NCSI
national cyber security index

14. Austria 85.00

Population	**9.1** million	**14th**	**National Cyber Security Index**	||||||||||||||||| **85 %**
Area (km²)	**83.9** thousand	**N/A**	**Global Cybersecurity Index**	||||||||||||||||| **89 %**
GDP per capita ($)	**70.5** thousand	**22nd**	**E-Government Development Index**	||||||||||||||||||| **91 %**
		20th	**Network Readiness Index**	||||||||||||||| **66 %**

NCSI DEVELOPMENT TIMELINE
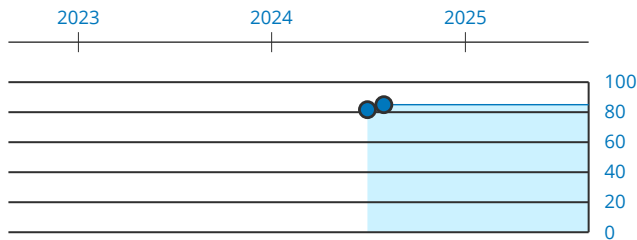
RANKING TIMELINE
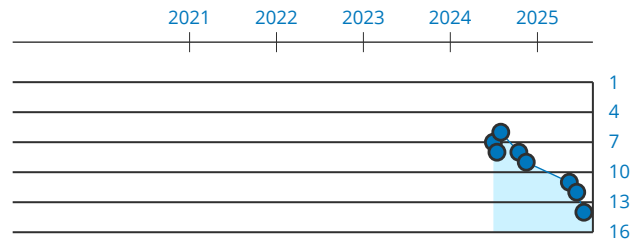
NCSI FULFILMENT PERCENTAGE

Policy · Global · Education · R&D · CII · Enablers · Awareness · Personal · CIRC · Crises · Police · Military
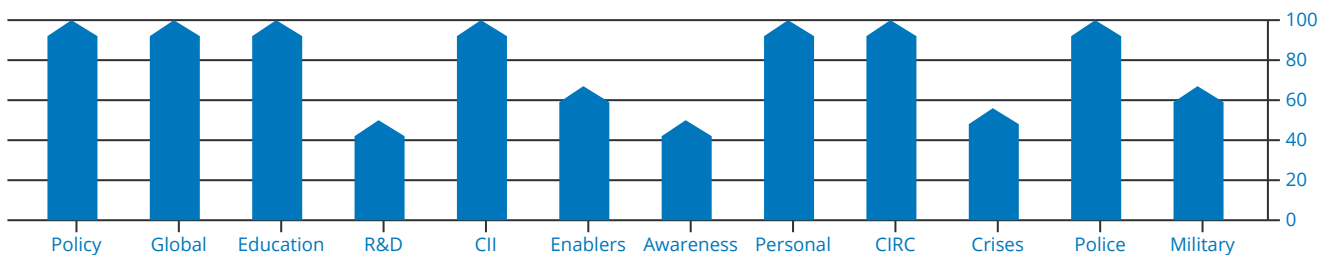
STRATEGIC CYBERSECURITY INDICATORS

1. CYBERSECURITY POLICY — 15 (100%)

1.1. High-level cybersecurity leadership	3
1.2. Cybersecurity policy development	3
1.3. Cybersecurity policy coordination	3
1.4. National cybersecurity strategy	3
1.5. National cybersecurity strategy action plan	3

2. GLOBAL CYBERSECURITY CONTRIBUTION — 6 (100%)

2.1. Cyber diplomacy engagements	3
2.2. Commitment to international law in cyberspace	1
2.3. Contribution to international capacity building in cybersecurity	2

3. EDUCATION AND PROFESSIONAL DEVELOPMENT — 10 (100%)

3.1. Cyber safety competencies in primary education	2
3.2. Cyber safety competencies in secondary education	2
3.3. Undergraduate cybersecurity education	2
3.4. Graduate cybersecurity education	3
3.5. Association of cybersecurity professionals	1

### 4. CYBERSECURITY RESEARCH AND DEVELOPMENT — 2 / 4 (50%)

|	
4.1. Cybersecurity research and development programmes	2
4.2. Cybersecurity doctoral studies	0 / 2

PREVENTIVE CYBERSECURITY INDICATORS

5. CYBERSECURITY OF CRITICAL INFORMATION INFRASTRUCTURE — 12 (100%)

5.1. Identification of critical information infrastructure — 3

5.2. Cybersecurity requirements for operators of critical information infrastructure — 3

5.3. Cybersecurity requirements for public sector organisations — 3

5.4. Competent supervisory authority — 3
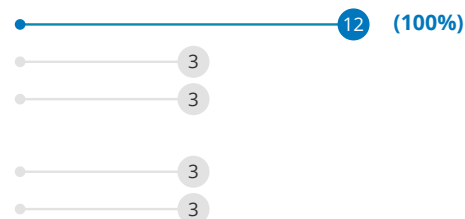
6. CYBERSECURITY OF DIGITAL ENABLERS — 8 / 12 (67%)

6.1. Secure electronic identification — 2

6.2. Electronic signature — 2

6.3. Trust services — 2

6.4. Supervisory authority for trust services — 2

6.5. Cybersecurity requirements for cloud services — 0 / 2

6.6. Supply chain cybersecurity — 0 / 2
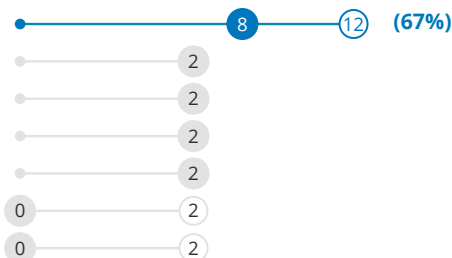
7. CYBER THREAT ANALYSIS AND AWARENESS RAISING — 6 / 12 (50%)

7.1. Cyber threat analysis — 0 / 3

7.2. Public cyber threat reports — 3

7.3. Public cybersecurity awareness resources — 3

7.4. Cybersecurity awareness raising coordination — 0 / 3
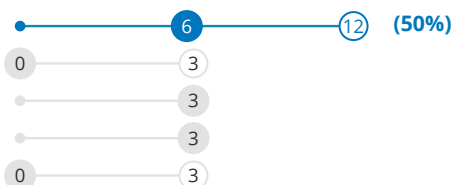
## 8. PROTECTION OF PERSONAL DATA — 4 (100%)

8.1. Personal data protection legislation — 2

8.2. Personal data protection authority — 2
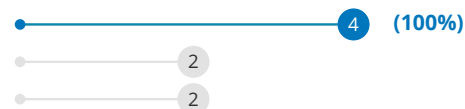
RESPONSIVE CYBERSECURITY INDICATORS

9. CYBER INCIDENT RESPONSE — 14 (100%)

9.1. National incident response capacity — 3

9.2. Incident reporting obligations — 3

9.3. Cyber incident reporting tool — 2

9.4. Single point of contact for international cooperation — 3

9.5. Participation in international incident response cooperation — 3
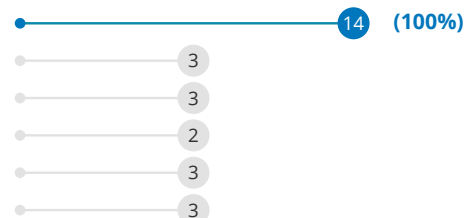
10. CYBER CRISIS MANAGEMENT — 5 / 9 (56%)

10.1. Cyber crisis management plan — 0 / 2

10.2. National cyber crisis management exercises — 3

10.3. Participation in international cyber crisis exercises — 2

10.4. Operational crisis reserve — 0 / 2
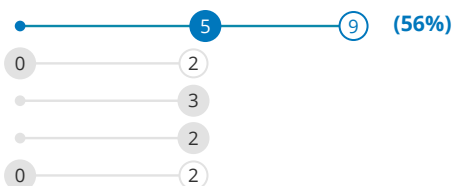
11. FIGHT AGAINST CYBERCRIME — 16 (100%)

11.1. Cybercrime offences in national law — 3

11.2. Procedural law provisions — 3

11.3. Ratification of or accession to the Convention on Cybercrime — 2

11.4. Cybercrime investigation capacity — 3

11.5. Digital forensics capacity — 2

11.6. 24/7 contact point for international cybercrime — 3

12. MILITARY CYBER DEFENCE — 4 / 6 (67%)

12.1. Military cyber defence capacity — 2

12.2. Military cyber doctrine — 0 / 2

12.3. Military cyber defence exercises — 2