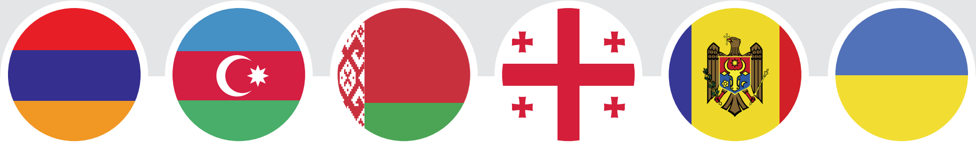
EU2017.EE

EaP | Eastern Partnership

eGA e-governance academy | 15 YEARS Empowering e-governance around the world

Situation Review:
Safety and Security of Cyberspace and E-Democracy in the Eastern Partnership Countries



ESTONIA DEVELOPMENT COOPERATION

SWEDEN

Situation Review: Safety and Security in the Cyberspace and E-Democracy in the Eastern Partnership Countries

Authors:
Kristina Reinsalu, Programme Director of E-democracy, e-Governance Academy
Raul Rikk, Programme Director of National Cyber Security, e-Governance Academy
Jelizaveta Krenjova, E-democracy expert, e-Governance Academy
Piret Pernik, Research Fellow, International Centre for Defence and Security

Project Manager:
Martin Lään, e-Governance Academy

Design:
Gerit Tiirik, Sviiter Creative Agency (www.sviiter.com)

Published by:
e-Governance Academy
Rotermanni 8, 10111 Tallinn, Estonia
ega.ee

Digital version of this publication is available for download on the eGA website:

http://ega.ee/publications/situation_review

Written in cooperation with

ECEAP ESTONIAN CENTER OF EASTERN PARTNERSHIP

RKK ICDS RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI · ESTONIA

Financed by

ESTONIA DEVELOPMENT COOPERATION

SWEDEN

The opinions expressed in this study are those of the authors and do not reflect the official position of the Republic of Estonia. The reproduction of extracts from this publication is authorized on condition that the source is properly cited.

ISBN 978-9949-88-026-3

Contents

Foreword

E-governance in the broadest sense has become a household term around the world, including in the Eastern Partnership countries (Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova and Ukraine). All partner countries have made significant steps towards using ICTs to make governance more transparent, efficient, and bringing it closer to citizens. In the context of global high level of attention to safety and security in cyberspace, aspects of keeping e-services secure have increased significantly in importance during the past years. While promoting democratic and transparent governance in a safe and secure electronic environment is a goal on its own, it is also very important to establish how and whether developing e-governance will serve the EU integration goals of the Eastern Partnership countries.

This Situation Review explores two specific aspects of e-governance in the Eastern Partnership countries: safety and security of cyber space and e-democracy. Both of these fields are crucially important for any country seeking to build and develop a modern, inclusive, and safe society with the help of ICT tools. It is also very important to ensure sharing best practices in these areas, and addressing bottlenecks, so that the existing very positive developments may continue in the future. This will benefit the citizens of the Eastern Partnership countries.

The Review was carried on by e-Governance Academy, an independent mission-based, non-profit organisation, dedicated to creation and transfer of knowledge and best practice concerning e-governance, e-democracy, national cyber security, and the development of open information societies. The work was financed jointly by the Estonian Development Cooperation funds and the Swedish International Development Cooperation Agency (SIDA).

Acknowledgements

Acknowledgements are due to many experts who provided detailed input on laws, procedures and best cases in their respective countries. Particular thanks are due to our national partners and experts:

Safety and Security in the Cyberspace focus area: Maia Abuladze (Georgia), **Tigran Afrikyan** (Armenia), **Roman Boiarchuk** (Ukraine), **Natalia Goderdzishvili** (Georgia), **Nijat Ibrahimli** (Azerbaijan), **Andrii Piskun** (Ukraine), **Anna Pobol** (Belarus) and **Veaceslav Puscasu** (Moldova).

E-democracy focus area: Lilit Arzoyan (Armenia), **Veronica Cretu** (Moldova), **Dmytro Khutkyy** (Ukraine), **Mahammad Muradov** (Azerbaijan), **Natallia Rabava** (Belarus), **Teona Turashvili** (Georgia)

Introduction

This Situation Review provides the current situation of the state of affairs in the field of cyber security and e-democracy in the Eastern Partnership (EaP) countries - Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova and Ukraine.

The researchers addressed the following questions:

- **What are the most prominent developments in these areas on strategic and legislative levels?**
- **What actors play a major role on the institutional level?**
- **How is e-democracy being implemented? What are the most prominent recent e-democracy initiatives in EaP countries and what can we learn from them?**
- **What are the actors' perceptions of the drivers and barriers of e-democracy implementation?**
- **What is the situation with cyber security in these countries?**
- **What are the main capacities, which are important on national level and which support the seamless development of information society?**
- **What are the cyber security capacity gaps unique for each country and common for all EaP countries?**

Policy recommendations have been formulated on the basis of the Situation Review. These recommendations are designed separately for the two focus areas, offering guidance and suggestions for the EaP countries on where the potential for impactful improvements is the strongest.

As the areas of safety and security of cyber space and e-democracy require a different approach, different methodologies were used to review the situation in EaP countries.

The safety and security of cyber space focus area used the National Cyber Security Index (NCSI) methodology developed by the e-Governance Academy. The methodology measures countries' preparedness to prevent the realisation of fundamental cyber threats and readiness to manage cyber incidents, crimes and large-scale cyber crises. The methodology has 3 areas, 12 capacities and 60 specific indicators. All indicators are backed with publicly available evidence materials.

In the area of cyber security, the study focuses on the measurable aspects of cyber security implemented by the central government. These aspects are legislation, existing organisations and departments dealing with the subject matter, cooperation formats (committees, councils, permanent working groups) and outcomes of the activities undertaken. In the study the methodology used for the cyber security overview is compared with the EU baseline in the areas of cyber, network and information security. The EU baseline is defined by EU legislative acts (including legislation about data protection, cybercrime and electronic identity and trust services).

For mapping the situation regarding e-democracy qualitative methodology has been used. The authors collected primary data via semi-structured interviews with different stakeholders – institutionalised and non-institutionalised civil society representatives (NGOs and civic activists), representatives of state authorities, journalists and bloggers, donors and international experts in the field. The authors also conducted 35 interviews in total (5-6 interviews in each country) having the broad spectrum of various perspectives present in every country mission. For secondary data authors relied on public sources, concept papers, international project reports and data gathered through the questionnaires (6) addressed to the local experts in each country. The interviews were organised along the following topics: main strategies and action plans, legal framework, institutional frameworks/main actors in the field, notable ICT tools and related projects/cases, barriers and driving forces in the development of the field.

Whereas the emphasis of previous studies of e-governance in the EaP region has been on ICT infrastructure and e-services[1], the current study focuses on how the potential of ICTs has been used to increase the transparency of governmental decision-making, the access to public information and the creation of opportunities for citizens to participate in decision-making processes. The area of e-democracy in the region is very dynamic and has numerous new developments, which constitute good showcases not just for the Eastern Partnership region, but also for the EU countries. Thus, the current Review contributes to the knowledge transfer on e-participation and transparency in the EaP region, in Europe, and also to countries beyond European borders.

[1] *See e.g. "Harmonisation of the Digital Markets in the Eastern Partnership" (2015). Accessible at: https://europa.eu/capacity4dev/hiqstep/document/harmonisation-digital-markets-eastern-partnership-study-report*

Focus area #1 Cyber Security Arrangements for Ensuring the Trust and Development of Information Society

Raul Rikk,
Programme Director of National Cyber Security,
e-Governance Academy

Piret Pernik,
Research Fellow,
International Centre for Defence and Security

Introduction

In this situation review, Cyber Security is a general term for digital data protection, computer security, network security, e-services security, ICT security, cyber safety, etc.

The review gives a structured overview about the cyber security situation in the Eastern Partnership (EaP) countries: Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova and Ukraine. The focus has been on the main capacities, which are important on the national level and which support the seamless development of information society.

Our goal has been to map the cyber security situation in EaP countries and indicate successful developments in this field as well as point out the areas where improvement is needed. Additionally, our goal has been to find out, what are the areas where all EaP countries need cooperation, collaboration and joint development.

The study was done during the 2nd quarter of 2017 and the report was created in August 2017.

1. Methodology

Methodology of the research

The National Cyber Security Index (NCSI) methodology was used to compile the review. The NCSI is a global index, which measures countries' preparedness to prevent the realisation of fundamental cyber threats and readiness to manage cyber incidents, crimes and large-scale cyber crises. Additionally, the NCSI is a global database providing links and documents about national cyber security, and a tool for national cyber security capacity-building describing strategic measures of cyberspace protection.

The structured questionnaire of the NCSI includes 3 dimensions, 12 national level capacities and 60 specific indicators. The dimensions and capacities of the questionnaire are as follows:

I. GENERAL CYBER SECURITY INDICATORS

1. Policy development for the protection of cyberspace (5 indicators)
2. Understanding and analysis of cyber threats (2 indicators)
3. Cyber security education on all levels and professional development (9 indicators)
4. International cooperation and influence in the cyber security field (6 indicators)

II. BASELINE CYBER SECURITY INDICATORS

5. Cyber and information security baseline standard (6 indicators)
6. Secure environment for e-services (2 indicators)
7. Electronic identification and electronic signature (6 indicators)
8. Protection of essential e-services and critical information infrastructure (4 indicators)

III. INCIDENT AND CRISIS MANAGEMENT INDICATORS

9. Capacity to manage cyber incidents (4 indicators)
10. Capacity to manage large-scale cyber crises (6 indicators)
11. Fight against cybercrime (5 indicators)
12. National cyber defence capability (5 indicators)

The focus of the methodology is on the measurable aspects of cyber security implemented by the central government. These aspects are:

- Legislation (legal acts, regulations, official orders, etc.)
- Existing units (organisations, departments, sections, etc.)
- Cooperation formats (committees, councils, permanent working groups, etc.)
- Outcomes (policies, strategies, exercises, websites, programmes, technologies, etc.)

The methodology takes into consideration only publicly available information. All evidence materials are transparent and presented in the report.

The methodology is described in more detail on the NCSI website: www.ncsi.ega.ee

The NCSI questionnaire was given to each EaP country and answers with relevant evidence materials were requested. In addition to the questionnaire, structured interviews were organised with main stakeholders and responsible actors in each country. After data collection, the study team analysed collected information and developed the report.

The outcome of the study is presented in the chapter "Research Results". The conclusions and recommendations are presented in the chapter "Policy Recommendations".

EU cyber security baseline and the NCSI methodology relationships

This chapter provides an overview of the EU baseline in the area of cyber, network and information security that refers to cyber security of information and communication systems (ICT) that support the functioning of societies and economies. In this chapter, the NCSI methodology will be compared with the EU baseline.

While cyber security is a broader issue including cyber diplomacy, cybercrime, and cyber defence, etc., the EU baseline includes only legally binding legislation to Member States, consisting of EU regulations, directives and decisions in three areas:

1. network and information security
2. electronic identification and electronic trust services
3. personal data protection.

Non-binding documents such as policy recommendations, communications, guidelines published by various EU institutions were not included in the baseline.

The NCSI has 12 areas of cyber security capacities. Most of these areas are covered by the EU baseline consisting of five legislative acts:

1. **NIS Directive** – Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
2. **eIDAS Regulation** – Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
3. **General Data Protection Regulation** – Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC), which will apply from 25 May 2018
4. **General Data Protection Directive** – Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (General Data Protection Directive). The Member States have to transpose it into their national law by 6 May 2018
5. **Cybercrime Directive** – Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA

In the following areas of the NCSI the EU baseline either does not prescribe exact requirements for Member States or only encourages Member States to consider related activities:

1. primary, secondary, vocational, and academic (bachelor, masters, doctoral) cyber security education
2. cyber crisis management
3. military's cyber defence operations
4. international cooperation.

For example, the NIS Directive requires Member States to adopt a national cyber security strategy, and establish a Computer Security Incident Response Team (CSIRT) and a national NIS authority that will oversee the implementation of the directive. National CSIRTs must provide situational awareness, risk and incident analysis, as well as incident response. These requirements are also covered in the NCSI, which assesses if a country has adopted a national cyber security strategy and an implementation plan, established a cyber threat analysis unit (which is usually CSIRT), and a unit for developing cyber security policy and a format for coordinating cyber security on the national level. Thus, there is an overlap between the requirements of the NCSI and the EU baseline, but specific roles and functions of CSIRTs described in the NIS Directive are included in more general criteria in the NCSI.

The NIS Directive includes requirements for operators of essential services that will have to take appropriate security measures and notify the relevant national authority of serious incidents. Digital service providers likewise will have to comply with the security and notification requirements. These requirements are reflected in the NCSI criteria for defining essential services that depend on ICT (critical information infrastructures), and setting up an agency with a primary function is the protection of critical information infrastructure that coordinates and supervises the implementation of specific security measures for operators of essential services. The requirement that operators of essential services and digital providers apply security measures is reflected in the NCSI criteria for establishing service continuity requirements. The NIS directive also encourages operators of essential services and digital providers to apply the EU and international cyber security standards, and this criterion is part of an ability of a country to provide baseline cyber security measures, including the application of international standards.

Overall, the NIS Directive has specific requirements in nine capacity-building areas of the NCSI that are presented in Table 1. The requirements of NIS Directive do not always match the exact capacity descriptions of the NCSI, which generally cover much broader scopes of activities. At the same time, within some capacity-building areas of the NCSI, the EU baseline is more detailed.

The eIDAS Regulation regulates Member States' electronic identification and electronic trust services, which overlaps the NCSI capacity areas of secure environments for e-services, e-identification and e-signatures. The regulation ensures the use of national electronic identification schemes to access public services in other EU countries where these systems are available. It ensures that electronic trust services (e-signatures, e-seals, time stamp, e-delivery service and website authentication) work across borders and have the same legal status as traditional paper-based processes.[1]

As evident in Table 1, the NCSI capacity-building areas five and six focus on these issues, but in addition to the basic requirements of having a legal framework for e-signatures, ensuring that e-signatures have a legal effect, and that trust service providers are qualified and supervised by a public authority, the NCSI criteria also includes the application of two-factor authentication for e-services.

The General Data Protection Regulation (GDPR) focuses on reinforcing individuals' rights, ensures stronger enforcement of the rules, streamlines international transfers of personal data and sets global data protection standards. The regulation provides a "right to be forgotten", data protection by design and by default, easier access to an individual's data and the right to know when it has been hacked. In addition, data protection authorities of Member States will be able to fine companies that do not comply with EU rules.[2]

The General Data Protection Directive (GDPD) protects individuals' fundamental right to data protection whenever personal data are used by criminal law enforcement authorities. It ensures that the personal data of victims, witnesses, and suspects of crime are duly protected and will facilitate cross-border cooperation in the fight against crime and terrorism.[3]

GDPR and GDPD allocate a responsibility to personal data controllers and processors to notify of personal data breaches. These areas are more broadly covered by the NCSI with a requirement to establish a data protection authority as part of ensuring baseline cyber security levels in the country, and with a requirement of critical information infrastructure providers, and all public authorities report about cyber incidents to a national competent authority.

The Cybercrime Directive is covered in the NCSI in the capacity-building area of fighting cybercrimes. The NCSI evaluates whether cybercrimes are criminalised in domestic legislation, if there is a unit in the police that is specialised in cybercrime prevention and investigation, and if there is a 24/7 contact point for international cooperation, among other criteria. In addition, the NCSI also assesses if a country is implementing the Budapest Convention on cybercrimes. While GDPD provides that national personal data supervisory authorities must cooperate and provide international mutual assistance, the NCSI measures this capacity on

[1] *https://ec.europa.eu/digital-single-market/en/trust-services-and-eid. Accessed on 14 August 2017.*
[2] *http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm. Accessed on 14 August 2017.*
[3] *http://ec.europa.eu/justice/data-protection/reform/index_en.htm. Accessed on 14 August 2017.*

the national level, looking at the various cooperation forms, such as formal cooperation agreements with other countries, having a governmental department whose task is international cooperation, cooperating in various international cyber security cooperation formats.

In summary, while the NCSI does not directly address a number of more detailed requirements that the EU baseline prescribes (presented in Table 1), in the opinion of the research team it nevertheless includes the most important requirements that the Eastern Partnership countries should prioritise in order to harmonise their legislative, organisational, and operational frameworks with the EU. Moreover, as demonstrated in this chapter in a number of areas the NCSI includes some important indicators without which it would be difficult to provide that capacity. For example, in the area of crisis management, the NCSI assesses if a country has established a special operational level centre for managing a major cyber crisis on the national level. This aspect is not included directly in the EU baseline, but without them it would be very hard to handle a major cyber crisis that impacts several public and private sector actors.

Thus, we conclude that by large the 12 the NCSI capacity-building areas overlap with the EU baseline, while it also has requirements in three areas: education, military cyber defence, and international cooperation.

Table 1. NCSI compatibility with the EU baseline

No		EU baseline
1	Capacity to develop national cyber security policies	
1.1	National-level cyber security policy unit (department, etc.)	NIS Directive, article 8 • Designate competent authorities and contact point to ensure implementation of directive
1.2	National-level cyber security coordination format (committee, etc.)	N/A
1.3	National-level cyber security terms and definitions	N/A
1.4	National-level cyber security strategy (valid)	NIS Directive, article 7 • Adopt national strategy • Adopt national strategy defining policy measures
1.5	National-level cyber security implementation plan (valid)	N/A
2	Capacity to analyse national-level cyber threats	
2.1	National-level cyber threat analysis unit (department, etc.)	NIS Directive, article 7 • National strategy shall include a risk assessment plan to identify risks NIS Directive, article 9 • CSIRTs must be responsible for risk and incident handling

		NIS Directive, article 10 • Competent authority or CSIRT must receive incident notifications NIS Directive, annex I • CSIRTS must provide dynamic risk and incident analysis and situational awareness
2.2	Annual public cyber threat reports are published	Personal Data Directive, article 49 • Supervisory authority must make public annual reports that may include infringements of personal data.
3	Capacity to provide cyber security education	
3.1	Cyber safety website for the general public	N/A
3.2	Nation-wide public awareness raising activity in the last 3 years	N/A
3.3	Cyber safety competencies in primary education	N/A
3.4	Cyber safety competencies in secondary education	N/A
3.5	Cyber safety competencies in vocational education	N/A
3.6	Bachelor's level cyber security programme (at least 1)	N/A
3.7	Master's level cyber security programme (at least 1)	N/A
3.8	PhD level cyber security programme (at least 1)	N/A
3.9	Cyber security professional association	N/A
4	Capacity to provide international cyber security	
4.1	International cyber security cooperation unit (department, etc.)	N/A
4.2	Implementation of the Convention on Cybercrime	N/A
4.3	Cooperation agreements with other countries (at least 1 country)	N/A

4.4	Representation in international cooperation formats (at least 1)	NIS Directive, Article 11 and 12 • Member States must belong to the Coordination Group and CSIRTs network at the EU level that exchanges information, lessons learnt from exercises. NIS Directive, Article 16 • Competent authority of CSIRT must inform when appropriate and if the incident concerns other member states the other affected member states.
4.5	International / regional cyber security organisation in the country	N/A
4.6	Capacity-building project in another country in the last 3 years	N/A
5	Capacity to ensure baseline cyber security	
5.1	Baseline cyber security management unit (agency, etc.)	NIS Directive, Article 8: • One or more competent authorities • Monitoring of the application of the directive • Contact points • Sufficient resources NIS Directive, (67) • Competent authorities should have legislative powers to obtain sufficient information in order to assess the level of security
		• National level point of contact to collaborate with the EU cooperation group, EU members states, EU CSIRTs network
5.2	Personal data protection authority (independent organisation)	EU Directive 2016/680, Chapter VI • Independent supervisory authorities
5.3	Legislation for information classification (public, confidential, etc.)	N/A
5.4	Information / cyber security management standard	NIS Directive, Article 19: • Encourage the use of EU and international standards
5.5	Accreditation of public sector ICT solutions before introduction	NIS Directive, (69) • Network and information systems testing, security assessments and compliance monitoring NIS Directive, Article 16: • 1. a) the security of systems and facilities • 1. d) monitoring, auditing and testing

5.6	Regular audits of public sector ICT solutions	NIS Directive, (69): • Network and information systems testing, security assessments and compliance monitoring NIS Directive, Article 15: • 2. Information about ICT security and policies (operators of essential services) • 2. Evidence of effective implementation of security policies – audit for example (operators of essential services) NIS Directive, Article 16: • 1. a) the security of systems and facilities • 1. d) monitoring, auditing and testing NIS Directive, Article 17: • 2. Information about ICT security and policies (digital service providers)
6	Capacity to provide secure environment for e-services	
6.1	Secure data exchange environment for e-services	eIDAS Regulation
6.2	Up-to-date cryptographic solution for the environment	N/A
7	Capacity to provide e-identification and e-signatures	
7.1	Citizens and legal entities have a unique identifier	N/A
7.2	Public e-services identify users via a unique identifier	N/A
7.3	Public e-services use 2-factor authentication	
7.4	A legal framework for electronic signature	eIDAS Regulation
7.5	Supervision over qualified trust services providers (responsibility)	eIDAS Regulation
7.6	A qualified electronic signature has legal effect	eIDAS Regulation

8	Capacity to protect essential e-services / CII	
8.1	The essential e-services / CII are defined	NIS Directive, Article 5: • Criteria for identification of the operators of essential services NIS Directive (19, 25) • Assess entities in sectors and subsectors • Establish a list of services, review regularly and update if necessary
8.2	National-level essential e-services / CII protection unit	NIS Directive, Article 8: • One or more competent authorities • Monitoring of the application of the directive • Contact points • Sufficient resources A competent authority must have a mandate to give mandatory guidelines to private sector operators, thus this right must be stipulated in legislation
8.3	Service continuity requirements for essential e-services / CII operators	NIS Directive, Article 14: • Responsibility to take appropriate measures (mandatory for essential service operators) NIS Directive (49) • Digital service providers take measures they consider appropriate
		NIS Directive, Article 21: • Effective, proportionate, dissuasive penalties must be identified and implemented. Personal Data Protection Directive, article 29: • Controller and processor of personal data must implement technical and organisational measures to ensure security Personal Data Protection Directive, Article 57: • Effective, proportionate, dissuasive penalties must be identified and implemented
8.4	Essential e-services / CII operators have a cyber security manager	Personal Data Protection Directive, article 32: • Controller must designate a data protection officer

9	Capacity to detect and respond to cyber incidents 24/7	
9.1	National-level cyber incidents response unit	NIS Directive, Article 9: • Designated CSIRT(s) responsible for risk and incident handling • Adequate resources to carry out tasks • Cooperation with EU's CSIRTs network • Access to appropriate and secure ICT infrastructure on the national level • Competences/authorities and incident handling procedures NIS Directive, Annex 1 • CSIRT roles and responsibilities ◦ High availability of communication channels ◦ Secure premises and IT systems ◦ Ensure business continuity (requests system, infrastructure, staff) ◦ Fulfil its tasks ◦ Establish cooperation with the private sector ◦ Promote common incident and risk handling procedures; incident, risk, and information classification schemes ◦ Policy and regulations must support fulfilment of tasks
9.2	Cyber incidents reporting responsibility	NIS Directive, Article 10: • CSIRTs receive incident notifications or incidents' data NIS Directive, Article 14: • Notification responsibility including information on whether there will be any cross-border impact (operators of essential services) NIS Directive, Article 16: • Notification responsibility including information on whether there will be any cross-border impact (digital service providers) NIS Directive, (67), Article 20: • Voluntary notification responsibility (other operators and providers) Personal Data Protection Directive, (61), Article 30: • Notification responsibility (controllers and processors of personal data) for personal data breaches Personal Data Protection Regulation, Article 33: • Notification responsibility (controllers and processors of personal data) for personal data breaches

9.3	Official format for practical public-private cooperation	NIS Directive, Article 7: • National strategy shall identify measures for preparedness, response and recovery, including cooperation between the public and private sectors NIS Directive, annex I: • CSIRTs shall establish cooperation relationship with the private sector NIS Directive, (35): • To encourage operators of essential services and digital service providers to cooperate informally
9.4	Exchange of classified information	NIS Directive, (59) • CSIRTs should keep information about product vulnerabilities strictly confidential • Competent authorities should preserve informal and trusted channels of information-sharing
10	Capacity to manage large-scale cyber crises	
10.1	Cyber crisis management plan	NIS Directive, (69) • Service continuity strategy and contingency plans, disaster recovery capabilities. NIS Directive, Article 7: • National strategy must identify measures for preparedness, response and recovery, including cooperation between the public and private sectors NIS Directive, (69) • Implementation acts of the directive should take into account service continuity contingency plans, exercise contingency plans.
10.2	Cyber security/crisis operations centre	N/A
10.3	Crisis management exercise with cyber component in the last 3 years	N/A
10.4	National-level cyber crisis management exercise in the last 3 years	NIS Directive, (36), (38), (42), (69): • Exercises and drills NIS Directive, Article 11: • k) drills, education and training NIS Directive, Article 12: • h) drills European Parliament Resolution of 12 June 2012 on critical information infrastructure protection (2011/2284 (INI)) • “organise regular national and pan-European cyber incident exercises”

10.5	Participation in international cyber crisis exercises in the last 3 years	European Parliament Resolution of 12 June 2012 on critical information infrastructure protection (2011/2284 (INI)) • “organise regular national and pan-European cyber incident exercises”
10.6	Using volunteers in cyber crisis management	N/A
11	Capacity to fight against cybercrime	
11.1	Cybercrimes are criminalised	Directive 2013/40/EU on attacks against information systems • Articles 3, 4, 5, 6, 7, 8
11.2	Unit for fighting against cybercrime (department, agency, etc.)	N/A
11.3	Unit for digital forensics (department, agency, etc.)	N/A
11.4	Electronic evidences are regulated	N/A
11.5	24/7 contact point for international cybercrime	Directive 2013/40/EU on attacks against information systems • Article 13
12.	Capacity to conduct military cyber defence operations	
12.1	Cyber operations planning unit (department, command, etc.)	N/A
12.2	Cyber operations units	N/A
12.3	Exercise with a cyber operations component in the last 3 years	N/A
12.4	Cyber operation exercise in the last 3 years	N/A
12.5	Participation in international cyber exercise in the last 3 years	N/A

2. Research results

Armenia

I GENERAL CYBER SECURITY INDICATORS

1. Capacity to develop national cyber security policies

1.1 National-level cyber security policy unit (department, etc.)

Criteria: *A central government entity has a national level department or organisation that is specialised in national cyber security policy development. Work outcomes of this unit are for example the official national cyber security strategy and implementation plan.*

Situation in the country: ⊗ No such capacity.

Comment: The Secretariat of the National Security Council under the Presidential Administration was coordinating the development of Information Security Concept of 2009.

1.2 National-level cyber security coordination format (committee, etc.)

Criteria: *The central government has established the national-level cyber security coordination format (committee, council, working group, etc.) for cyber security policy coordination. This format includes relevant public, private and third sector entities.*

Situation in the country: ⊗ No such capacity.

1.3 National-level cyber security terms and definitions

Criteria: *The central government has established national-level cyber security terms and definitions by legislation.*

Situation in the country: ⊗ No such capacity.

Comment: The Information Security Concept defines key terms related to information security, but cyber-security terms are not defined in any regulation.

1.4 National-level cyber security strategy (valid)

Criteria: *The central government has established the national-level cyber security strategy or other equivalent document.*

Situation in the country: ⊗ No such capacity.

1.5 National-level cyber security implementation plan (valid)

Criteria: *The central government has established the national-level cyber security implementation plan or another equivalent document.*

Situation in the country: ⊗ No such capacity.

2. Capacity to analyse national-level cyber threats

2.1 National-level cyber threat analysis unit (department, etc.)

Criteria: *A central government entity has a national level department or organisation that is specialised in national cyber threat analysis. The work outcomes of this unit are regular comprehensive cyber threat analysis and risk assessments. These risk assessments are the basis for national-level cyber security planning (national cyber security strategy development, etc.).*

Situation in the country: ⊗ No such capacity.

2.2 Annual public cyber threat reports are published

Criteria: *The public part of the national cyber threat analysis is published at least once a year. The aim of this report is to inform and educate the general public.*

Situation in the country: ⊗ No such capacity.

3. Capacity to provide cyber security education

3.1 Cyber safety website for the general public

Criteria: *Public authorities provide or finance at least one cyber safety website for the general public. The website provides up-to-date information about cyber threats and security measures related to ICT systems, as well as other useful materials and guidance for regular users. The website should inform about timely threats and security measures related to ICT systems (computers, mobile devices, information systems, e-services, etc.). Websites that inform only about social media threats (cyber bullying, etc.) are not alone accepted. These websites could be added as additional materials.*

Situation in the country: ⊗ No such capacity.

3.2 Nationwide public awareness-raising activity in the last 3 years

Criteria: *Public authorities have organised at least one public awareness-raising activity in the last 3 years. The media campaign should be nationwide (TV, radio, newspapers, etc.).*

Situation in the country: ⊗ No such capacity.

3.3 Cyber safety competencies in primary education

Criteria: *Primary education (ISCED 2011 Level 1) curricula include cyber safety / computer safety competences.*

Situation in the country: ⊗ No such capacity.

3.4 Cyber safety competencies in secondary education

Criteria: *Secondary education (ISCED 2011 Level 2-4) curricula include cyber safety / computer safety competences.*

Situation in the country: ⊗ No such capacity.

3.5 Cyber safety competencies in vocational education

Criteria: *Vocational education (ISCED 2011 Level 3-4) curricula include cyber safety / computer safety components.*

Situation in the country: ⊗ No such capacity.

3.6 Bachelor's level cyber security programme (at least 1)

Criteria: *There is at least one cyber security / electronic information security focused programme on the bachelor's or equivalent level (ISCED 2011 Level 6).*

Situation in the country: ⊗ No such capacity.

3.7 Master's level cyber security programme (at least 1)

Criteria: *There is at least one cyber security / electronic information security focused programme on the master's or equivalent level (ISCED 2011 Level 7)*

Situation in the country: ⊗ No such capacity.

3.8 PhD level cyber security programme (at least 1)

Criteria: *There is at least one cyber security / electronic information security focused programme on the PhD or equivalent level (ISCED 2011 Level 8).*

Situation in the country: ⊗ No such capacity.

3.9 Cyber security professional association

Criteria: *There is a professional association of cyber/information security specialists, managers or auditors.*

Situation in the country: ⊗ No such capacity.

4. Capacity to provide international cyber security

4.1 International cyber security cooperation unit (department, etc.)

Criteria: *The ministry responsible for foreign affairs has a department or an organisation that is specialised in international cyber security.*

Situation in the country: ⊗ No such capacity.

4.2 Implementation of the Convention on Cybercrime

Criteria: *The government has enforced the Convention on Cybercrime of the Council of Europe. The government has ratified or acceded to the convention. The convention is fully implemented.*

Situation in the country: ✓ There is such a capacity.

Reference: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=u9Jjs5so

http://parliament.am/legislation.php?sel=show&ID=1349&lang=eng#9

4.3 Cooperation agreements with other countries (at least 1 country)

Criteria: *The government has bilateral, regional, international cyber security cooperation agreements with other countries or international organisations. One other agreement is sufficient that is not the Convention on Cybercrime of the Council of Europe.*

Situation in the country: ⊗ No such capacity.

4.4 Representation in international cooperation formats (at least 1)

Criteria: *The government is represented regularly in a cooperation format that deals with international cyber security.*

Situation in the country: ⊗ No such capacity.

4.5 International cyber security organisation in the country

Criteria: *A regional or international cyber security organisation with regional or international functions is located in the country.*

Situation in the country: ⊗ No such capacity.

4.6 Cyber security capacity-building

Criteria: *The country has (co)financed or (co)organised at least one capacity-building project for another country in the last 3 years.*

Situation in the country: ⊗ No such capacity.

II. BASELINE CYBER SECURITY INDICATORS

5. Capacity to ensure baseline cyber security

5.1 Baseline cyber security management unit (agency, etc.)

Criteria: *A central government entity has a department or organisation that is specialised in national-level baseline cyber security management – development, implementation, co-ordination and supervision.*

Situation in the country: ⊗ No such capacity.

5.2 Personal data protection authority (independent organisation)

Criteria: *There is an independent public supervisory authority that is responsible for personal data protection.*

Situation in the country: ✓ There is such a capacity.

Reference: http://www.arlis.am/DocumentView.aspx?DocID=100952
http://www.arlis.am/DocumentView.aspx?DocID=110606

5.3 Legislation for information classification (public, confidential, etc.)

Criteria: *There is legislation for information classification – public, private, classified, restricted, confidential, critical, etc.*

Situation in the country: ⊗ No such capacity.

5.4 Information / cyber security management standard

Criteria: *There is a baseline regulation or an adopted standard for information/cyber security management for public sector entities. The regulation or standard is mandatory for public sector entities.*

Situation in the country: ⊗ No such capacity.

5.5 Accreditation of public sector ICT solutions before introduction

Criteria: *Before the introduction of an ICT solution (information system, public e-service, etc.) in the public sector, an official security accreditation/audit takes place.*

Situation in the country: ⊗ No such capacity.

5.6 Regular audits of public sector ICT solutions

Criteria: *The operators of public sector ICT solutions (information systems, e-services, etc.) have to order regular independent ICT security audits.*

Situation in the country: ⊗ No such capacity.

6. Capacity to provide a secure environment for e-services

6.1 Secure data exchange environment for e-services

Criteria: *There is a secure inter-organisational data exchange environment in the country (secure internet), which enables public sector entities to provide secure web services for citizens and entrepreneurs. Private sector and other entities will be interfaces with the environment, if they provide a public service or participate in it.*

Situation in the country: ⊗ No such capacity.

6.2 Up-to-date cryptographic solution for the environment

Criteria: *In the data exchange environment, the cryptographic requirement complies with recognised up-to-date guidelines (NIST Special Publication 800-78-3, ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012), etc.)*

Situation in the country: ⊗ No such capacity.

7. Capacity to provide e-identification and e-signatures

7.1 Citizens and legal entities have a unique identifier

Criteria: *All citizens, residents and legal entities are identifiable via a persistent unique identifier. The identifier is used on public sector registries. It is not a number of the personal identification document, but a unique number assigned to a person for life.*

Situation in the country: ⊗ No such capacity.

7.2 Public e-services identify users via a unique identifier.

Criteria: *The public-sector e-services use the identifier for identification; there is no need for additional queries. There is a legal framework for electronic identification and authentication. The framework is based on the unique identifier.*

Situation in the country: ⊗ No such capacity.

7.3 Public e-services use 2-factor authentication

Criteria: *Public sector e-services use 2-factor authentication and strong cryptographic solutions in national electronic authentication. The cryptographic solution has to comply with NIST Special Publication 800-78-3, ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012), etc.*

Situation in the country: ⊗ No such capacity.

7.4 A legal framework for electronic signature

Criteria: *A legal framework for electronic signature is established in the country. The electronic signature system is based on the aforementioned unique identifier. There are requirements for trust services required for electronic signature. These requirements are established by legislation.*

Situation in the country: ✓ There is such a capacity.

Reference: http://www.parliament.am/law_docs/150105HO40eng.pdf

7.5 Supervision over qualified trust services providers

Criteria: *There is an authority that is responsible for the supervision of qualified trust service providers and for granting the qualified status.*

Situation in the country: ⊗ No such capacity.

7.6 A qualified electronic signature has legal effect

Criteria:	*A qualified electronic signature has the equivalent legal effect of a handwritten signature.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://www.parliament.am/law_docs/150105HO40eng.pdf
Comment:	Chapter 2, Article 4.

8. Capacity to protect essential e-services / CII

8.1 The essential e-services / CII are defined

Criteria:	*The essential e-services / critical information infrastructure (CII) are defined by legislation.*
Situation in the country:	✗ No such capacity.

8.2 National level essential e-services / CII protection unit

Criteria:	*A central government entity has a department or organisation that is specialised in essential e-services / critical information infrastructure protection. The unit has the responsibility to develop adequate security measures, and coordinate and supervise the implementation of specific security measures.*
Situation in the country:	✗ No such capacity.

8.3 Service continuity requirements for essential e-services / CII operators

Criteria:	*Data processing and service continuity requirements (downtime elimination time, readiness for disruption, etc.) are established for essential e-services / CII operators by legislation.*
Situation in the country:	✗ No such capacity.

8.4 Essential e-services / CII operators have a cyber security manager

Criteria:	*The essential e-services / CII operators have to appoint a cyber/information security manager.*
Situation in the country:	✗ No such capacity.

III. INCIDENT AND CRISIS MANAGEMENT INDICATORS

9. Capacity to detect and respond to cyber incidents 24/7

9.1 National-level cyber incident response unit

Criteria: *The government has a unit (common name is CERT, CIRC, etc.) that is specialised in national-level cyber incident detection and response. The unit is responsible for 24/7 data gathering of incidents in cyberspace. The authority manages the comprehensive picture of incidents in national cyberspace.*

Situation in the country: ⊗ No such capacity.

9.2 Cyber incidents reporting responsibility

Criteria: *Public sector entities and CII operators have the responsibility to report about cyber incidents.*

Situation in the country: ⊗ No such capacity.

9.3 Official format for practical public-private cooperation

Criteria: *There is an official cooperation format (organisation, association, etc.) for operational (practical) public, private and third sector cooperation. Activities are specified in the legislation, agreement or in another official format.*

Situation in the country: ⊗ No such capacity.

9.4 Exchange of classified information

Criteria: *According to legislation, public, private and third sector entities may exchange classified information.*

Situation in the country: ⊗ No such capacity.

10. Capacity to manage large-scale cyber crises

10.1 Cyber crisis management plan

Criteria: *The government has established a comprehensive crisis management plan for large-scale cyber incidents. The plan and its different components must be established by legislation.*

Situation in the country: ⊗ No such capacity.

10.2 Cyber security/crisis operations centre

Criteria: *The government has established a permanent national-level cyber security/crisis operations centre. The centre acts as the cyber situation centre and operations staff for the crisis manager.*

Situation in the country: ⊗ No such capacity.

10.3 Crisis management exercise with cyber component

Criteria: *The government has conducted a crisis management exercise with a cyber component in the last 3 years.*

Situation in the country: ⊗ No such capacity.

10.4 National-level cyber crisis management exercise

Criteria: *The government has conducted the national-level cyber crisis management exercise in the last 3 years. The main focus of the exercise is the management of large-scale cyber incidents.*

Situation in the country: ⊗ No such capacity.

10.5 Participation in international cyber crisis exercises

Criteria: *The country has participated in an international cyber crisis management exercise in the last 3 years.*

Situation in the country: ⊗ No such capacity.

10.6 Using volunteers in cyber crisis management

Criteria: *The government has established a system for using volunteers in large-scale cyber crisis management. The procedures for using volunteers must be established by legislation.*

Situation in the country: ⊗ No such capacity.

11. Capacity to fight cyber crimes

11.1 Cyber crimes are criminalised

Criteria: *The state has defined cybercrimes and established them by legislation. The regulations are in line with the Council of the Europe Convention on Cybercrime. Law enforcement authorities are obliged to start a criminal investigation if there are sufficient grounds for a criminal offence.*

Situation in the country: ✓ There is such a capacity.

Reference: http://www.arlis.am/DocumentView.aspx?docid=48028
http://parliament.am/legislation.php?sel=show&ID=1349&lang=eng#9

11.2 Unit for fighting cyber crime (department, agency, etc.)

Criteria: *The government has the capacity to conduct criminal proceedings for cybercrimes. A government entity has a department or an organisation that is specialised in combating cybercrime. The unit has competence in the following areas: 1) Prevention of cybercrime. 2) Conducting surveillance measures or special investigation techniques. 3) Conducting pre-trial investigations. The role and responsibilities of the units must be established by legislation.*

Situation in the country: ✗ No such capacity.

11.3 Unit for digital forensics (department, agency, etc.)

Criteria: *A government entity has a department or an organisation that is specialised in digital forensics:*

- *computer forensics*
- *mobile forensics*
- *hardware forensics, i.e. skimmers*
- *software forensics, malware analysis*

The role and responsibilities of the units must be established by legislation.

Situation in the country: ✓ There is such a capacity.

Reference: http://www.nbe.am/index.php?option=com_content&view=article&id=404&Itemid=544&lang=en

11.4 Electronic evidences are regulated

Criteria: *National regulations provide for rules on the collection and use of electronic evidence. General rules on evidence collection and use alike that also cover electronic evidence or a specific regulation on electronic evidence have been accepted.*

Situation in the country: ✗ No such capacity.

11.5 International cyber crimes 24/7 contact point

Criteria: *There is an international contact point for cyber crimes, which operates 24/7.*

Situation in the country:	✓ There is such a capacity.
Reference:	https://rm.coe.int/16804b3493 http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/declarations?p_auth=YWNX7YZF
Comment:	The Division on High-Tech Crime, Main Department on Combat Against Organised Crime of the Police of the Republic of Armenia

12. Capacity to conduct military cyber defence operations

12.1 Cyber operation planning unit (department, command, etc.)

Criteria:	*Military forces have a department or an organisation that is specialised in cyber operation planning. This unit could be part of a general operation planning unit.*
Situation in the country:	⊗ No such capacity.

12.2 Cyber operation units

Criteria:	*Military forces have a unit that is specialised in cyber operations.*
Situation in the country:	⊗ No such capacity.

12.3 Exercise with a cyber operations component

Criteria:	*Military forces have conducted an exercise with a cyber operations component in the last 3 years.*
Situation in the country:	⊗ No such capacity.

12.4 Cyber operation exercise in the last 3 years

Criteria:	*Military forces have conducted a cyber operation exercise in the last 3 years.*
Situation in the country:	⊗ No such capacity.

12.5 Participation in international cyber exercise in the last 3 years

Criteria:	*The country's military team has participated in an international cyber operation exercise in the last 3 years.*
Situation in the country:	⊗ No such capacity.

Azerbaijan

I GENERAL CYBER SECURITY INDICATORS

1. Capacity to develop national cyber security policies

1.1 National-level cyber security policy unit (department, etc.)

Criteria: *A central government entity has a national level department or organisation that is specialised in national cyber security policy development. Work outcomes of this unit are for example the official national cyber security strategy and implementation plan.*

Situation in the country: ⊗ No such capacity.

1.2 National-level cyber security coordination format (committee, etc.)

Criteria: *The central government has established the national-level cyber security coordination format (committee, council, working group, etc.) for cyber security policy coordination. This format includes relevant public, private and third sector entities.*

Situation in the country: ⊗ No such capacity.

1.3 National-level cyber security terms and definitions

Criteria: *The central government has established national-level cyber security terms and definitions by legislation.*

Situation in the country: ⊗ No such capacity.

1.4 National-level cyber security strategy (valid)

Criteria: *The central government has established the national-level cyber security strategy or other equivalent document.*

Situation in the country: ⊗ No such capacity.

Comment: The National Strategy of the Republic of Azerbaijan on the Development of the İnformation Society for the years 2014-2020 contains elements on cyber security.

1.5 National-level cyber security implementation plan (valid)

Criteria: *The central government has established the national-level cyber security implementation plan or another equivalent document.*

Situation in the country: ⊗ No such capacity.

2. Capacity to analyse national-level cyber threats

2.1 National-level cyber threat analysis unit (department, etc.)

Criteria: *A central government entity has a national level department or organisation that is specialised in national cyber threat analysis. The work outcomes of this unit are regular comprehensive cyber threat analysis and risk assessments. These risk assessments are the basis for national-level cyber security planning (national cyber security strategy development, etc.).*

Situation in the country: ✓ There is such a capacity.

Reference: http://e-qanun.az/framework/24353

Comment: Article 4.

2.2 Annual public cyber threat reports are published

Criteria: *The public part of the national cyber threat analysis is published at least once a year. The aim of this report is to inform and educate the general public.*

Situation in the country: ⊗ No such capacity.

3. Capacity to provide cyber security education

3.1 Cyber safety website for the general public

Criteria: *Public authorities provide or finance at least one cyber safety website for the general public. The website provides up-to-date information about cyber threats and security measures related to ICT systems, as well as other useful materials and guidance for regular users. The website should inform about timely threats and security measures related to ICT systems (computers, mobile devices, information systems, e-services, etc.). Websites that inform only about social media threats (cyber bullying, etc.) are not alone accepted. These websites could be added as additional materials.*

Situation in the country: ✓ There is such a capacity.

		Reference:	www.cert.az www.cert.gov.az
3.2	Nationwide public awareness-raising activity in the last 3 years	Criteria:	*Public authorities have organised at least one public awareness-raising activity in the last 3 years. The media campaign should be nationwide (TV, radio, newspapers, etc.).*
		Situation in the country:	✓ There is such a capacity.
		Reference:	https://www.cert.az/en/news/cat21/ http://www.mincom.gov.az/media/xeberler/details/12062 http://websecurity.hackathonazerbaijan.org/
3.3	Cyber safety competencies in primary education	Criteria:	*Primary education (ISCED 2011 Level 1) curricula include cyber safety / computer safety competences.*
		Situation in the country:	✗ No such capacity.
3.4	Cyber safety competencies in secondary education	Criteria:	*Secondary education (ISCED 2011 Level 2-4) curricula include cyber safety / computer safety competences.*
		Situation in the country:	✗ No such capacity.
3.5	Cyber safety competencies in vocational education	Criteria:	*Vocational education (ISCED 2011 Level 3-4) curricula include cyber safety / computer safety components.*
		Situation in the country:	✗ No such capacity.
3.6	Bachelor's level cyber security programme (at least 1)	Criteria:	*There is at least one cyber security / electronic information security focused programme on the bachelor's or equivalent level (ISCED 2011 Level 6).*
		Situation in the country:	✗ No such capacity.
3.7	Master's level cyber security programme (at least 1)	Criteria:	*There is at least one cyber security / electronic information security focused programme on the master's or equivalent level (ISCED 2011 Level 7)*

Situation in the country:	⊗ No such capacity.

3.8 PhD level cyber security programme (at least 1)

Criteria:	*There is at least one cyber security / electronic information security focused programme on the PhD or equivalent level (ISCED 2011 Level 8).*
Situation in the country:	⊗ No such capacity.

3.9 Cyber security professional association

Criteria:	*There is a professional association of cyber/information security specialists, managers or auditors.*
Situation in the country:	⊗ No such capacity.

4. Capacity to provide international cyber security

4.1 International cyber security cooperation unit (department, etc.)

Criteria:	*The ministry responsible for foreign affairs has a department or an organisation that is specialised in international cyber security.*
Situation in the country:	⊗ No such capacity.

4.2 Implementation of the Convention on Cybercrime

Criteria:	*The government has enforced the Convention on Cybercrime of the Council of Europe. The government has ratified or acceded to the convention. The convention is fully implemented.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://e-qanun.az/framework/18619

4.3 Cooperation agreements with other countries (at least 1 country)

Criteria:	*The government has bilateral, regional, international cyber security cooperation agreements with other countries or international organisations. One other agreement is sufficient that is not the Convention on Cybercrime of the Council of Europe.*
Situation in the country:	✓ There is such a capacity.

Reference:	http://www.e-qanun.az/framework/33840
Comment:	"Memorandum of Understanding between the Ministry of Communications and High Technologies of the Republic of Azerbaijan and the Ministry of Communications and Information Technology of the Islamic Republic of Iran on cooperation in the field of electronic security"

4.4 Representation in international cooperation formats (at least 1)

Criteria:	*The government is represented regularly in a cooperation format that deals with international cyber security.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://e-qanun.az/framework/24353
Comment:	FIRST

4.5 International cyber security organisation in the country

Criteria:	*A regional or international cyber security organisation with regional or international functions is located in the country.*
Situation in the country:	✗ No such capacity.

4.6 Cyber security capacity-building

Criteria:	*The country has (co)financed or (co)organised at least one capacity-building project for another country in the last 3 years.*
Situation in the country:	✗ No such capacity.

II. BASELINE CYBER SECURITY INDICATORS

5. Capacity to ensure baseline cyber security

5.1 Baseline cyber security management unit (agency, etc.)

Criteria:	*A central government entity has a department or organisation that is specialised in national-level baseline cyber security management – development, implementation, coordination and supervision.*
Situation in the country:	✗ No such capacity.

5.2 Personal data protection authority (independent organisation)

Criteria: *There is an independent public supervisory authority that is responsible for personal data protection.*

Situation in the country: ⊗ No such capacity.

5.3 Legislation for information classification (public, confidential, etc.)

Criteria: *There is legislation for information classification – public, private, classified, restricted, confidential, critical, etc.*

Situation in the country: ✓ There is such a capacity.

Reference: http://e-qanun.gov.az/framework/3525
http://www.e-qanun.az/framework/5526
http://www.e-qanun.az/alpidata/framework/data/11/c_f_11142.htm

Comment: 1) Law on information, digitalisation and protection of information of the Republic of Azerbaijan. 3) see Article 34

5.4 Information / cyber security management standard

Criteria: *There is a baseline regulation or an adopted standard for information/cyber security management for public sector entities. The regulation or standard is mandatory for public sector entities.*

Situation in the country: ⊗ No such capacity.

5.5 Accreditation of public sector ICT solutions before introduction

Criteria: *Before the introduction of an ICT solution (information system, public e-service, etc.) in the public sector, an official security accreditation/audit takes place.*

Situation in the country: ⊗ No such capacity.

5.6 Regular audits of public sector ICT solutions

Criteria: *The operators of public sector ICT solutions (information systems, e-services, etc.) have to order regular independent ICT security audits.*

Situation in the country: ⊗ No such capacity.

6. Capacity to provide a secure environment for e-services

6.1 Secure data exchange environment for e-services

Criteria: *There is a secure inter-organisational data exchange environment in the country (secure internet), which enables public sector entities to provide secure web services for citizens and entrepreneurs. Private sector and other entities will be interfaces with the environment, if they provide a public service or participate in it.*

Situation in the country: ⊗ No such capacity.

6.2 Up-to-date cryptographic solution for the environment

Criteria: *In the data exchange environment, the cryptographic requirement complies with recognised up-to-date guidelines (NIST Special Publication 800-78-3, ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012), etc.)*

Situation in the country: ⊗ No such capacity.

7. Capacity to provide e-identification and e-signatures

7.1 Citizens and legal entities have a unique identifier

Criteria: *All citizens, residents and legal entities are identifiable via a persistent unique identifier. The identifier is used on public sector registries. It is not a number of the personal identification document, but a unique number assigned to a person for life.*

Situation in the country: ⊗ No such capacity.

7.2 Public e-services identify users via a unique identifier.

Criteria: *The public-sector e-services use the identifier for identification; there is no need for additional queries. There is a legal framework for electronic identification and authentication. The framework is based on the unique identifier.*

Situation in the country: ⊗ No such capacity.

7.3 Public e-services use 2-factor authentication

Criteria: *Public sector e-services use 2-factor authentication and strong cryptographic solutions in national electronic authentication. The cryptographic solution has to comply with NIST Special Publication 800-78-3, ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012), etc.*

Situation in the country:	✓ There is such a capacity.
Reference:	www.e-gov.az

7.4 A legal framework for electronic signature

Criteria:	*A legal framework for electronic signature is established in the country. The electronic signature system is based on the aforementioned unique identifier. There are requirements for trust services required for electronic signature. These requirements are established by legislation.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://e-qanun.az/framework/5916

7.5 Supervision over qualified trust services providers

Criteria:	*There is an authority that is responsible for the supervision of qualified trust service providers and for granting the qualified status.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://e-qanun.az/framework/5916
Comment:	Article 33.

7.6 A qualified electronic signature has legal effect

Criteria:	*A qualified electronic signature has the equivalent legal effect of a handwritten signature.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://e-qanun.az/framework/5916
Comment:	Article 3.

8. Capacity to protect essential e-services / CII

8.1 The essential e-services / CII are defined

Criteria: *The essential e-services / critical information infrastructure (CII) are defined by legislation.*

Situation in the country: ⊗ No such capacity.

8.2 National level essential e-services / CII protection unit

Criteria: *A central government entity has a department or organisation that is specialised in essential e-services / critical information infrastructure protection. The unit has the responsibility to develop adequate security measures, and coordinate and supervise the implementation of specific security measures.*

Situation in the country: ⊗ No such capacity.

8.3 Service continuity requirements for essential e-services / CII operators

Criteria: *Data processing and service continuity requirements (downtime elimination time, readiness for disruption, etc.) are established for essential e-services / CII operators by legislation.*

Situation in the country: ⊗ No such capacity.

8.4 Essential e-services / CII operators have a cyber security manager

Criteria: *The essential e-services / CII operators have to appoint a cyber/information security manager.*

Situation in the country: ⊗ No such capacity.

III. INCIDENT AND CRISIS MANAGEMENT INDICATORS

9. Capacity to detect and respond to cyber incidents 24/7

9.1 National-level cyber incident response unit

Criteria: *The government has a unit (common name is CERT, CIRC, etc.) that is specialised in national-level cyber incident detection and response. The unit is responsible for 24/7 data gathering of incidents in cyberspace. The authority manages the comprehensive picture of incidents in national cyberspace.*

Situation in the country: ✓ There is such a capacity.

Reference: www.cert.az
http://www.e-qanun.az/framework/25375

9.2 Cyber incidents reporting responsibility

Criteria: *Public sector entities and CII operators have the responsibility to report about cyber incidents.*

Situation in the country: ⊗ No such capacity.

9.3 Official format for practical public-private cooperation

Criteria: *There is an official cooperation format (organisation, association, etc.) for operational (practical) public, private and third sector cooperation. Activities are specified in the legislation, agreement or in another official format.*

Situation in the country: ⊗ No such capacity.

9.4 Exchange of classified information

Criteria: *According to legislation, public, private and third sector entities may exchange classified information.*

Situation in the country: ⊗ No such capacity.

10. Capacity to manage large-scale cyber crises

10.1 Cyber crisis management plan

Criteria: *The government has established a comprehensive crisis management plan for large-scale cyber incidents. The plan and its different components must be established by legislation.*

Situation in the country: ⊗ No such capacity.

10.2 Cyber security/crisis operations centre

Criteria: *The government has established a permanent national-level cyber security/crisis operations centre. The centre acts as the cyber situation centre and operations staff for the crisis manager.*

Situation in the country: ⊗ No such capacity.

10.3 Crisis management exercise with cyber component

Criteria: *The government has conducted a crisis management exercise with a cyber component in the last 3 years.*

Situation in the country: ⊗ No such capacity.

10.4 National-level cyber crisis management exercise

Criteria: *The government has conducted the national-level cyber crisis management exercise in the last 3 years. The main focus of the exercise is the management of large-scale cyber incidents.*

Situation in the country: ⊗ No such capacity.

10.5 Participation in international cyber crisis exercises

Criteria: *The country has participated in an international cyber crisis management exercise in the last 3 years.*

Situation in the country: ⊗ No such capacity.

10.6 Using volunteers in cyber crisis management

Criteria: *The government has established a system for using volunteers in large-scale cyber crisis management. The procedures for using volunteers must be established by legislation.*

Situation in the country: ⊗ No such capacity.

11. Capacity to fight cyber crimes

11.1 Cyber crimes are criminalised

Criteria: *The state has defined cybercrimes and established them by legislation. The regulations are in line with the Council of the Europe Convention on Cybercrime. Law enforcement authorities are obliged to start a criminal investigation if there are sufficient grounds for a criminal offence.*

Situation in the country: ⊗ No such capacity.

11.2 Unit for fighting cyber crime (department, agency, etc.)

Criteria: *The government has the capacity to conduct criminal proceedings for cybercrimes. A government entity has a department or an organisation that is specialised in combating cybercrime. The unit has competence in the following areas: 1) Prevention of cybercrime. 2) Conducting surveillance measures or special investigation techniques. 3) Conducting pre-trial investigations. The role and responsibilities of the units must be established by legislation.*

Situation in the country: ⊗ No such capacity.

11.3 Unit for digital forensics (department, agency, etc.)

Criteria: *A government entity has a department or an organisation that is specialised in digital forensics:*

- *computer forensics*
- *mobile forensics*
- *hardware forensics, i.e. skimmers*
- *software forensics, malware analysis*

The role and responsibilities of the units must be established by legislation.

Situation in the country: ⊗ No such capacity.

11.4 Electronic evidences are regulated

Criteria: *National regulations provide for rules on the collection and use of electronic evidence. General rules on evidence collection and use alike that also cover electronic evidence or a specific regulation on electronic evidence have been accepted.*

Situation in the country: ⊗ No such capacity.

11.5 International cyber crimes 24/7 contact point

Criteria: *There is an international contact point for cyber crimes, which operates 24/7.*

Situation in the country: ✓ There is such a capacity.

Reference: https://rm.coe.int/16804b3493

12. Capacity to conduct military cyber defence operations

12.1 Cyber operation planning unit (department, command, etc.)

Criteria: *Military forces have a department or an organisation that is specialised in cyber operation planning. This unit could be part of a general operation planning unit.*

Situation in the country: ⊗ No such capacity.

12.2 Cyber operation units

Criteria: *Military forces have a unit that is specialised in cyber operations.*

Situation in the country: ⊗ No such capacity.

12.3 Exercise with a cyber operations component

Criteria: *Military forces have conducted an exercise with a cyber operations component in the last 3 years.*

Situation in the country: ⊗ No such capacity.

12.4 Cyber operation exercise in the last 3 years

Criteria: *Military forces have conducted a cyber operation exercise in the last 3 years.*

Situation in the country: ⊗ No such capacity.

12.5 Participation in international cyber exercise in the last 3 years

Criteria: *The country's military team has participated in an international cyber operation exercise in the last 3 years.*

Situation in the country: ⊗ No such capacity.

Belarus

I GENERAL CYBER SECURITY INDICATORS

1. Capacity to develop national cyber security policies

1.1 National-level cyber security policy unit (department, etc.)

Criteria: *A central government entity has a national level department or organisation that is specialised in national cyber security policy development. Work outcomes of this unit are for example the official national cyber security strategy and implementation plan.*

Situation in the country: ⊗ No such capacity.

1.2 National-level cyber security coordination format (committee, etc.)

Criteria: *The central government has established the national-level cyber security coordination format (committee, council, working group, etc.) for cyber security policy coordination. This format includes relevant public, private and third sector entities.*

Situation in the country: ✓ There is such a capacity.

Reference: http://www.newsby.org/documents/ukazp/2012/ukase-by1/ukaz2012-belarus-0258.htm

Comment: Statute on the Council for the Development of the Information Society Under the President of the Republic of Belarus. Chapter 2. Point 5. One of the main functions of the council is to define measures to strengthen information security.

1.3 National-level cyber security terms and definitions

Criteria: *The central government has established national-level cyber security terms and definitions by legislation.*

Situation in the country: ✗ No such capacity.

1.4 National-level cyber security strategy (valid)

Criteria: *The central government has established the national-level cyber security strategy or other equivalent document.*

Situation in the country: ✗ No such capacity.

Comment: There is no specific strategy for cyber / information security. The Strategy of Digitalisation contains elements on cyber security strategy (chapter 3.8), but some main elements are missing.

1.5 National-level cyber security implementation plan (valid)

Criteria: *The central government has established the national-level cyber security implementation plan or another equivalent document.*

Situation in the country: ✗ No such capacity.

2. Capacity to analyse national-level cyber threats

2.1 National-level cyber threat analysis unit (department, etc.)

Criteria: *A central government entity has a national level department or organisation that is specialised in national cyber threat analysis. The work outcomes of this unit are regular comprehensive cyber threat analysis and risk assessments. These risk assessments are the basis for national-level cyber security planning (national cyber security strategy development, etc.).*

Situation in the country: ✓ There is such a capacity.

Reference: https://cert.by/?page_id=24&lang=en

Comment: The National Computer Emergency Response Team (CERT) is responsible for cyber threat analysis.

2.2 Annual public cyber threat reports are published

Criteria: *The public part of the national cyber threat analysis is published at least once a year. The aim of this report is to inform and educate the general public.*

Situation in the country: ⊗ No such capacity.

Reference: http://mvd.gov.by/ru/main.aspx?guid=3311

Comment: Statistics about cybercrimes is published by the Ministry for Internal Affairs of the Republic of Belarus.

3. Capacity to provide cyber security education

3.1 Cyber safety website for the general public

Criteria: *Public authorities provide or finance at least one cyber safety website for the general public. The website provides up-to-date information about cyber threats and security measures related to ICT systems, as well as other useful materials and guidance for regular users. The website should inform about timely threats and security measures related to ICT systems (computers, mobile devices, information systems, e-services, etc.). Websites that inform only about social media threats (cyber bullying, etc.) are not alone accepted. These websites could be added as additional materials.*

Situation in the country: ⊗ No such capacity.

3.2 Nationwide public awareness-raising activity in the last 3 years

Criteria: *Public authorities have organised at least one public awareness-raising activity in the last 3 years. The media campaign should be nationwide (TV, radio, newspapers, etc.).*

Situation in the country: ⊗ No such capacity.

3.3 Cyber safety competencies in primary education

Criteria: *Primary education (ISCED 2011 Level 1) curricula include cyber safety / computer safety competences.*

Situation in the country: ✗ No such capacity.

3.4 Cyber safety competencies in secondary education

Criteria: *Secondary education (ISCED 2011 Level 2-4) curricula include cyber safety / computer safety competences.*

Situation in the country: ✓ There is such a capacity.

Reference: http://www.adu.by/images/2016/07/up-OBG-2-5kl-rus.pdf
http://www.adu.by/wp-content/uploads/2014/umodos/ypyp/Informatika_rus.pdf

Comment: The Curriculum on the subject "Fundamentals of Life Safety" developed by the Ministry of Education (obligatory for institutions of general secondary education) for V classes (2016) includes the following components: "Internet addiction. The harm of excessive use of the Internet, its impact on human health. Possible dangers of social networks, Internet addiction. Safety of work on the Internet. Fraud on the Internet, advertising and spam. The danger of deception in social networks. Inadmissibility of using the Internet for threats or deliberately false messages about the danger." According to the typical plan of secondary education, from the VI class (11-13 years old), the discipline "Informatics" becomes obligatory. Its Curriculum includes the following components: "Security on the Internet; Malicious software and information security".

3.5 Cyber safety competencies in vocational education

Criteria: *Vocational education (ISCED 2011 Level 3-4) curricula include cyber safety / computer safety components.*

Situation in the country: ✓ There is such a capacity.

Reference: http://itiubsu.by/perepodgotovka/matematicheskoe-obespechenie-komp-yuternoj-bezopasnosti/

Comment: The Institute for Professional Development of Information Technologies and Management at the Belarusian State University hosts a vocational training programme on Computer Security Software providing the qualification "information protection expert".

3.6 Bachelor's level cyber security programme (at least 1)

Criteria: *There is at least one cyber security / electronic information security focused programme on the bachelor's or equivalent level (ISCED 2011 Level 6).*

Situation in the country: ✓ There is such a capacity.

Reference: http://rfe.bsu.by/info/spec/kb
https://abitur.bsuir.by/spetsialnosti-bguir

Comment: Belarusian State University hosts a bachelor's-level programme "Computer security" embracing the following specialisations: "Complex provision of information security of telecommunications and information systems"; "Software and hardware and information security systems"; "Intellectual technologies of information systems protection"; "Modelling and analysis of information systems".
Belarusian State University for Informatics and Radioelectronics hosts several related programmes: "Electronic Security Systems", "Information systems and technologies (in ensuring industrial safety)", "Electronic information protection", "Protection of information in telecommunications".

3.7 Master's level cyber security programme (at least 1)

Criteria: *There is at least one cyber security / electronic information security focused programme on the master's or equivalent level (ISCED 2011 Level 7)*

Situation in the country: ✓ There is such a capacity.

Reference: https://www.bsu.by/ru/main.aspx?guid=4661
https://www.bsuir.by/ru/kaf-informatsion-radiotekh/magistratura

Comment: Belarusian State University hosts a master's-level programme "1-98 80 02 – Mathematical and Information Security Software". The same programme is hosted by Polotsk State University.
Belarusian State University for Informatics and Radio-electronics hosts a master's-level programme 1-98 80 03 "Hardware and software and hardware for information security".

3.8 PhD level cyber security programme (at least 1)

Criteria: *There is at least one cyber security / electronic information security focused programme on the PhD or equivalent level (ISCED 2011 Level 8).*

Situation in the country:	✓ There is such a capacity.
Reference:	http://www.vak.org.by/resolution-of-the-higher-attestation-commission-4 http://www.vak.org.by/szd/tech http://www.vak.org.by/node/231
Comment:	The PhD programmes "Methods and systems of information protection" and "Information security" are officially acknowledged by the High Attestation Committee. The passport of the programme is published. The PhD courses are suggested by Belarusian State University and Belarusian State University for Informatics and Radio-electronics and acknowledged by the High Attestation Committee.

3.9 Cyber security professional association

Criteria:	*There is a professional association of cyber/information security specialists, managers or auditors.*
Situation in the country:	⊗ No such capacity.

4. Capacity to provide international cyber security

4.1 International cyber security cooperation unit (department, etc.)

Criteria:	*The ministry responsible for foreign affairs has a department or an organisation that is specialised in international cyber security.*
Situation in the country:	⊗ No such capacity.

4.2 Implementation of the Convention on Cybercrime

Criteria:	*The government has enforced the Convention on Cybercrime of the Council of Europe. The government has ratified or acceded to the convention. The convention is fully implemented.*
Situation in the country:	⊗ No such capacity.

4.3 Cooperation agreements with other countries (at least 1 country)

Criteria:	*The government has bilateral, regional, international cyber security cooperation agreements with other countries or international organisations. One other agreement is sufficient that is not the Convention on Cybercrime of the Council of Europe.*

Situation in the country:	✓ There is such a capacity.
Reference:	http://base.spinform.ru/show_doc.fwx?rgn=66894 http://www.pravo.by/upload/docs/op/A01300055_1421096400.pdf
Comment:	Cooperation of the Member States of the Commonwealth of Independent States in the Sphere of Ensuring Information Security (approved by the Decision of the Council of Heads of State of the CIS of October 10, 2008). Agreement between the Government of the Republic of Belarus and the Government of the Russian Federation on Cooperation in the Field of International Information Security.

4.4 Representation in international cooperation formats (at least 1)

Criteria:	*The government is represented regularly in a cooperation format that deals with international cyber security.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://www.cisatc.org/137/143
Comment:	Antiterrorist centre of the member states of the Commonwealth of Independent States that is also specialised in countering cyber-attacks was created by the Decision of the Council of CIS Heads of State of June 21, 2000, is a permanent specialised branch body of the CIS and is intended to ensure coordination of interaction between the competent bodies of the CIS member states in the field of combating international terrorism and other manifestations of extremism.

4.5 International cyber security organisation in the country

Criteria:	*A regional or international cyber security organisation with regional or international functions is located in the country.*
Situation in the country:	✗ No such capacity.

4.6 Cyber security capacity-building

Criteria:	*The country has (co)financed or (co)organised at least one capacity-building project for another country in the last 3 years.*
Situation in the country:	✗ No such capacity.

II. BASELINE CYBER SECURITY INDICATORS

5. Capacity to ensure baseline cyber security

5.1 Baseline cyber security management unit (agency, etc.)

Criteria: *A central government entity has a department or organisation that is specialised in national-level baseline cyber security management – development, implementation, coordination and supervision.*

Situation in the country: ✓ There is such a capacity.

Reference: http://oac.gov.by/files/files/pravo/prikazi_oac/Prikaz_OAC_62.htm
http://oac.gov.by/files/files/pravo/ukazi/Ukaz98-16.htm

Comment: Operational and Analytical Centre under the President of the Republic of Belarus (OAC) is a single regulator in the area of technical and cryptographic information in Belarus. OAC carries out the state regulation and control in the field of technical and cryptographic protection of information.

5.2 Personal data protection authority (independent organisation)

Criteria: *There is an independent public supervisory authority that is responsible for personal data protection.*

Situation in the country: ✗ No such capacity.

Comment: There is no distinct authority responsible for personal data protection. Belarus has not joined the EU Data Protection Convention yet. The Law on Personal Data Protection is in the process of development.

5.3 Legislation for information classification (public, confidential, etc.)

Criteria: *There is legislation for information classification – public, private, classified, restricted, confidential, critical, etc.*

Situation in the country: ✓ There is such a capacity.

Reference: http://www.pravo.by/document/?guid=3871&p0=h10800455

Comment: The Law of the Republic of Belarus dated 10 November 2008 No. 455-3 “On information, digitalisation and protection of information” stipulates that “Legal regulation of information relations is carried out on the basis of protection of information on personal life of a natural person and personal data". The Law defines the types of information, access to which, distribution and (or) provision of which is not limited (restricted) (Public information) (Art 16), the types of information, distribution and (or) provision of which is limited (Art 17); the information on the private life of an individual and personal data (Art 18); the official information of limited distribution (Art 18-1); the measures on protection of personal data (Art 32); the rights and obligations of the information user (Art 34).

5.4 Information / cyber security management standard

Criteria: *There is a baseline regulation or an adopted standard for information/cyber security management for public sector entities. The regulation or standard is mandatory for public sector entities.*

Situation in the country: ⊗ No such capacity.

5.5 Accreditation of public sector ICT solutions before introduction

Criteria: *Before the introduction of an ICT solution (information system, public e-service, etc.) in the public sector, an official security accreditation/audit takes place.*

Situation in the country: ✓ There is such a capacity.

Reference:
http://oac.gov.by/files/files/pravo/ukazi/Ukaz_196.htm
http://www.government.by/ru/solutions/2030
http://oac.gov.by/files/files/pravo/prikazi_oac/Prikaz_OAC_86.htm
http://oac.gov.by/files/files/pravo/prikazi_oac/Prikaz_OAC_3.htm

Comment: Decree of the President of Belarus of 16 April 2013 г. No. 196 "On some measures of information protection improvement": "19. Means of cryptographic protection of information used in the information protection systems, information systems for processing of information of limited distribution and (or) access not referred to state secrets, and critical information infrastructure objects, are subject to certification in the National System of Conformity Confirmation of the Republic Belarus for compliance with the technical regulations or state expertise."

Regulations on the procedure of technical protection of information in information systems designed for processing, distribution and (or) provision of data not classified as state secrets are approved by Order of OAC of 30.08.2013 No. 62, the requirements are set for the design of the system of information security, its creation, the specifics of operation of such a system are explained.

5.6 Regular audits of public sector ICT solutions

Criteria: *The operators of public sector ICT solutions (information systems, e-services, etc.) have to order regular independent ICT security audits.*

Situation in the country: ✓ There is such a capacity.

Reference: http://oac.gov.by/files/files/pravo/prikazi_oac/Prikaz_OAC_42.htm

http://oac.gov.by/files/files/pravo/ukazi/Ukaz_196.htm

Comment: Art. 3, 4. Regular audit is prescribed by the Decree of the President of Belarus of 16 April 2013 No. 196 “On some measures of information protection improvement”, which approves the Regulation on technical and cryptographic protection of information in Belarus, relevant to:

- objects of information intended for processing of information comprising state secrets;
- information systems for processing of information, which distribution and (or) access to is limited but not referred to state secrets;
- critical information infrastructure objects (CII).

The procedure and benchmarks are prescribed by Order of the Operations and Analysis Centre under the President of the Republic of Belarus No. 42 dated 30 April 2012 “On Approval of the Instruction for the Procedure of the External Control of Critically Important Information Facilities”

6. Capacity to provide a secure environment for e-services

6.1 Secure data exchange environment for e-services

Criteria: *There is a secure inter-organisational data exchange environment in the country (secure internet), which enables public sector entities to provide secure web services for citizens and entrepreneurs. Private sector and other entities will be interfaces with the environment, if they provide a public service or participate in it.*

Situation in the country: ✓ There is such a capacity.

Reference: http://portal.gov.by/
http://bit.ly/2ymXvhy

Comment: National automated information system (portal for e-services).

6.2 Up-to-date cryptographic solution for the environment

Criteria: *In the data exchange environment, the cryptographic requirement complies with recognised up-to-date guidelines (NIST Special Publication 800-78-3, ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012), etc.)*

Situation in the country: ✓ There is such a capacity.

Reference: http://oac.gov.by/files/files/pravo/prikazi_oac/Prikaz_OAC_33_2013.htm
https://nces.by/wp-content/uploads/2017/02/%D0%95%D0%A2%D0%A2-%D0%A1%D0%9C%D0%94%D0%9E.pdf
http://oac.gov.by/files/files/pravo/prikazi_oac/118-2015.htm

Comment: The Order of the Operational and Analytical Centre under the President of the Republic of Belarus of May 27, 2013 No. 33 “On approval of the Instruction on the procedure for interaction of departmental electronic document management systems with the system of interdepartmental electronic document circulation of state bodies” determines the requirements for interdepartmental and inter-system electronic compatibility (interoperability). It ensures compatibility of newly developed state information systems used by the government control agencies for interdepartmental services.
The procedure of connection to IDMS posted on the official website of IDMS operator includes a necessary step “2. To acquire means of electronic digital signature. To work in the IDMS system, the user should acquire the means of electronic digital signature in the state certification centre GosSUOC” (Art. 7 of the “Uniform technical requirements for organisation of access of departmental systems of electronic document flow to IDMS”, established by the National Centre for Electronic Services on 24.02.2017.) See indicator 6.4. for details of the SPKMS (GosSUOK) system organisation.

7. Capacity to provide e-identification and e-signatures

7.1 Citizens and legal entities have a unique identifier

Criteria: *All citizens, residents and legal entities are identifiable via a persistent unique identifier. The identifier is used on public sector registries. It is not a number of the personal identification document, but a unique number assigned to a person for life.*

Situation in the country: ✓ There is such a capacity.

Reference: http://mvd.gov.by/imgmvd/dgim/418.pdf

Comment: Article 9. Identification number. All citizens of the Republic of Belarus as well as other categories of physical entities registered in the State Population Register also have the unique identification number that is assigned to a person for a lifetime. Since 2013, this also concerns the children since they obtain a certificate of birth. Decision of the Ministry of Internal Affairs of the Republic of Belarus October 18, 2011 No. 345» establishes the order of formation of the "Identification number, which is the main identifying characteristic of an individual in the process of entering his personal data into information systems, updating, excluding, storing, restoring, providing and using them". For legal entities, the payer's account number (УНП/PAN) assigned to them at registration of the legal entity is used as a unique identifier.

7.2 Public e-services identify users via a unique identifier.

Criteria: *The public-sector e-services use the identifier for identification; there is no need for additional queries. There is a legal framework for electronic identification and authentication. The framework is based on the unique identifier.*

Situation in the country: ✓ There is such a capacity.

Reference: http://mvd.gov.by/imgmvd/dgim/345.pdf
https://nces.by/wp-content/uploads/2016/03/Formats.pdf

Comment: Comment: Art. 1. The digital signature certificate field – Subject: serial number. The portal for e-government services is operating on the basis of the National Automated Information System (NAIS). NAIS provides e-services for physical persons and legal entities. Identification and authorisation are possible via:

- Email registration with obligatory indication of personal passport data including personal identification number, family name and name, passport data and date of birth (for physical persons);
- Authorisation with electronic digital signature issued by the republican certification centre of the GosSUOK system (see indicator 6.4) (for both legal entities and physical person possessing such EDS);
- Authorisation with electronic digital signature issued by the certification centre of MailGov (for public authorities delivering e-services).

7.3 Public e-services use 2-factor authentication

Criteria: *Public sector e-services use 2-factor authentication and strong cryptographic solutions in national electronic authentication. The cryptographic solution has to comply with NIST Special Publication 800-78-3, ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012), etc.*

Situation in the country: ✓ There is such a capacity.

Reference: https://portal.gov.by/

Comment: Public sector e-services use 2-factor authentication and strong cryptographic solutions in the national electronic authentication (obligatory for all legal entities and voluntary for physical persons). 2-factor authentication is accomplished through electronic digital signature (stored at physical carrier (USB-disk) + knowledge-based verification (personal password for which this key was created) (see login page).

For physical persons not possessing the electronic digital signature (currently most of them) the actual practice of electronic identification of person currently includes the use in information systems of several stages of passwords; distribution of text notification by each operation performed using the payment card (optional, paid service); the 3D-secure technology (identification of the account owner by entering of the code sent automatically to the mobile phone number registered for this user). This can be considered the 2-factor authentication as well as it combines the ownership of the physical carrier (mobile phone) and knowledge of login and password.

The country has technical standards (cryptographic protocols) for user authentication that were developed on the basis of international standards and supplemented with regard to encryption.

7.4 A legal framework for electronic signature

Criteria: *A legal framework for electronic signature is established in the country. The electronic signature system is based on the aforementioned unique identifier. There are requirements for trust services required for electronic signature. These requirements are established by legislation.*

Situation in the country: ✓ There is such a capacity.

Reference: http://oac.gov.by/files/files/pravo/zakoni/Zakon_113z.htm

Comment: A legal framework for electronic signature is established for the country by the Law of the Republic of Belarus of December 28, 2009 No. 113-Z "On electronic document and digital signature".

7.5 Supervision over qualified trust services providers

Criteria: *There is an authority that is responsible for the supervision of qualified trust service providers and for granting the qualified status.*

Situation in the country: ✓ There is such a capacity.

Reference: http://oac.gov.by/files/files/pravo/prikazi_oac/Prikaz_OAC_89.htm

Comment: Operations and Analysis Centre under the President of the Republic of Belarus is responsible for the supervision of qualified trust service providers and for granting the qualified status. The procedure for the accreditation of service providers in GosSUOC and for monitoring compliance with accreditation conditions is determined by the "Instruction on the procedure for accreditation of service providers in the State system for managing public keys for checking the electronic digital signature of the Republic of Belarus and for monitoring compliance with accreditation conditions" approved by the OAC Order of November 29 2013 No. 89

7.6 A qualified electronic signature has legal effect

Criteria: *A qualified electronic signature has the equivalent legal effect of a handwritten signature.*

Situation in the country: ✓ There is such a capacity.

Reference: http://oac.gov.by/files/files/pravo/zakoni/Zakon_113z.htm

Comment: The Law of the Republic of Belarus of December 28, 2009 No. 113-Z “On electronic document and digital signature”, Article 22. Legal force of electronic document: A genuine electronic document is equated to a document on paper, signed personally, and has the same legal effect.

8. Capacity to protect essential e-services / CII

8.1 The essential e-services / CII are defined

Criteria: *The essential e-services / critical information infrastructure (CII) are defined by legislation.*

Situation in the country: ✓ There is such a capacity.

Reference: http://oac.gov.by/files/files/pravo/ukazi/Ukaz_486.htm
http://oac.gov.by/files/files/pravo/prikazi_oac/Prikaz_OAC_96.htm
http://oac.gov.by/tzi/kvoi/

Comment: Chapter 1 Art. 2. The State Registry of the Critically Important objects of Information Infrastructure.

8.2 National level essential e-services / CII protection unit

Criteria: *A central government entity has a department or organisation that is specialised in essential e-services / critical information infrastructure protection. The unit has the responsibility to develop adequate security measures, and coordinate and supervise the implementation of specific security measures.*

Situation in the country: ✓ There is such a capacity.

Reference: http://oac.gov.by/tzi/kvoi/svedeniya.html

Comment: The Operations and Analysis Centre under the President of the Republic of Belarus is authorised to:

- coordinate the activities of state bodies and other organisations to provide technical protection of information processed on critically important objects of information infrastructure;
- create and maintain the State Register of critically important objects of information infrastructure, as well as provide information from it to authorised state bodies and organisations;

- within its authority – to supervise the activity ensuring the technical protection of information processed on critically important objects of information infrastructure;
- adopt normative legal acts on the assignment of objects to critically important objects of information infrastructure and ensuring their safety;
- realise other powers in the field of operation and maintenance of critically important objects of information infrastructure established by legislative acts.

8.3 Service continuity requirements for essential e-services / CII operators

Criteria: *Data processing and service continuity requirements (downtime elimination time, readiness for disruption, etc.) are established for essential e-services / CII operators by legislation.*

Situation in the country: ✓ There is such a capacity.

Reference: http://oac.gov.by/files/files/kvoi/TKP.pdf

Comment: Art. 6.2. The requirements of Technical codes of practice TKP 483-2013 “Information technology and security. Safe operation and reliable operation of critically important objects of information infrastructure. General requirements” (complies with ISO/IEC 27001) are mandatory for entities engaged in activities related to the creation and operation of critically important objects of information infrastructure. The Technical Code sets requirements for operational reliability and safe operation.

8.4 Essential e-services / CII operators have a cyber security manager

Criteria: *The essential e-services / CII operators have to appoint a cyber/information security manager.*

Situation in the country: ✓ There is such a capacity.

Reference: http://oac.gov.by/files/files/kvoi/TKP.pdf

Comment: Art. 7. General requirements” establishes a set of requirements for the Security Service/Department at the critically important information infrastructure objects.

III. INCIDENT AND CRISIS MANAGEMENT INDICATORS

9. Capacity to detect and respond to cyber incidents 24/7

9.1 National-level cyber incident response unit

Criteria: *The government has a unit (common name is CERT, CIRC, etc.) that is specialised in national-level cyber incident detection and response. The unit is responsible for 24/7 data gathering of incidents in cyberspace. The authority manages the comprehensive picture of incidents in national cyberspace.*

Situation in the country: ✓ There is such a capacity.

Reference: https://cert.by/?page_id=24&lang=en

Comment: CERT.BY is the National Computer Emergency Response Team of the Republic of Belarus, it was launched and is maintained by the Operation and Analytical Centre under the President of Belarus.

CERT.BY carries out accumulation, storage and handling of statistical data related to malware dissemination and network attacks on the territory of the Republic of Belarus, as well as incident response in the informational systems of the state bodies and organisations.

9.2 Cyber incidents reporting responsibility

Criteria: *Public sector entities and CII operators have the responsibility to report about cyber incidents.*

Situation in the country: ✓ There is such a capacity.

Reference: http://oac.gov.by/files/files/kvoi/TKP.pdf

Comment: Technical codes of practice TKP 483-2013 “Information technology and security. Safe operation and reliable operation of critically important objects of information infrastructure. General requirements” set requirements for the operational reliability and safe operation of critically important objects of information infrastructure, including the “procedures for handling security events in the CII and procedures for reporting, responding and recovering from security incidents in the CII.”

9.3 Official format for practical public-private cooperation

Criteria:	*There is an official cooperation format (organisation, association, etc.) for operational (practical) public, private and third sector cooperation. Activities are specified in the legislation, agreement or in another official format.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://infopark.by/node/5122
Comment:	The Committee for Information Security was established in 2013 under the auspice of the Infopark Scientific and Technological Association in a format of public-private cooperation. Its activities, among others, include: • Development of cooperation with public authorities on effective implementation of information security and information protection systems in the organisations of the Republic of Belarus; • Development of cooperation with associations, unions, associations of information technology users working in information security and information protection.

9.4 Exchange of classified information

Criteria:	*According to legislation, public, private and third sector entities may exchange classified information.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://www.kgb.by/ru/zakon170-3/
Comment:	The Law of the Republic of Belarus “On State Secrets” of 19 July 2010 N 170-3 regulates the exchange of information treated as state secrets with legal and physical entities.

10. Capacity to manage large-scale cyber crises

10.1 Cyber crisis management plan

Criteria:	*The government has established a comprehensive crisis management plan for large-scale cyber incidents. The plan and its different components must be established by legislation.*
Situation in the country:	✕ No such capacity.

10.2 Cyber security/crisis operations centre

Criteria: *The government has established a permanent national-level cyber security/crisis operations centre. The centre acts as the cyber situation centre and operations staff for the crisis manager.*

Situation in the country: ⊗ No such capacity.

10.3 Crisis management exercise with cyber component

Criteria: *The government has conducted a crisis management exercise with a cyber component in the last 3 years.*

Situation in the country: ⊗ No such capacity.

10.4 National-level cyber crisis management exercise

Criteria: *The government has conducted the national-level cyber crisis management exercise in the last 3 years. The main focus of the exercise is the management of large-scale cyber incidents.*

Situation in the country: ⊗ No such capacity.

10.5 Participation in international cyber crisis exercises

Criteria: *The country has participated in an international cyber crisis management exercise in the last 3 years.*

Situation in the country: ✓ There is such a capacity.

Reference: http://www.cis.minsk.by/news.php?id=6396

Comment: A joint anti-terrorist exercise of states-participants of the Commonwealth of Independent States "Cyber-Anti-terror-2016" (including Belarus, Armenia, Kyrgyzstan, Kazakhstan and Russia) was held in 2016 in Novolukoml (Belarus). The legend was that an extremist website had published an appeal to the international terrorist organisation of massive computer DDoS-attacks on the servers of critical infrastructure in Belarus. The security agencies and special services of these countries with the support of the CIS Anti-Terrorist Centre carried out a series of measures to detect and respond to cyber-terrorism activities."

10.6 Using volunteers in cyber crisis management

Criteria: *The government has established a system for using volunteers in large-scale cyber crisis management. The procedures for using volunteers must be established by legislation.*

Situation in the country: ⊗ No such capacity.

11. Capacity to fight cyber crimes

11.1 Cyber crimes are criminalised

Criteria: *The state has defined cybercrimes and established them by legislation. The regulations are in line with the Council of the Europe Convention on Cybercrime. Law enforcement authorities are obliged to start a criminal investigation if there are sufficient grounds for a criminal offence.*

Situation in the country: ✓ There is such a capacity.

Reference: http://www.pravo.by/webnpa/text.asp?RN=HK9900275

Comment: The Criminal Code of Belarus contains a chapter defining the criminal offences and sanctions for attacks against information systems and computer data: Chapter 31. Crimes against information security (Art. 349. Unauthorised access to computer information; Art. 350. Modification of computer information; Art. 351. Computer sabotage; Art. 352. Illegal occupation of computer information; Art. 353. Manufacture or sale of special funds for unauthorised access to a computer system or network; Art. 354. The development, use or distribution of malware; Art. 355. Violation of the rules of operation of a computer system or network.

11.2 Unit for fighting cyber crime (department, agency, etc.)

Criteria: *The government has the capacity to conduct criminal proceedings for cybercrimes. A government entity has a department or an organisation that is specialised in combating cybercrime. The unit has competence in the following areas: 1) Prevention of cybercrime. 2) Conducting surveillance measures or special investigation techniques. 3) Conducting pre-trial investigations. The role and responsibilities of the units must be established by legislation.*

Situation in the country: ✓ There is such a capacity.

Reference: http://mvd.gov.by/main.aspx?guid=1881

Comment: The Office for the Detection of High-Tech Crime at the Ministry of Internal Affairs of the Republic of Belarus (Office "K") is an independent operational and search division of the Ministry, directly subordinate to the Head of the Main Directorate of Criminal Police.

11.3 Unit for digital forensics (department, agency, etc.)

Criteria: *A government entity has a department or an organisation that is specialised in digital forensics:*

- *computer forensics*
- *mobile forensics*
- *hardware forensics, i.e. skimmers*
- *software forensics, malware analysis*

The role and responsibilities of the units must be established by legislation.

Situation in the country: ⊗ No such capacity.

11.4 Electronic evidences are regulated

Criteria: *National regulations provide for rules on the collection and use of electronic evidence. General rules on evidence collection and use alike that also cover electronic evidence or a specific regulation on electronic evidence have been accepted.*

Situation in the country: ⊗ No such capacity.

11.5 International cyber crimes 24/7 contact point

Criteria: *There is an international contact point for cyber crimes, which operates 24/7.*

Situation in the country: ✓ There is such a capacity.

Reference: http://mvd.gov.by/main.aspx?guid=1881
https://www.coe.int/ar_QA/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/belarus

12. Capacity to conduct military cyber defence operations

12.1 Cyber operation planning unit (department, command, etc.)

Criteria: *Military forces have a department or an organisation that is specialised in cyber operation planning. This unit could be part of a general operation planning unit.*

Situation in the country: ⊗ No such capacity.

12.2 Cyber operation units

Criteria:	*Military forces have a unit that is specialised in cyber operations.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://belarmy.by/lenta-novostei/podrazdeleniya-boevyx-xakerov-budut-protivodejstvovat-kiberugrozam
Comment:	Deputy Minister of Defence, Major General has announced that special units to combat cyber threats are created in the Belarusian army.

12.3 Exercise with a cyber operations component

Criteria:	*Military forces have conducted an exercise with a cyber operations component in the last 3 years.*
Situation in the country:	✗ No such capacity.

12.4 Cyber operation exercise in the last 3 years

Criteria:	*Military forces have conducted a cyber operation exercise in the last 3 years.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://www.cis.minsk.by/news.php?id=6396
Comment:	A joint anti-terrorist exercise of states-participants of the Commonwealth of Independent States “Cyber-Antiterror-2016” (including Belarus, Armenia, Kyrgyzstan, Kazakhstan and Russia) was held in 2016 in Novolukoml (Belarus). The legend was that an extremist website had published an appeal to the international terrorist organisation of massive computer DDoS-attacks on the servers of critical infrastructure in Belarus.

12.5 Participation in international cyber exercise in the last 3 years

Criteria:	*The country’s military team has participated in an international cyber operation exercise in the last 3 years.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://www.cis.minsk.by/news.php?id=6396

Comment: A joint anti-terrorist exercise of states-participants of the Commonwealth of Independent States “Cyber-Antiterror-2016” (including Belarus, Armenia, Kyrgyzstan, Kazakhstan and Russia) was held in 2016 in Novolukoml (Belarus). The legend was that an extremist website had published an appeal to the international terrorist organisation of massive computer DDoS-attacks on the servers of critical infrastructure in Belarus.

Georgia

I GENERAL CYBER SECURITY INDICATORS

1. Capacity to develop national cyber security policies

1.1 National-level cyber security policy unit (department, etc.)

Criteria: *A central government entity has a national level department or organisation that is specialised in national cyber security policy development. Work outcomes of this unit are for example the official national cyber security strategy and implementation plan.*

Situation in the country: ✓ There is such a capacity.

Reference: http://www.dea.gov.ge/uploads/National%20Cyber%20Security%20Strategy%20of%20Georgia_ENG.pdf
http://www.dea.gov.ge/?action=page&p_id=156&lang=eng

Comment: Link 1: page 2 – The Cyber Security Strategy has been developed by the Permanent Inter-agency Commission under the auspices of the National Security Council tasked with coordinating drafting national security strategic documents
Link 2: page 67, Art. 3.8.2 b. – Since the beginning of 2011 the Data Exchange Agency (DEA) has been actively participating in the process of developing a national strategy for cyber security in Georgia. The process was going on within the framework of the working group established by the National Security Council.

1.2 National-level cyber security coordination format (committee, etc.)

Criteria: *The central government has established the national-level cyber security coordination format (committee, council, working group, etc.) for cyber security policy coordination. This format includes relevant public, private and third sector entities.*

Situation in the country: ✓ There is such a capacity.

Reference:
http://www.sscmc.gov.ge/en
https://nsc.gov.ge/eng
https://matsne.gov.ge/ka/document/view/2764463

Comment: Office of State Security and Crisis Management Council constitutes the national-level cyber security coordination format. National Security Concept of Georgia and Law of Georgia on “National Security Policy Planning and Coordination” stipulate cyber security as a part of National Security. The process of planning the national security policy are coordinated by the National Security Council and the State Security and Crisis Management Council. The council is an advisory board for the Prime Minister of Georgia and is directly subordinated to him. Accordingly, the Prime Minister is the head of the Council. The council is composed of the following permanent members: Secretary of the Council, Minister of Internal Affairs, Minister of Defence, Minister of Foreign Affairs and Minister of Finance.
Link 3: Law of Georgia on “National Security Policy Planning and Coordination”, Art. 19

1.3 National-level cyber security terms and definitions

Criteria: *The central government has established national-level cyber security terms and definitions by legislation.*

Situation in the country: ✓ There is such a capacity.

Reference:
https://matsne.gov.ge/en/document/view/1679424
http://www.dea.gov.ge/?action=page&p_id=156&lang=eng

Comment: State-wide cyber security terms are defined by the Information Security Act of Georgia adopted by Parliament in 2012. Definitions of terms like cyber incident, cyberattack, cyber space, critical information system subject, computer emergency response team, information security, cyber security specialists. The scope of this law covers all legal persons and state authorities that are critical information system subjects. This law shall also apply to the organisations and agencies that are subordinated or related to the critical information system subject through labour, internship, contractual, or other relationships and that provide access to information assets under such relationships. This is the principle legal document on information and cyber security having national level application.

Cybersecurity Terms and Definitions are additionally enshrined in national policy and strategy documents, like the National Security Concept of Georgia, E-Georgia strategy, Cybersecurity Strategy of Georgia

1.4 National-level cyber security strategy (valid)

Criteria: *The central government has established the national-level cyber security strategy or other equivalent document.*

Situation in the country: ✓ There is such a capacity.

Reference: http://gov.ge/files/469_59439_212523_14.pdf

Comment: National Cyber Security Strategy for the years 2017-2018 has been approved by the Government of Georgia. The main directions of state cyber security policy are:

Research and analysis; Development and improvement of legal basis; Capacity-building in cyber security sphere; Awareness-raising of society and development of educational basis; International cooperation.

The National Cyber Security Strategy of Georgia is a core document in the sphere of cyber policy of the state, which defines strategic goals, essential principles, forms objectives and determines activities that have to be accomplished in order to ensure safe cyber space for Georgia.

1.5 National-level cyber security implementation plan (valid)

Criteria: *The central government has established the national-level cyber security implementation plan or another equivalent document.*

Situation in the country: ✓ There is such a capacity.

Reference: http://gov.ge/files/469_59439_212523_14.pdf

Comment: Action Plan of the National Cyber Security Strategy for the years 2017-2018 has been approved by the Government of Georgia. The Action Plan includes activities, a timeframe, responsible and supporting agencies, source of funding and performance indicators for the implementation of the National Cyber Security Strategy.

According to the Action Plan, Georgia will continue to study the best practices of developed countries, and initiate new legislative acts and bylaws to ensure information security. Additionally, Georgia will deepen institutional coordination, initiate public awareness activities and educational programs in the cyber security field. Further training of staff and technical personnel to make them familiar with international standards of information security will be high on the agenda. The state will deepen cooperation with international organisations, actively participate in international activities, conferences, seminars, workshops, and support educational initiatives on a regional basis, as well as initiate bilateral and multilateral cooperation with international organisations working in the cybersecurity field.

2. Capacity to analyse national-level cyber threats

2.1 National-level cyber threat analysis unit (department, etc.)

Criteria: *A central government entity has a national level department or organisation that is specialised in national cyber threat analysis. The work outcomes of this unit are regular comprehensive cyber threat analysis and risk assessments. These risk assessments are the basis for national-level cyber security planning (national cyber security strategy development, etc.).*

Situation in the country: ✓ There is such a capacity.

Reference: https://matsne.gov.ge/en/document/view/1679424

Comment: Law of Georgia on Information Security, Art. 8.

The State Security and Crisis Management Council performs the functions of the national-level Cyber Threat Analysis Unit. Relevant functions of the State Security and Crisis Management Council are provided by law as follows: “The council identifies and assesses internal and external threats and develops appropriate measures to prevent those threats.” In addition to that, according to the law on the Establishment of a “Legal Entity of Public Law under the Ministry of Justice of Georgia – Data Exchange Agency”, one of the main functions of the DEA is the identification of risks related to information security. CERT.GOV.GE – the national and government Computer Emergency Response Team within the DEA is responsible for management and analysis of cyber incidents against information security in the cyberspace of Georgia.

2.2 Annual public cyber threat reports are published

Criteria: *The public part of the national cyber threat analysis is published at least once a year. The aim of this report is to inform and educate the general public.*

Situation in the country: ✓ There is such a capacity.

Reference: http://bit.ly/2hfjIds

Comment: The Data Exchange Agency annually from 2012 publishes its activity reports, which contain information about identified cyber incidents, numbers and categories, vectors and targets of threats and implemented measures to combat them. The DEA annual Report of 2015 is provided as a reference (in Georgian).

3. Capacity to provide cyber security education

3.1 Cyber safety website for the general public

Criteria: *Public authorities provide or finance at least one cyber safety website for the general public. The website provides up-to-date information about cyber threats and security measures related to ICT systems, as well as other useful materials and guidance for regular users. The website should inform about timely threats and security measures related to ICT systems (computers, mobile devices, information systems, e-services, etc.). Websites that inform only about social media threats (cyber bullying, etc.) are not alone accepted. These websites could be added as additional materials.*

Situation in the country: ✓ There is such a capacity.

Reference: https://www.facebook.com/certgovge

3.2 Nationwide public awareness-raising activity in the last 3 years

Criteria: *Public authorities have organised at least one public awareness-raising activity in the last 3 years. The media campaign should be nationwide (TV, radio, newspapers, etc.).*

Situation in the country: ✓ There is such a capacity.

Reference: https://www.youtube.com/user/DataExchangeAgency

Comment: There have been two TV campaigns running from October till December, 2014 and from May till June, 2015. The first campaign included 5 short TV series aired on the 1st and 2nd channels of the Georgian Public Broadcaster. The second campaign featured 4 short TV series aired on nationwide commercial TV stations (Rustavi 2, Imedi, Maestro). Video materials used in both campaigns are available on the DEA's YouTube channel

3.3 Cyber safety competencies in primary education

Criteria: *Primary education (ISCED 2011 Level 1) curricula include cyber safety / computer safety competences.*

Situation in the country: ⊗ No such capacity.

3.4 Cyber safety competencies in secondary education

Criteria: *Secondary education (ISCED 2011 Level 2-4) curricula include cyber safety / computer safety competences.*

Situation in the country: ⊗ No such capacity.

3.5 Cyber safety competencies in vocational education

Criteria: *Vocational education (ISCED 2011 Level 3-4) curricula include cyber safety / computer safety components.*

Situation in the country: ⊗ No such capacity.

3.6 Bachelor's level cyber security programme (at least 1)

Criteria: *There is at least one cyber security / electronic information security focused programme on the bachelor's or equivalent level (ISCED 2011 Level 6).*

Situation in the country: ⊗ No such capacity.

3.7 Master's level cyber security programme (at least 1)

Criteria: *There is at least one cyber security / electronic information security focused programme on the master's or equivalent level (ISCED 2011 Level 7)*

Situation in the country: ⊗ No such capacity.

3.8 PhD level cyber security programme (at least 1)

Criteria: *There is at least one cyber security / electronic information security focused programme on the PhD or equivalent level (ISCED 2011 Level 8).*

Situation in the country: ⊗ No such capacity.

3.9 Cyber security professional association

Criteria: *There is a professional association of cyber/information security specialists, managers or auditors.*

Situation in the country: ⊗ No such capacity.

4. Capacity to provide international cyber security

4.1 International cyber security cooperation unit (department, etc.)

Criteria: *The ministry responsible for foreign affairs has a department or an organisation that is specialised in international cyber security.*

Situation in the country: ⊗ No such capacity.

4.2 Implementation of the Convention on Cybercrime

Criteria: *The government has enforced the Convention on Cybercrime of the Council of Europe. The government has ratified or acceded to the convention. The convention is fully implemented.*

Situation in the country: ✓ There is such a capacity.

Reference: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

4.3 Cooperation agreements with other countries (at least 1 country)

Criteria: *The government has bilateral, regional, international cyber security cooperation agreements with other countries or international organisations. One other agreement is sufficient that is not the Convention on Cybercrime of the Council of Europe.*

Situation in the country: ✓ There is such a capacity.

Reference: https://2009-2017.state.gov/r/pa/prs/ps/2016/08/260838.htm

Comment: The Security and Defence Working Group of the U.S.–Georgia Strategic Partnership Commission met on July 20, 2016, in Washington, DC. The Working Group noted the historic events leading up to this meeting, including the signing of the Memorandum on Deepening the Defence and Security Partnership between the United States of America and Georgia.

4.4 Representation in international cooperation formats (at least 1)

Criteria: *The government is represented regularly in a cooperation format that deals with international cyber security.*

Situation in the country: ✓ There is such a capacity.

Reference:
http://guam-organization.org/en/node/1990
https://www.first.org/members/teams/
http://mncdet.wixsite.com/mncdet-nato

Comment: Link 1: GUAM (Georgia, Ukraine, Azerbaijan, Moldova), SELEC (South-East European Law Enforcement Centre)
Link 2: FIRST
Link 3: MN CD E&T – Multinational Cyber Defence Education and Training Programme.

4.5 International cyber security organisation in the country

Criteria: *A regional or international cyber security organisation with regional or international functions is located in the country.*

Situation in the country: ✗ No such capacity.

4.6 Cyber security capacity-building

Criteria: *The country has (co)financed or (co)organised at least one capacity-building project for another country in the last 3 years.*

Situation in the country: ✓ There is such a capacity.

Reference:
http://dea.gov.ge/uploads/NEWSLETTER_January%202014_ENG.pdf
http://www.dea.gov.ge/?web=0&action=news&news_id=106&lang=eng
http://dea.gov.ge/uploads/NEWSLETTER_June2015_ENG.PDF

Comment: 1) Since 2012 the representatives of the DEA have participated as invited experts and trainers and co-organised some international training events in information and cyber security. In 2014, on January 20-21, the training events were held for Moldavian specialists in the field of information and cyber security as well. The training events held by NATO's Program – The Science of Peace and Security.

2) On February 9-10, 2016 DEA representatives were again invited for administrating training sessions. This time training events were held for Azerbaijani specialists of corresponding profiles and the learning objectives included information and cyber security issues, including – Cyber Security Mechanisms, Security of Websites and Portals, Securing Network Monitoring, Cryptography, Discovering, Registration, Analysis, and Prevention of Cyber Incidents, etc.

3) In 2015, DEA held the two regional workshops on Cyber Security. The first regional workshop, within the NATO program "Science for Peace and Security" (SPS), was dedicated to a cybersecurity's improved means identification and providing cyber defence in South Caucasus and Black Sea countries.

The event was organised by the DEA, which brought together more than 50 representatives from 18 countries to participate in the workshop. The workshop was attended by NATO member countries' cyber security experts, even more various international organisations and cyber and information security agencies from Georgia, working in all departments, who discussed the institutional capacity development tools in the cyber defence field, malware programs and cyber threat neutralisation and modern methods and enhancing cooperation in this direction.

As for the second workshop, it was held in October, as an extension of a large-scale workshop, which was held in June. The common use of critical infrastructure cyber security issues was discussed at the meeting, as well as the means of the institutional capacity development issues and the prospects of enhancing cooperation in this direction. The DEA hosted up to 15 representatives from different countries – NATO member countries' cyber security experts, specialists of the region countries and the representatives, working in the direction of cyber security issues in Georgia.

II. BASELINE CYBER SECURITY INDICATORS

5. Capacity to ensure baseline cyber security

5.1 Baseline cyber security management unit (agency, etc.)

Criteria:	*A central government entity has a department or organisation that is specialised in national-level baseline cyber security management – development, implementation, coordination and supervision.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://www.dea.gov.ge/uploads/DEA_Law_ENG.PDF
Comment:	Art. 6 DEA is the main government agency responsible for information and cyber security management (development, implementation, coordination and supervision of information/cyber security initiatives and solutions) in public sector and critical infrastructure.

5.2 Personal data protection authority (independent organisation)

Criteria:	*There is an independent public supervisory authority that is responsible for personal data protection.*
Situation in the country:	✓ There is such a capacity.
Reference:	https://personaldata.ge/en/home
Comment:	The Institute of the Personal Data Protection Inspector was established in 2013 on the basis of the Georgian Law on Personal Data Protection. The Inspector controls and supervises the implementation of personal data protection legislation and legitimacy of personal data processing.

5.3 Legislation for information classification (public, confidential, etc.)

Criteria:	*There is legislation for information classification – public, private, classified, restricted, confidential, critical, etc.*
Situation in the country:	✓ There is such a capacity.
Reference:	https://matsne.gov.ge/en/document/view/1679424 https://matsne.gov.ge/ka/document/view/1561437 https://matsne.gov.ge/en/document/view/2750311 https://matsne.gov.ge/en/document/view/16270

Comment: Personal Data Protection Law
Law on State Secrets
Information Security Act.
General Administrative Code of Georgia (Chapter 3)

5.4 Information / cyber security management standard

Criteria: *There is a baseline regulation or an adopted standard for information/cyber security management for public sector entities. The regulation or standard is mandatory for public sector entities.*

Situation in the country: ⊗ No such capacity.

5.5 Accreditation of public sector ICT solutions before introduction

Criteria: *Before the introduction of an ICT solution (information system, public e-service, etc.) in the public sector, an official security accreditation/audit takes place.*

Situation in the country: ⊗ No such capacity.

5.6 Regular audits of public sector ICT solutions

Criteria: *The operators of public sector ICT solutions (information systems, e-services, etc.) have to order regular independent ICT security audits.*

Situation in the country: ⊗ No such capacity.

6. Capacity to provide a secure environment for e-services

6.1 Secure data exchange environment for e-services

Criteria: *There is a secure inter-organisational data exchange environment in the country (secure internet), which enables public sector entities to provide secure web services for citizens and entrepreneurs. Private sector and other entities will be interfaces with the environment, if they provide a public service or participate in it.*

Situation in the country: ✓ There is such a capacity.

Reference: http://www.dea.gov.ge/?web=2&action=page&p_id=35&lang=eng

Comment: The Georgian Government granted authorisation to the Data Exchange Agency to establish and maintain the Georgian Government Gateway – a security platform for data

exchange between the government and private entities.
G3 – a Georgian Governmental Gateway Data Exchange infrastructure tier that enables e-ID management (registration, authentication and authorisation), security, applications interoperability and e-services integration, using web-based workflow for interconnection of back-office systems, providing a single integrated view of the Government by standardising the process for submitting transactions and documents and providing a single registration and single sign-on experience.

6.2 Up-to-date cryptographic solution for the environment

Criteria: *In the data exchange environment, the cryptographic requirement complies with recognised up-to-date guidelines (NIST Special Publication 800-78-3, ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012), etc.)*

Situation in the country: ⊗ No such capacity.

7. Capacity to provide e-identification and e-signatures

7.1 Citizens and legal entities have a unique identifier

Criteria: *All citizens, residents and legal entities are identifiable via a persistent unique identifier. The identifier is used on public sector registries. It is not a number of the personal identification document, but a unique number assigned to a person for life.*

Situation in the country: ✓ There is such a capacity.

Reference: https://matsne.gov.ge/en/document/download/31504/28/en/pdf
https://matsne.gov.ge/ka/document/view/88696

Comment: Link 1: Art. 1
Link 2: Art. 12
Citizens and businesses alike are uniquely identified in Georgia.
The personal number is a unique identification number of a person that shall not be changed.
The appropriate authority – Public Service Development Agency shall assign a personal identity number to a person during:
a) Birth registration;
b) Acquisition of citizenship of Georgia.
The identification number of a legal person is a unique number assigned to a legal person when being registered

in the business registry, one unique number is assigned to a business entity, used for tax and state registration purposes at the same time. An identification number of a legal person is permanent and shall not be changed. The number of digits in a legal person's identification number is different based on the organisational form of the business (sole entrepreneur physical person or corporate company).

7.2 Public e-services identify users via a unique identifier.

Criteria: *The public-sector e-services use the identifier for identification; there is no need for additional queries. There is a legal framework for electronic identification and authentication. The framework is based on the unique identifier.*

Situation in the country: ✓ There is such a capacity.

Reference: https://matsne.gov.ge/en/document/view/31504

Comment: According to the law on the Procedure for Registering Citizens of Georgia and Aliens Residing in Georgia, for Issuing Identity (Residence) Cards and Passports of a Citizen of Georgia, the personal number is a unique identification number of a person that shall not be changed, except as expressly provided for by the legislation of Georgia" (Article 11).
Article 14 of this law defines the requisites of an electronic ID card and indicates that an e-ID card contain a qualified electronic signature certificate, its respective electronic signature creation data and the activation data protecting the creation data from unauthorised use (par. 41).
Please see the image of a digital certificate as evidence of a unique identification number of natural person contains.
#certificate details:
C=GE
O=Citizen
SERIAL NUMBER= xxxxxxxxxxx (unique identification number)
CN=Name/surname

7.3 Public e-services use 2-factor authentication

Criteria: *Public sector e-services use 2-factor authentication and strong cryptographic solutions in national electronic authentication. The cryptographic solution has to comply with NIST Special Publication 800-78-3, ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012), etc.*

Situation in the country: ✓ There is such a capacity.

Reference: https://matsne.gov.ge/en/document/download/31504/28/en/pdf

Comment: Law on the “Procedure for Registering Citizens of Georgia and Aliens Residing in Georgia, for Issuing Identity (Residence) Cards and Passports of a Citizen of Georgia”, Article 14 defines the “e” characteristics of the ID card and its certificate requirements

Government Decree No. 88 on “Approval of Technical Regulation of Digital Signature Certificates and Certification Authorities Issuing Digital Signature Certificates” Article 3 states that qualified certificates shall comply with ETSI TR 102 437 “Guidance on TS 101 456”.

PKI applet used for cryptographic functions of ID card has algorithm RSA-2048

7.4 A legal framework for electronic signature

Criteria: *A legal framework for electronic signature is established in the country. The electronic signature system is based on the aforementioned unique identifier. There are requirements for trust services required for electronic signature. These requirements are established by legislation.*

Situation in the country: ✓ There is such a capacity.

Reference: https://matsne.gov.ge/ka/document/view/3654557

Comment: Law of Georgia on Electronic Signature and Electronic Documents was enacted on March 14, 2008 and established a legal framework for electronic documents and the use of electronic signatures, but didn’t apply to electronic trust services. A new law on Electronic Document and Electronic Trust Services, which will substitute existing law on e-Signatures, was enacted on April 21, 2017. The new law replaced the old regulation and sets legal grounds for the application of electronic documents and electronic trust services, such as qualified electronic signature and seal, timestamp, qualified preservation service for qualified electronic signatures, etc. The new law fully complies with Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

7.5 Supervision over qualified trust services providers

Criteria: *There is an authority that is responsible for the supervision of qualified trust service providers and for granting the qualified status.*

Situation in the country: ✓ There is such a capacity.

Reference: https://matsne.gov.ge/ka/document/view/3654557

Comment: The law on " Electronic Document and Electronic Trust Services" vests all control and supervision of trust service providers to the DEA. Art. 11.

7.6 A qualified electronic signature has legal effect

Criteria: *A qualified electronic signature has the equivalent legal effect of a handwritten signature.*

Situation in the country: ✓ There is such a capacity.

Reference: https://matsne.gov.ge/ru/document/download/20866/4/en/pdf

Comment: Law on "Electronic Document and Electronic Trust Services" declares that "a qualified electronic signature is perceived as equal to the handwritten signature". Art. 3.

8. Capacity to protect essential e-services / CII

8.1 The essential e-services / CII are defined

Criteria: *The essential e-services / critical information infrastructure (CII) are defined by legislation.*

Situation in the country: ✓ There is such a capacity.

Reference: https://matsne.gov.ge/en/document/view/2333175
https://matsne.gov.ge/en/document/view/2521602

Comment: Link 1: Resolution of Government No. 312 of Georgia on Approval of the list of critical infrastructure system subjects
Link 2: Resolution of Government No. 567 of Georgia on Approval of the list of critical infrastructure system subjects in the sphere of defence

8.2 National level essential e-services / CII protection unit

Criteria: *A central government entity has a department or organisation that is specialised in essential e-services / critical information infrastructure protection. The unit has the responsibility to develop adequate security measures, and coordinate and supervise the implementation of specific security measures.*

Situation in the country: ✓ There is such a capacity.

Reference: http://www.dea.gov.ge/uploads/GISA_ENG_FINAL_2015_ver.pdf

Comment: Chapter II Art. 4
DEA (CERT.GOV.GE, Information Security and policy Division) is a specialised entity authorised for strengthening the cyber security of critical information infrastructure subjects. The unit has the responsibility to develop adequate security measures for CII, and coordinate and supervise the implementation of CII-specific security measures

8.3 Service continuity requirements for essential e-services / CII operators

Criteria: *Data processing and service continuity requirements (downtime elimination time, readiness for disruption, etc.) are established for essential e-services / CII operators by legislation.*

Situation in the country: ✓ There is such a capacity.

Reference: https://matsne.gov.ge/en/document/view/1679424
https://matsne.gov.ge/ka/document/view/1831782
http://cert.gov.ge

Comment: DEA (CERT.GOV.GE, Information Security and Policy Division) is the specialised entity authorised to strengthen the cyber security of critical information infrastructure subjects. The unit has the responsibility to develop adequate security measures for CII, and coordinate and supervise the implementation of CII-specific security measures.

8.4 Essential e-services / CII operators have a cyber security manager

Criteria: *The essential e-services / CII operators have to appoint a cyber/information security manager.*

Situation in the country: ✓ There is such a capacity.

Reference: http://www.dea.gov.ge/uploads/GISA_ENG_FINAL_2015_ver.pdf

Comment: Art. 7
According to the Law on Information Security, the critical information system subject shall be obliged to determine the person(s) or the employee(s) (Information Security Manager) responsible for observing the information security requirements of the critical information system subject.

III. INCIDENT AND CRISIS MANAGEMENT INDICATORS

9. Capacity to detect and respond to cyber incidents 24/7

9.1 National-level cyber incident response unit

Criteria: *The government has a unit (common name is CERT, CIRC, etc.) that is specialised in national-level cyber incident detection and response. The unit is responsible for 24/7 data gathering of incidents in cyberspace. The authority manages the comprehensive picture of incidents in national cyberspace.*

Situation in the country: ✓ There is such a capacity.

Reference: https://matsne.gov.ge/en/document/view/1679424
http://cert.gov.ge/

Comment: Art. 8
Computer Emergency Response Team (CERT Georgia) established in 2011 under the Data Exchange Agency of the Ministry of Justice of Georgia serves as a focal point for identification, prevention and mitigation of cyber incidents in the cyberspace of Georgia.

9.2 Cyber incidents reporting responsibility

Criteria: *Public sector entities and CII operators have the responsibility to report about cyber incidents.*

Situation in the country: ☒ No such capacity.

9.3 Official format for practical public-private cooperation

Criteria: *There is an official cooperation format (organisation, association, etc.) for operational (practical) public, private and third sector cooperation. Activities are specified in the legislation, agreement or in another official format.*

Situation in the country: ✓ There is such a capacity.

Reference:
http://gov.ge/files/469_59439_212523_14.pdf
https://matsne.gov.ge/ka/document/view/1831535
http://www.dea.gov.ge/uploads/Newsletter_ENG/NEWSLETTER_June%202013_ENG.pdf

Comment: Link 1: "Today, Georgia has a successful practice of public-private partnership. This practice has mostly accumulated within the frame of the Georgian Cyber Security Forum where almost every major player operating in the Georgian telecommunications market and all state agencies engaged in cyber security are represented. This format of partnership has enabled both the public and the private sectors to share their views on important issues of cyber security and to promote joint initiatives. Thus, within the scope of the Action Plan of the Strategy, the Cyber Security Forum is planned to institutionalise and expand its functions and composition. This will prompt the active participation of the private sector in the planning and implementation of the cyber security policy" (Part IV, section 3 of the Strategy).
Link 2: Article 3. C)
Link 3: Page 3. CYBER SECURITY FORUM OFF SITE MEETING

9.4 Exchange of classified information

Criteria: *According to legislation, public, private and third sector entities may exchange classified information.*

Situation in the country: ✓ There is such a capacity.

Reference:
https://matsne.gov.ge/en/document/view/2750311
https://matsne.gov.ge/ka/document/view/1831535

Comment: Link 1: Art. 19, 20
Link 2: Art. 5.2

10. Capacity to manage large-scale cyber crises

10.1 Cyber crisis management plan

Criteria: *The government has established a comprehensive crisis management plan for large-scale cyber incidents. The plan and its different components must be established by legislation.*

Situation in the country: ⊗ No such capacity.

10.2 Cyber security/crisis operations centre

Criteria: *The government has established a permanent national-level cyber security/crisis operations centre. The centre acts as the cyber situation centre and operations staff for the crisis manager.*

Situation in the country: ⊗ No such capacity.

10.3 Crisis management exercise with cyber component

Criteria: *The government has conducted a crisis management exercise with a cyber component in the last 3 years.*

Situation in the country: ⊗ No such capacity.

10.4 National-level cyber crisis management exercise

Criteria: *The government has conducted the national-level cyber crisis management exercise in the last 3 years. The main focus of the exercise is the management of large-scale cyber incidents.*

Situation in the country: ✓ There is such a capacity.

Reference: http://csbd.gov.ge/news.php?news_number=63&news_type=geo_news&lang=en

Comment: On 27th of November, in the David Agmashenebeli National Defence Academy of Georgia, the Data Exchange Agency of the Ministry of Justice of Georgia and LEPL Cyber Security Bureau with the partnership of the State Security and Crisis Management Council, held cyber security simulated exercise – “Cyber-exe Georgia” 2015.
The aim of this event was to prepare IT specialists for cyber-attacks in critical situations in public and private organisations, which will contribute to the country’s and thereafter citizens’ defence as well.

10.5 Participation in international cyber crisis exercises

Criteria: *The country has participated in an international cyber crisis management exercise in the last 3 years.*

Situation in the country: ✓ There is such a capacity.

Reference: https://www.cyberex.es/international/result

Comment: In 2017, Georgia came in 8th place and is one of the best 10 teams.

10.6 Using volunteers in cyber crisis management

Criteria: *The government has established a system for using volunteers in large-scale cyber crisis management. The procedures for using volunteers must be established by legislation.*

Situation in the country: ⊗ No such capacity.

11. Capacity to fight cyber crimes

11.1 Cyber crimes are criminalised

Criteria: *The state has defined cybercrimes and established them by legislation. The regulations are in line with the Council of the Europe Convention on Cybercrime. Law enforcement authorities are obliged to start a criminal investigation if there are sufficient grounds for a criminal offence.*

Situation in the country: ✓ There is such a capacity.

Reference: https://matsne.gov.ge/ka/document/view/16426

Comment: Georgian Legal Framework on cybercrime covers all offences against confidentiality, integrity and availability of computer data and systems as well as computer-related offences and content-related offences, as required by the Convention on Cybercrime. Georgian cyber crime legislation is in line with the principles and rules of the Budapest Convention both in terms of substantive and procedural aspects. Namely, national law criminalises illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, Offences related to child pornography, offences related to infringements of copyright and related rights.

11.2 Unit for fighting cyber crime (department, agency, etc.)

Criteria: *The government has the capacity to conduct criminal proceedings for cybercrimes. A government entity has a department or an organisation that is specialised in combating cybercrime. The unit has competence in the following areas: 1) Prevention of cybercrime. 2) Conducting surveillance measures or special investigation techniques. 3) Conducting pre-trial investigations. The role and responsibilities of the units must be established by legislation.*

Situation in the country: ✓ There is such a capacity.

Reference: http://bit.ly/2hg0T6l

Comment: The Ministry of Internal Affairs (MIA) of Georgia is the responsible entity for cyber crime law enforcement. This activity is carried out by the Central Criminal Police Department (CCPD), under which the Division for Fighting Cyber Crime (CCD) was established in December 2012. The CCD was created within the framework of the European Convention on Cyber Crime, which requires member states to have an institutional setup in order to investigate cases of cyber crime. Currently, the CCD has more than 15 staff members, cyber crime investigators and IT specialists.

11.3 Unit for digital forensics (department, agency, etc.)

Criteria: *A government entity has a department or an organisation that is specialised in digital forensics:*

- *computer forensics*
- *mobile forensics*
- *hardware forensics, i.e. skimmers*
- *software forensics, malware analysis*

The role and responsibilities of the units must be established by legislation.

Situation in the country: ✓ There is such a capacity.

Reference: http://bit.ly/2hg0T6l
http://expertiza.gov.ge/

11.4 Electronic evidences are regulated

Criteria: *National regulations provide for rules on the collection and use of electronic evidence. General rules on evidence collection and use alike that also cover electronic evidence or a specific regulation on electronic evidence have been accepted.*

Situation in the country: ✓ There is such a capacity.

Reference: https://matsne.gov.ge/ka/document/view/90034

11.5 International cyber crimes 24/7 contact point

Criteria: *There is an international contact point for cyber crimes, which operates 24/7.*

Situation in the country:	✓ There is such a capacity.
Reference:	http://police.ge/en/projects/kiberdanashauli http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/declarations?p_auth=eNcHkRc4

12. Capacity to conduct military cyber defence operations

12.1 Cyber operation planning unit (department, command, etc.)

Criteria:	*Military forces have a department or an organisation that is specialised in cyber operation planning. This unit could be part of a general operation planning unit.*
Situation in the country:	✗ No such capacity.

12.2 Cyber operation units

Criteria:	*Military forces have a unit that is specialised in cyber operations.*
Situation in the country:	✗ No such capacity.

12.3 Exercise with a cyber operations component

Criteria:	*Military forces have conducted an exercise with a cyber operations component in the last 3 years.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://csbd.gov.ge/news.php?news_number=3&news_type=geo_news&lang=en
Comment:	“Didogri 2014” is an inter-agency Command and Staff Exercise aimed to streamline the ways of interaction between various government institutions, improving command and control systems and preparing staffs of GAF during crisis situations and warfare. This year, for the first time the relevant departments of the civil office of the Ministry of Defence and LEPL Cyber Security Bureau are taking part in the exercise. The Cyber Security Bureau initiated 4 injects [???] during the war gaming.

12.4 Cyber operation exercise in the last 3 years

Criteria:	*Military forces have conducted a cyber operation exercise in the last 3 years.*

Situation in the country:	⊗ No such capacity.

12.5 Participation in international cyber exercise in the last 3 years

Criteria:	*The country's military team has participated in an international cyber operation exercise in the last 3 years.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://bit.ly/2wuzCHH

Republic of Moldova

I GENERAL CYBER SECURITY INDICATORS

1. Capacity to develop national cyber security policies

1.1 National-level cyber security policy unit (department, etc.)

Criteria:	*A central government entity has a national level department or organisation that is specialised in national cyber security policy development. Work outcomes of this unit are for example the official national cyber security strategy and implementation plan.*
Situation in the country:	⊗ No such capacity.

1.2 National-level cyber security coordination format (committee, etc.)

Criteria:	*The central government has established the national-level cyber security coordination format (committee, council, working group, etc.) for cyber security policy coordination. This format includes relevant public, private and third sector entities.*
Situation in the country:	⊗ No such capacity.
Comment:	No. coordination format is defined. The responsibilities related to cyber/information security are divided between different government institutions and coordination is performed between them directly. Usually the private sector is not involved. Recently, in the context of implementing Government Decision No. 201 from 24 February

2017 regarding the approval of the Minimal Cyber Security Requirements, the Minister of Information Technology was made responsible for the implementation of these requirements.

1.3 National-level cyber security terms and definitions

Criteria:	*The central government has established national-level cyber security terms and definitions by legislation.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://lex.justice.md/viewdoc.php?action=view&view=doc&id=361818&lang=2
Comment:	Government decision No. 811 from 2015 “National Cybersecurity Agenda of the Republic of Moldova for the years 2016–2020” defines the main cyber security terms and definitions: 1st Chapter “General Provisions”.

1.4 National-level cyber security strategy (valid)

Criteria:	*The central government has established the national-level cyber security strategy or other equivalent document.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://lex.justice.md/viewdoc.php?action=view&view=doc&id=361818&lang=2 http://ncsi.ega.ee/app/uploads/2016/05/ruhg-nr-811-29.10.2015.pdf
Comment:	Government decision No. 811 from 2015 “National Cybersecurity Agenda of the Republic of Moldova for the years 2016–2020”

1.5 National-level cyber security implementation plan (valid)

Criteria:	*The central government has established the national-level cyber security implementation plan or another equivalent document.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://lex.justice.md/UserFiles/File/2015/mo306-310ru/anexa%20nr.1_811.docx

Comment: Appendix 1 of the National Cybersecurity Program: “Action plan on the implementation of the national cybersecurity program of the Republic of Moldova for 2016–2020”.

2. Capacity to analyse national-level cyber threats

2.1 National-level cyber threat analysis unit (department, etc.)

Criteria: *A central government entity has a national level department or organisation that is specialised in national cyber threat analysis. The work outcomes of this unit are regular comprehensive cyber threat analysis and risk assessments. These risk assessments are the basis for national-level cyber security planning (national cyber security strategy development, etc.).*

Situation in the country: ⊗ No such capacity.

Comment: The government and private sector have their own CIRC teams, which exchange information and cooperate mostly during such incidents.

2.2 Annual public cyber threat reports are published

Criteria: *The public part of the national cyber threat analysis is published at least once a year. The aim of this report is to inform and educate the general public.*

Situation in the country: ⊗ No such capacity.

3. Capacity to provide cyber security education

3.1 Cyber safety website for the general public

Criteria: *Public authorities provide or finance at least one cyber safety website for the general public. The website provides up-to-date information about cyber threats and security measures related to ICT systems, as well as other useful materials and guidance for regular users. The website should inform about timely threats and security measures related to ICT systems (computers, mobile devices, information systems, e-services, etc.). Websites that inform only about social media threats (cyber bullying, etc.) are not alone accepted. These websites could be added as additional materials.*

Situation in the country: ✓ There is such a capacity.

Reference: http://www.cert.gov.md/
http://siguronline.md

Comment: Government CERT provides cyber security and incident management related information. The SigurOnline website promotes the safe use of the Internet and provides information for children, parents and teachers.

3.2 Nationwide public awareness-raising activity in the last 3 years

Criteria: *Public authorities have organised at least one public awareness-raising activity in the last 3 years. The media campaign should be nationwide (TV, radio, newspapers, etc.).*

Situation in the country: ✓ There is such a capacity.

Reference: http://cert.gov.md/noutati/international-conference-2014.html

Comment: The Centre of Special Telecommunications has organised several public awareness-raising events every year in October as part of the European Cyber Security Month. A video clip is made for raising wider understanding of cyber threats.

3.3 Cyber safety competencies in primary education

Criteria: *Primary education (ISCED 2011 Level 1) curricula include cyber safety / computer safety competences.*

Situation in the country: ⊗ No such capacity.

3.4 Cyber safety competencies in secondary education

Criteria: *Secondary education (ISCED 2011 Level 2-4) curricula include cyber safety / computer safety competences.*

Situation in the country: ⊗ No such capacity.

3.5 Cyber safety competencies in vocational education

Criteria: *Vocational education (ISCED 2011 Level 3-4) curricula include cyber safety / computer safety components.*

Situation in the country: ⊗ No such capacity.

3.6 Bachelor’s level cyber security programme (at least 1)

Criteria:	*There is at least one cyber security / electronic information security focused programme on the bachelor’s or equivalent level (ISCED 2011 Level 6).*
Situation in the country:	✓ There is such a capacity.
Reference:	http://utm.md/studii/planuri/zi/FCIM/plan2011-si-zi.pdf http://bit.ly/2f9gGmx
Comment:	In 2011, Technical University of Moldova, Department of Software Engineering and Informatics launched the specialty 526.5 “Informational Security” cycle I, License (240 credits) with teaching in the Romanian language.

3.7 Master’s level cyber security programme (at least 1)

Criteria:	*There is at least one cyber security / electronic information security focused programme on the master’s or equivalent level (ISCED 2011 Level 7)*
Situation in the country:	⊗ No such capacity.

3.8 PhD level cyber security programme (at least 1)

Criteria:	*There is at least one cyber security / electronic information security focused programme on the PhD or equivalent level (ISCED 2011 Level 8).*
Situation in the country:	⊗ No such capacity.

3.9 Cyber security professional association

Criteria:	*There is a professional association of cyber/information security specialists, managers or auditors.*
Situation in the country:	⊗ No such capacity.

4. Capacity to provide international cyber security

4.1 International cyber security cooperation unit (department, etc.)

Criteria:	*The ministry responsible for foreign affairs has a department or an organisation that is specialised in international cyber security.*
Situation in the country:	⊗ No such capacity.

4.2 Implementation of the Convention on Cybercrime

Criteria: *The government has enforced the Convention on Cybercrime of the Council of Europe. The government has ratified or acceded to the convention. The convention is fully implemented.*

Situation in the country: ✓ There is such a capacity.

Reference: http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=u9Jjs5so
http://lex.justice.md/viewdoc.php?action=view&view=doc&id=333508&lang=1
http://bit.ly/2jl0BJU

4.3 Cooperation agreements with other countries (at least 1 country)

Criteria: *The government has bilateral, regional, international cyber security cooperation agreements with other countries or international organisations. One other agreement is sufficient that is not the Convention on Cybercrime of the Council of Europe.*

Situation in the country: ⊗ No such capacity.

4.4 Representation in international cooperation formats (at least 1)

Criteria: *The government is represented regularly in a cooperation format that deals with international cyber security.*

Situation in the country: ⊗ No such capacity.

4.5 International cyber security organisation in the country

Criteria: *A regional or international cyber security organisation with regional or international functions is located in the country.*

Situation in the country: ⊗ No such capacity.

4.6 Cyber security capacity-building

Criteria: *The country has (co)financed or (co)organised at least one capacity-building project for another country in the last 3 years.*

Situation in the country: ⊗ No such capacity.

II. BASELINE CYBER SECURITY INDICATORS

5. Capacity to ensure baseline cyber security

5.1 Baseline cyber security management unit (agency, etc.)

Criteria: *A central government entity has a department or organisation that is specialised in national-level baseline cyber security management – development, implementation, co-ordination and supervision.*

Situation in the country: ✗ No such capacity.

5.2 Personal data protection authority (independent organisation)

Criteria: *There is an independent public supervisory authority that is responsible for personal data protection.*

Situation in the country: ✓ There is such a capacity.

Reference: http://www.datepersonale.md/en/start/

5.3 Legislation for information classification (public, confidential, etc.)

Criteria: *There is legislation for information classification – public, private, classified, restricted, confidential, critical, etc.*

Situation in the country: ✓ There is such a capacity.

Reference: http://lex.justice.md/viewdoc.php?action=view&view=doc&id=330847&lang=2

http://lex.justice.md/viewdoc.php?action=view&view=doc&id=312792&lang=2

http://lex.justice.md/viewdoc.php?action=view&view=doc&id=340495&lang=2

Comment: There are 3 laws in the Republic of Moldova, which regulate information classifications:
1. State Secrets Act (No. 245 from 2008)
2. Commercial Secrets Act (No. 171 from 1994)
3. Personal Data Protection Act (No. 133 from 2011)

5.4 Information / cyber security management standard

Criteria: *There is a baseline regulation or an adopted standard for information/cyber security management for public sector entities. The regulation or standard is mandatory for public sector entities.*

Situation in the country: ✓ There is such a capacity.

Reference: http://lex.justice.md/viewdoc.php?action=view&view=doc&id=369772&lang=2

Comment: Government decision No. 201 from 2017 regarding the approval of minimum compulsory cyber security requirements.

5.5 Accreditation of public sector ICT solutions before introduction

Criteria: *Before the introduction of an ICT solution (information system, public e-service, etc.) in the public sector, an official security accreditation/audit takes place.*

Situation in the country: ✓ There is such a capacity.

Reference: http://lex.justice.md/viewdoc.php?action=view&view=doc&id=369772&lang=2

Comment: Chapter V "Mandatory minimum requirements for the cybersecurity in the procurement of new information systems or upgrading existing" defines under point 7: "Prior to the introduction of a new system it should be made sure that its safety features operate in accordance with pre-established requirements and appropriate tests should be carried out by a third party".

5.6 Regular audits of public sector ICT solutions

Criteria: *The operators of public sector ICT solutions (information systems, e-services, etc.) have to order regular independent ICT security audits.*

Situation in the country: ✓ There is such a capacity.

Reference: http://lex.justice.md/viewdoc.php?action=view&view=doc&id=369772&lang=2

Comment: Government decision No. 201 from 2017 regarding the approval of minimum compulsory cyber security requirement defines several places the need of regular audits: Chapter IV, point 21 9), 10); Chapter V, point 22 7).

6. Capacity to provide a secure environment for e-services

6.1 Secure data exchange environment for e-services

Criteria: *There is a secure inter-organisational data exchange environment in the country (secure internet), which enables public sector entities to provide secure web services for citizens and entrepreneurs. Private sector and other entities will be interfaces with the environment, if they provide a public service or participate in it.*

Situation in the country: ✓ There is such a capacity.

Reference: http://bit.ly/2xkQUGb

http://www.cts.md/en/content/telecommunication-services

Comment: Government e-services exchange data via the government interoperability platform "M-Connect". Additionally, government institutions are connected to the Private Government Network managed by the Centre of Special Telecommunications.

6.2 Up-to-date cryptographic solution for the environment

Criteria: *In the data exchange environment, the cryptographic requirement complies with recognised up-to-date guidelines (NIST Special Publication 800-78-3, ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012), etc.)*

Situation in the country: ✓ There is such a capacity.

Reference: https://pki.cts.md/fileadmin/templates/pki_files/about_legislatie/64.pdf

http://www.cts.md/en/content/telecommunication-services

Comment: Government's decision regarding the approval of the technical norms in the field of digital signature (No. 64 from 2006). Chapter II, Creating and Administering Public and Private Electronic Keys. The minimum length of public and private keys:

- 2048 bits for the RSA algorithm for digital signature users;
- 4096 bits for the RSA algorithm for certification centres;
- 2048 bits for the DSA algorithm;
- 160 bits for the DSA algorithm based on elliptic curves;
- 512 bits for the SM GOST 34.10: 2006 algorithm.

7. Capacity to provide e-identification and e-signatures

7.1 Citizens and legal entities have a unique identifier

Criteria: *All citizens, residents and legal entities are identifiable via a persistent unique identifier. The identifier is used on public sector registries. It is not a number of the personal identification document, but a unique number assigned to a person for life.*

Situation in the country: ✓ There is such a capacity.

Reference: http://lex.justice.md/viewdoc.php?action=view&view=doc&id=326009&lang=2

http://lex.justice.md/viewdoc.php?action=view&view=doc&id=296142&lang=2

Comment: Law on State Registration of Legal Entities And individual entrepreneurs (No. 220 from 2007). Article 11. The registration procedure says: (2) The legal entity at registration shall be assigned a state identification number (IDNO), which shall be indicated on the title sheet of the instruments of incorporation.
Government decision "State Register of the Population" and the Regulation on the State Registry of the Population" (No. 333 from 2002). Article 13. "Categories of identification number": An Identification Number of Person (IDNP) shall be assigned to each individual at the time of initially entering the data about it in the RSPP and remains unchanged throughout the lifetime of such data, and shall be included in all documents of the individual concerned.

7.2 Public e-services identify users via a unique identifier.

Criteria: *The public-sector e-services use the identifier for identification; there is no need for additional queries. There is a legal framework for electronic identification and authentication. The framework is based on the unique identifier.*

Situation in the country: ✓ There is such a capacity.

Reference: https://mpass.gov.md/?lang=en

http://lex.justice.md/viewdoc.php?action=view&view=doc&id=353612&lang=2

Comment: M-Pass is Moldovan government's authentication service, which uses the electronic signature for authentication. Law on Electronic Signature and Electronic Document (No. 91 from 2014). Article 31: The holder's identification data for the user's public key certificate is the name, surname and identification number of the individual (IDNP) and / or the alias, if any, and in the case of the public key of the service provider Certification – Provider's name and legal entity identification number (IDNO).

7.3 Public e-services use 2-factor authentication

Criteria: *Public sector e-services use 2-factor authentication and strong cryptographic solutions in national electronic authentication. The cryptographic solution has to comply with NIST Special Publication 800-78-3, ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012), etc.*

Situation in the country: ✓ There is such a capacity.

Reference: https://mpass.gov.md/?lang=en

Comment: The government's e-Identification service "M-Pass" includes 2-factor authentication methods.

7.4 A legal framework for electronic signature

Criteria: *A legal framework for electronic signature is established in the country. The electronic signature system is based on the aforementioned unique identifier. There are requirements for trust services required for electronic signature. These requirements are established by legislation.*

Situation in the country: ✓ There is such a capacity.

Reference: http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=353612

Comment: The Law on Electronic Signature and Electronic Document. Law No. 91 from 2014.

7.5 Supervision over qualified trust services providers

Criteria: *There is an authority that is responsible for the supervision of qualified trust service providers and for granting the qualified status.*

Situation in the country: ✓ There is such a capacity.

Reference: http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=353612

Comment: The Law on Electronic Signature and Electronic Document. Law No. 91 from 2014. Chapter V Monitoring and Control, Article 36: “The competent body responsible for the development and promotion of state policy and exercising control in the application of all types of electronic signatures is the Intelligence and Security Service.”

7.6 A qualified electronic signature has legal effect

Criteria: *A qualified electronic signature has the equivalent legal effect of a handwritten signature.*

Situation in the country: ✓ There is such a capacity.

Reference: http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=353612

Comment: The Law on Electronic Signature and Electronic Document. Law No. 91 from 2014. Chapter II, Article 5, point 2) “Qualified advanced electronic signature has the same legal value as a handwritten signature.”

8. Capacity to protect essential e-services / CII

8.1 The essential e-services / CII are defined

Criteria: *The essential e-services / critical information infrastructure (CII) are defined by legislation.*

Situation in the country: ✗ No such capacity.

8.2 National level essential e-services / CII protection unit

Criteria: *A central government entity has a department or organisation that is specialised in essential e-services / critical information infrastructure protection. The unit has the responsibility to develop adequate security measures, and coordinate and supervise the implementation of specific security measures.*

Situation in the country: ✗ No such capacity.

8.3 Service continuity requirements for essential e-services / CII operators

Criteria: *Data processing and service continuity requirements (downtime elimination time, readiness for disruption, etc.) are established for essential e-services / CII operators by legislation.*

Situation in the country: ⊗ No such capacity.

8.4 Essential e-services / CII operators have a cyber security manager

Criteria: *The essential e-services / CII operators have to appoint a cyber/information security manager.*

Situation in the country: ⊗ No such capacity.

III. INCIDENT AND CRISIS MANAGEMENT INDICATORS

9. Capacity to detect and respond to cyber incidents 24/7

9.1 National-level cyber incident response unit

Criteria: *The government has a unit (common name is CERT, CIRC, etc.) that is specialised in national-level cyber incident detection and response. The unit is responsible for 24/7 data gathering of incidents in cyberspace. The authority manages the comprehensive picture of incidents in national cyberspace.*

Situation in the country: ✓ There is such a capacity.

Reference: http://cert.gov.md/about-us/about-cert-gov-md.html

Comment: Government CERT

9.2 Cyber incidents reporting responsibility

Criteria: *Public sector entities and CII operators have the responsibility to report about cyber incidents.*

Situation in the country: ⊗ No such capacity.

9.3 Official format for practical public-private cooperation

Criteria: *There is an official cooperation format (organisation, association, etc.) for operational (practical) public, private and third sector cooperation. Activities are specified in the legislation, agreement or in another official format.*

Situation in the country: ⊗ No such capacity.

9.4 Exchange of classified information

Criteria: *According to legislation, public, private and third sector entities may exchange classified information.*

Situation in the country:	✓ There is such a capacity.
Reference:	http://lex.justice.md/viewdoc.php?action=view&view=doc&id=330847&lang=2
Comment:	State Secrets Act (No. 245 from 2008): Article 19. Mutual transmission of information classified as a state secret, by the public authorities and other legal persons. Article 21. Transmission of information classified as state secret to other states or international organisations

10. Capacity to manage large-scale cyber crises

10.1 Cyber crisis management plan

Criteria:	*The government has established a comprehensive crisis management plan for large-scale cyber incidents. The plan and its different components must be established by legislation.*
Situation in the country:	✗ No such capacity.

10.2 Cyber security/crisis operations centre

Criteria:	*The government has established a permanent national-level cyber security/crisis operations centre. The centre acts as the cyber situation centre and operations staff for the crisis manager.*
Situation in the country:	✗ No such capacity.

10.3 Crisis management exercise with cyber component

Criteria:	*The government has conducted a crisis management exercise with a cyber component in the last 3 years.*
Situation in the country:	✗ No such capacity.

10.4 National-level cyber crisis management exercise

Criteria:	*The government has conducted the national-level cyber crisis management exercise in the last 3 years. The main focus of the exercise is the management of large-scale cyber incidents.*
Situation in the country:	✗ No such capacity.

10.5 Participation in international cyber crisis exercises

Criteria: *The country has participated in an international cyber crisis management exercise in the last 3 years.*

Situation in the country: ⊗ No such capacity.

10.6 Using volunteers in cyber crisis management

Criteria: *The government has established a system for using volunteers in large-scale cyber crisis management. The procedures for using volunteers must be established by legislation.*

Situation in the country: ⊗ No such capacity.

11. Capacity to fight cyber crimes

11.1 Cyber crimes are criminalised

Criteria: *The state has defined cybercrimes and established them by legislation. The regulations are in line with the Council of the Europe Convention on Cybercrime. Law enforcement authorities are obliged to start a criminal investigation if there are sufficient grounds for a criminal offence.*

Situation in the country: ✓ There is such a capacity.

Reference: www.legislationline.org/documents/id/8906

Comment: Criminal Code of the Republic of Moldova: Special part, Chapter XI.

11.2 Unit for fighting cyber crime (department, agency, etc.)

Criteria: *The government has the capacity to conduct criminal proceedings for cybercrimes. A government entity has a department or an organisation that is specialised in combating cybercrime. The unit has competence in the following areas: 1) Prevention of cybercrime. 2) Conducting surveillance measures or special investigation techniques. 3) Conducting pre-trial investigations. The role and responsibilities of the units must be established by legislation.*

Situation in the country: ✓ There is such a capacity.

Reference: http://politia.md/ro/advanced-page-type/structura
http://bit.ly/2jI0BJU
http://procuratura.md/en/struct/
http://lex.justice.md/viewdoc.php?action=view&view=doc&id=333508&lang=1

Comment: Centre for Combating Cyber Crimes at the National Investigation Inspectorate.
Information Technology and Cybercrime Division at the Office of the Prosecutor General.
The responsibilities of different entities are defined in Law No. 20 from 2009 “Preventing and combating cybercrime”.

11.3 Unit for digital forensics (department, agency, etc.)

Criteria: *A government entity has a department or an organisation that is specialised in digital forensics:*

- *computer forensics*
- *mobile forensics*
- *hardware forensics, i.e. skimmers*
- *software forensics, malware analysis*

The role and responsibilities of the units must be established by legislation.

Situation in the country: ✓ There is such a capacity.

Reference: http://politia.md/ro/advanced-page-type/structura
http://bit.ly/2jI0BJU
http://lex.justice.md/viewdoc.php?action=view&view=doc&id=333508&lang=1

Comment: Centre for Combating Cyber Crimes at the National Investigation Inspectorate. The functions of this unit are: computer forensics, mobile forensics, hardware forensics (i.e. skimmers), software forensics, malware analysis. The responsibilities of different entities are defined in Law No. 20 from 2009 “Preventing and combating cybercrime”.

11.4 Electronic evidences are regulated

Criteria: *National regulations provide for rules on the collection and use of electronic evidence. General rules on evidence collection and use alike that also cover electronic evidence or a specific regulation on electronic evidence have been accepted.*

Situation in the country: ✓ There is such a capacity.

Reference: http://lex.justice.md/md/326970/

Comment: The Code of Criminal Proceedings of the Republic of Moldova (No. 122 from 2003). Article 164. Audio or video recordings, photographs and other forms of information carriers: Audio and video recordings, photographs, technical, electronic, magnetic, optical and other technical-electronic information carriers acquired under this Code are evidence of whether they contain data or sound indices of the preparation or commission of an offense; and If their content contributes to finding the truth in the case.

11.5 International cyber crimes 24/7 contact point

Criteria: *There is an international contact point for cyber crimes, which operates 24/7.*

Situation in the country: ✓ There is such a capacity.

Reference: https://rm.coe.int/16804b3493
http://bit.ly/2jI0BJU

Comment: There are two official contact points in the Republic of Moldova:
Section for combating IT crimes at the Office of the Prosecutor General
Centre for combating cybercrime at the National Inspectorate for Investigations

12. Capacity to conduct military cyber defence operations

12.1 Cyber operation planning unit (department, command, etc.)

Criteria: *Military forces have a department or an organisation that is specialised in cyber operation planning. This unit could be part of a general operation planning unit.*

Situation in the country: ✗ No such capacity.

12.2 Cyber operation units

Criteria: *Military forces have a unit that is specialised in cyber operations.*

Situation in the country: ✗ No such capacity.

12.3 Exercise with a cyber operations component

Criteria:	*Military forces have conducted an exercise with a cyber operations component in the last 3 years.*
Situation in the country:	☒ No such capacity.

12.4 Cyber operation exercise in the last 3 years

Criteria:	*Military forces have conducted a cyber operation exercise in the last 3 years.*
Situation in the country:	☒ No such capacity.

12.5 Participation in international cyber exercise in the last 3 years

Criteria:	*The country's military team has participated in an international cyber operation exercise in the last 3 years.*
Situation in the country:	☒ No such capacity.

Ukraine

I GENERAL CYBER SECURITY INDICATORS

1. Capacity to develop national cyber security policies

1.1 National-level cyber security policy unit (department, etc.)

Criteria:	*A central government entity has a national level department or organisation that is specialised in national cyber security policy development. Work outcomes of this unit are for example the official national cyber security strategy and implementation plan.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://www.rnbo.gov.ua/documents/425.html
Comment:	The National Cyber Security Coordination Centre under the National Security and Defence Council of Ukraine. According to the Constitution of Ukraine and under the procedure established by law the National Security and Defence Council of Ukraine is to coordinate and control activities of the entities of security and defence sector, ensuring the cyber security of Ukraine.

1.2 National-level cyber security coordination format (committee, etc.)

Criteria: *The central government has established the national-level cyber security coordination format (committee, council, working group, etc.) for cyber security policy coordination. This format includes relevant public, private and third sector entities.*

Situation in the country: ✓ There is such a capacity.

Reference: http://zakon5.rada.gov.ua/laws/show/242/2016#n9

Comment: The National Cybersecurity Coordination Centre is the working body of the National Security and Defence Council of Ukraine. The members of the Centre are:

- First Deputy or Deputy Minister of Defence of Ukraine,
- Chief of the General Staff of the Armed Forces of Ukraine,
- Head of the Security Service of Ukraine,
- Head of the Foreign Intelligence Service of Ukraine,
- Head of the National Police of Ukraine,
- Head of the National Bank of Ukraine (with consent), whose responsibilities include cybersecurity issues,
- Head of the Main Directorate of Intelligence of the Ministry of Defence of Ukraine
- Head of the Office of Intelligence of the Administration of the State Border Guard Service of Ukraine,
- Head of the State Service for Special Communications and Information Protection of Ukraine.

1.3 National-level cyber security terms and definitions

Criteria: *The central government has established national-level cyber security terms and definitions by legislation.*

Situation in the country: ✗ No such capacity.

Comment: Additional material: Draft Law of Ukraine on the Basic Principles for the Cybersecurity of Ukraine

1.4 National-level cyber security strategy (valid)

Criteria: *The central government has established the national-level cyber security strategy or other equivalent document.*

Situation in the country: ✓ There is such a capacity.

Reference: http://zakon2.rada.gov.ua/laws/show/96/2016/paran11#n11
http://cert.gov.ua/pdf/NationalCyberSecurityStrategy.pdf

Comment: Cyber Security Strategy of Ukraine approved by Presidential Decree of Ukraine No. 96/2016 dated 15 March 2016
Unofficial translation is under link 2.

1.5 National-level cyber security implementation plan (valid)

Criteria: *The central government has established the national-level cyber security implementation plan or another equivalent document.*

Situation in the country: ✓ There is such a capacity.

Reference: http://zakon3.rada.gov.ua/laws/show/440-2016-%D1%80
http://zakon2.rada.gov.ua/laws/show/155-2017-%D1%80

Comment: Action Plan for 2016 to implement cyber security strategy of Ukraine, approved by the Cabinet of Ministers of Ukraine, from June 24, 2016, No. 440-p
Action Plan for 2017 to implement cyber security strategy Ukraine, approved by the Cabinet of Ministers of Ukraine, from March 10, 2017 No. 155-p

2. Capacity to analyse national-level cyber threats

2.1 National-level cyber threat analysis unit (department, etc.)

Criteria: *A central government entity has a national level department or organisation that is specialised in national cyber threat analysis. The work outcomes of this unit are regular comprehensive cyber threat analysis and risk assessments. These risk assessments are the basis for national-level cyber security planning (national cyber security strategy development, etc.).*

Situation in the country: ✗ No such capacity.

2.2 Annual public cyber threat reports are published

Criteria: *The public part of the national cyber threat analysis is published at least once a year. The aim of this report is to inform and educate the general public.*

Situation in the country: ✗ No such capacity.

3. Capacity to provide cyber security education

3.1 Cyber safety website for the general public

Criteria: *Public authorities provide or finance at least one cyber safety website for the general public. The website provides up-to-date information about cyber threats and security measures related to ICT systems, as well as other useful materials and guidance for regular users. The website should inform about timely threats and security measures related to ICT systems (computers, mobile devices, information systems, e-services, etc.). Websites that inform only about social media threats (cyber bullying, etc.) are not alone accepted. These websites could be added as additional materials.*

Situation in the country: ✓ There is such a capacity.

Reference: http://cert.gov.ua
http://websecurity.com.ua

Comment: The CERT-Ukraine provides on its website recommendations and technical assistance. It is also possible to request penetration tests.

3.2 Nationwide public awareness-raising activity in the last 3 years

Criteria: *Public authorities have organised at least one public awareness-raising activity in the last 3 years. The media campaign should be nationwide (TV, radio, newspapers, etc.).*

Situation in the country: ⊗ No such capacity.

3.3 Cyber safety competencies in primary education

Criteria: *Primary education (ISCED 2011 Level 1) curricula include cyber safety / computer safety competences.*

Situation in the country: ⊗ No such capacity.

3.4 Cyber safety competencies in secondary education

Criteria: *Secondary education (ISCED 2011 Level 2-4) curricula include cyber safety / computer safety competences.*

Situation in the country: ⊗ No such capacity.

3.5 Cyber safety competencies in vocational education

Criteria:	*Vocational education (ISCED 2011 Level 3-4) curricula include cyber safety / computer safety components.*
Situation in the country:	⊗ No such capacity.

3.6 Bachelor's level cyber security programme (at least 1)

Criteria:	*There is at least one cyber security / electronic information security focused programme on the bachelor's or equivalent level (ISCED 2011 Level 6).*
Situation in the country:	✓ There is such a capacity.
Reference:	http://ac.opu.ua/specialization/kiberbezpeka
Comment:	Odessa National Polytechnic University

3.7 Master's level cyber security programme (at least 1)

Criteria:	*There is at least one cyber security / electronic information security focused programme on the master's or equivalent level (ISCED 2011 Level 7)*
Situation in the country:	✓ There is such a capacity.
Reference:	http://www.dut.edu.ua/ua/pages/372
Comment:	State University of Telecommunications

3.8 PhD level cyber security programme (at least 1)

Criteria:	*There is at least one cyber security / electronic information security focused programme on the PhD or equivalent level (ISCED 2011 Level 8).*
Situation in the country:	✓ There is such a capacity.
Reference:	http://start.karazin.ua/programs/8/7/125/31 https://drive.google.com/open?id=0B8Suxom_d1mAM0l1WkEyam5Za3M

3.9 Cyber security professional association

Criteria:	*There is a professional association of cyber/information security specialists, managers or auditors.*

	Situation in the country:	✓ There is such a capacity.
	Reference:	http://www.isaca.org.ua
	Comment:	ISACA Kyiv Chapter

4. Capacity to provide international cyber security

4.1 International cyber security cooperation unit (department, etc.)	Criteria:	*The ministry responsible for foreign affairs has a department or an organisation that is specialised in international cyber security.*
	Situation in the country:	⊗ No such capacity.
4.2 Implementation of the Convention on Cybercrime	Criteria:	*The government has enforced the Convention on Cybercrime of the Council of Europe. The government has ratified or acceded to the convention. The convention is fully implemented.*
	Situation in the country:	✓ There is such a capacity.
	Reference:	http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=u9Jjs5so http://zakon5.rada.gov.ua/laws/show/994_575
4.3 Cooperation agreements with other countries (at least 1 country)	Criteria:	*The government has bilateral, regional, international cyber security cooperation agreements with other countries or international organisations. One other agreement is sufficient that is not the Convention on Cybercrime of the Council of Europe.*
	Situation in the country:	⊗ No such capacity.
4.4 Representation in international cooperation formats (at least 1)	Criteria:	*The government is represented regularly in a cooperation format that deals with international cyber security.*
	Situation in the country:	✓ There is such a capacity.

Reference:	https://www.first.org/members/teams/cert-ua http://www.impact-alliance.org/countries/alphabetical-list.html
Comment:	Forum for Incident Response and Security Teams (FIRST) International Multilateral Partnership Against Cyber Threats (IMPACT)

4.5 International cyber security organisation in the country

Criteria:	*A regional or international cyber security organisation with regional or international functions is located in the country.*
Situation in the country:	⊗ No such capacity.

4.6 Cyber security capacity-building

Criteria:	*The country has (co)financed or (co)organised at least one capacity-building project for another country in the last 3 years.*
Situation in the country:	⊗ No such capacity.

II. BASELINE CYBER SECURITY INDICATORS

5. Capacity to ensure baseline cyber security

5.1 Baseline cyber security management unit (agency, etc.)

Criteria:	*A central government entity has a department or organisation that is specialised in national-level baseline cyber security management – development, implementation, co-ordination and supervision.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://www.rnbo.gov.ua/documents/425.html http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=89831&cat_id=89828
Comment:	National Cybersecurity Coordination Centre State Service for Special Communications and Information Protection of Ukraine

5.2 Personal data protection authority (independent organisation)

Criteria:	*There is an independent public supervisory authority that is responsible for personal data protection.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://www.ombudsman.gov.ua/ http://zakon3.rada.gov.ua/laws/show/776/97-%D0%B2%D1%80 http://goo.gl/efj1pb
Comment:	Personal data protection is carried out by the Ukrainian Parliament Commissioner for Human Rights.

5.3 Legislation for information classification (public, confidential, etc.)

Criteria:	*There is legislation for information classification – public, private, classified, restricted, confidential, critical, etc.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://zakon2.rada.gov.ua/laws/show/2657-12
Comment:	Law on Information.

5.4 Information / cyber security management standard

Criteria:	*There is a baseline regulation or an adopted standard for information/cyber security management for public sector entities. The regulation or standard is mandatory for public sector entities.*
Situation in the country:	✗ No such capacity.

5.5 Accreditation of public sector ICT solutions before introduction

Criteria:	*Before the introduction of an ICT solution (information system, public e-service, etc.) in the public sector, an official security accreditation/audit takes place.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://zakon3.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

Comment: Law on the Protection of Information in Information and Telecommunications Systems (link). Article 8 states the requirement for accreditation.

5.6 Regular audits of public sector ICT solutions

Criteria: *The operators of public sector ICT solutions (information systems, e-services, etc.) have to order regular independent ICT security audits.*

Situation in the country: ✓ There is such a capacity.

Reference: http://zakon4.rada.gov.ua/laws/show/z0090-15

Comment: Art. 10. Regular audits are performed in state bodies, military formations, organisations and institutions at least once every five years.

6. Capacity to provide a secure environment for e-services

6.1 Secure data exchange environment for e-services

Criteria: *There is a secure inter-organisational data exchange environment in the country (secure internet), which enables public sector entities to provide secure web services for citizens and entrepreneurs. Private sector and other entities will be interfaces with the environment, if they provide a public service or participate in it.*

Situation in the country: ✗ No such capacity.

6.2 Up-to-date cryptographic solution for the environment

Criteria: *In the data exchange environment, the cryptographic requirement complies with recognised up-to-date guidelines (NIST Special Publication 800-78-3, ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012), etc.)*

Situation in the country: ✓ There is such a capacity.

Reference: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=120158&cat_id=119123

Comment: The Administration of the State Service for Special Communications and Information Protection of Ukraine introduces new standards for cryptographic information security

7. Capacity to provide e-identification and e-signatures

7.1 Citizens and legal entities have a unique identifier

Criteria: *All citizens, residents and legal entities are identifiable via a persistent unique identifier. The identifier is used on public sector registries. It is not a number of the personal identification document, but a unique number assigned to a person for life.*

Situation in the country: ✓ There is such a capacity.

Reference: http://zakon3.rada.gov.ua/laws/show/z0124-98

Comment: Taxpayer Identification Number. It is unique, and is issued at the same time as a passport. There is however a procedure available for citizens to avoid obtaining this number (for religious or other reasons)

7.2 Public e-services identify users via a unique identifier.

Criteria: *The public-sector e-services use the identifier for identification; there is no need for additional queries. There is a legal framework for electronic identification and authentication. The framework is based on the unique identifier.*

Situation in the country: ✓ There is such a capacity.

Reference: http://zakon3.rada.gov.ua/laws/show/z0124-98

Comment: (Art 1.2) The use of identification numbers mandatory for citizens:
..... data are used in other information systems Ukraine.

7.3 Public e-services use 2-factor authentication

Criteria: *Public sector e-services use 2-factor authentication and strong cryptographic solutions in national electronic authentication. The cryptographic solution has to comply with NIST Special Publication 800-78-3, ECRYPT II Yearly Report on Algorithms and Keysizes (2011-2012), etc.*

Situation in the country: ⊗ No such capacity.

7.4 A legal framework for electronic signature

Criteria: *A legal framework for electronic signature is established in the country. The electronic signature system is based on the aforementioned unique identifier. There are requirements for trust services required for electronic signature. These requirements are established by legislation.*

Situation in the country:	✓ There is such a capacity.
Reference:	http://zakon2.rada.gov.ua/laws/show/852-15
Comment:	Law of Ukraine on electronic digital signature

7.5 Supervision over qualified trust services providers

Criteria:	*There is an authority that is responsible for the supervision of qualified trust service providers and for granting the qualified status.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://zakon2.rada.gov.ua/laws/show/717/2011/paran85#n17 http://www.dsszzi.gov.ua/dsszzi/control/uk/index
Comment:	The State Service for Special Communication and Information Protection of Ukraine

7.6 A qualified electronic signature has legal effect

Criteria:	*A qualified electronic signature has the equivalent legal effect of a handwritten signature.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://zakon2.rada.gov.ua/laws/show/852-15
Comment:	Art. 3

8. Capacity to protect essential e-services / CII

8.1 The essential e-services / CII are defined

Criteria:	*The essential e-services / critical information infrastructure (CII) are defined by legislation.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://zakon3.rada.gov.ua/laws/show/563-2016-%D0%BF

Comment:	Resolution of the Cabinet of Ministers of Ukraine on Approval of the Procedure for the Establishment of the List of Information and Telecommunications Systems of the State Critical Infrastructure Facilities

8.2 National level essential e-services / CII protection unit

Criteria:	*A central government entity has a department or organisation that is specialised in essential e-services / critical information infrastructure protection. The unit has the responsibility to develop adequate security measures, and coordinate and supervise the implementation of specific security measures.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://www.dknii.gov.ua/content/informaciyna-bezpeka
Comment:	State Agency for E-Governance of Ukraine

8.3 Service continuity requirements for essential e-services / CII operators

Criteria:	*Data processing and service continuity requirements (downtime elimination time, readiness for disruption, etc.) are established for essential e-services / CII operators by legislation.*
Situation in the country:	✗ No such capacity.

8.4 Essential e-services / CII operators have a cyber security manager

Criteria:	*The essential e-services / CII operators have to appoint a cyber/information security manager.*
Situation in the country:	✗ No such capacity.

III. INCIDENT AND CRISIS MANAGEMENT INDICATORS

9. Capacity to detect and respond to cyber incidents 24/7

9.1 National-level cyber incident response unit

Criteria:	*The government has a unit (common name is CERT, CIRC, etc.) that is specialised in national-level cyber incident detection and response. The unit is responsible for 24/7 data gathering of incidents in cyberspace. The authority manages the comprehensive picture of incidents in national cyberspace.*

Situation in the country:	✓ There is such a capacity.
Reference:	http://cert.gov.ua/?page_id=207
Comment:	Computer Emergency Response Team of Ukraine

9.2 Cyber incidents reporting responsibility

Criteria:	*Public sector entities and CII operators have the responsibility to report about cyber incidents.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://zakon4.rada.gov.ua/laws/show/z0603-08
Comment:	Order of the Administration of the State Service for Special Communications and Information Protection of Ukraine: "The Procedure for coordination of state authorities, local authorities, military units, enterprises, institutions and organisations irrespective of ownership on the prevention, detection and elimination of consequences of unauthorised actions concerning state information resources in information, telecommunications and information and telecommunications systems"

9.3 Official format for practical public-private cooperation

Criteria:	*There is an official cooperation format (organisation, association, etc.) for operational (practical) public, private and third sector cooperation. Activities are specified in the legislation, agreement or in another official format.*
Situation in the country:	✗ No such capacity.

9.4 Exchange of classified information

Criteria:	*According to legislation, public, private and third sector entities may exchange classified information.*
Situation in the country:	✓ There is such a capacity.
Reference:	http://zakon3.rada.gov.ua/laws/show/3855-12
Comment:	The Law on State Secrets includes all different organisations.

10. Capacity to manage large-scale cyber crises

10.1 Cyber crisis management plan

Criteria: *The government has established a comprehensive crisis management plan for large-scale cyber incidents. The plan and its different components must be established by legislation.*

Situation in the country: ⊗ No such capacity.

10.2 Cyber security/crisis operations centre

Criteria: *The government has established a permanent national-level cyber security/crisis operations centre. The centre acts as the cyber situation centre and operations staff for the crisis manager.*

Situation in the country: ✓ There is such a capacity.

Reference: http://zakon3.rada.gov.ua/laws/show/n0002525-15

Comment: The Main Situation Centre of Ukraine is established as a permanent national-level cyber crisis operations centre. The centre acts as the cyber situation centre and operations staff for the crisis manager.

10.3 Crisis management exercise with cyber component

Criteria: *The government has conducted a crisis management exercise with a cyber component in the last 3 years.*

Situation in the country: ⊗ No such capacity.

10.4 National-level cyber crisis management exercise

Criteria: *The government has conducted the national-level cyber crisis management exercise in the last 3 years. The main focus of the exercise is the management of large-scale cyber incidents.*

Situation in the country: ⊗ No such capacity.

10.5 Participation in international cyber crisis exercises

Criteria: *The country has participated in an international cyber crisis management exercise in the last 3 years.*

Situation in the country: ⊗ No such capacity.

10.6 Using volunteers in cyber crisis management

Criteria: *The government has established a system for using volunteers in large-scale cyber crisis management. The procedures for using volunteers must be established by legislation.*

Situation in the country: ⊗ No such capacity.

11. Capacity to fight cyber crimes

11.1 Cyber crimes are criminalised

Criteria: *The state has defined cybercrimes and established them by legislation. The regulations are in line with the Council of the Europe Convention on Cybercrime. Law enforcement authorities are obliged to start a criminal investigation if there are sufficient grounds for a criminal offence.*

Situation in the country: ✓ There is such a capacity.

Reference: http://zakon3.rada.gov.ua/laws/show/2341-14/page11

Comment: Criminal Code of Ukraine, Chapter XVI.

11.2 Unit for fighting cyber crime (department, agency, etc.)

Criteria: *The government has the capacity to conduct criminal proceedings for cybercrimes. A government entity has a department or an organisation that is specialised in combating cybercrime. The unit has competence in the following areas: 1) Prevention of cybercrime. 2) Conducting surveillance measures or special investigation techniques. 3) Conducting pre-trial investigations. The role and responsibilities of the units must be established by legislation.*

Situation in the country: ✓ There is such a capacity.

Reference: https://www.cybercrime.gov.ua/
https://www.npu.gov.ua/uk/publish/article/1816252

Comment: The National Police of Ukraine is responsible for:
Protection of human and civil rights and freedoms, defence of society and state interests from criminal attacks in cyberspace;
Prevention, detection, suppression and exposure of cyber crime;
Raising public awareness about security in cyberspace;

11.3 Unit for digital forensics (department, agency, etc.)

Criteria: *A government entity has a department or an organisation that is specialised in digital forensics:*

- *computer forensics*
- *mobile forensics*
- *hardware forensics, i.e. skimmers*
- *software forensics, malware analysis*

The role and responsibilities of the units must be established by legislation.

Situation in the country: ✓ There is such a capacity.

Reference: https://www.npu.gov.ua/uk/publish/article/1816252

11.4 Electronic evidences are regulated

Criteria: *National regulations provide for rules on the collection and use of electronic evidence. General rules on evidence collection and use alike that also cover electronic evidence or a specific regulation on electronic evidence have been accepted.*

Situation in the country: ✗ No such capacity.

11.5 International cyber crimes 24/7 contact point

Criteria: *There is an international contact point for cyber crimes, which operates 24/7.*

Situation in the country: ✓ There is such a capacity.

Reference: https://rm.coe.int/16804b3493

Comment: Department for Combating Cybercrime, Ministry of Internal Affairs of Ukraine

12. Capacity to conduct military cyber defence operations

12.1 Cyber operation planning unit (department, command, etc.)

Criteria: *Military forces have a department or an organisation that is specialised in cyber operation planning. This unit could be part of a general operation planning unit.*

Situation in the country: ✗ No such capacity.

12.2 Cyber operation units

Criteria: *Military forces have a unit that is specialised in cyber operations.*

Situation in the country: ⊗ No such capacity.

12.3 Exercise with a cyber operations component

Criteria: *Military forces have conducted an exercise with a cyber operations component in the last 3 years.*

Situation in the country: ⊗ No such capacity.

12.4 Cyber operation exercise in the last 3 years

Criteria: *Military forces have conducted a cyber operation exercise in the last 3 years.*

Situation in the country: ⊗ No such capacity.

12.5 Participation in international cyber exercise in the last 3 years

Criteria: *The country's military team has participated in an international cyber operation exercise in the last 3 years.*

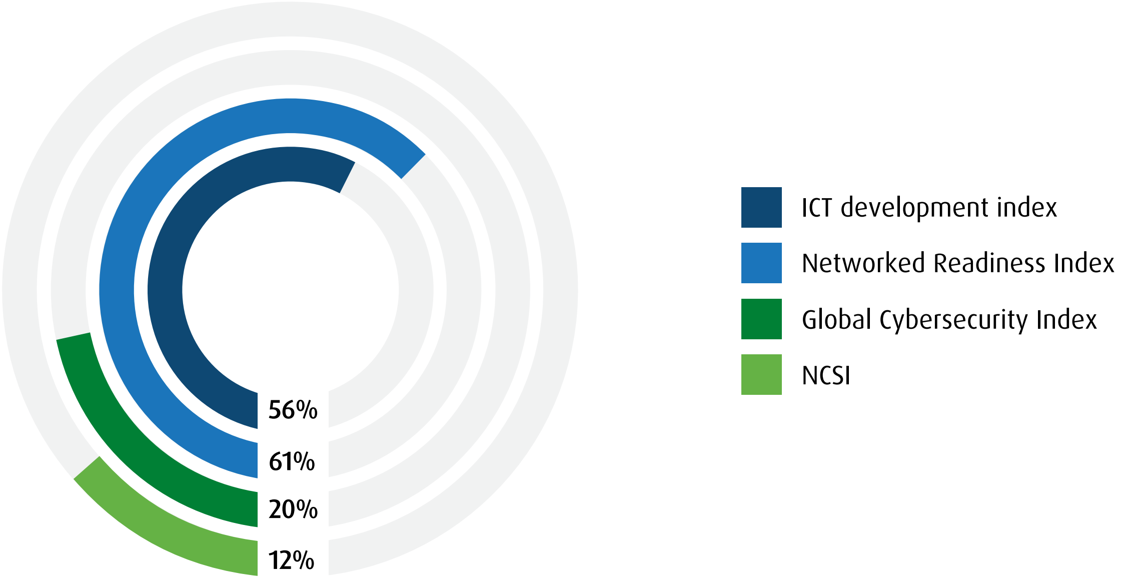
Situation in the country: ⊗ No such capacity.

3. Policy recommendations

Armenia

Regarding the general ICT development, Armenia has fulfilled 56% of the ICT development index (2016). It places Armenia in 71st place in the index. According to the Networked Readiness Index (2017), Armenia has fulfilled 61% of the maximum criteria. It places Armenia in 56th place in the index. Both these indices show that general ICT development in Armenia is above average.

Regarding Cyber Security development, the Global Cybersecurity Index (2017) shows that Armenia has fulfilled 20% of the criteria. It places Armenia in 110th place in the world. Our current study (NCSI) shows that Armenia has fulfilled 12% of the cyber security criteria.



In general, it means the gap between ICT development and cyber security is relatively large. Armenia has paid attention to ICT development, but now it also needs to pay attention to cyber security development.

There is good progress in the area of combating cybercrime where Armenia fulfils 60% of the criteria. Armenia has criminalised cybercrimes, and has a unit for digital forensics and 24/7 contact point for international cybercrime.

Additionally, there has been progress in baseline security development and electronic signature areas. Armenia has a personal data protection authority and a legal framework for electronic signature. Such a positive development should be continued.

In general, it seems that Armenia needs to take a more comprehensive and systematic approach to national cyber security development. It would be good to organise strategic cyber security management first and after that pay attention to sectorial capacity development.

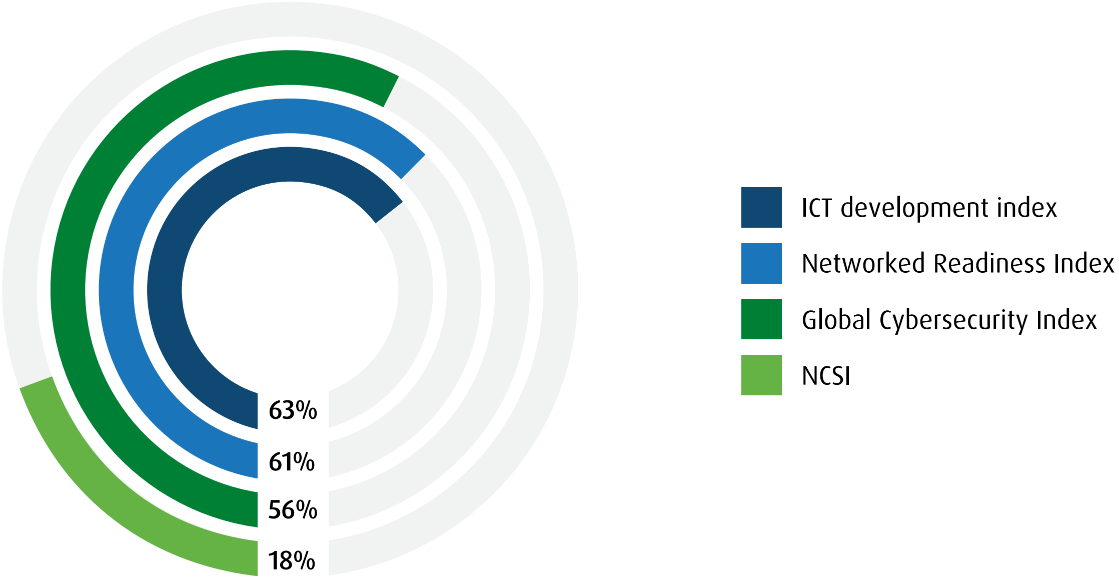
	Percentage of maximum capacity (capacities have different weights)	12.12%
I	GENERAL CYBER SECURITY INDICATORS	
1.	Policy development for the protection of cyberspace	0%
2.	Understanding and analysis of cyber threats	0%
3.	Cyber security education on all levels and professional development	0%
4.	International cooperation in the cyber security field	10%
II	BASELINE CYBER SECURITY INDICATORS	
5.	Cyber and information security baseline standard	27%
6.	Secure environment for e-services	0%
7.	Electronic identification and electronic signature	25%
8.	Protection of essential e-services and critical information infrastructure	0%
III	INCIDENT AND CRISIS MANAGEMENT INDICATORS	
9.	Capacity to manage cyber incidents	0%
10.	Capacity to manage large-scale cyber crises	0%
11.	Fight against cybercrime	60%
12.	National cyber defence capability	0%

Armenia’s cyber security situation according to the NCSI.

Azerbaijan

Regarding the general ICT development, Azerbaijan has fulfilled 63% of the ICT development index (2016). It places Azerbaijan in 58th place in the index. According to the Networked Readiness Index (2017), Azerbaijan has fulfilled 61% of the maximum criteria. It places Azerbaijan in 53rd place in the index. Both these indices show that general ICT development in Azerbaijan is above average.

Regarding the Cyber Security development, the Global Cybersecurity Index (2017) shows that Azerbaijan has fulfilled 56% of the criteria. It places Azerbaijan in 48th place in the world. Our current study (NCSI) shows that Azerbaijan has fulfilled 18% of the cyber security criteria.



In general, it means a gap between ICT development and cyber security exists, and Azerbaijan needs to pay more attention to cyber security development.

There is good progress in the cyber threat analysis area where Azerbaijan has fulfilled 75% of the criteria. Additionally, the electronic identification and electronic signature area is relatively well developed (50%).

From the table, we can also see that there has been some progress in the cyber incident management field (44%), in the international cooperation field (30%), in the cyber security education field (20%), in the field on combating cybercrime (10%) and in the baseline security field (9%).

In general, there are many cyber security areas where Azerbaijan needs to pay attention in order to support good development in the ICT area. It seems that Azerbaijan needs to take a more comprehensive and systematic approach to national cyber security development. It would be good to organise strategic cyber security management first and after that pay attention to sectorial capacity development.

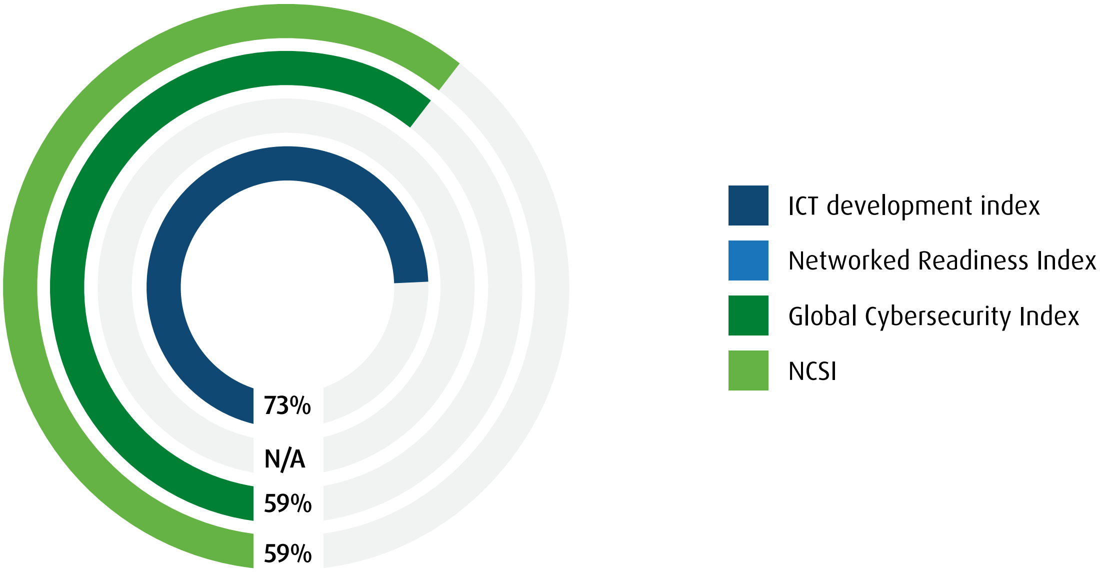
	Percentage of maximum capacity (capacities have different weights)	18.18%
I	GENERAL CYBER SECURITY INDICATORS	
1.	Policy development for the protection of cyberspace	0%
2.	Understanding and analysis of cyber threats	75%
3.	Cyber security education on all levels and professional development	20%
4.	International cooperation in the cyber security field	30%
II	BASELINE CYBER SECURITY INDICATORS	
5.	Cyber and information security baseline standard	9%
6.	Secure environment for e-services	0%
7.	Electronic identification and electronic signature	50%
8.	Protection of essential e-services and critical information infrastructure	0%
III	INCIDENT AND CRISIS MANAGEMENT INDICATORS	
9.	Capacity to manage cyber incidents	44%
10.	Capacity to manage large-scale cyber crises	0%
11.	Fight against cybercrime	10%
12.	National cyber defence capability	0%

Azerbaijan’s cyber security situation according to the NCSI.

Belarus

Regarding general ICT development, Belarus has fulfilled 73% of the ICT development index (2016). It places Belarus in 31st place in the index. It shows that general ICT development in Belarus is very good.

Regarding Cyber Security development, the Global Cybersecurity Index (2017) shows that Belarus has fulfilled 59% of the criteria. It places Belarus in 39th place in the world. Our current study (NCSI) shows that Belarus has also fulfilled 59% of the cyber security criteria.



In general, cyber security development in Belarus is above average (59% of the maximum). However, taking into consideration that ICT development is much higher (73% of the maximum), more attention needs to be paid to cyber security.

There are four areas where Belarus has 100% capacity. These areas are (6.) secure environment for e-services, (7.) electronic identification and electronic signature, (8.) protection of essential e-services and critical information infrastructure and (9.) capacity to manage cyber incidents.

The less developed areas are (10.) management of large-scale cyber crises, (4.) international cooperation in the cyber security field, and (1.) policy development. Belarus has taken part in an international cyber crisis management exercise, but it lacks the national capacity to manage cyber crises. Additionally, in the international cooperation area, Belarus needs progress. For example, Belarus has not implemented the Council of Europe’s Convention on Cybercrime.

Regarding the cyber policy development, Belarus has a coordination format, but no specialised unit for policy development. Additionally, Belarus lacks cyber security terms and definitions, national cyber security strategy and a national level implementation plan.

In general, the Belarusian cyber security situation is relatively well developed and this good progress needs to be taken further.

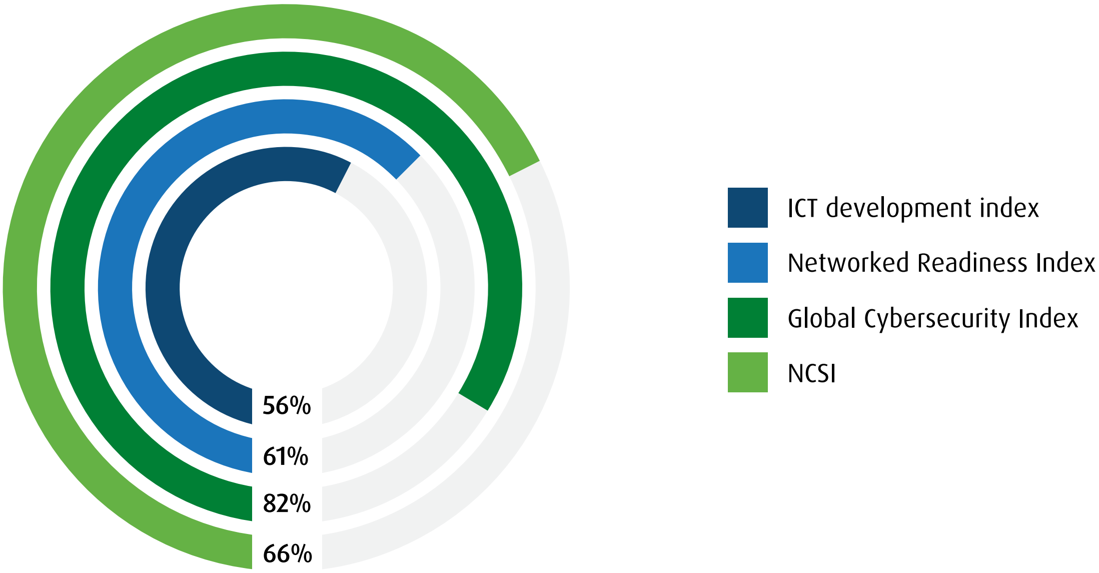
	Percentage of maximum capacity (capacities have different weights)	59.09%
I	GENERAL CYBER SECURITY INDICATORS	
1.	Policy development for the protection of cyberspace	25%
2.	Understanding and analysis of cyber threats	75%
3.	Cyber security education on all levels and professional development	55%
4.	International cooperation in the cyber security field	20%
II	BASELINE CYBER SECURITY INDICATORS	
5.	Cyber and information security baseline standard	55%
6.	Secure environment for e-services	100%
7.	Electronic identification and electronic signature	100%
8.	Protection of essential e-services and critical information infrastructure	100%
III	INCIDENT AND CRISIS MANAGEMENT INDICATORS	
9.	Capacity to manage cyber incidents	100%
10.	Capacity to manage large-scale cyber crises	11%
11.	Fight against cybercrime	60%
12.	National cyber defence capability	60%

Belarus’ cyber security situation according to the NCSI.

Georgia

Regarding general ICT development, Georgia has fulfilled 56% of the ICT development index (2016). It places Georgia in 72nd place in the index. According to the Networked Readiness Index (2017), Georgia has fulfilled 61% of the maximum criteria. It places Georgia in 58th place in the index. Both these indices show that general ICT development in Georgia is above average.

Regarding the Cyber Security development, the Global Cybersecurity Index (2017) show that Georgia has fulfilled 82% of the criteria. It places Georgia in 8th place in the world. Our current study (NCSI) shows that Georgia has fulfilled 66% of the cyber security criteria.



Georgia is one of the few countries where cyber security development is ahead of ICT development. From the cyber security point of view, the situation is very good. Now it is necessary to consider how to balance cyber security development with ICT development.

Georgia has maximum level capacity (100%) in five areas: (1.) policy development, (2.) understanding and analysis of cyber threats, (7.) electronic identification and electronic signature, (8.) protection of essential e-services and critical information infrastructure, and (11.) fight against cybercrime. It is very good that centrally important capacities like policy development and threat analysis have maximum scores. It shows that the potential for balanced security development is high.

Additionally, the (9.) incident management area, (6.) secure environment for e-services, and (5.) baseline cyber security are relatively well developed. Areas that need the most attention are (3.) cyber security education, (12.) cyber defence capability, (4.) international cooperation and influence, and (10.) management of large-scale cyber crises.

In general, we can say the national-level cyber security is very well arranged in Georgia. Despite the fact that there are some areas that need attention, the overall cyber security capacity is well organised in Georgia.

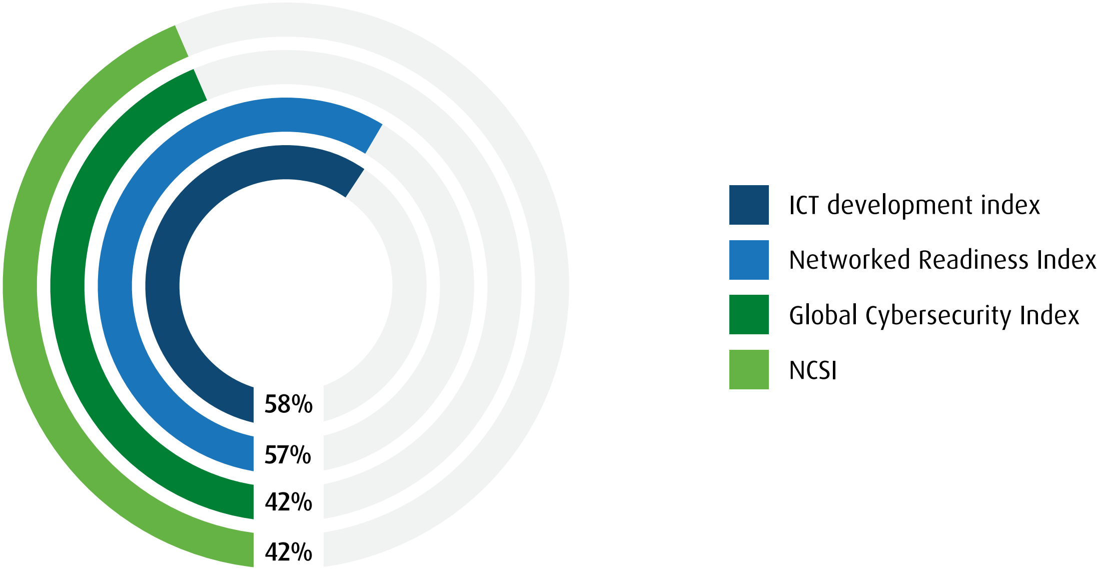
	Percentage of maximum capacity (capacities have different weights)	65.66%
I	GENERAL CYBER SECURITY INDICATORS	
1.	Policy development for the protection of cyberspace	100%
2.	Understanding and analysis of cyber threats	100%
3.	Cyber security education on all levels and professional development	20%
4.	International cooperation in the cyber security field	40%
II	BASELINE CYBER SECURITY INDICATORS	
5.	Cyber and information security baseline standard	64%
6.	Secure environment for e-services	75%
7.	Electronic identification and electronic signature	100%
8.	Protection of essential e-services and critical information infrastructure	100%
III	INCIDENT AND CRISIS MANAGEMENT INDICATORS	
9.	Capacity to manage cyber incidents	89%
10.	Capacity to manage large-scale cyber crises	33%
11.	Fight against cybercrime	100%
12.	National cyber defence capability	20%

Georgia’s cyber security situation according to the NCSI.

Republic of Moldova

Regarding general ICT development, Moldova has fulfilled 58% of the ICT development index (2016). It places Moldova in 68th place in the index. According to the Networked Readiness Index (2017), Moldova has fulfilled 57% of the maximum criteria. It places Moldova in 71st place in the index. Both these indices show that the general ICT development in Moldova is above average.

Regarding Cyber Security development, the Global Cybersecurity Index (2017) shows that Moldova has fulfilled 42% of the criteria. It places Moldova in 72nd place in the world. Our current study (NCSI) shows that Moldova has also fulfilled 42% of the cyber security criteria.



Moldova has made significant developments in the areas of (6.) secure environment for e-services, (7.) electronic identification and electronic signature, and (11.) fight against cybercrimes. In all these areas Moldova has got 100% of the maximum level.

Additionally, baseline cyber security is relatively well developed in Moldova (73% of the maximum). Moldova has a personal data protection authority, legislation for information classification, minimum requirements for cyber security, and requirements for ICT systems' audit. An important capability that Moldova doesn't have at the moment is a responsible authority for cyber security. It is a very important capability that needs to be developed in the near future.

Areas where Moldova has made some progress are (1.) policy development, (3.) education, (4.) international cooperation and (9.) cyber incident management. Moldova has a national programme for cyber security development (strategy) and implementation plan. What is needed in the policy development area is clear management and coordination.

Regarding education, Moldova has a cyber safety website and several public awareness activities. Addi-

	Percentage of maximum capacity (capacities have different weights)	42.42%
I	GENERAL CYBER SECURITY INDICATORS	
1.	Policy development for the protection of cyberspace	38%
2.	Understanding and analysis of cyber threats	0%
3.	Cyber security education on all levels and professional development	30%
4.	International cooperation in the cyber security field	10%
II	BASELINE CYBER SECURITY INDICATORS	
5.	Cyber and information security baseline standard	73%
6.	Secure environment for e-services	100%
7.	Electronic identification and electronic signature	100%
8.	Protection of essential e-services and critical information infrastructure	0%
III	INCIDENT AND CRISIS MANAGEMENT INDICATORS	
9.	Capacity to manage cyber incidents	56%
10.	Capacity to manage large-scale cyber crises	0%
11.	Fight against cybercrime	100%
12.	National cyber defence capability	0%

Moldova's cyber security situation according to the NCSI.

tionally, Moldova has a cyber security programme on the bachelor's level. In the future, Moldova needs to pay more attention to general cyber safety education in schools as well as professional development.

Regarding incident management, Moldova has a 24/7 Government Computer Incident Response Team. At the same time, Moldova lacks a regulation that makes reporting about cyber incidents compulsory. Additionally, Moldova needs to pay attention to the creation of a format for public-private cooperation.

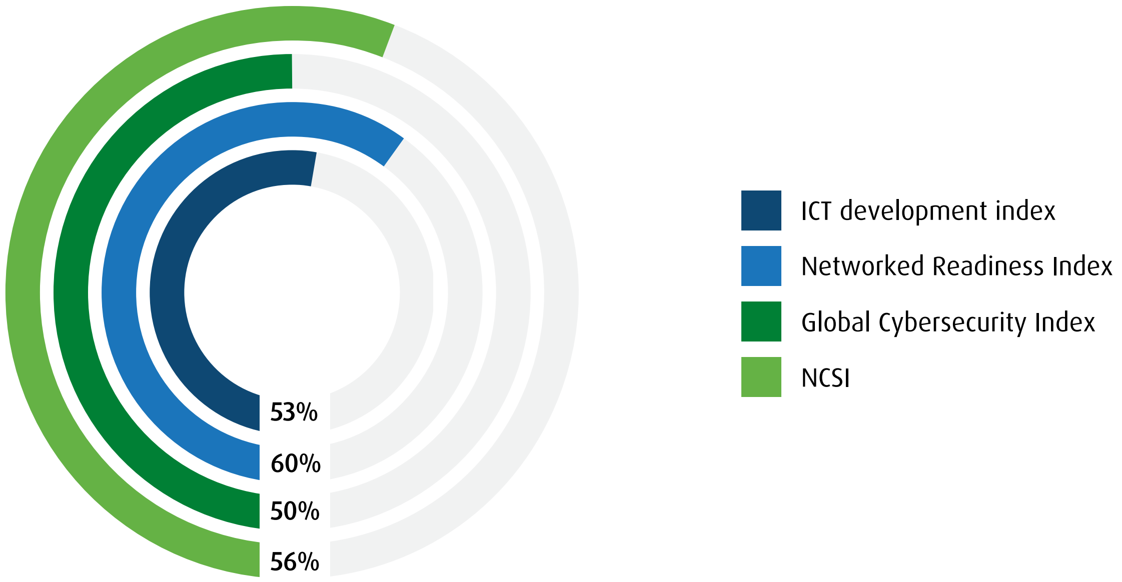
Areas where Moldova needs developments the most are (2.) cyber threat analysis, (8.) protection of essential e-services and critical information infrastructure, (10.) capacity to manage large-scale cyber crises, and (12.) national defence capabilities.

In general, it seems that Moldova needs to take a more comprehensive and systematic approach to national cyber security development. It would be good to organise strategic cyber security management first and after that pay attention to sectorial capacity development.

Ukraine

Regarding general ICT development, Ukraine has fulfilled 53% of the ICT development index (2016). It places Ukraine in 76th place in the index. According to the Networked Readiness Index (2017), Ukraine has fulfilled 60% of the maximum criteria. It places Ukraine in 64th place in the index. Both these indices show that general ICT development in Ukraine is above average.

Regarding Cyber Security development, the Global Cybersecurity Index (2017) shows that Ukraine has fulfilled 50% of the criteria. It places Ukraine in 58th place in the world. Our current study (NCSI) shows that Ukraine has fulfilled 56% of the cyber security criteria.



In general, ICT development and cyber security development in Ukraine are about the same level. From the cyber security perspective, the balance between these areas is good. It should be kept in mind during the information society development.

There are five cyber security capacities that are very well developed in Ukraine. These are (11.) fight against cybercrime, (1.) policy development, (5.) baseline cyber security, (7.) electronic identification and electronic signature, and (3.) cyber security education. In these areas, Ukraine has got 75–90% of the maximum capacity.

The less developed areas are (2.) understanding and analysis of cyber threats, (12.) national cyber defence capability, (4.) international cooperation, (6.) secure environment for e-services and (10.) capacity to manage large-scale cyber crises.

There are many areas where Ukraine needs specific and sectorial cyber security capacity development. Cyber threat analysis and information dissemination among the general public, businesses and the public sector are certainly capacities that need to be taken in focus. It will make society stronger and better prepared for cyber incidents. National cyber defence capacity is another area where significant developments are needed.

	Percentage of maximum capacity (capacities have different weights)	56.06%
I	GENERAL CYBER SECURITY INDICATORS	
1.	Policy development for the protection of cyberspace	88%
2.	Understanding and analysis of cyber threats	0%
3.	Cyber security education on all levels and professional development	75%
4.	International cooperation in the cyber security field	20%
II	BASELINE CYBER SECURITY INDICATORS	
5.	Cyber and information security baseline standard	82%
6.	Secure environment for e-services	25%
7.	Electronic identification and electronic signature	88%
8.	Protection of essential e-services and critical information infrastructure	67%
III	INCIDENT AND CRISIS MANAGEMENT INDICATORS	
9.	Capacity to manage cyber incidents	67%
10.	Capacity to manage large-scale cyber crises	33%
11.	Fight against cybercrime	90%
12.	National cyber defence capability	0%

Ukraine’s cyber security situation according to the NCSI.

General recommendations for the Eastern Partnership Countries

As a general principle, national cyber security capacity development has to be approximately on the same level as ICT development in the country. If a country is interested in information society development, the country has to pay equal attention to cyber security. These areas must be balanced. The following table gives a general overview about EaP countries' ICT development and cyber security development and shows the gap between these areas.

General overview regarding EaP countries' ICT and Cyber Security Development.

% of the maximum level	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
ICT development	58.5%	62%	73%	58.5%	57.5%	56.5%
ICT Development Index	56%	63%	73%	56%	58%	53%
Networked Readiness Index	61%	61%	N/A	61%	57%	60%
Cyber security development	16%	37%	59%	74%	42%	53%
Global Cybersecurity Index	20%	56%	59%	82%	42%	50%
Current Study (NCSI)	12%	18%	59%	66%	42%	56%
Gap						
Gap	42.5	25	14	15.5	15.5	3.5

According to the table, the most balanced situation is in **Ukraine**. The average ICT development percentage is 56.5 and the cyber security average development is 53%. The gap is only 3.5 percentage points.

Georgia is the only country where cyber security development is ahead of ICT development. The ICT development average is 58.5% and the average cyber security development is 74%. The gap is 15.5 percentage points and it favours cyber security.

The following table gives general results of the current study. The dark green colour shows capacities that are completed 50% or more. The light green colour shows capacities that are completed 25-50%. The white colour shows capacities that are completed less than 25%.

General overview of countries' results.

		Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
I	GENERAL CYBER SECURITY INDICATORS						
1.	Policy development	0%	0%	25%	100%	38%	88%
2.	Threat assessment	0%	75%	75%	100%	0%	0%
3.	Education	0%	20%	55%	20%	30%	75%
4.	International cooperation	10%	30%	20%	40%	10%	20%
II	BASELINE CYBER SECURITY INDICATORS						
5.	Baseline security	27%	9%	55%	64%	73%	82%
6.	E-services security	0%	0%	100%	75%	100%	25%
7.	E-ID and e-signature	25%	50%	100%	100%	100%	88%
8.	CIIP	0%	0%	100%	100%	0%	67%
III	INCIDENT AND CRISIS MANAGEMENT INDICATORS						
9.	CIRC	0%	44%	100%	89%	56%	67%
10.	Crisis management	0%	0%	11%	33%	0%	33%
11.	Cybercrimes	60%	10%	60%	100%	100%	90%
12.	National defence	0%	0%	60%	20%	0%	0%

The table indicates areas where EaP countries are doing well and areas that need more attention. We recommend prioritising cooperation areas where EaP countries have common cyber security shortcomings.

According to the results, we can say that the best developed capacities are:

- Baseline security
- E-ID and E-signature
- Computer Incident Response Capacity
- Fight against cybercrime

The less developed areas are:

- International cyber security development and influence
- Cyber crisis management
- National defence capability in the cyber field

More specifically, an overview of EaP countries' cyber security situation is presented in the following table. It gives an overview on YES (x) and NO (-) basis and indicates what specific capacities exist in the countries and what capacities need to be developed.

For example, one of the areas where all EaP countries need capacity-building is cyber security knowledge in primary education. There is a need to teach basic online and computer security aspects to children. Additionally, the table indicates that a professional association for cyber / information security experts exists only in Ukraine. Other EaP countries lack this capacity.

Another area where all EaP countries need capacity development is Cyber Crisis Management. None of the EaP countries have a crisis management plan for large-scale cyber incidents. A Cyber Operations Centre exists only in Ukraine. Cyber crisis management exercises are organised only in Belarus. A couple of countries have taken part in international cyber crisis management exercises. All these aspects indicate that cyber crisis management capacity development should be in focus.

Detailed overview of countries' results.

		Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
I	GENERAL CYBER SECURITY INDICATORS						
1.	Policy development	0%	0%	25%	100%	38%	88%
	Policy development unit	-	-	-	X	-	X
	Coordination format	-	-	X	X	-	X
	Terms and definitions	-	-	-	X	X	-
	Cyber security strategy	-	-	-	X	X	X
	Implementation plan	-	-	-	X	X	X
2.	Threat assessment	0%	75%	75%	100%	0%	0%
	Threat analysis unit	-	X	X	X	-	-
	Annual public reports	-	-	-	X	-	-

3.	Education	0%	20%	55%	20%	30%	75%
	Cyber safety website	-	x	-	x	x	x
	Public awareness-raising	-	x	-	x	x	-
	Primary education	-	-	-	-	-	-
	Secondary education	-	-	x	-	-	-
	Vocational education	-	-	x	-	-	-
	Bachelor education	-	-	x	-	x	x
	Master’s education	-	-	x	-	-	x
	PhD education	-	-	x	-	-	x
	Professional association	-	-	-	-	-	x
4.	International cooperation	10%	30%	20%	40%	10%	20%
	Cooperation unit	-	-	-	-	-	-
	Convention on Cybercrime	x	x	-	x	x	x
	Cooperation agreement	-	x	x	x	-	-
	Internat. representation	-	x	x	x	-	x
	Int. Org. in the country	-	-	-	-	-	-
	Capacity-building	-	-	-	x	-	-
II	BASELINE CYBER SECURITY INDICATORS						
5.	Baseline security	27%	9%	55%	64%	73%	82%
	Baseline security unit	-	-	x	x	-	x
	Data protection authority	x	-	-	x	x	x
	Information classification	-	x	x	x	x	x
	Security standard	-	-	-	-	x	-

	ICT systems' accreditation	-	-	X	-	X	X
	ICT systems' audit	-	-	X	-	X	X
6.	E-services security	0%	0%	100%	75%	100%	25%
	E-services security	-	-	X	X	X	-
	Up-to-date cryptography	-	-	X	-	X	X
7.	E-ID and e-signature	25%	50%	100%	100%	100%	88%
	Unique identifier	-	-	X	X	X	X
	E-services use unique ID	-	-	X	X	X	X
	2-factor authentication	-	X	X	X	X	-
	Electronic signature	X	X	X	X	X	X
	Trust services providers	-	X	X	X	X	X
	E-signature is legal	X	X	X	X	X	X
8.	CIIP	0%	0%	100%	100%	0%	67%
	CII is defined	-	-	X	X	-	X
	Protection unit	-	-	X	X	-	X
	Continuity requirements	-	-	X	X	-	-
	Cyber security manager	-	-	X	X	-	-
III	INCIDENT AND CRISIS MANAGEMENT INDICATORS						
9.	CIRC	0%	44%	100%	89%	56%	67%
	CIRC unit	-	X	X	X	X	X
	Reporting responsibility	-	-	X	-	-	X
	Public-private cooperation	-	-	X	X	-	-
	Exchange classified info	-	-	X	X	X	X

10.	Crisis management	0%	0%	11%	33%	0%	33%
	Crisis management plan	-	-	-	-	-	-
	Operations centre	-	-	-	-	-	x
	Exercise with cyber comp.	-	-	-	-	-	-
	Cyber crisis exercise	-	-	-	x	-	-
	Participation in Int. Ex.	-	-	x	x	-	-
	Usage of volunteers	-	-	-	-	-	-
11.	Cybercrimes	60%	10%	60%	100%	100%	90%
	Criminalisation	x	-	x	x	x	x
	Unit for cybercrimes	-	-	x	x	x	x
	Unit for digital forensics	x	-	-	x	x	x
	Evidence is regulated	-	-	-	x	x	-
	24/7 contact point	x	x	x	x	x	x
12.	National defence	0%	0%	60%	20%	0%	0%
	Cyber Ops planning unit	-	-	-	-	-	-
	Cyber operation unit	-	-	x	-	-	-
	Exercise with cyber comp.	-	-	-	x	-	-
	Cyber Ops exercise	-	-	x	-	-	-
	Participation in Int. Ex.	-	-	x	x	-	-

Focus area #2
E-Democracy: ICTs for Promoting Civic Participation and Transparency of Government Decision-Making Processes

Kristina Reinsalu
Programme Director of E-democracy,
e-Governance Academy

Jelizaveta Krenjova
Expert on E-democracy,
e-Governance Academy

Introduction

The aim of this study report is to provide a review of the state of affairs in the field of e-democracy in the Eastern Partnership (EaP) countries – Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova and Ukraine.

In order to reach our aim, we address the following questions:

- **What are the most prominent developments of the area on the strategic and legislative levels?**
- **What actors play a major role on the institutional level?**
- **How is e-democracy being implemented? More specifically, we look at recent e-democracy initiatives and what can be learned from them. We also examine the actors' perceptions of the drivers and barriers of e-democracy implementation.**

On the basis of this review, we provide policy recommendations on how to overcome the existing barriers and to use the potential of technology for enhancing democratic processes in the EaP region.

The current study has been conducted using **qualitative methodology**. Primary data have been collected via semi-structured interviews with different stakeholders – institutionalised and non-institutionalised civil society representatives (NGOs and civic activists), representatives of state authorities, journalists and bloggers, donors and international experts in the field. We conducted 35 interviews in total (5-6 interviews in each country) with a broad spectrum of various perspectives present in every country mission. Secondary data have been collected relying on public sources, concept papers, international project reports and data gathered through questionnaires (6) addressed to local experts in each country. The questionnaire and the interviews (annexes 1 and 2) were organised along the following topics: main strategies and action plans, legal framework, institutional frameworks/main actors in the field, notable ICT tools and related projects/cases, barriers and driving forces in the development of the field.

Based on previous studies, one of the biggest challenges and barriers in EaP countries for e-democracy and the general development of democracy as such is the level of trust in the government and the immaturity of political and civic culture. To define and describe the essence and reasons for mistrust and fears in civil society, quantitative methods have their limits. Using qualitative data, semi-structured interviews in particular, enables all cultural-social and other factors like fears, mental barriers and enablers behind the existing practices to be understood. This understanding, in turn, helps to design activities needed to boost e-participation and compile recommendations to implement them in order to have a clear impact.

Whereas the emphasis of previous studies of e-governance in the EaP region has been on ICT infrastructure and e-services[1], the current study focuses on how the potential of ICTs has been used to increase the transparency of governmental decision-making, access to public information and the creation of opportunities for citizens to participate in decision-making processes. We were able to identify a similar study on e-democracy in Ukraine (within the EGAP project[2]) using qualitative methods as well (focus group and interviews with different stakeholders). Apart from that, no systematic overviews on the topic were made

[1] *See, e.g. "Harmonisation of the Digital Markets in the Eastern Partnership" (2015). Accessible at: https://europa.eu/capacity4dev/hiqstep/document/harmonisation-digital-markets-eastern-partnership-study-report*

[2] *The policy papers elaborated within the framework of the EGAP project can be accessed here http://egap.in.ua/natsionalna-polityka/*

in the region and, hence, there is no solid comparative study of EaP countries on the topics of transparency and e-participation. At the same time, the area of e-democracy in the region is very dynamic, having numerous new developments, which could constitute good showcases not just for the EaP region, but for all EU countries. Thus, the current review contributes to the knowledge transfer on e-participation and transparency in the EaP region, in Europe and beyond its borders.

It has to be noted that the current focus area of the study has no intention of providing an in-depth comprehensive analysis of the legislative framework concerning general civic participation in decision-making; neither is it aimed at examining the general e-governance architecture in the region, since other studies have already dealt with these research areas (see e.g. CoE 2016; CoE 2017). Likewise, it is out of the scope of this study to provide an overview of all existing ICT tools and platforms in the region. We strive to cover the **variety of initiatives by selecting cases that aim to enhance different democratic values, such as transparency, accountability and participation, as well as cases that were initiated both by civil society actors as well as the government.** We also aim to stress those cases that have had an evident impact and the potential to invoke changes in society based on the perceptions of our partners and interviewees. Acknowledging all the contextual differences in the region, we nevertheless assume that the tools and solutions presented in the report have the potential to be replicated in other countries, that undoubtedly will have to adjust and indigenise them in accordance with their views and needs.

The study report is structured as follows. Firstly, the conceptual framework of e-democracy as a subsection of this introductory chapter is presented: we emphasise the need for a pragmatic approach towards e-democracy. Next, the chapter with findings of the study begins with the brief insights of the e-readiness of EaP countries. This is followed by the subchapter on the legislative framework that identifies the important strategic documents and legislative acts adopted in the realm of e-democracy in the particular country. Here, we turn our attention to the commitments of the countries to the Open Government Partnership[3] as one of the latest multilateral initiatives for promoting open, transparent and responsive governance. Further, an overview of institutional actors playing a major role in developing the area is provided. The variety of e-democracy showcases from each country is presented in subchapter 1.4, while the next part of the report (subchapter 1.5) provides the country reflections with a consolidated overview of important developments in e-democracy based on the aforementioned legislative, institutional and implementation aspects addressed in the previous country subchapters. It also brings into the discussion the actors' perceptions of e-democracy development and implementation in their respective countries. Finally, we examine the barriers and drivers of e-democracy and provide recommendations on what could be done to address the challenges and to enhance the force of the drivers.

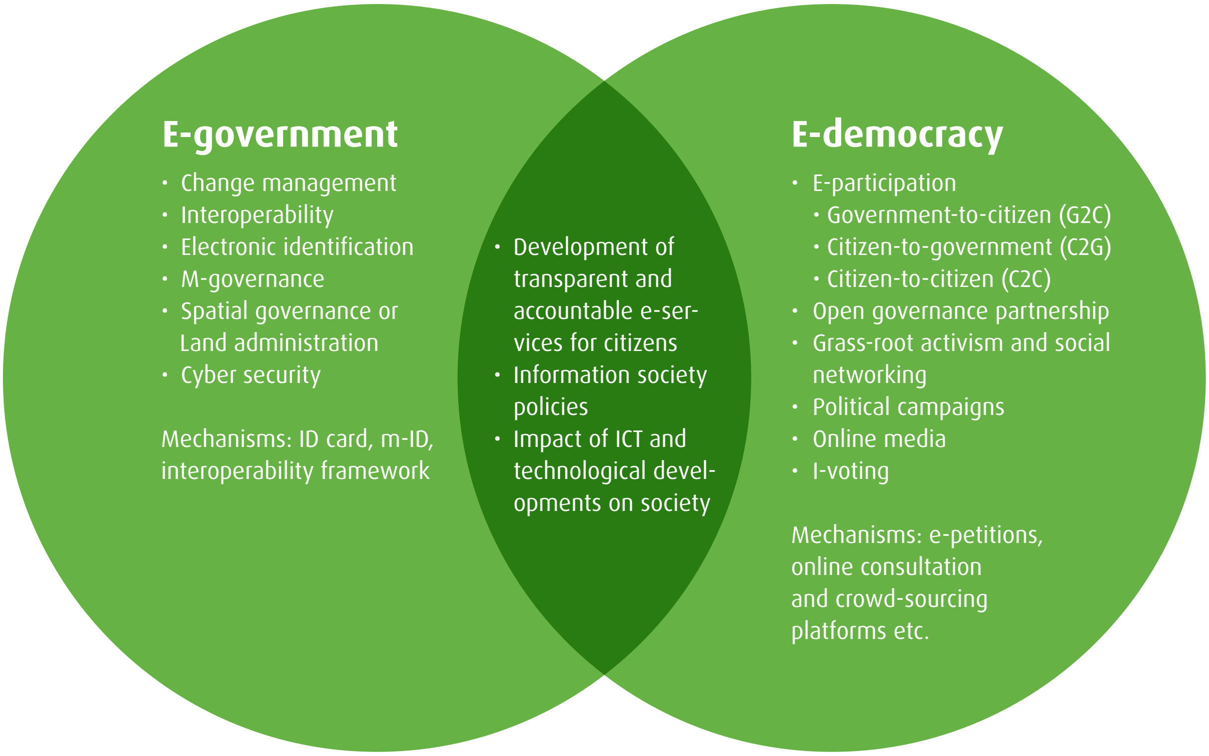
[3] The Open Government Partnership is a multilateral initiative that aims to secure concrete commitments from governments to promote transparency, empower citizens, fight corruption, and harness new technologies to strengthen governance.

Concepts

The essence of e-democracy lies in the support and enhancement of democratic processes and democratic institutions by means of technology. It offers citizens an additional opportunity to participate in political processes.

E-democracy is an integral part of e-governance development and has joint overlapping areas with e-government.

Figure 1.
Integration of e-government and e-democracy


E-government
• Change management
• Interoperability
• Electronic identification
• M-governance
• Spatial governance or Land administration
• Cyber security
Mechanisms: ID card, m-ID, interoperability framework
• Development of transparent and accountable e-services for citizens
• Information society policies
• Impact of ICT and technological developments on society
E-democracy
• E-participation
• Government-to-citizen (G2C)
• Citizen-to-government (C2G)
• Citizen-to-citizen (C2C)
• Open governance partnership
• Grass-root activism and social networking
• Political campaigns
• Online media
• I-voting
Mechanisms: e-petitions, online consultation and crowd-sourcing platforms etc.

The potential of the Internet to enhance democracy and citizen engagement has attracted growing interest from political science, communication and media scholars (Schalken et al., 1996; Hacker and van Dijk, 2000; Musso and Weare, 2005). Proponents of digital democracy have argued that such modernisation boosts democratic and civic participation (Coleman, 1999; Fawkes and Gregory, 2000; McQuail, 2005). Opponents, on the other hand, have claimed that all tools designed to encourage societal and political activism are popular only among a limited number of technology enthusiasts who tend to be politically active anyway, leaving the apathetic untouched (Alvarez and Nagler, 2000; van Dijk, 2000, 2005; Margolis and Resnick, 2000; Wilhelm, 2000; Putnam, 2001). Recently, however, scholars have pointed out some signs of the potential of ICTs to reach the disengaged and bring them closer to society and politics. For instance, this effect is evident on the Internet voting or voting advice applications (Alvarez et al., 2009).

E-democracy does not substitute “offline” democracy, but has great potential to enhance and amplify existing offline democratic processes. Hence, in order to outline the stages of e-democracy, we refer to one of the most commonly used conceptual frameworks of stages of democratic participation, which originates from the OECD report Citizens as Partners

(2001)[4]. It states that democratic political participation should involve the means to be informed, the mechanisms to take part in decision-making and the ability to contribute and influence the policy agenda. If we transfer this concept to the realm of e-democracy, we can refer to the following stages:

- **E-information** (online provision of information): a one-way relation in which government produces and delivers information in its online channels for public use by citizens. It covers both "passive" access to information upon demand by citizens and "active" measures by government to disseminate information to citizens.

- **E-consultation**: a two-way relation in which citizens provide feedback to government using online tools. It is based on the prior definition by government of the issue on which citizens' views are being sought and requires the provision of information.

- **Active e-participation or e-partnership**: a relation based on partnership with government, in which citizens actively engage in the policy-making process via different online-tools. It acknowledges a role for citizens in proposing policy options and shaping the policy dialogue – although the responsibility for the final decision or policy formulation rests with government.

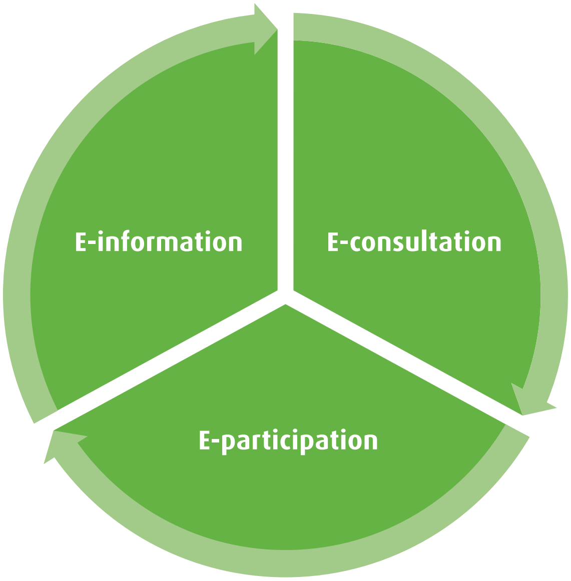


Figure 2. Stages of e-democracy
Source: the authors

In our conceptual framework, we emphasise the pragmatic approach towards the implementation of e-democracy. In contrast to the established normative view of citizen participation (see e.g. Arnstein, 1969), we consider every stage of the participatory conceptual framework presented below as equally important. Hence, in contrast to either pyramid or linear visualisation of the stages of democratic participation, we present them in a circular form (Figure 2), where we see the implementation of these stages as a continuous process: citizens are constantly receiving new information while being consulted or asked for their proposals. The provision of information online (both passive and active) strengthens such democratic values as transparency and accountability, while e-consultation and e-partnership strive to engage citizens in the decision-making processes serving the value of citizens' participation. We consider the concept of e-partnership as the most suitable one to reflect the outcomes of citizens-government collaboration, where both parties are equal partners searching for the best solutions for the challenges of modern societies.

In the current study, we look at the development of e-democracy in the region through the prism of the conceptual framework presented above. We look at e-information, e-consultation and e-participation processes between governments and NGOs or individual citizens that serve the democratic values of transparency, accountability and participation. We leave political online communication (e.g. online campaigning, online media) as a separate area of e-democracy that is out of the scope of this study.

[4] *http://www.internationalbudget.org/wp-content/uploads/Citizens-as-Partners-OECD-Handbook.pdf*

1. Findings

1.1 E-readiness

The assessments of the national governments in terms of readiness and capacity in the realms of e-government and e-participation are prepared by the United Nations every two years in the E-Government Survey. The Survey looks at the progress of 193 countries in the realm of e-government development via the **E-Government Development Index (EGDI)**[5], which measures the readiness and capacity of national administrations to use ICTs to deliver public services. The **E-Participation Index (EPI)** reflects the government's readiness to use ICTs to promote citizen participation. It is a supplementary index to the UN E-Government Survey that focuses on three components: e-information sharing, i.e. provision of information on the Internet; e-consultation, i.e. engaging citizens in contributions to and deliberation on public policies and services; and e-decision-making, i.e. involving citizens directly in decision-making processes (UN E-Government Survey 2016).

It should be stressed that the purpose of EPI is to offer insight into how countries use online tools to promote interaction between citizens and government as well as among citizens. This index does not prescribe any particular practice and, similarly to EDGI, does not constitute an absolute measure of e-participation, but "captures the performance of countries relative to one another at a particular point in time" (UN E-Government Survey 2014, 45). Hence, the comparative ranking of countries serves only illustrative purposes and indicates the broad trends in promoting citizen engagement (UN E-Government Survey 2016).

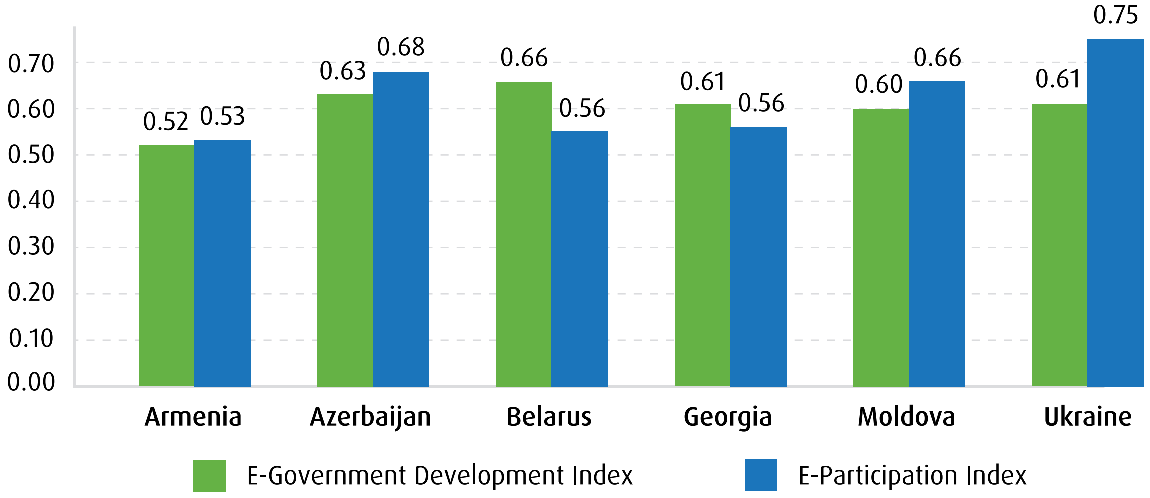


Figure 3. E-Government Development Index (EGDI) and E-Participation Index (EPI) in the EaP Region.
Source: UN E-Government Survey 2016.

[5] *EGDI is a composite indicator based on three important dimensions: the adequacy of telecommunications infrastructure, the ability of human resources to promote and use ICT, and the availability of online services and content (UN E-Government Survey 2016)*

	E-Government Development Index (2014)	E-Government Development Index (2016)	E-Participation Index (2014)	E-Participation Index (2016)
Armenia	61	87	59	84
Azerbaijan	68	56	77	47
Belarus	55	49	92	76
Georgia	56	61	49	76
Moldova	66	65	40	50
Ukraine	87	62	77	32

Table 1. Rankings based on UN E-Government Development and E-Participation Indices from 2014 and 2016.

Acknowledging all the nuances of the measurement of e-participation, it is worth outlining some of the general trends that the data demonstrate. As Figure 3 and Table 1 indicate, Ukraine has made outstanding improvement in the e-participation ranking (moving from 77th to 32nd place in the EPI). It also has the highest e-participation index in the EaP region (0.75). Furthermore, according to the data, Azerbaijan and Belarus have also advanced their positions in both indices, whereas Georgia and Armenia are likely to face challenges. Moldova has performed relatively stably in the EGDI but had a slight decline in the EPI.

While international rankings can encourage countries to strive towards demonstrating better results, it is also essential to have the national capacity to analyse the country's performance in the development of e-governance. Hence, the situation review attempted to identify the national surveys conducted on e-readiness in different EaP countries and organisations in charge of conducting these surveys.

In **Armenia** the Ministry of Transport, Communication and Information Technologies publishes the yearly report of "Communication and Information Telecommunications Technology Indicators according to the Guidelines of the International Telecommunication Union (ITU)". In 2012, the Government approved the template of necessary information and indicators with regards to the recommendations and requirements of various international organisations[6]. In **Moldova**, the e-Government Centre is the institution in charge of the implementation of the E-government Agenda. It conducts regular surveys and assessments related to e-readiness for particular public services. However, it does not conduct comprehensive e-readiness surveys on the country level. In **Azerbaijan**, the focus is on the assessment reports and national index to measure the availability of some e-participation components (e-information, e-consultation) in the public service delivery. For instance, the Open Public Information Index developed by the Multimedia İnformation Systems and Technology Centres focuses largely on the e-information component in public websites of state agencies[7]. Furthermore, the E-development index of state agencies developed by Transparency Azerbaijan (TI) in 2016 focused on five components: "digitalisation" of public services provided by state agencies, development stage of e-services, e-participation level of e-services, e-infrastructure use in e-services, and level of electronic data exchange[8]. **Belarus** refers to the major international indexes on e-readi-

[6] *Among others, these include ICT infrastructure and access indicators, use by households and individuals, use in enterprises, indicators related to ICT use in the education field and others. The full list (in Armenian) is accessible at: mtcit.am*

[7] *The Index is based on the Law on Access to Information and international best practices and measures information openness via 13 indicators, such as contact information, budget, tenders, services and others.*

[8] *See the full report at http://www.transparency.az/alac/E-gov_report_eng.pdf*

ness and uses them as progress indicators in national governmental programs. It is noteworthy that international surveys are also being analysed by independent researches[9]. Both Georgia and Ukraine conduct national e-readiness surveys. In **Georgia**, the survey on the e-readiness was conducted in 2016 by Tetra Tech (the Good Governance Initiative, which is a five-year activity funded by USAID/Georgia). E-readiness Study in Georgia[10] is a nationwide survey with the objective of understanding the degree of "e-readiness", to which individuals and households are ready, willing or prepared to take advantage of the benefits that arise from the use of ICT. In **Ukraine**, all major surveys were conducted by professional private sociological firms or think tanks. These include a nationwide survey conducted in February 2015 by the Kiev National Institute of Sociology[11] that was devoted exclusively to e-governance and e-democracy. A national public opinion poll carried out in November 2015 by the Razumkov Centre[12] also included a module on e-petitions. An expert survey (of the six stakeholder groups in civil society, business, central and local authorities, academia, youth, and the media) was conducted in November 2015 by the Centre for Innovations Development[13], to illuminate e-governance and e-democracy awareness. Furthermore, a nationwide omnibus survey was conducted in February 2016 by the Kiev National Institute of Sociology[14] and had several questions on Internet usage.

In view of the above, we would like to encourage all countries in the EaP region to conduct comprehensive e-readiness/e-governance surveys on the national level in order to have the internal capacity to evaluate a country's performance and gain sustainability in measurement activities.

[9] *See, for instance, following publications (in Russian): «На пути к электронному правительству в Беларуси». Accessible at: http://sympa-by.eu/sites/default/files/library/policy_paper_e-Government_bipart.pdf «Государственные услуги онлайн: от предоставления информации к электронному правительству». Accessible at: http://sympa-by.eu/sites/default/files/library/book-4_final.pdf and «E-участие как инструмент инклюзивного государственного управления». Accesiible at: http://sympa-by.eu/sites/default/files/library/gosudarstvennye_uslugi_onlain_ot_predostavleniya_informacii_k_elektronnomu_pravitelstvu_.pdf*

[10] *The full survey is available at: http://www.dea.gov.ge/uploads/E-readiness_ENG2.pdf*

[11] *Kiev International Institute of Sociology. 2015. E-government and E-democracy: What do Ukrainians Think? Accessible at: http://egap.in.ua/biblioteka/e-uryad-ta-e-demokratiya/*

[12] *Centre for Innovations Development. 2015. Public Opinion about e-Petitions in Ukraine. Kyiv.*

[13] *Tomkova, Jordanka, Mariya Boguslav, Natalia Garashenko, Dmytro Khutkyy, Serhyi Loboyko, Olena Pravylo, and Andrii Semenchenko. 2016. E-democracy in Ukraine: Citizens' & Key Stakeholders' Perspectives. Accessible at: http://egap.in.ua/wp-content/uploads/2016/01/07.07.pdf*

[14] *Kiev International Institute of Sociology. 2016. The Dynamics of Internet Usage in Ukraine: February-March 2016. Accessible at: http://www.kiis.com.ua/?lang=ukr&cat=reports&id=621*

1.2 Strategic and Legal Frameworks

This section provides a brief overview of the strategic and legislative frameworks of EaP countries in the field of e-participation and transparency of decision-making processes. It follows the aim of looking at the most prominent developments of e-democracy on the strategic and legislative levels. The main strategies and action plans related to e-governance were examined in order to identify the concrete commitments of national governments to address the interaction with citizens via online-tools. Additionally, the Action Plans of Open Government Partnership were examined focusing on commitments related to citizens' (e)-participation in decision-making and access to public information. In addition to that, the most significant legislative developments were addressed.

Armenia

The civic participation and transparency are addressed in **"The RA Anti-Corruption Strategy and the Implementation Action Plan for 2015–2018"**. The Strategy specifically addresses the formation of a transparent and accountable governance system as an important prerequisite for the prevention of corruption. For achieving the latter – it is important to ensure full access to information. It also stresses the formation of a participatory government system and cooperation with civil society. It highlights the importance of ensuring the sustainable development of communication and continuous dialogue between civil society, governmental bodies and public institutions. Measures to this end include the introduction of certain instruments of e-democracy such as e-surveys, i-voting, and electronic communication channels for collecting suggestions, public opinion, and others. Other actions foreseen by the Strategy concern the provision of electronic services and an electronic system for monitoring public service delivery.

E-governance-related commitments are addressed in the **Armenia Development Strategy 2014–2025**[15], which has actions in the sphere of electronic administration. The actions include: mappings of databases, creating electronic registries and ensuring interoperability between various agencies; they also specify the degree of sensitivity of data (public, disclosed upon request or restricted).

The Law on Freedom of Information[16], which is applicable on national, regional and local levels, covers institutions supported by the state budget and other organisations of public importance and their officials. According to this law, the information holder has to publish the information related to his activity at least once a year, such as services provided to the public, budget, list of personnel, recruitment procedures, day, time and place for accepting citizens and other information[17]. This information is published "via means accessible for the public, and in cases when the information holder has an internet page, also via that page" (Article 7, 5th clause).

[15] *https://eeas.europa.eu/sites/eeas/files/armenia_development_strategy_for_2014-2025.pdf*

[16] *http://www.foi.am/u_files/file/legislation/FOIeng.pdf*

[17] *See the full list in the Law on Freedom of Information, Article 7. "Ensuring Information Access and Publicity"*

Since **the adoption of the Government Decision on Minimum Requirements of Official Government Websites**, all websites of state bodies should include a section on policies and legislation, news and available public services. Before the e-draft.am platform, government decisions, drafts of proposed laws and policies were published after being signed into law. The mentioned platform, **e-draft.am**, is one of the latest commitments of Armenia under the **OGP initiative** (with the portal being launched in February 2017). It accumulates drafts of legal acts allowing for the registered users[18] to get acquainted with the drafts and to present their suggestions, to receive public feedback on them, to get notifications concerning selected areas of interest, and has other functionalities. As the state representative outlined, the order from the prime minister was given to line ministries to actively put all draft legal acts on the portal[19]. Additionally, the interviewee stated that the draft law on e-petitions was being elaborated and discussed[20].

Another recent commitment under the third OGP Action Plan[21] concerned ensuring the transparency and accountability of allocation of grants from the State Budget, which was the suggestion of an active individual participant (not institutionalised civil society). It is worth noting that the third Action Plan was elaborated through **crowdsourcing**: the Armenian Government, with the support of Kolba Innovations Lab of the UN Development Program in Armenia, announced an open call for ideas to contribute to the Action Plan 2016–2018 (see more in section 1.4).

The latest amendments of the **Electoral Code of the Republic of Armenia** (as of 30 June 2016)[22] are worth paying attention to. For transparency reasons the law defines the accessibility of lists of electors (article 13), stating that the list of electors of the Republic of Armenia, except for the cases provided for by the Law, shall be open to the public. During elections of the National Assembly, the Community Councils of Yerevan, Gyumri and Vanadzor, the authorised body shall post the list of electors by electoral precincts 40 days and 4 days before the voting day, on the www.police.am website. Even though the Electoral Code prescribed that the list of voters having participated shall not be published, following the parliamentary elections that took place in April 2017 "the Central Election Commission published scanned copies of the signed voter lists from all PECs, allowing for public checks of those who voted, including those allegedly abroad" (OSCE 2017; 9). Even though this can be seen as a measure to prevent potential fraud, concerns over disclosure of private data should undoubtedly be taken into account[23] (OSCE 2017; CoE 2016).

Azerbaijan

There are no strategies or action plans specifically designed for civic participation in Azerbaijan. However, the **Open Government Action Plan in 2016–2018**[24] can be considered as an action plan comprising the

[18] Registration via e-mail is needed for presenting one's opinion, but is not required for seeing the acts.

[19] The Government decree (1134-N dated 2.09.2016; accessible in Armenian at: https://www.e-gov.am/gov-decrees/item/27861/) made amendments in the Government decision on "The procedure for organisation and implementation of public discussions" (296-N dated 25.03.2010; accessible in Armenian at: http://www.arlis.am/DocumentView.aspx?docID=57300). Due to these amendments in Article 7 and Article 8 the governmental bodies competent in law-making must publish the draft of the regulatory/legal act, justification of adoption of the legal act, as well as other materials at the discretion of the agency along with the invitation to public discussion on the website of the competent authority and on the unified website administrated by the Ministry of Justice. According to the same decree, the Article 9 was also amended providing the provisions for answering the questions and suggestions via a unified platform: the competent authority should approve within two working days the suggestions/recommendations received via unified platform to be visible to the public and the recommendations received via email or mail within 10 working days so all content-related suggestions and recommendations are included in the Summary paper of the draft proposal discussion. For each content-related suggestion and recommendation, the law-making authority provides a conclusion – accepted, accepted partially or has been taken into consideration.

[20] The Law on Public and an Individual Petition is currently at the review and amendments stage. It has been initiated by the Ministry of Justice and was discussed on www.e-draft.am platform. The law has exact provisions for oral, written, individual, collective, double and electronic petitions. Though it is difficult to predict when an electronic platform will be created, there are provisions for submitting the petition electronically or publishing the petition via electronic platforms.

[21] https://www.opengovpartnership.org/sites/default/files/Armenia_NAP3_2016-18.pdf

[22] https://www.ecoi.net/file_upload/1226_1468568887_armenia-electoral-code-as-of-30june2016.pdf

[23] As stated in the Declaration by the European Commission for Democracy through Law (Venice Commission 2016): "A balance needs to be struck between data protection and secrecy of the vote on the one hand and stakeholders' interest in consulting the signed (or stamped) voter lists on the other. The publication of the lists of voters having participated in the elections could be considered as a measure capable of deterring electoral fraud, but it could also be seen as a tool to control or pressure voters, and publishing the list could also have an impact on voter participation."

[24] http://ogp.org.az/wp-content/uploads/2017/02/Action-Plan-final-version-1.pdf

government's commitments in terms of transparency and civic participation. Among the latest commitments in the OGP Action Plan are the following: expansion of public participation; supporting the activities of civil society members; measures in the field of prevention of corruption, improvement of legislation, and others. It has to be pointed out that although the current status of Azerbaijan in OGP is inactive[25], the OGP initiative and the government's commitments **towards Open Government Principles has had a clear effect on involvement in civil society, including e-involvement.** The drafting process of the National Action Plan on Promotion of Open Government Principles for the years of 2016–2018 (NAP 2) lasted for 6 months with inclusive and close involvement of international organisations, civil society organisations, media and state bodies. All stakeholders were informed proactively through multiple channels, including internet pages, NGOs' networks, and radio sessions. It should be noted that besides the interests of NGOs, state bodies and international organisations, the Anti-Corruption Commission also took into consideration the opinions of citizens through radio sessions and they were reflected in NAP 2. According to NAP 2, an "Open Government Partnership Dialogue Platform" was established in 2016 to strengthen the cooperation, communication and partnership among state bodies and civil society organisations and to contribute to further expansion of OGP principles/values in Azerbaijan[26]. The platform is open to any civil society organisation. The Charter Platform and the list of member organisations and state bodies are available on the website of the platform. Additionally, one of the commitments to increase transparency and accountability was the "Electron Monitoring System". The new system simplifies and expedites the submission of progress reports by state bodies tasked with carrying out specific measures under NAP 2 and facilitates reviewing and monitoring by the Anti-Corruption Commission. For example, state bodies through the new e-portal www.ems.gov.az are currently sending progress reports including images, videos and other relevant documents for each specific measure envisaged in NAP 2[27].

Nevertheless, the constitution of Azerbaijan recognises the right of people to launch legislative initiatives if 40,000 signatures of citizens of the Republic of Azerbaijan enjoying suffrage are accumulated. So far, this clause of the constitution has not been used by the people.

Access to public information is coordinated by **Law of the Republic of Azerbaijan on Access to Information**[28]**, Law of the Republic of Azerbaijan on Freedom of Information**[29]**, Law on Information, Informatisation and Protection of Information**[30].

To create legal grounds for the public participation of civil society organisations in policy-making, the **Law on Public Participation**[31] is accepted by the parliament. Despite presenting the detailed list of public participation forms (e.g. public councils, public discussions, public hearings, public discussion of draft legal acts, written consultation, etc.), and declaring that the realisation of public participation in other forms is not limited, the law does not refer to online-environments/tools.

There is no legal act that coordinates **e-participation**; however, according to the aforementioned Law on Public Participation, the Secretariat of the Parliament of the Republic of Azerbaijan should organise public hearings and public discussions on draft laws. For this reason, the Secretariat of the Parliament places all draft laws registered on the special section of the website of the Parliament within 3 days from being sent to a relevant committee. The necessary information to be published in its website is the following: information about the initiator of the draft law; the registration number of the draft law; the committee(s) to which it has been sent; the schedule and location of public hearings, as well as the duration and rules for conducting public discussion; the rules for submitting opinions, remarks, and proposals; and the duration and results of consideration.

The Secretariat of the Parliament also informs the public of the results of consideration of submitted

[25] *https://www.opengovpartnership.org/countries/azerbaijan*
[26] *http://ogp.org.az/index.php/2017/02/10/azerbaijan-creates-government-civil-society-dialogue-platform/*
[27] *https://www.opengovpartnership.org/sites/default/files/Azerbaijan_OGP-full-report_May2017.pdf*
[28] *http://www.stat.gov.az/menu/3/Legislation/information_rules_en.pdf*
[29] *http://www.commission-anticorruption.gov.az/upload/file/Law%20on%20%20freedom%20of%20information.pdf*
[30] *http://www.wipo.int/edocs/lexdocs/laws/en/az/az019en.pdf*
[31] *http://www.commission-anticorruption.gov.az/upload/file/Law%20on%20Public%20Participation.pdf*

opinions, recommendations, and proposals, and publishes the updated draft law after the first and second readings.

Nevertheless, the Law on Public Participation does not contain any specific mandatory requirements to state agencies to promote e-participation tools on its website, such as an e-public discussion platform, etc. For example, there is no mandatory clause to require state agencies or the president to make statements about applications made online. Although citizens can apply to the president online to express their individual and collective concerns, we cannot consider it as an e-petition. Mostly, citizens complain to the President to solve their individual problems, rather than to raise awareness of public problems, and in this case, it would be correct to refer to e-appeals.

Belarus

The strategies providing general guidelines in the area of information society include **the National Strategy of Sustainable Socio-economic Development of the Republic of Belarus 2030**[32]**, the Strategy on the Development of Informatisation in the Republic of Belarus 2016–2022**[33]**, the National Program on the Development of Digital Economy and Information Society 2016–2020**[34]. However, the activities and plans envisaged in the ICT development strategies mostly aim at improvement of infrastructure and governmental interdepartmental communication while civic participation and disclosure of information on the Internet are not vividly addressed.

There are no legal acts specifically focused on coordinating e-participation. Yet, the Presidential Decree of February 01, 2010 **“On Measures to Improve the Use of the National Segment of the Internet”**[35] touches upon the issues of e-participation. The decree stipulates that all state bodies and organisations are required to publish information about their activities on the Internet and regularly analyse the attendance of their websites and take measures to implement the proposals of citizens aimed at improving the operation of these sites.

The Law of the Republic of Belarus on Information, Informatisation and Protection of Information[36] divides all information into “fully accessible” and “restricted” (e.g. professional and state secrets) and regulates relations in the sphere of information exchanges. The Law being adopted in 2008 has replaced the Law on Informatisation dating from 1995. It nevertheless fails to make substantial improvements in the regulation of information exchanges. There is ambiguity in a number of its provisions and its effects on citizens’ information rights have been criticised by the OSCE Representative on Freedom of the Media[37]. The Law entitles the heads of public agencies to limit the dissemination of information at their discretion. Furthermore, the Council of Ministers approved a wide range of limited dissemination information with the resolution “On Official Information of Limited Distribution”[38].

The legislation also provides for the right of citizens and legal entities to apply to state bodies, the implementation of which is regulated by the Law on Appeals of Citizens and Legal Entities[39], the Presidential Decree on Additional Measures for Working with Appeals of Citizens and Legal Persons[40], the Law on the Basics of Administrative Procedures[41] and the Presidential Decree “On Improving Work with the Population”.[42] According to the provisions of **the Law on Regulatory Legal Acts of the Republic of Belarus**[43], citizens eligible to vote can submit their proposals for the adoption of a normative legal act or submit a draft regulatory legal

[32] *http://economy.gov.by/uploads/files/NSUR.pdf*
[33] *http://e-gov.by/zakony-i-dokumenty/strategiya-razvitiya-informatizacii-v-respublike-belarus-na-2016-2022-gody*
[34] *http://www.government.by/upload/docs/file4c1542d87d1083b5.PDF*
[35] *https://portal.gov.by/i/portalgovby/download/ukaz-60.pdf*
[36] *http://pravo.by/document/?guid=3871&p0=h10800455 or http://www.e-belarus.org/docs/informationlawdraft.html (unofficial English translation)*
[37] *For a detailed overview see http://www.osce.org/fom/31227*
[38] *http://www.pravo.by/document/?guid=3871&p0=C21400783&p1=1*
[39] *http://www.pravo.by/document/?guid=3871&p0=h11100300*
[40] *http://pravo.by/document/?guid=3871&p0=p30700498*
[41] *http://pravo.by/document/?guid=3871&p0=H10800433*
[42] *http://www.pravo.by/pdf/2005-7/2005-7(003-005).pdf*
[43] *http://pravo.by/document/?guid=3871&p0=h10000361*

act to state bodies (officials) with appropriate powers. While drafting normative legal acts, the proposals of civil society organisations (CSOs) and citizens should also be taken into account. The procedures governing the right of citizens to propose law or amendments are prescribed by **the Law on the Procedure for the Implementation of Legislative Initiative by Citizens of the Republic of Belarus**[44]. In 2015, the Law was amended with a provision allowing the recovery of procedural costs from applicants in the case of the systematic sending of "unreasonable requests"[45].

Article 33 of the Constitution of Belarus[46] guarantees freedom of opinion, belief and their free expression. Monopolisation of the media and censorship are not allowed. At the same time, legislative acts regulating registration, licensing and media activities introduce restrictions that do not meet the legitimate aims of respecting the rights and reputation of others, protecting state security, public order, health or morality of the population. Additionally, a number of amendments to the law on mass media expands the powers of the Government to ban websites of those deemed harmful to national interests.

The decision of the Council of Ministers regulates the functioning of websites of state bodies, with the aim of providing comprehensive, reliable information. Presidential Decree No. 105 "About the Database of the Republic of Belarus Draft Laws" (24 February 2012) stipulates that texts of draft laws should be placed in the public domain on the portal **pravo.by** (in Belarusian), or **law.by** (in English). This database of draft laws[47] provides access to the texts of draft laws submitted to the Parliament by the subjects of the law initiative, though no interactive dialogue or comments is possible. Furthermore, there is no contextual information about the purpose of the legislative changes, or data and analysis to inform potentially interested parties about the scope and context of the legislation. Additionally, in some instances, the drafts are not made public (e.g. the changes to the draft Electoral Code) (CoE 2016)

Belarus is not a member of the OGP initiative. Also, as stated in the Council of Europe report (2016), there is no general legislation that stipulates standards and procedures of civil society participation in policy-making on national or regional levels.

Georgia

The following strategic documents and action plans are relevant to the area of e-participation and transparency: Public Administration Reform Roadmap 2020 (PAR)[48], the e-Georgia Strategy and Action Plan 2014–2018[49], Georgia Open Government Action Plans, Anti-Corruption Strategy.

The thematic priority "e-participation and open government" of the e-Georgia Strategy is focused on the citizen feedback on e-services, co-design of e-services, open data, and e-participation in decision-making. The e-Georgia Strategy was later incorporated into the Public Administration Reform Roadmap 2020 that foresees the implementation of the Strategy as part of Service Delivery and Accountability policy areas of PAR. PAR states that the implementation of the Strategy and Action Plan is the main measure for the improvement of the e-services system.

PAR also foresaw the implementation of the OGP Action Plan 2014–2015[50] as the main measure for 2015 for the improvement of the situation regarding transparency and accountability in the country. Georgia joined the Open Government Partnership in 2011. The OGP Georgia Action Plan for 2014–2015 included 29 commitments, out of which 9 were not fully completed by 2015[51]. Some of these were included

[44] *http://www.pravo.by/document/?guid=3871&p0=H10300248*

[45] *More regulatory documents available at: https://portal.gov.by/PortalGovBy/faces/oracle/webcentre/portalapp/pages/info/regulatoryDocuы
ments.jspx?_adf.ctrl-state=zn52c1gx4_4&_afrLoop=63923617184266*

[46] *http://www.wipo.int/edocs/lexdocs/laws/en/by/by016en.pdf*

[47] *http://pravo.by/bank-dannykh-proektov-zakonov-respubliki-belarus/bank-dannykh-proektov-zakonov-respubliki-belarus/*

[48] *http://government.ge/files/425_49309_322150_15.07.21-PublicAdministrationReformRoadmap2020(Final)(1).pdf*

[49] *http://dea.gov.ge/?action=news&news_id=47&lang=eng*

[50] *http://www.opengovpartnership.org/sites/default/files/OGP%20AP%20GEORGIA.pdf*

[51] *For a review of the accomplished and non-accomplished obligations for the OGP Action Plan 2014–2015 see https://idfi.ge/en/ogp-2014-2015-action-plan-accomplished-and-non-accomplished-obligations. Additionally, the report published by the IRM (the Independent Reporting Mechanism) about Georgia: https://www.opengovpartnership.org/country/georgia/irm*

[52] *https://www.opengovpartnership.org/countries/georgia/irm*

in the next OGP Action Plan for 2016–2017[52], such as the development of the new **Freedom of Information Law**, implementing a monitoring system for public officials' asset declarations, a new communication channel to connect with the Emergency Centre 112 and two commitments on increasing the transparency of surveillance and procurement data. **The online petition portal "I-Change.ge"**, which was one of the commitments in the OGP Action Plan 2014–2016, was not carried over to the next OGP Action Plan[53]. However, on May 18, 2017, the government approved a decree regulating the use and conditions of the platform and it is planned to be launched soon.

Georgia's OGP Action Plan for 2016–2017 consists of 24 commitments, categorised into five grand challenges[54]: 1) improving public services; 2) increasing public integrity; 3) managing public resources more effectively; 4) creating safer communities; 5) increasing corporate accountability. Some of the commitments worth emphasising include the **"Budget Monitor"** – an interactive platform implemented by the State Audit (Challenge III). Additionally, what remains important is the development of the **Freedom of Information Law** (Challenge II). Even though Georgia has legal provisions on access to information (i.e. there is a special chapter in the General Administrative Code regulating freedom of information procedures), there is a clear need for a modern stand-alone act of freedom for information. There is no oversight authority that would monitor and ensure the enforcement of the corresponding legal provisions. As stated in OECD report (2016) in anti-corruption reforms, in addition to the lack of sufficient training and awareness raising, this impacts the implementation of the right to information in Georgia, which remains low. It is, hence, unfortunate that this commitment of the first OGP Action Plan was not fulfilled. Nevertheless, in the framework of the Action Plan 2016–2017, a special Working Group comprised of the representatives of the Ministry of Justice, Anti-Corruption Council and NGOs was created; the draft law should be presented to the Parliament in December 2017. (CoE 2016; Georgia's Action Plan 2016–2017; OECD 2016)

Based on OGP Action Plan commitments, the Georgian Government adopted the decree **"About the Form of the Electronic Request of Information and Proactive Disclosure of Public Information"**[55] on September 1, 2013. It obliged all agencies under the supervision of the Executive to release information on their activities electronically, free of charge and in easy-to-use, open forms. It also defined the standards for electronic submission of Freedom of Information requests. A list of information to be published proactively was attached to the decree. This list was developed by the civil society of Georgia and was later revised and adopted by the Government. It contains the following types of information to be published by public institutions regularly: general information about the institution, information about the Freedom of Information officers, and associated procedures and regulations, vacancy announcements and the relevant information, procurements, budgets, laws and official documents regarding the activities of the institution, and information on fees, taxes and revenues of the institution. According to OECD report on anti-corruption reforms in Georgia[56] (2016) the introduction of this system was indeed an important reform. Nevertheless, the report outlines that its implementation is uneven as well as there are many public authorities that do to comply with the decree and the standards it sets. Additionally, the open data portal (http://data.gov.ge/) requires a comprehensive legal framework that would ensure that public institutions regularly update datasets in open format.

Apart from the central government, separate OGP Action Plans were adopted by Tbilisi City Hall[57] and the Parliament of Georgia[58].

[53] *The OGP Action Plan 2016–2017 foresees, nevertheless, the implementation of the electronic petitions on the local level (by Zugdidi Municipality)*

[54] *For a good review of commitments undertaken by the Government of Georgia in its 2016–2017 OGP Action Plan see https://idfi.ge/en/review_of_ogp_2006_2017_action_plan_obligations_undertaken_by_georgian_government*

[55] *https://ogpblog.files.wordpress.com/2013/09/decree-of-the-governemnt-of-georgia-219-eng.pdf*

[56] *https://www.oecd.org/corruption/acn/Georgia-Round-4-Monitoring-Report-ENG.pdf*

[57] *For the information on the Tbilisi OGP Action Plan 2017 visit http://ogp.tbilisi.gov.ge/img/original/2016/11/17/Tbilisi_Action_Plan_2017_final.pdf and https://idfi.ge/en/tbilisi_government_approved_2017_action_plan_within_ogp*

[58] *For the information on the Open Parliament Georgia 2017–2018 Action Plan visit https://idfi.ge/en/georgia_2017_2018_parliamentary_openness_action_plan_is_approved and https://idfi.ge/en/recommendations_of_idfi_on_ogp_action_plan_2016_2017*

Republic of Moldova

The main strategy giving general guidelines for the information society in Moldova is a **National Strategy for Information Society Development or Digital Moldova 2020.** It has been mainly inspired by the Europe 2020 agenda and it is based on three main pillars: infrastructure, content and services, accessibility and skills. However, it has to be pointed out that we could not identify many initiatives for raising the skills of using ICT tools of average citizens. Mostly the National Strategy is boosting the IT industry competitiveness.

Moldova has a **Law on Transparency in Decision-making Processes** from 2008[59]. The Moldovan Government also has experience in implementing/managing a National Participation Council; however, it is currently in the renewal process. It was established based on a Government Decree from 2010[60]. In addition to the above, the Government had approved the Strategy for Civil Society Development for 2012–2015, which was actively discussed during the second half of 2016 with different stakeholders. A new strategy has not been approved yet. Nevertheless, it is not yet clear how these regulations contribute to the development of e-participation.

Even though currently there is a legal framework related to transparency in decision-making and engagement of citizens in consultations/decision-making processes as part of the **Law on Transparency in Decision-making Processes**, there are a number of provisions that are still confusing. For example, the Law does not foresee publishing the decisions obligatorily on the websites of the central public administration authorities, along with the announcement about the elaboration of these decisions. There are no other ICT tools/aspects mentioned as part of it. Thus, while the Law is in place, stipulations concerning the use of ICTs are still unclear and vague.

Similarly, the **Law on Access to Information**[61], which exists from 2000, does not envisage any provisions related to disclosure of information via online means. The law clarifies that requests for information can be submitted in written form, without specifying whether they can be submitted online, via email, or by other electronic means.

The major problem, however, is related to the absence of compliance mechanism: there are no "sanctions" for those who do not follow the provisions and there is a lot of interpretation of what and how these laws are to be implemented. The civil society organisations have been raising concerns about the issue for several years now; however, the change does not happen due to a lack of formal mechanisms for keeping the government in compliance with the stipulations of these laws.

Regarding the **OGP Action Plans** and **commitments**, Moldova has already implemented two action plans on open government. The second action plan (for 2014) placed more emphasis on citizen engagement and transparency in decision-making through its commitment to elaborate a **Citizen Engagement Guide**[62]. This commitment was accomplished and the Guide provides a set of tools and templates for civil servants in implementing the Law on Transparency in Decision-making, in particular. The Guide is available in online-format; and to make it even more user-friendly and "digestible", a short, attractive version of it, the ABC Guide to Citizen Engagement[63], was also elaborated and published (both are available in English and Romanian).

The **Citizen Engagement Guide** was elaborated as part of close cooperation between the Estonian e-Governance Academy, Open Government Institute Moldova and Moldova e-Government Centre[64]. Nevertheless,

[59] *http://lex.justice.md/viewdoc.php?action=view&view=doc&id=329849&lang=2 (available only in Russian and Moldovan)*

[60] *http://lex.justice.md/viewdoc.php?action=view&view=doc&id=333477&lang=2 (available only in Russian and Moldovan)*

[61] *http://lex.justice.md/viewdoc.php?action=view&view=doc&id=311759&lang=2 (available only in Russian and Moldovan)*

[62] *https://sites.google.com/site/citizenengagementguide/home (English version)*

[63] *https://issuu.com/e-Governanceacademy/docs/abc-guide-on-citizen-engagement-eng (English version)*

[64] *The Citizen Engagement Guide was one of the activities of the project "The implementation of principles of Open Government in engaging citizens in decision-making processes in Moldova", financed by the Estonian Ministry of Foreign Affairs in the framework of Estonian Development Cooperation. The project "The implementation of principles of Open Government in engaging citizens in decision-making processes in Moldova" supported and trained the Moldovan Government and civil society to create more open and transparent policy-making and decision-making processes and supported the engagement of civic organisations and individual citizens.*

one of the challenges lies in the very fact that the Guide was not institutionalised, and the government has changed several times ever since it was piloted back in 2015.

Despite the relatively high level of e-readiness of Moldova, there are no separate documents/strategies or papers that would focus on e-participation. That would require a lot of expertise on harmonisation of current legislation and its review from the perspective of the online tools/mechanisms and practices. As stated by our interviewees', currently, the government does not have the capacity or resources to carry out such work.

Nevertheless, it has to be pointed out that in the area of open data, Moldova has made remarkable progress. It is important to mention the **Open Data Methodology**[65] from 2014, which is a new entry point on access to information/data for Moldovan citizens along with the Government Decree from 2014 on Open Data[66]. The e-Government Centre has also done a lot to push the open data agenda forward. Yet, currently the Centre does not have an open data coordinator to work closely with ministries on the disclosure of open data. The portal www.date.gov.md is currently not updated either.

Ukraine

Legislative developments linked to e-democracy in Ukraine can be divided into two periods: pre-2014 with mostly declarative documents with a low rate of implementation and post-2014 with more visible legislative developments[67].

Regarding the first period, one of the milestones was the adoption of **the Law on Access to Public Information** adopted in 2011, which enabled citizens to access public information through government websites as well as obliged state institutions to reply to public queries. Post-2014 among the most prominent achievements were the amendments to **the Law on Access to Public Information** and **Cabinet of Ministers Resolution on the Approval of Regulation on Datasets to be Published in Open Data Format**, which opened more than 300 public registries. The state web portal data.gov.ua was created to host the released datasets. Additionally, in the realm of transparency **the Law on the Open Use of Public Funds**, which obliges all state bodies, organisations and enterprises to publish their expenditures in an open data format at the portal spending.gov.ua. (Tomkova, Konashevych 2016). Furthermore, the legislation on public procurement and online public procurement portal Prozorro was approved in 2015 and was another step towards enhancing transparency. **The Law on Citizens Petitions** could be regarded as a breakthrough in the field of e-participation in Ukraine. Ukrainian citizens could send their petitions online to state bodies on the national as well as local levels[68].

In 2014–2015 a series of policy papers in the field of e-governance were produced, which were mostly setting up the agenda with the e-democracy area being only partially and sometimes indirectly referred to – **the Digital Agenda for Ukraine 2015**[69] (by the Economic Development and Trade Ministry and the State Agency for E-Governance), the **Green Paper for the Electronic Governance in Ukraine**[70] (by a Working Group for the Public Policy on e-governance at the Ministry of Regional Development and Municipal Economies), the **White Paper for the Policy on Electronic Democracy**[71] (by the Strategic Advisory Group on Electronic Governance at the State Agency for Electronic Governance in Ukraine). The 2014–2015 policy papers highlighted some directions, but in practice, the developments were far from systematically planned, but rather unrelated initiatives promoted by

[65] *http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=354534*

[66] *http://lex.justice.md/md/354533/*

[67] *Tomkova, Jordanka, Oleksii Konashevych. 2016. Policy Briefs on Good E-governance. Issue #1: Legislative Aspects on E-democracy in Ukraine. Accessed August 1, 2016 http://egap.in.ua/natsionalna-polityka*

[68] *The legislative aspects of E-democracy in Ukraine have been thoroughly described and analysed in the study by Tomkova and Konashevych (2016).*

[69] *The Economic Development and Trade Ministry. 2015. The Digital Agenda for Ukraine 2015. https://www.slideshare.net/KyivSchoolofEconomics/da-event-ver5-02-042015*

[70] *eTransformation. 2014. The Green Paper for the Electronic Governance in Ukraine. http://etransformation.org.ua/2014/11/17/318/, http://etransformation.org.ua/2014/11/24/355/*

[71] *Mykolaiv City Development Fund. 2015. The White Paper for the Policy on Electronic Democracy. http://www.frgn.mk.ua/wp-content/uploads/2015/11/WB_eDem_1.0.docx*

different authorities and civil society actors.

The upcoming years of 2016–2017 opened up a new phase in e-governance and e-democracy policy-making. The 2016–2017 policy papers are co-authored by wide alliances of actors from civil society, the donor community, academia, business, and authorities. The involvement of the State Agency for Electronic Governance in Ukraine in each of them implies adoption by the Cabinet of Ministers, which would make future initiatives much easier to be implemented. Additionally, their Action Plans include state funding schemes, which, combined with donor grants, should create a bigger pool of opportunities for implementation.

For the development of infrastructural and institutional capacities, in late 2016-early 2017, **the Digital Agenda for Ukraine 2020**[72] was being elaborated. It is promoted by the Economic Development and Trade Ministry, and a wide group of stakeholders from business, civil society, and authorities. In the transparency realm, in early 2017, a debate started around **the Draft Roadmap for the Development of Open Data in Ukraine**[73].

The most recent and the most comprehensive strategic document in the field of e-democracy is the **Draft Concept Paper and the Action Plan for the Development of Electronic Democracy in Ukraine**[74], elaborated by the State Agency for Electronic Governance in Ukraine. This is also one of the commitments of Ukraine for Open Government Partnership. The **Concept Paper** covers the period of 2017–2020, while the Action Plan is targeted for 2017–2018. In March-April 2017 both draft documents underwent a series of open offline[75] and online[76] public discussions for a wide and inclusive deliberation. The document is co-authored by a wide **Coalition for the Advance of e-democracy in Ukraine**, and was adopted by the Cabinet of Ministers of Ukraine in May 2017. It is worth mentioning that a democratically organised multi-stakeholder coalition was created. Authorities, international donors, and civil society organisations productively collaborated for months, producing an elaborate strategic document, framing the development of e-democracy in the country. More detailed information is presented in chapter 1.4

[72] HiTech Office. 2016. The Digital Agenda for Ukraine 2020. https://drive.google.com/drive/folders/0B8Oa6Q2zfKDSN2Q2MnNJd1NXa0U

[73] The Cabinet of Ministers of Ukraine. 2017. On March 10, the Roadmap for the Development of Open Data in Ukraine for 2017 will be Presented. This encompassing document is co-authored and advocated by the State Agency for Electronic Governance in Ukraine, TAPAS Project, and other authors.
Accessible at: http://www.kmu.gov.ua/control/uk/publish/article?art_id=249795642&cat_id=247229066

[74] The Cabinet of Ministers of Ukraine. 2017. Draft Concept Paper and the Action Plan for the Advance of E-democracy in Ukraine. Accessible at: http://www.e.gov.ua/sites/default/files/proekt_koncepciyi_z_e-demokratiyi_.pdf

[75] The State Agency for E-governance in Ukraine. 2017. Regional Public Discussions of the Concept Paper for the Development of Electronic Democracy in Ukraine. Accessible at: http://www.e.gov.ua/content/regionalni-publichni-obgovorennya-koncepciyi-rozvytku-elektron-noyi-demokratiyi-v-ukrayini

[76] E-democracy. 2017. Public Discussion of Draft Laws. Accessible at: http://e-zakon.org/e-dem

1.3 Institutional Framework and Actors

Armenia

While **the Government of Republic of Armenia** and the **Ministry of Justice** are the main actors when it comes to e-governance coordination and implementation of e-government projects. It is worth emphasising that both institutions, the Ministry of Justice of Armenia and Government Staff of Armenia were the pioneers in the experience of **governance innovation**, dedicating a space for ideation and testing for their employees in collaboration with KolbaLab[77] and FutureGov[78]. More specifically, the Pop-Up Innovation Lab gave the opportunity for public servants to explore the process of design and delivery of public services, go into the "user experience" both from the service provider's and consumers' perspectives. After having tested the prototypes of their ideas at the pop-up lab, public servants were more confident in applying to the call for innovative ideas in the public sector, which aimed at optimising working processes, making public services more participatory and ensuring an effective feedback and communication mechanism[79].

Other actors include **the Anticorruption Council**[80], which has the role of developing and ensuring the implementation of an anticorruption policy and strategy in Armenia. E-governance tools are vividly stressed in the policy and strategy developed by the Council. The institution aims to ensure that various agencies cooperate in the implementation of e-tools and, as well as use e-government solutions for transparent operations. Chaired by the Prime Minister of the Republic of Armenia, the Council is composed as follows: Minister-Chief of Government Staff, Minister of Justice, Minister of Finance, Prosecutor General, Chairman of Ethics Committee, representatives from parliamentary opposition parties, President of Public Council and a representative from the Union of Communities. Furthermore, the **Internet Governance Council (IGC)** founded by the RA Government is a multi-stakeholder council that consists of representatives from the Government, private sector, academia, media and NGOs. It is headed by the Deputy Minister of the Transport and Communications and has been formed to find the solutions for emerging challenges of Internet governance in the country.

Furthermore, **EKENG**[81] is the company coordinating e-government projects in the Republic of Armenia. It was founded by the Government of the Republic of Armenia that also owns the shares of the company. EKENG is responsible for implementing e-society projects (incl. the development and progress of e-government) and is the only company in the Republic of Armenia authorised to issue electronic digital signatures to natural people in their ID cards as well as to maintain the ID card system.

Azerbaijan

When it comes to the institutions responsible for e-governance, the conceptual development of public services and electronic services as well as monitoring of implementation thereof is performed by the **State Agency for Citizens Services and Social Innovations** (ASAN). Currently, this institution conducts monitoring of public services and e-services and guides their conceptual development. A presidential decree gives authority to ASAN to evaluate the quality of public services of all state agencies. In this regard, the ASAN Index of public service delivery standards was developed. Based on this evaluation, ASAN provides its recommendations to relevant state agencies. The ASAN Index methodology contains monitoring questions that cover e-information and e-consultation

[77] UNDP's Kolba Lab is an idea incubator. It collaborates with active citizens and government innovators to address big social challenges. Read more at: http://kolba.am/en/page/about-us/

[78] FutureGov is a UK-based Public Sector Innovation Group. Read more at http://www.wearefuturegov.com/about

[79] Read more about this experience here: https://medium.com/@KolbaLab/government-clockmakers-907908709486 and http://kolba.am/en/post/public-sector-innovation-challenge/

[80] http://www.gov.am/en/anti-corruption-strategy

[81] https://www.ekeng.am

components of e-participation. The questions include, for example, the conduct of an online survey, the existence of a social media account, the monitoring possibility of the status of citizen's complaints on the state agency's website, and others.

The Data Processing Centre under the **Ministry of Information and Communication Technologies** serves as a technical operator for the e-government portal and provides technical support for service providers. The Data Processing Centre created a feedback mechanism by which citizens can address its feedback to e-service providers (ministries).

None of the governmental institutions are directly responsible for civic (e)-participation. Nevertheless, the service delivery and feedback mechanism conducted via ASAN service centres are worth emphasising. Although ASAN service centres are not direct actors in the field of e-participation/e-democracy, the mechanisms and tools they use for collecting citizen feedback to improve their service delivery deserve attention and can be used as a good example for other (EaP) countries.

The Azerbaijani Service and Assessment Network, more commonly known as the **ASAN Service**, comprises 'one-stop-shop'-based locations that bring together representatives of various government entities and private companies for citizens and residents who need to access public services. The centre was formed in 2012 to make Azerbaijan's state bureaucracy simpler and more accessible. ASAN's central principle is to place representatives of different government departments "under one roof". Many administrative tasks, from tax registration to driving licence renewal, can be performed at an ASAN Service Centre or via the ASAN website[82].

ASAN regularly seeks feedback from clients. Touchscreens are installed in the centres, so clients can rate the quality of ASAN's services. ASAN also has an innovations department to encourage the generation of new ideas by staff and volunteers. The ideas concern the improvements of the work of ASAN and other state bodies, especially in the provision of electronic services.

Regarding other actors in the field of democracy/e-democracy, **Transparency Azerbaijan** and the **Multimedia Information Centre** promote civic e-participation and transparency tools in public e-service delivery. The Multimedia Information Centre focuses more on the e-information component of e-participation, and Transparency Azerbaijan focuses on the e-consultation aspect of e-participation. For instance, based on the recommendation of TI Azerbaijan, the Ministry of Justice and the Agency for the Protection of Authors Rights established online chat rooms on their websites.

Belarus

The Ministry of Communications and Informatisation of the Republic of Belarus is one of the main actors when it comes to ICTs. However, the Ministry is responsible mainly for infrastructure. **The National Centre of Electronic Services**, which operates under the Operative Analytical Centre, is also an active player in the field. There is no governmental institution responsible for/coordinating civic (e)-participation.

It should be emphasised that **non-governmental actors in Belarus** are active in promoting civic (e)-participation and transparency. These include, for instance, the SYMPA Public Administration Research Centre (School of Young Managers in Public Administration); Office of European Expertise and Communications; Assembly of Pro-Democratic NGOs; the Human Constanta expert team, and others. Some international organisations dealing with the support of civil society initiatives in Belarus state that civic space has become more vibrant and diverse over the years (PACT 2015[83]). Some successful advocacy campaigns as well as improvements in the operation capacity of NGOs are observable. Nevertheless, as the research indicates, the area of advocacy in Belarus is still in the stage of development with a limited number of advocacy campaigns, but has an extensive spectrum of societal questions that they aim to address[84] (Chulitsakaja et al., 2016).

[82] *http://asan.gov.az/az*

[83] *http://www.pactworld.org/news/top-10-belarus-civil-society-2015*

[84] *For extensive and detailed research on the advocacy organisations in Belarus see http://oeec.by/wp-content/uploads/2016/03/Адвокатирование_полная.pdf*

Georgia

The **Government Administration of Georgia** coordinates and plans government policies in terms of e-governance. The Department of Political Analysis, Strategic Planning and Coordination incorporates the following units: The Unit for Governmental Plans and Innovation and the Unit of Electronic Governance. The Government Administration plays the leading role in e-governance coordination.

Next, **the Data Exchange Agency (DEA)**, under the Ministry of Justice of Georgia, is the main institution dealing with e-governance implementation in Georgia. More specifically, it supports the following fields: e-governance development; creation and installation of the unified Georgian Governmental Gateway (3G) as well as its monitoring; establishment of data exchange infrastructure. Setting ICT standards for public sector entities and elaborating information security policies are another of the agency's important responsibilities. Hence, the Agency's core functions are divided into 3 directions: e-governance; data exchange infrastructure; information security. **The Ministry of Justice** coordinates Georgia's anti-corruption policies and involvement in OGP initiatives.

Other governmental stakeholders in the field include the **Public Service Development Agency**, which operates under the management of the Ministry of Justice of Georgia. The function of this Agency is to support the development of its services as well as public services, in general; to introduce innovative services in the public sector; to maintain and constantly improve the registry of citizens and issue-related documents.

Apart from the Government, civil society organisations actively promote new mechanisms for participation. They are members of various councils. For instance, the **Intergovernmental Anti-Corruption Council** coordinates anti-corruption activities in the country, updates and controls implementation of anti-corruption strategy and action plans, controlling and reporting to international organisations, initiating corresponding legislative actions and preparing recommendations. Further, the **Open Government Georgia Forum** is a consultancy mechanism created within the framework of the Anti-Corruption Council. As it is known, the regulations of OGP envisage that working on the Action Plan should be based on support from civil society and through active consultations with broader society, taking into account the existing guidelines and processes. Additionally, the guideline documents consider the necessity of the existence of a coordination and monitoring mechanism on the national level. Georgian CSOs are quite effectively using this opportunity to advocate for developing new tools for holding the government accountable and ensuring civil participation in decision-making processes. Additionally, the **Inter-Factional Group** and the **Open Parliament Georgia Working Group** were created within the framework of the project "Supporting Parliament of Georgia Involvement in Open Government Partnership Initiative"[85]. The goal of these institutions is to support the development of an open parliament and civic participation in the activities of the legislative branch of Georgia.

Republic of Moldova

In Moldova, the **e-Government Centre** and the **Ministry of Informational Technologies** are the national entities in charge of the e-transformation agenda. The e-Government Centre was established in 2010 with the support of the World Bank. The Ministry of Information Technology is developing policies and the e-Government Centre is the implementation agency. Yet, sometimes the Centre also steps in to the field of policies, coordinates some issues and cooperates with the Ministry of ICT in different policies and strategies in the same sector.

Based on the interviews with representatives of the Ministry and e-Government Centre we identified a slight discrepancy between the division of tasks between the Ministry and the e-Government Centre. The Ministry considers the development of IT solutions for other central authorities in terms of better engagement of target audience via consultative approach to be in the competence of the e-Government Centre.

Regardless of the good work of the Moldovan e-Government Centre in coordinating the implementation of

[85] *https://idfi.ge/en/supporting-parliament-of-georgia-involvement-in-ogp*

the E-government Agenda, there is no separate entity mandated with responsibility for e-participation. The Law of Transparency in Decision-making Processes and the Law on Access of Information set the framework for participation and in addition to that, each central public administration authority must have collegiums/committees also involving representatives of civil society. However, in many cases these laws and requirements are functional and implemented only in a few ministries.

The current Public Administration Reform might bring more light to this matter; however, currently there is no separate platform or mechanism for civic participation that any of the central public authorities would be in charge of. Moldova does not have a Ministry of Civic Engagement (as Romania does), or at least a multi-stakeholder forum on open government such as Ukraine, Georgia, and other countries, in which civic participation is encouraged.

When it comes to the National Participation Council, this is a good example of bringing the voice of civil society to the government. Yet, there is a risk of transforming it into a filter. The National Participation Council not represent the entirety of civil society and there should be alternative ways, channels to elaborate and bring the opinion of civil society to the government. As some civil society organisations sense, they are left out of that circle or they do not trust the official engagement process; they search for alternative channels and one of them is the international media.

Ukraine

In the governmental sector **the State Agency for Electronic Governance** in Ukraine plays a major role in e-democracy development. The Agency sees as one of the main achievements in the field the emerged perception and understanding in the governmental sector that this is the priority area. The Concept Paper was initiated as well as developed by the Agency that perceives it as an essential step towards proper planning and implementation of a fragmented field.

Additionally, the cooperation experience with civil society within the framework of **the E-democracy Coalition** is seen as successful and important. The E-Democracy Coalition gathers representatives of NGOs, businesses, donors that were jointly working on the development of the Concept Paper. It is worth noting that NGOs and civil society in general are rather active in Ukraine. Numerous organisations deal with advocacy, agenda-setting, implementation of e-democracy instruments. These include, for instance, the Electronic Democracy Group, Reanimation Package of Reforms, Centre for Innovations Development, Electronic Democracy, Eidos, Podil Agency of Regional Development, Centre of Policy and Legal Reform, Transparency International Ukraine, E-data, CASE Ukraine, the Association of Open Cities, My Voice, Civil Society Online, Social Boost, League of Interns and others.

1.4 E-democracy Showcases

In this section, we provide a variety of e-democracy showcases from all six EaP countries.

In spite of having numerous interesting initiatives in all countries covered by this study, unfortunately, we had to limit the number of selected cases to presenting two initiatives per country. Nevertheless, we tried to cover the variety of initiatives by selecting the cases that are aiming to enhance different democratic values, such as transparency, accountability and participation, as well as cases that were initiated both by civil society actors as well as the government. For a more clarified understanding of the purposes of these different initiatives we categorise all cases into two groups: 1) transparency and accountability; 2) participation; and locate them in a timeline of e-democracy tools (Figure 3). As noted in the conceptual

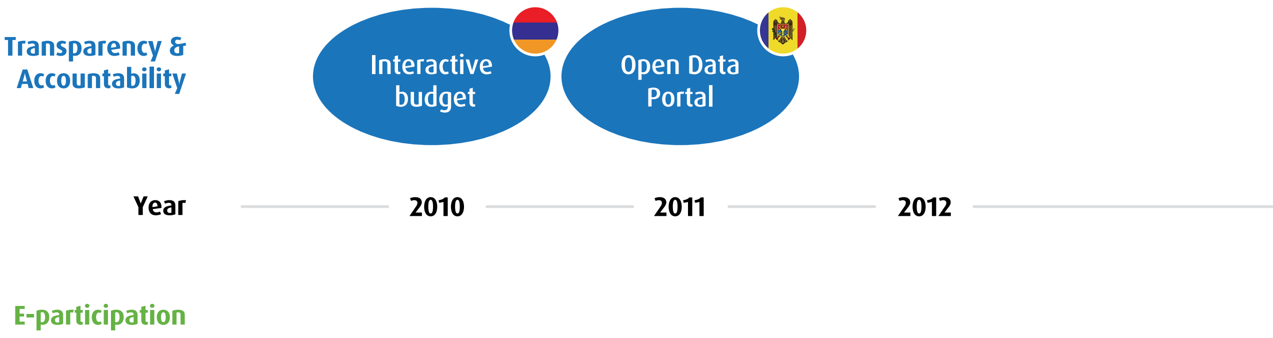
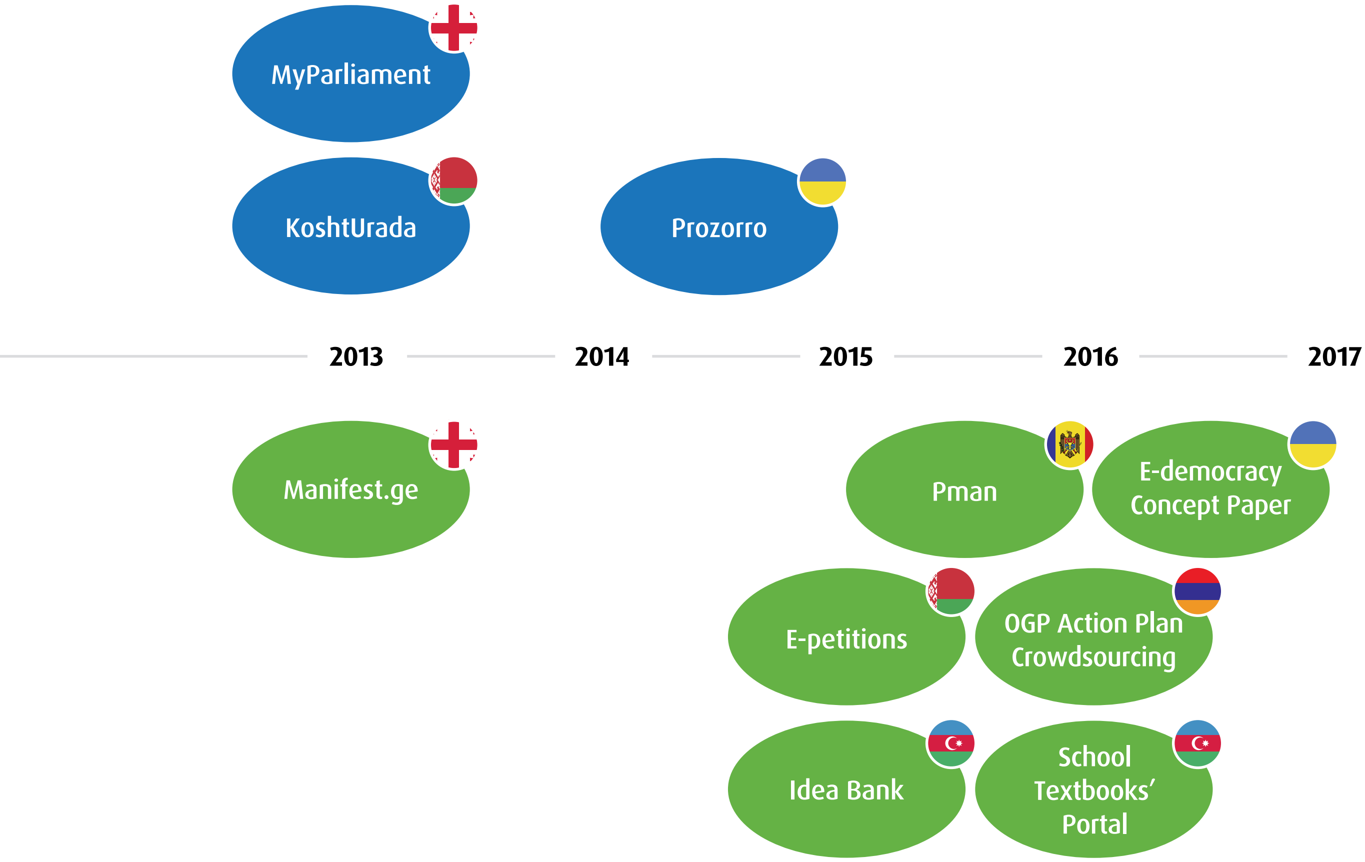


Figure 3. Timeline of e-democracy showcases in EaP region

section of the introductory chapter, the e-information stage of democratic participation strengthens such democratic values as transparency and accountability, while stages of e-consultation and e-partnership strive to engage citizens in the decision-making processes serving the value of citizens' participation.

Our case studies look at the initiatives that aim to engage citizens in deliberations, making proposals and participating in the decision-making. We highlight not only specific e-tools or platforms created, but also processes of e-engagement in the elaboration of a regulatory framework, as well as gathering citizens' ideas for the improvement of public services. We aimed at applying a unified approach in the demonstration of the cases; however, due to their heterogeneity not all aspects were covered equally in each case presented. We, therefore, encourage the actors in each country to work on the elaboration of a thorough and comprehensive overview of the e-democracy tools created in order to build a "menu" of different tools that both civil society and government could use.

We would like once again to express our gratitude to our partners in all EaP countries that provided valuable information on these showcases.



Armenia

The first showcase from Armenia strives to enhance transparency and accountability in the realm of public finance by presenting financial data in a user-friendly manner, while the second demonstrates the engagement practice of citizens in the third OGP Action Plan.

It is also noteworthy that both cases are linked through the OGP initiative: the crowdsourcing of commitments of the third Action Plan resulted in the initiative on the improvement of the Interaction Budget in accordance with open data principles.

Interactive Budget

Functionality: The interactive budget provides information about the yearly budget structure according to the spheres of economy and programs. At any given moment, each citizen can observe how much is spent from the total budget, the direction, purpose and the method (open completion or sole source) of every procurement as well as the remaining amount for the budgetary unit. The interactive budget allows tracking each budget line up until the source of the procurement and the contract. Only information considered sensitive is not included in the budget.

Established: 2010

Statistics: The website www.e-gov.am has on average 45,000 visitors monthly in 2017.

Managing Institution & Team: The Government Staff of Armenia is responsible for the maintenance of the website, but the information in interactive budget is updated simultaneously with data entry by the Ministry of Finance of the Republic of Armenia. Before 2012 the website was developed and administrated by Helix Consulting at the company's own initiative to gather various e-government solutions, including the interactive budget in a single website.

Main achievements: The current version allows citizens to become familiar with the structure of the State Budget – estimated vs actual expenditures in accordance with functional classification via the online electronic interactive budget posted on the websites of the Government and the Ministry of Finance.

Main challenges & lessons learnt: The challenge of the website is linked to the fact that even though it provides users with comprehensive information on the State Budget it is not built upon "open data" principles. The system does not provide users with an opportunity to download the data and process it for their own purposes. The Open Government Partnership Third Action Plan of the Republic of Armenia has an initiative for a "more interactive budget" – ensuring transparency of the State Budget by applying the "open data" principle. Improvement of the system will provide an opportunity to interactively show not only estimated revenues, but also the actual revenue through sources of generation, to make the search for particular data possible by applying relevant advanced instruments (e.g. the distribution of expenditures of the State Budget among state bodies), as well as to make the information machine-readable for further processing by users. It will ensure that the information on the State Budget is user-friendly and will improve transparency of the information on actual expenditures and collected revenues.

Website: https://www.e-gov.am/interactive-budget/

Crowdsourcing the OGP Action Plan

Functionality: The Armenian Government, with the support of Kolba Innovations Lab and UNDP, announced an open call for ideas to contribute to the Action Plan 2016–2018. The crowdsourcing online tool for making proposals to the Action Plan was created with the aim of enlarging the potential contributors regardless of their legal and organisational status. Additionally, a series of public outreach meetings, both in the regions and in the capital, were conducted to engage regional and specialised NGOs as well as to raise awareness about the OGP outside the capital.

Established: Spring 2016

Statistics: As a result of the open call for ideas, 18 proposals were submitted through the online tool and 70 proposals have been received during regional meetings.

Managing Institution & Team: The Armenian Government, with the support of Kolba Innovations Lab and UNDP

Main achievements: Two commitments of the third OGP Action Plan emerged as a result of the regional meetings, where active individual participants made their proposals. One of the commitments aims at ensuring the transparency and accountability of the allocation of grants from the State Budget, while the other was linked to Open Data Standards and Protocols in Armenia and was applied to the interactive budget.

Main challenges & lessons learnt: It is important to think of innovative ways of public engagement and to do things in an unconventional way. Bringing potential individual contributors (in addition to institutionalised civil society) as well as reaching out to the regions raising awareness of the OGP activities was an important step in this direction.

Website: http://ogp.am/en

Azerbaijan

Azerbaijan has remarkable mechanisms and tools for collecting citizen feedback to improve public service delivery. The section below presents cases where the governmental sector interacts with citizens for gaining their vision of its work. In the first case, the State Agency for Public Service and Social Innovation gathers citizens' ideas for the improvement of public services. In the second, the Ministry of Education provides an opportunity for public discussion on the drafts of school textbooks.

The Idea Bank

Functionality: The aim of the Idea Bank is to collect ideas of citizens to improve public services provided by the State Agency for Public Service and Social Innovation (ASAN), including its one-stop shop public service centres. Since March 2015 two other public institutions – the Ministry of Education and State Examination Centre – have joined the portal. Every citizen can send his or her ideas and recommendations to improve the public services of these public institutions. Received ideas fall into three categories: improvement of public services provided by one-stop shop centres (ASAN service centres); improvement of e-services; and general ideas. The state agency gives monetary incentives for the best ideas.

Established: The portal www.ideya.az was created and started to function in 2015; however, the authorities started to gather ideas in 2012 via e-mail and service interfaces.

Statistics: 4545 users have been registered. 5699 ideas have been sent, 2482 out of them have been evaluated, 732 of them have been realised.

Managing institution & team: The State Agency for Public Service and Social Innovation manages the everyday work of the portal. 2 employees are mainly involved in this project. An IT company provides system support to the portal.

Main achievements: Some examples of implemented ideas include the creation of ASAN radio, which aims to disseminate information about public services and to discuss public service-related issues with citizens and public officials; the creation of the "exit poll", where citizens can provide their feedback on ATM in the entrance of ASAN service centres to anonymously express their experience with public services provided. Citizens are asked questions that fall into three categories: waiting in queues; the attitudes of service providers towards citizens; and the ethical behaviour of service providers towards citizens.

Main challenges & lessons learnt: One of the challenges faced during implementation of this process, as stated by ASAN, is linked to encouragement methods for the more active participation of citizens. Nevertheless, it is important to remember for the public authorities that people are the main sources of ideas. Additionally, public institutions should give incentives to citizens to make proposals and, hence, encourage participation through providing certificates or monetary awards.

Website: www.ideya.az

Trims.edu.az Portal – Online Discussion of School Textbooks

Functionality: This portal provides citizens with an opportunity to search for school textbooks by subject, class, author, language or publishing company and to comment on drafts of school textbooks designed in 3 languages (Azerbaijani, Russian, Georgian) for children from 1st to 10th grades.

Established: Since April 2016 all drafts and current school textbooks have been open to public discussion on the tims.edu.az portal.

Managing Institution & Team: The Ministry of Education, Department of Management of Educational Resources is primarily responsible for daily management of the portal.

Main achievements: The transparency that the current portal provided led to an active public discussion on the geography textbook designed for the 10th grade resulting in the religious verses being removed from the text. The discussion that initially derived from the portal was later brought to social media (Facebook), receiving extensive public attention. It was triggered by the fact that the religious (creationist) point of view in explaining the creation of the Earth was presented next to the scientific evolutionary approach. The debate was heated by the fact that students had to prepare a presentation about the creation of the Earth on the basis of verses of the Koran. It was argued by activists that this contradicts the Law on Education, as well as the requirements of the Council of Europe. As a result of this broad public debate, the references to verses of the Koran were removed.

Website: www.trims.edu.az

Belarus

We see the encouragement of the work of institutionalised civil society as an integral part of e-democracy development. We present cases initiated and managed by the civil society sector that aim at enhancing democratic values of citizens' participation in the decision-making processes (online petitions platform) as well as transparency and accountability (Kosht Urada). They also aim at increasing public awareness about citizens' right to voice their concerns regarding the activities and performance of their government.

Online Petitions' Platform – Petitions.By

Functionality: This platform provides citizens with the opportunity to create and sign petitions, discuss them, send messages and submit them to state bodies, whereas the latter is done by the administrating institution.

Established: October 2015

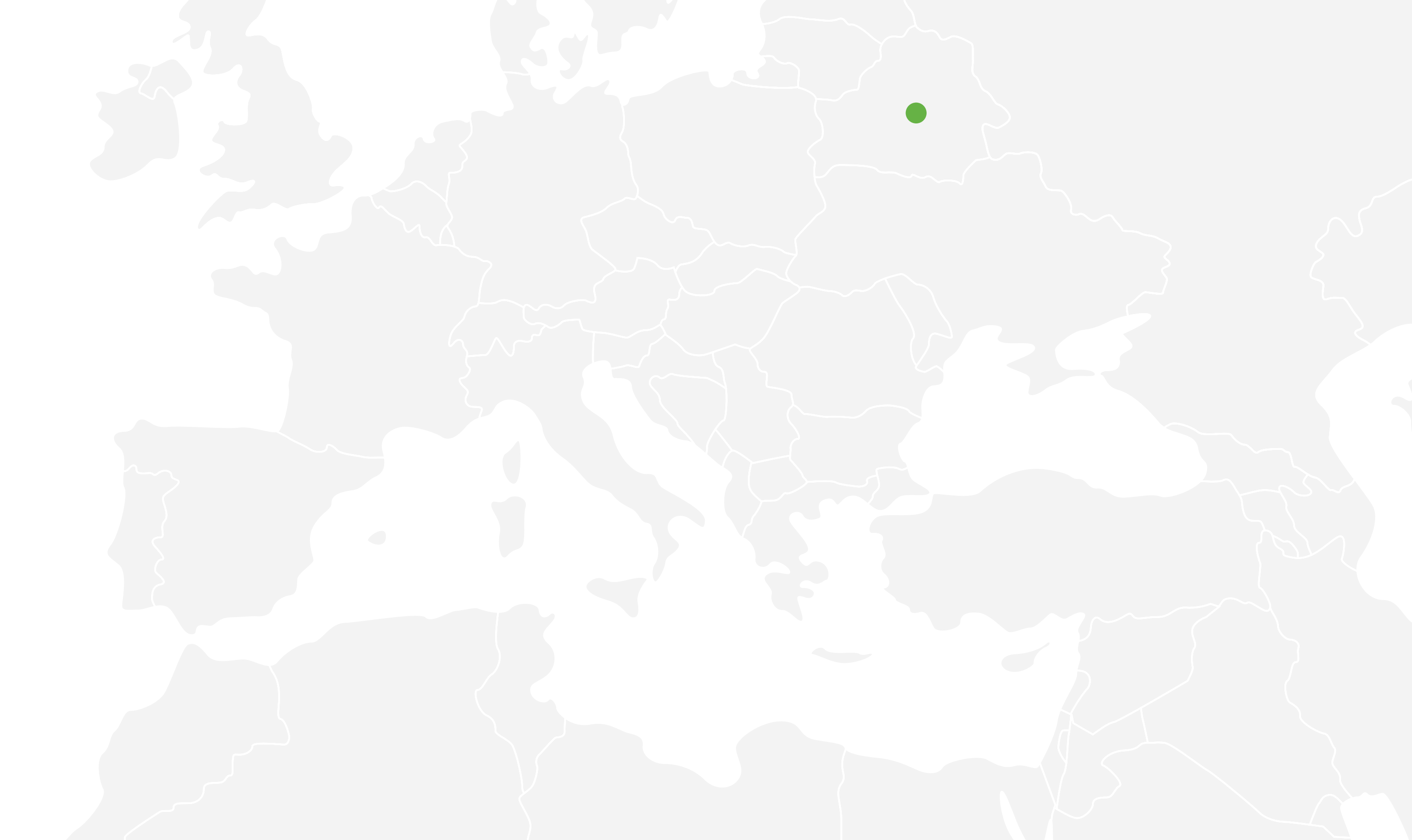
Statistics: The portal has more than 70,000 users

Administrating Institution and Team: The School of Young Managers of Public Administration SYMPA

Main achievements: The users of the portal signed 650 petitions and got 464 responses from state bodies. Some examples of petitions resulting in concrete changes include the case of the disabled people in the city of Minsk who are often faced with the fact that the parking places for their vehicles, in violation of traffic rules, were occupied by cars of non-disabled drivers. As a consequence of the online petition that was created bringing the topic to public attention, the head of the traffic police department initiated a toughening of liability for drivers who illegally occupy parking places intended for the disabled[90].

Website: http://petitions.by/

[90] *See the petition at: https://petitions.by/petitions/138*



Kosht Urada - the Price of the State

Functionality: "Kosht Urada" is the interactive website that shows in a convenient and simple form where money in the state budget comes from and how it is spent. The portal is provided for everyone interested in state finances and, as it says, in the price of the government. The portal provides different opportunities for the user in the form of entertainment to improve his or her understanding of the tax issues in particular and public spending in general. For instance, among many other possibilities, the user can put together a state budget according to his or her preferences and compare it with the real one.

Established: August 2013

Managing Institution & Team: The team of the project BIPART, which is a part of the SYMPA School of Young Managers of Public Administration, aims to make the government more transparent and efficient, and to raise general awareness and understanding of the state finances and work of the government.

Main achievements: About 150,000 visitors, more than 300 publications on budget issues

Website: https://коштурада.бел

Georgia

An important milestone in the Georgian scene of e-democracy is the "comeback" of the e-petitions portal – ichange.ge. We hope this initiative will be functioning in the nearest future. Before that, we present an important non-governmental online petition portal that clearly demonstrates the demand from civil society for this type of e-democracy tool. We also present the transparency-oriented tool on the parliamentary level that enables two-way communication between MPs and citizens and strives to raise public interest about the work of the legislature.

My Parliament – ChemiParlamenti.Ge

Functionality: The website enables any user, without any requirement for registration, to view information about Members of Parliament, which includes their public asset declarations, voting records, background information, professional experience, and attendance statistics. All of the information is presented in a user-friendly manner, in interactive charts/graphs. Moreover, the website allows any user to send a question to any MP. All submitted questions are available and visible on the site and can be easily sorted through. Once an answer has been submitted by the MP, the answer also appears on the website. This openness allows for naming-and-shaming, since it is easy whether the particular MP responds to the questions of the citizens. The website also allows users to subscribe to free text updates. Users can choose which parliamentary committee they are interested in and receive text updates that are composed by Transparency International Georgia's parliamentary team. These text updates enable subscribers to always be in the loop on draft law proceedings and the work of the parliament. Moreover, the website allows the citizens to send their ideas for legislative proposals straight to the parliament. The website automatically generates the required form and allows the citizen to either print the form or have it directly sent to the parliament online.

Established: 2013

Statistics: The site does not require registration, but Google Statistics show an average of 750 unique users per quarter.

Managing institution & team: Parliamentary team of TI Georgia. Three people.

Main achievements: The main achievement was centralising information on MPs that was previously scattered throughout different government websites into one platform, as well as enabling two-way communication between MPs and citizens.

Main challenges & lessons learnt: The main challenge is raising public interest about the work of the legislature, as well as enabling them to have a positive impact on the legislative process. On the other hand, there is also a challenge of fostering political will within the legislature to be more open and accountable to the demands of their citizens. It is recommended to provide information on the activities of the parliament in a timely manner and in an open data format, but that alone isn't sufficient to raise public interest and engagement in the legislative process. It is imperative to support the friendly and interactive display of this information in an effort to ensure easier and more efficient use by citizens.

Website: www.chemiparlamenti.ge

Online Petitions' Portal – Manifest.Ge

Functionality: Internet users can register petitions and collect enough signatures through the platform. Addressees are usually different public institutions.

Established: The domain name was purchased in February 2013. The first version of the website was launched in summer, 2013. The platform was re-branded in March 2015 with the financial support of the Open Society Georgia Foundation (OSGF).

Statistics: Manifest.ge has 7,957 registered users, including: natural people – 7,875; legal entities 34; initiative groups – 48; Newsletter subscribers – 1,603; Number of Petitions registered as of now: 1,435; successful petitions collecting enough signatures: 104. Managing institution & team: Manifest.ge is registered as N(N)LE – a non-commercial legal entity under Georgian law. It is managed by the board. Currently, two people are involved in the everyday work of the organisation/platform.

Main achievements: As the numbers indicate, the platform became quite popular and people are actively using it for collecting signatures of supporters for particular cases. As platform representatives claim, there were several successful cases when the platform helped people to show the need for particular policy changes to decision-makers. For instance, the Tbilisi-based NGO Georgian Centre for Security and Development (http://www.gcsd.org.ge) was successful in raising awareness and voicing the need for regulating safety requirements for milk and dairy products. In general, it is always difficult to claim that particular policy changes were caused by collected signatures; however, this platform became an effective tool for accumulating public support and demand.

Main challenges & lessons learnt: The major challenge the platform managers are facing is connected to a lack of funding. Also, its representatives have claimed that they would like to have better partnerships with other non-governmental organisations, with rich advocacy experience. They would especially like e-signatures to be accepted and promoted in the country. It will further increase the efficiency of the platform, as collected signatures will have legal power. People are actively using particular online tools if they see that there will be an actual result from it. Additionally, there is a demand from society for such kinds of initiatives; however, in some cases, the government is not open to such civic initiatives. Development and promotion of the use of e-signatures is essential for such initiatives to become successful.

Website: https://manifest.ge

Republic of Moldova

In Moldova, most platforms established by the government focus on services rather than providing opportunities for interactive participation in decision-making. For instance, the popular platform https://servicii.gov.md established by the e-Government Centre aims at providing access to existent online public services, but does not have an engagement/interaction component with citizens. The National Platform www.particip.gov.md established by the government is an ambitious one, however, unfortunately, does not boast high participation from the community in terms of providing feedback on laws/decrees and policy

Open Data Portal

Functionality: the portal provides geo-spatial data, cadastre data, public procurement, national statistics, legal acts, business entities registry, crime data, education data, time tables of the national and international auto routes, etc. The portal provides details on data reuse.

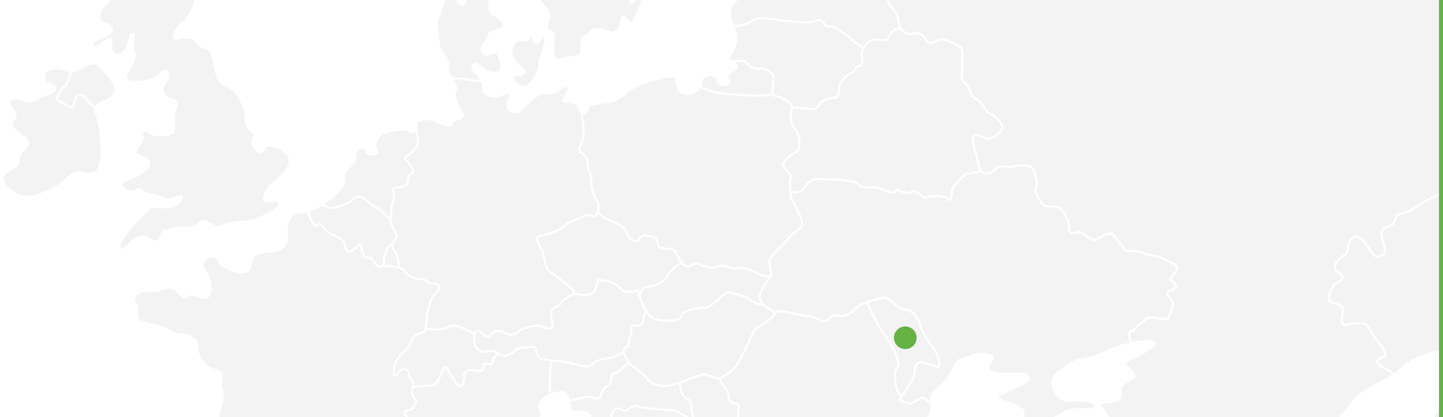
Established: 2011

Administrating institution & team: The State Chancellery starting from 2017 oversees the portal; however, the technical partner is the e-Government Centre, which has been previously the main lead for the portal.

Statistics: 983 data sets (as of August 28, 2017)
Main achievements: Solid legal framework, the key principle embedded in the policy is opening up government data by default. Moldova's open data initiative is guided by three additional key principles: 1) open up primary data in the formats collected from the source, with the highest possible granularity level, disaggregated and unchanged; 2) publish data online, in a timely manner and in automatically processable formats on the open government data portal date.gov.md: 3)protect sensitive data. Other achievements include: around 30 applications developed based on open data from the portal; Moldova with 5th place in the Open Company Data Index; personal data protection remains an integral element in the release of open government data.

Main Challenges and Lessons Learnt: Lack of full ownership for the portal; currently there is no coordinator to update the portal, to work with open data coordinators, to ensure that there is a demand for open data. Open Data became a sort of 'sleeping beauty' and a lot needs to be done to revitalise the initiative and the broader open government agenda.

Website: http://date.gov.md/



papers in general. Nevertheless, as mentioned in the previous subchapters, Moldova has considerable achievements in the realm of open data. Hence, below are presented two substantially different initiatives: an open data portal providing different types of governmental data and the PMAN platform aiming at crowdsourcing project ideas and boosting civic activism. While the former presents something to be further advanced and nurtured, the latter initiative demonstrates the challenges that civil society of Moldova currently faces. Together they aim at building a more sustainable ecosystem of e-democracy in Moldova.

The Crowdsourcing Platform – PMAN

Functionality: This e-democracy platform is in its essence a crowdsourcing platform that allows its users to initiate and develop projects together. The projects need to be of public relevance: for instance, cleaning up an urban space or proposing a legislation reform. The author of the new initiative has the possibility to insert a brief description of the project and to add images, files, statistics, links and to tag other users. The other users have a possibility to comment, vote and add information to the existing proposal.

Established: October 2015

Statistics: The platform has between 350 and 400 users

Managing institution & team: Granat with the support of the Institute for Public Policy (www.ipp.md).

Main achievements: PMAN is a project that focuses on community building and also uses offline activities for this. For instance, VR camps are organised in order to encourage young people to use VR technologies for the creation of social projects in such fields as education, migration, ecology and health. Specific equipment is provided for the teams to work on project development. During the last VR camp, the platform was used to promote the 6 projects developed and their teams.

Main challenges & lessons learnt: One of the main challenges that PMAN initiators faced was the difficulty of the online engagement of people, since most of them are used to interacting via Gmail and Facebook, platforms that are already very familiar to them, and very few step out of these platforms to visit other civic-engagement platforms. For this reason, the presence of PMAN on Facebook is very strong. The PMAN Facebook page has an active community and it serves as the main connecting channel to the general public. However, in order to form online healthy habits of the civic community, firstly, one has to build a healthy offline community. The PMAN team commits to training people, talking to them, working alongside them and afterwards moving to the online sphere. As the initiators underline: “The tool is not the most important instrument, as long as people don’t understand how to use it.” The PMAN team strives to be flexible in the work – organising offline events, managing Facebook communication, proactively promoting the tool and asking for feedback – which gives them the opportunity to grow alongside civil society and to build a community of “doers”.

Website: www.pman.md

Ukraine

The Maidan revolution "pulled the trigger" for civic activism and different civic movements to burst – this is where the kick-start of Ukrainian e-democracy took place and numerous e-democracy programs started to emerge. Today, Ukraine has many successful tools, processes and partnerships; however, there is still low level of public awareness and e-democracy literacy. We present below two outstanding initiatives that both have

Public E-procurement System "ProZorro"

Functionality: ProZorro is a fully online public procurement platform and a collaboration environment that ensures open access to public procurement (tenders) in Ukraine. All of the functionality offered by this online portal is available to the general public without the need to register and without any barriers to access. All public tender information in Ukrainian and procurement announcements in English over certain price thresholds are available on the portal. In this way, ProZorro ensures transparent and efficient spending of public funds by simplifying oversight opportunities for civil society and by enabling enhanced, open competition among businesses that aim to supply goods and services to government entities in Ukraine.

Established: The idea emerged at the beginning of 2014 after the Revolution of Dignity. In February 2015, the first piloting of the system took place. It was fully implemented in 2016.

Statistics: As of August 2017, 1 mln tenders listed, 27,800 purchasing entities. Various statistics available online at bi.prozorro.org/en

Managing institution & team: The system was administrated and maintained by Transparency International Ukraine starting from the pilot and until it was transferred to the government on December 28, 2015. For the moment, it is under the control of the state-owned enterprise ProZorro, which is under the Ministry of Economic Development and Trade Management.

Main achievements: Fully implemented in 2016 as a hybrid system (both centralised public and decentralised private marketplaces), it has since been globally recognised as one of the most innovative public procurement systems delivering government services in a stakeholder-focused, transparent, effective, fair and low-cost way.

Main challenges & lessons learnt: One of the essential challenges was to rebuild trust in the public procurement system in Ukraine. Hence, it was important to invest time and effort into creating a strong brand, organising anticorruption campaigns and demonstrating good practices and showcases. Also, the unwillingness of municipal governments to implement the system was a considerable barrier that the team had to overcome. Having no financial support from the state budget, another challenge that the team had to face was the struggle for finding the resources for IT development, since these costs are frequently not covered by donors' funds. The story of implementation of ProZorro indicates that one can implement something usable and efficient only with three partnerships in place – civil society, business and government should all be involved in the process. Furthermore, it is important to remember that ICTs will not solve problems automatically. Most problems are behind the technological part.

Website: prozorro.gov.ua

partnerships at the core of their success: ProZorro, the Public E-procurement System, and the elaboration of the E-democracy Concept Paper. While the former is now globally recognised as the one of the most innovative procurement systems ensuring maximum transparency, the latter sets an important precedent by collaboratively developing a legal framework for strategic e-democracy development on the national level in Ukraine.

E-democracy Concept Paper

Functionality: The case demonstrates that engaging civil society actors in the elaboration of governmental strategic and regulatory documents can be productive. It also sets a precedent establishing a legal framework and a mandate for e-democracy development on the national level in Ukraine.

Established: From December 2016 till May 2017 in multi-stakeholder format; from June 2017 till August 2017 in the Cabinet of Ministers.

Statistics: Hundreds to thousands of direct users in authorities (75 ministries, 450 cities) and in civil society.

Administrating institution & team: Upon consent and agreement, at different stages representatives of EGAP[86], CID NaUKMA[87], CPLR[88], EIDOS[89], and the State Agency for E-governance led the initiative.

Main achievements: An open, democratically organised multi-stakeholder coalition was created. Authorities, international donors, and civil society organisations productively collaborated for months, producing an elaborate strategic document, framing the development of e-democracy in the country. The participation was open and inclusive, announced online. At the same time, openness was balanced by the requirement to have at least some expertise in the field. Summaries of the meetings were published online with photos of participants and sketches of ideas. The drafted document was discussed with stakeholders offline and online. The hundreds of comments obtained were discussed and incorporated by the core expert group.

Main challenges & lessons learnt: The main challenge in the particular engagement process is linked to ensuring full transparency of the documentary work. The criticism of this practice focused on the detailed follow-ups being available only to the core group as well as providing more clear reasoning behind the acceptance or rejection of the public inputs could have enhanced the accountability of the working group. Additionally, since the decision-making power is vested with the Cabinet of Ministers, amendments of the collaboratively created document might be made. However, the case demonstrates that even in a country with low trust in authorities, it is possible to conduct a multi-stakeholder forum bringing productive results. The combination of expertise from professionals and the wider public, offline and online, can be useful.

Website: http://e-zakon.org/e-dem/

[86] *EGAP is a Swiss-funded Program (2015-19) on E-governance for Accountability and Participation in Ukraine co-implemented by the East Europe Foundation, National Academy for Public Administration under the President of Ukraine and Swiss INNOVABRIDGE Foundation (www.egap.in.ua)*

[87] *The Centre for Innovations Development at National University of Kyiv-Mohyla Academy is working on ideas and projects of sustainable technologies development, and other innovations that are important for finding solutions to key problems of Ukraine and the world. (http://www.ukma.edu.ua/eng/index.php/research/centres/centre-for-innovations-development)*

[88] *The Centre for Policy and Legal Reform is a think tank aiming to root democracy, the rule of law and responsible government in Ukraine (http://pravo.org.ua/en/about/)*

[89] *The Eidos Centre for Political Studies and Analysis is an analytical and resource organisation that sees their mission in the creation of mutual responsibility between the authorities and the citizens of Ukraine. (http://eng.eidos.org.ua/pro-nas/)*

1.5 ICTs at the Service of Democratic Processes: Country Reflections

This subchapter provides a consolidated overview of important developments in e-democracy based on the aforementioned legislative, institutional and implementation aspects addressed in the previous country subchapters. It also brings into the discussion the actors' perceptions of e-democracy development and implementation in their respective countries and provides illustrative quotations from the interviews.

Armenia

The gathered data indicate that the Armenian governmental sector has unique experience in the region in the area of **governance innovation**: public servants were encouraged to provide innovative ideas on how to make government perform better[91]. In the design and delivery of public services it is important to engage directly with the person in order to explore the working process and to see the challenges that he or she faces. It is hence important to see the provision of public services from both perspectives, the provider's and the user's, in order to elaborate well-designed services. In the words of one of our interviewees:

> *"If you are empowering one single citizen, it's such a force that you do not know how it will multiply and how the whole environment will benefit from it. And the same with governance challenges. You find one champion inside the government and then it's catalytic."*
>
> *Civil society representative*

The openness and the willingness of the main actors in the field, **the Government Staff and the Ministry of Justice**, cannot be overestimated here. This is exemplified as well in the fact that the Government of Armenia approached the elaboration of the recent OGP Action Plan in an innovative way, through **crowdsourcing**. Furthermore, one of the latest commitments of the Ministry of Justice under the OGP initiative, the platform **e-draft.am**, has the potential to contribute to participatory law-making processes, provided there will be compliance of the state institutions with the standards set for these processes. In view of these developments, Armenia has the prospects of advancing the e-consultation and e-partnership stages of e-democracy. Whereas the e-information stage and the values of transparency and accountability, exemplified by the budget monitor as well as standards on Minimum Requirements of Official Government Websites, has been well acknowledged.

Nevertheless, one of the challenges that Armenia faces, according to our data, **is the lack of capacity as well as willingness of institutionalised civil society** to use the potential of technologies as well as existing open data in a transformative way. It has been argued that NGOs in Armenia are in the transition period not yet having realised the new era of ICTs and what they enable to do for enhancing democratic processes. The area of **open data** in Armenia requires more in-depth understanding by all sectors of society – not only NGOs, but the IT community as well, which has to be stimulated to be part of the social innovation developments. For instance, analytical tools for the government to use open data for policy-making could be elaborated (such as correlative tools, predictive analysis and others). Additionally, different visualisations of the existing data sets could make them understandable and usable for ordinary citizens. As one of the interviewees clearly stated:

> *"If you have these data, it's a natural resource. /… / it's one of the most expensive things in the modern world. Why don't you use it?"*
>
> *Civil society representative*

Since the realm of open data and transparency that it enables is becoming more and more widespread, a lot of attention has to be paid to the **regulations on data protection**, which is an issue of concern according to our data gathered.

Furthermore, Armenia has a variety of e-solutions; however, with rather low usability. Still **a lot has to be done in the public awareness domain**. Additionally, in terms of initiating or developing new solutions, it is vital to encourage the adaptation and adjustment of these solutions to the local needs, as opposed to "dropping" the solution into society. There should be **a pragmatic tandem between the donor and the government** enabling piloting of new projects before having large-scale implementation.

Azerbaijan

State authorities in Azerbaijan are actively working on the advancement of public service delivery. The **State Agency for Citizens Services and Social Innovations** conducts monitoring of public services and e-services as well as guides their conceptual development in all state agencies. The ASAN INDEX developed by the agency also contains monitoring questions, which cover such components as e-information and e-consultation. However, the analysis of the monitoring results and the outcomes of this process **could be clearer**. Although ASAN service centres are not direct actors in the field of e-participation/e-democracy, the mechanisms and tools they use for collecting citizen feedback to improve their service delivery deserve attention and can be used as a good example for other (EaP) countries.

Despite the relative improvements in the international indices, ranking e-participation in Azerbaijan relatively high, there is **weak legal and institutional mechanism and regulation for e-participation** in Azerbaijan; there are no strategies or action plans designed for civic participation or e-participation. The strategic document that can be considered as the government's commitment in terms of transparency and civic participation is the latest OGP Action Plan for 2016–2018. No legal acts regulate e-participation; the **Law on Public Participation** does not contain any specific mandatory requirements to state agencies to promote e-participation tools on their websites. Nevertheless, most websites of public bodies also publish laws, draft laws on their websites and there is always a comment section. However, a clearer understanding and transparency on what type of feedback is given by citizens is missing. As civil society representatives point out, they are not aware of any discussions on parliament committees, plenary sessions or any other institutions born out of that feedback.

There is **a good model of collecting feedback** from citizens on public service delivery around ASAN, which can be considered as one of the important aspects of interaction between government and citizens; however, this is still mostly the offline service centre. As to e-services, the accessibility and quality of these is still very unsteady. The Ministry of Taxation is in the forefront; the e-services of the Ministry of Social Protection and Labour need to be improved. Hence, on the one hand, ASAN works well as a one-stop-shop for public services, while on the other, the development of e-services is less advanced. During the interviews, some examples regarding the usage of e-services were brought, which indicated that it was still necessary to visit state institutions physically and several times, in particular in the social care sector. This could be avoided with better information society policy design and increased cooperation between different actors involved. This principle is also reflected by a state representative who pointed out:

[91] *For more details, see subchapter 1.4*

> *"Our goal is to move from a "one-stop-shop" to the "non-stop-shop". We are working in this direction."*
>
> *Representative of state authorities*

Yet, it is clear that transformation from offline service delivery to online services requires supportive legal and institutional mechanisms as well as re-design of processes. To quote one of the respondents:

> *"We like to repeat over here that if you are digitalising chaos, you will end up having e-chaos. You have to put everything in order first. /... / This is reflected from our side in the simplification of the public services. If a citizen has to provide the same information and papers in the electronic form, this is unacceptable for us. We try to minimise the requirements for services."*
>
> *Representative of state authorities*

Belarus

The activities and plans envisaged in the ICT development strategies of Belarus mostly aim at improvement of infrastructure and governmental interdepartmental communication while civic participation is not vividly addressed. The topic of **open data**, nevertheless, has its place in the strategic vision and is currently on the governmental agenda. Our interview data indicate that there are plans in the governmental sector **to initiative the unified platform for discussion of draft laws**. This theme is addressed in the National Strategy of Sustainable Socio-economic Development of the Republic of Belarus 2030[92] along with the development of feedback technologies for fostering open dialog with the citizens. At present, the texts of draft laws are placed in the public domain on the portal **pravo.by**, but no interactive dialogue or comments possible, neither is the contextual information about the purpose of the legislative changes present. Also, the regulation of potential public discussions and the feedback mechanism is not addressed on the legislative level (CoE 2016; Volodin, Sushko 2016).

Furthermore, as the research demonstrates, Belarus is successfully advancing its government-centric approach when it comes to the implementation of ICTs: having achievements in the development of infrastructure and state information systems (Sokolova 2011; Sushko 2016). This technocratic approach should be counterbalanced with a citizen-centric attitude towards e-governance.

As mentioned previously, **the Law of the Republic of Belarus on Information**[93], Informatisation and Protection of Information fails to make substantial improvements in the regulation of information exchanges; additionally, its effects on citizens' information rights have been criticised by the OSCE Representative on Freedom of the Media[94]. Nevertheless, it should be noted that the government foresees the need for the revisions of legislative framework in the realm of information society:

> *"We have the Law of Personal Data in the action plan of law-drafting ... and I am sure that when we approve it, we will need to have a drastically different revision of the Law on information, information protection, access to information.../... /. I am sure that in a year we will have to deal in-depth with a totally new version that will take into account the new reality."*
>
> *Representative of state authorities*

Belarus places importance on the work related to citizens' appeals. The interview data demonstrated that e-appeals are considered to be the instrument now widely integrated into society. However, there still remain considerable challenges in the regulation sphere of interactions between citizens and government, in particular, when it comes to the shift of this interaction into the online space (Volodin, Sushko 2016). Also, there is a lack of effective tools of identification and authentication, and the issue of personal data protection is widely acknowledged. In the words of one of the interviewees:

> *"I think that the main spheres where we need certain actions or changes ... starting from personal data protection, and I mean legislation ... because if you do not have regulations of personal data protection, it is really difficult to use any electronic identification and authentication system"*
>
> *Civil society representative*

The tendency is observable that non-governmental actors in Belarus are getting more active in promoting civic (e)-participation and transparency. This sector experiences several successful advocacy campaigns as well as improvements in the operation capacity of NGOs. Nevertheless, as the national research demonstrated (Chulitsakaja et al., 2016) the participation of advocacy organisations in the political process is limited. Although it is possible to practice advocacy at most stages of political processes, the main form of engagement still remains putting forward proposals for solving problems without a guarantee or an opportunity of controlling their adoption. It is important to note that advocacy actors **are mostly excluded from the important stage of decision-making**, which is the least transparent and least influenced. Additionally, one of the important problems in the sphere of advocacy is the lack of transparency of decision-making by different state authorities as well as the fact that civil activists have no or hardly any access to decision-makers. (Chulitsakaja et al., 2016)

Also, according to Chulitskaja et al. (2016), in the studied cases advocacy organisations used ICTs a lot at various stages of campaigns; however, the respondents of this research did not mention ICTs specifically, which might be partially due to the methodology of the research or the underestimation of ICTs as an effective tool for awareness raising and actualisation of their advocacy topic. Using **more intensively traditional and new mass media** in order to promote the topic to the wider audience could be beneficial. Furthermore, the low level of collaboration between actors and low awareness of each other might impose an obstacle in having a bigger impact. It is hence recommended to enhance networking activities and engage the **analytical community** (e.g. experts, researchers, think tanks) in advocacy campaigns. The donors' community, international organisations and development agencies are encouraged to initiate **joint thematic activities for experience sharing and networking**. (Chulitskaja et al. 2016) As argued by one of the respondents:

> *"The dialog between different stakeholders, and by different, I mean agencies, NGOs, groups of activists, business and private sector activists to create a common agenda. And the next thing...social network and petitions become more and more popular. I think it is proper time to start a dialogue about proper services and e-participation, access to legal information and the drafts of laws..."*
>
> *Civil society representative*

Last, but not least, even though the current review is not focusing on local level practices, the experience of Minsk's city administration in collecting citizen feedback on various topics is worth attention. As outlined by several interviewees, **the local level initiatives** might be the best way to approach the advancement of e-participation in Belarus, especially those concerning the sphere of city planning.

Georgia

The e-Georgia Strategy encompasses components focusing on citizen feedback on e-services, co-design of e-services, open data, and e-participation in decision-making. Also, the National Anti-Corruption Strategy and Action Plan prescribes actions related to e-participation, freedom of information and transparency. Additionally, some **OGP commitments** have created good prerequisites for e-participation; however, several worthy initiatives were postponed in fulfilment. The forthcoming **OGP Chairmanship** that Georgia will take over in September 2017 is likely to have contributed to the accelerated very recent developments **in the realm of access to public information as well as online platforms for decision-making**. These developments are very welcome, but it is unfortunate that they were postponed for several years. After all, as one of the interviewees rightly pointed out:

> *"I think OGP is more an instrument rather than a driving force. For OGP to work you have to have like a window for opportunity, you need to have political will to make it work."*
>
> *Civil society representative*

The draft of the Law on Freedom of Information that was undergoing the second round of consultations at the moment of this research being conducted should be sent to the parliament at the end 2017. It has to introduce higher standards of public access to information and open data processing. Regarding the latter, Georgia does have **the open data portal** – data.gov.ge, but lacks the legislative framework that would make it mandatory for the public institutions to publish data on the portal. However, in addition to publishing, it is important to process so-called "raw" open data and make them understandable for the general public.

It could be made by NGOs, e.g. Transparency International having good examples, as well as governmental bodies themselves – **the State Audit Office's "Budget Monitor" portal being one of the exemplary cases**. Additionally, in terms of online platforms for decision-making, given that the decree regulating the work of the online petitions portal, I-change.ge, is approved by the Government, this possibility of online participation is likely to be implemented soon. There are, however, specific issues concerning the mechanism of the initiative that should be taken into account when launching the platform (e.g. the adequate number of required signatures). Meanwhile, the portal **Manifest.ge** (addressed in the previous chapter) clearly demonstrates that there is a demand from society for such kinds of initiatives.

Furthermore, the efforts of **governmental institutions** dealing with e-governance (i.e. the Ministry of Justice and its subordinate agency – DEA), seem to be more focused on service delivery orientation. In this field, the update of e-signature law is on the governmental agenda in order to allow citizens to receive online services (as a further step after one-stop-shop services). This should lead to further development of my.gov.ge – the platform accumulating public services, but that, according to our interview data, is currently mostly used only by NGOs requesting public information.

Education of the governmental sector in terms of using ICT for enhancement of democratic processes is essential. The openness to proposals from civil society and citizens is yet to be reached; however, the OGP format is contributing to this. After all, ICTs are just instruments that are able to contribute to better democracy. In the words of one of the interviewees:

> *"E-government is not a goal, it's a tool. It is using online tools being a government".*
>
> *Representative of state authorities*

Additionally, the research also demonstrated that there is the great need for making the results of the international support projects visible as well as understandable for ordinary citizens. This argument was strongly present in all interviews with civil society sector representatives. NGOs here play an essential part as well. There is a need for modernisation of this sector. As one of the interviewees mentioned:

> *"We need more... modern NGOs, let's put it this way. Or the NGOs that exist right now should modernise more. More digital, more tools /... / they produce a lot of good studies, /... / a lot of great content in terms of studies and research. But they only publish it for certain stakeholders, they hold the press conference and that's it, but nobody remembers it any more. They should talk more about it with citizens. They should find creative ways to talk about it."*
>
> *Civic activist*

Institutionalised civil society should be more active in the dissemination of their messages through attractive communication channels. More intensively using social media for disseminating the results of the OGP initiative or other good governance projects is advisable. It has been argued that Facebook in Georgia "is beyond a social network. It really is a place of discussion" as well as a place for consuming information. Hence, it is of the utmost importance to take this contextual factor into account. Furthermore, mobile Internet is widely used in the remote regions in Georgia, and hence, adapting e-democracy tools to mobile versions might make it easier to reach a larger audience.

Finally, it is worth mentioning that the developments in the realm of citizen participation on the local level in Georgia deserve separate attention. In brief, even though the amendments of the Local Self-Government Code[95] in 2014 prescribed a number of engagement mechanisms for local authorities (e.g. a general assembly of a settlement, the council of civil advisors, participatory budget) the level of awareness of their existence both of citizens as well as local authorities themselves is rather low.

[92] *Accessible at: http://economy.gov.by/uploads/files/NSUR.pdf*

[93] *Accessible at: http://pravo.by/document/?guid=3871&p0=h10800455 or http://www.e-belarus.org/docs/informationlawdraft.html (unofficial English translation)*

[94] *Accessible at: http://economy.gov.by/uploads/files/NSUR.pdf*

[95] *https://matsne.gov.ge/en/document/download/2244429/15/en/pdf*

Republic of Moldova

The main strategy providing general guidelines for information society is the **National Strategy for Information Society Development or Digital Moldova 2020**. It has been mainly inspired by the Europe 2020 agenda and is clearly focusing on boosting the IT industry's competitiveness. The existing laws, **the Law on Access to Information and the Law on Transparency in Decision-Making Processes**, set a number of general provisions for transparency and engagement of citizens in decision-making, but do not envisage any concrete provisions related to interaction with citizens via online means.

Nevertheless, it has to be pointed out that in the area of **open data**, Moldova has made remarkable progress both in adjusting its legal framework and implementing the principles of open data.

From a **coordination perspective**, there is a strong e-government implementation actor in Moldova – the **e-Government Centre**. However, the coordination mechanisms and distribution of responsibilities of actors in the field needs to be revised in order to set clear strategic goals and guidelines for state institutions for their service provision as well as for engagement practices.

The existence of the **National Participation Council**, which serves as a civil society consultative body for the Government in Moldova, is a good example of bringing the voice of civil society to the government (yet, there is a risk of transforming it into a "filter"). On the other hand, public servants have mentioned the weak engagement of CSOs in decision-making processes: the passiveness of civil society and little input from citizens/civil society in general demotivates public servants to conduct engagement practices. However, if proper mechanisms are established, there are more chances for citizens to participate and contribute smartly.

As to new challenges for Moldova regarding e-democracy and trust services, it has to be mentioned that there **is certain degree of readiness, demand and even an initial action plan for i-voting**[96]. Having a big number of citizens abroad, this is an important step forward to guaranteeing the possibility to exercise citizens' rights and democratic functions for a broader community. However, there are still concrete legal (e.g. secrecy of voting) and technical issues (e.g. electronic identity) to be addressed and solved before implementing i-voting in Moldova.

Furthermore, **the issue of privacy protection versus transparency needs clearer addressing**. One of the initiatives to push for more transparency focused on the publishing of corporate ownership information, which was initiated by the Prime Minister's Economic Council. However, on the grounds of personal data protection, the National Centre of Data Protection has blocked the initiative.

One of the barriers of e-democracy development in Moldova (which is also applicable to the entire region) is **poor civic education**, which is the driving force to boost the participation of civil society. One of the key factors to improving the situation is to **set up a clear cooperation mechanism for different ministries coordinating these fields** (e.g. Ministry of ICT and Ministry of Education). Currently, there is a lack of this sort of policy setting and cooperation. One important aspect of civic education is the perception of corruption and manipulation with power. Thus, it is important to raise awareness about these issues and find innovative solutions, as one of our interviewees' argued:

> *"We need to have hard data on corruption. And I think something like an app is available, you know, reporting. First of all, we make it nice, second you promote it efficiently to businessmen, in hospitals, in universities and so on; then you start pumping information from society, who is paying where, how much. And around this you can make much better arguments as to what you want to advocate for, for cutting something and so on. This is what we are thinking about."*
>
> *Representative of civil society*

The tendency of Moldovan **NGOs to build a coalition around certain issues in order to have a bigger impact is worth outlining**. As civil society represent-

[96] *To the authors' knowledge, the Central Electoral Commission has an action plan to pilot i-voting in the 2018 parliamentary elections (the project is mainly supported by the Swedish government).*

atives admitted, they are not interested anymore in exchanging opinions, but as the problems are clear, the time has come to do the "real thing". So far there were many funds, but still little impact out of the activity of CSOs. Hence, one of the challenges is to create more innovativeness and capacity for novel approaches in the work of NGOs. This attitude might also help to ease the traditional confrontation of government and civil society, when NGOs are accused of being just "round-tables" without a clear output and impact. However, the ways and methods to achieve this change and breakthrough in innovativeness and activeness in civil society is still to be tackled.

Another good example and "take-away" from Moldova is **the systematic monitoring of the public perception of e-governance** done by the e-Government Centre.

> *"Surveys on an annual basis... at least to just keep the hand on the pulse of society. /... /*
> *So, we used this /... /, to showcase how a public perception survey can help you deliver what citizens indeed want and what they can understand. Our survey also had a lot of data on how people trust the virtual space and their personal data protection. Do they trust public institutions in accessing e-services? Do they support the reform itself? Because it would be ridiculous to go on with the reform if you see that less than 50% of citizens support it and do not understand the notion of e-governance. The annual surveys have given us all these valuable inputs from year to year but we have also used citizen engagement in all our exercises like strategic planning, like service prioritisation, /... /"*
>
> *Representative of state authorities*

As elsewhere, government representatives refer to the temporal factor that e-transformation cannot happen overnight. It requires **good communication management to explain to citizens the benefits of e-government**, in particular in the realm of opening up data. **There should be more emphasis on creating demand and developing skills for using the data.**

> *"And I think that open data is still like "a sleeping beauty". It is beautiful, it is a lot of data but it is not yet very well used. It is also because the local public authorities still not implement Smart City initiatives and Smart City is one of biggest, adding value to open data."*
>
> *Representative of state authorities*

However, the biggest barrier to fast e-transformation is presumably the **lack of trust in government**. In the words of the representative of civil society:

> *"/.../When it comes to people benefiting from that, they don't even know that this is e-government bringing values to them. But when it comes to someone stealing a billion, it doesn't matter if this is e-governance or governance. They stole that billion. This is what happens. So, we were sometimes victims of governance in general behaviour and "misgovernance". And still not harvesting benefits when it comes literally to our achievements, to our direct contribution".*
>
> *Representative of civil society*

Ukraine

Our study indicates that even in the post-Maidan (post-revolutionary) phase in Ukraine there is strong **human capital** observable. The Maidan revolution "pulled the trigger" for civic activism and different civic movements to burst – this is where the kick-start of Ukrainian e-democracy took place. Active citizens and mind-leaders emerged with a vision and an idea of bringing power to the people with the help of technology. The advantage of Ukraine lies in its **active civil society** that is trying to lead the country into a better future by being actively engaged in various coalition networks with the government, such as the **E-democracy Coalition and Reanimation Package of Reforms**, but additionally, launching and initiating e-democracy instruments on their own – Prozorro, E-petitions to name a few. Those instruments are in turn gradually creating a critical mass of people getting more knowledgeable about e-democracy and its purpose. Ukraine is also characterised by rapid diffusion of e-oriented movements, civic enthusiasm and to some extent civic euphoria about the possibilities of IT in the field of democracy. This mind-set enabled the country to implement instruments rapidly and without the preparatory ground work (e.g. Open Data Portal, Prozorro).

We can also observe that **international initiatives and donors** are playing an essential role in driving the field forward – some of them happen to play a decisive role in the inception of new ideas and in counterbalancing some of the barriers in the field. Additionally, we can see that the **governmental sector is gradually becoming more engaged** and is taking up civic initiatives at the later stage of their development. These are; however, concrete "agents of change" that are driving the agenda inside this sector.

The normative acts and regulations in the realm of e-democracy in Ukraine have expanded especially in the post-2014 period. The Law on Citizens' Petitions, the Law on Access to Public Information, and the Law on the Open Use of Public Funds are major acknowledged achievements. The elaboration **of the E-democracy Concept Paper** (described in section 1.4) by the main actor in the field, the **State Agency for Electronic Governance**, sets an important precedent **establishing a legal framework and a mandate for e-democracy development on the national level in Ukraine**. This process can be perceived as an important step towards proper planning of the fragmented field using a collaborative, multi-stakeholder approach. The cooperation experience with civil society within the framework of the E-democracy Coalition is seen as successful and important. As stated by the representative of state authorities:

> *"We have finally reached the acknowledgment that this area is the one having priority. This is in the Action Plan of the OGP initiative where the elaboration of the E-democracy Concept Paper is mentioned. /… / I would also mention as one of the success stories the formation of the E-democracy Coalition. Being a public servant myself, I consider it to be a great achievement that state institutions are willing to communicate and engage the civil society sector and the civil society also demonstrated its interest in collaborating."*
>
> *Representative of state authorities*

There are, nevertheless, certain barriers that impede the development of e-democracy. One of the interviewees stated the challenge very clearly:

> *"Relationships, relationships…and I cannot stress it enough, because there is so much capital in this country, but the fabric and glue, the cohesiveness are not there, the system is not there to meet these wonderful individuals and the human capital."*
>
> *Representative of the donors' community*

The massive energy of the Maidan revolution resulted in **the institutional and instrumental fragmentation** in the field of e-democracy, the traces of which can still be visible. The competitiveness between NGOs and the lack of collaborative capital in society is impeding the promotion of reforms. **The lack of trust** between different actors in society – citizens, business, government – is one of the crucial barriers that has an impact on the implementation of e-democracy instruments. It partially refers to the psychological obstacle for a strong digital identification – citizens are not willing to participate and express their opinions openly. At the same time, in the context of undeclared war with the Russian Federation, the issue of cyber security comes to the forefront. **The lack of the culture of dialogue** has a tremendous impact on how the field is developing – citizens are distrustful of the government, while the government is still lacking the capacity and knowledge on how to properly structure and implement its communication with citizens. Both of these sides will benefit from joint collaborative tasks/projects that will force working for the common agenda. The need for partnership and collaboration has been specifically stressed by our interviewees:

> *"Firstly, establish partnerships. When the government decides to develop something without the consultancy with business and civil society it leads to unusable tools. You can implement something really usable and efficient only if you have these three partnerships – civil society, business and government."*
>
> *Representative of civil society*

> *"At the end of the day building this kind of capital, human capital and collaborative capital that you can't really quantify, but anyway in the near future that is what you are going to need, and it is not going to be that visible, but it is going to be cohesive in all these instruments. It is people actually working together, co-creating together."*
>
> *Representative of the donors' community*

The awareness building is also taking place; however, there is still a lot to be done for the enhancement of the understanding about **the purpose** of e-democracy instruments and **the impact** they might have.

2. Concluding Remarks: Drivers and Barriers of E-democracy in the Region

The study at hand aimed at providing a review of the state of affairs in the field of e-democracy in the Eastern Partnership (EaP) countries – Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine. Before presenting country-specific policy recommendations, we look at some of the major drivers and barriers that could either foster improvements in the implementation of e-democracy or hinder its potential development in the region. We also make general recommendations for the region on how to overcome existing challenges.

First and foremost, as the study demonstrated, the **Open Government Partnership initiative** that provides an international platform for domestic reformers to commit to making their governments more open, transparent and participatory, has clearly played an important role in fostering e-democracy **in most countries of the region that joined the initiative**. The vast majority of governmental commitments in the EaP region related to e-democracy derive from OGP Action Plans that undergo independent international monitoring and evaluation. From this perspective, **OGP can be regarded as a "soft pressure" mechanism** as well as a driver at least to the extent of fostering the "kick-off" process of e-democracy development in the EaP region.

Next, good practice of building multi-stakeholder **partnerships** should be stressed. We have witnessed this gradually growing acknowledgement of collaboration both in **Ukraine** and **Moldova**. The emerging partnership mind-set has implications for both intra-sectorial collaboration as well as cooperation between different sectors of society. For instance, building coalitions of NGOs around certain issues proved to have a bigger impact as exemplified in the case of Ukraine. Furthermore, as the study indicated NGOs that are interested in going beyond the "roundtable" discussions and achieving clear outcomes might help to foster partnership between government and civil society. Last, but not least, as clearly stressed in the case of the ProZorro initiative, the "golden triangle of partnership" – civil society, business and government – is one of the most important keys to success.

The case of ProZorro in **Ukraine** also reveals the necessity and vital importance of creating **a strong brand** around any e-democracy tool to be launched: raising awareness and demonstrating the benefits of the tool could help to rebuild the trust of potential users (and citizens) in governmental systems. Similarly, this case indicates that **international initiatives and the donors' community** are playing an essential role in driving the field forward – some of them happen to play a decisive role in the inception and what is more important institutionalisation of new ideas.

Finally, even though the focus of the review at hand has been on e-democracy on the central level, it has to be stressed that **local level activism** plays an essential role in boosting general e-activism in a society, since the local level is the closest link between citizens and the state. The high potential of local level initiatives to advance the implementation of e-democracy was observable in all countries in the region.

As to the **barriers and challenges** that EaP countries currently face in the realm of e-democracy, the study revealed that there is **a lack of comprehensive national surveys** in regards to e-governance development and e-readiness in general in the EaP region as well as a lack of sustainability in the measurement activities. The case of **Ukraine** is an exception here, having a number of recent studies focusing on e-democracy as well as public opinion polls and surveys with the questions of e-governance. Since international rankings provide only limited overviews of the trends and developments of the national information societies, it is important to build the institutional capacity and establish a mechanism for measuring and analysing the governmental performance.

In addition to civil society, it is partly the role of journalists to be **democracy watchdogs and analyse the performance of government**. In most EaP countries, in **Azerbaijan** and **Belarus** in particular, one of the most important groups to conduct target training with is journalists, investigative journalists in particular. In **Ukraine**, on the other hand, there seems to be a critical mass of journalists working with an investigative focus and using open data. However, it is important to stress that in creating any new e-tool or platforms, using open data for analysing the performance of different actors, it essential to adhere to rules and regulations of privacy and personal data protection. Violation of these destroys the trust of citizens in e-democracy tools.

Furthermore, there is still a lot to be done **in all EaP countries** for the enhancement of understanding what the purpose of e-democracy instruments is and what impact they might have. **Despite the existence of numerous e-democracy tools, the low level of "e-democracy literacy" is evident in all countries in the region.** Hence, one of the barriers is a lack of civic education, which could potentially become a driving force to boost the participation of civil society. One of the approaches to raising awareness and contributing to reaching higher e-literacy levels is to set up a clear cooperation mechanism for different ministries coordinating these fields (e.g. Ministry of ICT and Ministry of Education). Additionally, there is a strong need to make the results of the international support projects (e.g. good governance projects) visible as well as understandable for ordinary citizens. This could be addressed through general education on issues of corruption and manipulation with power.

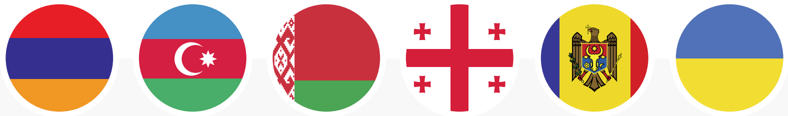
Likewise, **targeted training in the governmental sector** in terms of using ICTs for the enhancement of democratic processes is essential. For instance, among the core competencies of the public servants that need special attention is the knowledge of the legal framework regulating transparency in decision-making; a clear understanding of the concepts of e-participation, open data as well a link between open data and transparency; awareness about different e-consultation and e-participation platforms and mechanisms available for different stages of the decision-making process.

Additionally, actors in each country are encouraged to work on the elaboration of a thorough and **comprehensive overview of e-democracy tools** created in order to build a "menu" of different tools that both civil society and government could be using. As the study indicated, the majority of e-democracy tools fall into the category of transparency and accountability, and only a handful of them strive to enhance participation. Hence, there is an imbalance in terms of the implemented stages of e-democracy: e-information and e-consultation are clearly dominant in e-democracy implementation in the region. A similar tendency is observable on the strategic level.

The low level of enforcement of existing legislation as well as weak institutionalised mechanism and regulation of e-participation constitute substantial barriers to coherent e-democracy implementation in the region. There is no compliance mechanism or "sanctions" for violation of, for instance, regulations of provisions coordinating citizen participation; additionally, there is a lot of interpretation of what laws are to be implemented and how. This has been one of the main concerns of civil society for several years. Furthermore, if the coordination of e-governance policies is centralised in the hand of technical agencies, the e-democracy part tends to be out of focus. Also, the mandate of the agency is likely to be limited when it comes to imposing standards and regulations on other institutions. Bringing e-governance issues under subordination of higher executive levels could be beneficial. The State Agency for Electronic Governance of **Ukraine** sets an important precedent establishing a strategic framework and a mandate for e-democracy development on the national level.

One of the biggest barriers referred to both by government representatives and by civil society representatives in various countries is general passiveness and low interest in participation in decision-making processes. Establishing a clear mechanism of keeping track of gathered feedback as well as of ensuring authorities' public response to citizen feedback could be beneficial.

Finally, we would like to underline **the importance of "offline" activities** and tools and their integral role in the development of e-democracy. It should be kept in mind that online and offline spaces complement each other, and, hence, their combination is necessary for efficient civic engagement to take place. This was most evident in the initiatives of **Moldova** and **Armenia**. It should be remembered that technology is not a magic wand for boosting transparency and civic participation, but is merely supportive of existing democratic practices.



General recommendations for the Eastern Partnership countries

In view of the above, we would like to draw several general recommendations that we believe could be useful for all countries in the region to take into account:

- All stakeholders should remember that ICTs are instruments at the service of democratic processes. They are the tools that enable societies to advance and "deepen" democracy. Hence, "offline" activities should not be neglected. It is **the combination of online and offline tools** that contributes to the emergence of successful participatory practices.

- All stakeholders are encouraged to cooperate in the work on the elaboration of a thorough and comprehensive overview of available e-democracy instruments in order **to build a "menu" of different tools** that both civil society and government could be using.

- **Local level activism** should be encouraged and nurtured. It plays an essential role in boosting general e-activism in society, being the closest link between citizens and the state.

- **Public awareness and e-literacy campaigns** should be conducted in order to tackle the low usage of e-democracy instruments. Additionally, strong brands around e-democracy tools demonstrating its benefits should be created.

- Targeted training in **the governmental sector** in terms of using ICTs for enhancement of democratic processes is essential. Governments should also acknowledge e-democracy as an integral part of e-governance and underpin its developments with clear strategic and legislative frameworks.

E-democracy is not linked so much to technologies as to the political and cultural choices of every country in terms of the level of involvement of the citizens in the political spheres, the level of accountability and openness.

3. Policy recommendations

Armenia

- The experience of Armenia in **governance innovation** (via pop-up innovation lab) should be promoted and encouraged further. The openness and the willingness of the main governmental actors in the field cannot be overestimated.

- Armenia has a variety of e-solutions; however, with rather low usability. **A lot still has to be done in the public awareness domain.** All stakeholders are encouraged to work on the elaboration of a thorough and comprehensive overview of the e-democracy tools created in order to build a "menu" of different tools that both civil society and government could use.

- The area of **open data** requires more in-depth understanding by all sectors of society. The **capacity of institutionalised civil society** to use the potential of technologies as well as existing open data in a transformative way should be addressed. The IT community has to be stimulated to be part of the social innovation developments.

- Since the realm of open data and transparency that it enables is becoming more and more widespread, a lot of attention has to be paid to **data protection regulations**, which is an issue of concern according to the study.

- The **local level** in Armenia has active developments supported by NGOs and donors. It is important to continue working in this direction and to raise the awareness of local communities about alternative forms of engagement.

- It is vital to encourage the adaptation and adjustment of new solutions to local needs. There should be **a pragmatic tandem between the donor and the government** enabling piloting of new projects before attempting large-scale implementation. The engagement of the IT community in these pilots (and finding proper stimuli for that) would facilitate synergy between the non-governmental and IT sectors.

Azerbaijan

- **A legal and institutional mechanism and regulation for e-participation is important.** Currently there are no strategies or action plans designed for civic participation or e-participation. The only strategic document that can be considered the government's commitment in terms of transparency and civic participation is the latest OGP Action Plan for 2016–2018. However, as the current status of Azerbaijan in OGP is inactive, its implementation at the moment is hard to predict.

- **Support for monitoring of public information provision is recommended.** Enforcement of the Law on Access to Information, which was adopted in 2005, could be monitored by an institution of Ombudsman of Information, which was initially considered as a necessary body, but was eliminated later on.

- Regarding the online provision of information, **support for local governments in the area of provision of information via official webpages is suggested**. For instance, the development of a template with a specific layout of public information on the webpages of local government. This would facilitate easier access to information on the local level for the residents as well as provide local governments with a fairly easy tool for structuring their information.

- Emphasis should be put on more **homogenous development of e-services**. Currently the accessibility and quality of e-services is still uneven. There are clear forerunners among state authorities, but there are also those who are lagging behind. Yet, it is clear that transformation from offline service delivery to online services requires a supportive legal and institutional mechanism as well as re-design of processes.

- **A monitoring mechanism is needed on the usability and access to e-services** in order to enable citizens to use the full potential of e-services that already exist as well as to design new ones. Additionally, analysis of the monitoring results and the outcomes of this process should be clear. The ASAN Index developed by the Agency also contains monitoring questions, which cover such components as e-information and e-consultation, yet, it is not so clear how the monitoring results and the outcomes of this process are used for developing e-services and e-participation.

Belarus

- There is a need for amendments or renewal of the legislative framework on **the access to public information and data protection** that would take into account developments in the field of ICTs.

- NGOs should more intensively use new mass media in order to promote the topic to the wider audience. It is also essential to raise their awareness about the concept of e-participation in order to facilitate the overall development of participatory culture in the third sector.

- The low level of collaboration between actors and low awareness of each other might impose an obstacle in reaching a bigger impact. It is hence recommended to **enhance networking activities** and engage the Belarusian **analytical community** (e.g. experts, researchers, think tanks) in advocacy campaigns. The donor community, international organisations and development agencies are encouraged to initiate **joint thematic activities for experience sharing and networking.**

- **The local level initiatives** might be the best way to approach the advancement of e-democracy in Belarus. The potential for further developments could be feasible via e-consultation activities about tangible issues, such as city spatial planning.

Georgia

- The predominance of e-democracy instruments focusing on transparency and accountability is observable. Hence, more e-democracy tools focusing **on participation of citizens in the decision-making processes** is needed. The e-petitions platform (ichange.gov.ge) that is now back on the governmental agenda has the potential to drive the area of e-democracy forward. Given the low digital literacy rate, it is recommended to lower the threshold of signatures for a petition in order to not demotivate citizens to use the platform.

- There is a clear need for a modern standalone act of freedom for information, hence the development of **the Freedom of Information Law** addressing among others the topic of disclosure of public sector data remains important. Additionally, establishment of an oversight authority that would monitor and ensure the enforcement of the corresponding legal provisions is recommended.

- **Institutionalised civil society** should be more active in disseminating **their messages** through attractive communication channels. Using social media more intensively for disseminating the results of good governance projects is advisable. Raising public awareness about and proper education on the usage of existing e-democracy instruments elaborated by NGOs should be one of the focal points in development of this area.

- **Targeted training in the governmental sector** (both on local and national levels) on the topic of using ICTs for the enhancement of democratic processes is essential. Deepening the knowledge of public servants on the legal framework regulating transparency in decision-making; on the concepts of e-participation, open data and transparency; as well as building awareness about different e-consultation and e-participation platforms and mechanisms available for different stages of decision-making processes.

Republic of Moldova

- **Coordination mechanisms and distribution of responsibilities** between actors in the field need to be revised in order **to set clear strategical goals and guidelines** for state institutions for their service provision as well as for engagement practices. The area of e-democracy in Moldova has so far been under the responsibility of the e-Government Centre. It will be shifted in the nearest future under the jurisdiction of the State Chancellery. **Collaboration between the e-Government Centre and the State Chancellery** would then be of the utmost importance as well as the proactive work of the latter in building public awareness of existing e-democracy developments. In order to have sustainability of the results achieved by e-Government Centre, **stable funding** from the state budget for this institution has to be ensured.

- Activities of the e-Government Centre that **focus on gathering feedback from citizens** need further support and encouragement. More specifically, these include such undertakings as annual public perception surveys that provide valuable input from year-to-year on what citizens actually want (e.g. services prioritisation, trust in virtual space, etc.)

- To improve the **quality of civic education** it is important to **set up a clear cooperation mechanism for different ministries** coordinating these fields. One important aspect of civic education is the perception of corruption and manipulation with power. Thus, it is important to raise awareness on why to keep track of corruption and how it functions.

- **E-transformation** cannot happen overnight. It requires **good communication management to explain to citizens what the benefits of e-government are**, in particular in the realm of opening up data. Additionally, the mistrust of citizens towards government needs clear addressing, cultural changes might be pushed forward by awareness conducting campaigns. As part of this topic, the question of **privacy protection versus transparency** needs clearer addressing.

- **There should be more emphasis on creating demand and developing skills for using the data.** The e-Government Centre is involved in an **open data** project with donors' funding that enables numerous datasets to be opened. However, better understanding and awareness is needed on what one could do with the data. Additionally, there is a need for more intensive commitment from local governments, since a lot of data that could be potentially interesting for the citizens is local.

- **Collaboration mechanisms between the government and CSOs have to be reinvented/improved.** The National Participation Council has been established as the main platform for this purpose, but there are some changes expected in its operation. Currently it is not seen as an effective communication channel between different stakeholders.

Ukraine

- In the governmental sector, the **institutionalisation of e-democracy** has to take place, i.e. the creation of relevant departments and the allocation of human and financial resources for them. The State Agency is currently taking the coordinating role in this area; however, other governmental institutions also have to become involved. There have to be **clear guidelines** for every institution taking part in the implementation of e-democracy initiatives. Communication departments could be the focal points for e-democracy activities and instruments.

- The massive energy of the Maidan revolution resulted in institutional and instrumental fragmentation in the field of e-democracy, the traces of which can still be visible. **The holistic governmental approach in the area of e-democracy** is now gradually being developed through the development of the E-democracy Concept Paper. This direction and single vision should be encouraged further.

- **The active civil society** of Ukraine should continue performing its proactive role in the development of e-democracy.

- All e-democracy initiatives have to be accompanied by **awareness raising campaigns and training.** A good example of how this kind of awareness raising and training helps to establish a good ecosystem for an e-initiative and make it sustainable is the case of ProZorro.

- Increasing public awareness through **concrete community projects** where different stakeholders are working towards a common agenda could enhance the creation of **a culture of dialogue** and hence, could help Ukrainian e-democracy to flourish.

References

- ABC Guide on Citizen Engagement (2015). Accessible at: https://issuu.com/e-governanceacademy/docs/abc-guide-on-citizen-engagement-eng
- Alvarez, R. and Nagler, J. (2000). The Likely Consequences of Internet Voting for Political Representation. *Loyola of Los Angeles Law Review*, 34:1115.
- Alvarez, R., Hall, T., and Trechsel, A. (2009). Internet Voting in Comparative Perspective: The Case of Estonia. *PS: Political Science and Politics*, 42(03):497–505.
- Arnstein, Sherry R. (1969). A ladder of citizen participation. *Journal of the American Institute of planners* 35.4: 216-224.
- *Azerbaijan creates government-civil society dialogue platform* (2017). Accessible at http://ogp.org.az/index.php/2017/02/10/azerbaijan-creates-government-civil-society-dialogue-platform/
- Centre for Innovations Development (2015). *Public Opinion about E-petitions in Ukraine*. Kyiv
- Chulitskaya, T., Ryabova, N., Vidanova, I., Markushevski, D., Kovalkin, V. (2016) *Advocacy in Belarus: Experience of Civil Society Organisations.* Office of European Expertise and Communications. Accessible at http://eng.oeec.by/advocacy-in-belarus-experience-of-civil-society-organisations/
- Coleman, S. (1999). "Cutting out the middle man: from virtual representation to direct deliberation" In: *Digital Democracy: Discourse and decision-making in the Information Age*, Hague, B.N. & Loader, B.D.(eds), pp. 195–210. Routledge, London and New York
- Council of Europe (2016). Civil Participation in Decision Making in the Eastern Partnership Countries - Part One: Laws and Policies. Accessible at: https://edoc.coe.int/en/partnerships/7401-civil-participation-in-decision-making-in-the-eastern-partnership-countries-part-one-laws-and-policies.html
- Council of Europe (2017). Civil Participation in Decision Making in the Eastern Partnership Countries - Part Two: Practice and Implementation. Accessible at: https://edoc.coe.int/en/partnerships/7402-civil-participation-in-decision-making-in-the-eastern-partnership-countries-part-two-practice-and-implementation.html
- European Commission for Democracy through Law (2016). *Interpretative Declaration to the Code of Good Practice in Electoral Matters on the Publication of Lists of Voters Having Participated in Elections*. Accessible at: http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2016)028-e
- Fawkes, J. and Gregory, A. (2000) "Can existing communication models apply to the Internet?", *Journal of Communication Management*, Vol 5, No 2, pp 109-124
- Hacker, K.L., and van Dijk, J. (2000) "What is Digital Democracy?", in Hacker, K.L., and van Dijk, J. (eds.), *Digital Democracy: Issues of Theory and Practice*, London: Sage.
- *Harmonisation of the Digital Markets in the Eastern Partnership* (2015). Accessible at: https://europa.eu/capacity4dev/hiqstep/document/harmonisation-digital-markets-eastern-partnership-study-report
- IDFI (2016). *OGP Georgia Action Plan for 2014-2015 – Completed and Unfulfilled Commitments.* Accessible at: https://idfi.ge/en/ogp-2014-2015-action-plan-accomplished-and-non-accomplished-obligations
- Kiev International Institute of Sociology (2015). *E-government and E-democracy: What do Ukrainians Think*? Accessible at: http://egap.in.ua/biblioteka/e-uryad-ta-e-demokratiya/
- Kiev International Institute of Sociology (2016). *The Dynamics of Internet Usage in Ukraine: February-March 2016*. Accessible at: http://www.kiis.com.ua/?lang=ukr&cat=reports&id=621
- Margolis, M. and Resnick, D. (2000) *Politics as usual. The Cyberspace "revolution"*. Sage: California.
- Markushevsky, D. (2016). *На пути к электронному правительству в Беларуси*.

Accessible at: http://sympa-by.eu/sites/default/files/library/policy_paper_e-government_bipart.pdf

- McQuail, D. (2005). *Mass Communication Theory.* SAGE Publications
- Musso, J. and Weare Ch., (2005). "Implementing Electronic Notification in Los Angeles: Citizen Participation Politics by Other Means", *International Journal of Public Administration*, Vol 28, Issue 7/8, 599–620.
- OECD (2001). *Citizens as Partners*. Accessible at: http://www.internationalbudget.org/wp-content/uploads/Citizens-as-Partners-OECD-Handbook.pdf
- OECD (2016). Anti-Corruption Reforms in Georgia. Fourth Round of Monitoring of the Istanbul Anti-Corruption Action Plan. Accessible at: https://www.oecd.org/corruption/acn/Georgia-Round-4-Monitoring-Report-ENG.pdf
- OSCE (2017). *Republic of Armenia. Parliamentary Elections 2 April 2017. OSCE/ODIHR Election Observation Mission Final Report.* Accessible at: http://www.osce.org/odihr/328226?download=true
- PACT (2015). *Top 10 of Belarus Civil Society in 2015.* Accessible at: http://www.pactworld.org/news/top-10-belarus-civil-society-2015
- Putnam, R. (2001). *Bowling Alone: The Collapse and Revival of American Community.* Simon and Schuster.
- Schalken, C., Depla, P. And Tops, P. (1996). "Information and Communication Technologies and Democracy", in: Bekkers, V., Koops, B.J. and Nowt, S. (eds.). *Emerging Electronic Highways. New Challenges for Politics and Law,* pp. 47–54, The Hague: Kluwer Law International.
- Sokolova, M. (2011). Электронное правительство в Беларуси: преодолеть инерцию информатизации. Accessible at http://www.e-belarus.org/docs/egov2011.pdf
- Sushko, A. (2017). *Государственные услуги онлайн – от предоставления информации к электронного правительств.* Accessible at: http://sympa-by.eu/sites/default/files/library/gosudarstvennye_uslugi_onlain_ot_predostavleniya_informacii_k_elektronnomu_pravitelstvu_.pdf
- Tetra Tech (2016). *Good Governance Initiative (GGI) in Georgia – E-readiness Study in Georgia.* Accessible at: http://www.dea.gov.ge/uploads/E-readiness_ENG2.pdf
- *The activity of the Government of Azerbaijan in Open Government Partnership* (2017). Accessible at: https://www.opengovpartnership.org/sites/default/files/Azerbaijan_OGP-full-report_May2017.pdf
- Tomkova, J., Boguslav, M., Garashenko, N., Khutkyy D., Loboyko, D., Pravylo, O., and Andrii Semenchenko. (2016) *eDemocracy in Ukraine: Citizens' & Key Stakeholders' Perspectives*. Accessible at: http://egap.in.ua/wp-content/uploads/2016/01/07.07.pdf
- Tomkova, J., Konashevych, O. (2016). Policy Briefs on Good E-governance. Issue #1: Legislative Aspects on E-democracy in Ukraine. http://egap.in.ua/natsionalna-polityka
- United Nations (2014) E-Government Survey. Accessible at: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2014
- United Nations (2016) E-Government Survey. Accessible at: https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016
- van Dijk, J. (2000) Widening Information Gaps and Policies of Prevention. *Digital Democracy: Issues of Theory and Practice*, pages 166–183
- van Dijk, J. (2005) *The Deepening Divide: Inequality in the Information Society.* Sage Publications, Inc.
- Varazi, N., Avalishvili, L. and Kldiashvili, G. (2016) *Review of Commitments Undertaken by the Government of Georgia in its 2016-2017 Open Government Action Plan.* Accessible at: https://idfi.ge/en/review_of_ogp_2006_2017_action_plan_obligations_undertaken_by_georgian_government
- Volodin, D., Sushko, A. (2017) *Е-участие как инструмент инклюзивного государственного управления* Accessible at http://sympa-by.eu/sites/default/files/library/brif_issledovaniya_e-uchastie_kak_instrument_inklyuzivnogo_gosupravleniya_bipart_a_sushko.pdf
- Wilhelm, A.G. (2000) *Democracy in the Digital Age. Challenges to Political Life in Cyberspace.* New York: Routledge.

Strategies and legal acts

Armenia

- Armenia Development Strategy 2014–2025 (2014). Accessible at: https://eeas.europa.eu/sites/eeas/files/armenia_development_strategy_for_2014-2025.pdf
- Electoral Code of the Republic of Armenia (2016). Accessible at: https://www.ecoi.net/file_upload/1226_1468568887_armenia-electoral-code-as-of-30june2016.pdf
- Government Decision on the Procedure for Organisation and Implementation of Public Discussions (2010). Accessible at: http://www.arlis.am/DocumentView.aspx?docID=57300 (in Armenian)
- Law of the Republic of Armenia on Freedom of Information (2003). Accessible at: http://www.foi.am/u_files/file/legislation/FOIeng.pdf
- Open Government Partnership. Third Action Plan of the Republic of Armenia (2016-2018). Accessible at: https://www.opengovpartnership.org/sites/default/files/Armenia_NAP3_2016-18.pdf

Azerbaijan

- Law of the Republic of Azerbaijan on Access to Information (2005). Accessible at: http://www.stat.gov.az/menu/3/Legislation/information_rules_en.pdf
- Law of the Republic of Azerbaijan on Freedom of Information (2010). Accessible at: http://www.commission-anticorruption.gov.az/upload/file/Law%20on%20%20freedom%20of%20information.pdf
- Law on Information, Informatisation and Protection of Information (2010). Accessible at: http://www.wipo.int/wipolex/en/details.jsp?id=9203
- Law on Public Participation (2014). Accessible at: http://www.commission-anticorruption.gov.az/upload/file/Law%20on%20Public%20Participation.pdf
- National Action Plan for 2016-2018 on Promotion of Open Government (2016). Accessible at: http://ogp.org.az/wp-content/uploads/2017/02/Action-Plan-final-version-1.pdf

Belarus

- Constitution of the Republic of Belarus of 1994 (2004), Article 33. Accessible at: http://www.wipo.int/edocs/lexdocs/laws/en/by/by016en.pdf
- Law of the Republic of Belarus on Information, Informatisation and Protection of Information (2016). Accessible at: http://pravo.by/document/?guid=3871&p0=h10800455 and http://www.e-belarus.org/docs/informationlawdraft.html (unofficial English translation)
- Law of the Republic of Belarus on Appeals of Citizens and Legal Entities (2015). Accessible at: http://www.pravo.by/document/?guid=3871&p0=h11100300
- Law of the Republic of Belarus on Regulatory Legal Acts of the Republic of Belarus (2009). Accessible at: http://pravo.by/document/?guid=3871&p0=h10000361
- Law of the Republic of Belarus on the Basics of Administrative Procedures (2017). Accessible at: http://pravo.by/document/?guid=3871&p0=H10800433
- Law of the Republic of Belarus on the Procedure for the Implementation of Legislative Initiative by Citizens of the Republic of Belarus (2015). Accessible at: http://www.pravo.by/document/?guid=3871&p0=H10300248
- National Program of the Republic of Belarus on the Development of Digital Economy and Information Society 2016–2020 (2016). Accessible at: http://www.government.by/upload/docs/file4c1542d87d1083b5.PDF
- National Strategy of Sustainable Socio-economic Development of the Republic of Belarus 2030 (2015). Accessible at: http://economy.gov.by/uploads/files/NSUR.pdf
- Presidential Decree "On Improving Work with the Population" (2005). Accessible at: http://www.pravo.by/pdf/2005-7/2005-7(003-005).pdf
- Presidential Decree "On Measures to Improve the Use of the National Segment of the Internet" (2010). Accessible at: https://portal.gov.by/i/portalgovby/download/ukaz-60.pdf
- Presidential Decree on Additional Measures for Working with Appeals of Citizens and Legal Persons (2016). Accessible at: http://pravo.by/document/?guid=3871&p0=p30700498
- Resolution of Council of Ministers "On Official Information of Limited Distribution" (2014). Accessible at: http://www.pravo.by/document/?guid=3871&p0=C21400783&p1=1
- Strategy on the Development of Informatisation in the Republic of Belarus 2016–2022 (2015). Accessible at: http://e-gov.by/zakony-i-dokumenty/strategiya-razvitiya-informa-

tizacii-v-respublike-belarus-na-2016-2022-gody

Georgia

- Government Decree "About the Form of the Electronic Request of Information and Proactive Disclosure of Public Information" (2013). Accessible at: https://ogpblog.files.wordpress.com/2013/09/decree-of-the-governemnt-of-georgia-219-eng.pdf
- OGP Action Plan 2014–2015. Accessible at: http://www.opengovpartnership.org/sites/default/files/OGP%20AP%20GEORGIA.pdf
- OGP Action Plan for 2016–2017. Accessible at: https://www.opengovpartnership.org/countries/georgia/irm
- Open Parliament Georgia Action Plan 2015-2016. Accessible at: https://idfi.ge/public/upload/Open%20Parliament%20Georgia%20Action%20Plan%20(2015-2016).pdf
- Public Administration Reform Roadmap 2020 (2015). Accessible at: http://government.ge/files/425_49309_322150_15.07.21-PublicAdministrationReformRoadmap2020(Final)(1).pdf
- Tbilisi Action Plan 2017. Open Government Partnership. Accessible at: http://ogp.tbilisi.gov.ge/img/original/2016/11/17/Tbilisi_Action_Plan_2017_final.pdf
- The e-Georgia Strategy and Action Plan 2014–2018 (2013). Accessible at: http://dea.gov.ge/?action=news&news_id=47&lang=eng

Moldova

- Government Decree on National Participation Council from 2010 (2016). Accessible at: http://lex.justice.md/viewdoc.php?action=view&view=doc&id=333477&lang=2 (available in Russian and Moldovan)
- Government Decree on Open Data Principles (2014). Accessible at: http://lex.justice.md/md/354533/ (available in Russian and Moldovan)
- Government Decree on the Approval of Open Data Methodology (2014). Accessible at: http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=354534 (available in Russian and Moldovan)
- Law of the Republic of Moldova on Access to Information from 2000 (2015). Accessible at: http://lex.justice.md/viewdoc.php?action=view&view=doc&id=311759&lang=2 (available in Russian and Moldovan)
- Law of the Republic of Moldova on Transparency in Decision-making Processes from 2008 (2016). Accessible at: http://lex.justice.md/viewdoc.php?action=view&view=doc&id=329849&lang=2 (available in Russian and Moldovan)
- National Strategy of the Republic of Moldova for Information Society Development (2013). Accessible at: http://www.who.int/goe/policies/countries/mda_support1.pdf
- Open Government Partnership National Action Plan 2016-2018. Accessible at: https://www.opengovpartnership.org/countries/moldova

Ukraine

- Cabinet of Ministers Resolution on the Approval of Regulation on Datasets to be Published in Open Data Format (2015) Accessible at: http://zakon5.rada.gov.ua/laws/show/835-2015-п
- E-democracy (2017) Public Discussion of Draft Laws. Accessible at: http://e-zakon.org/e-dem
- eTransformation (2014) The Green Paper for the Electronic Governance in Ukraine.
- HiTech Office (2016) The Digital Agenda for Ukraine 2020. https://drive.google.com/drive/folders/0B8Oa6Q2zfKDSN2Q2MnNJd1NXa0U
- Law of Ukraine on Access to Public Information from 2011 (2015) Accessible at: http://zakon4.rada.gov.ua/laws/show/2939-17
- Law of Ukraine on Citizens Petitions (2015). Accessible at: zakon5.rada.gov.ua/laws/show/577-19/paran2#n2.
- Law of Ukraine on the Open Use of Public Funds (2015). Accessible at: zakon5.rada.gov.ua/laws/show/183-19
- Mykolaiv City Development Fund (2015) The White Paper for the Policy on Electronic Democracy. http://www.frgn.mk.ua/wp-content/uploads/2015/11/WB_eDem_1.0.docx
- The Cabinet of Ministers of Ukraine (2017) Draft Concept Paper and the Action Plan for the Advance of E-democracy in Ukraine. Accessible at: http://www.e.gov.ua/sites/default/files/proekt_koncepciyi_z_e-demokratiyi_.pdf (in Ukrainian)
- The Economic Development and Trade Ministry of Ukraine (2015). The Digital Agenda for Ukraine 2015. https://www.slideshare.net/KyivSchoolofEconomics/da-event-ver5-02-042015

Annex 1

Situation Review: Safety and Security of Cyberspace
and E-democracy in the Eastern Partnership Countries

Interview Guide

Focus area #2: ICT tools for promoting civic participation and transparency of government decision-making processes

I part: Overview

- What are the main achievements in the field of e-participation and transparency?
- What is the driving force and motivation for the development of this field?
- What are the main barriers that inhibit the development of this field?
- Who are the key stakeholders on the country level, in addition to the government, being responsible for/or playing an active role in promoting civic e-participation? How are they cooperating? What is the structure of their relations?
- In your opinion, what governmental institution(s) should be responsible for the field of civic participation and transparency of government decision-making processes?
- Which commitments envisaged in governmental strategic plans were not (fully) implemented by the Government?
    - What are the main occurred/potential barriers to their implementation?
    - What factors stimulated their implementation?
- What are the commitments of your Government to Open Government Partnership?
    - To what extent were/are these commitments being implemented?
- What would be your recommendations for improvement of this field in your country?

II part: Notable ICT cases

- What are the most prominent cases of e-participation and transparency in decision-making?
- The following questions apply if the interviewee is knowledgeable about the case
    - Who initiated the process/the creation of the tool?
    - When did it take place (time interval)? / When was it launched?
    - What was its cost?
    - Who is managing it today?
    - How was information about the process/the tool provided to the general public?
    - What is the average number of users?
    - What were the challenges faced during implementation of the process/tool?
    - What in your opinion are major outcomes?
    - What is the impact of the process/tool?
    - What are the lessons learnt from this case?

Annex 2

Situation Review: Safety and Security of Cyberspace
and E-democracy in the Eastern Partnership Countries

Questionnaire

Focus area #2: ICT tools for promoting civic participation and transparency of government decision-making processes

Please provide answers to the following questions. NB! The size of the answers section is indicative.
Do not hesitate to provide more information, if this is needed.

E-readiness

Apart from major international indexes (E-Government Readiness Index, E-Participation Index, etc.), are there any national surveys conducted on e-readiness in your country?

Main strategies and action plans

What are the main strategies and action plans of the Government in the area of civic participation and transparency? Please provide links if these acts or their summaries are in English or in Russian

Do these governmental strategies take into account ICT-related civic participation and disclosure of public information on the Internet by central and local level authorities?

To what extent were/are the activities and plans envisaged in these strategies being implemented?

Which commitments were not (fully) implemented by the Government? What are the main occurred/potential barriers to their implementation?

What are the commitments to Open Government Partnership and to what extent were/are these commitments being implemented?

Legal framework

What kind of legal acts stipulate citizen participation in decision-making both on the national and local levels? Please provide links if these acts or their summaries are in English or in Russian

Are there any legal provisions on the country level related to e-participation? Laws, strategies, others. Please provide links if these acts or their summaries are in English or in Russian

What are the legal provisions on the country level related to access to public information (i.e. constitutional provisions, laws, acts or regulations)? Please provide links if these acts or their summaries are in English or in Russian

Is there a nationally accepted and shared definition for public information?

Institutional framework/actors

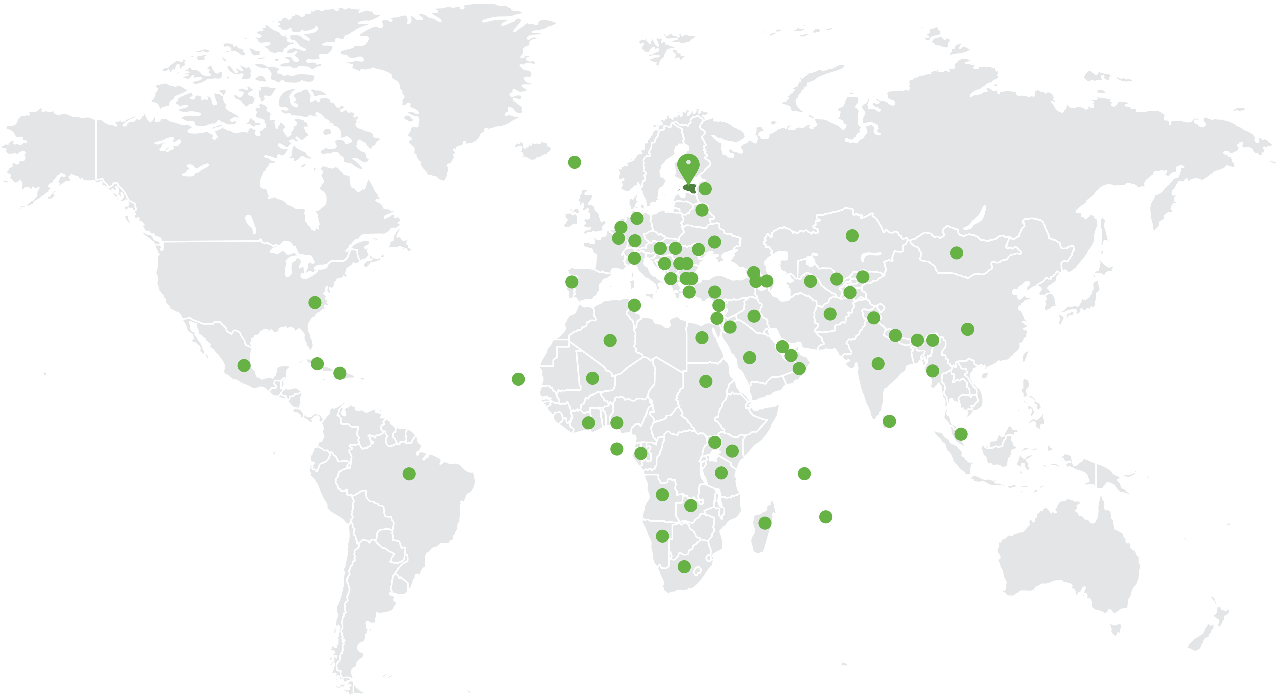
What governmental institution(s) is/are responsible for civic (e)-participation?

Who are the key stakeholders on the country level, in addition to the government, being responsible for/or playing an active role in promoting civic e-participation? Who is responsible for ensuring transparency in decision-making along with demanding transparency?

Main ICT tools and related projects

What are the most prominent cases of e-participation? Please briefly describe them and add the link if there is any information available about this case on the Internet.

eGA's activities around the world



eGA e-governance academy | 15 YEARS Empowering e-governance around the world

e-Governance Academy
Rotermanni 8, 10111 Tallinn, Estonia
+372 663 1500 | info@ega.ee | ega.ee
Follow us on Facebook | Twitter | LinkedIn: egovacademy