

27. Hungary 83.33

Population 10.6 million Area (km²) 93.0 thousand GDP per capita (\$) **45.0** thousand 27th National Cyber Security Index N/A Global Cybersecurity Index E-Government Development Index |||||||||| 80 % **Network Readiness Index** |||||||| 55 %

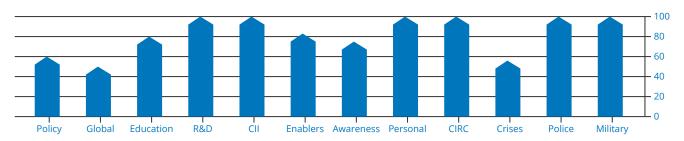
NCSI DEVELOPMENT TIMELINE







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

(60%) 3 3 0 3

- 3
- 0 3

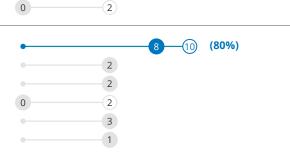
2. GLOBAL CYBERSECURITY CONTRIBUTION

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

(50%) 3 0 (1)

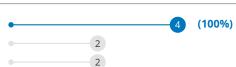
3. EDUCATION AND PROFESSIONAL DEVELOPMENT

- 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



4. CYBERSECURITY RESEARCH AND DEVELOPMENT

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



PREVENTIVE CYBERSECURITY INDICATORS

6.3. Trust services 6.4. Supervisory authority for trust services 6.5. Cybersecurity requirements for cloud services 6.6. Supply chain cybersecurity 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 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection legislation	5. CYBERSECURITY OF CRITICAL INFORMATION INFRASTRUCTURE	•			(100%)
infrastructure 5.3. Qivbersecurity requirements for public sector organisations 5.4. Competent supervisory authority 5.6. CYBERSECURITY OF DIGITAL ENABLERS 6.1. Secure electronic identification 6.2. Electronic signature 6.2. Electronic signature 6.3. Electronic signature 6.4. Supervisory authority for trust services 6.5. Ophersecurity requirements for cloud services 6.5. Supervisory authority for trust services 6.5. Supervisory authority requirements for cloud services 7.1. Opher therat analysis 7.2. Public cyber security awareness resources 7.3. Public cyber threat reports 7.4. Ophersecurity awareness resources 7.5. A public cyber security awareness resources 7.6. Supervisor of the formation allowity and the security awareness resources 7.7. Ophersecurity awareness resources 7.8. Personal data protection legislation 8. Personal data protection legislation 8. Personal data protection authority 8. Personal data protection authority 8. Supervisor of PERSONAL DATA 8.1. Personal data protection authority 8. Supervisor of PERSONAL 8. Personal data protection authority 8. Supervisor of PERSONAL 8. Personal data protection authority 8. Supervisor of PERSONAL 8. Personal data protection authority 8. Supervisor of PERSONAL 8. Personal data protection authority 8. Personal data protection authority 9. Cyber indicate reporting obligations 9. Cyber indicate reporting obligations 9. Supervisor of PERSONAL 9. Cyber indicate reporting tool 9. Supervisor of PERSONAL 9. Cyber indicate reporting tool 9. Supervisor of PERSONAL 9. Cyber indicate reporting obligations 9. Supervisor of PERSONAL 9. Cyber indicate repo	5.1. Identification of critical information infrastructure	•	3		
5.3. Cybersecurity requirements for public sector organisations 5.4. Competent supervisory authority 3 6. CYBERSECURITY OF DIGITAL ENABLERS 6.1. Secure electronic identification 2. 6.2. Electronic signature 2. 6.3. Trust services 3. Trust services 3. 2. 6.4. Supervisory authority for trust services 5.5. Cybersecurity requirements for cloud services 6.5. Opersecurity requirements for cloud services 6.5. Opersecurity requirements for cloud services 6.5. Opersecurity requirements for cloud services 6.6. Supply chain cybersecurity 2 7. CYBER THREAT ANALYSIS AND AWARENESS RAISING 7.1. Opber threat analysis 7.2. Public cyber threat reports 7.3. Public cyber threat reports 7.3. Public cyber security awareness resources 7.4. Cybersecurity awareness raising coordination 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection legislation 8.2. Personal data protection legislation 8.2. Personal data protection authority 7. Public cyber trists and data protection authority 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection authority 9. CYBER INCIDENT RESPONSE 9. CYBER INCIDENT RESPONSE 9.1. Anional incident response capacity 9.2. Indient 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 9.5. Participation in international cyber crisis exercises 10.3. Participation in international cyber crisis exercises 10.4. Operational crisis reserve 10.1. Cyber crisis management plan 10. CYBER CRISIS MANAGEMENT 10.4. Operational crisis reserve 10. 2 11. FIGHT AGAINST CYBERCEIME 11.1. Cybercrime offences in national law 11.2. Proceedural law provisions 11.3. Ratification of or accession to the Convention on Cybercrime 11.4. Cybercrime investigation capacity 11.5. Upital forenisc capacity 11.6. 24/7 contact point for international cybercrime 11.2. Milliary cyber defence capacity 12.2. Milliary cyber defence capacity 12.2. Milliary cyber defence capacity	5.2. Cybersecurity requirements for operators of critical information	•	3		
5.4. Competent supervisory authority 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 6.5. Cybersecurity requirements for cloud services 6.5. Supervisory authority for trust services 7.1. Cyber threat analysis 7.1. Cyber threat analysis 7.2. Public cyber threat reports 7.3. Public cyber threat reports 7.4. Cybersecurity awareness resources 7.4. Cybersecurity awareness resources 7.5. Public cyber threat reports 7.6. Cybersecurity awareness resources 7.7. Cybersecurity awareness raising coordination 7. Supervisory awareness raising coordination 7. Supervisory awareness raising coordination 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection legislation 8.2. Personal data protection authority 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection legislation 8.2. Presonal data protection authority 9. CYBER INCIDENT RESPONSE 9. CYBER INCIDENT RESPONSE 9.1. National incident response capacity 9.2. Incident reporting boil audions 9.3. Cyber incident response capacity 9.5. Participation in international incident response cooperation 9.5. Participation in international incident response cooperation 9.5. Participation in international pyber crisis exercises 10.4. Operational crisis reserve 10. Cyber Crisis management exercises 10.4. Operational crisis reserve 10. Cyber Crisis management exercises 10.4. Operational crisis reserve 10. Cyber Crisis management exercises 10.4. Operational crisis reserve 10. Cyber Crisis management exercises 10.4. Operational crisis reserve 10. Cyber Crisis management exercises 10.4. Operational crisis reserve 10. Cyber Crisis management ex	infrastructure				
6. CYBERSECURITY OF DIGITAL ENABLERS 6.1. Secure electronic identification 6.2. Electronic signature 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 7. CYBER THREAT ANALYSIS AND AWARENESS RAISING 7. CYBER THREAT ANALYSIS AND AWARENESS RAISING 7. Cyber threat analysis 7.2. Public cyber threat reports 7.3. Public cyber threat reports 7.4. Cyber security waverness resources 7.5. Cyber threat analysis 7.5. Public cyber security waverness resources 7.6. Cybersecurity waverness raising coordination 7.6. PROTECTION OF PERSONAL DATA 7.6. PROTECTION OF PERSONAL DATA 7.7. Personal data protection legislation 7.7. Personal data protection authority 7. Personal data protection authority 7. Personal data protection legislation 7. Personal data protection authority 7. PRESPONSIVE CYBERSECURITY INDICATORS 7. Personal data protection authority 7. Personal data protection legislation 7. Personal data protection authority 7. Personal d	5.3. Cybersecurity requirements for public sector organisations	•	3		
6.1. Secure electronic identification 6.2. Electronic signature 6.2. Electronic signature 6.3. Frust services 6.4. Supervisory authority for trust services 6.5. Cybersecurity requirements for cloud services 6.5. Cybersecurity requirements for cloud services 6.5. Superly chain cybersecurity 7. CYBER THREAT ANALYSIS AND AWARENESS RAISING 7.1. Cyber threat analysis 7.2. Public cyber threat reports 7.3. Public cyber security awareness resources 7.3. Public cybersecurity awareness resources 7.3. Public cybersecurity awareness raising coordination 8. PROTECTION OF PERSONAL DATA 8. PROTECTION OF PERSONAL DATA 8. PERSONAL DATA 8. Personal data protection legislation 8. PERSONSIVE CYBERSECURITY INDICATORS 9. CYBER INCIDENT RESPONSE 9. Single point of contact for international cooperation 9. S. Participation in international incident response cooperation 9. S. Participation in international dyber crisis exercises 9. Cyber crisis management exercises 9. C	5.4. Competent supervisory authority	•	3		
6.2. Electronic signature 6.3. Trust services 6.5. Superly subtrority for trust services 6.5. Cybersecurity requirements for cloud services 6.6. Superly chain cybersecurity 7. CYBER THREAT ANALYSIS AND AWARENESS RAISING 7.1. Cyber threat analysis 7.2. Public cyber threat reports 7.3. Public cyber security awareness resources 7.4. Cybersecurity awareness raising coordination 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection legislation 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection authority 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection authority 8. PROTECTION OF PERSONAL DATA 9. CYBER NICIDENT RESPONSE 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 9.5. Participation in international incident response cooperation 9.5. Participation in international cyber crisis exercises 10.4. Operational crisis reserve 10.2 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 11.5. Digital forensics capacity 11.6. 24/7 contact point for international cybercrime 12. MILITARY CYBER DEFENCE 12. Military cyber defence capacity 12.2. Military cyber defence capacity	6. CYBERSECURITY OF DIGITAL ENABLERS	•		10—12	(83%)
6.3. Trust services 6.4. Supervisory authority for trust services 6.5. Cybersecurity requirements for cloud services 6.6. Supply chain cybersecurity 7. CYBER THREAT ANALYSIS AND AWARENESS RAISING 7.1. Cyber threat analysis 7.2. Public cyber threat reports 7.3. Public cyber security awareness resources 7.3. Public cybersecurity awareness resources 7.4. Cybersecurity awareness rating coordination 8. PROTECTION OF PERSONAL DATA 8. PROTECTION OF PERSONAL DATA 8. Personal data protection legislation 9. Personal data protection authority 7. Personal data protection authority 8. PROTECTION OF PERSONAL DATA 9. Personal data protection authority 8. Personal data protection authority 8. Personal data protection legislation 9. Cyber Incident response 9. Cyber Incident response capacity 9. Protection of the protection authority 9. Protection authority 9. Protectio	6.1. Secure electronic identification	•	2		
6.4. Supervisory authority for trust services 6.5. Cybersecurity requirements for cloud services 6.6. Supply chain cybersecurity 2 7. CYBER THREAT ANALYSIS AND AWARENESS RAISING 7. Cyber threat analysis 7.2. Public cyber threat reports 7.3. Public cyber threat reports 7.3. Public cyber threat reports 7.4. Cybersecurity awareness resources 7.5. Public cybersecurity awareness raising coordination 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection authority 8.2. Personal data protection authority 9. CyBER INCIDENT RESPONSE 9. CyBER INCIDENT RESPONSE 9. Cyber incident reporting obligations 9.3. Cyber incident reporting obligations 9.3. Syber incident reporting obligations 9.4. Single point of contact for international cooperation 9.5. Participation in international incident response cooperation 9.5. Participation in international incident response cooperation 9.5. Participation in international cyber crisis exercises 10.1. Cyber crisis management plan 10. 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. 2 11. FIGHT AGAINST CYBER CRIME 11. Cybercrime offences in national law 11. Cybercrime offences in national law 11. Cybercrime offences in national law 11. Spitial forensics capacity 11. Digital forensics capacity 11. Spitial forensics capacity 12. Military cyber defence capacity	6.2. Electronic signature	•	2		
6.5. Cybersecurity requirements for cloud services 6.6. Supply chain cybersecurity 2 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 resources 7.5. Public cybersecurity awareness resources 7.6. Cybersecurity awareness resources 7.7. Eyersonal data protection legislation 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection authority 8. PERSONIVE CYBERSECURITY INDICATORS 9. CYBER INCIDENT RESPONSE 9. CYBER INCIDENT RESPONSE 9. Incident reporting obligations 9. Subject incident reporting obligations 9. Subject incident reporting tool 9. Subject incident reporting tool 9. Subject incident response capacity 9. Incident reporting tool 9. Subject incident response cooperation 9. Subject incident reporting tool 9. Participation in international incident response cooperation 9. Subject incident reporting tool 9. Participation in international cyber crisis exercises 10. Cyber crisis management plan 10. Cyber crisis management plan 10. Cyber crisis management plan 10. Cyber crisis management exercises 10. A Operational crisis reserve 10. Cybercrime offences in national law 11. I Cybercrime offences in national law 11. Procedural law provisions 11. Raiffication of or accession to the Convention on Cybercrime 11. Cybercrime investigation capacity 11. So Digital forensics capacity 12. Military cyber defence capacity	6.3. Trust services	•	2		
6.6. Supply chain cybersecurity 7. CYBER THREAT ANALYSIS AND AWARENESS RAISING 7.1. Cyber threat analysis 7.2. Public cyber threat reports 7.3. Public cyber threat reports 7.4. Cybersecurity awareness resources 7.5. Public cybersecurity awareness resources 7.6. Cybersecurity awareness raising coordination 8. PROTECTION OF PERSONAL DATA 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection legislation 8.2. Personal data protection authority 8.2. Personal data protection authority 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection authority 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection authority 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection authority 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection legislation 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection legislation 8. PROTECTION OF PERSONAL DATA 9. (100%) 9. S. PROTECTION OF PERSONAL DATA	6.4. Supervisory authority for trust services	•	2		
7.1. CyBert THREAT ANALYSIS AND AWARENESS RAISING 7.1. Cyber threat analysis 7.2. Public cyber threat reports 7.3. Public cyber threat reports 7.3. Public cyber threat reports 7.4. Cybersecurity awareness resources 7.4. Cybersecurity awareness raising coordination 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection legislation 8.2. Personal data protection authority 8.2. Personal data protection authority 8.2. Personal data protection authority 8.2. Presonal data protection authority 9.2. Incident reporting tool 9.3. Cyber incident response capacity 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 9.5. Participation in international incident response cooperation 9.6. Vyber crisis management plan 10. Cyber crisis management plan 10. Lyber crisis management exercises 10.3. Participation in international cyber crisis exercises 10.4. Operational crisis reserve 10.5. Operational crisis reserve 10.6. (100%) 11.1. Cyber crisis management exercises 10.3. Participation in international 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 11.5. Digital forensics capacity 11.5. Digital forensics capacity 12. Military cyber defence capacity 12. Military cyber defence capacity 12. Limilitary cyber defence capacity	6.5. Cybersecurity requirements for cloud services	0	2		
7.1. Cyber threat analysis 7.2. Public cyber threat reports 3 7.3. Public cyber security awareness resources 7.4. Cybersecurity awareness resources 7.5. Public cybersecurity awareness resources 7.6. Cybersecurity awareness raising coordination 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection legislation 8.2. Personal data protection authority 8.2. Personal data protection authority 8.2. Personal data protection authority 8.3. Cyber Incident response capacity 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 9.6. Participation in international incident response cooperation 9.7. Cyber crisis management plan 10. Cyber crisis management exercises 10.3. Participation in international cyber crisis exercises 10.4. Operational crisis reserve 10. 2 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 11.4. Cybercrime investigation capacity 11.5. Digital forensics capacity 11.6. 24/7 contact point for international cybercrime 12. Militrary cyber defence capacity 12.2. Militrary cyber defence capacity 12.2. Militrary cyber defence capacity	6.6. Supply chain cybersecurity	•	2		
7.2. Public cyber threat reports 7.3. Public cybersecurity awareness resources 7.4. Cybersecurity awareness raising coordination 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection legislation 8.2. Personal data protection legislation 8.2. Personal data protection authority 8.2. Personal data protection authority 8.3. Cyber Incident response capacity 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 9.6. Participation in international incident response cooperation 9.7. Participation in international response cooperation 9.8. Participation in international response cooperation 9.9. Participation in international response cooperation 9.1. Cyber crisis management plan 10.2. National cyber crisis management exercises 10.3. Participation in international cyber crisis exercises 10.4. Operational crisis reserve 10.2 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 12. Militrary cyber defence capacity	7. CYBER THREAT ANALYSIS AND AWARENESS RAISING	•	9		(75%)
7.3. Public cybersecurity awareness resources 7.4. Cybersecurity awareness raising coordination 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection legislation 8.2. Personal data protection legislation 8.2. Personal data protection authority 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 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. 2 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 12. MILITARY CYBER DEFENCE 12.1. Militrary cyber defence capacity 12.2. Militrary cyber defence capacity	7.1. Cyber threat analysis	•	3		
7.4. Cybersecurity awareness raising coordination 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection legislation 8.2. Personal data protection authority 2. 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 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 10.4. Operational crisis reserve 10.5. Digital forensics capacity 11.5. Digital forensics capacity 11.6. 24/7 contact point for international cybercrime 11.6. 24/7 contact point for international cybercrime 12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 12.2. Military cyber defence capacity	7.2. Public cyber threat reports	•	3		
8. PROTECTION OF PERSONAL DATA 8. 1. Personal data protection legislation 8. 2. Personal data protection legislation 8. 2. Personal data protection authority 2 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 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 10.4. Operational crisis reserve 10.5. Procedural law provisions 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 11.5. Digital forensics capacity 11.6. 24/7 contact point for international cybercrime 12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 12.2. Military cyber defence capacity	7.3. Public cybersecurity awareness resources	•	3		
8.1. Personal data protection legislation 8.2. Personal data protection authority RESPONSIVE CYBERSECURITY INDICATORS 9. CYBER INCIDENT RESPONSE 9. 1. National incident response capacity 9. 2. Incident reporting obligations 9. 3. Cyber incident reporting obligations 9. 4. Single point of contact for international cooperation 9. 5. Participation in international incident response cooperation 9. 5. Participation in international incident response cooperation 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 10.4. Operational crisis reserve 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 12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 12.2. Military cyber defence capacity 12.2. Military cyber defence capacity 12.2. Military cyber defence capacity	7.4. Cybersecurity awareness raising coordination	0	3		
8.2. Personal data protection authority 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 9.6. Participation in international incident response cooperation 9.7. Participation in international incident response cooperation 9.8. Participation in international expercises 9.0. Autional cyber crisis management plan 9.0. Participation in international cyber crisis exercises 9.0. Participation in international cyber crisis exercises 9.0. Participation in international cyber crisis exercises 9. Cyber crisis management exercises 9. Cyber crisis management plan 9. Poperational crisis reserve 9. Cybercrime offences in national law 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 12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 12.2. Military cyber defence capacity 12.2. Military cyber defence capacity	8. PROTECTION OF PERSONAL DATA	•		4	(100%)
8.2. Personal data protection authority 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 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 10.4. Operational crisis reserve 11.5. 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 12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 12.2. Military cyber defence capacity	8.1. Personal data protection legislation	•	2		
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 10. CYBER CRISIS MANAGEMENT 10.2. National cyber crisis management plan 10.2. National cyber crisis management exercises 10.3. Participation in international cyber crisis exercises 10.4. Operational crisis reserve 10.4. Operational crisis reserve 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 12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 12.2. Military cyber defence capacity 12.2. Military cyber defence capacity	8.2. Personal data protection authority	•	2		
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 3 9.5. Participation in international incident response cooperation 3 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 10.4. Operational crisis reserve 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 12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 12.2. Military cyber defence capacity 12.2. Military cyber doctrine	RESPONSIVE CYBERSECURITY INDICATORS				
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 3 9.5. Participation in international incident response cooperation 3 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 10.4. Operational crisis reserve 11.5. 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 11.5. Digital forensics capacity 11.6. 24/7 contact point for international cybercrime 12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 12.2. Military cyber defence capacity 12.2. Military cyber doctrine 2	9. CYBER INCIDENT RESPONSE	•		14	(100%)
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 3 9.5. Participation in international incident response cooperation 3 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 10.4. Operational crisis reserve 11.5. 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 11.5. Digital forensics capacity 11.6. 24/7 contact point for international cybercrime 12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 12.2. Military cyber defence capacity 12.2. Military cyber doctrine 2		•	3		
9.3. Cyber incident reporting tool 9.4. Single point of contact for international cooperation 9.5. Participation in international incident response cooperation 3 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 10.4. Operational crisis reserve 11.5. IFIGHT AGAINST CYBERCRIME 11.1. Cybercrime investigation capacity 11.5. Digital forensics capacity 11.5. Digital forensics capacity 11.6. 24/7 contact point for international cybercrime 12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 12.2. Military cyber defence capacity 12.2. Military cyber defence capacity 12.3. Military cyber defence capacity 12.4. Military cyber defence capacity 12.5. Military cyber defence capacity 12.6. 24. Military cyber defence capacity 22. Military cyber defence capacity 23. Military cyber defence capacity 24. Cybercrime contact point for international cybercrime 25. Military cyber defence capacity 26. Cybercrime cybercrime capacity 27. Cybercrime cybercrime capacity 28. Cybercrime cybercrime capacity 29. Cybercrime cybercrime capacity 20. Cybercrime cybercrime capacity 20. Cybercrime cybercrime cybercrime capacity 20. Cybercrime cybercr		•	3		
9.4. Single point of contact for international cooperation 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 10.3. Participation in international cyber crisis exercises 2 10.4. Operational crisis reserve 0 2 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 12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 12.2. Military cyber defence capacity 12.2. Military cyber defence capacity		•			
9.5. Participation in international incident response cooperation 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 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 12. MILITARY CYBER DEFENCE 13. (100%) 14. Military cyber defence capacity 15. Military cyber defence capacity 16. (100%)		•	3		
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 10.4. Operational crisis reserve 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 12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 12.2. Military cyber doctrine 13		•	3		
10.2. National cyber crisis management exercises 10.3. Participation in international cyber crisis exercises 10.4. Operational crisis reserve 10.4. Operational crisis reserve 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 12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 12.2. Military cyber doctrine 13 14 15 16 16 17 100% 16 100% 17 100% 18 100% 19 100% 100% 100% 100% 100% 100% 1	10. CYBER CRISIS MANAGEMENT	•	5	9	(56%)
10.2. National cyber crisis management exercises 10.3. Participation in international cyber crisis exercises 10.4. Operational crisis reserve 10.4. Operational crisis reserve 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 12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 12.2. Military cyber doctrine 13 14 15 16 16 17 100% 16 100% 17 100% 18 100% 19 100% 100% 100% 100% 100% 100% 1	10.1. Cyber crisis management plan	0			
10.3. Participation in international cyber crisis exercises 10.4. Operational crisis reserve 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 12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 12.2. Military cyber doctrine 13 (100%)		•	3		
10.4. Operational crisis reserve 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 12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 12.2. Military cyber defence capacity 12.2. Military cyber doctrine		•	2		
11.1. Cybercrime offences in national law 11.2. Procedural law provisions 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 12.1. Military cyber defence capacity 2 12.2. Military cyber doctrine 2		0	2		
11.2. Procedural law provisions 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 12.1. Military cyber defence capacity 2 12.2. Military cyber doctrine 2	11. FIGHT AGAINST CYBERCRIME	•		16	(100%)
11.2. Procedural law provisions 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 12.1. Military cyber defence capacity 2 12.2. Military cyber doctrine 2	11.1. Cybercrime offences in national law	•	3		
11.4. Cybercrime investigation capacity 11.5. Digital forensics capacity 2 11.6. 24/7 contact point for international cybercrime 3 12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 2 12.2. Military cyber doctrine 2	11.2. Procedural law provisions	•	3		
11.5. Digital forensics capacity 11.6. 24/7 contact point for international cybercrime 12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 12.2. Military cyber doctrine 2 12.2. Military cyber doctrine	11.3. Ratification of or accession to the Convention on Cybercrime	•	2		
11.6. 24/7 contact point for international cybercrime 12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 12.2. Military cyber doctrine 2	11.4. Cybercrime investigation capacity	•	3		
12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 12.2. Military cyber doctrine 2	11.5. Digital forensics capacity	•	2		
12.1. Military cyber defence capacity 12.2. Military cyber doctrine 2	11.6. 24/7 contact point for international cybercrime	•	3		
12.2. Military cyber doctrine	12. MILITARY CYBER DEFENCE	•		6	(100%)
12.2. Military cyber doctrine	12.1. Military cyber defence capacity	0	2		
12.3. Military cyber defence exercises	12.2. Military cyber doctrine	•	2		
	12.3. Military cyber defence exercises	•	2		



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