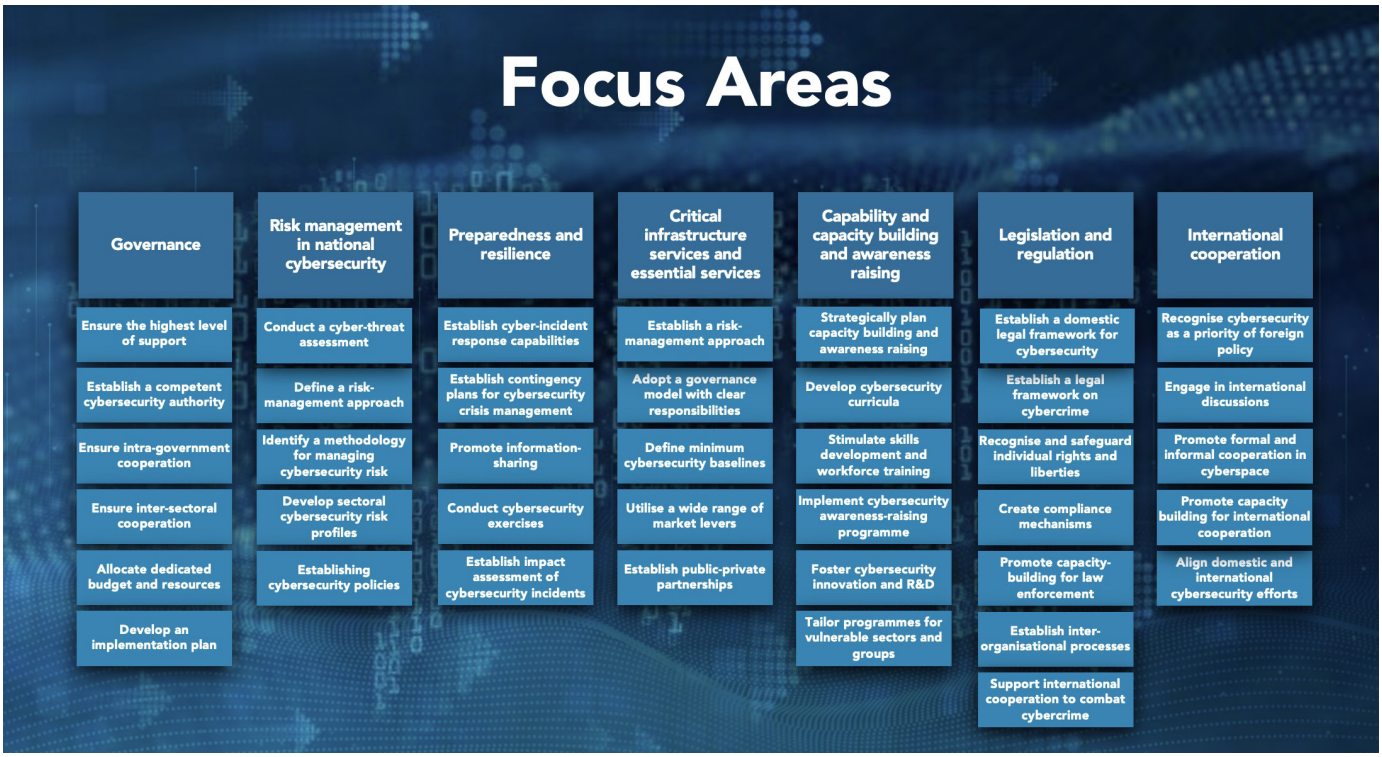


Figure 3. Focus areas of NCS good practice.

List of Partners

Council of Europe (CoE)
Commonwealth Secretariat (ComSec)
Commonwealth Telecommunications Organisation (CTO)
Deloitte
Forum of Incident Response Teams (FIRST)
Geneva Centre for Security Sector Governance (DCAF)
Global Cyber Security Capacity Centre (GCSCC)
Geneva Centre for Security Policy (GCSP)
Global Partners Digital (GPD)
International Criminal Police Organization (Interpol)
International Telecommunication Union (ITU)
Microsoft
NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)
Potomac Institute for Policy Studies (PIPS)
RAND Europe
The World Bank
United Nations Institute for Disarmament Research (UNIDIR)
United Nations Counter-Terrorism Office (UNOCT)
United Nations University (UNU)

Observers: Axon Partners Group (Axon), Cyber Readiness Institute (CRI), Global Forum on Cyber Expertise (GFCE), Organization of American States (OAS), World Economic Forum (WEF)

Figure 4. List of Partners.

NOTES

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