NCSI
national cyber security index

Upgrading National Cyber Resilience

National Cybersecurity in Practice 2

Upgrading National Cyber Resilience

National Cybersecurity in Practice 2

The handbook National Cyber Security in Practice is financed by the Estonian Ministry of Foreign Affairs from the funds of development cooperation and humanitarian aid.

Publication composed by Kadri Kaska
Contributors: Henrik Beckvard, Kadri Kaska, Hannes Krause, Merle Maigre, Anna-Maria Osula, Radu Serrano, Martin Švéda
Photos: iStock
Design: OÜ Dada AD
Print: Aktaprint AS
Translation and editing: Refiner OÜ

Published by:
e-Governance Academy
Rotermanni 8, 10111 Tallinn
ega.ee

Tallinn, 2022
ISBN 978-9949-7467-3-6

Contents

6 Foreword

8 Introduction

12 What is the National Cybersecurity Index and how does it work?

14 The NCSI: An ever-evolving tool

20 Strategic cybersecurity leadership

26 How do global engagements matter for national cyber resilience?

31 What can we learn from the revised European approach to critical infrastructure cybersecurity?

36 Building cyber resilience through crisis preparedness

44 Cybersecurity support for digital transformation

48 Contributing to the NCSI

49 Contributors

Foreword

Hannes Astok

Chairman of the Management Board,
e-Governance Academy

This year marks the 20th anniversary of the e-Governance Academy (eGA). Driven by our mission to increase the prosperity and openness of societies through digital transformation, we have worked since 2002 with numerous countries around the world to build successful digital societies that improve their citizens' lives, strengthen their economies, and deliver transparent, democratic and effective public administration.

The world has changed in these two decades, and so have governments' ways of operation. Twenty years ago, only one in ten people in the world used the internet; by 2022, that number had grown to two out of three. The United Nations 2003 Global E-government Survey noted governments' progress in embracing information and communications technologies (ICT) for e-government, manifested in their use of the internet and having a website presence, with the more ambitious ones establishing e-government portals for one-stop service sites.[1]

Today, the top achievements of that era have become baselines for nearly all countries,[2] with current aspirations revolving around the use of big data, machine learning, and artificial intelligence to improve public services for citizens.

Cyberspace, the environment where e-services and people interact, has grown immensely more complex over these past two decades. Product and service innovation, new and legacy technologies, and complex supply chains all shape the boundaries of what is possible. Various actors – individuals, organisations, and states – use digital technologies to enable and empower their goals and activities, with benevolent or malevolent intents. People see digitalisation as among the greatest opportunities and cyber threats as among the most pertinent threats to public security. The stakes are high, and whether digitisation becomes a country's success story depends on how wisely countries seize the opportunities and manage the risks involved.

1 UN Global E-Government Survey 2003, https://desapublications.un.org/file/787/download

2 UN E-Government Survey 2022, https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2022

Cybersecurity must therefore be at the core of the digital transformation – in the inception, implementation, and delivery of e-services and solutions, and a fundamental component of digital societies.

Over the years, cybersecurity has grown to occupy a major part of our work at the eGA. We have helped more than 40 countries assess their national readiness to prevent and respond to cyber threats, establish cybersecurity governance and risk management mechanisms, draft the relevant legislation, strengthen incident prevention and response capacities, or take stock of best practices in cybersecurity awareness raising. Our National Cybersecurity Index (NCSI) has since 2016 served as a key tool to support these activities and to help countries develop their cybersecurity capacities.

This publication portrays how the NCSI has developed through the years and offers insights from experienced cybersecurity practitioners on enhancing national preparedness and resilience, both through domestic and international actions. Complementing our 2020 National Cyber Security in Practice handbook,[3] we hope this publication will be useful for leaders, policymakers, legislative experts, and others working to strengthen the cybersecurity posture of their countries.

The e-Governance Academy wishes to thank Henrik Beckvard, Kadri Kaska, Hannes Krause, Merle Maigre, Anna-Maria Osula, Radu Serrano, and Martin Švéda for contributing their insights, and the number of experts who have been involved in developing the NCSI, including Markko Künnapu, Helar Laasik, Epp Maaten, Piret Pernik, Raul Rikk, Radu Serrano, and Hauke Schulz. We are grateful to the Estonian Ministry of Foreign Affairs for their long-time support for the development of the NCSI and the expansion of the National Cyber Security in Practice handbook.

We wish you insightful and enjoyable reading!

3 National Cyber Security in Practice. e-Governance Academy, 2020. https://ega.ee/wp-content/uploads/2020/05/Kuberturvalisuse_kasiraamat_ENG.pdf

Introduction

Merle Maigre
Cybersecurity Programme Director, e-Governance Academy

Kadri Kaska
Composer of the publication, Senior Cybersecurity Expert, e-Governance Academy

Digital is the new normal of the modern world: the habitual way of life for individuals, governments, businesses, and civil society hinges on reliable digital infrastructure. That means that cybersecurity is not a mere technological challenge, but a matter of societal resilience and stability. While businesses are responsible for the cybersecurity of the services they provide, and individuals need to take care of their digital assets, the cybersecurity of the country is ultimately the responsibility of the state and of national governments.

For countries building their national cybersecurity system, the range of issues to be considered and addressed may seem intimidating. The e-Governance Academy's NCSI offers a tool to systematically measure countries' cyber resilience and to develop the necessary capacities. First launched in 2016, the NCSI offers a framework to assess national preparedness in key areas and helps countries identify their existing cybersecurity gaps to fill as well as strengths to build on. It also allows them to evaluate their overall and sectoral cybersecurity maturity relative to the rest of the world.

The NCSI incorporates our experience from the dozens of cybersecurity projects we have undertaken with our partners and experts. Cooperating with cybersecurity experts and national contributors, the eGA keeps developing the NCSI to ensure it remains a relevant, timely cybersecurity tool. The methodology is regularly updated to take into account the evolving technology and cyber threat environment, as well as the best cybersecurity practices relevant to the current resilience objectives.

This publication presents the outcome of the NCSI methodology update conducted during 2021–2022 and describes how the NCSI has developed through the years. Furthermore, following the effort of our 2020 National Cyber Security in Practice handbook to give national policymakers, legislative experts, and others responsible for securing the digital environment an overview of the key elements that underpin the national cybersecurity architecture, this publication takes a closer look at additional areas of national cybersecurity: strategic leadership, global engagements, a stronger legal framework for cyber resilience, and crisis preparedness.

The **first and second chapters** of this publication give an overview of the NCSI – its purpose, scope, capacity areas and methodology, the changes in the latest version, and an outline of how the NCSI has evolved over time. Since its start in 2016, the index has grown in substance, scope, and presentation to better serve the interests of the global community.

The next part of the publication further expands on some of the capacity areas of the NCSI. The expert views section of the publication begins with **chapter three**, emphasising the importance of a risk management approach to cybersecurity, even at the whole-of-society level. Prioritisation is essential when it comes to cybersecurity: it is not possible to secure everything, yet infrastructure interdependencies and the different operating logics of public and private sector actors means that nations must take extra care to ensure that the critical infrastructure that determines the functioning of societies remains operational.

Chapter four emphasises that building national cyber resilience is not a purely domestic matter, but requires cooperation among states, regional and international institutions, and industry, academia, and civil society stakeholders. The author shares her experience on how strengthening and expanding international, regional, and multistakeholder partnerships allows countries to promote their values and vision for cyberspace, support their economic interests and digital transformation, and negotiate over cyberspace rules, norms and principles aimed at preventing conflict.

The author of **chapter five** gives an overview of the recently updated European approach to the cybersecurity of critical infrastructure, drawing lessons from the implementation of the previous European Union Directive on Network and Information Systems Security (NIS Directive), one of the world's most influential transnational cybersecurity legislative frameworks. The expanded range of regulated entities, more specific security requirements, stricter incident reporting, and unified crisis management is expected to make Europeans safer in cyberspace, but implementation of the new rules will be a challenge for both infrastructure owners and governments.

Chapter six shares some useful measures based on practical experience in cyber crisis preparedness. By installing clear cybersecurity governance structures that serve the country well in normal circumstances, setting up regular coordination fora and mechanisms, planning for crisis scenarios and conducting regular exercises, and building strong networks of trust, a country can be better prepared for and remain resilient in a crisis scenario.

How does the e-Governance Academy help countries ensure that their digital transformation is undertaken with cybersecurity in mind? In the final part of this publication, Merle Maigre, the eGA's Cybersecurity Programme Director explains how the e-Governance Academy provides expertise on the security aspects of digital transformation and the trustworthiness of the national cyberspace. In line with the NCSI criteria, the eGA is focusing on the organisational, regulatory, and technical aspects of cybersecurity. Through support for developing policy and regulation, building cyber incident management capacities, and cybersecurity awareness raising, we show that it is possible to apply the security-by-design approach to digital transformation.

But cybersecurity will always be a matter of cooperation and never a one-way-street. The NCSI remains a substantial public knowledge base, containing information from over 160 countries worldwide, thanks to our network of contacts who have helped keep the information up to date and publicly accessible online. Radu Serrano, the lead of the NCSI team, concludes this publication by explaining how those interested in becoming NCSI international partners and country contributors can contact us.

We hope that this publication will provide useful insights and inspiration to all those responsible for national cybersecurity. Let's make digital transformation resilient everywhere!

What is the National Cybersecurity Index (NCSI) and how does it work?

Kadri Kaska

Senior Cybersecurity Expert, e-Governance Academy

The NCSI, introduced by the e-Governance Academy in 2016, is one the world's most detailed tools to track countries' cybersecurity commitment and readiness.

The NCSI monitors institutionalised national cybersecurity capacities as implemented by the central government, measuring countries' preparedness to prevent cyber threats and manage cyber incidents. All NCSI findings are based on objective and measurable criteria supported by publicly available evidence. These could be legal and policy instruments (legal acts, regulations, policies, administrative orders), institutions (established organisations, departments, units), cooperation formats (committees, working groups), activities (exercises, technologies, established programmes), or other deliverables (websites, curricula, official statements).

The index monitors countries' performance in 12 cybersecurity capacity areas, grouped into three pillars:

- **Strategic capacities**, including aspects related to cybersecurity governance and policy, global engagement, education, and innovation;
- **Preventive capacities**, which involve aspects such as secure digital infrastructure and cyber threat analysis;
- **Responsive capacities**, related to responding to cyber threats of various natures and scales, and to managing cyber incidents and cybercrime.

The 12 capacity areas are further divided into a total of 49 unique indicators, which describe the relevant assessment criteria and the types of evidence used to support the findings. For example, the cybersecurity policy capacity area includes five indicators that assess whether a country has established high-level accountability for cybersecurity, assigned responsibilities for policy development and coordination, and adopted a cybersecurity strategy and an action plan to implement it. Under preventive capacities, the cybersecurity of critical information infrastructure capacity area monitors whether a mechanism for identifying critical information infrastructure has been established; whether infrastructure operators and public sector organisations are required to assess and manage cyber risks and/or implement cybersecurity measures; and whether a competent supervisory authority has been designated and allocated powers to supervise the implementation of cyber/information security measures. Among the responsive capacities, the fight against cybercrime capacity area measures the country's preparedness and commitment to combat cybercrime by establishing the necessary legislative measures, organisational frameworks, and international cooperation.

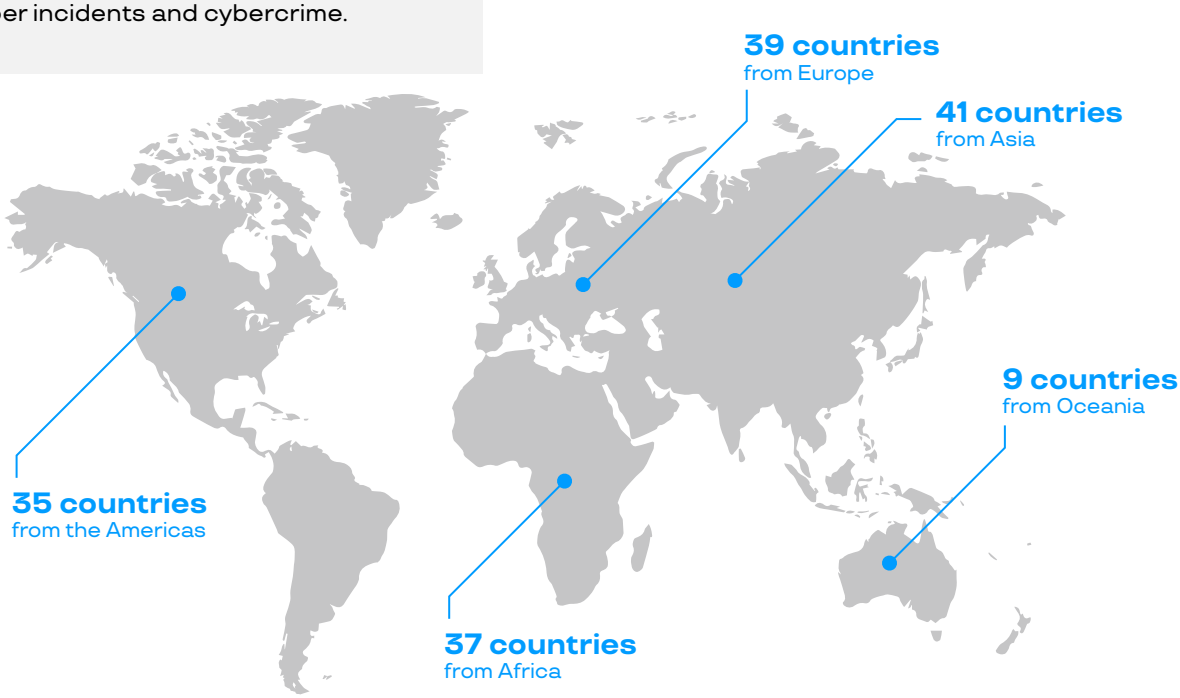


Figure 1. NCSI assessed countries by regions. Find out more at ncsi.ega.ee

The many uses of the NCSI

The NCSI is a comprehensive resource for cybersecurity capacity building that can be used in several ways.

It is a **live global index** that includes data from more than 160 countries. A public online portal, ncsi.ega.ee, presents countries on a world map with a ranking and a score: the ranking indicates the country's global position in the index, and the score reflects the percentage the country received from the maximum total value of all NCSI indicators. The NCSI website allows users to compare countries globally, at the regional level, or within international organisations. The data is updated on a rolling basis as new evidence becomes available, without publishing annual rankings.

The NCSI additionally serves as a **cybersecurity reference tool**: its country pages provide hundreds of links to national policy and legal documents, institutions, and programmes. Each country page first displays an overview of national performance in the NCSI and other global cybersecurity indexes such as the International Telecommunication Union's (ITU) Global Cybersecurity Index,[4] as well as in global digitalisation indexes. Following this, the country page presents an outline of all capacity areas and indicators along with descriptions, and the corresponding evidence supporting the findings for the country for each indicator. This makes the NCSI a source of information to show how any particular country is building its cybersecurity capacity.

Finally, the NCSI is used by the eGA and national governments as a cybersecurity **assessment and capacity building tool**, with transparent criteria and methodology that allow countries to evaluate their existing national cybersecurity essentials, indicating areas of solid performance and capacities that need to be built and/or improved.

What is new in the revised NCSI?

The eGA reviews the NCSI indicators and criteria periodically to ensure they remain relevant to current global good practices. The NCSI 3.0 includes revised maturity indicators, taking into account developments in technology, the evolving risk environment, as well as the ongoing maturation of countries' cybersecurity practices. These changes are reflected in the revised structure and substantive requirements.

NCSI 3.0 includes new indicators for political leadership, commitment to international law in cyberspace, and cybersecurity research and development (Strategic pillar); cybersecurity of cloud services and the supply chain, and cybersecurity awareness raising coordination (Preventive pillar); and cyber incident reporting tools, participation in international incident response cooperation, procedural law, and military cyber doctrine (Responsive pillar).

The NCSI 3.0 has merged the protection of digital and essential services into a single capacity area and further merged some indicators for electronic identity and trust services, while omitting indicators concerning international cybersecurity organisations hosted by countries and participation in international (military) cyber exercises. The revised structure and indicators are presented in Table 1 below.

All NCSI indicators and required evidence are also complemented by more detailed explanations, describing the substance and importance of the indicators and providing further guidance on the required evidence. The updated NCSI also includes revised indicator scores and weights that reflect the significance of the particular aspect in the national cybersecurity system.

4 Global Cybersecurity Index. International Telecommunication Union, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Table 1. Revised indicators in the National Cybersecurity Index 3.0

Strategic Capacities	Preventive capacities	Responsive Capacities
1 CYBERSECURITY POLICY 1.1 High-level cybersecurity leadership 1.2 Cybersecurity policy development 1.3 Cybersecurity policy coordination 1.4 National cybersecurity strategy 1.5 National cybersecurity strategy action plan **2 GLOBAL CYBERSECURITY CONTRIBUTION** 2.1 Cyber diplomacy engagements 2.2 Commitment to international law in cyberspace 2.3 Contribution to international capacity building in cybersecurity **3 EDUCATION AND PROFESSIONAL DEVELOPMENT** 3.1 Cyber safety competencies in primary education 3.2 Cyber safety competencies in secondary education 3.3 Undergraduate cybersecurity education 3.4 Graduate cybersecurity education 3.5 Association of cybersecurity professionals **4 CYBERSECURITY RESEARCH AND DEVELOPMENT** 4.1 Cybersecurity research and development programmes 4.2 Cybersecurity doctoral studies	**5 CYBERSECURITY OF CRITICAL INFORMATION INFRASTRUCTURE** 5.1 Identification of critical information infrastructure 5.2 Cybersecurity requirements for operators of critical information infrastructure 5.3 Cybersecurity requirements for public sector organisations 5.4 Competent supervisory authority **6 CYBERSECURITY OF DIGITAL ENABLERS** 6.1 Secure electronic identification 6.2 Electronic signature 6.3 Trust services 6.4 Supervisory authority for trust services 6.5 Cybersecurity requirements for cloud services 6.6 Supply chain cybersecurity **7 CYBER THREAT ANALYSIS AND AWARENESS RAISING** 7.1 Cyber threat analysis 7.2 Public cyber threat reports 7.3 Public cybersecurity awareness resources 7.4 Cybersecurity awareness raising coordination **8 PROTECTION OF PERSONAL DATA** 8.1 Personal data protection legislation 8.2 Personal data protection authority	**9 CYBER INCIDENT RESPONSE** 9.1 National incident response capacity 9.2 Incident reporting obligations 9.3 Cyber incident reporting tool 9.4 Single point of contact for international cooperation 9.5 Participation in international incident response cooperation **10 CYBER CRISIS MANAGEMENT** 10.1 Cyber crisis management plan 10.2 National cyber crisis management exercises 10.3 Participation in international cyber crisis exercises 10.4 Operational crisis reserve **11 FIGHT AGAINST CYBERCRIME** 11.1 Cybercrime offences in national law 11.2 Procedural law provisions 11.3 Ratification of or accession to the Convention on Cybercrime 11.4 Cybercrime investigation capacity 11.5 Digital forensics capacity 11.6 24/7 contact point for international cybercrime **12 MILITARY CYBER DEFENCE** 12.1 Military cyber defence capacity 12.2 Military cyber doctrine 12.3 Military cyber defence exercises

The NCSI: An ever-evolving tool

Radu Serrano
Project Manager,
NCSI Data Lead,
e-Governance Academy

The NCSI is a global live index that assesses the preparedness of over 160 countries to prevent cyber threats and manage cyber incidents. However, it was not so extensive from the beginning. With the advent of the updated methodology, the NCSI team thought it would be interesting for our readers to learn about how the NCSI was born and its consequent evolution throughout the years.

The NCSI is a global live index that assesses the preparedness of over 160 countries to prevent cyber threats and manage cyber incidents. However, it was not so extensive from the beginning. With the advent of the updated methodology, the NCSI team thought it would be interesting for our readers to learn about how the NCSI was born and its consequent evolution throughout the years.

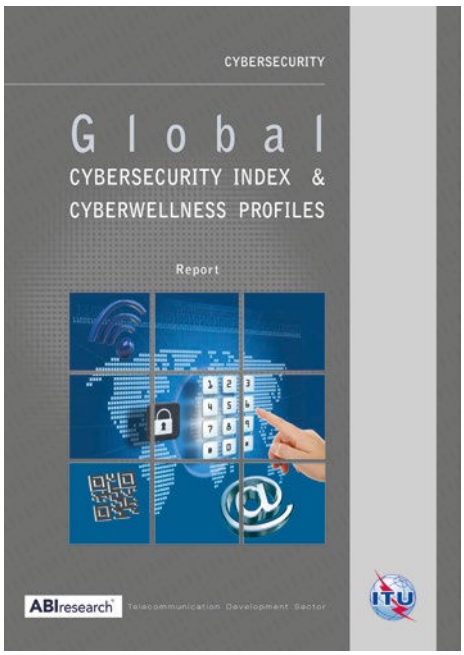


Figure 1. The first Global Cybersecurity Index (GCI) 2014

Let us travel back almost a decade, to 2014, when the ITU began developing its Global Cybersecurity Index (GCI). The first iteration of the GCI was dated April 2015 and contained the results of the 2014 survey, to which 105 countries had responded.[5] At the same time, Estonia's Cyber Security Strategy 2014–2017 expressed the country's vision of becoming one of the global leaders in cybersecurity policy through, among other things, the development of an international Cyber Security Index, as presented in the corresponding Implementation Plan.[6]

Therefore, in March 2015, the eGA was selected to develop a national cybersecurity assessment methodology and implement it in Moldova. This mini-project lasted seven months and was funded by Estonia's Ministry of Foreign Affairs.[7] In addition to the assessment methodology and its pilot, the project would also deliver the web-environment for this future index. Moldova had been chosen for the pilot because the eGA had been helping develop the country's information society and security for years; it had created the national cybersecurity development plan in 2013–2014. Therefore, this mini-project was a continuation of the improvement of Moldova's cybersecurity capabilities.

Having successfully completed a pilot of the methodology, in January 2016, the NCSI received funding from Estonia's Ministry of Foreign Affairs for a two-year global implementation project. On 31 May, version 1.0 of the NCSI was officially launched at the 2016 e-Governance Conference.[8] Quite similar to the current version, version 1.0 had four categories, 12 capacities and a total of 60 indicators. It set the base principles for the NCSI: the index would focus on clearly measurable aspects of national cybersecurity (i.e., legislation, units, cooperation formats, and outcomes); its methodology would take into consideration only publicly available information; and it would also double as a database and tool for national capacity building in the field.

This version would then be used to review the cybersecurity situation and capacity of Eastern Partnership countries in 2017.[9]

5 GCI 2014. Available online at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2014.aspx

6 Estonia's Cyber Security Strategy 2014–2017

7 Development of a National Cyber Security Index. Available online at: https://ega.ee/project/implementation-of-a-national-cyber-security-index/

8 Raul Rikk, Cyber Security Programme Director, e-Governance Academy Estonia. Available online at: https://www.youtube.com/watch?v=bM1aNbmqHvk

9 Situation Review of EU's Eastern Partnership countries. Available online at: https://ega.ee/project/situation-review-of-eus-eastern-partnership-countries/

General Cyber Security Indicators

1. Policy development
2. Threat assessment
3. Cyber security education

Baseline Cyber Security Indicators

4. Baseline cyber security
5. Protection of e-services
6. E-identification and e-signature
7. Critical information infrastructure protection

Incident and Crisis Management Indicators

8. Incident detection and management 24/7
9. Cyber crisis management
10. Fight against cyber crime
11. Military cyber operations

International influence indicators

12. International cyber security

Figure 2. NCSI v.1.0 categories and capacties

Vestiges of this iteration of the NCSI can be found in the project's corresponding publication, Situation Review: Safety and Security of Cyberspace and e-Democracy in the Eastern Partnership Countries.[10] By the end of 2017, the NCSI website contained information about 40 countries.

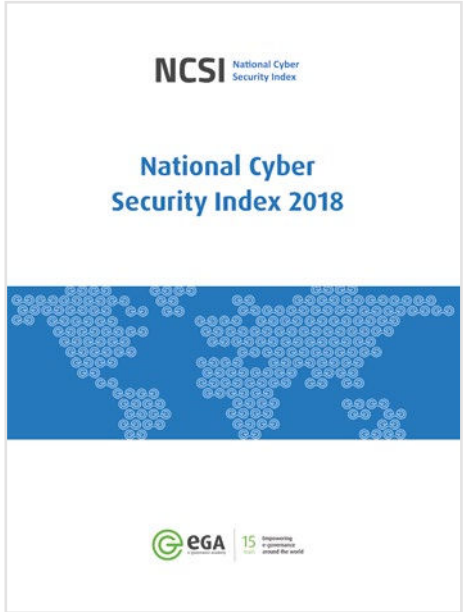


Figure 3. NCSI 2018 Booklet

In March 2018, the NCSI received funding for a further two-year period, to continue its international application.[11] This extension allowed the NCSI methodology to be updated to version 2.0, which had been in the works since 2017 and could now be implemented. The index had been restructured into three categories, 12 capacities and 46 indicators, and its visual identity was modernised. Although it was designed to be a live index, a one-off publication was drafted to commemorate the eGA's 15th anniversary and to introduce the new NCSI methodology iteration. Thus, a snapshot of the national cybersecurity status of 100 countries as of May 2018 was compiled in the NCSI 2018 booklet.[12] For the remaining period of the project, the team focused on adding more countries to the index and drafting the National Cyber Security in Practice handbook.[13]

10 Situation Review: Safety and Security of Cyberspace and e-Democracy in the Eastern Partnership Countries. Available online at: https://ega.ee/publication/situation-review-safety-and-security-of-cyberspace-and-e-democracy-in-the-eastern-partnership-countries/

11 Shaping of Trusted Information Societies in Developing Countries. Available online at: https://ega.ee/project/shaping-trusted-information-societies-developing-countries/

12 NCSI booklet 2018. Available online at: https://ega.ee/publication/ncsi-booklet-2018/

13 National Cyber Security in Practice. Available online at: https://ega.ee/publication/national-cyber-security-handbook/

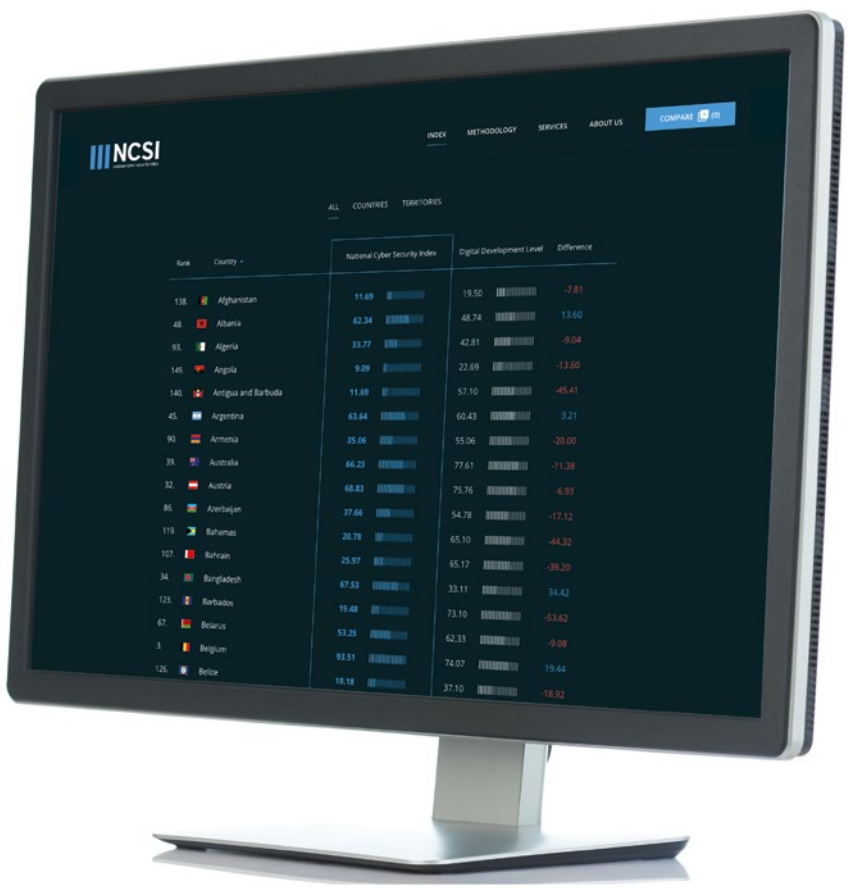
By the end date of the project in April 2020, 160 countries figured in the NCSI, thanks to the team and 116 representatives from 77 countries who provided us with data during that time.

The global pandemic brought about the rapid digitalisation of governments and a massive increase in the use of the Internet and teleworking. However, with e-solutions being developed very fast, there was no guarantee that they included a high level of security. National cybersecurity was now more important than ever. The NCSI was funded once again for a period of two years in October 2020, with the main objectives: maintaining and updating in a timely manner the large database of country evidence, updating the NCSI methodology, and piloting the Cybersecurity Maturity Assessment.[14] A Cybersecurity Maturity Assessment enables target countries to identify strengths, gaps, and areas of improvement in their cybersecurity posture, and accordingly improve their resilience against cyber incidents and attacks.

The Cybersecurity Maturity Assessments are conducted using the NCSI methodology and the results are also used to update the relevant country data in the NCSI.

Alongside the maturity assessments, the eGA also supports the set-up and implementation of capacity building programmes in the target countries. The assessments can also be potentially followed by a series of specific workshops for the main stakeholders in the target countries, focusing on sharing best practices for implementing cybersecurity reforms and providing examples of different services from various other countries. The pilot Cybersecurity Maturity Assessments focused on Armenia, Botswana, Georgia, Jamaica, Kyrgyzstan, Moldova, Northern Macedonia, and Uganda.[15]

In the end of the year 2022, we are glad to report that we have been rolling out continuous country updates. The NCSI now has over 160 countries, the maturity assessments have been successfully piloted, and the NCSI methodology has been updated and elaborated once more. We strive to keep this tool available and relevant for the benefit of the global community.



14 Advancing Cybersecurity Capacities for Digital Transformation. Available online at: https://ega.ee/project/advancing-cyber-security-capacities-for-digital-transformation/

15 Ibid.

Expert perspectives

Strategic cybersecurity leadership

Henrik Beckvard

Strategy researcher, NATO Cooperative Cyber Defence Centre of Excellence

The digital revolution has brought changes to almost every aspect of our lives. It has transformed the way that we live, think, work, and do business. The services that we may receive from government authorities and how we interact with one another are to a large extent shaped by the possibilities provided in and through cyberspace. The digital revolution is here to stay.

Most governments have realised that for their country to be competitive in the world market, digital solutions need to be implemented. There are immense benefits to be harvested from such an approach, but with them also come a growing number of threats and vulnerabilities.

Possibilities... and risks

The more reliant a nation is on digital solutions, the more vulnerable it becomes to cyberattacks that have become a daily occurrence in most societies.

Cyberattacks are not only becoming more frequent but also generally more sophisticated. A firewall may not be enough to stop phishing or distributed denial-of-service (DDoS) attacks flooding a network. It may also not be enough to block information or identity theft. Firewalls also cannot block ransomware attacks, where information is taken hostage by encrypting it and a ransom is demanded in exchange for an encryption key to unlock the data. The threats are as many and varied as there are malicious actors (criminals, hacktivists, state-sponsored hackers and so on). Cybersecurity is something that concerns everyone – private persons, business corporations and nation-states.

Nations must ensure that their critical infrastructure remains operational. What constitutes critical infrastructure may vary from nation to nation, but overall it may be described as the assets, systems, and networks, whether physical or virtual, that are so essential that their incapacitation or destruction would have a debilitating effect on national security, economic stability, public health, safety, or any combination thereof.

As there are many interdependencies between the various sectors that constitute a nation's critical infrastructure, there is a need for overall coordination of the efforts to protect these (Figure 1 below).

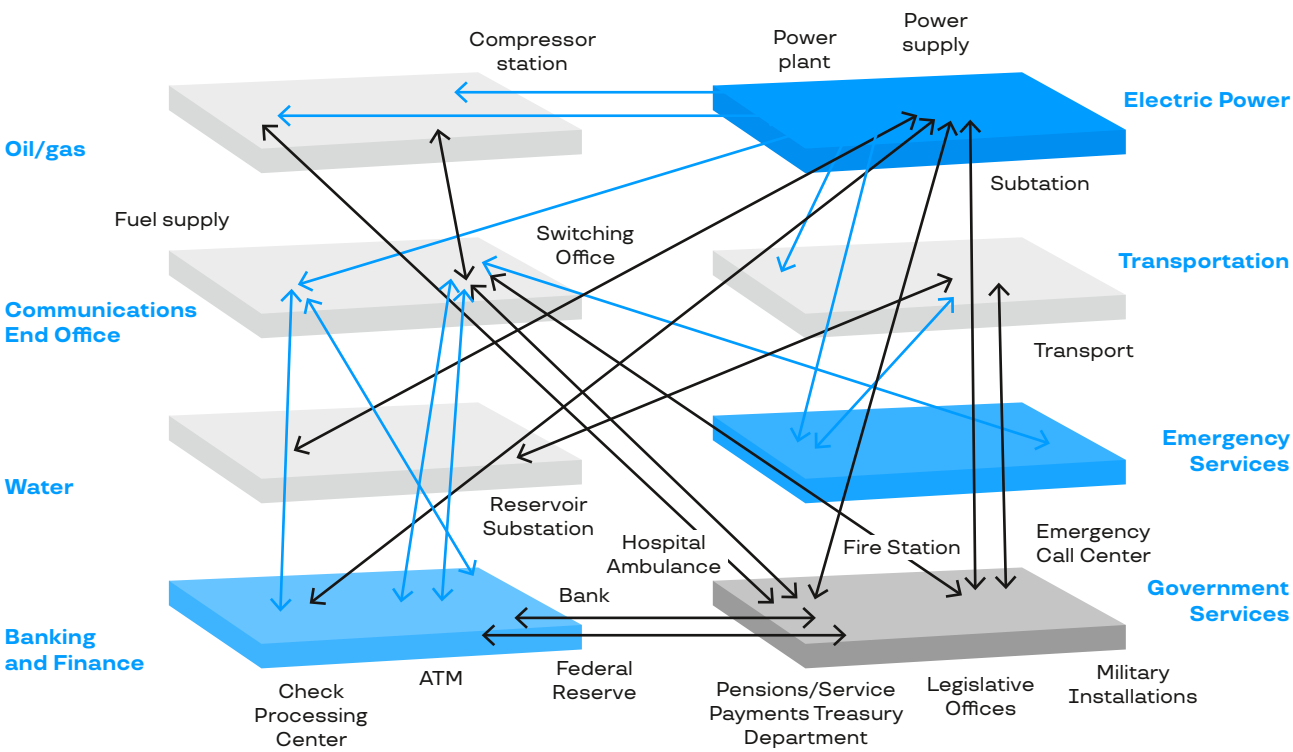


Figure 1: Interdependencies between critical infrastructure sectors[16]

16 Source: OECD Reviews of Risk Management Policies: Good Governance for Critical Infrastructure Resilience, https://www.oecd-ilibrary.org/sites/76326acb-en/index.html?itemId=/content/component/76326acb-en

In most cases, individual sectors are governed by the relevant ministry (economy, transportation, energy, etc.) and it therefore will be the responsibility of the government to ensure that protective measures are taken by the various sectors – and that these efforts are coordinated at the national strategic level. It will never be sufficient for a sector to protect only itself. The government must also ensure that sectors on which these sectors rely function as required. For example, for the financial sector to function smoothly it needs the telecommunication and the energy (power) sectors to also operate properly.

> **It will never be sufficient for a sector to protect only itself.**

Some functions of a government have been (partly) outsourced to private companies. Take telecommunications as an example. If a government is to ensure the smooth functioning and integrity of the sector, it will have to work closely with the telecommunications provider. In this regard, the required government safety mechanisms must be clearly laid out and followed.

In any nation, therefore, it is the government that bears the ultimate responsibility for ensuring the data integrity and functioning of sectors that are deemed part of the nation's critical infrastructure.

> **It is the government that bears the ultimate responsibility for ensuring the data integrity and functioning of sectors that are deemed part of the nation's critical infrastructure.**

How do we minimise risk?

There are several ways to strengthen resilience and minimise the risks to a nation's critical infrastructure, and given enough time and resources that defence may become very effective. However, there's a global shortage of time and resources. Quite often, we need to strengthen our resilience 'yesterday', and will get no additional funding to get the job done.

Because of interdependencies, there is a natural tendency to try to protect everything. Frederic the Great, an 18th-century King of Prussia who was an influential military theorist of his time, reportedly stated that 'He who defends everything, defends nothing'. This still holds true: prioritisation is essential when it comes to the protection of critical infrastructure.

There are various models for risk management at the organisational level, but it can be a challenge to devise a strategic risk management approach for an entire country, especially as the sector responsible for maintaining a critical infrastructure service and those who actually perform the service may not be the same. The degree of privatisation may vary from nation to nation but, in many cases, services have been outsourced to private companies. Therefore, the mission owner (sector) and asset owner (i.e. a company) may be different.

One way of approaching cyber risk management is the Mission Assurance Process,[17] created for the US administration. The illustration of the Mission Assurance Process (Figure 2 below) has been slightly amended to make it more generically applicable yet detailed enough to be of direct value for nations wishing to strengthen the protection of their critical infrastructure.

The Mission Assurance Process contains three phases and aims to produce a risk decision concerning the threats and hazards facing a given element of critical infrastructure.

17 Based on (US) Department of Defense Directive 3020.40 (2016).

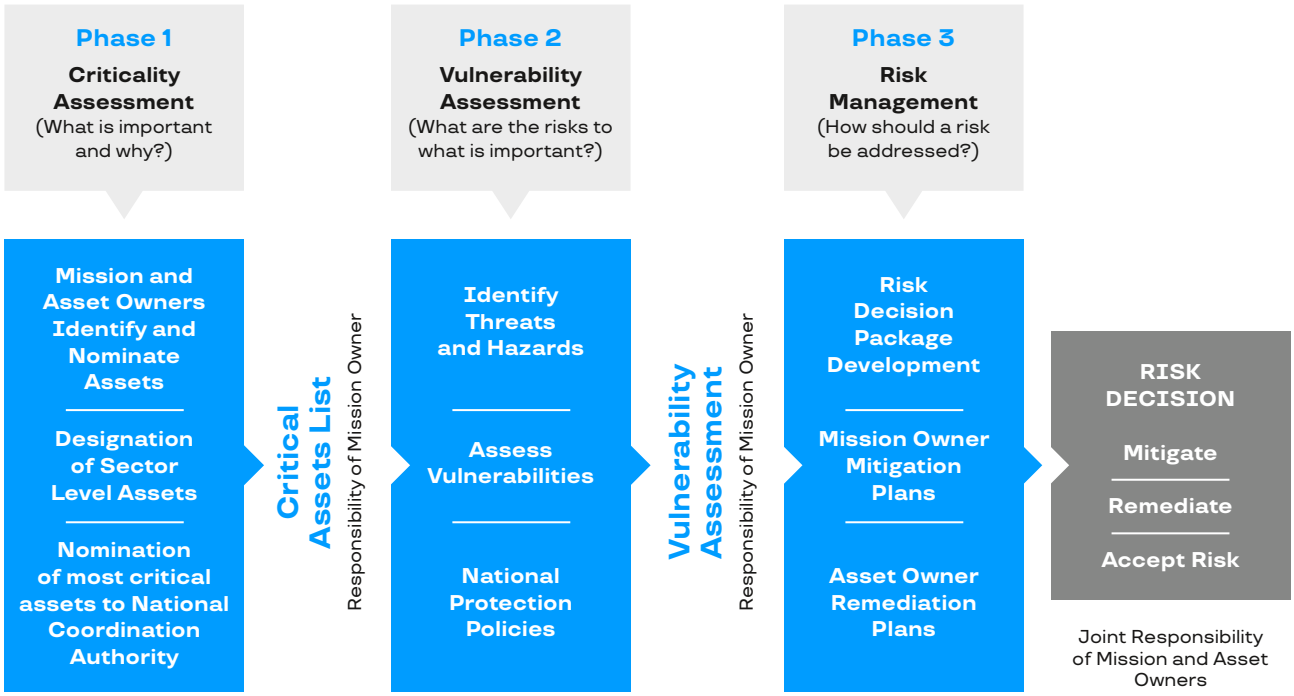


Figure 2: Mission Assurance Process[18]

The phases of the Mission Assurance Process are:

- **Phase 1** – Mission owners and asset owners make a Criticality Assessment determining what is important and why by identifying and nominating assets to a national coordination authority. The mission owner puts these assets on the critical assets list as the outcome of this phase.
- **Phase 2** – The asset owner identifies threats and hazards by determining what the risks are to what is important. The outcome of phase 2 is a vulnerability assessment.
- **Phase 3** – A plan for risk management is formulated by looking at how the risks should be addressed. The mission owner will determine what steps can be taken to mitigate the risk, and the asset owner will plan steps to address the hazards.

18 Figure 2 is based on Defense Information Systems Agency (DISA) illustration of US Department of Defense Directive 3020.40.

Thus, the outcome of phases 1–3 in the Mission Assurance Process is the formulation of a risk decision to either mitigate risks, remediate them, or accept them as a condition.

The Mission Assurance Process should form a part of strategic cybersecurity leadership, but it becomes readily apparent on examination of the content of the process that there is a need for a national coordination authority in which all sectors are represented. Mapping all the critical infrastructure and the interdependencies of different sectors would be a first step (i.e., determining which sectors rely on the services of others).

As Figure 1 illustrates, most critical infrastructure sectors are interdependent and, therefore, there is a great need for cross-functional coordination and collaboration. In many instances, the sectors' responses to risks are 'stove-piped', without sufficient coordination between sectors. Therefore, something more is needed: strategic cybersecurity leadership.

Ultimately, to quote the French author and pilot Antoine de Saint-Exupéry, 'A goal without a plan is just a wish'. In this context, there is a need for strategic engagement in cybersecurity in order to establish and drive the processes to set strategic-level goals for a nation and build bodies such as a national coordination authority.

How do we foster strategic cybersecurity leadership?

The word strategic implies the identification of long-term or overall national aims and interests and the means of achieving them. What is the vision for the nation, and what are the goals and objectives that support this vision? Speaking from the viewpoint of a democracy, it is fair to say that politicians' vision may only reach as far as the end of their term in office, which is not very conducive to strategic thinking. However, if the government could include the opposition in formulating clear, long-term, strategic goals for the nation, then there is a good chance of avoiding changes to national strategies every time power changes hands. The goals should remain the same regardless of which party is currently at the helm.

For nations that have not yet developed a comprehensive cyber strategy, many sources of guidance are available. The first place to get inspiration could be the Guide to Developing a National Cybersecurity Strategy (2nd Edition 2021). Under the overall coordination of the ITU, this guide has been developed by 20 partners from intergovernmental and international organisations, the private sector, academia and civil society. The guide is available for free at https://ncsguide.org/.

Section 5 of the guide deals with National Cybersecurity Strategy Good Practice and lists seven focus areas: 1) governance; 2) risk management in national cybersecurity; 3) preparedness and resilience; 4) critical infrastructure and essential services; 5) capability and capacity building and awareness raising; 6) legislation and regulation; and 7) international cooperation.

Consider governance. How does a nation operationalise this? The Guide to Developing a National Cybersecurity Strategy offers nine action points.

NINE ACTION POINTS

- Ensure the highest level of support (i.e. get the government on board)
- Establish a competent cybersecurity authority (responsibility for executing the strategy)
- Ensure intragovernmental cooperation (effective communication and coordination among government agencies)
- Ensure intersectoral cooperation (understand the interdependencies)
- Allocate a dedicated budget and resources (money, people, and materiel)
- Develop an implementation plan (how are the individual strategic aims achieved?)

The ITU's GCI measures actions taken by nations in terms of cybersecurity to tackle cyber risks by assessing their commitment to five pillars: legal, technical, cooperative, organisational and capacity building measures.

The GCI may complement other cybersecurity measures by enabling nations (governments, private industry, civil society and academia) to understand where action has been taken, what action may be insufficient and the landscape of successes.

Regional organisations may also be helpful in fostering strategic cybersecurity leadership in a nation. In the EU, for instance, the European Union Agency for Cybersecurity (ENISA) supports efforts to improve overall cybersecurity in the Member States at both the national and EU levels.

To help governments turn plans into specific action, institutions such as the nonprofit e-Governance Academy (eGA) in Tallinn, Estonia, have gone beyond just sharing good practices and have delivered digital transformation solutions in transitional societies, especially in Eastern and Central Europe, Asia and Africa. Still, the eGA has stressed that digital transformation is a strategic process that will have to be driven by governments.

Harvesting the benefits of the digital revolution and reducing risk requires strong and visionary strategic cybersecurity leadership and the courage to learn from others.

How do global engagements matter for national cyber resilience?

Anna-Maria Osula

Digital and Cyber Diplomacy,
Estonian Ministry
of Foreign Affairs
Senior Researcher,
Tallinn University
of Technology School
of Information Technologies[19]

While cybersecurity is generally seen as an actor's ability to protect against and prevent cyber threats, resilience refers to the ability to mitigate the damage resulting from an incident and being able to continue operations. In today's world, both elements – cybersecurity and cyber resilience – are relevant for the functioning of our societies and allow people to trust, use and benefit from innovation, connectivity and automation.

19 Any views or opinions expressed in this article are personal and do not represent those of institutions or organizations that the author is associated with in her professional capacity.

National cyber resilience is not a distinct area of regulation or policy that can be easily separated from other domains. Instead, its development is directly connected with the policy and regulation of other areas, such as digitisation, digital identity, privacy, data protection, cybercrime, and the safety and security of our societies.

While it is clear that the integrity, availability and confidentiality of data and systems are an issue of strategic importance on a national level, considerations related to cyber resilience have also become an inseparable element of foreign policy. This means that building national cyber resilience is not an issue merely on domestic agendas but requires cooperation among states, regional and international institutions, and the multistakeholder community.

> **Building national cyber resilience is not an issue merely on domestic agendas, but requires cooperation among states, regional and international institutions, and the multistakeholder community.**

Countries have realised that strengthening and expanding international, regional and multistakeholder partnerships allows them to promote their values and vision for cyberspace, support economic interests and digital transformation, and negotiate over cyberspace rules, norms and principles essentially aimed at preventing conflict. Developments in ICTs have clear implications for not just peace and security but also human rights and sustainable development, thereby affecting the very foundations of modern societies.

Why cyber diplomacy?

Cyber diplomacy focuses on advancing state interests in cyberspace by employing diplomatic tools. At the core of cyber diplomacy, states are negotiating over various issues pertaining to cyberspace, such as norms of state behaviour, the role of international law, confidence building measures and capacity building. By committing to strengthening global capacities to address cyber threats, countries contribute to increasing global cyber resilience.

The prime examples of current multilateral venues are the United Nations Open-Ended Working Group (OEWG), the Ad Hoc Committee on Cybercrime, and the Council of Europe and its work on the Budapest Convention on Cybercrime. Countries are also discussing options to establish a permanent institutional framework – Programme of Action – for pulling together the UN efforts to support the capacities of states to implement their commitments in their use of ICTs.

Regional organisations active in this domain include the Organisation of Security and Cooperation in Europe (OSCE) (notably its efforts on cyber condidence building measures), the African Union, the Association of Southeast Asian Nations (ASEAN), the Organisation of American States (OAS), and the Shanghai Cooperation Organisation's efforts on cooperation in the field of ensuring international information security. Examples of multistakeholder platforms include the Paris Call and the Global Forum for Cyber Expertise (GFCE).

As a clear trend, countries around the world are paying more attention to cyber diplomacy. Regional and international venues have become increasingly active and ministries of foreign affairs are appointing cyber, digital and tech ambassadors to represent national priorities in cyberspace. Although traditionally diplomacy is seen as a strictly state-to-state activity, the nature of cyberspace necessitates the involvement of industry, academia and civil society actors in these discussions.

Norms of responsible state behavior in cyberspace

Norms of responsible state behaviour reflect commitment to an agreed-upon framework that, while not legally binding, is generally respected and followed. Norms play an important role in representing the expectations and standards of the international community, increasing predictability, and reducing the risk of misperceptions, thus contributing to the prevention of conflict. By agreeing on a common set of rules, norms and principles for responsible state behaviour, the international community can also assess the activities of states. Importantly, the main aim of such norms is to provide additional specific guidance on what constitutes responsible state behaviour in the use of ICTs, and not to replace or amend the already existing rights and obligations of states under international law.

The UN has been and still is the most active platform for discussing norms for states in cyberspace. Building on the norms agreed upon by several iterations of the UN Group of Governmental Experts (GGEs) since 2005 and endorsed by the UN General Assembly,[20] a cyber stability framework is currently being discussed under the auspices of the OEWG and is expected to continue until 2025.

The agreed norms address effective cooperation, mitigation and prevention of cyber incidents. For example, states have agreed that their territory should not be used to conduct malicious cyber operations against other countries. They have also agreed to work on protecting supply chain security and reporting ICT vulnerabilities. The 2021 OEWG report reiterated the importance of protecting critical infrastructure and expressed the consensus agreement that states should not conduct or knowingly support ICT activity that violates their obligations under international law and intentionally damages or otherwise impairs the use and operation of critical infrastructure that provides services to the public.

In addition to global negotiations, important efforts to substantiate norms and support their implementation are also underway at the regional and national levels. Examples include the ASEAN and the OAS. By engaging in these discussions, a country can voice its needs and interests, and ensure they are considered in the process.

How does international law guide state behavior in cyberspace?

International law forms the foundation for stability and predictability between states as it reflects legally binding agreements over accepted state behaviour. This is equally true in cyberspace. International law also offers options for legal responses to cyber operations targeted against a state. In particular, international law plays an important role in protecting small nations that lack military power or resources. Arguably, the predictability provided by international law may potentially act as a deterrent against possible malicious cyber operations.

Based on consensus reports concluded by GGEs since 2013, the UN has consistently affirmed the applicability of international law, and in particular the UN Charter, in cyberspace. The consensus on the applicability of international law in cyberspace was reiterated in the 2021 OEWG report.

By now, the discussion on international law has shifted from asking whether international law applies to cyberspace to asking how it applies. The 2021 GGE report noted the application of specific principles, such as respect for sovereignty, non-intervention in the internal affairs

20 Groups of Governmental Experts (GGEs) have been formed in 2004/5, 2009/10, 2012/13, 2014/15, 2016/17 and 2020/21, and have issued consensus reports in 2010, 2013, 2015 and 2021 to examine the existing and potential threats in cyberspace and possible cooperative measures to address them. These reports have also been presented to the UN General Assembly for endorsement.

of another state, refraining from threats or the use of force, and the responsibility of states to meet their obligations regarding internationally wrongful acts. Notably, the GGE reports have also underlined the applicability of international humanitarian law and the human rights regime in cyberspace. In addition to the UN First Committee discussions, the UN Third Committee is negotiating a treaty in the Ad Hoc Committee on Cybercrime.

> **International law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace, security and stability in the ICT environment.**
>
> 2021 UN OEWG Report

With some exceptions (such as the Council of Europe's Budapest Convention on Cybercrime), there are currently no international agreements specifically regulating state behaviour in cyberspace. Since international law is made by states, state practices and national declarations on the interpretation of international law applicable to cyber operations are valuable for increased legal certainty and transparency. However, currently only a fairly limited number of states have published comprehensive views on international law in cyberspace. Therefore, states are encouraged to develop and share with international partners their national views and assessments of how international law applies to their use of ICTs in the context of international security. Recommendations on norms, rules and principles of responsible state behaviour complement legal norms and provide further guidance for their application.

Confidence building measures: Practical actions and mechanisms to form trust

Voluntary state engagements focusing on transparency, cooperation and stability in the relationship between states – the implementation of confidence building measures (CBMs) – can contribute to preventing conflicts, avoiding misperceptions and misunderstandings, and reducing tensions between states. Together with the other pillars of the framework for responsible state behaviour, CBMs can help build a common understanding among states, thereby contributing to a more peaceful international environment. CBMs can be implemented as the first step in building trust and clarity among different actors and thereby laying the ground for additional agreements in the future.

The United Nations plays a crucial role in the discussions on the substance and implementation of cyber-specific CBMs. The aforementioned GGE and OEWG reports have proposed various CBMs that countries are invited to undertake on top of the existing national and regional mechanisms and structures. CBMs may include technical, organisational, policy, strategic and legal capacity building activities aimed at introducing, developing and assessing a predefined knowledge set related to ICT security for international participants. For example, the 2021 OEWG report encouraged Member States to nominate a national point of contact (POC) for, inter alia, diplomatic, policy, legal and technical exchanges, and incident reporting and response. In addition to being a CBM in itself, the POC network may be useful for the implementation of other CBMs and prove invaluable in times of crisis.

Notably, regional organisations such as the OSCE, ASEAN and the ASEAN Regional Forum, and the OAS have contributed to the efforts to develop CBMs in specific contexts, striving to enhance their implementation, raise awareness and share information. The 2021 OEWG report concluded that because not all states are members of a regional organisation and not all regional organisations have CBMs in place, such measures are complementary to the work of the UN and other organisations to promote CBMs.

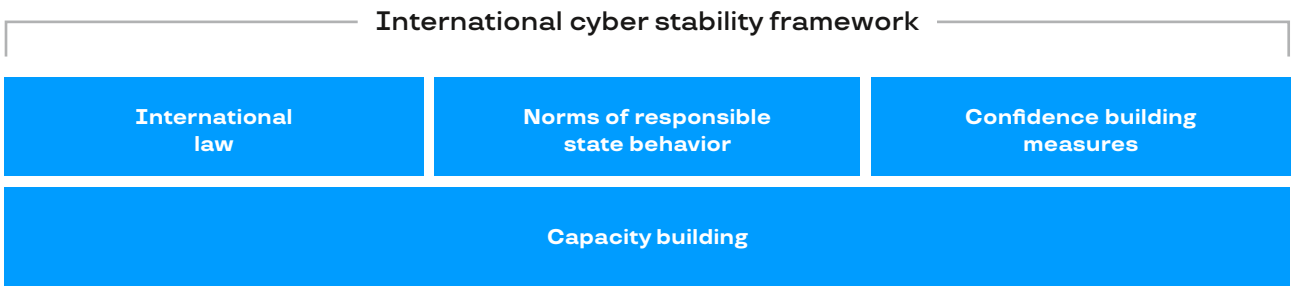


Figure 3: International Cyber Stability Frameworks

Engaging in capacity building

Finally, international cybersecurity depends not only on a shared commitment to the rules of the game, but also on the capacity of states to fulfil their commitments. Importantly, national cyber resilience depends on various technical, policy, organisational and legal measures. This resilience contributes directly to the regional and global ability to prevent or mitigate the impact of malicious ICT activities, thereby allowing countries to fully enjoy the benefits of ICTs. In the context of cyber diplomacy and the framework of responsible state behaviour, states also benefit from capacities that support participation in and contribution to international negotiations, upholding commitments, and exercising their rights.

The 2021 OEWG report introduced several principles that should guide capacity building in relation to state use of ICTs in the context of international security. Capacity building should be a sustainable reciprocal process comprising specific activities by and for different actors. These activities should have a clear purpose and be result-oriented, evidence-based, politically neutral, transparent, accountable and without conditions. Importantly, capacity building should support the shared objective of an open, secure, stable, accessible and peaceful ICT environment, and be undertaken with full respect for the principle of state sovereignty. It should be tailored to specific needs and contexts, demand-driven, and based on mutual trust. Crucially, capacity building must respect human rights and fundamental freedoms, and be gender-sensitive, inclusive, universal, and nondiscriminatory.[21]

Capacity building efforts are ongoing at the national, regional and global levels. Examples of these are conferences, seminars, training courses and materials, consulting efforts, assistance to countries for specific tasks and priorities, and the exchange of best practices. To tap into available capacity building activities and resources, information about these efforts can be accessed via national coordinating bodies, dedicated entities, and the abovementioned thematic and international organisations. Some global organisations, such as the GFCE, aim to strengthen cyber capacity by offering an overview of various capacity building activities and coordinating requests for cyber assistance and offers of support.

21 See the 2021 OEWG report's section on capacity building for a full list of principles.

What can we learn from the revised European approach to critical infrastructure cybersecurity?

Martin Švéda

Head of Private Sector Regulation Unit
Czech National Cyber and Information Security Agency

European countries have paid increasing attention to cybersecurity in the past 15 years. Many EU Member States addressed the issue in national legislation, but for a long time, there was no tool that would harmonise cybersecurity requirements across the region. To fill this gap, the EU-wide Directive on Network and Information Systems Security (NIS Directive)[22] came into force in 2016. This piece of legislation set a goal that all countries in the European Union must achieve, leaving it up to individual countries to formulate national legislation to achieve these goals.

22 Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148

Notwithstanding its achievements, a review of the NIS Directive has revealed inherent shortcomings that prevent it from effectively addressing contemporaneous and emerging cybersecurity challenges. In 2020, the European Commission launched a revision of the NIS Directive to incorporate the practices and lessons accumulated over the previous four years. Based on a survey, reports and country visits by the European Union Agency for Cybersecurity (ENISA), the European Commission introduced seven main objectives that it would like to achieve in the revision as a response to the most relevant issues identified:

- Cover a larger portion of the economy and society (more sectors)
- Systematically focus on larger and more critical players within sectors
- Align security requirements across Member States
- Streamline incident reporting obligations
- Align provisions on national supervision and enforcement
- Greater operational cooperation, including on crisis management
- Align with the proposed Resilience of Critical Entities Directive

The reasons for setting these objectives are to overcome the existing fragmentation of obligations across Member States, support the further development of the Digital Single Market, and enhance sectoral implementation, cross-border and cross-organisational cooperation, and information sharing between stakeholders as a key to cyber resilience.

At the time of writing this article, there is already a political consensus on the content of the revised Directive (NIS2 Directive) and its publication is presumably only a few weeks away. We can therefore already look at whether and how these objectives have been achieved and use this to illustrate the essence of future harmonised cybersecurity regulation in the European Union.

New sectors, more services

One of the biggest changes is the overall change in the approach to determining the scope of regulation. The original NIS concept was based on the premise that regulation should target organisations in which a cyber incident could significantly disrupt a service that is important to the state. In other words, the first NIS Directive emphasised the impact aspect – the entity is as important as the impact its service may have on society. Therefore, Member States generally aligned with these requirements by setting criteria to identify such services, with the aim of assessing whether a service is essential.

The NIS2 Directive, however, takes a different approach by including all medium and large organisations[23] that operate within specified sectors or provide key services as defined in its scope. The reason for this approach is that the original approach of the NIS Directive led to a wide divergence between Member States and did not achieve the desired level of harmonisation. In addition, in some cases, it did not systematically cover all the areas needed. This change of approach prioritises harmonisation and elimination of Member State divergences over the rationale of public regulation of cybersecurity, ensuring state oversight of services that are truly important to society and maintaining freedom where state oversight is not needed. While the change is controversial for this reason, the new approach is now the agreed basis for the NIS2 Directive's handling of what it calls 'regulated organisations' – the infrastructure and service providers that shoulder obligations under the directive.

23 According to the definitions given by the Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF

The practical impact is that the new approach will lead to a major increase in the number of regulated organisations in most, if not all, Member States. This increase in the number of regulated organisations will also place much greater demand on the capacity of supervisory bodies and might lead to the involvement of more such entities.

> The new approach will lead to a major increase in the number of regulated organisations and place greater demands on the capacity of supervision bodies.

The legislation will also apply to new services that have not been subject to regulation before. Examples include the hydrogen, waste management and food industries. This increase could result in two different outcomes. The first is an increased demand to develop cybersecurity rather than overlook it. The second is paralysis, with national competent authorities being overwhelmed as they are expected to provide a wide range of services to regulated organisations, including incident handling.

More specific security requirements

The obligation to implement preventive security measures and to report cyber incidents to the relevant (state) authorities is the essence of public regulation of cybersecurity. The NIS Directive required Member States to ensure regulated organisations take appropriate and proportionate technical and organisational measures to manage security risks posed to their systems, with the aim of preventing incidents or minimising their impact. If an incident does occur, which can never be completely prevented, the law imposes an obligation that it be reported without undue delay if it has a serious impact on the continuity of the services. This approach, which is similar to the obligations under the General Data Protection Regulation, gave Member States a high degree of flexibility in how they approached the implementation of security measures and incident reporting. Of course, Member States generally relied on existing standards such as ISO/IEC 27001 or the National Institute of Standards and Technology (NIST) Cybersecurity Framework, but if they did not accept these standards in their entirety, they could modify the details of the requirements as they deemed appropriate.

The NIS2 Directive aims to reduce divergence among Member States. The directive specifies a list of topics to be covered when imposing appropriate and proportionate risk management measures. These include areas such as risk analysis, incident handling, and cybersecurity governance within organisations (which involves management responsibility for organisations' cybersecurity), which many Member States already address in their legislation. A fundamental innovation in the NIS2 Directive is the power of the European Commission to adopt implementing acts that lay down the technical, methodological and sectoral requirements, as necessary, of the security measures. This is a significant interference with the freedom of Member States to determine security measures for regulated organisations.

> The NIS2 Directive specifies a list of topics to be covered when imposing appropriate and proportionate risk management measures.

Stricter incident reporting

The same is applicable to incident reporting. The NIS2 Directive maintains the obligation to report incidents with a significant impact on the provision of service. Let us leave aside the fact that 'significant impact' is difficult to define and, more importantly, difficult to recognise at the onset of or during the incident.

A special three-step incident reporting process has been projected, which includes:

- **Early warning phase:** Initial information about the incident must be reported without undue delay and in any event within 24 hours of having become aware of the incident.

- **Incident notification phase:** An initial assessment of the incident, its severity and its impact must be shared with the designated national cybersecurity authority without undue delay and in any event within 72 hours after having become aware of the incident.
- **Final report phase:** A detailed description of the incident, its severity and impact, the type of threat or root cause, and the mitigation measures applied must be completed not later than one month after the submission of the incident notification.

> Meeting these obligations will certainly place new challenges on Member States, and the process will have to be managed well.

This process is complemented by intermediate status updates at the request of the national cybersecurity authority. Meeting these obligations will certainly place new challenges on Member States, and the process will have to be managed well. Otherwise, it may very easily overburden the regulated organisations. As with security measures, the European Commission will have a significant role in incident reporting, as it has been given the power to adopt implementing acts further specifying the type of information, the format and the procedure for notification, as well as acts specifying the cases in which an incident shall be considered to be significant.

Unified crisis management

The new scope of legislation also affects cyber crisis management. Several Member States already have some form of interconnection between national crisis management and cybersecurity rules. They have either directly merged the requirements for entities subject to cybersecurity with crisis management rules or have created linkages between them. The NIS2 Directive itself addresses this issue in a similar way – organisations falling under the proposed crisis management directive (Resilience of Critical Entities Directive) are automatically also regulated organisations under the NIS2 Directive. This approach certainly appears logical, as cybersecurity is not a special issue anymore today and critical entities providing vital services to citizens are the ones that should be dealing with it in the first place.

One of the objectives of the new legislation was also a more operational approach to cooperation, including on crisis management. The NIS2 Directive, therefore, sets more specific requirements for national as well as international cooperation and maintains several already existing platforms, including the Cooperation Group for Member State cybersecurity authorities and the computer security incident response teams (CSIRT) network for national computer security incident response teams. It also looks to further develop platforms such as the EU Cyber Crisis Liaison Organisation Network (EU-CyCLONe) to improve coordinated management of large-scale cybersecurity incidents and crises.

> The NIS2 Directive sets more specific requirements for national as well as international cooperation and maintains several already existing platforms.

The role of the state

The NIS2 Directive identifies various institutions responsible for meeting these obligations in the EU Member States, such as competent authorities, CSIRTs or single points of contact. In some Member States, these are different entities, in others, a single organisation takes on all these roles. Either way, in light of the abovementioned requirements, the NIS2 Directive places new and higher demands on these organisations, especially in terms of cooperation.

Summary

Modern society is increasingly dependent on cyberspace and its proper functioning. European society has historically been characterised by, among other things, a strong emphasis on individual freedoms, privacy and data protection. From this perspective, the European Commission is following its stated objectives and the NIS2 Directive, although still following its original orientation, introduces more precise and strict requirements that aim to make essential services more safe and secure.

Building cyber resilience through crisis preparedness

Hannes Krause

Country Coordinator for Mauritius, Cyber Resilience for Development (Cyber4Dev); former Head of Strategic Communication, Estonian Government Office

A very important cybersecurity question countries ask is what clear and measurable steps can be taken to prepare for a cyber crisis. In a world with a growing number of digital dependencies, it is naturally impossible to avoid cyber incidents altogether. The focus, therefore, should be on improving the cyber resilience of societies, and there are some proven ways to do this.

The NCSI outlines a set of clear-cut baselines for cyber crisis preparedness. However, there are still a variety of ways to organise those baseline components, especially in smaller states where the lack of resources is often a significant constraint. This article looks at the key elements of cyber crisis preparedness and offers practical examples from several countries.

Innovating cyber resilience

With conventional war having returned to Europe in a particularly atrocious way, a country that can serve as an example of a resilient society is obviously Ukraine. Even during high-intensity conventional war, Ukraine has made intentional efforts to keep its government and society, including the digital components that uphold public services, functioning and innovating. The means of achieving the kind of cyber resilience we have seen in Ukraine in 2022 is something to be researched in years to come, and there are many lessons to be learned from Ukraine on how to build a resilient society. Some of Ukraine's solutions are already being adopted in other countries – for example, Estonia, no doubt an advanced digital society, has decided to use Ukraine's Diia application, which facilitates all kinds of interactions between the state and individuals, as the basis for piloting its own national mobile application. This is surely just the first example in this direction.

But countries looking to prepare themselves for uncertain futures without conventional war ever reaching their soil also need guidance, and for that, the NCSI provides benchmarks that can help a country be ready to face a worst-case event.

Coordination is key to preparedness

In the recent discussions at the Tallinn Digital Summit 2022, the strength and clarity of cybersecurity governance mechanisms were repeatedly outlined as preconditions for cybersecurity in a global crisis scenario. With digitalisation affecting all aspects of society, cybersecurity is the responsibility of every sector and every person, even where the lead responsibility has been assigned to a particular entity. The same remains true for crisis preparedness. Therefore, establishing a national coordinating governance committee for cybersecurity is an elementary step for all countries that take cybersecurity seriously. Besides ensuring coherent day-to-day management of national cybersecurity, such a national cybersecurity committee should also have a central role in crisis preparedness and in managing the cyber aspects of any ongoing crises.

However, everyone who has participated in such governance committees knows how easily they can lose sight of strategic cybersecurity considerations when political or bureaucratic battles taking place outside of the committee have a major influence on its discussions. So it is valid to ask whether there are any ways to avoid such a situation and ensure a basis for impartial leadership and management of the committee.

STEPS TO SUCCESSFUL CYBER CRISIS PREPAREDNESS

- **Set up strong and clear cybersecurity governance mechanisms** that serve the country well in peacetime – and can sustain it in a crisis.
- **Establish a standing coordination body and regular mechanisms** to coordinate the cybersecurity activities and responses of different actors.
- **Prepare for crises by planning for them**, at both the organisational and national levels. Analyse cyber risk scenarios and establish a crisis response plan. Test and improve it through regular exercises.
- **Invest in network building**. A network of trust, involving organisations and experts from both the public and private sectors can provide the amplification that helps limit damage and recover quickly in crises. Make sure their tasks and authority are clearly established beforehand.

Mauritius is an example of a country with mature cybersecurity. At the end of 2021, it adopted a new cybersecurity and cybercrime act. Based on this law, a new national cybersecurity committee was created, with some interesting aspects because of which this mechanism and its future operations might be looked at more closely. First, the mandate of this committee comes straight from the head of the government: the Prime Minister is assigned the authority to appoint the chairman of the committee, without specifying the exact office or person holding that responsibility. Although the cybersecurity domain in Mauritius is governed by the Ministry of IT, Communication and Innovation, this governance system gives the committee a much wider mandate, which can insulate it from the bureaucratic infighting that happens in all governments. After the initial meetings of the new governance committee, the chairmanship was given by the Prime Minister not to any of the administrative units represented in the committee, but to the CEO of a domestic cybersecurity company. A national cybersecurity committee chaired by a private sector representative with a prime-ministerial mandate can facilitate innovation and public-private partnerships, and when this globally distinctive governance mechanism begins operations, it will serve as a valuable case to learn from.

'Plans are nothing, planning is everything'

An important function of such governance and coordination committees should also be to oversee the creation, maintenance and coherence of national cyber crisis plans, so that they can act as a clearinghouse in case of conflicts between the crisis preparations of different governmental entities, in particular where it concerns the availability of personnel and other resources.

A cyber crisis plan might address, among other matters, the criteria to decide whether a cyber incident is significant enough to escalate to a higher level and involve resources beyond normal operations. It should identify the resources and skills that might be needed for crisis resolution and explain how to activate them. It should also outline the tasks and responsibilities of different actors and the related decision-making processes. Further, it should lay out the processes for information sharing and coordination. Other aspects such as public and international communication may also be considered.

> A cybersecurity coordination committee tasked with overseeing the coherence of national cyber crisis plans can ensure that tensions between sectoral activities and resources are addressed, and press entities across sectors to draw up their crisis plans in the first place.

One might ask whether such crisis plans need to be adopted for all governmental units, or if a national-level plan will suffice. However, this question does not approach preparedness correctly. Planning for the management of cyber incidents is a critical necessity for any organisation, be it a private company or a governmental body.

At the organisational level, there is value in the planning process itself that should not be overlooked. The key importance of crisis plans is not necessarily that they are faultless in their final form – the process leading to them is itself illuminating. 'Plans are nothing, planning is everything', says a famous military quote that very much holds true for cyber preparedness. The process of creating and finalising a crisis plan is something that helps every organisation – be it a company, a ministry or a country – to think through its vital processes and their weakness, and plan for ways to mitigate those. Having a crisis response plan means being prepared to respond quickly, contain the damage and restore operations. Then, even if the national-level cyber crisis plan is imperfect in form or function, a well-functioning national cybersecu-

rity committee with its clearinghouse role can bridge the gaps as needed.

> Cybersecurity exercises are a proven way of building, training and assessing the national operational response network.

Another critical element of national readiness for cyber crises is the actual operational networks of experts working in national cybersecurity institutions. This, too, should be developed and tested in times of stability to ensure that it is ready when a crisis hits. Participation in or organisation of cybersecurity exercises is a proven and clear-cut way to build, train and measure that network. Again, Mauritius offers a good example for the African continent, having already hosted two African Cyber Drills, the latest of which drew 42 CSIRT teams from 41 countries in September 2022. As the next step, Mauritius is planning to organise a technical live-fire exercise in 2023, together with the EU-funded Cyber Resilience for Development (Cyber4Dev) programme, in which technical teams from many developing countries can participate.

Preparing and engaging a crisis reserve

After setting up a clear good governance mechanism – with both organisations and crisis plans established – and strengthening a good operational network through cyber exercises, another layer of cyber crisis readiness can be built by developing a reserve system of cyber experts to whom governmental cyber institutions can turn in case of large-scale cyber incidents. An operational cyber reserve would follow the same logic as reserves in other security realms – they are a layer of support for national cybersecurity institutions for times when a large-scale incident has taken place in the country. Such reserves can provide significant relief to the government cyber incident response teams and crisis management efforts and help contain damage and speed up recovery. Any cyber crisis will create a sudden spike in demand for operationally ready expertise, so it is wise to prepare for such situations beforehand.

Many countries have set up some form of cyber reserves. For example, Estonia developed the concept of a Cyber Unit and established it within its voluntary defence organisation, the Estonian Defence League, right after the large-scale cyberattacks that hit the country in 2007. Considering the growth and maturation of the country's digitalisation, and looking at the current security environment in Europe, the country decided in 2022 to strengthen its readiness by creating a civilian cyber reserve around the national cybersecurity agency, the Estonian Information System Authority (RIA), following a similar model. The civilian reserve is a rapid-response fallback consisting of civilian experts working in the IT powerhouses of the Estonian government who are ready to react and support the national computer emergency response team, in accordance with their expertise and availability, within 24 hours to help resolve an ongoing crisis.

> We have long realised that the only way to keep our information systems secure is to engage the wider infosec community, and to best achieve this, the notion of adding a civilian cyber reserve level to our risk mitigation mechanisms was born.
>
> Gert Auväärt,
> Director of Cybersecurity at RIA

The revised readiness system removes any kind of military command structure from the process of provisioning cybersecurity expertise and assistance around the national CSIRT in Estonia, leaving it to the Estonian Defence League Cyber Unit the task to react during times of conflict, when the need for assistance is even greater and may last much longer, as the experience in Ukraine has shown. The first exercises for this renewed crisis management structure will be conducted in the second half of 2022. The government will also invest in the civilian cyber reserve by giving its members free access to world-class training. As with the previous model, Estonia is likely to evaluate the experience of this multilayered reserve structure and keep improving it in years to come.

Where to start with cybersecurity development?

Cybersecurity support for digital transformation

Merle Maigre

Cybersecurity Program Director, e-Governance Academy

Digital transformation has become a key driver of economic growth and societal change. A state's cyberspace, its digital society and e-services, form a complex environment that cannot safely exist without solid cybersecurity protection. The logic is simple: people use digital services that they trust, and they can only trust services that are secure. Therefore, governments and organisations have a responsibility to develop and maintain cybersecurity capacities that ensure the safe usage of digital services

The e-Governance Academy provides expertise on the security aspects of digital transformation and the trustworthiness of the national cyberspace. In line with the NCSI, eGA is focusing on the organisational, regulative and technical aspects of cybersecurity. All this requires strong political will, resources, supportive legislation, change management and implementation.

Developing policy and regulation

The eGA's support for developing policy and regulations can mean the assessment of a country's cybersecurity maturity, following the criteria of the NCSI, adjusting cybersecurity legislation or, more generally, supporting the establishment of a functional cybersecurity governance model. There are several aspects of establishing strong cybersecurity governance: a national cybersecurity strategy must ensure the engagement of all possible parties – governmental, non-governmental and industry – in a multistakeholder cooperation model and formalise and map interagency cooperation mechanisms for the protection of critical infrastructure. Laws and regulations are needed to translate concepts and strategies into rules, principles, rights and obligations for individuals, organisations and society at large. Legislation must establish an adequate legal basis for the cybersecurity of critical infrastructure to ensure that cybersecurity measures are implemented, significant incidents are reported, and accountability and enforcement mechanisms are in place.

The eGA can support the development of policy and regulations in several ways. We assist countries through the process of preparing national cybersecurity strategies and action plans, advise and coach them on drafting cybersecurity legislation, and conduct cybersecurity maturity assessments based on the NCSI methodology. Regardless of the road taken, one thing is certain – a successful cybersecurity policy with an institutional framework and governance model that leads to effective implementation is predominantly a matter of political will. A high-level political commitment to cybersecurity reforms and increased prioritisation of cybersecurity needs to be adopted at the government level and across public administration. Political leaders need to stay engaged and commit time, budget and political capital to the cause of cybersecurity.

Building cyber incident management skills

To help states strengthen their cyber incident management capacities, eGA conducts training, workshops and exercises. Providing the right training to ICT and cybersecurity staff is more essential than ever and it is not enough to take a merely theoretical approach. The current tidal wave of technology is constantly opening up new opportunities, but also making skills obsolete more quickly, so it is essential to keep up with the evolving environment by learning new skills that truly build human capital and equip for the future. Investing in training and education is probably the best kind of investment one can make for incident prevention and response.

Cybersecurity needs to be constantly exercised to maintain readiness. The eGA organises cybersecurity exercises to develop comprehensive cyber capacity skills at the technical level, as well as to raise awareness at the managerial level of the effects that cyber incidents can have. Usually, these exercises simulate the real-world operations of an organisation under cyberattack. The exercises last from a couple of hours to a few days, and include initial familiarisation, hands-on experience phase and evaluation. Participants work in teams on several issues at a time.

Red-on-blue technical exercises provide a safe setting for participating teams to stress test their processes and challenge their capabilities. They do so in responding to real-world cyber incidents through a realistic simulation in a sandbox environment. The red team imitates real-world cyberattacks that can hit an organisation. The blue team aims to defend, change defence mechanisms and regroup to make incident response quicker and stronger.

Red-on-blue incident response training sessions typically take place in a cyber range, which serves as a virtual training ground for cyber exercises. It is a powerful ICT system with a unique set of characteristics, hardware and software that imitate actual computer networks and data traffic. In this simulated exercise environment, all technology, infrastructure and testbeds are specifically crafted in virtual environments. This setting allows extensive cyber defence practice and testing of the resistance of IT systems without hampering live systems. The cyber range capability can be securely accessed remotely.

Cybersecurity exercise and training tools often lack visualisation. Yet, it is an aspect that most impacts how security teams interact with and communicate data. The ability of a decision-maker – be it a user, incident responder or manager – to digest the information is a critical measure of success. Visualisation is most effective when it is used to put data in context. Good visualisation provides an overview of the structure and state of the exercise environment and helps viewers monitor exercise proceedings. With this approach, different factors in cyber exercises – defence and attack, success and failure – become traceable and easy to evaluate. Evaluation not only provides measures of effectiveness and performance, but also offers an improved understanding of domain-specific concerns (network operations, forensics, threat monitoring), tasking (data analysis, decision-making, communication), and work style (individual or collaborative, peer-to-peer or hierarchical).

Cybersecurity awareness-raising

Although cybersecurity is one of the most important challenges faced by governments today, public awareness often remains limited. Almost everybody has heard of cybersecurity and its importance, however, the behaviour of citizens does not always reflect a high level of awareness. Cybersecurity is essential for individuals and for public and private organisations, yet it is often difficult to observe secure practices.

The eGA supports raising cybersecurity awareness through recommendations and advice about better cybersecurity communication. Based on cooperation with ENISA, eGA has identified good practices of EU Member States for organising awareness raising activities, measuring their effectiveness and ensuring appropriate outreach. eGA can share the challenges and lessons learned from the design of such activities and propose recommendations for improving cybersecurity awareness in society, considering all the above elements.

> **Digital security is not an expense but an investment.**

In today's digitally dependent society, people are the most important factor. And here the rule is simple: irrespective of our jobs, our age or our level of responsibility, we all need some technological literacy if we want to not only function in a digitised society, but also make sure we do not create risks to our own or others' assets through our behaviour. In Estonia, all public officials regularly have to undergo cyber hygiene courses to learn about the changing nature of cyber threats and about secure behaviour.

In many countries, the government's responsibility for cybersecurity is decentralised, divided among ministers, ministries and institutions, meaning that investment and prioritisation of cybersecurity vary significantly. It is important to keep in mind that digital security is not an expense, but an investment. The national government as a whole has a duty to make sure that the environment is safe and secure, and that the tools to ensure such safety are effective, adequate and lawful.

eGA cybersecurity services

Contact us at

Let's develop and strengthen your national cybersecurity capacities in the areas of...

Cybersecurity governance and policy

- Cybersecurity maturity assessment
- National cybersecurity strategy and action plan
- Organizational framework
- Cybersecurity crisis management system
- Processes, procedures and policies
- Executive-level cybersecurity exercises

Cybersecurity legal framework

- Legislative gap analysis and revision, including harmonization with EU law
- Development of cybersecurity legislation
- Legislative impact assessments
- International law and cyber norms

Cybersecurity of critical information infrastructure

- Conceptualizing and mapping critical information infrastructure (CII)
- Baseline cybersecurity frameworks
- Cyber risk assessments and continuity plans for CII operators

Cyber incident response

- Skills, gaps and needs assessment
- National CSIRT organizational framework and community building
- CSIRT technical capacity and professional training
- Technical cyber range-based cybersecurity exercises

Cybersecurity awareness-raising

- Executive tabletop exercises
- Design of awareness-raising programs
- Cybersecurity competencies in ICT curricula
- Awareness-raising activities

eGA offers assessments, consultation and coaching, workshops, training, and tabletop and hands-on exercises to support you in your digital transformation journey.

Contributing to the NCSI

Radu Serrano
Project Manager, NCSI Data Lead,
e-Governance Academy

Even though we have discussed national cybersecurity throughout this publication, it is not a siloed venture. International and regional cooperation on this topic is a necessity to stay at the forefront of threats in cyberspace. Our own NCSI could not have made it this far without the help of our international partners and country contributors.

The NCSI team would like to thank everyone who has contributed to the development and evolution of the NCSI. We also would like to acknowledge the multitude of country contributors, whose volunteer effort and dedication allow us to keep the index up to date as much as possible.

CONTACT US!

If your country does not appear in the index, or if the information on it is outdated or incorrect and you can provide the relevant evidence, please contact us at ncsi@ega.ee.

Contributors

Henrik Beckvard

Henrik Beckvard has an army infantry officer and legal background. Since September 2018, he has served as a researcher in the Strategy Branch of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia. Henrik is on the team preparing the strategic track for the cyber defence exercise Locked Shields, focusing on decision-making at the strategic level. He also serves as the CCDCOE Course Director for the Critical Information Infrastructure Protection Course and, together with colleagues from the CCDCOE conducts the flag officer-level Executive Cyber Seminar, which aims to introduce participants to the cyber domain and explore its impact on today's decision-makers.

Kadri Kaska

Kadri Kaska joined the eGA in the spring of 2022, having previously served at the NATO CCDCOE as a cybersecurity legal and policy researcher, and head of its Law Branch. Her research there mainly focused on national cybersecurity strategies and governance frameworks, as well as on state cyber activities. Seconded to Estonia's Information System Authority in 2017–2018, Kadri worked with cyber threat assessments, policy analysis and legal drafting; she was the lead author and editor of Estonia's annual Cybersecurity Assessments and a co-author of Estonia's Cybersecurity Act and Cybersecurity Strategy. Earlier, Kadri had served at Estonia's national communications and competition authorities as a legal adviser. She holds a master's degree in law from the University of Tartu and is currently studying behavioural science at the same university.

Hannes Krause

Hannes Krause has more than ten years of experience in formulating and implementing the cybersecurity policy of the Estonian government and has represented it on cybersecurity topics at the European Union and NATO. He has been the head of analysis and policy at the Estonian Information System Authority, playing a critical role in providing strategic-level reporting and analysis on different cyber incidents that had impacted Estonia. His last role with the government was to serve as the Head of Strategic Communication at the Estonian Government Office, with responsibility for planning and implementing governmental strategic and crisis communication, most notably during the COVID-19 pandemic. Since 2019, Hannes has also worked as the Indian Ocean Region coordinator in Cyber Resilience for Development (Cyber4Dev), an EU-funded cyber resilience capacity building project, where he has achieved the biggest results with Mauritius, which in 2022 became a Cyber4Dev Hub for Africa.

Merle Maigre

Merle Maigre is the Programme Director of Cybersecurity at the eGA. Previously she was Executive Vice President for Government Relations at CybExer Technologies, an Estonian firm that provides cyber training. In 2017–2018 Merle served as the Director of the NATO CCDCOE in Tallinn. Prior to that, she was Security Policy Adviser to Estonian presidents Kersti Kaljulaid and Toomas Hendrik Ilves. Merle has also served in the Policy Planning Unit of the Private Office of NATO Secretary General Anders Fogh Rasmussen. She is the Chairman of the Advisory Board of the Forum International de la Cybersécurité (FIC) and a member of the CCDCOE's International Advisory Board.

Anna-Maria Osula

Dr Anna-Maria Osula is currently working at the Estonian Ministry of Foreign Affairs in the Department of Digital and Cyber Diplomacy. She is also serving as a senior researcher at Tallinn University of Technology, where her research focuses on cyber diplomacy and international law applicable to cyber operations. She is also a research fellow at Masaryk University under the project 'Cyber Security, Cyber Crime and Critical Information Infrastructures Centre of Excellence'. Previously, Anna-Maria worked at Guardtime as a senior policy officer, and before that as a legal researcher at the NATO CCDCOE, undertaking projects on national cybersecurity strategies, international organisations, international criminal cooperation and cyber norms. In addition to a PhD in law from the University of Tartu, she holds an LLM degree in information technology law from Stockholm University.

Radu Serrano

Radu Serrano supervises and updates the NCSI database, and develops and manages other cybersecurity projects at the eGA. He has also contributed to the development and successful completion of e-democracy, technology, and smart governance projects in European Neighbourhood Policy (ENP), EU, and Western Balkan countries. Previously, Radu served at the Panamanian Ministry of Foreign Affairs and Ministry of Commerce and Industries, where he contributed to the content of international trade treaties, and assisted with the establishment of businesses in the Republic of Panama, respectively. He holds a joint Master's degree in Public Sector Innovation and e-Governance from the Katholieke Universiteit Leuven, University of Münster and Tallinn University of Technology, and is currently pursuing a PhD in Public Administration and Technology Governance.

Martin Švéda

Martin Švéda joined the Czech National Cyber Security Centre in 2017 after graduating from Masaryk University's Faculty of Law. He was part of the creation of the Czech National Cyber and Information Security Agency, where he is a lawyer focusing on national cybersecurity regulation. Since 2021, he has been leading the agency's private sector regulation unit. His main focus is on issues related to the interpretation of the Czech Act on Cyber Security and its implementing legislation, and he is involved in drafting amendments to the legislation. He is also currently coordinating the preparatory work for the amendment of the Act on Cyber Security in connection with the adoption of the NIS2 Directive.

Rotermanni 8, 10111, Tallinn, Estonia
+372 663 1500
ncsi@ega.ee | ncsi.ega.ee

NCSI is held and developed by
e-Governance Academy Foundation
Company code: 90007000