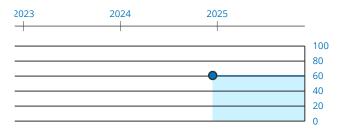


59. Bahrain 60.83

Population 1.6 million
Area (km²) 0.8 thousand
GDP per capita (\$) 63.5 thousand

59th National Cyber Security Index ||||||||||||| 61 %
N/A Global Cybersecurity Index ||||||||||||||| 98 %
18th E-Government Development Index ||||||||||||| 92 %
51st Network Readiness Index ||||||||||||| 54 %

NCSI DEVELOPMENT TIMELINE

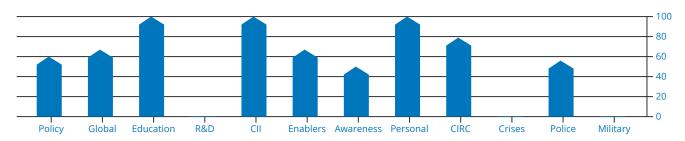


RANKING TIMELINE

0



NCSI FULFILMENT PERCENTAGE



STRATEGIC CYBERSECURITY INDICATORS

1. CYBERSECURITY POLICY

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

9 (60%) 3 3 0 3

2. GLOBAL CYBERSECURITY CONTRIBUTION

- 2.1. Cyber diplomacy engagements
- 2.2. Commitment to international law in cyberspace
- ${\it 2.3.} \ Contribution \ to \ international \ capacity \ building \ in \ cybersecurity$



3

3

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

0 2 10 (100%) 2 2 2 2 3 3 1

4. CYBERSECURITY RESEARCH AND DEVELOPMENT

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



PREVENTIVE CYBERSECURITY INDICATORS

5. CYBERSECURITY OF CRITICAL INFORMATION INFRASTRUCTURE	•			(100%)
5.1. Identification of critical information infrastructure	•	3		
5.2. Cybersecurity requirements for operators of critical information	•	3		
infrastructure				
5.3. Cybersecurity requirements for public sector organisations	•	3		
5.4. Competent supervisory authority	•	3		
6. CYBERSECURITY OF DIGITAL ENABLERS	•	8		(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	•	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	•		4	(100%)
8.1. Personal data protection legislation	•	2		
8.2. Personal data protection authority	•	2		
RESPONSIVE CYBERSECURITY INDICATORS				
9. CYBER INCIDENT RESPONSE			11	(79%)
9.1. National incident response capacity		3		(1270)
9.2. Incident reporting obligations		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	0			(0%)
10.1. Cyber crisis management plan	0			
10.2. National cyber crisis management exercises	0	3		
10.3. Participation in international cyber crisis exercises	0			
10.4. Operational crisis reserve	0			
11. FIGHT AGAINST CYBERCRIME	•	9	<u>(16)</u>	(56%)
11.1. Cybercrime offences in national law		3		(2211)
11.2. Procedural law provisions		3		
11.3. Ratification of or accession to the Convention on Cybercrime	0	2		
11.4. Cybercrime investigation capacity	•	3		
11.5. Digital forensics capacity	0			
11.6. 24/7 contact point for international cybercrime	0	3		
12. MILITARY CYBER DEFENCE	0		<u></u>	(0%)
12.1. Military cyber defence capacity	0			-
12.2. Military cyber doctrine	0			
12.3. Military cyber defence exercises	0			



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

Rotermanni 8 10111 Tallinn Estonia P: +372 663 1500 E: ncsi@ega.ee W: www.ega.ee