

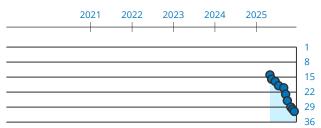
31. Croatia 82.50

Population 3.9 million
Area (km²) 88.1 thousand
GDP per capita (\$) 45.6 thousand

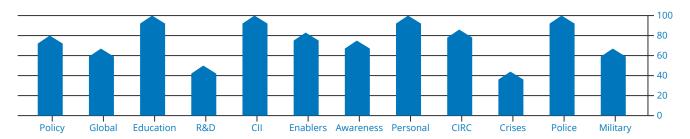
NCSI DEVELOPMENT TIMELINE



RANKING TIMELINE



NCSI FULFILMENT PERCENTAGE



STRATEGIC CYBERSECURITY INDICATORS

4.2. Cybersecurity doctoral studies

1. CYBERSECURITY POLICY (80%) 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 0 3 2. GLOBAL CYBERSECURITY CONTRIBUTION (67%) 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 0 3. EDUCATION AND PROFESSIONAL DEVELOPMENT (100%)3.1. Cyber safety competencies in primary education 2 3.2. Cyber safety competencies in secondary education 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 (50%)4.1. Cybersecurity research and development programmes 2

0

2

PREVENTIVE CYBERSECURITY INDICATORS

| 5.1. Identification of critical information infrastructure 3 | 5. CYBERSECURITY OF CRITICAL INFORMATION INFRASTRUCTURE | • | | 12 | (100%) |
|--|---|---|---|----------------|--------|
| Infrastructure 3.3. Cybersecurity requirements for public sector organisations 3.4. Competers supervisory authority 3.6. 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 for trust services 6.5. Supervisory authority requirements for cloud services 7.1. Cyber Threat analysis 7.2. Public cyber security 7.2. Public cyber security awareness resources 7.3. Public cyber threat reports 7.3. Public cyber security awareness resources 7.4. Cybersecurity awareness resources 7.5. 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 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 authority 8. PROTECTION OF PERSONAL DATA 8. PROTECTION OF PERSONAL DATA 8. Personal data protection authority 8. PROTECTION OF PERSONAL DATA 9. CyBER INCIDENT RESPONSE 9.1. National incident response capacity 9.2. Incident reporting obligations 9.3. Syler incident reporting obligations 9.3. Syler 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 c | 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 6.2. Electronic signature 6.2. Trust services 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 6.6. 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 7.3. Public cyber threat reports 7.4. Cybersecurity awareness resources 7.5. Public cyber threat reports 7.6. Supervisory authority of trust services 7.7. Public cyber threat reports 7.8. Personal data protection legislation 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection legislation 8.2. Personal data protection authority 7. CYBER INCIDENT RESPONSE 9. CYBER INCIDENT RESPONSE 9. Cyber incident reporting tobligations 9. Cyber incident reporting tobligations 9. Cyber incident reporting tobligations 9. Sparticipation in international incident response cooperation 9. Participation in international incident response cooperation 9. Sparticipation in international cyber crisis exercises 9. Output the provision of the provision of the cooperation of th | 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. 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 7.4. Cybersecurity awareness resources 7.4. Cybersecurity awareness raising coordination 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection authority 2 RESPONSIVE CYBERSECURITY INDICATORS 9. CYBER INCIDENT RESPONSE 9. CYBER INCIDENT RESPONSE 9. CYBER INCIDENT RESPONSE 9. Cyber incident reporting obligations 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 10.1. Cyber crisis management exercises 10.3. Participation in international cyber crisis exercises 10.4. Operational crisis reserve 10. CYBER INCIDENT (PERSONE) 11. RIGHT AGAINST CYBERCRIME 11. Cybercrime offences in national law 11.2. Procedural law provisions 11.3. Raiffcation of or accession to the Convention on Cybercrime 11.6. LYBer Crisis management exercises 10. Cyber Cyber of effence capacity 11.5. Digital forensics capacity 11.6. LYBer Cyber Defence 12. Military cyber defence capacity 12. Military cyber defence capacity 12. Limitary cyber dectrine | infrastructure | | | | |
| 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 6.6. Supply chain cybersecurity 7. CyBER THREAT ANALYSIS AND AWARENESS RAISING 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 cyber threat reports 7.5. Personal data protection legislation 8. PROTECTION OF PERSONAL DATA 8. PROTECTION OF PERSONAL DATA 8. PERSONSIVE CYBERSECURITY INDICATORS 9. CYBER INCIDENT RESPONSE 9. CYBER INCIDENT RESPONSE 9. Protection did and protection legislations 9. Service of the composition of the compo | 5.3. Cybersecurity requirements for public sector organisations | • | 3 | | |
| 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 6.5. Cybersecurity requirements for cloud services 6.6. Supply chain cybersecurity 2 7.1. 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 raising coordination 8. PROTECTION OF PERSONAL DATA 8. Personal data protection legislation 8.2. Personal data protection legislation 8.2. Personal data protection authority 7. National incident response capacity 9. Cyber Nicolent reporting boil gations 9. Cyber Nicolent reporting tool 9. Superincident reporting to | 5.4. Competent supervisory authority | • | 3 | | |
| 6.2. Electronic signature 6.3. Trust services 6.4. Supen'sory authority for trust services 6.5. Cybersecurity requirements for cloud 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 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 authority 8.2. Personal data protection authority 8.2. Personal data protection authority 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. National cyber crisis management plan 10. Cyber crisis management plan 11. Cybercrime offences in national law 11. Procedural law provisions 11. Rediffication of or accession to the Convention on 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 capacity 12. Military cyber dectrine | 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 7.4. Cybersecurity awareness resources 7.5. Public cybersecurity awareness resources 7.6. Supply chain cybersecurity awareness resources 7.6. Cybersecurity awareness raising coordination 8. PROTECTION OF PERSONAL DATA 8. PROTECTION OF PERSONAL DATA 8. Personal data protection legislation 8.2. Personal data protection legislation 8.2. Personal data protection legislation 8.2. Personal data protection legislation 9. Cyber Incident response capacity 9. Cyber Incident response capacity 9. A single point of contact for international cooperation 9. S. Participation in international incident response cooperation 9. S. Participation in international incident response cooperation 9. S. Participation in international incident response cooperation 9. Cyber crisis management plan 10. Cyber crisis management exercises 10. 3 analysis awareness 10. 3 analysis awareness 10. 3 analysis awareness 10. 3 analysis awareness 10. 4 Operational cyber crisis exercises 10. 4 Operational crisis reserve 10. 11. Cybercrime offences in national law 11. 2. Procedural law provisions 11. Raiffication of or accession to the Convention on Cybercrime 11. Cybercrime investigation capacity 11. D. Digital forensics capacity 11. D. Digital forensics capacity 12. Military cyber defence capacity | 6.1. Secure electronic identification | • | 2 | | |
| 6.5. Suppervisory authority for trust services 6.5. Cybeps ceutrity requirements for cloud services 6.6. Supply chain cybersecurity 2 7. CYBER THERAT ANALYSIS AND AWARENESS RAISING 7. Public 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 cyber threat reports 7.6. Cybersecurity awareness resources 7.7. Cyber threat analysis 7.7. Public cyber threat reports 7.8. Public cyber threat reports 7.9. Public cyber threat reports 7.9. Cyber incident reporting obligation 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection legislation 8.2. Personal data protection authority 8.2. Personal data protection authority 8. Cyber incident reporting obligations 9. Cyber incident reporting obligations 9. Cyber incident reporting obligations 9. Syber incident reporting obligations 9. Syber incident reporting tool 9. Syber incident reporting tool 9. Syber incident reporting tool 9. Syber incident reporting obligations 9. Syber incident reporting obligations 9. Syber incident reporting tool 9. Syb | 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 7.3. 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. Eyersonal data protection legislation 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 RESPONSE 9. Sparticipation in international cooperation 9. Sparticipation in international incident response cooperation 9. Sparticipation in international incident response cooperation 9. Sparticipation in international incident response cooperation 9. CYBER CRISIS MANAGEMENT 9. Cyber crisis management plan 10. Cyber crisis management exercises 10. Aparticipation in international cyber crisis exercises 10. Aparticipation in international international international international international internationa | 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 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. Personal data protection authority 8.4. Cybersecurity INDICATORS 9. CYBER INCIDENT RESPONSE 9.1. National incident response capacity 9.2. Incident reporting tool 9.2. A 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 management plan 10.2. Vyber crisis management plan 10.2. National cyber crisis management exercises 10.3. Participation in international cyber crisis exercises 10.4. Operational crisis reserve 11.1. Cyber crisis management plan 12. International cyber crisis exercises 13. Ratification of or accession to the Convention on Cybercrime 11.1. Cybercrime investigation capacity 11.1. Cybercrime investigation capacity 11.5. Digital forensics capacity 11.5. Digital forensics capacity 12. Military cyber defence capacity 12. Military cyber doctrine | 6.4. Supervisory authority for trust services | • | 2 | | |
| 7. CYBER THREAT ANALYSIS AND AWARENESS RAISING 7. CYBER THREAT RANLYSIS AND AWARENESS RAISING 7.1. Cyber threat reports 7.3. 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 cybersecurity awareness raising coordination 7.6. Cybersecurity awareness raising coordination 7.7. Personal data protection legislation 7.7. Personal data protection authority 7. Personal data | 6.5. Cybersecurity requirements for cloud services | 0 | 2 | | |
| 7.1. Cyber threat analysis 7.2. Public cyber security awareness resources 7.3. Public cybersecurity awareness resources 7.4. Cybersecurity awareness raising coordination 0 3 8. PROTECTION OF PERSONAL DATA 8.1. Personal data protection legislation 8.2. Personal data protection legislation 8.2. Personal data protection authority 8.3. Cyber Incident response capacity 9.2. Incident response capacity 9.3. Institual incident response capacity 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 10.2. National cyber crisis management exercises 10.3. Participation in international cyber crisis exercises 10.4. Operational crisis reserve 10.5. Operational crisis reserve 10.6. The protection of 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 | 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. Q- 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. Cyber crisis management plan 10.2. National cyber crisis management 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. Militrary Cyber defence capacity 12. Militrary Cyber defence capacity 12. Militrary cyber defence capacity 12. Militrary cyber doctrine 12. Militrary cyber doctrine | 7. CYBER THREAT ANALYSIS AND AWARENESS RAISING | • | | (12) | (75%) |
| 7.3. Public obersecurity 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. Cybercrime offences in national law 11. Procedural law provisions 11. Ratification of or accession to the Convention on Cybercrime 11. Cybercrime investigation capacity 11. S. Digital forensics capacity 11. S. Digital forensics capacity 11. S. Digital forensics capacity 12. Militrary CYBER DEFENCE 12. Militrary cyber defence capacity 12. Militrary cyber defence capacity 12. Military 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 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. 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 | 7.2. Public cyber threat reports | • | 3 | | |
| 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 tool 9. 4. Single point of contact for international cooperation 9. 5. Participation in international incident response cooperation 9. 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. 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 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 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 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 | 7.4. Cybersecurity awareness raising coordination | 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 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 | 8. PROTECTION OF PERSONAL DATA | • | | 4 | (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 9.6. Participation in international incident response cooperation 9.7. Participation in international incident response cooperation 9.8. Participation in international incident response cooperation 9.9. Participation in international incident response cooperation 9.0. CYBER CRISIS MANAGEMENT 9.0. Autional cyber crisis management plan 9.1. Cyber crisis management plan 9.2. National cyber crisis management exercises 9.3. Participation in international cyber crisis exercises 9.3. Participation in international cyber crisis exercises 9.3. Participation in international cyber crisis exercises 9.3. Participation of or international cyber crisis exercises 9.3. Participation in inte | 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 10.1. 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 | 8.2. Personal data protection authority | • | 2 | | |
| 9.1. National incident response capacity 9.2. Incident reporting obligations 9.3. Cyber incident reporting tool 0 2 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. 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 | RESPONSIVE CYBERSECURITY INDICATORS | | | | |
| 9.2. Incident reporting obligations 9.3. Cyber incident reporting tool 0 2 9.4. Single point of contact for international 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 defence capacity 12.2. Military cyber doctrine | 9. CYBER INCIDENT RESPONSE | • | | 12 —14) | (86%) |
| 9.2. Incident reporting obligations 9.3. Cyber incident reporting tool 0 2 9.4. Single point of contact for international 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 defence capacity 12.2. Military cyber doctrine | | • | 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 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 10.5. Digital forensics 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 12.2. Military cyber doctrine | | • | | | |
| 9.4. Single point of contact for international cooperation 9.5. Participation in international incident response cooperation 3 10. CYBER CRISIS MANAGEMENT 4 9 (44%) 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 11.5. 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 | | 0 | | | |
| 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 doctrine 10.4 (44%) 10.4 (44%) 10.4 (44%) 10.4 (44%) 10.4 (44%) 10.4 (44%) 10.4 (44%) 10.5 (100%) 11.5 (100%) 12. (100%) 13. (100%) 14. (100%) 15. (100%) 16. (100%) 17. (100%) 18. (100%) 19. (| | • | 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 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 12. Military cyber doctrine 13. Military cyber doctrine | | 0 | 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 17 16 17 16 17 17 18 18 18 18 18 19 19 10 20 20 20 20 20 20 20 20 20 | 10. CYBER CRISIS MANAGEMENT | • | 4 | 9 | (44%) |
| 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 12.3. Military cyber doctrine 13. Military cyber doctrine 14. (67%) | 10.1. Cyber crisis management plan | • | 2 | | |
| 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 13 15 16 100%) 16 16 16 100%) 3 17 4 6 16 17 18 18 19 19 10 20 20 20 20 20 20 20 20 20 | 10.2. National cyber crisis management exercises | 0 | 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 (100%) 16 (100%) 3 (100%) 3 (100%) 4 (67%) | 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 (67%) | 10.4. Operational crisis reserve | 0 | 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 (67%) | 11. FIGHT AGAINST CYBERCRIME | • | | 16 | (100%) |
| 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 (67%) | 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 0 2 | | 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 2 (67%) | 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 3 (67%) | 11.4. Cybercrime investigation capacity | • | 3 | | |
| 12. MILITARY CYBER DEFENCE 12.1. Military cyber defence capacity 12.2. Military cyber doctrine (67%) | 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 | • | 4 | <u>(6)</u> | (67%) |
| 12.2. Military cyber doctrine | 12.1. Military cyber defence capacity | • | 2 | | |
| | | 0 | | | |
| | 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