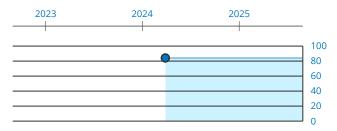


17. United States 84.17

Population 334.9 million
Area (km²) 9.8 million
GDP per capita (\$) 82.8 thousand

17th National Cyber Security Index ||||||||||||||| 84 %
N/A Global Cybersecurity Index ||||||||||||||| 100 %
19th E-Government Development Index |||||||||||||||| 92 %
1st Network Readiness Index ||||||||||||| 79 %

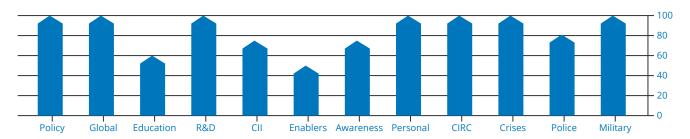
NCSI DEVELOPMENT TIMELINE



RANKING TIMELINE



NCSI FULFILMENT PERCENTAGE



STRATEGIC CYBERSECURITY INDICATORS

1. CYBERSECURITY POLICY (100%) 3 1.1. High-level cybersecurity leadership 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 (100%) 3 2.1. Cyber diplomacy engagements 2.2. Commitment to international law in cyberspace 1 2.3. Contribution to international capacity building in cybersecurity 2 3. EDUCATION AND PROFESSIONAL DEVELOPMENT (60%) 3.1. Cyber safety competencies in primary education 2 0 3.2. Cyber safety competencies in secondary education 0 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 (100%)4.1. Cybersecurity research and development programmes 2 4.2. Cybersecurity doctoral studies 2

PREVENTIVE CYBERSECURITY INDICATORS

5.1. Identification of critical information infrastructure 5.2. Cybersecurity requirements for operators of critical information infrastructure 5.3. Oybersecurity requirements for public sector organisations 5.4. Competent supervisory authority 6. Cybersecurity requirements for public sector organisations 5.5. A. Competent supervisory authority 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. Supervisory authority for trust services 6.5. Supervisory authority requirements for cloud services 6.5. Supervisory authority for further services 7. Supervisory authority for further services 7. Supervisory authority for further services 7. Supervisory authority further serv	5. CYBERSECURITY OF CRITICAL INFORMATION INFRASTRUCTURE	•		12	(75%)
infrastructure 5.3. Cybersecurity requirements for public sector organisations 5.4. Competent supervisory authority 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. Supervisory authority requirements for cloud services 6.5. Supervisory authority requirements for cloud services 6.5. Supervisory authority requirements for cloud services 6.5. Supervisory experiments for cloud services 7. Supervisory than or services 7. Supervisory servisory services 7. Supervisory ser	5.1. Identification of critical information infrastructure	•	3		
5.3. Cybersecurity requirements for public sector organisations 5.4. Competent supervisory authority 6. CYBERSECURITY OF DIGITAL ENABLERS 6.1. Secure electronic Identification 9.2. Call Electronic Signature 9.3. Trust services 9.2. Call Electronic Signature 9.4. Supervisory authority for trust services 9.5. Cybersecurity requirements for cloud services 9.5. Cybersecurity requirements for cloud services 9.7. Cybersecurity equirements for cloud services 9.7. Cybersecurity environments for cloud services 9.7. Cybersecurity environments for cloud services 9.7. Cybersecurity environments for cloud services 9.7. Sublic cyber threat reports 9.7. Sublic cyber threat reports 9.7. Sublic cyber threat reports 9.7. Sublic cybersecurity awareness resources 9.7. Sublic cybersecurity awareness resources 9.7. Sublic cybersecurity awareness resources 9. Sublic cybersecurity awareness resources 9. Cybersecurity awareness resources 9. Sublic cybersecurity awareness resources 9. Cybersecurity indicates response capacity 9. Cybersecurity awareness resources 9. Cybersecurity indicates response capacity 9. Cybersecurity indicates response capacity 9. Cybersecurity awareness resources 9. Cybersecurity indicates response capacity 9. Cybersecurity indicates response capacity 9. Cybersecurity awareness resources 9. Cybersecurity indicates response capacity 9. Cybersecurity response capacity 9. Cybersecurity response cap	5.2. Cybersecurity requirements for operators of critical information	0	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. Cybersecurity requirements for cloud services 6.5. Supply chain cybersecurity 7. CYBER THERAT 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 security awareness resources 7.4. Cybersecurity awareness raising coordination 7.5. Public cyber security awareness raising coordination 7.6. Personal data protection legislation 8.7. Personal data protection legislation 8.7. Personal data protection authority 8.7. Personal data protection in international cooperation 9.7. Personal data protection international cooperation 9.7. Personal data protection international cooperation 9.7. Personal data protection international cooperation 9.7. Participation in international incident response cooperation 9.7. Participation in international cooperation	infrastructure				
6.1. Secure electronic identification 6.2. Electronic signature 6.3. Trust services 6.3. Trust services 6.4. Supenvisory authority for trust services 6.5. Cybersecurity requirements for cloud services 6.6. Supply chain cybersecurity 7. CYBER THERAT ANALYSIS AND AWARENESS RAISING 7. CYBER THERAT ANALYSIS AND AWARENESS RAISING 7. CYBER THERAT ANALYSIS AND AWARENESS RAISING 7. Loyber threat analysis 7. Cyber threat analysis 7. Dublic cyber security awareness resources 7. Cyber security awareness resources 7. Cyber security awareness raising coordination 8. PROTECTION OF PERSONAL DATA 9. Cyber security indicated tresponse capacity 9. Cyber incident response capacity 9. Cyber incident response capacity 9. Servicipation in international cooperation 9. Solver incident response capacity 9. Servicipation in international incident response cooperation 10. Cyber Crisis management plan 10. Lyber crisis management plan 10. Lyber crisis management plan 10. August crisis management plan 10. August crisis management exercises 10.3. Participation in international cyber crisis 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. Raiffication 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 capacity 12. Military cyber defence capacity 12. Military cyber defence capacity 12. Limitary cyber deternice capacity 12. Limitary cyber deternice capacity 12. Military cyber deternice 12. Military cyber deternice capacity	5.3. Cybersecurity requirements for public sector organisations	•	3		
6.1. Secure electronic identification 6.2. Electronic signature 6.2. Trust services 6.4. Supervisory authority for trust services 6.5. Cybersecurity requirements for cloud services 7. CyBERT THREAT ANALYSIS AND AWARENESS RAISING 7. CyBERT THREAT ANALYSIS AND AWARENESS RAISING 7. CyBERT THREAT Enabysis 7. Cybert threat reports 7. CyBERT THREAT ANALYSIS AND AWARENESS RAISING 7. Cybersecurity awareness resources 7. Cybersecurity awareness resources 7. Cybersecurity awareness raising coordination 8. PROTECTION OF PERSONAL DATA 9. Cyber RICIDENT RESPONSE 9. Cyber RICIDENT RESPONS	5.4. Competent supervisory authority	•	3		
6.2. Electronic signature 6.3. Trust services 6.4. Supervisory authority for trust services 6.5. Cybersecurity requirements for cloud services 6.6. Supphy chalin 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 7.5. Public cybersecurity awareness resources 7.6. Supphy Chalin of PERSONAL DATA 7.6. Public Cybersecurity awareness raising coordination 7.7. Public Cybersecurity awareness raising coordination 7.8. PROTECTION OF PERSONAL DATA 7.9. Personal data protection legislation 7.9. Personal data protection authority 7.0. Personal data protection autho	6. CYBERSECURITY OF DIGITAL ENABLERS	•	6	(12)	(50%)
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 security awareness resources 7.3. Public cybersecurity awareness resources 7.3. Public cybersecurity awareness resources 7.3. Public cybersecurity awareness raising coordination 8. PROTECTION OF PERSONAL DATA 9. (100%) 9. CYBER INCIDENT RESPONSE 9. CYB	6.1. Secure electronic identification	0			
6.4. Supervisory authority for trust services 6.5. Cybptersecurity requirements for cloud services 6.6. Supply chain cybersecurity 2 7. CYBER THERAT ANALYSIS AND AWARENESS RAISING 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 cyber threat reports 7.6. 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 9.1. 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. National cyber crisis management plan 10. C. National cyber crisis management exercises 10.3. Participation in international cyber crisis exercises 10.4. Operational crisis reserve 11. FIGHT AGAINST CYBERCRIME 11. Cybercrime offences in national law 11. Procedural law provisions 11. Raiffication of or accession to the Convention on Cybercrime 11.1. 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. Military cyber doctrine	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 cyber threat reports 7.3. Public cyber security awareness resources 7.4. Cybersecurity awareness resources 7.5. Public cybersecurity awareness resources 7.6. Cybersecurity awareness resources 7.7. Cybersecurity awareness resources 7.8. Protection OF PERSONAL DATA 8.1. 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 apacity 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 10.1. Cyber crisis management plan 10. 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 forensic scapacity 11.5. Digital forensic scapacity 11.5. Digital forensic scapacity 12. Military cyber defence capacity 12. Limilitary cyber defence capacity 12.2. Military cyber defence capacity 12.2. Military cyber defence capacity	6.3. Trust services	0	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 resources 7.7. Cybersecurity awareness resources 7.8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection authority 8.2. Personal data protection authority 8.2. Personal data protection authority 8.2. Personal data protection authority 8.3. 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. Yellow in international incident response cooperation 9.7. Authoral 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 11. FIGHT AGAINST CYBERCRIME 11. Cybercrime offences in national law 11. 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 12.1. Military cyber defence capacity 12.2. Military cyber defence capacity 12.2. Military cyber defence capacity 12.2. Military cyber doctrine	6.4. Supervisory authority for trust services	0	2		
7. CVBER 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 security awareness resources 7.4. Cybersecurity awareness resources 7.4. Cybersecurity awareness raising coordination 7.5. Public cyber security 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 9.2. Incident reporting tool gladions 9.3. Cyber incident response capacity 9.2. Incident reporting tool gladions 9.3. Syber incident reporting tool 2 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. 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 11. FIGHT AGAINST CYBERCRIME 11. Cybercrime offences in national law 11. Cybercrime investigation capacity 11. S. Digital forensics capacity 12. Militrary cyber defence capacity	6.5. Cybersecurity requirements for cloud services	•	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 7.4. 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 9.5. Participation in international incident response cooperation 9.10. Cyber Crisis MANAGEMENT 9.10. Cyber crisis management plan 10.2. National cyber crisis management exercises 10.3. Participation in International cyber crisis exercises 10.4. Operational crisis reserve 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 2.2. Military 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 resources 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 8.2. Personal data protection authority 8.3. 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 9.6. 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 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. Military cyber defence capacity	7. CYBER THREAT ANALYSIS AND AWARENESS RAISING	•		(12)	(75%)
7.2. Public cyber threat reports 7.3. Public cybersecurity awareness resources 7.4. Cybersecurity awareness resources 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 8.2. Personal data protection authority 8.3. 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 9.6. 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 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. Military cyber defence capacity	7.1. Cyber threat analysis	•	3		
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 authority 2. RESPONSIVE CYBERSECURITY INDICATORS 9. CYBER INCIDENT 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 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 2. Incident exponse cooperation 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	-	•	3		
7.4. Cybersecurity awareness raising coordination 8. PROTECTION OF PERSONAL DATA 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 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 12.1. Military cyber defence capacity 12.2. Military cyber defence capacity		•	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 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 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 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 12.2. Military cyber defence capacity		0	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 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 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 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 12.2. Military cyber defence capacity	8 PROTECTION OF PERSONAL DATA				(100%)
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 9.5. Participation in international incident response cooperation 9.5. Participation in international incident response cooperation 9.6. CYBER CRISIS MANAGEMENT 9.7. Autional cyber crisis management plan 9.8. Participation in international cyber crisis exercises 9.9. Participation in international cyber crisis exercises 9.0.4. Operational crisis reserve 9. 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 12.1. Military cyber defence capacity 12.2. Military cyber defence capacity 12.2. Military cyber defence capacity			2		(10070)
RESPONSIVE CYBER SECURITY 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 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					
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 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					
9.1. 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 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 13. Gillowhill in the convention on the conven	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 0.1. Cyber crisis management plan 0.2. National cyber crisis management exercises 10.3. Participation in international cyber crisis exercises 10.4. Operational crisis reserve 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 12.2. Military cyber doctrine	9. CYBER INCIDENT RESPONSE	•		14	(100%)
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 9. (100%) 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 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 13. (100%) 14. Military cyber defence capacity 15. Military cyber defence capacity 16. (100%) 17. Military cyber defence capacity 17. Military cyber defence capacity 18. Military cyber defence capacity 19. (100%)	9.1. National incident response capacity	•	3		
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 9 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 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 12.2. Military cyber doctrine	9.2. Incident reporting obligations	•	3		
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 2 11. FIGHT AGAINST CYBERCRIME 12. 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%) 17. Military cyber defence capacity 18. Military cyber defence capacity 19. Military cyber defence capacity 20. (100%)	9.3. Cyber incident reporting tool	•	2		
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 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. Military cyber defence capacity		•	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 2 11. FIGHT AGAINST CYBERCRIME 11. Cybercrime offences in national law 11. Procedural law provisions 11. Ratification of or accession to the Convention on Cybercrime 11. Cybercrime investigation capacity 11. Digital forensics capacity 11. Digital forensics capacity 12. MILITARY CYBER DEFENCE 12. Military cyber defence capacity 12. Military cyber defence capacity 12. Military cyber defence capacity 12. Military cyber doctrine	9.5. Participation in international incident response cooperation	•	3		
10.2. National cyber crisis management exercises 10.3. Participation in international cyber crisis exercises 10.4. Operational crisis reserve 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 doctrine	10. CYBER CRISIS MANAGEMENT	•		9	(100%)
10.3. Participation in international cyber crisis exercises 10.4. Operational crisis reserve 2 11. FIGHT AGAINST CYBERCRIME 11. Cybercrime offences in national law 11. Procedural law provisions 11. A Ratification of or accession to the Convention on Cybercrime 11. Cybercrime investigation capacity 11. Digital forensics capacity 11. Digital forensics capacity 12. MILITARY CYBER DEFENCE 12. Millitary cyber defence capacity 12. Millitary cyber defence capacity 12. Millitary cyber defence capacity 12. Millitary cyber doctrine	10.1. Cyber crisis management plan	•	2		
10.4. Operational crisis reserve 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 doctrine	10.2. National cyber crisis management exercises	•	3		
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 (81%) 14 (81%) 15 (81%) 16 (100%)	10.3. Participation in international cyber crisis exercises	•	2		
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 3 (100%)	10.4. Operational crisis reserve	•	2		
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 17 17 18 18 18 19 19 10 10 10 10 10 10 10 10	11. FIGHT AGAINST CYBERCRIME	•		13—(16)	(81%)
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	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 12.2. Military cyber doctrine 2	11.2. Procedural law provisions	0	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	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 6 (100%)	11.5. Digital forensics capacity	•	2		
12.1. Military cyber defence capacity 12.2. Military cyber doctrine	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	•	2		
		•	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