NCSI
national cyber security index

88. Myanmar 21.67

Population	**54.1** million	88th	**National Cyber Security Index**	‖‖‖‖‖‖‖‖‖‖‖ **22 %**
Area (km²)	**676.6** thousand	N/A	**Global Cybersecurity Index**	‖‖‖‖‖‖‖‖‖‖‖ **74 %**
GDP per capita ($)	**6.0** thousand	138th	**E-Government Development Index**	‖‖‖‖‖‖‖‖‖‖‖ **50 %**
		N/A	**Network Readiness Index**	‖‖‖‖‖‖‖‖‖‖‖ **0 %**

NCSI DEVELOPMENT TIMELINE
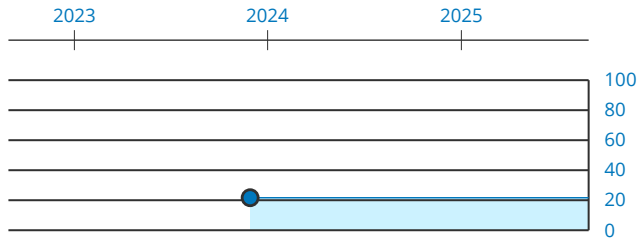
RANKING TIMELINE
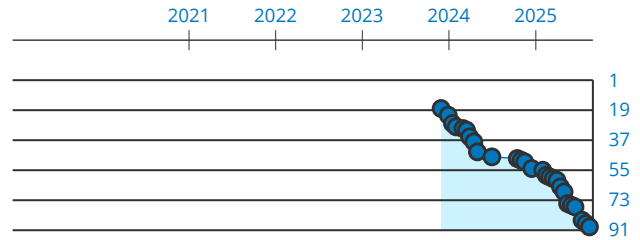
NCSI FULFILMENT PERCENTAGE

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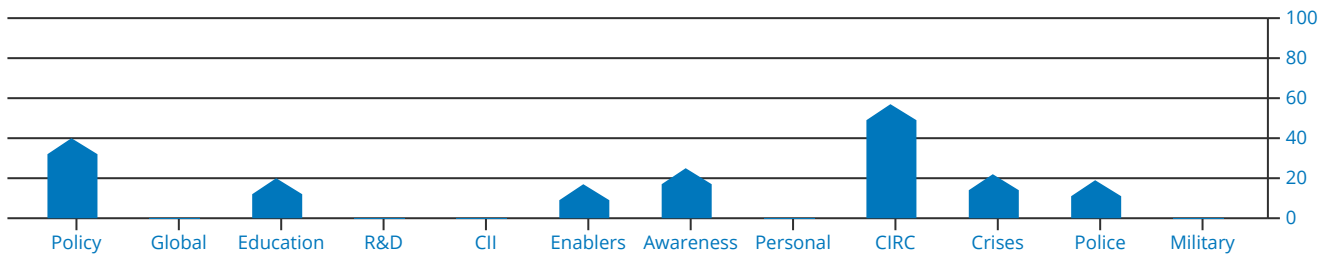
STRATEGIC CYBERSECURITY INDICATORS

1. CYBERSECURITY POLICY — 6 / 15 **(40%)**

|	
1.1. High-level cybersecurity leadership	0 — 3
1.2. Cybersecurity policy development	— 3
1.3. Cybersecurity policy coordination	0 — 3
1.4. National cybersecurity strategy	— 3
1.5. National cybersecurity strategy action plan	0 — 3
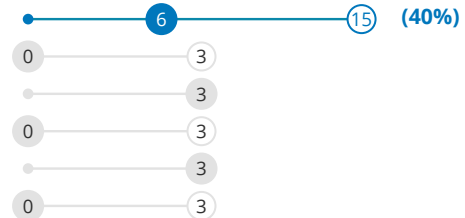
2. GLOBAL CYBERSECURITY CONTRIBUTION — 0 / 6 **(0%)**

2.1. Cyber diplomacy engagements	0 — 3
2.2. Commitment to international law in cyberspace	0 — 1
2.3. Contribution to international capacity building in cybersecurity	0 — 2

3. EDUCATION AND PROFESSIONAL DEVELOPMENT — 2 / 10 **(20%)**

3.1. Cyber safety competencies in primary education	0 — 2
3.2. Cyber safety competencies in secondary education	0 — 2
3.3. Undergraduate cybersecurity education	— 2
3.4. Graduate cybersecurity education	0 — 3
3.5. Association of cybersecurity professionals	0 — 1
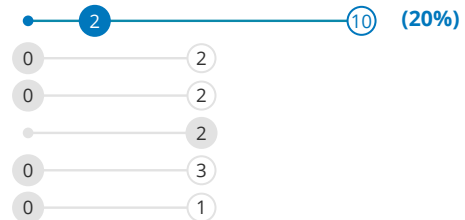
4. CYBERSECURITY RESEARCH AND DEVELOPMENT — 0 / 4 **(0%)**

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

PREVENTIVE CYBERSECURITY INDICATORS

5. CYBERSECURITY OF CRITICAL INFORMATION INFRASTRUCTURE — 0 / 12 (0%)

5.1. Identification of critical information infrastructure — 0 / 3
5.2. Cybersecurity requirements for operators of critical information infrastructure — 0 / 3
5.3. Cybersecurity requirements for public sector organisations — 0 / 3
5.4. Competent supervisory authority — 0 / 3

6. CYBERSECURITY OF DIGITAL ENABLERS — 2 / 12 (17%)

6.1. Secure electronic identification — 0 / 2
6.2. Electronic signature — 2
6.3. Trust services — 0 / 2
6.4. Supervisory authority for trust services — 0 / 2
6.5. Cybersecurity requirements for cloud services — 0 / 2
6.6. Supply chain cybersecurity — 0 / 2

7. CYBER THREAT ANALYSIS AND AWARENESS RAISING — 3 / 12 (25%)

7.1. Cyber threat analysis — 0 / 3
7.2. Public cyber threat reports — 0 / 3
7.3. Public cybersecurity awareness resources — 3
7.4. Cybersecurity awareness raising coordination — 0 / 3

8. PROTECTION OF PERSONAL DATA — 0 / 4 (0%)

8.1. Personal data protection legislation — 0 / 2
8.2. Personal data protection authority — 0 / 2

RESPONSIVE CYBERSECURITY INDICATORS

9. CYBER INCIDENT RESPONSE — 8 / 14 (57%)

9.1. National incident response capacity — 3
9.2. Incident reporting obligations — 0 / 3
9.3. Cyber incident reporting tool — 2
9.4. Single point of contact for international cooperation — 0 / 3
9.5. Participation in international incident response cooperation — 3

10. CYBER CRISIS MANAGEMENT — 2 / 9 (22%)

10.1. Cyber crisis management plan — 0 / 2
10.2. National cyber crisis management exercises — 0 / 3
10.3. Participation in international cyber crisis exercises — 2
10.4. Operational crisis reserve — 0 / 2
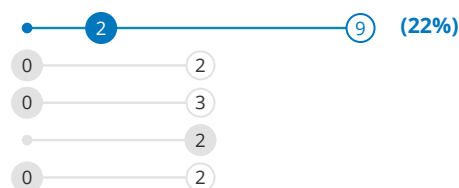
11. FIGHT AGAINST CYBERCRIME — 3 / 16 (19%)

11.1. Cybercrime offences in national law — 3
11.2. Procedural law provisions — 0 / 3
11.3. Ratification of or accession to the Convention on Cybercrime — 0 / 2
11.4. Cybercrime investigation capacity — 0 / 3
11.5. Digital forensics capacity — 0 / 2
11.6. 24/7 contact point for international cybercrime — 0 / 3
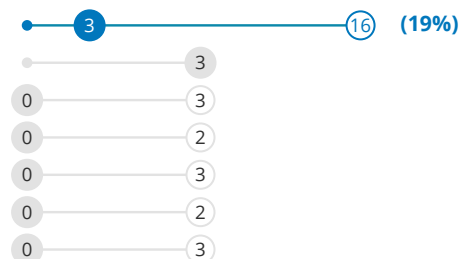
12. MILITARY CYBER DEFENCE — 0 / 6 (0%)

12.1. Military cyber defence capacity — 0 / 2
12.2. Military cyber doctrine — 0 / 2
12.3. Military cyber defence exercises — 0 / 2