NCSI
national cyber security index

2. Lithuania 93.51

Population	**2.9** million		2nd	**National Cyber Security Index**	|||||||||||||| **94 %**
Area (km²)	**65.3** thousand		6th	**Global Cybersecurity Index**	|||||||||||||| **98 %**
GDP per capita ($)	**34.1** thousand		41st	ICT Development Index	|||||||||||| **72 %**
			33rd	Networked Readiness Index	|||||||||||||||| **4 %**

NCSI DEVELOPMENT TIMELINE

2023   2024   2025

100
80
60
40
20
0

RANKING TIMELINE

2021   2022   2023   2024   2025

1
5
9
13
17
21
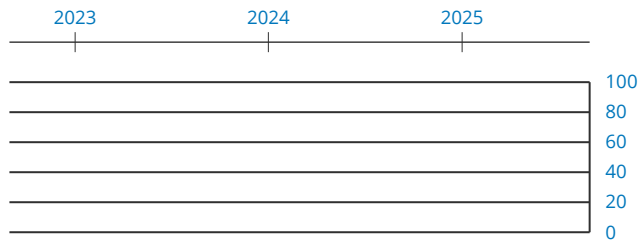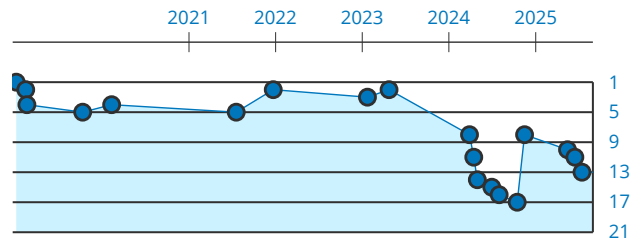
NCSI FULFILMENT PERCENTAGE

100
80
60
40
20
0

Policy · Threats · Education · Global · Digital · Essential · eID & TS · Personal · CIRC · Crisis · Police · Military
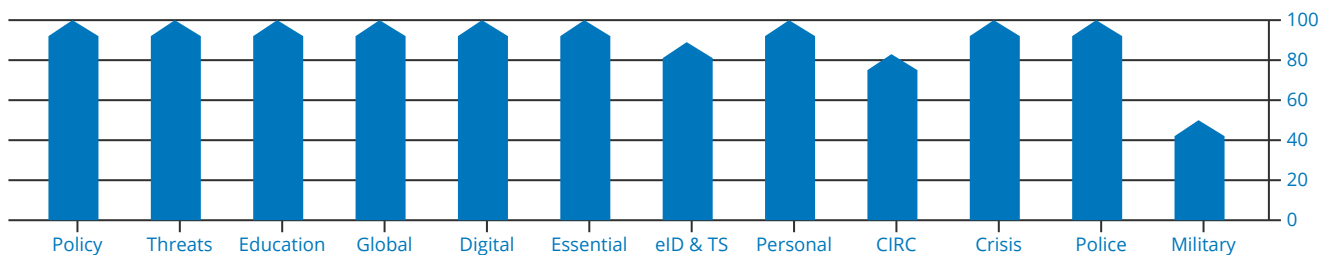
GENERAL CYBER SECURITY INDICATORS

1. Cyber security policy development — 7 **(100%)**

1.1. Cyber security policy unit — 3
1.2. Cyber security policy coordination format — 2
1.3. Cyber security strategy — 1
1.4. Cyber security strategy implementation plan — 1

2. Cyber threat analysis and information — 5 **(100%)**

2.1. Cyber threats analysis unit — 3
2.2. Public cyber threat reports are published annually — 1
2.3. Cyber safety and security website — 1

3. Education and professional development — 9 **(100%)**

3.1. Cyber safety competencies in primary or secondary education — 1
3.2. Bachelor's level cyber security programme — 2
3.3. Master's level cyber security programme — 2
3.4. PhD level cyber security programme — 2
3.5. Cyber security professional association — 2

### 4. Contribution to global cyber security — 6 **(100%)**

4.1. Convention on Cybercrime — 1
4.2. Representation in international cooperation formats — 1
4.3. International cyber security organisation hosted by the country — 3
4.4. Cyber security capacity building for other countries — 1

BASELINE CYBER SECURITY INDICATORS

5. Protection of digital services — 5 (100%)

5.1. Cyber security responsibility for digital service providers — 1

5.2. Cyber security standard for the public sector — 1

5.3. Competent supervisory authority — 3
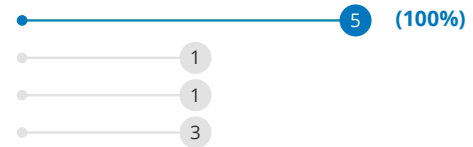
6. Protection of essential services — 6 (100%)

6.1. Operators of essential services are identified — 1

6.2. Cyber security requirements for operators of essential services — 1

6.3. Competent supervisory authority — 3

6.4. Regular monitoring of security measures — 1

7. E-identification and trust services — 8 / 9 (89%)

7.1. Unique persistent identifier — 1

7.2. Requirements for cryptosystems — 0 / 1

7.3. Electronic identification — 1

7.4. Electronic signature — 1

7.5. Timestamping — 1

7.6. Electronic registered delivery service — 1

7.7. Competent supervisory authority — 3
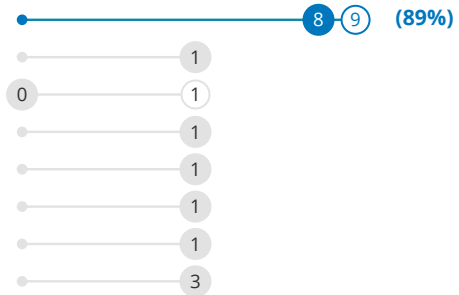
8. Protection of personal data — 4 (100%)

8.1. Personal data protection legislation — 1

8.2. Personal data protection authority — 3
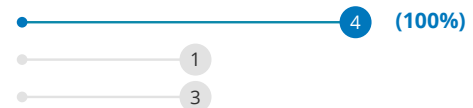
INCIDENT AND CRISIS MANAGEMENT INDICATORS

9. Cyber incidents response — 5 / 6 (83%)

9.1. Cyber incidents response unit — 3

9.2. Reporting responsibility — 0 / 1

9.3. Single point of contact for international coordination — 2

10. Cyber crisis management — 5 (100%)

10.1. Cyber crisis management plan — 1

10.2. National-level cyber crisis management exercise — 2

10.3. Participation in international cyber crisis exercises — 1

10.4. Operational support of volunteers in cyber crises — 1
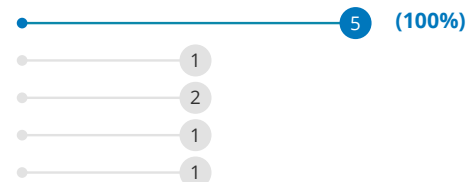
11. Fight against cybercrime — 9 (100%)

11.1. Cybercrimes are criminalised — 1

11.2. Cybercrime unit — 3

11.3. Digital forensics unit — 3

11.4. 24/7 contact point for international cybercrime — 2
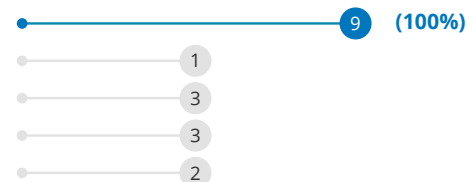
12. Military cyber operations — 3 / 6 (50%)

12.1. Cyber operations unit — 0 / 3

12.2. Cyber operations exercise — 2

12.3. Participation in international cyber exercises — 1