

# National Cyber Security Index 3.0

Methodology



### Contents

Purpose and scope	4
Methodology	5
NCSI data	6
What is new in version 3.0	7
1 Cybersecurity policy	8
1.1 High-level cybersecurity leadership	8
1.2 Cybersecurity policy development	9
1.3 Cybersecurity policy coordination	9
1.4 National cybersecurity strategy	9
1.5 National cybersecurity strategy action plan	10
2 Global cybersecurity contribution	11
2.1 Cyber diplomacy engagements	11
2.2 Commitment to international law in cyberspace	12
2.3 Contribution to international capacity building in cybersecurity	12
3 Education and professional development	14
3.1 Cyber safety competencies in primary education	14
3.2 Cyber safety competencies in secondary education	15
3.3 Undergraduate cybersecurity education	15
3.4 Graduate cybersecurity education	15
3.5 Association of cybersecurity professionals	16
4 Cybersecurity research and development	17
4.1 Cybersecurity research and development programmes	17
4.2 Cybersecurity doctoral studies	17
5 Cybersecurity of critical information infrastructure	19
5.1 Identification of CII	20
5.2 Cybersecurity requirements for operators of CII	20
5.3 Cybersecurity requirements for public sector organisations	21
5.4 Competent supervisory authority	21
6 Cybersecurity of digital enablers	22
6.1 Secure electronic identification	22
6.2 Electronic signature	23
6.3 Trust services	23

6.4 Supervisory authority for trust services	24
6.5 Cybersecurity requirements for cloud services	24
6.6 Supply chain cybersecurity	24
7 Cyber threat analysis and awareness raising	
7.1 Cyber threat analysis	26
7.2 Public cyber threat reports	27
7.3 Public cybersecurity awareness resources	27
7.4 Cybersecurity awareness raising coordination	27
8 Protection of personal data	29
8.1 Personal data protection legislation	29
8.2 Personal data protection authority	29
9 Cyber incident response	
9.1 National incident response capacity	31
9.2 Incident reporting obligations	32
9.3 Cyber incident reporting tool	33
9.4 Single point of contact for international cooperation	33
9.5 Participation in international incident response cooperation	33
10 Cyber crisis management	
10.1 Cyber crisis management plan	34
10.2 National cyber crisis management exercises	35
10.3 Participation in international cyber crisis exercises	35
10.4 Operational crisis reserve	36
11 Fight against cybercrime	
11.1 Cybercrime offences in national law	37
11.2 Procedural law provisions	
11.3 Ratification of or accession to the Convention on Cybercrime	
11.4 Cybercrime investigation capacity	39
11.5 Digital forensics capacity	39
11.6 24/7 contact point for international cybercrime	40
12 Military cyber defence	
12.1 Military cyber defence capacity	41
12.2 Military cyber doctrine	41
12.3 Military cyber defence exercises	42

### **Purpose and scope**

The National Cyber Security Index (NCSI) is a comprehensive resource for cybersecurity capacity building. Established by the Estonian e-Governance Academy (eGA) in 2018, the NCSI is one the world's most detailed tools to measure countries' cybersecurity commitment and readiness.

The NCSI findings rely on institutionalised national cybersecurity capacities as implemented by each nation's central government. The index monitors countries' performance in twelve cybersecurity capacity areas, grouped into three pillars: **strategic** capacities, including cybersecurity governance and policy, as well as global engagement, education, and innovation; **preventive** capacities, which involve aspects such as secure digital infrastructure and cyber threat analysis; and **responsive** capacities related to managing cyber incidents and responding to cyber threats of various nature. The capacity areas in turn are divided into a total of 49 indicators.

The NCSI has several uses. It is a **live global index** that includes data from over 160 countries. Information in the NCSI is accessible through a public online portal – <u>ncsi.ega.ee</u> – and is updated on a rolling basis, without publishing annual rankings.

The NSCI additionally serves as a **cybersecurity reference tool**. As all NCSI findings are supported by publicly available evidence, the NCSI country pages provide hundreds of links to national policy and legal documents, institutions, and programmes. Therefore, NCSI is a source of information detailing how countries are building their cyber capacities.

Finally, the NCSI uses transparent criteria and methodology for evaluating existing national cybersecurity essentials. The index therefore serves as a **cybersecurity assessment and capacity building tool**, indicating areas of solid performance and those that need to be built and/or improved.

The NCSI is managed and updated by the eGA. Founded in 2002, the eGA is a non-profit organisation that creates and transfers knowledge and best practices in public sector digital transformation. The mission of the eGA is to increase the competitiveness of societies through digital transformation, transparency, and openness. To this end, it transfers Estonian and international best practices to governments and other stakeholders around the world. The eGA's activities are made up of the Smart e-Democracy, Governance, Technology, and Cybersecurity programmes.

STRATEGIC	PREVENTIVE	RESPONSIVE
1. POLICY DEVELOPMENT 2. GLOBAL CONTRIBUTION	5. ESSENTIAL SERVICES 6. DIGITAL ENABLERS	9. CYBER INCIDENT RESPONSE
3. EDUCATION AND PROFESSIONAL DEVELOPMENT	7. THREAT ANALYSIS AND AWARENESS	11. FIGHT AGAINST CYBERCRIME
4. RESEARCH AND DEVELOPMENT	8. PROTECTION OF PERSONAL DATA	12. MILITARY CYBER DEFENCE

### Methodology

Across the strategic, preventive, and responsive pillars, the NCSI follows countries' institutionalised capacities in twelve areas. Each of the twelve capacity areas is further divided into unique indicators, which establish the relevant assessment criteria and the type of evidence required. 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.

Each indicator is assigned a value that shows its relative importance in the index. The methodology details the contents of the capacities and indicators, and explains their significance.

While the NCSI primarily uses the term 'cybersecurity', it recognises the varied use of

terminology (information security, ICT security, etc.) as well as the diversity of administrative and organisational approaches. Assessment for fulfiling the NCSI metrics is based on the substantive criteria presented in the indicator and does not require specific terms or organisational composition.

Based on the NCSI criteria, countries are assigned an NCSI score that shows the percentage the country received from the maximum value of total indicators (100%).

The NCSI website, <u>ncsi.ega.ee</u>, displays both the aggregate scores and rankings of countries, as well as their performance in each capacity area. The index allows countries to compare their rankings globally, at the regional level, or within international organisations. It also shows how a country's position in the index has changed over time. For reference, the index also provides an overview of each country's position in other digital/cyber indices.

The NCSI Score shows the percentage of the maximum points NCSI Score = Country Points X 100 Maximum Points

### **NCSI data**

To be recognised in the NCSI, national capacities must be in a certain objective and measurable form. The NCSI tracks:

- Legal and policy instruments: legal acts, regulations, policies, administrative orders, etc.
- Institutions: established organisations, departments, units, etc.
- Cooperation formats: committees, working groups, etc.
- Activities: exercises, technologies, established programmes, etc.
- Other deliverables: websites, curricula, official statements, etc.

The NCSI data and supporting evidence are collected through multiple means:

- Collected by the eGA's NCSI team
- Provided by the relevant government officials
- Provided by partner organisations or experts

Regardless of how it is collected, each piece of data is reviewed by a member of the NCSI team to ensure its validity and relevance.

The eGA does its utmost to gather and verify the evidence reflected in the NCSI portal. In addition, users are welcome to submit evidence for consideration by contacting the NCSI team at ncsi@ega.ee.

### What is new in version 3.0

The eGA reviews the NCSI indicators and criteria periodically to ensure they remain relevant to current good practices on the global level.

The NCSI 3.0 includes revised maturity indicators, taking into account developments in technology, the evolving risk environment, as well as the 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. Indicators concerning international cybersecurity organisations hosted by countries and participation in international military cyber exercises have been omitted.

All NCSI indicators and required evidence are now 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.



## STRATEGIC CYBERSECURITY INDICATORS

This pillar of the NCSI presents national-level indicators with a focus on strategic capacity, including governance, mechanisms to maintain a whole-of-society and whole-of-system approach to policy development, strategic vision and priorities established through a national cybersecurity strategy, and domestic and international engagement. It also includes indicators that track cybersecurity research and development as a means of ensuring the future sustainability of the country's digital society.

### **1 Cybersecurity policy**

**Purpose and scope:** This NCSI capacity area measures whether the country has established a coherent strategic approach to cybersecurity through the key components of high-level leadership, policy development and coordination, and an articulated national cybersecurity strategy.

**Relevance:** For a country to benefit from the social and economic promise of digitalisation, it must manage the accompanying risks and threats strategically at the highest level. A solid cybersecurity governance framework at the national level, with a clear allocation of roles and responsibilities, and coordination mechanisms, raises preparedness and resilience across all sectors and levels of society. A national cybersecurity strategy establishes the key national objectives and priorities, and drives systematic planning and accountability by laying down the implementation modalities in an action plan.

#### STRATEGIC CYBERSECURITY INDICATORS

#### 1 Cybersecurity policy

- 1.1 High-level ownership for cybersecurity
- 1.2 Cybersecurity policy development
- 1.3 Cybersecurity policy coordination
- 1.4 National cybersecurity strategy
- 1.5 National cybersecurity strategy action plan

## **1.1 High-level cybersecurity leadership**

**Criteria**: The country has appointed governmental leadership responsible for cybersecurity at the national level.

**Accepted evidence:** Legal act, national strategy, official statutes or terms of reference, or official website

What is measured: This indicator identifies whether responsibility for cybersecurity has been formally assigned at the highest governmental or political level. Ideally, this should be assigned permanently through legislation or national strategy to a position or institution exercising the country's executive power with a governmental mandate, such as the cabinet, a government minister, or a ministry. **Importance:** Without clearly identified political leadership at the highest level, cybersecurity does not get represented in political decision-making. A lack of representation in turn leads to a lack of government ownership, accountability, and appropriate resources.

**Evidence**: Legal act or policy document assigning high-level political responsibility for cybersecurity.

#### 1.2 Cybersecurity policy development

**Criteria**: There is a competent entity in the central government to whom responsibility is assigned for national cybersecurity strategy and policy development.

**Accepted evidence**: Legal act, official statute or terms of reference, or official website

What is measured: This indicator measures the presence of a specifically designated and empowered entity within the central government that holds national-level responsibility for leading and directing cybersecurity policy development. The same entity may lead national cybersecurity strategy development and oversee its implementation and periodic review. The indicator does not consider institutions whose mandate is limited to cybersecurity legislation or policy within a limited domain (e.g. a single ministry), without a lead role and mandate among stakeholders.

**Importance:** While cybersecurity policymaking is not an exclusive competence and a broad range of stakeholders should be involved in the process, a permanent body that is equipped and responsible for leading and overseeing cybersecurity policy development should be tasked with ensuring the coherence and sustainability of the national approach. Among others, such a body can ensure the effective implementation and sustainability of the national cybersecurity strategy.

**Evidence**: A dedicated government entity or unit, with terms of reference established by a legal act or national strategy.

#### 1.3 Cybersecurity policy coordination

**Criteria**: The country has a regular official format for cybersecurity policy coordination at the national level.

**Accepted evidence**: Legal act, official statute or terms of reference, or official website

What is measured: This indicator checks for the presence of an official mechanism that regularly engages relevant intragovernmental, public, and private actors in cybersecurity policy coordination and cooperation. Such mechanisms may take various forms, such as permanent committees, councils, or working groups.

**Importance:** Cybersecurity policy development and implementation involve multiple stakeholders, each responsible for their own area of governance and activities but working toward common goals over an extended period of time. Thus, there is a constant need for up-to-date inter-agency/wholeof-society communication, organisation, and coordination of efforts. Such coordination and cooperation formats should include stakeholders from the public and private sectors as well as civil society.

**Evidence**: A legal act endowing the coordination body or format with the relevant responsibility. Secondary sources such as official websites where such responsibility is cited may also be considered.

#### 1.4 National cybersecurity strategy

**Criteria**: The central government has established a national-level cybersecurity strategy defining strategic cybersecurity objectives and measures to improve cybersecurity across society.

Accepted evidence: Valid official document

**What is measured:** This indicator tracks the existence of a high-level national strategic document that outlines the country's agenda, objectives, and priorities with regard to improving the nation's cybersecurity, resilience, and related interests. A national cybersecurity strategy typically addresses

topics such as clarifying the roles and responsibilities of various government institutions and other actors with regard to cybersecurity, protecting the country's critical information infrastructure and other important assets, prevention and management of cyber incidents, cybersecurity raising and awareness education, fighting cybercrime, and national and international cooperation. It considers various tools and mechanisms for strengthening cybersecurity: technological and organisational measures, risk management, legislation, and capacity building. The 'Guide to Developing a National Cybersecurity Strategy"1 provides a comprehensive overview of what constitutes successful cybersecurity strategies around the globe.

**Importance:** A national cybersecurity strategy, formally adopted at the highest level, signifies a country's willingness to treat cybersecurity as a national priority. More specifically, a national cybersecurity strategy communicates a commitment to intentionally and systematically developing a country's cybersecurity by identifying the priorities and objectives of various stakeholders and aligning them.

**Evidence**: A high-level official document containing the country's cybersecurity objectives and priorities as described above, regardless of its title (strategy, policy, policy framework). The cybersecurity strategy may be a structural part of another national strategy (e.g. a Cyberspace Strategy or Digital Agenda, National Security Strategy, or other) if the necessary substantive elements are present. It must be currently valid and publicly available in order to be accepted.

## **1.5 National cybersecurity strategy** action plan

**Criteria**: The central government has established an action plan to implement the national cybersecurity strategy.

**Accepted evidence**: Current official document, legal act, or official statement

What is measured: This indicator tracks the existence of an action plan (also known as an implementation plan or implementation matrix) to ensure the implementation of the national cybersecurity strategy. The plan should contain concrete steps on how to achieve the desired goals, including specific tasks, entities responsible for the execution of these tasks, and relevant timelines. The action plan should also set forth the financial and other resources necessary to implement the strategy. Preferably, the strategy should define performance indicators or metrics against which implementation progress may be tracked, and a clearly defined accountability mechanism, such as regular implementation reviews.

**Importance:** An action plan translates the national cybersecurity strategy priorities and objectives into concrete initiatives to be implemented, allocates the human and financial resources necessary for implementation, and establishes timeframes and metrics. An action plan thereby establishes a clear and actionable outline for the effective implementation of the strategy.

**Evidence**: The action plan must be currently valid and be no more than five years old to be accepted. Secondary evidence, such as an official statement, minutes of a government session, or press release, can be accepted if the action plan is not a publicly releasable document. For action plans integrated into the cybersecurity strategy, the same criteria apply.

<sup>&</sup>lt;sup>1</sup> <u>https://ncsguide.org/the-guide/</u>

### **2 Global cybersecurity contribution**

**Purpose and scope:** This NCSI capacity area measures regional and international engagement in shaping the global normative environment and contributing to stability and security in cyberspace via engagement in regional and international cyber diplomacy as well as capacity building efforts. The aim of cyber diplomacy is to cooperate, negotiate, and identify acceptable state behaviour in cyberspace to safeguard international peace and security. In addition, shaping cybersecurity requires the contribution of multiple sectors and disciplines (technology, policy, law, etc.), necessitating a multi-stakeholder approach that allows for the incorporation of views from academia, industry, and non-governmental organisations.

The indicators in this capacity area reflect the elements of the UN global cyber stability framework: norms, rules, and principles; international law; confidence-building measures (CBMs); international cooperation and assistance in ICT security and capacity building.<sup>2</sup>

**Relevance**: A secure, trustworthy, and stable interconnected global cyberspace is a prerequisite for reliable digital infrastructure and services. A secure global cyberspace not only features economic merits, but also allows for the seamless functioning of societies, upholding rights both offline and online, and reaping the benefits of technological innovation. As cyberspace extends beyond the borders of any single country, there is a clear need for effective regional and international cooperation. International cooperation enhances dialogue and coordination, facilitates information sharing, and is key to building trust.

#### STRATEGIC CYBERSECURITY INDICATORS

- 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

#### 2.1 Cyber diplomacy engagements

**Criteria:** The government contributes to international or regional cooperation formats dedicated to cybersecurity and cyber stability.

**Accepted evidence**: Official website of the organisation or cooperation format, official statement or contribution

What is measured: This indicator assesses the commitment of the country to engage in dialogue on

international cybersecurity and stability in regional and international fora. This may include bilateral or multilateral platforms and multistakeholder cooperation formats, and involve topics such as the development and furtherance of cyber norms and CBMs, international law, capacity building, or fighting cvbercrime. Some relevant examples include participating in discussions at the United Nations Open-Ended Working Group (OEWG) and the Ad Hoc Committee on Cybercrime <sup>3</sup> and submitting

<sup>&</sup>lt;sup>2</sup> UN Group of Governmental Experts (GGE) 2013; GGE 2015; GGE 2021; OEWG 2021 reports endorsed by the UN General Assembly.

<sup>&</sup>lt;sup>3</sup> Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes

statements or contributions; contributing to the Organisation for Security and Co-operation in Europe's (OSCE) efforts on CBMs; contributing to the cybersecurity efforts of organisations such as the African Union, the Association of Southeast Asian Nations (ASEAN), the Organisation of American States (OAS), or to the Shanghai Cooperation Organisation's efforts on cooperation in the field of ensuring international information security, and to other such initiatives; membership in the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), the Global Forum of Cyber Expertise (GFCE), the Paris Call, and similar groups or initiatives. The indicator is limited to strategic-level cooperation; operational-level incident response cooperation and cross-border law enforcement cooperation are addressed separately under NCSI capacity areas 9-12.

**Importance:** Whereas national security remains the competence of governments, it is generally acknowledged that international cooperation is vital for reaching and maintaining a high level of security of information and communication technologies (ICTs) with the aim of enhancing international security and stability.

**Evidence**: Formalised engagement in cybersecurityoriented organisations or fora and/or in an international organisation with a specific unit or format dedicated to cybersecurity, and/or other established cyber-specific formats. Mere membership in an international organisation that deals with cybersecurity among an array of other topics is not sufficient.

## **2.2 Commitment to international law in cyberspace**

**Criteria:** The country has an official position on the application of international law, including human rights, in the context of cyber operations.

**Accepted evidence**: Official document or statement, international indexes

**What is measured:** This indicator assesses the commitment of the country to uphold the rules-based international order in cyberspace. The indicator takes into account the country's official statements in the context of international law and cyber operations as well as joining relevant multilateral treaties. Importantly, the country should demonstrate commitment to its international obligations, including human rights obligations, in the online environment.

**Importance:** International law forms the foundation for stability and predictability among states in cyberspace as it reflects common views of acceptable state behaviour. The UN GGE as well as OEWG have affirmed that international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace, security, and stability in the ICT environment. In particular, the UN Universal Declaration on Human Rights guides states to protect human rights and fundamental freedoms online as well as offline.

**Evidence**: Documented official statements made on behalf of the state. Examples of such commitment are sharing the country's views on the interpretation of international law in the context of the UN GGE or OEWG processes, and officially publishing a domestic interpretation or statements made in response to breaches of international obligations. Publications by reputable international human rights observers (e.g. Freedom House).

## 2.3 Contribution to international capacity building in cybersecurity

**Criteria**: The country has led or supported cybersecurity capacity building for another country in the past three years.

**Accepted evidence**: Official website or project document

**What is measured:** This indicator assesses the readiness of the country to finance, organise, or otherwise contribute to capacity building project(s) targeted at specific countries or a group of countries. Capacity building may address issues in both the

public and the private sector, and focus on technical, organisational, policy, strategic and/or legal matters. The support may, for example, involve direct funding or organising/co-organising capacity building projects or events.

**Importance:** A secure and stable cyberspace relies on each country's ability to prevent and mitigate the impact of malicious cyber incidents. Such abilities depend on a wide array of capabilities in the technical, strategic, policy, and legal domains. Capacity building activities address the development of national institutions, policies, skills, and human resources. Importantly, CBMs support countries' adherence to international law as well as to the implementation of cyber norms.

**Evidence**: The activity must have the financial and/or organisational contribution of the country and evidence of the event(s) or programme(s) must be publicly available.

### **3 Education and professional development**

**Purpose and scope:** This NCSI capacity area considers whether the country has a systematic approach to cybersecurity education and professional development. The modern interconnected world requires baseline skills and knowledge in young people, which also serve as a foundation for further education. Sustainable education opportunities are necessary to allow for the development of talent and ensure a sufficiently large and knowledgeable workforce for ICT and cybersecurity. Additionally, cooperation among specialists and the sharing of good practices can strengthen national cyber resilience.

**Relevance:** A rapidly changing cyberspace, where new technologies and threats emerge, and previously adequate security solutions become outdated, leads to the need to deal consistently with developing sustainable cybersecurity education and workforce training that takes into consideration both existing and future needs. Meeting the personnel needs of the public and private sectors requires developing educational curricula that can provide a wide spectrum of knowledge and skills. At the same time, it is also necessary to analyze the training needs of current professionals and plan resources for training cyber experts who are already working in the field.

#### PREVENTIVE CYBERSECURITY INDICATORS

- 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

### **3.1 Cyber safety competencies in primary education**

**Criteria**: Primary education curricula in the public education system include cyber safety (online safety, computer safety) competencies.

**Accepted evidence**: Official curriculum or official report

**What is measured:** Primary education should set the ground rules for safe, responsible, and ethical online behaviour. This can be established through national curricula that introduce cyber/computer safety and cyber/computer hygiene at the primary education levels. The scope of this indicator includes cybersecurity competencies in the public education system, that is, the most accessible form of primary education available in the country.

**Importance:** Through early training on secure online behaviour and ways to safeguard the ICT devices that children use, the younger generation can grow up to become safe and responsible online users and be better prepared to face the challenges of cyberspace. Especially because children are exposed to ICT early on through the inclusion of computer skills, programming, robotics, etc. in general education, it is important that such training also involve security skills.

**Evidence**: The evidence must demonstrate an established practice, such as specific or integrated curricula intended for long-term use. Sporadic

events such as one-time guest lectures do not qualify.

### **3.2 Cyber safety competencies in secondary education**

**Criteria**: Secondary education curricula in the public education system include cyber safety (online safety, computer safety) competencies.

Accepted evidence: Official curriculum or official report

**What is measured:** Like the previous indicator, this one considers the inclusion of cybersecurity skills in national general education curricula, but the focus here is on secondary-level education. The relevant curricula should address cyber/computer safety and cyber/computer hygiene as a part of the secondary education available in the public education system, that is, the most accessible form of secondary education available in the country.

**Importance:** As students become more exposed to the online environment and grow into more experienced users, their cybersecurity knowledge and practical skills should grow appropriately.

**Evidence**: The evidence must demonstrate an established practice, such as specific or integrated curricula at the secondary education level. Sporadic events such as one-time guest lectures do not qualify.

### 3.3 Undergraduate cybersecurity education

**Criteria**: At least one undergraduate education programme is available in the country to train students in cybersecurity.

Accepted evidence: Accredited study programme

**What is measured:** The indicator measures the availability of undergraduate cybersecurity or equivalent (ICT security, electronic information security) education at the national level – that is, a bachelor's degree, vocational training, or equivalent. It acknowledges both distinct cybersecurity

programmes and the integration of cybersecurity into undergraduate ICT education.

**Importance:** A cybersecurity programme at the undergraduate level should provide the knowledge and skills necessary to build safer ICT systems, as well as teach how to defend against and manage cyberattacks and incidents. Theoretical knowledge should be supported by practical studies, such as labs or practice lessons.

**Evidence**: Both national curricula focused on cyber/computer security, and curricula with distinct cybersecurity modules count as evidence. Curricula with a single cybersecurity course will not be accepted as evidence.

#### 3.4 Graduate cybersecurity education

**Criteria**: At least one cybersecurity education programme is available in the country at the graduate level.

Accepted evidence: Accredited study programme

**What is measured:** The indicator measures the availability of graduate cybersecurity or equivalent (ICT security, electronic information security) education in the country – that is, a master's degree or equivalent. It acknowledges both distinct cybersecurity programmes and the integration of cybersecurity into graduate ICT education.

Importance: А graduate (master's-level) cybersecurity programme trains students in subjects computer such as security, cvbersecurity governance and risk management, networking and infrastructure, and information security analysis and monitoring from the individual system-level perspective or that of large, mission-critical networks. Such cybersecurity graduate programmes are typically designed for students with a technical background (computer science, mathematics, or others), but they can also be cybersecurity programmes designed for students with an undergraduate degree in a non-technical discipline.

**Evidence**: Both national curricula focused on cyber/computer security, and curricula with distinct

cybersecurity modules count as evidence. Curricula with a single cybersecurity course will not be accepted as evidence.

## 3.5 Association of cybersecurity professionals

**Criteria**: A professional association of cybersecurity specialists, managers, or auditors exists in the country.

Accepted evidence: Official website

What is measured: An established and functioning association of professionals in cybersecurity, (electronic) information security, or the equivalent. For example, associations that promote international cybersecurity expert certifications (e.g. CISSP), such as ISACA country chapters or organisations of cybersecurity auditors, are recognised here. Their membership may include cybersecurity specialists, managers, and others. The index does not consider organisations that limit membership based on criteria other than professional qualification. In addition to specialist members, the organisation may have corporate members.

**Importance:** As digital technologies advance, cyber threats and risks are constantly evolving, and cybersecurity professionals need to keep their knowledge and skills up to date. Professional associations for information security officers, IT auditors, and others are a widespread and valuable form of exchanging experience and best practices. The associations organise events for their members and for the general public and manage information exchange channels for members. There are also training and collaboration opportunities available via such associations that make membership a worthwhile investment for professionals who need to stay current with the developments in the field.

**Evidence**: Website of the professional association that demonstrates the existence and activities of that association. Information published by a government authority that confirms these elements can also be considered.

### **4 Cybersecurity research and development**

**Purpose and scope:** This NCSI capacity area focuses on strategic national cybersecurity capacity building by encouraging research and development and creating favorable conditions for the cybersecurity industry and cybersecurity innovation. Through a commitment to research and development in cybersecurity, the country builds readiness to keep up with the evolving technological and risk environment, and has the capacity to proactively influence the environment rather than merely reacting to it.

**Relevance:** National research and development capacity is of key importance for cybersecurity knowledge development and innovation: through research and development, new solutions, products, and services are created and enter the market. A strong and capable national research sector has several important benefits for a country: their innovation contributes to the country's economic development; they can supply cybersecurity solutions needed for the digital society and the government; and they can ensure the availability and transmission of cybersecurity knowledge and talent in the country. Cybersecurity research and development capacity is also becoming progressively more important in determining a country's global and regional competitiveness.

#### STRATEGIC CYBERSECURITY INDICATORS

- 4 Cybersecurity research and development
- 4.1 Cybersecurity research and development programmes
- 4.2 Cybersecurity doctoral studies

## 4.1 Cybersecurity research and development programmes

**Criteria**: A cybersecurity research and development (R&D) programme or institute exists and is recognised and/or supported by the government.

**Accepted evidence:** Official programme or official website

What is measured: The indicator measures government engagement in cybersecurity research and development, demonstrated through formal recognition and/or public funding and support for a relevant research programme. The criterion is inclusive of both government and industry programmes, but in order to be considered for the purposes of national capacity, the involvement of formal governmental support is required, whether through a (co-)funding commitment, research grants, or cooperation agreement. **Importance:** Established research and development programmes can ensure that scientific knowledge results in actual prototypes, patents, products, and solutions. In particular, cooperation arrangements between the government, academia, and industry can ensure that the country's strategic cybersecurity priorities are reflected in its research agenda, so that the country's needs are sustainably met.

**Evidence**: Official documents or other official references indicating fundamental or applied research and development programmes with a demonstrable government contribution.

#### 4.2 Cybersecurity doctoral studies

**Criteria**: An officially recognised PhD programme exists accommodating research in cybersecurity.

Accepted evidence: Official programme or official website

What is measured: The indicator recognises the availability of PhD study programmes that allow students to develop substantive knowledge in cybersecurity, and design, and conduct original, specialised research in cybersecurity. Research topics may range from technical matters (for example cryptography, computer and network security, or digital forensics) to relevant social sciences issues (for example strategic or behavioural issues). The PhD programme does not necessarily have to be limited to cybersecurity, broader ICT doctoral programmes are accepted if they produce cybersecurity graduates.

**Importance:** A PhD programme provides a structured and sustained setting to develop talent and innovate beyond preparing the workforce for existing market needs. PhD students are trained in research methods and gain a deeper understanding of cybersecurity issues.

**Evidence**: Officially accredited or otherwise officially recognised PhD programme that is focused on cybersecurity or produces cybersecurity degrees.

## PREVENTIVE CYBERSECURITY INDICATORS

This pillar of the NCSI comprises indicators exhibiting the country's capacity to prevent cyber threats and build cyber resilience by managing cyber risks to the security of ICT and digital infrastructure, which are crucial for the essential functions of modern societies. The pillar also considers cyber threat assessment capacity, cybersecurity awareness activities targeted at the public, as well as cybersecurity education and workforce development.

### **5** Cybersecurity of critical information infrastructure

**Purpose and scope:** This NCSI capacity area merges the earlier NCSI capacity areas 5 and 6, removing the distinction between digital and essential services. The indicators in this area assess a systematic national approach to managing cyber threats and risks to critical information infrastructure (CII) – the digital solutions and services that underpin essential public functions, regardless of whether the terminology used for them is critical infrastructure (CI), essential service, important entities, or any other similar term. The NCSI tracks whether such infrastructure is systematically identified and whether operators are accountable for assessing risks to the continuity of their services and implementing adequate risk management measures. It also tracks whether the country has a cybersecurity regulatory or competent authority with an enforcement mandate and powers.

**Relevance:** Information systems and digital services are an inseparable part of a country's infrastructure that allows modern societies to function. Some of these infrastructure elements are considered critical: their disruption or destruction could have a serious impact on the health, safety, security, and economic well-being of citizens, or the functioning of the government or economy. Many such systems are dependent on information infrastructure – industrial control systems (ICS), supervisory control and data acquisition (SCADA) applications, or other digital solutions, services or processes – some of which are critical to the operation and continuity of the CI itself. It is a matter of public safety and national security for countries to have established national mechanisms to manage such risks and prevent them from materializing.

#### PREVENTIVE CYBERSECURITY INDICATORS

- 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

## 5.1 Identification of critical information infrastructure

**Criteria**: There is a framework or a mechanism to identify operators of critical information infrastructure.

Accepted evidence: Legal or administrative act

What is measured: This indicator measures the presence of a legally established framework or mechanism to identify the information infrastructure component of CI or essential services. This objective may be addressed within the scope of defining critical sectors, infrastructure or services, or through a standalone mechanism for identifying CII. National legislation that is limited to contingency planning and disaster recovery without evident application to cybersecurity is not counted under this indicator.

Importance: Certain sectors and services are commonly recognised to be essential to the normal functioning of society, the economy, and the state. These typically include energy production and supply, communications, financial services, healthcare, utilities, and others. A solid national framework for managing cyber risks to such critical sectors or services is built on the premise that such sectors/services/operators should first be identified, and then the information infrastructure components within them upon which service provision critically depends should be addressed. While not all information infrastructure within such critical sectors/infrastructure/services are necessarily critical to the continuity of the sector/infrastructure/service, certain assets are such that their loss or compromise could have a major detrimental impact on the availability or integrity of the actual CI or essential service. Therefore, governments must have an established methodical framework to address such risks.

**Evidence**: The indicator recognises both legislation that foresees a CI identification process, or the designation of such infrastructure by an administrative act. In either case, it is required that

such designation have cybersecurity implications for the infrastructure operator.

# **5.2 Cybersecurity requirements for operators of critical information infrastructure**

**Criteria**: Operators of critical (information) infrastructure are required to assess and manage cyber risks and/or implement cybersecurity measures.

**Accepted evidence**: Legal act, or mandatory cybersecurity framework or standard

What is measured: The indicator tracks whether operators that are critical/essential are required to take preventive and reactive measures to manage cybersecurity risks to their network and information systems. This could include an obligation to assess cyber risks and implement appropriate technical and organisational measures, according to international standards such as the ISO 27000 family, U.S. NIST framework, or other recognised regional or sectoral standards or best practices. It could also include an obligation to comply with nationally established cybersecurity requirements or standards. On the reactive side, incident notification and response requirements should be established; however, the mere existence of responsive requirements does not satisfy the criteria for this indicator. The criteria need not be applied to micro and small enterprises.

**Importance:** The implementation of cybersecurity requirements for CII safeguards the continuity or undisrupted operation of CI and critical services that are essential for the normal functioning of the state and society. Making these requirements mandatory ensures that they are implemented consistently and that operators are accountable for the implementation.

**Evidence**: Legislation or regulatory measures that foresee a mandatory cybersecurity standard for CII operators, or obligations to operators to assess and manage cyber risks. The regulation may be established in a standalone act or be explicitly addressed in a legal act imposing security and continuity requirements upon CI owners or operators.

### 5.3 Cybersecurity requirements for public sector organisations

**Criteria**: Public sector organisations are required to assess and manage cyber risks and/or implement cybersecurity measures.

**Accepted evidence**: Legal or administrative act, mandatory cybersecurity framework or standard

What is measured: The indicator assesses the mandatory implementation of cybersecurity (or ICT security/information security) measures in the public sector. Such requirements may be defined directly in legislation, or they may refer to a national or widely recognised international cybersecurity standard. The obligation should at a minimum include mandatory cybersecurity measures applicable to the information infrastructure used in executing state functions and tasks (that is, legislative, administrative, and judicial powers), but may further include certification of products and services for procurement by state, municipal, local, and government authorities.

The existence of mandatory cybersecurity measures for the public sector remains a distinct indicator due to the frequent practice of not including the government in the scope of CII/essential service operators. If the government falls under the same CII/essential service requirements, separate regulation is not required.

**Importance:** When it comes to ensuring the state's cybersecurity, it is of key importance that the state's organs and entities adhere to a set of basic security requirements stemming from information security solutions, at least at the level required by a domestic legal act. The basis for ensuring information security at public sector institutions is adherence to national or widely recognised cyber/information security requirements and standards.

**Evidence**: Legal or administrative act laying down cybersecurity requirements for public sector organisations, or a legal or administrative act explicitly including public sector services under the national cybersecurity requirements for CII, where these exist.

#### 5.4 Competent supervisory authority

**Criteria**: A competent authority has been designated and allocated powers to supervise the implementation of cyber/information security measures.

Accepted evidence: Legal act or official website

What is measured: The indicator tracks whether a cybersecurity regulator/competent authority has been established with a relevant mandate and enforcement powers. Its constituency may include operators of essential services/CI, public sector organisations, or a broader range of actors. In any case, a cybersecurity supervising system to monitor essential services should be established, and critical (information) infrastructure operators should regularly provide evidence of the effective implementation of cybersecurity measures. The supervisory competence should be concentrated in the cybersecurity authority and not be decentralized among sectoral authorities performing supervision in their respective sectors.

**Importance:** Cyber threats are universal and do not differ significantly between different essential sectors and services. In addition, the cross-sectoral impact of cyber threats, as well as the cross-sectoral dependencies of CII are more pronounced and potentially time-critical than in traditional critical sectors. A national supervisory system to oversee the implementation of cybersecurity measures is more mature if the respective competence is concentrated in a single supervisory authority and not dispersed between sectoral regulators.

**Evidence**: The indicator does not require a distinct cybersecurity regulatory body per se but the presence of supervisory powers over the implementation of cybersecurity measures. Regular supervision means that supervisory activities, including audits or similar assessments, are conducted at least once every three years

### **6 Cybersecurity of digital enablers**

**Purpose and scope:** This NCSI capacity area measures existing national mechanisms to ensure the cybersecurity of a nation's fundamental digital enablers that are not explicitly in the scope of essential services. The revised NCSI 3.0 broadens the scope of this capacity from electronic identity (eID) and trust services that supply security and reduces the number and weight of eID-specific indicators.

**Relevance:** To benefit from digitalisation, it is essential that the state ensures the security and reliability of the digital systems that sustain governmental and administrative functions, and that digital transactions among individuals and businesses can be trusted. Functional e-identification and trust services provide a solid, powerful basis to develop digital solutions and services both for domestic users and across borders. An example of good practice for trusted cross-border digital transactions is the European eIDAS Regulation (Regulation on electronic identification and trust services), which creates a predictable regulatory environment for businesses, citizens, and public authorities to carry out secure and seamless electronic interactions. The rapid evolution of the digital environment requires states to remain agile and adapt to technological change in order to safeguard the security and reliability of fundamental digital enablers.

#### PREVENTIVE CYBERSECURITY INDICATORS

- 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

#### 6.1 Secure electronic identification

**Criteria**: A national electronic identification solution exists that allows for officially recognised and secure electronic identification of natural and/or legal persons.

**Accepted evidence**: Legal act, nationally recognised identification scheme, or official website

**What is measured:** A nationally recognised solution that allows for the secure and reliable identification of individuals in online transactions. Such a solution must, at the minimum, be available for interaction with public sector organisations with

the possibility to be adopted in the private sector. The index does not take into account eIDs that do not cover the majority of the population or are, by design, only limited to certain sectors or services.

**Importance:** In legal transactions, it is important to securely identify the parties. Traditionally, this is done by relying on identity documents issued by the government. In online transactions, equivalent assurances can be provided through a secure digital identity, that is, a certificate that can be definitely associated with a specific person.

The best method to uniquely identify a natural or legal person is by a nationally recognised unique, population-wide identifier. Such an identifier may be created during the population registration process, or another identifier (such as a social security number or a taxpayer account identifier) may be extended to the whole population. From an interoperability perspective, it is important that eID uses the same identifier that is used in identity documents.

For eID to have legally binding significance, its issuance must be regulated by law, assuring equivalent protection to what is assured for passports or other identity documents. The protection of cryptographic keys or other security features must be guaranteed by law. The availability of secure eID also reduces the likelihood of crimes related to online identity theft.

**Evidence**: The evidence must establish the legal recognition and availability of a national (nationwide) eID solution. A legal act, nationally recognised identification scheme, or official website demonstrating the required elements is suitable evidence.

#### **6.2 Electronic signature**

**Criteria:** A nationally recognised and publicly available solution exists to issue secure and legally binding electronic signatures.

Accepted evidence: Legal act or official website

**What is measured:** A software or service to issue secure electronic signatures, which are generated using a digital certificate and cryptographically bound to the document through public key infrastructure (PKI), are publicly available and legally accepted by the country without their use being limited to specific sectors or purposes. The use of up-to-date secure cryptography is required to accept the signature as legally binding.

**Importance:** Like with a signature on paper, it must be possible to verify individuals' declarations of intent in cyberspace to trust and consider them valid. For this, the concerned procedure must be regulated by law and the electronic signature must be given protection and legal consequences equivalent to those given to paper signatures.

For the subsequent verification of the validity of the electronic signature of the signed document, it must be possible to verify at the time of signing the validity of the certificate used for signing. For the claimed signing time to be reliable, it is important to have a trustworthy time service that issues the timestamp attached to the document with the signature. The requirements for the trust service (such as certificate validity check and time stamping) must be provided by law.

**Evidence**: The evidence must establish the legal recognition and availability of electronic signatures. A legal act or official website demonstrating the required elements would be suitable.

#### 6.3 Trust services

**Criteria:** Trust services (e.g. digital certificates, timestamps, private key management service) are regulated, at least for use in the public sector.

Evidence: Legal act or official website

What is measured: Regulations lay down minimal security and liability obligations (including, but not limited to, accepted cryptographical parameters) for trust service providers and their services, as well as the process and conditions for supervision and liability. Established requirements should be applicable to the trust services that are provided on the market (e.g. digital certificates, timestamps, private key management service, or others), at least where these are used in the public sector and public sector services.

**Importance:** Trust services are based on cryptography. The evolution of hacking technologies may mean that algorithms become weak over time and need to be replaced. Where the provision and use of trust services are widespread in society, the renewal of technical systems related to algorithms affects a very large number of parties. Therefore, to maintain the reliability of trust services,

organisational and technical requirements must be established in national legislation to determine which cryptographical algorithms and cybersecurity mechanisms are allowed.

**Evidence**: The evidence must establish the legal regulation and recognition for trust services provided in the country. A legal act or official website demonstrating the required elements would be suitable.

### 6.4 Supervisory authority for trust services

**Criteria**: An independent authority has been designated and given the power to supervise trust services and trust service providers.

Accepted evidence: Legal act or official website

What is measured: The state must have a designated authority that oversees the reliability of trust services throughout its lifecycle. This includes authorisation to launch a service into the market and supervision over compliance with existina requirements throughout the period of operation. Regulations must either set requirements for trust service providers or assign this mandate to a competent institution or authority. This may be a supervisory body, a technical regulatory authority, or a similar institution. The powers of the supervisory body must stem from and be specified in a legal act.

**Importance:** A duly authorised supervisory authority is a necessary guarantor for the reliability of trust services throughout their lifecycle. The role of the supervisory authority is to oversee that both the organisation providing the trust service and the services themselves comply with existing requirements.

**Evidence**: The evidence must establish the presence of a legal act that defines a supervisory authority together with its tasks and supervisory mandate.

## 6.5 Cybersecurity requirements for cloud services

**Criteria**: Requirements are established for the secure use of cloud services in government and/or public sector organisations.

**Accepted evidence**: Legal or administrative act, cybersecurity framework or standard

**What is measured:** This indicator tracks the emerging trend of establishing secure use requirements or principles for the use of cloud services. Such security requirements should, at the minimum, extend to the use of cloud services in the government sector.

**Importance:** The use of cloud computing for collaboration is growing in prevalence among both governments and businesses. To ensure the confidentiality, integrity, and availability of data and applications stored on the cloud, security measures must be implemented to protect them from cyber threats.

**Evidence**: A legal act, government guideline, or similar that defines cybersecurity requirements or principles, applicable as mandatory at least for governmental institutions.

#### 6.6 Supply chain cybersecurity

**Criteria:** Requirements are established to identify and manage cybersecurity risks through the ICT supply chain.

Accepted evidence: Legal act or official website

What is measured: This is a new indicator of the NCSI, appraising whether controls and processes are enforced to manage potential cyber risks to the supply chain. 'Supply chain' involves the whole cycle of design, development, production, deployment, and support for products, services, or processes. These could involve, for example, regular supply chain audits, risk assessments and management, and/or specific requirements for suppliers based on their risk profiles. Supply chain attacks are malicious activities at any location in the supply chain

(technology development, engineering and manufacturing development, production and deployment, and operation and support). The relevant security mechanisms should be established at least for operators of essential services and/or public sector organisations, and preferably also for their third-party providers and vendors.

**Importance:** In order to ensure the continuity of essential services and infrastructure, it is important that the technology comes from a reliable manufacturer and that risk management processes

and measures are in place to ensure that the technology used to provide the essential service is not manipulated by a potentially malicious actor.

**Evidence**: The criterion accepts national-level and sector-based standardisation and certification schemes, as well as other cyber/information security measures. It is deliberately designed to be broad, to allow the recognition of all countries that have addressed this issue in law.

### 7 Cyber threat analysis and awareness raising

**Purpose and scope:** This NCSI capacity area reviews the capacities and practices related to aggregating, analysing, and communicating cyber threat information. These activities are undertaken with two purposes: to raise public awareness about cybersecurity and to offer situational awareness and guidance to various actors so they can take measures to protect themselves. The indicators cover aspects such as cyber threat assessment and analytical capacity; public threat alerts and the provision of public cybersecurity guidance, advisories, and awareness resources; and ensuring coherent awareness raising through national coordination.

**Relevance:** A country that has a good understanding of the risks that it is exposed to is able to manage them more effectively. It is important to realise that cyber incidents can never be completely prevented. The rapid development of technology and society's growing reliance on it also increases the potential for security incidents. Thus, it is important to identify and understand the potential threats and risks, the factors contributing to or alleviating them, and the potential consequences.

#### PREVENTIVE CYBERSECURITY INDICATORS

- 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

#### 7.1 Cyber threat analysis

**Criteria**: A government entity has been assigned the responsibility for national-level cybersecurity and/or cyber threat assessments.

**Accepted evidence**: Legal act, statute, or official website

What is measured: This indicator assesses the capacity and practice of conducting national-level cyber threat and trend assessments. The assessments may, for example, be compiled by an established government entity or unit (such as a department or an agency) or an interagency joint task force. Whether a centralised or distributed approach is followed, the inputs of various sources should be consolidated into a national-level threat picture, and the outcome should assess the cyber

threat and cybersecurity status at the national level, covering all sectors.

**Importance:** National cyber threat assessments and reports enable consistent characterisation of cyber threats and risks and allow the identification of trends and changes in the activities of malicious actors, new vulnerabilities, or key technological developments impacting national resilience. Information about cyber incidents, threats, and vulnerabilities is analysed and aggregated to provide timely and actionable information to government planning and decision-making entities.

**Evidence**: An established unit that has been assigned the task of analysing cyber threat information, or a legal or administrative act assigning the relevant responsibility to an existing body.

#### 7.2 Public cyber threat reports

**Criteria**: Public cyber threat reports and notifications are issued at least once a year.

**Accepted evidence**: Official website, official social media channel, or public report

**What is measured:** This indicator tracks the practice of sharing cyber threat awareness, including both timely cyber threat notification and forward-looking insights, anticipating how changes in the cyber landscape may affect public and private institutions.

Importance: No single organisation can defend against cyber threats on its own; it is vital that the public and private sectors work together to be aware of and understand the challenges they face. To support public threat awareness, the government should regularly publish public cyber threat reports or notices. The purpose is to inform the public about significant cyber incidents, major threats and/or vulnerabilities, and to give insight into trends. Such reports and notices may also alert the public to current cyberattack campaigns or systemic vulnerabilities. By sharing timely information, the government can motivate organisations to work together to prevent cyber incidents and achieve safer cyberspace.

**Evidence**: Regular public threat notifications and reports, social media posts, and so on by, for example, the national computer security incident response team (CSIRT) or computer emergency response team (CERT), or another relevant authority count as evidence. To be recognised in the NCSI, such reports should be issued at least once a year.

### 7.3 Public cybersecurity awareness resources

**Criteria**: Public authorities provide publicly available cybersecurity advisories, tools, and resources for users, organisations, and ICT and cybersecurity professionals.

**Accepted evidence**: Official website, public advisories

What is measured: This indicator recognises the ready availability of public cybersecurity awareness resources such as cybersecurity guidance and advisories. These could be public awareness raising campaigns promoting cyber hygiene or dedicated websites with information, guidelines, and tips on how to keep data and assets safe online. They could be targeted at the general public or also address specific target groups such as cybersecurity professionals and small or medium enterprises.

**Importance:** Cybersecurity ultimately depends on the skills of each user and asset owner to act responsibly in the online environment. The purpose of public cybersecurity resources, therefore, is to empower individuals, businesses, and civil society actors to improve their cybersecurity and protect their assets online.

**Evidence**: A dedicated public website or readily available public cyber hygiene resources.

## 7.4 Cybersecurity awareness raising coordination

**Criteria**: There is an entity with the clearly assigned responsibility to lead and/or coordinate national cybersecurity awareness activities.

**Accepted evidence**: Legal act, official document, or official website

**What is measured:** This indicator appraises a systematic approach to cybersecurity awareness through a clear allocation of cybersecurity awareness coordination tasks: providing direction, coordinating actions, and monitoring the implementation of cybersecurity awareness activities.

**Importance:** A clearly assigned coordination and oversight role for cybersecurity awareness activities facilitates more effective and efficient awareness raising. In addition to providing direction, coordinating actions, and monitoring the

implementation of awareness activities, the lead agency can identify the stakeholders to be involved in the development and implementation of the awareness activities, clarify the roles of different stakeholders, address gaps or duplications, and manage expectations throughout the process. Whether a centralised or a more distributed model is used, all parties involved should have a clear understanding of their respective roles and responsibilities so that accountability and progress can be ensured.

**Evidence**: A legal act, statute, or other official document outlining the responsibilities and accountability for coordinating cybersecurity awareness.

### 8 Protection of personal data

**Purpose and scope:** This NCSI capacity area addresses a field closely interrelated with cybersecurity: online privacy and personal data protection. The indicators look at cyber-specific aspects of national data protection legislation and existing enforcement mechanisms.

**Relevance:** The rapid growth of digital economies has led to a significant increase in the collection, processing, and sharing of personal data on online platforms and services. To protect individuals' fundamental rights to privacy and to reinforce control over their information in the online environment, countries are – or should be – revising and updating their personal data protection laws. The law should ensure that privacy and security guarantees for processing personal data are adequate for the modern digital environment and that organisations are accountable for securing the integrity and confidentiality of personal data.

#### PREVENTIVE CYBERSECURITY INDICATORS

8 Protection of personal data

- 8.1 Personal data protection legislation
- 8.2 Personal data protection authority

#### 8.1 Personal data protection legislation

**Criteria**: There is a legal act for personal data protection that is applicable to the protection of data online or in digital form.

Accepted evidence: Legal act

What is measured: The presence of a national law that sets out the principles of data processing, the rights of the individual (data subject) with regard to their data, and the obligations and liability of data controllers and processors. The applicability of the data protection law to the digital/online environment must either be stated explicitly or established through its inclusive nature that allows individuals the protection of their data processed online.

**Importance:** The right to privacy is a fundamental human right that countries must protect and promote, regardless of the platform or medium where the data is processed, and regardless of who – state authorities or commercial service providers – is processing the personal data. Security assurances, including a legal basis for data processing, should be

defined in legislation that provides the conditions and procedures for processing personal data as well as the liability for violations.

**Evidence**: Personal data protection legislation that applies to data processing by both government and private sector actors in the digital/online environment.

#### 8.2 Personal data protection authority

**Criteria**: An independent public supervisory authority has been designated and allocated powers to supervise personal data protection.

Accepted evidence: Legal act or official website

**What is measured:** The country should appoint and equip a public supervisory authority to make sure that its data protection laws are applied and enforced consistently when it comes to online data processing.

**Importance:** An independent authority overseeing data processors' compliance with personal data protection requirements is an essential component of

individuals' rights to privacy and data protection. National legislation should provide a legal basis for the supervisory authority and define its role, duties, and supervisory powers. **Evidence**: A data protection authority with oversight and enforcement powers allocated by law. The mandate must apply to oversight over data processing by both government and private sector actors in the digital/online environment.

## RESPONSIVE CYBERSECURITY INDICATORS

This pillar of the NCSI examines national preparedness to respond to cyber threats and incidents. It considers established national capacities in the areas of operational cyber incident management, fighting cybercrime, and military cyber defence. The pillar also includes indicators concerning cyber crisis management plans and exercises.

### 9 Cyber incident response

**Purpose and scope:** This NCSI capacity area examines the establishment and sustainability of effective national capabilities to prevent, detect, respond to, and recover from cyber incidents. The central aspect of this capacity is the presence of an established, functioning national computer security incident response team (CSIRT), also known as a computer emergency response team (CERT) or cyber incident response team (CIRT). The remaining indicators in this area address the key facets and tools of CSIRT operation: the national CSIRTs relations and communication with its constituency, as well as its engagement in international cooperation networks.

**Relevance:** Appropriate national incident response capabilities are a central constituent of national cyber resilience. A dedicated, adequately resourced national CSIRT can significantly lower cyber risks to a country's economy and society by providing proactive and preventive services. In the event of a cyber incident, national CSIRTs coordinate incident response at the national and international levels, thereby helping to minimise damage and recover quickly from the incident.

#### **RESPONSIVE CYBERSECURITY INDICATORS**

#### 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

#### 9.1 National incident response capacity

**Criteria**: There is a CERT designated with nationwide responsibilities for cyber incident detection and response.

Accepted evidence: Legal act or official website

**What is measured:** The indicator tracks the presence of a national CSIRT/CERT/CIRT in the country. In line with the Carnegie Mellon University definition, the NCSI acknowledges as national CSIRTs those CERTs that are designated by a country or economy to have specific responsibilities regarding the cyber protection of the country or economy. Such

national CSIRTs can be located inside or outside the government but must be specifically recognised by the government as having nationwide powers and responsibility.

The IETF Request for Comments 2350 specifies what is expected of CSIRTs.<sup>4</sup> A CSIRT should clearly define its constituency and publish information about its services and communication channels. Services provided by a CSIRT can be divided into two broad categories: real-time activities directly related to their main task of incident response and proactive activities in support of the incident response task. The basic tasks of a CSIRT include monitoring cyber incidents at the national level, providing early warnings, alerts, announcements and information to relevant stakeholders about risks and incidents, responding to incidents, and participating in the CSIRT networks.

**Importance:** A well-functioning national CSIRT is central to the national-level capacity to prevent, detect, respond to and mitigate cyber incidents and manage cyber risks. CSIRTs should have sufficient technical and organisational capabilities to carry out these tasks and should be able to participate in international cooperation networks.

National CSIRTs act as focal points and coordinate incident response at the national and international levels. Many CSIRTs also help protect their country's government networks and CII.

**Evidence**: A legal act designating the role of a national CSIRT, official governmental website or official website of the national CSIRT, or website of a recognised international CSIRT forum such as the Forum of Incident Response and Security Teams (FIRST)<sup>5</sup> or the Task Force on Computer Security Incident Response Teams (TF-CSIRT).<sup>6</sup>

#### 9.2 Incident reporting obligations

**Criteria**: Operators of critical information infrastructure and/or government institutions are obliged to notify the designated competent authorities about cyber incidents.

Accepted evidence: Legal act or official website

**What is measured:** The indicator assesses whether a legal obligation exists to require certain critical sectors and organisations to notify the relevant government authority about significant cyber incidents. The obligation may extend to operators of CI/CII, digital service providers, essential services, government institutions, and other relevant actors. Such notifications are usually addressed to the national CSIRT or a national cybersecurity authority.

**Importance:** Mandatory incident notification serves both responsive and preventive aims. It allows the national CSIRT to know when, where, and how to respond most effectively. It also enables the CSIRT to fulfil its threat awareness and analysis responsibilities, and provide alerts or preventive and mitigation guidance to potentially affected parties. To facilitate timely and informative incident reporting, the national CSIRT or another relevant authority could publish official criteria, guidelines, and tools. The law should also define confidentiality assurances to the notifying and affected parties, as appropriate.

**Evidence**: Legislation that foresees mandatory reporting of significant cyber incidents, applicable at least for CII operators and/or government entities.

<sup>&</sup>lt;sup>4</sup> <u>https://tools.ietf.org/html/rfc2350</u>

<sup>&</sup>lt;sup>5</sup> https://www.first.org

<sup>&</sup>lt;sup>6</sup> <u>https://www.trusted-introducer.org</u>

#### 9.3 Cyber incident reporting tool

**Criteria**: A publicly available official resource is provided for notifying competent authorities about cyber incidents.

**Evidence**: Official website

**What is measured:** The indicator tracks the practice of providing a widely accessible way to notify the national CSIRT, law enforcement, or other competent body about cyber incidents. The use of the tool does not need to be limited to mandatory incident reporting by operators of CII and government authorities.

**Importance:** The ready, round-the-clock availability of an online incident reporting tool facilitates timely and informative incident reporting to the national CSIRT. It is important to ensure the confidentiality and integrity of information submitted over this channel and to communicate such assurances clearly when information is submitted. The authorities should follow up on any submissions as required.

**Evidence**: An official website with incident reporting functionality.

## 9.4 Single point of contact for international cooperation

**Criteria:** The government has designated a single point of contact for international cybersecurity cooperation.

Accepted evidence: Legal act or official website

**What is measured:** The country should have a designated national single point of contact (SPOC) to be available for liaising with international counterparts on issues related to cyber incident management and vulnerability information sharing. The SPOC coordinates with other affected countries in the event of a cross-border cyber incident. The role may be assigned to an existing authority, such as the national CSIRT.

**Importance:** SPOCs simplify coordination and communication when dealing with cross-border threats and incidents, especially where several

countries and multiple national authorities are involved in threat mitigation or incident resolution. For example, the SPOC may consult and cooperate with the relevant national law enforcement and data protection authorities where appropriate and in accordance with national law. Any relevant national authority or the CSIRT can entrust the SPOC to forward incident information to other national SPOCs. To carry out their tasks effectively, the SPOCs should have adequate technical, financial, and human resources.

**Evidence**: A legal act or official website establishing an entity as the national SPOC for cyber incident coordination.

## 9.5 Participation in international incident response cooperation

**Criteria:** The national cyber incident response team (CSIRT/CERT/CIRT) participates in international or regional cyber incident response formats.

Accepted evidence: Official website or official document

**What is measured:** This indicator assesses the country's membership and participation in international cooperation formats focusing on handling security vulnerabilities and cyber incident responses. The relevant organisations include FIRST, TF-CSIRT, AfricaCERT, CSIRTAmericas, OIC-CERT, or other regional CSIRT organisations operating at the global level and in other regions.

**Importance:** Membership in international and regional incident response organisations allows the national CSIRT to respond to security incidents more rapidly and effectively, cooperate and coordinate with other global and regional members on incident prevention, and facilitate information-sharing. These organisations may also offer additional services and resources to their members.

**Evidence**: Website or other documents by the relevant CSIRT umbrella organisations confirming the membership of the country's national CSIRT.

### **10 Cyber crisis management**

**Purpose and scope:** This NCSI capacity area addresses factors that determine the country's readiness to deal with large-scale cyber incidents or cyber-induced crises on a national level. It examines the preventive aspects of crisis management, such as consideration of cyber risks in national crisis scenarios and crisis plans. It also tracks whether such plans, crisis management processes, and skills are regularly tested and practiced in crisis exercises nationally and internationally. Finally, it surveys the level of readiness to engage other actors in support of the government's crisis management activities.

**Relevance:** A large-scale cyberattack or a cyber incident affecting critical services could lead to a broader national or societal crisis, affecting multiple sectors and causing cascading effects. As such, a country must proactively prepare for such cases by preparing relevant crisis management plans. Further preparations that a country can undertake include the development of national-level crisis management exercises – either fully focused on cybersecurity or having a cyber component – and/or participation in international cyber crisis management exercises. Finally, if a cyber crisis emerges, a swift response involving all relevant stakeholders is necessary in order to resolve the situation as quickly as possible. Involving cyber professionals as operational support in such cases can raise the effectiveness of the response and minimise damage from the incident if such reserves are planned and prepared beforehand.

#### **RESPONSIVE CYBERSECURITY INDICATORS**

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

#### **10.1 Cyber crisis management plan**

**Criteria**: The government has established a crisis management plan for large-scale cyber incidents.

#### Accepted evidence: Legal act or official website

**What is measured:** The indicator measures the existence of a national-level crisis plan for handling large-scale cyberattacks, incidents, or significant threats. This plan may be a separate cyber crisis-specific document, or cyber aspects may be integrated into a more comprehensive crisis plan. In either case, the plan should consider the specifics of cyber incidents and assign key roles regarding the

crisis management authority, parties involved, and their responsibilities.

**Importance:** Cyber crises differ from traditional crisis scenarios in that they can be expected to affect several sectors either directly or through secondary spill-over effects. A cyber crisis also requires the involvement and coordination of specific capabilities from a range of parties: technical knowledge and skills to analyse the threat vectors and methods involved; situational awareness, cyber intelligence, and analysis capabilities; support to restore affected assets; international coordination network; and public and international communication.

**Evidence**: A formally adopted crisis plan addressing national-scale events. Organisational crisis plans or crisis plans limited to a specific sector generally do not suffice. Where the plan or parts of it are classified, public evidence must at least confirm the existence of a valid crisis plan.

### **10.2 National cyber crisis management exercises**

**Criteria**: Regular interagency cyber crisis management exercises or crisis management exercises with a cyber component are arranged at the national level at least every other year.

**Accepted evidence**: Exercise document, official website, or press release

What is measured: The indicator checks for the practice of regular interagency crisis management exercises in which response to a large-scale cyber incident is practiced. Such exercises may be wholly concentrated on cybersecurity, or they may be comprehensive exercises that involve cyber components in their training scenarios.

Cyber crisis exercises may be held in various forms and at different levels. Exercises can test strategic decision-making, operational processes, or both. A tabletop exercise involves key personnel discussing simulated scenarios in an informal setting. This type of exercise is also used to assess plans, policies, and procedures. Exercises can also practice technical and operational aspects in a hands-on environment, with participants practicing incident mitigation techniques and cooperation.

**Importance:** Cyber exercises improve readiness to respond to and contain ongoing crises. These exercises also help reduce the likelihood that a cyber incident will escalate into a full-blown national crisis. In order to ensure that crisis plans are realistic and that those charged with various crisis management roles are up to the task, regular joint exercises should be held to test and improve cyber crisis plans and processes, and to practice cooperation with other parties.

Cyber crisis exercises should engage the country's political leadership, CI/CII/essential service providers, and organisations that have cybersecurity responsibilities. Ideally, such exercises also involve private sector actors such as CII operators.

**Evidence**: An official document or confirmation verifying an interagency cyber crisis management exercise or a national-level crisis management exercise with a cyber component in the past two years.

## **10.3 Participation in international cyber crisis exercises**

**Criteria**: The country participates in an international cyber crisis management exercise at least every other year.

Accepted evidence: Exercise document/website or press release

What is measured: In an international cyber crisis management exercise, relevant aovernment authorities from more than one country are jointly involved in preparation and execution. The purpose of international crisis exercises is to test and train cross-border cooperation. As with the previous indicator, such exercises may be wholly focused on cybersecurity or have a cyber component integrated into a broader training scenario. The exercise may be a bilateral or multilateral event or conducted in the framework of a regional or international organisation. Exercises delivered by one country or international organisation to another country with the aim of only testing the national processes within that country are not considered in the scope of this indicator.

**Importance:** International exercises are important learning tools for countries for practicing compatibility of crisis management procedures and cross-border cooperation. They are a useful tool from which countries with little or no crisis experience can draw knowledge and gain lessons and insights from those who have undergone such events. As cyber threats are growing more complex and severe, participating in international cyber crisis exercises

serves as a means for building better, more rapid responses.

**Evidence**: An official document or confirmation verifying participation in the planning and/or execution of an international (bilateral, multilateral, or regional) cyber crisis management exercise or a crisis management exercise with a cyber component in the past two years.

#### **10.4 Operational crisis reserve**

**Criteria**: A mechanism for engaging reserve support has been established to reinforce government bodies in managing cyber crises.

Accepted evidence: Legal act or official website

**What is measured:** Operational reserves or quick reaction forces may be arranged in different ways: as a special (volunteer) unit, emergency response

network, government reserve, or arrangements for assistance from the private sector. The fundamental matter is that the engagements must be formalised.

**Importance:** A large-scale incident tests any country's routine resources, and assistance beyond its own capacities can significantly help resolve a crisis. The option to count on the operational support of a crisis reserve of cybersecurity professionals gives the country additional volume, network, and skills when dealing with a cyber crisis. To ensure that the activities of such a reserve during a crisis are lawful and effective, its tasks and the procedure for calling on its assistance must be established beforehand.

**Evidence**: A legal act or official website demonstrating the existence of a formal basis to engage reserve support.

### 11 Fight against cybercrime

**Purpose and scope:** This NCSI capacity area measures the country's preparedness and commitment to combat cybercrime by establishing the necessary legislative measures, organisational frameworks, and international cooperation. Cybercrime involves criminal activities where computer systems and computer data are either a primary tool to commit a crime or a primary target of the crime. It includes offences against the confidentiality, integrity, and availability of computer systems or data, as well as traditional offences committed using computer systems (e.g. fraud, forgery) and content-related offences (e.g. online distribution of child pornography). The NCSI's main focus is on offences against the confidentiality, integrity, and availability of computer data and computer systems, as described in Articles 2-6 of the Convention on Cybercrime (Budapest Convention)<sup>7</sup> concerning illegal access, illegal interception, data interference, system interference, and misuse of devices.

**Relevance:** Cybercrime is increasing worldwide and causing significant damage to citizens, businesses, and governments. In recent years, cybercrime has also become more complicated and sophisticated. While most cybercrime is driven by financial profit, it can have a serious negative impact on the wellbeing, economy, and security of a country, in particular where cyberattacks are conducted on a large scale or target government systems and networks, e-services, and CII. Governments have a positive obligation to take legislative and other measures to protect the country from cybercrime and ensure that sufficient legislative and organisational frameworks exist to detect, respond to, and investigate those crimes.

#### **RESPONSIVE CYBERSECURITY INDICATORS**

- 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

## **11.1 Cybercrime offences in national law**

**Criteria**: Cybercrime offences are defined in national legislation.

#### Accepted evidence: Legal act

**What is measured:** The indicator tracks whether the following cybercrime offences are criminalised in national law: intentional access without right to a computer system (by infringing security measures) (*illegal access*); intentional interception by using technical means of non-public transmission of computer data without right (*illegal interception*); intentional damaging, deletion, deterioration, alteration or suppression of computer data without right (*data interference*); intentional serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data (system interference); and intentional commission of specific acts of a preparatory nature involving certain devices or

<sup>&</sup>lt;sup>7</sup> <u>https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185</u>

accessing data to be used to commit the cybercrime offences referred to above (*misuse of devices*).<sup>8</sup> The NCSI addresses cybercrime offences or cyberenabled offences targeting computer systems and data. Other computer-related or cyber-dependent offences are beyond the scope of the NCSI.

**Importance:** A legal basis to prevent and fight against cybercrime is a fundamental part of the national cybersecurity framework, needed to ensure an effective criminal justice response. As a point of reference, the NCSI relies on the Budapest Convention on Cybercrime, which is currently the only legally binding international instrument on cybercrime, has a global effect, and is also considered a standard for capacity building.

**Evidence**: Official legislative act, whether it is a distinct cybercrime act or provisions in a comprehensive penal code.

#### **11.2 Procedural law provisions**

**Criteria**: Legislation defines the powers and procedures for cybercrime investigations and proceedings and for the collection of electronic evidence.

#### Accepted evidence: Legal act

What is measured: National procedural law that, at the minimum, addresses investigative and prosecutorial powers and measures related to cybercrime, and the collection and handling of electronic evidence for investigating and prosecuting crimes. Such provisions should comprise the criminal justice measures needed for cybercrime investigation, including measures to preserve or secure computer data (*preservation order*); produce or obtain computer data (production order); seize, secure, search, or access computer systems, computer data, and storage media, as well as to issue

orders to obtain necessary information (*search and seizure*); and collect traffic data, intercept content, and compel service providers to collect and record data transmitted by means of a computer system in real time (*real-time interception*).<sup>9</sup>

**Importance:** While substantive law provisions criminalize acts regarded as cybercrime, procedural law measures are needed to start a criminal investigation and to collect or obtain computer data that can be used as electronic evidence in criminal proceedings. Without proper powers and measures to obtain and use electronic evidence, it is not possible to investigate cybercrime, identify potential suspects, and bring them to justice.

Effective and successful cybercrime investigations are a prerequisite to providing restitution to the victims, either in the form of compensation for damages suffered or recovery of property.

**Evidence**: The relevant procedural provisions may be contained in a separate (cybercrime) act or clearly integrated into a comprehensive code of criminal procedure. Generic clauses are not acceptable unless they also cover computer systems and computer data.

## **11.3 Ratification of or accession to the Convention on Cybercrime**

**Criteria**: The country has ratified or acceded to the Council of Europe (CoE) Convention on Cybercrime.

**Accepted evidence**: Legal act on Convention ratification or accession, website of the CoE Treaty Office

**What is measured:** Ratification of or accession to the CoE Convention on Cybercrime (the Budapest Convention).<sup>10</sup>

**Importance:** The Budapest Convention is currently the only legally binding international instrument on

<sup>&</sup>lt;sup>8</sup> More detail about the cybercrime offences (offences against confidentiality, integrity, and availability of computer systems and data) and their fundamental elements are provided by Articles 2-6 of the Budapest Convention on Cybercrime.

<sup>&</sup>lt;sup>9</sup> More detail about the relevant procedural measures are provided by Articles 16–21 of the Budapest Convention on Cybercrime.

<sup>&</sup>lt;sup>10</sup> <u>https://www.coe.int/en/web/conventions/full-</u> list?module=treaty-detail&treatynum=185

cybercrime. It addresses criminal offences committed against computer systems as well as computeroffences, child related pornography, and infringements of copyright and related rights. In addition to substantive law, the Convention also provides for procedural law measures to address computer data or electronic evidence, and a legal basis for international cooperation. It also contains a series of procedural powers, including to search computer systems and intercept computer data. The main objective of the Convention is to pursue a common criminal policy aimed at protecting society against cybercrime, especially by adopting the appropriate legislation and fostering international cooperation.

The Budapest Convention is open for accession to all countries. As of September 2022, there were 67 members, with twelve more in the accession process, representing all continents. The signing and ratification of the Convention, or, in the case of non-member states, acceding to the Convention, provides further legal basis and mechanisms for international cooperation among state parties, including the use of the 24/7 point-of-contact network. Therefore, participation in the Convention notably strengthens a country's possibilities to fight cybercrime. Other regional cybercrime conventions (e.g. African Union, Arab League) lack equivalent mechanisms and are therefore not tracked by the NCSI.

**Evidence**: National legal act on the ratification or accession to the Convention or official data published by the CoE Treaty Office<sup>11</sup> counts as evidence.

#### **11.4 Cybercrime investigation capacity**

**Criteria**: Law enforcement has a specialised function and capacity to prevent and investigate cybercrime offences.

Accepted evidence: Legal act or official website

**What is measured:** The purpose of this indicator is to assess the organisational capacity of the country to enforce cybercrime laws. Units with clear competencies and jurisdiction over cybercrime investigations, such as a Cybercrime or High-Tech Crime Unit, are considered to meet the criteria. The presence of a central specialised unit does not preclude additional local or regional units or officers.

**Importance:** Cybercrime investigations as well as criminal investigations involving electronic evidence require specialised skills and knowledge. Cybercrime investigations and the analysis of objects containing electronic evidence also require specific analytical training and knowledge of digital forensics.

Officers working in such units should have received specialised training that enables them to conduct investigations and use measures to obtain computer data. Specialised units also need to have the necessary powers to use more intrusive procedural measures such as search and seizure, and, in particular, real-time interception of communications (computer data) that might not be available to all units.

**Evidence**: Official recognition of a specialised cybercrime unit; a legal act, bylaw, or statute of the unit. Evidence of specialised cybercrime investigative staff serving within a broader unit (e.g. High-Tech or technology crime) is also accepted.

#### **11.5 Digital forensics capacity**

**Criteria**: Law enforcement has a specialised function and capacity for digital forensics.

**Accepted evidence**: Legal act, statute, official document, or official website

**What is measured:** This indicator considers the digital forensics capacity of law enforcement. Digital forensics is an area of forensic science that aims to obtain digital evidence, analyse it, and present it in

<sup>11</sup> https://www.coe.int/en/web/conventions/full-

list?module=signatures-by-treaty&treatynum=185

court. Its scope includes computer, mobile, network, and malware forensics. The NCSI assesses whether a designated authority or digital forensic laboratory is responsible for handling, extracting, and analysing digital evidence and conducting digital forensics examinations for criminal justice purposes. Since law enforcement is a state prerogative, private investigative entities are outside the scope of this indicator.

**Importance:** Almost any type of modern crime leaves electronic evidence or computer data that can serve as evidence in court proceedings; often it will be the only lead that law enforcement authorities and prosecutors can pursue and collect.

**Evidence**: Proof of the existence of a specialised unit or specialised staff serving within a broader unit (e.g. high-tech or technological crime forensics laboratory) is accepted as evidence.

## **11.6 24/7 contact point for international cybercrime**

**Criteria**: The government has designated an international 24/7 point of contact for assistance on cybercrime and electronic evidence.

**Accepted evidence**: Official website, legal act or statute

**What is measured:** This indicator assesses whether a point of contact has been established for criminal justice purposes that is operational 24 hours

a day, seven days a week, regardless of where this entity is located (for example, police, prosecutor's office, or another authority).

Importance: Electronic evidence is often stored in Therefore, foreign jurisdictions. criminal investigations often require crossа border/international request to obtain electronic evidence from other countries, including evidence bv multinational service providers. held As cybercrime can be of transborder nature and electronic evidence could be located in any country, it is also necessary to ensure that a point of contact is available and operational outside office hours. In urgent or emergency situations, another country might need to consult with the national point of contact. A 24/7 point of contact can also be used to quickly contact other countries to send requests and exchange information. Contact points can be used to transmit requests to obtain, preserve, and secure computer data, as well as for other forms of international cooperation and mutual assistance. Countries may also rely on other existing units or points of contact for 24/7 international cybercrime cooperation, such as Interpol.

**Evidence**: Officially appointed 24/7 point of contact for international cybercrime, including those designated in the framework of the Budapest Convention, Interpol, or other international cooperation formats in criminal matters.

### 12 Military cyber defence

**Purpose and scope:** This NCSI capacity area addresses defensive military cyber capacities with responsibility for the defence of the sovereignty, territorial integrity, and constitutional order of the country against external threats. The NCSI does not take into account military capabilities designed specifically for offensive cyber operations, nor does it assess capabilities related to units and activities that are considered classified or secret under domestic law. The indicators in this capacity area track military cyber entities, established mandates and oversight of the military use of cyber tools, and the practice of military cyber defence exercises.

**Relevance:** The use of cyber operations and cyberspace has become an established part of modern conflicts. The United Nations Charter recognises the right of states to individual or collective self-defence in case of an armed attack. Cyber defence is an important element of national defence capacity, and many countries are developing cyber units for military purposes. With military cyber units becoming an established part of national defence organisations, countries are obliged to ensure their full compliance with international law, including international humanitarian law.

#### **RESPONSIVE CYBERSECURITY INDICATORS**

12 Military cyber defence12.1 Military cyber defence capacity12.2 Military cyber doctrine12.3 Military cyber defence exercises

#### 12.1 Military cyber defence capacity

**Criteria**: Armed forces have designated units responsible for the cybersecurity of military operations and/or for cyber operations.

**Accepted evidence**: Legal act, statute, other official document or official website

What is measured: This indicator examines whether the country's armed forces (or other government-sponsored and militarily arranged organisations tasked with territorial defence) have designated entities that relate either to cyber operations or to the cybersecurity of military operations, with the corresponding tasks and mandates. Such entities can be organised as a distinct branch, service, or joint force, with their tasks usually involving ICT infrastructure operations, defensive and/or offensive cyberspace operations, cyber intelligence operations, and providing cyber advice to military commanders and units. This indicator considers command-level responsibility, without assessing the organisation's actual capacity to direct and control cyber operations in its own right.

**Importance:** Military cyber defence is an important component of overall national defence capacity against existential external threats, including those enabled or amplified by cyberspace.

**Evidence**: Official evidence of the existence of cyber units and their tasks as defined in the criteria.

#### **12.2 Military cyber doctrine**

**Criteria**: The tasks, principles, and oversight of armed forces for military cyber operations are established by official doctrine or legislation.

**Accepted evidence**: Legal act, official doctrine, or official website

**What is measured:** The role or tasks, principles, and oversight of the military regarding planning and conducting cyber operations are defined in legislation

or official doctrine. These documents establish a common, authorised framework to guide and set lawful boundaries for the military as it pursues national security objectives. Legislation or doctrine may include subjects such as the purpose, goals, uses, and authorisation related to the use of cyber capabilities.

Military doctrines may be fully or partially public, or access-restricted. To be considered by the NCSI, public evidence of their existence and of the presence of key components (tasks and oversight) is required.

**Importance:** Public doctrine stimulates lawfulness, predictability, and responsible behaviour by the armed forces engaging in cyber operations.

**Evidence**: Legal act, official doctrine, or official confirmation of their existence, with some details on the key components of these documents. A military strategy that does not define mandatory principles on the operational level does not qualify as evidence.

#### **12.3 Military cyber defence exercises**

**Criteria**: Armed forces have conducted or participated in a cyber defence exercise or an exercise with a cyber defence component in the past three years.

**Accepted evidence**: Official website or official document

What is measured: Engagement in both domestic and international exercises that practice the cyber defence tasks and responsibilities of the armed forces. The NCSI does not consider the particular type or level of the cyber defence exercise: these may be technical live-fire cyber defence exercises; strategic-level decision-making exercises; integrated technical-operational, cyber-kinetic, or civil-military exercises; military exercises with a cyber component; a crisis exercise with a military cyber component; or other.

**Importance:** Cyber defence exercises are an important mechanism for testing, improving, and practicing procedures and the skills needed to manage large-scale crisis scenarios, including civil-military cooperation.

**Evidence**: Official website or official document, including exercise document, website, or press release. The exercise must have taken place within the past three years.

### Indicator weights and scores

		Weight	Score
	STRATEGIC CYBERSECURITY INDICATORS	35	
	1. CYBERSECURITY POLICY	HIGH	15
1	1.1 High-level cybersecurity leadership		3
2	1.2 Cybersecurity policy development		3
3	1.3 Cybersecurity policy coordination		3
4	1.4 National cybersecurity strategy		3
5	1.5 National cybersecurity strategy action plan		3
	2. GLOBAL CYBERSECURITY CONTRIBUTION	LOW	6
6	2.1 Cyber diplomacy engagements		3
7	2.2 Commitment to international law in cyberspace		1
8	2.3 Contribution to international capacity building in cybersecurity		2
	3. EDUCATION AND PROFESSIONAL DEVELOPMENT	MEDIUM	10
9	3.1 Cyber safety competencies in primary education		2
10	3.2 Cyber safety competencies in secondary education		2
11	3.3 Undergraduate cybersecurity education		2
12	3.4 Graduate cybersecurity education		3
13	3.5 Association of cybersecurity professionals		1
	4. CYBERSECURITY RESEARCH AND DEVELOPMENT	LOW	4
14	4.1 Cybersecurity research and development programmes		2
15	4.2 Cybersecurity doctoral studies		2
	PREVENTIVE CYBERSECURITY INDICATORS	40	
	5. CYBERSECURITY OF CRITICAL INFORMATION INFRASTRUCTURE	HIGH	12
16	5.1 Identification of critical information infrastructure		3
17	5.2 Cybersecurity requirements for operators of critical information infrastructure		3
18	5.3 Cybersecurity requirements for public sector organisations		3
19	5.4 Competent supervisory authority		3
	6. CYBERSECURITY OF DIGITAL ENABLERS	MEDIUM	12
20	6.1 Secure electronic identification		2
21	6.2 Electronic signature		2
22	6.3 Trust services		2
23	6.4 Supervisory authority for trust services		2
24	6.5 Cybersecurity requirements for cloud services		2
25	6.6 Supply chain cybersecurity		2
	7. CYBER THREAT ANALYSIS AND AWARENESS RAISING	HIGH	12
26	7.1 Cyber threat analysis		3
27	7.2 Public cyber threat reports		3
28	7.3 Public cybersecurity awareness resources		3
29	7.4 Cybersecurity awareness raising coordination		3

	8. PROTECTION OF PERSONAL DATA	LOW	4
30	8.1 Personal data protection legislation		2
31	8.2 Personal data protection authority		2
	RESPONSIVE CYBERSECURITY INDICATORS	45	
	9. CYBER INCIDENT RESPONSE	HIGH	14
32	9.1 National incident response capacity		3
33	9.2 Incident reporting obligations		3
34	9.3 Cyber incident reporting tool		2
35	9.4 Single point of contact for international cooperation		3
36	9.5 Participation in international incident response cooperation		3
	10. CYBER CRISIS MANAGEMENT	MEDIUM	9
37	10.1 Cyber crisis management plan		2
38	10.2 National cyber crisis management exercises		3
39	10.3 Participation in international cyber crisis exercises		2
40	10.4 Operational crisis reserve		2
	11. FIGHT AGAINST CYBERCRIME	HIGH	16
41	11.1 Cybercrime offences in national law		3
42	11.2 Procedural law provisions		3
43	11.3 Ratification of or accession to the Convention on Cybercrime		2
44	11.4 Cybercrime investigation capacity		3
45	11.5 Digital forensics capacity		2
46	11.6 24/7 contact point for international cybercrime		3
	12. MILITARY CYBER DEFENCE	LOW	6
47	12.1 Military cyber defence capacity		2
48	12.2 Military cyber doctrine		2
49	12.3 Military cyber defence exercises		2
			120





Rotermanni 8, 10111, Tallinn, Estonia



www.ega.ee

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

