EU4Digital

EU4Digital: supporting digital economy and society in the Eastern Partnership

Cybersecurity guidelines for the Eastern Partner countries

June, 2020

Table of contents

1 Summary

EU4Digital facility team identified the main obstacles and gaps to address in the area of cybersecurity, and in order to strengthen the cybersecurity resilience in each Eastern Partner country. It was identified that countries are at different levels in implementing effective measures to manage cyber risks and threats.

The picture is quite varied in the case of cybersecurity legislation. Armenia, Azerbaijan, and Belarus have not yet adopted the national **cybersecurity strategies**, however, they implemented some other national regulations which partially address the issues related to cybersecurity, and in the case of Azerbaijan, the draft of the first Cybersecurity Strategy with the Action Plan has been submitted for approval by the President. Other countries like Moldova and Ukraine are in the process of reviewing and updating the existing strategy for the second time. Only Georgia has developed the third version of the National Cybersecurity Strategy and Action Plan for years 2020-2024, which is already waiting for approval.

None of the Eastern Partner countries have adopted the practices defined in the **NIS Directive** and current national regulations are not fully compatible with its requirements. Also, it was found that an object-oriented approach instead of service-oriented was established in all countries, thus the operators of essential services within the meaning of the NIS Directive are not identified in the Eastern Partner countries at the national level.

All countries designated the **entities responsible** for initiating and developing of cybersecurity policy, however, in some cases not all of them have been already established, and in other cases it can be observed that the responsibility for cybersecurity is scattered among different national authorities.

Regarding **baseline technical and organisational measures**, most of the Eastern Partner countries defined some of the key elements connected to cybersecurity, which are mainly based on ISO/IEC 27000 family of standards, but in some cases their application is limited to very particular sectors, usually banking and financial.

It was also found, that **cyber risk assessment** is not conducted at the national level in most of the Eastern Partner countries. In addition, analysed Eastern Partner countries do not have the methodology dedicated for national cyber risk assessment, however, in Azerbaijan, Belarus and Georgia cyber threat identification and analysis is a part of the generic risk assessment performed at the national level. For this reason, in most countries, cyber threats and vulnerabilities, notably those related to critical information infrastructures are currently not fully addressed.

Also, the **incident response mechanism** requires further improvement. Although most Eastern Partner countries build their incident response capabilities by creating a Computer Emergency Response Team (CERT) at the national level, the analysis shows that there is no obligation to report about cybersecurity incidents or it is limited to state information resources/electronic communication network operators. In addition, National Cyber Incident Response Plans are not established in most of the Eastern Partner countries. Thus, some improvements in incident reporting mechanism should be made by establishing criteria for incident classification and imposing an obligation on private and public entities to report incidents. Also, the adoption of a new law setting out the obligations arising from incident management is worth considering for both public and private sectors.

Regarding the **cooperation mechanism**, almost all countries declare cooperation with each other on specific cybersecurity incidents and sharing information about cyber risks.
In addition, national entities are engaged in cooperation and information sharing with other partners abroad, but cross-sectoral information exchange mechanisms require further development to raise the level of cybersecurity.

The detailed overview on cybersecurity of each Eastern Partner country's state of play, main challenges, and next actions are provided in the individual Eastern Partner country reports, which are annexed to this document and will serve as an input into the EU4Digital: Improving Cyber Resilience in the Eastern Partner Countries programme[1]. The essential extract from the information provided in particular state reports is Chapter 5: *Challenges and recommendations on key actions identified for the Eastern Partner region based on the country approaches to the cybersecurity* presenting details on the security measures implemented by individual Eastern Partner countries and indicating areas for improvement. In addition, the key challenges and recommended activities for the Eastern Partner region in the field of cybersecurity were indicated. It is worth pointing out, that

1 EU4Digital - The objective of the programme is to increase and enhance the cyber-resilience and criminal justice capacities of the Eastern Partner countries to better address the challenges of cyber threats and improve their overall security. It will focus on two goals, first - development of technical and cooperation mechanisms that increase cybersecurity and preparedness against cyber-attacks, second - the full implementation of an effective framework to combat cybercrime.

https://eufordigital.eu/discover-eu/eu4digital-improving-cyber-resilience-in-the-eastern-partnership-countries/

currently there are some initiatives/projects in region or specific countries running, which address some gaps/challenges, description of which was presented in Chapter 6.

The table and diagram below provide a very brief summary of the key observations and the general directions of cybersecurity for Eastern Partner countries.

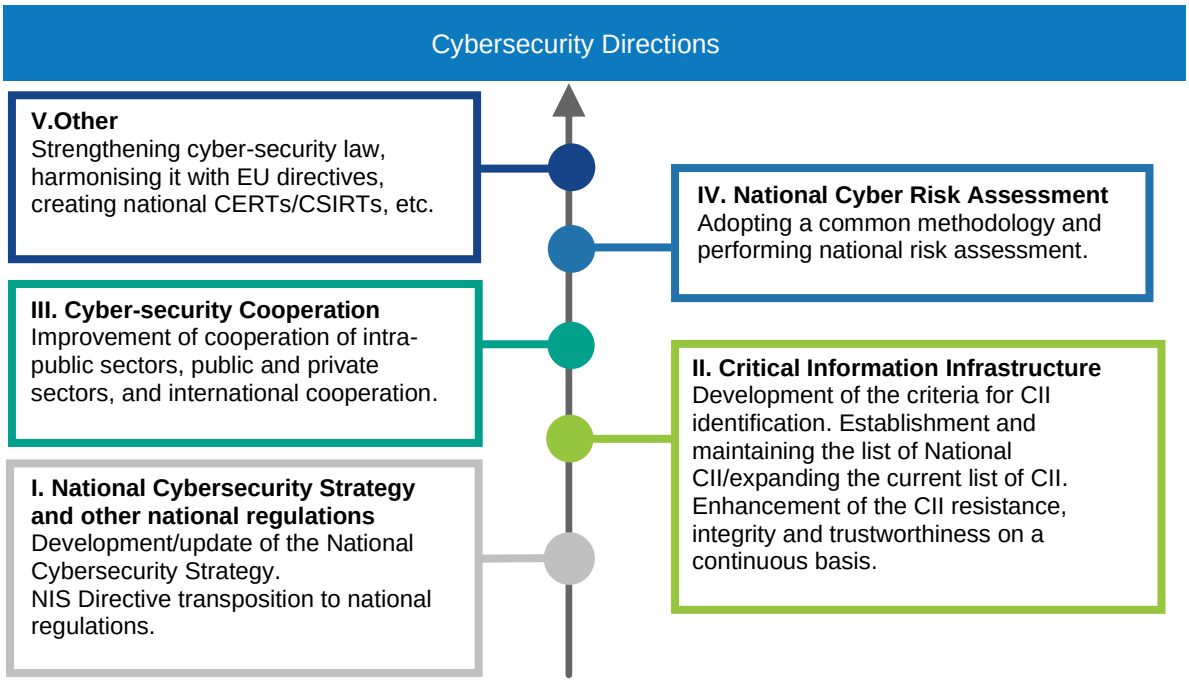
Country	Highlights
AM	The main challenges are insufficient funds and interest of authorities, lack of knowledge and expertise, legacy hardware and software which present a very high risk of cybersecurity incidents. In cybersecurity, the next steps for AM are the adoption of the national cybersecurity strategy, establishment of the national CERT, identification of critical infrastructure (CI) and critical information infrastructure (CII) operators.
AZ	The main challenges are insufficient funding, lack of qualified personnel and resources in the cybersecurity area, and insufficient commitment of national authorities to cybersecurity matters. The next steps for AZ are the creation of a security operations centre (SOC) within National CERT, harmonisation of personal data legislation with GDPR, development of legislation related to CII.
BY	Lack of national cyber risk management methodology is the major challenge in BY, as well as lack of qualified personnel and resources in the cyber area. The next steps for BY are creation and use of trusted/secure channels and services for constant (real-time) information exchange in the cybersecurity field and effective international cooperation between BY and the Eastern Partner countries.
GE	The main cybersecurity challenges in GE are insufficient funding, insufficient commitment of national authorities to cybersecurity matters, lack of awareness, and lack of qualified personnel and resources. The next steps in the cybersecurity area are strengthening the law on information security, adopting the practices defined in the NIS Directive, enhancing international cooperation, development of legislation related to CII.
MD	The main challenges in MD are lack of national CERT, lack of qualified personnel and resources, and insufficient funds dedicated for cybersecurity. The next steps for MD to strengthen cybersecurity resilience should be the establishment of national CERT, development of cyber-related skills, transposition of NIS directive, control and monitoring the application of minimum cybersecurity requirements.
UA	The main challenges in UA are insufficient funds and low interest of authorities in cybersecurity aspects, lack of qualified personnel and resources, and large volumes of legacy hardware and software presenting high cyber risks. The next steps for UA are enhancement of cross-border cooperation, adopting the practices defined in the NIS Directive, updating cybersecurity strategy, development of the partnership with technological and industrial partners.

Cybersecurity gaps and directions

Key gaps/ obstacles identified imply the key development directions that of establishment of national cyber security strategies, critical information infrastructure identification and risk management, cross-border and cross-sectoral cooperation, national-level cyber risk management and establishment of national CERTs/ CSIRTs

Common Gaps and Obstacles

1. Lack of qualified personnel.
2. Insufficient dedicated and systematic funding.
3. No National Cyber Strategy (NSC) or it is outdated and not aligned with NIS Directive.
4. Not established national-level contingency plans.
5. Not defined or incomplete Critical Information Infrastructure (CII) lists at a national level.
6. Not performed cyber risk assessments at the national level.


Cybersecurity Directions
V.Other
Strengthening cyber-security law, harmonising it with EU directives, creating national CERTs/CSIRTs, etc.
IV. National Cyber Risk Assessment
Adopting a common methodology and performing national risk assessment.
III. Cyber-security Cooperation
Improvement of cooperation of intra-public sectors, public and private sectors, and international cooperation.
II. Critical Information Infrastructure
Development of the criteria for CII identification. Establishment and maintaining the list of National CII/expanding the current list of CII. Enhancement of the CII resistance, integrity and trustworthiness on a continuous basis.
I. National Cybersecurity Strategy and other national regulations
Development/update of the National Cybersecurity Strategy.
NIS Directive transposition to national regulations.

2 Introduction

Information and communication technologies (ICT) have become the main cause of growth in the European markets. Since our reliance on digital assets will only increase in the future and the markets and environmental volatility is becoming the norm, the Internet, digital technologies, network and information systems are becoming the core of Europe's Society and the Digital Single Market. Therefore, ensuring the security of information systems has become one of the main objectives. In the EU, since 2010 several legal regulations have been established to support the development of digital transformation, for both public administration and private enterprises.

First of all, in 2010 the European Commission has launched the **Europe 2020 Strategy**[2]. One of the flagship initiatives of which was **Digital Agenda for Europe**[3], published in May 2010 and focused on the economic and social use of ICT services, promoting digital skills and high-performance computing, digitising industry and modernising public services by introducing eGovernment services, which are to contribute to reducing costs and saving time for public administration authorities.

The implementation of the Agenda's provisions expected the growth of innovations, economic growth, and improvement of everyday life of citizens and enterprises. In addition, the implementation of the Agenda's provisions expected the growth of innovations, economic growth, and improvement of everyday life of citizens and enterprises. In addition, it considered the need to create a truly single market for online content and services, i.e. borderless and safe EU web services and digital content markets, with high levels of trust and confidence as well as a balanced regulatory framework with clear rights regimes and transformation of governments.

To achieve this goal, in 2015 the Commission launched the **Digital Single Market** (DSM)[4], which designates the strategy for the best possible access to the online world for individuals and businesses, ensuring access and engagement in online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence. The accomplishment of the DSM was identified as one of the European Commission's 10 political priorities. In addition, it announces the launch of a new **eGovernment Action Plan for 2016 - 2020**[5], a political instrument, which sets out concrete actions to accelerate the implementation of existing legislation and the related take-up of online public services. The Action Plan provides coordination of public sector modernisation efforts and resources in the field of eGovernment helping to remove existing digital barriers to the Digital Single Market and to prevent further IT fragmentation arising in the context of the public sector modernisation.

Opening the data and services between public administrations within and across borders, on the one hand, increases their efficiency and facilitates the free movement of businesses and citizens, but on the other hand, it needs proper protection of all data and systems. Cyber threats are constantly evolving and can have disastrous effect on data. Thus, securing network and information systems in the European Union is essential to keep the online economy running and to ensure prosperity.

According to that, the European Union takes a number of initiatives to promote cyber resilience. The first piece of EU-wide legislation on cybersecurity is the **Network and Information Security (NIS) Directive**[6], which was adopted by the European Parliament on 6 July 2016. This first comprehensive legislation on cybersecurity aims to raise the overall level of security of the online environment in Europe. It was created for increasing both cyber and physical resilience of essential services (energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure) and network and information systems that are critical for the provision of digital services (search engines, cloud computing services, and online marketplaces). Indeed, the failure of information systems managed by the operators of essential services (OES) and digital service providers (DSP) might have strong consequences, from the monetary losses and reputation for companies to the disruption of the provision of goods, essential services to the society, loss of health and a long-lasting economic crisis throughout the European Union. Thus, it has become even more critical to ensure the cyber resilience of OES's and DSPs.

Therefore, under the NIS Regulations both, operators of essential services and digital service providers, have been required to comply with the security and notification requirements. That means they have to take appropriate and proportionate technical and organisational measures to manage risks posed to the security of the network and information systems on which their services rely. As cybersecurity is a joint effort, the NIS

2 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC2020&from=EN

3 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN

4 https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market

5 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0179&from=EN

6 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

Regulations impose also the obligation on the Member States to become highly recommendable to European partner countries. Accordingly, they are required to build their incident response capabilities by creating a Computer Security Incident Response Team (CSIRT) at the national level and cooperate with each other on specific cybersecurity incidents and sharing information about cyber risks.

A further step taken by the Commission in its efforts to build a coherent, secure, single cybersecurity market – in terms of products, services, and processes was the adoption of the **Cybersecurity Act**. The regulation adopted by the Council on 9 April 2019, reinforces the mandate of the European Union Agency for Cybersecurity and establishes a certification framework for ICT digital products, services, and processes, to help understand their security features and avoid fragmentation in the European Single Market.

To keep cyberspace open and stable there is also a growing need to protect the integrity and security of the states and their citizens against malicious cyber activities. All states in Europe have to increase their cooperation on cyber defence and strengthen their capacities in this field. To help achieve this goal, on 17 May 2019 the Council adopted an updated version of the European Union **Cyber Defence Policy Framework**, which allows the EU to take account of the changing security challenges. This is the first time when the Council decision allows the EU to sanction persons or entities associated with them that are responsible for cyber-attacks, provide financial, technical, or material support for such attacks, which constitute external threat not only to the EU or its member states, but also to non-EU states or international organisations.

In addition, continuously evolving challenges presented by the cyberspace undoubtedly impose requirements for investment in stronger pioneering cybersecurity capacity and technological solutions. Recognising this need, the Commission proposed a regulation establishing the **European Cybersecurity Industrial, Technology and Research Competence Centre** and the **Network of National Coordination Centres**[7], which allows for better use of the existing cybersecurity resources and expertise and for better coordination between cybersecurity investments at the EU level. The main aim of the regulation is building the community of a large and diverse group of entities involved in cybersecurity technology, including in particular research entities, industries, and the public sector, which will help retain and develop the capacities necessary to secure the Digital Single Market.

Digitalisation is not a choice, but a necessity for European businesses and economies as a whole. To make better use of the great opportunities offered by digital technologies, which do not know any borders, all states should have the same understanding of the measures and standards in providing security of these areas. They must work on a number of fronts to promote cyber resilience, which means they must develop and establish specific laws in the area of network security information, prepare an appropriate organisational and legal framework for the development of business in cyberspace, implement appropriate cybersecurity measures, understand the risk posed by cyber threats and respond to cybersecurity attacks. As the importance of cross-border cooperation between the countries and free movement of services is increasing day by day, it is important to include and accompany the Eastern Partner countries in this transition as well.

Through the *EU4Digital: supporting digital economy and society in the Eastern Partnership* (project number ENI/2018/396-727) between 2019 and 2022, the Council of Europe and the European Union aims to extend the benefits of the European Union's Digital Single Market to the Eastern Partner states. The programme focuses on support across six key policy areas. One of them, *Trust and security,* supports States participating in the Eastern Partner Facility (Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine) among others in strengthening their cybersecurity and improvement of their critical information infrastructure resilience, which is necessary not only to develop e-governance but also for commercial and cultural content and services flow across borders. The project has provided an opportunity to assess the readiness and capability of ensuring safety and security of the cyberspace across the region and exchange ideas for improvement. The assessment describes the as-is situation of implementation of cybersecurity policies and measures in the Eastern Partner countries. An additional attempt has been made to provide an overview of the current gaps and weaknesses of the state's regulations, policies and security measures already implemented by six Eastern Partner countries and determine the level of maturity of individual cybersecurity solutions in each country.

Furthermore, the main goal of the project is to provide a set of good practices and recommendations to Eastern Partner countries' national authorities in the field of cybersecurity, which will contribute to a stronger and resilient cyberspace among the partner countries and decrease the risk of disruption or failure of network information systems.

7 https://ec.europa.eu/digital-single-market/en/european-cybersecurity-industrial-technology-and-research-competence-centre

3 Identification of main stakeholders

Invitations to participate in the study were sent to the expert groups and other Eastern Partner countries' representatives, responsible for the cybersecurity in their country. The stakeholders from the Eastern Partner region involved in the project included mainly the representatives of the national cybersecurity authorities, national regulatory authorities/institutions, responsible for initiating and developing cybersecurity policy and regulations or ministries responsible for communication and information technologies, cybersecurity. In particular, the following public organisations or national authorities were engaged:

1. **Armenia** – representatives from public organisations, e.g. EKENG CJSC – Office of Implementation of Electronic Governance Infrastructure, coordinator of e-government projects in the Republic of Armenia, founded by the Government of the Republic of Armenia, Ministry of High-tech Industries of the Republic of Armenia, which currently coordinates the activities related to cybersecurity.
2. **Azerbaijan** – representatives from public authorities, e.g. Ministry of Transport, Communications and High Technologies of the Republic of Azerbaijan, a governmental agency within the Cabinet of Azerbaijan in charge of regulation of the communications sector and development of information technologies in the country.
3. **Belarus** – representatives from public authorities, e.g. Operations and Analysis Center under the President of the Republic of Belarus.
4. **Georgia** – representatives from public authorities, e.g. Data Exchange Agency.
5. **Moldova** – representatives from public authorities, e.g. Ministry of Economy and Infrastructure.
6. **Ukraine** – representatives from public authorities, e.g. State Service of Special Communication and Information Protection of Ukraine.

4 Methodology

The project used a combination of three empirical techniques:

1. a literature review (public accessible standards, guidelines, the Eastern Partner countrys' government published data, ENISA's publications, white papers which describe cybersecurity best practices, etc.);
2. a documentation review (national and international regulations, e.g. National Strategies, Action Plans, etc.);
3. interviews with relevant stakeholders from all six countries of the Eastern Partner Region.

As a first step, to gain the necessary information a questionnaire was prepared and distributed to representatives of the Eastern Partner countries during the Trust and security network workshop in Chisinau, Moldova on 12-13 June 2019.

The information gained through the questionnaire was complemented by desk research and a series of interviews with representatives of the national cybersecurity authorities or national regulatory authorities of all six Eastern Partner countries.

Following the completion of the interview and analysis phase, a mapping of the implemented measures across the examined cybersecurity domains was created. Based on this, the Cybersecurity state reports were created for each particular Eastern Partner country containing the description of the implemented security measures in the following areas:

- Cybersecurity Legislation;
- Mandatory minimum requirements for cybersecurity;
- Critical Infrastructure/Critical Information Infrastructure;
- National Risk Assessment;
- Reporting Mechanism/Incident Management;
- Cooperation Mechanisms;
- Data Protection;
- Cybersecurity Culture;
- Cybercrime;
- Funding Mechanisms.

In addition, the reports contain the list of the current gaps and weaknesses of the state's regulations, policies and security measures already implemented by six Eastern Partner countries together with the list of main obstacles and barriers in the implementation of cybersecurity initiatives. The reports constitute an integral part of this document, which will be provided to the European Commission. Separately each of the reports will be distributed to a particular Eastern Partner country as an attachment to the guidelines.

As a final step, recommendations were identified and prepared in the form of the guidelines constituting Chapter 5 of this document. The results of the guidelines have been presented at the *EU4Digital: Trust and Security Network, Teleconference*, on 17 April 2020; inputs and comments gathered during the workshop were elaborated and included in this guide.

The guidelines provide recommendations to countries on how to continue with the development of their cybersecurity and recommendations for effective practices in developing, implementing, evaluating, and maintaining cybersecurity measures.

5 Challenges and recommendations on key actions identified for the Eastern Partner countries based on the countries' approach on cybersecurity

Countries of the Eastern Partnership, as many other states around the world have been the target of cyberattacks and other security incidents in recent years. As it was recognised in the Global Strategy for the European Union's Foreign and Security Policy[8] that the internal security of the EU depends on external security, thus apart from the EU Member States, neighbor countries need to be closely involved in building the resilience of cyberspace as well.

The cybersecurity of network and information systems represent the first layer of protection of online services. Thus, it is extremely important to review the approach of each country on cybersecurity, identify current gaps and weaknesses in this field, which serves the basis to take appropriate actions to strengthen the cybersecurity and improve the critical infrastructure resilience.

To accomplish these goals the analysis of already implemented security measures was conducted in the following areas:

- Cybersecurity Legislation;
- Mandatory minimum requirements for cybersecurity;
- Critical Infrastructure/Critical Information Infrastructure;
- National Risk Assessment;
- Reporting Mechanism/Incident Management;
- Cooperation Mechanisms;
- Data Protection;
- Cybersecurity Culture;
- Cybercrime;
- Funding Mechanisms.

The core of this chapter is the summary description of the state of play for each of the six Eastern Partner countries. It provides a brief overview of the current status regarding cybersecurity in the Eastern Partner countries region. This part of the document was prepared for the purpose of creating a comprehensive summary of implemented security measures in 10 above mentioned areas, from which officials of the Eastern Partner countries can draw meaningful conclusions and gain a better understanding of major challenges in the field of cybersecurity. The main objective of this analysis is the enhancement of the Eastern Partner countries' cybersecurity awareness and identification of areas for improvement. In addition, the key challenges cybersecurity officials face and the priority activities that need to be taken are listed.

The table below summarises the results of the analysis of cyber-maturity levels of individual cybersecurity elements in each Eastern Partner country. Cyber-maturity levels for each country have been drawn from the assessment criteria described in Annex 1 and information gathered directly from the Eastern Partner countries. It presents an estimated country commitment to cybersecurity which has can be assigned by four categories: initial, managed, and defined.

The Cyber Security Maturity matrix provides a basic roadmap showing capability and progression in a particular area and indicating the domains, which have to be strengthened as a first priority. It shows, that all of the Eastern Partner countries take security measures to manage cyber risks and threats, however, the picture varies for particular cybersecurity domains. In general, the cybersecurity maturity for most of the areas was estimated as managed which means that cybersecurity processes are organised and structured.

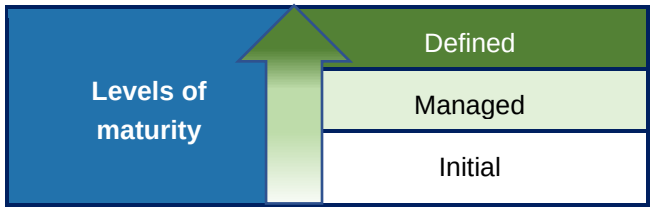
Security efforts are taken at the national level and some basic cybersecurity measures are established and implemented. All countries designated the entities responsible for initiating and developing cybersecurity policy, however in most cases the responsibility for cybersecurity is scattered among different national authorities. National regulations related to cybersecurity exist, but in many cases they do not fully address the issues related to this topic.

8 https://eeas.europa.eu/sites/eeas/files/eugs_review_web_0.pdf

The maturity of four cybersecurity domains related to essential services/CII identification, national risk assessment management, reporting, and founding mechanisms was estimated as initial, which shows that actions taken in these areas require further improvement and investment, making this security domain a core priority. Particularly, national authorities should have a clear understanding of the cybersecurity vulnerabilities and assets or processes that are potentially at risk to develop the efficient cybersecurity programme. Thus, Eastern Partner countries should conduct a cyber risk assessment to determine the greatest cybersecurity threats. To do this, a robust cyber risk assessment methodology is required to ensure all risks and vulnerabilities are identified. Threats and vulnerabilities should be documented and based on them proper security controls need to be selected and applied to mitigate assessed risks. In addition, suitable policies, procedures, and processes related to cybersecurity risk management need to be determined and communicated to all relevant stakeholders. The appropriate safeguards, developed and implemented, are important to ensure the delivery of critical infrastructure services. In addition, the monitoring system of information network and assets should be implemented together with the efficient reporting mechanism, to ensure timely and adequate response to a cybersecurity incident. A wide approach to security should be also implemented through the development of a security culture as well as a security model that encourages close cooperation between all relevant stakeholders, both within the public and private entities. Effective governance should be evidenced also in sufficient staffing, insightful training, and adequate funding.

Table 1: Summary of the estimate of maturity levels for each country drawn from the assessment criteria described in Annex 1 and information gathered from the Eastern Partner countries

Cybersecurity domains	AM	AZ	BY	GE	MD	UA
Cybersecurity Legislation	Managed	Managed	Managed	Managed	Managed	Managed
Cybersecurity Measures	Managed	Managed	Managed	Managed	Managed	Managed
Essential Services/CII	Initial	Initial	Managed	Initial	Initial	Managed
National Risk Assessment	Initial	Managed	Managed	Managed	Initial	Initial
Reporting Mechanism/ Incident Management	Initial	Managed	Managed	Managed	Managed	Managed
Cooperation Mechanism	Managed	Managed	Managed	Initial	Initial	Managed
Data Protection	Managed	Managed	Initial	Managed	Managed	Managed
Cybersecurity culture	Managed	Managed	Managed	Managed	Managed	Managed
Cybercrime	Managed	Managed	Managed	Managed	Managed	Managed
Funding mechanism	Initial	Initial	Managed	Managed	Managed	Managed



Source: Developed by EU4Digital Facility

In the table below there are details provided on the security measures implemented by Eastern Partner countries and areas for improvement. In addition, the key challenges and recommended activities for the Eastern Partner countries in the field of cybersecurity were indicated. However, as there are different levels of advancement in the Eastern Partner countries, specific activities and objectives should also be defined at later stages to address the specific situations of each country.

Table 2: Summary of the state of play in cybersecurity legislation in Eastern Partner countries: identified challenges and key recommended activities

<table>
<tr><th colspan="6">Cybersecurity Legislation</th></tr>
<tr><th colspan="3">Gaps/Challenges</th><th colspan="3">Key Recommended Activities</th></tr>
<tr><td colspan="3">National cybersecurity strategy is not established in half of the Eastern Partner countries.
Cybersecurity roles for national authorities are not clearly defined.
Newly created Cybersecurity Strategies are not fully implemented.
Some of the laws related to cybersecurity are outdated and not compatible with current EU legislation and cybersecurity standards.
The practices defined within NIS Directive are not adopted in the Eastern Partner countries.
Current national regulations are not fully compatible with the requirements of NIS directive.
Lack of awareness of the importance of NIS.</td><td colspan="3">Review of current legislation to verify its compatibility with EU legislation and good practices.
Need to consider adjustments of the national cyber legislation to take on practices of recent EU legislation (e.g. NIS Directive, Regulation (EU) 2019/881) and current standards.
Creation of a comprehensive legal framework by the competent authorities of the state, that covers all aspects of network and information security, including cybercrime and the protection of personal data.
Developing of cybersecurity governance: strengthening policies and awareness of decision-makers, development of necessary structures, and processes to help better govern cybersecurity.</td></tr>
<tr><th>ARMENIA</th><th>AZERBAIJAN</th><th>BELARUS</th><th>GEORGIA</th><th>MOLDOVA</th><th>UKRAINE</th></tr>
<tr><th colspan="6">National Cybersecurity Strategy</th></tr>
<tr><td>The National Cybersecurity Strategy is not established.</td><td>The National Cybersecurity Strategy is not established.
Note: at the time of preparation of this report, the draft of the Cybersecurity Strategy with the Action Plan has been submitted for approval by the President of the Republic of Azerbaijan.
multi-stakeholder consultation was</td><td>The National Cybersecurity Strategy is not established.
The Information Security Concept (the document is confidential) was prepared and approved in 2019.
Multi-stakeholder consultation was implemented during Information Security Concept development.</td><td>Third version of the National Cybersecurity Strategy and Action Plan for 2020-2024 has been developed but not adopted yet.
Multi-stakeholder consultation was implemented during strategy development.</td><td>The National Cybersecurity Program for the years 2016-2020 was approved in 2015.
Multi-stakeholder consultation was implemented during the strategy development.</td><td>The National Cybersecurity Strategy was established in 2016.
Multi-stakeholders consultation was implemented during strategy development.</td></tr>
</table>

	implemented during strategy development.				
Other National Legislation related to cybersecurity					
• National regulations related to cybersecurity are partially adopted, inter alia by legal acts that of: ○ Law on electronic communication; ○ Law on the electronic document and the electronic digital signature; ○ Law on Protection of Personal Data.	• National regulations related to cybersecurity are partially adopted, inter alia by legal acts that of: ○ Law on Information, Informatisation and Protection of Information; ○ Law on National Security; ○ Law on e-signature and e-document; ○ Law on Telecommunication; ○ Law on Protection of Personal Data.	• National regulations related to cybersecurity are partially adopted, inter alia by legal acts that of: ○ Law on information, informatisation and protection of information; ○ Law on e-document and digital signature; ○ Strategy of development of informatisation.	• National regulations related to cybersecurity are partially adopted, inter alia by legal acts that of: ○ Law on Information Security.	• National regulations related to cybersecurity are partially adopted inter alia by legal acts that of: ○ Law on electronic communications.	• National regulations related to cybersecurity are partially adopted inter alia by legal acts that of: ○ Law on base principles of Cybersecurity; ○ Law on information protection in information and telecommunication systems; ○ Order on Online Vulnerability Scanning of the State's Information Resources Online; ○ Order on Rules on the Protection of Information and Telecommunication Systems.
Responsible Entities					
Responsibility for cybersecurity is distributed among different national authorities.	Responsibility for cybersecurity is distributed among different national authorities.	One entity (Operational and Analytical Center - OAC) under the President of the Republic of Belarus responsible for initiating and developing cybersecurity policy is designated.	Responsibility for cybersecurity is distributed among different national authorities.	Responsibility for cybersecurity is distributed among different national authorities.	Responsibility for cybersecurity is distributed among different national authorities.
NIS Implementation					
Not implemented	Not implemented	Not implemented	Not implemented	Not implemented	Not implemented

Source: Developed by EU4Digital Facility

Table 3: Summary of the state of play on mandatory minimum requirements for cybersecurity in the Eastern Partner countries: identified challenges and key recommended activities

<table>
<tr><th colspan="6">Mandatory Minimum Requirements for Cybersecurity / Cybersecurity Measure</th></tr>
<tr><th colspan="3">Gaps/Challenges</th><th colspan="3">Key Recommended Activities</th></tr>
<tr><td colspan="3">1. Cybersecurity measures are not defined at the national level only in one Eastern Partner country.
2. Lack of audit standards for verifying whether baseline cybersecurity measures are implemented.</td><td colspan="3">1. Consider the implementation of the extensions to define the cybersecurity measures to be implemented by private companies.
2. Consider defining and executing the programmes for the implementation of security measures by critical information infrastructure operators.
3. Obliging governmental entities to adopt basic cybersecurity measures.
4. Establishing national audit standards and requirements.</td></tr>
<tr><th>ARMENIA</th><th>AZERBAIJAN</th><th>BELARUS</th><th>GEORGIA</th><th>MOLDOVA</th><th>UKRAINE</th></tr>
<tr><td colspan="6">Baseline Cybersecurity Measures and Obligations</td></tr>
<tr><td>• Not defined at a national level, only banking and financial sector follow the agreed technical and organisational measures.
• Mandatory only for banking and financial sector.</td><td>• Have been defined at a national level.
• Mainly based on ISO/IEC 27,000 family of standards.
• Mandatory for government entities, essential service operators, and private organisations (banking sector only).</td><td>• Have been defined at the national level.
• Based on Belarusian Standards STB 34.101.1-3 (Common Criteria), STB ISO/IEC 2700X - 270XX, STB 34.101.70.
• Mandatory for government entities, essential service operators, private organisations, critical information infrastructure operators.</td><td>• Have been defined at the national level.
• Mainly based on ISO/IEC 27,000 family of standards.
• Mandatory for critical information infrastructure operators.</td><td>• Have been defined at a national level.
• Mainly based on ISO/IEC 27,000 family of standards.
• Mandatory for electronic communication operators and the public authorities subordinated to the Government with the regard to the existing information systems and information systems under development.</td><td>• Have been defined at the national level.
• Mainly based on ISO and NIST standards.
• Mandatory for government entities, public organisations, private organisations.</td></tr>
<tr><td colspan="6">Audits</td></tr>
<tr><td>• Periodic audits conducted in government entities for compliance with the ISO/IEC 27,000 standard.</td><td>• Audits are carried out for verifying whether baseline cybersecurity measures are implemented in the government organisation audits in the private sector (banking only) are carried out according to their internal regulation.</td><td>• Audits are carried out every five years to verify whether baseline cybersecurity measures are implemented.</td><td>• Audits are carried out annually to verify whether baseline cybersecurity measures are implemented.</td><td>• Audits are carried out annually to verify whether baseline cybersecurity measures are implemented.</td><td>• Audits are carried out periodically to verify whether baseline cybersecurity measures are implemented.</td></tr>
</table>

Source: Developed by EU4Digital Facility

Table 4: Summary of the state of play analysis on the Critical Infrastructure protection approach in the Eastern Partner countries: identified challenges and key recommended activities

CRITICAL INFRASTRUCTURE (CI)						
GAPS/CHALLENGES		**KEY RECOMMENDED ACTIVITIES**				
1. The definitions of the term 'critical infrastructure' ('CI') vary across countries. 2. The official lists of CIs have not been established at the national level in half of the Eastern Partner countries. 3. In other Eastern Partner countries, CIs are identified at the national level, however in most cases there are still missing provisions on identifying CI and the clear delimitation of the attributions of the involved actors. 4. 'Object-oriented' (e.g. particular physical objects or locations) approach implemented rather than 'service-oriented'. In most cases the particular assets/objects instead of critical services are identified and protected at the national level. 5. The operators of essential services, within the meaning of the NIS Directive, are not identified at the national level.	1. Developing or enhancing of the national laws in the field of critical infrastructure (CI) protection. 2. Establishing methodology for identification of CI and designation of CI operators. 3. Identifying CI operators within the private sector. 4. Establishing a protection system dedicated to CI. 5. Enhancing CI resilience capabilities on a continuous basis. 6. Establishing regular testing of exercises to detect cybersecurity vulnerabilities in CI. 7. Identifying services, which are critical for the functioning of the state and society and operators responsible for the protection of the essential services. 8. Considering setting the national competent authority responsible for the identification at the national level.	• Defined as the most important/vital objects. • There is a formal list of assets identified as critical infrastructure. • CI operators have been officially designated (identified and officially approved) at the national level.	• Defined as assets and services critical to the proper functioning of the society and economy. • There is a formal list of assets identified as critical infrastructure (no private objects are listed as CI). • CI operators have been officially designated (identified and officially approved) at the national level.	• Lack of formal definition of CI. • There is no formal list of assets identified as critical infrastructure. • CI operators have not been officially designated (identified and officially approved) at the national level.	• Defined as an element, system or component essential for maintaining the vital functions of society, health, safety, security and social and economic well-being. • There is a formal list of assets identified as critical infrastructure. • CI operators have been officially designated (identified and officially approved) at the national level.	• No information. • There is no formal list of assets identified as critical infrastructure. • CI operators have not been officially designated (identified and officially approved) at the national level yet.

ARMENIA	AZERBAIJAN	BELARUS	GEORGIA	MOLDOVA	UKRAINE	ARMENIA
Essential Services						
• Lack of formal definition within the meaning of the NIS Directive. • Essential services are defined as systems which are connected to the government interoperability platform and documentation management systems. • There is no formal list of services critical to the proper functioning of the society and economy within the meaning of the NIS Directive. • Operators of essential services (in the meaning of the national definition) have been identified.	• Lack of formal definition within the meaning of the NIS Directive. • There is no formal list of services critical to the proper functioning of the society and economy within the meaning of the NIS Directive.	• Lack of formal definition within the meaning of the NIS Directive. • There is no formal list including both services and objects critical to the proper functioning of the society and economy.	• Lack of formal definition within the meaning of the NIS Directive. • There is no formal list of services critical to the proper functioning of the society and economy within the meaning of the NIS Directive.	• Lack of formal definition within the meaning of the NIS Directive. • There is no formal list of services critical to the proper functioning of the society and economy within the meaning of the NIS Directive.	• Lack of formal definition within the meaning of the NIS Directive. • There is no formal list of services critical to the proper functioning of the society and economy within the meaning of the NIS Directive.	• Lack of formal definition within the meaning of the NIS Directive. • Essential services are defined as systems which are connected to the government interoperability platform and documentation management systems. • There is no formal list of services critical to the proper functioning of the society and economy within the meaning of the NIS Directive. • Operators of essential services (in the meaning of the national definition) have been identified.

Source: Developed by EU4Digital Facility

Table 5: Summary of the state of play on the Critical Information Infrastructure approach in the Eastern Partner countries: identified challenges and key recommended activities

<table>
<tr><th colspan="6">CRITICAL INFORMATION INFRASTRUCTURE (CII)</th></tr>
<tr><th colspan="3">GAPS/CHALLENGES</th><th colspan="3">KEY RECOMMENDED ACTIVITIES</th></tr>
<tr><td colspan="3">1. There is no formal definition of critical information infrastructure (CII) in most of the Eastern Partner countries.
2. The official lists of CII and CII operators have not been established in most of the Eastern Partner countries.
3. In most cases there is lack of normative legislation determining the protection of critical information infrastructures.</td><td colspan="3">1. Development of national law in the field of critical information infrastructure (CII) protection.
2. Establishment of a methodology for identification of critical network and information systems (CII) and designation of CII operators.
3. Identification of CII operators within the private sector.
4. Enhancement, on a continuous basis, the CII cyber resilience integrity and trustworthiness.
5. Adopting methodologies for regular testing based on CII penetration testing principles to detect vulnerabilities in information systems and networks and performing the tests accordingly.
6. Identification and managing information about couplings and interrelations between CI and CII.
7. Considering the establishment of national competent authorities responsible for mapping and identifying of CII as well as supervising the fulfilment of obligations by CII operators.</td></tr>
<tr><th>ARMENIA</th><th>AZERBAIJAN</th><th>BELARUS</th><th>GEORGIA</th><th>MOLDOVA</th><th>UKRAINE</th></tr>
<tr><td colspan="6">Definition of CII</td></tr>
<tr><td>• No information</td><td>• There is no formal definition of Critical Information Infrastructure.</td><td>• No information</td><td>• Defined as a Critical Information System Subject – a legal entity or state agency, uninterrupted operation of information systems of which is important for the defense and/or economic security of the state, as well as for normal functioning of the state and/or society.</td><td>• There is no formal definition of Critical Information Infrastructure.</td><td>• Defined as a communication or technological system of the CI object whose cyber-attack would directly affect their sustainable operation.</td></tr>
</table>

Identification of CII					
• CII operators are not identified at the national level. • There is no formal list of Critical Information Infrastructure established at the national level.	• CII operators are not identified at the national level. • There is no formal list of Critical Information Infrastructure established at the national level.	• CII operators are identified at the national level – currently only within the public sector. • The list of important objects of informatisation are established at the national level.	• CII operators are identified at the national level – currently only within the public sector.	• CII operators are not identified at the national level. • There is no formal list of Critical Information Infrastructure established at the national level.	• CII operators are not identified at the national level. • There is no formal list of Critical Information Infrastructure established at the national level.

Source: Developed by EU4Digital Facility

Table 6: Summary state of play analysis on the national risk assessment process implemented in the Eastern Partner countries: identified challenges and key recommended activities

<table>
<tr><th colspan="6">NATIONAL RISK ASSESSMENT</th></tr>
<tr><th colspan="3">GAPS/CHALLENGES</th><th colspan="3">KEY RECOMMENDED ACTIVITIES</th></tr>
<tr><td colspan="3">1. No cyber risk assessments are conducted at the national level in all of the Eastern Partner countries.
2. Cyber risk assessment prevails and is limited to certain stakeholders, mainly to the banking sector.
3. Lack of methodology for national risk assessment.
4. In most countries, cyber threats and vulnerabilities, notably those related to critical information infrastructures, are not identified and not addressed.</td><td colspan="3">1. Establishment of national cyber risk assessment.
2. Alternatively, reinforcement/adaptation of existing national risk assessment methodology in order to include cybersecurity issues.
3. Designation of the national authorities responsible for the cyber risk assessment at the national level.
4. Developing the national programme dedicated for the implementation of cyber risk assessment and monitoring.
5. Involvement of CI and CII operators in conducting cyber risk assessment.
6. Identifying key cyber threats and vulnerabilities of Critical Infrastructures/Critical Information Infrastructures.</td></tr>
<tr><th>Armenia</th><th>Azerbaijan</th><th>Belarus</th><th>Georgia</th><th>Moldova</th><th>Ukraine</th></tr>
<tr><td colspan="6">Establishment</td></tr>
<tr><td>• Cyber risk assessment is not conducted at the national level.
• National risk assessment is not performed at the national level (national risk assessment is going to be established for the public entities with the Council of Digitalisation).</td><td>• Cyber risk assessment is not conducted at the national level, however national risk assessment addresses cyber threats.
• Cyber risk and vulnerability assessments are regularly carried out only in the financial sector.</td><td>• Cyber risk assessment is conducted at the national level as part of the national risk assessment.
• National risk assessment methodology has been developed based on ISO 27,000 family of standards and is used to assess any national threats at any area (including cyber).</td><td>• Cyber risk assessment is not conducted at the national level, however, national risk assessment addresses cyber threats.
• Cyber risk assessments are performed by CII operators, based on methodologies of their own choice.</td><td>• Cyber risk assessment is not conducted at the national level, however, some public institutions, including critical ones are obligated to conduct cyber risk assessment.
• National risk assessment does not address cyber threats.</td><td>• Cyber risk assessment is not conducted at the national level.
• National risk assessment is not performed at the national level.</td></tr>
</table>

Source: Developed by EU4Digital Facility

Table 7: Summary of the state of play on the reporting mechanism and incident management process implemented in the Eastern Partner countries: identified challenges and key recommended activities

<table>
<tr><th colspan="6">REPORTING MECHANISM/ INCIDENT MANAGEMENT</th></tr>
<tr><th colspan="3">GAPS/CHALLENGES</th><th colspan="3">KEY RECOMMENDED ACTIVITIES</th></tr>
<tr><td colspan="3">1. Not all countries have established national CERTs/CSIRTs.
2. Lack of sectoral CERTs/CSIRTs
3. Incident Response Mechanism has not been established in almost all Eastern Partner countries.
4. Lack of obligations for reporting cybersecurity incidents.
5. No cyber Contingency Plans are developed at the national level.
6. Lack of procedure describing how to act in case of occurrence of cybersecurity incidents.</td><td colspan="3">1. Establishment and operationalisation of national CERTs/CSIRTs. Development of regulations on establishing national CERTs/CSIRTs.
2. Considering the designation of one or more Computer Security Incident Response Teams (CSIRTs) for comprehensive incident management nationwide.
3. Considering the possibility of establishment of sectoral CERTs.
4. Creation or adaptation of the necessary structures and instruments within the competent authorities to secure the demands and capabilities of immediate incident response.
5. Developing an initiative to implement a monitoring system to alert unusual events on the network.
6. Involving private entities in the network security monitoring system.
7. Establishing the Incident Response Mechanism at the national level/Preparation of National Cyber Incident Response Plan.
8. Establishing criteria for the classification of cyber incidents.
9. Development of incident classification framework enabling the proper prioritisation of incidents, which allow to specify what kind of events have to be reported and how to handle incidents based on their category.
10. Imposing an obligation on private and public entities to report cyber incidents.
11. Adoption of a new law setting out the obligations arising from incident management for both public and private sectors.
12. Preparation of National Cyber Contingency Plan for responding and recovering services following major incidents that involve critical information infrastructures.</td></tr>
<tr><th>Armenia</th><th>Azerbaijan</th><th>Belarus</th><th>Georgia</th><th>Moldova</th><th>Ukraine</th></tr>
<tr><th colspan="6">Existence of Incident Response Mechanism</th></tr>
<tr><td>Not established at the national level.</td><td>Not established at the national level.</td><td>Not established at the national level.</td><td>Not established at the national level.</td><td>Not established at the national level.</td><td>Not established at the national level.</td></tr>
</table>

Obligation					
No obligation to report about cybersecurity incidents.	No obligation to report about cybersecurity incidents.	It is mandatory to report only incidents related to confidential/restricted information.	Public sector entities classified as CII operators are obliged to report significant security incidents.	Obligation to report about significant security incident imposed only for electronic communication network operators.	By law, public and private State Information Resources' operators are obliged to report any significant cybersecurity incidents.
CERT					
• There is no CERT established at the national level. • CERT AM and AM NREN CSIRT exist, but these are not official initiatives of national authorities. They are self-initiatives not supported by the government; however, they do cooperate with e-Governance Infrastructure Implementation Unit (EKENG) CJSC.	There are three CERT's established: 1. CERT.GOV.AZ (government CERT); 2. CERT.AZ (national CERT under the Ministry of Communication); 3. SCIENCE.CERT.AZ (under the National Academy of Science).	• The national CERT has been established (CERT.BY).	• The national CERT has been established. • Internal CERTs of public institutions are established. • CERT for the defense sector has been established.	• Center for Cyber Security - CERT-GOV-MD was created as a governmental CERT.	• The national CERT has been established (CERT-UA).
Cyber Contingency Plans					
• No National Cyber Contingency Plan at the national level.	• No National Cyber Contingency Plan at the national level, but Action Plan of Cybersecurity Strategy addresses this need. • Cyber contingency plans are obligatory for Energy, Information and Communications Technology, Water, Health, Transport, Food, Financial services, Public	• The National Cyber Contingency Plans are developed. • Cyber contingency plans are obligatory for Energy, Information and Communications Technology (ICT), Financial, Chemical, Environment sectors.	• No National Cyber Contingency Plan at the national level. • Cyber contingency plans are developed only by banking sector.	• No National Cyber Contingency Plan at the national level. • Cyber contingency plans are obligatory for public institutions, including critical ones.	• No National Cyber Contingency Plan at the national level. • Cyber contingency plans are obligatory for Energy, Information and Communications technology, Transport, Financial Services, Civil administration, Civil protection, Environment, Defense sectors.

	order and safety, Civil administration, Civil protection, Environment, Defense sectors.				

Source: Developed by EU4Digital Facility

Table 8: Summary of the state of play on the cooperation mechanism implemented in the Eastern Partner countries: identified challenges and key recommended activities

<table>
<tr><th colspan="6">COOPERATION MECHANISM</th></tr>
<tr><th colspan="3">GAPS/CHALLENGES</th><th colspan="3">KEY RECOMMENDED ACTIVITIES</th></tr>
<tr><td colspan="3">1. Not all Eastern Partner countries have established information-sharing and cross-sectoral information exchange mechanisms.
2. The partnership of public and private sectors requires further development as the existing memorandum of cooperation between public and private entities does not include often cybersecurity topics related, for example, to incident management and organisation of joint cyber incident management meetings/exercises or development of common standards and guidelines.
3. Not all countries have established cooperation with other Eastern Partner countries in the field of cybersecurity.</td><td colspan="3">1. Strengthening the cooperation in information sharing with other Eastern Partner countries and other EU countries in the field of cybersecurity.
2. Enhancement of the development of the public-private partnership especially with owners of the critical information infrastructure in the area of cybersecurity by building an understanding of common interest, increasing involvement and participation of the private sector in the development and implementation of cybersecurity policies and measures, development of the framework on managing and responding to major cybersecurity incidents and encouraging the establishment of CERTs by the private sector.
3. Establishing the information exchange mechanism at the national level.
4. Considering the possibility of the development of the specialised platform for information sharing to facilitate information and knowledge exchange with different stakeholders and other countries.
5. Developing the cross-sector information exchange mechanism.
6. Encourage cross-functional security and safety knowledge exchange.</td></tr>
<tr><th>Armenia</th><th>Azerbaijan</th><th>Belarus</th><th>Georgia</th><th>Moldova</th><th>Ukraine</th></tr>
<tr><td colspan="6">Information-sharing mechanism</td></tr>
<tr><td>Defined at the national level</td><td>Defined at the national level</td><td>Defined at the national level</td><td>Defined at the national level</td><td>Defined at the national level</td><td>Defined at the national level</td></tr>
<tr><td colspan="6">Mechanisms for cross-sector information exchange</td></tr>
<tr><td>Established</td><td>Established</td><td>Established</td><td>Established</td><td>Established</td><td>Established</td></tr>
<tr><td colspan="6">Public-private partnership in the area of cybersecurity</td></tr>
<tr><td>Established</td><td>Established</td><td>At the initial stage of development</td><td>Established</td><td>Established</td><td>Established</td></tr>
<tr><td colspan="6">Bilateral and Multilateral Cooperation</td></tr>
<tr><td>National entities are engaged in cooperation and information sharing with partners abroad.</td><td>• National entities are engaged in cooperation and information sharing with partners abroad.</td><td>• National entities are engaged in cooperation and information sharing with partners abroad.</td><td>• National entities are engaged in cooperation and information sharing with partners abroad.</td><td>• National entities are engaged in cooperation and information sharing with partners abroad.</td><td>National entities are engaged in cooperation and information sharing with partners abroad.</td></tr>
</table>

	• Information on cybersecurity incidents is shared with other Eastern Partner countries.	• There is no cooperation with other Eastern Partner countries in the area of cybersecurity.	• Information on cybersecurity incidents is shared with other Eastern Partner countries.	• Information on cybersecurity incidents is shared with other Eastern Partner countries.	

Source: Developed by EU4Digital Facility

Table 9: Summary of the state of play on the data protection mechanism implemented in the Eastern Partner countries: identified challenges and key recommended activities

<table>
<tr><th colspan="6">DATA PROTECTION</th></tr>
<tr><th colspan="3">GAPS/CHALLENGES</th><th colspan="3">KEY RECOMMENDED ACTIVITIES</th></tr>
<tr><td colspan="3">1. National laws on the protection of personal data are outdated.
2. Not all Eastern Partner countries require data breach notifications.
3. One of the Eastern Partner countries has not adopted a dedicated personal data protection law.</td><td colspan="3">1. Adoption of new legislation in line with the requirements of the General Data Protection Regulation (GDPR) or alignment of national regulation to the GDPR requirements.
2. Designation of clear responsibilities for national authorities in data protection.
3. Establishment of general requirements to report personal data protection breaches.</td></tr>
<tr><th>Armenia</th><th>Azerbaijan</th><th>Belarus</th><th>Georgia</th><th>Moldova</th><th>Ukraine</th></tr>
<tr><td colspan="6">National Data Protection Authority</td></tr>
<tr><td>Has been designated.</td><td>The responsibility for the National Data Protection Authority is distributed between five entities.</td><td>Has not been designated.</td><td>Has been designated.</td><td>Has been designated.</td><td>Has been designated.</td></tr>
<tr><td colspan="6">Data Protection Law</td></tr>
<tr><td>Established but needs to be updated.</td><td>Established but needs to be updated.</td><td>• Has not been adopted.
• Other national legislation currently regulates personal data protection:
○ Law on Information, Informatisation and Information Protection;
○ Law on Population Register.</td><td>Established but needs to be updated.</td><td>Established but needs to be updated.</td><td>Established but needs to be updated.</td></tr>
<tr><td colspan="6">Penalties</td></tr>
<tr><td>There are contractual penalties for non-compliance with the national data protection regulation.</td><td>There are contractual penalties for non-compliance with the national data protection regulation.</td><td>There are contractual penalties for non-compliance with the national data protection regulation.</td><td>There are contractual penalties for non-compliance with the national data protection regulation.</td><td>There are contractual penalties for non-compliance with the national data protection regulation.</td><td>There are no contractual penalties for non-compliance with the national data protection regulation.</td></tr>
</table>

Obligations					
Data breach notification is obligatory.	No obligation for data breach notification.	No obligation for data breach notification.	No obligation for data breach notification.	Data breach notification is obligatory.	No obligation for data breach notification.

Source: Developed by EU4Digital Facility

Table 10: Summary of the state of play on the cybersecurity culture in the Eastern Partner countries: identified challenges and key recommended activities

<table>
<tr><th colspan="6">CYBERSECURITY CULTURE</th></tr>
<tr><th colspan="3">GAPS/CHALLENGES</th><th colspan="3">KEY RECOMMENDED ACTIVITIES</th></tr>
<tr><td colspan="3">1. Lack of defined certification requirements for candidates applying for cybersecurity positions.
2. Cybersecurity exercises are not organised at the national level in all Eastern Partner countries.
3. Lack of educational programmes in the field of information security.
4. There is no national programme dedicated for Cyber Culture development.</td><td colspan="3">1. Conducting a national programme that will help society to understand what cybersecurity is.
2. Supporting cybersecurity researches.
3. Enhancement of cooperation among Eastern Partner region and European member states in cybersecurity exercises/conferences.
4. Involvement of national authorities in the organisation of cybersecurity exercises at the national level.
5. Establishing information security roles catalogue and the relevant mandatory/baseline educational background requirements for each information security role.
6. Development of requirements at the state level based on the need for the accreditation and certification of skilled personnel on cybersecurity in key working positions in the industrial sector (in critical infrastructure).
7. Strengthening the process of developing cybersecurity programmes for schools and universities.
8. Establishing a centralised budget for cybersecurity initiatives.
9. Development of qualification and certification requirements for people applying for a cybersecurity position (in critical infrastructure sector).</td></tr>
<tr><th>Armenia</th><th>Azerbaijan</th><th>Belarus</th><th>Georgia</th><th>Moldova</th><th>Ukraine</th></tr>
<tr><td colspan="6">Awareness-raising campaigns</td></tr>
<tr><td>A number of initiatives in this field have been taken, e.g. workshops, conferences, trainings.</td><td>A number of initiatives in this field have been taken, e.g. workshops, conferences, trainings.</td><td>A number of initiatives in this field have been taken, e.g. workshops, conferences, trainings.</td><td>A number of initiatives in this field have been taken, e.g. workshops, conferences, trainings.</td><td>A number of initiatives in this field have been taken, e.g. workshops, conferences, trainings.</td><td>A number of initiatives in this field have been taken, e.g. workshops, conferences, trainings.</td></tr>
<tr><td colspan="6">Cyber education</td></tr>
<tr><td>Providing a seminar on introduction to cryptography for children of school age.</td><td>There is the education programme at bachelor and master level cybero.az.</td><td>Cybersecurity is taught at the bachelor’s and master’s levels at state universities.</td><td>National authorities plan to help universities develop and establish cybersecurity programmes.</td><td>Master's degree programmes in cybersecurity have been opened at the universities.</td><td>Cybersecurity training programmes are launched in higher education institutions and in private training centres.</td></tr>
</table>

Cyber exercises					
Cybersecurity exercises are organised by private companies.	Cybersecurity exercises organised at the national level.	Cybersecurity exercises organised at the national level.	• Cybersecurity exercises organised at the national level. • Private companies do not organise exercises.	Cybersecurity exercises organised at the national level.	Cybersecurity exercises are organised by private companies.
Children protection initiatives					
No information.	• Programme Child Internet Security and Parental Control has been established. • Organisation of Youth Workshop on Cyber Security.	Child protection initiatives are being carried out.	• Development and implementation at the national level a cyber-hygiene programme for schoolchildren. • Printed and on-line materials with recommendations on child safety on the Internet prepared by State Inspector's Office.	Awareness campaigns during International Day of Internet Child Safety and during the Cyber Security Month.	Open lessons conducted on 'Introduction to Cyber Hygiene' in schools and lyceums of the Kyiv city.

Source: Developed by EU4Digital Facility

Table 11: Summary of the state of play on the cybercrime in the Eastern Partner countries: identified challenges and key recommended activities

<table>
<tr><th colspan="6">CYBERCRIME</th></tr>
<tr><th colspan="3">GAPS/CHALLENGES</th><th colspan="3">KEY RECOMMENDED ACTIVITIES</th></tr>
<tr><td colspan="3">1. Lack of contact point/platform for reporting cybercrimes.
2. Not all countries are engaged in cooperation against cybercrimes.</td><td colspan="3">1. Establishing a contact point or a platform for reporting cybercrime.
2. Developing the mechanism about the notification of cybercrimes.
3. Cybercrime regulations need to be amended to fully comply with the Budapest Convention. Complete implementation of Articles 2-6 offences against the confidentiality, integrity and availability of computer data and system is needed.
4. Providing specialised trainings for units dedicated to cybercrime.
5. Organisation or participation in international cybersecurity exercise dedicated to cybercrime.
6. Defining cybercrime term.</td></tr>
<tr><th>Armenia</th><th>Azerbaijan</th><th>Belarus</th><th>Georgia</th><th>Moldova</th><th>Ukraine</th></tr>
<tr><td colspan="6">Penalties</td></tr>
<tr><td>Penalties for committing cybercrime are defined.</td><td>Penalties for committing cybercrime are defined.</td><td>Penalties for committing cybercrime are defined.</td><td>Penalties for committing cybercrime are defined.</td><td>Penalties for committing a cybercrime are defined.</td><td>Penalties for committing a cybercrime are defined.</td></tr>
<tr><td colspan="6">Contact Point</td></tr>
<tr><td>No platform or contact point for reporting cybercrimes.</td><td>No clear mechanism of cybercrime reporting.</td><td>No information.</td><td>Contact point for reporting cybercrime is established.</td><td>Contact point for reporting cybercrime is established.</td><td>Contact point for reporting cybercrime is established.</td></tr>
<tr><td colspan="6">Cooperation against cybercrime</td></tr>
<tr><td>No information.</td><td>No information.</td><td>International cooperation for defense against cybercrime was established.</td><td>International cooperation for defense against cybercrime was established.</td><td>International cooperation for defense against cybercrime was established.</td><td>No information.</td></tr>
<tr><td colspan="6">Responsible Entities</td></tr>
<tr><td>Specialised cybercrime units are established at the national level.</td><td>There are designated entities responsible for cybercrime defense.</td><td>There are designated entities responsible for cybercrime defense.</td><td>Established specialised cybercrime unit.</td><td>Established specialised cybercrime units.</td><td>Established specialised cybercrime units.</td></tr>
</table>

Source: Developed by EU4Digital Facility

Table 12: Summary of the state of play on the funding mechanism implemented in the Eastern Partner countries: identified challenges and key recommended activities

FUNDING MECHANISM					
GAPS/CHALLENGES			**KEY RECOMMENDED ACTIVITIES**		
1. Mostly, there is no unified budget for cybersecurity programmes and cyber initiatives. 2. Funds for cybersecurity programmes and initiatives are described as insufficient. 3. Lack of strictly designated institutions responsible for cybersecurity initiatives.			1. Development of the national cybersecurity programmes and allocation of dedicated funds for cyber initiatives based on impact and risk assessments. 2. Establishing funding mechanisms for cybersecurity research. 3. Development of cooperation with research organisations and institutions dealing with cybersecurity.		
Armenia	**Azerbaijan**	**Belarus**	**Georgia**	**Moldova**	**Ukraine**
Institutions and programmes					
There are institutions and programmes supporting cybersecurity.	Programmes supporting cybersecurity are not developed.	There are institutions and programmes supporting cybersecurity.	There are institutions and programmes supporting cybersecurity.	There are institutions and programmes supporting cybersecurity.	Programmes supporting cybersecurity are not developed.
Funds					
Current funding of cybersecurity is considered insufficient.	There is no allocated budget for cybersecurity initiatives.	Some cybersecurity activities are supported by the state budget.	There is no unified budget for cybersecurity.	There is no unified budget for cybersecurity.	Current funding of cybersecurity is considered insufficient.
Research programmes					
Research funds have been allocated; however, they are considered insufficient.	Some researches in the field of cybersecurity are funded from the state budget funds.	The research funds are established at the national level.	The research funds are established at the national level.	There are no institutions carrying out research in the field of cybersecurity.	Research funds have not been allocated.

Source: Developed by EU4Digital Facility

6 Overview of the Eastern Partner programmes and projects

Enhancing cybersecurity and protecting critical information infrastructures require special initiatives/programmes together with dedicated and systematic funding in cybersecurity.

A broad range of projects and programmes covering areas such as data protection, cybersecurity legislation, cybersecurity culture, or reporting mechanisms are provided currently by the European Union. A consolidated list of initiatives under these high-level assistance activities can be found in the tables on the next pages. The main objective of them is the improvement of the legal and regulatory framework and setting up technical specifications for e-commerce, e-government, and open government data.

For example, under the EU4Digital initiative of the European Union the special programme EaPConnect was funded. Launched in July 2015 the project is expected to have a duration of five years. The European Commission's Directorate-General for Neighbourhood and Enlargements Negotiations (DG NEAR) is contributing 95% towards the cost of the EaPConnect project, providing funding for, for instance, establishment and operation a high-capacity broadband internet network for research and education, integration the national research and education networks in the region and facilitation of participation of local scientists, students, and academics in global research and education collaborations.

In addition, some projects, are also implemented by the World Bank (WB), to support the Eastern Partner countries in their development and early implementation of national broadband strategies, in line with relevant EU best practices and strategies. The programmes launched by WB help also the development of a common approach to improve the legal and regulatory frameworks of the Eastern Partner countries.

However, enhancing cybersecurity and protecting critical information infrastructures require also systematic programmes launched by particular Eastern Partner countries. Currently, there are some initiatives/projects in region or specific countries running, which address some gaps/challenges in the field of cybersecurity, but Eastern Partner countries rely heavily on external programmes to fund their cybersecurity activities. This is mainly due to the insufficient funding in cybersecurity, which has been indicated by all Eastern Partner countries as one of the main obstacles in achieving the required maturity in cybersecurity. Thus, systematic funding for cybersecurity-related activities should be established or increased at the national level by each Eastern Partner country to enable the launching a series of projects to improve their cybersecurity readiness and performance. These should address initiatives not only related to changes in the law, regulation and policies but also IT modernisation, generation of information-sharing protocols and mechanisms, or effective training of cybersecurity personnel, which are necessary to increase productivity and security and to help to reduce the likelihood that cyberattacks will be successful. In addition, a wide approach to security should be also implemented through the development of a security culture as well as a security model that encourages close cooperation between the government authorities and the private sector. But, to play catch-up with the private sector, national entities have to be directed to improve their governance, systems, and personnel to advance cyber-related security, must have a clear understanding of the cybersecurity vulnerabilities and what to expect from their cybersecurity programmes.

Table 13: Overview of Initiatives

Area/Domain	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Cybersecurity Legislation **Data Protection**	**ICT innovation:** 1. Public administration reform (budget support) – ongoing. 2. Support for the development following e-services – accomplished. 3. Roll-out of the national broadband strategies, in line with similar EU strategies – ongoing.	**ICT innovation:** 1. Enhancing the development of e-services (including e-commerce) in the Republic of Azerbaijan – accomplished. 2. Roll-out of the national broadband strategies, in line with similar EU strategies – ongoing.	**ICT innovation:** 1. Support to the creation of an Electronic System of Pre-Arrival Information Exchange between the Customs Authorities of Belarus and Ukraine (PRINEX). 2. Roll-out of the national broadband strategies, in line with similar EU strategies.	**ICT innovation:** 1. Roll-out of the national broadband strategies, in line with similar EU strategies – ongoing. 2. Support to the Georgian Competition Agency – ongoing.	**Telecom rules, eTrade, eHealth, Trust and Security, ICT Innovation, eSkills:** 1. Support to Public Administration Reform in Moldova. 2. Roll-out of the national broadband strategies, in line with similar EU strategies.	**ICT innovation:** 1. Special Measure III 2016 on Support to Rule of Law Reforms in Ukraine (PRAVO) – ongoing. 2. Special Measure 2017 II for Ukraine on Public Finance Management Reform.
Cooperation Mechanism **Cybersecurity Culture** **Reporting Mechanism**	-	**Trust and security:** 1. Cyber-related expert workshop and trainings – accomplished.	**eSkills:** 1. Strengthening the capacity for geospatial data management and interoperability of the National Cadastral Agency.	**Telecom rules:** 1. Supporting the Georgian National Communications Commission (GNCC) in the development of its electronic communications regulatory framework and operational capacities in line with EU regulatory framework – ongoing.	**Trust and security:** 1. Cyber-related expert workshop and trainings. 2. Support of the National Centre for Emergency Response Team (CERT) or the Centre for Special Telecommunication (CTS) under the Annual Action Programme 2017 (AAP 2017).	**Telecom rules:** 1. Supporting the enhancement of the Regulatory and Legal Competence of the National Commission for Communication Regulation and Informatisation of Ukraine (NCCR) regarding telecommunication sector regulation – accomplished.
Cybersecurity Legislation						**Trust and security:** 1. Actions through the TAIEX instrument (study visits and expert mission) – accomplished. 2. FMC to assess the UA cybersecurity legislation and its conformity with

Area/Domain	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
						adopting the best practices from the NIS Directive etc. – ongoing. 3. U- LEAD with Europe – ongoing.
Cybersecurity Legislation **Cybercrime** **Cooperation Mechanism** **Cybersecurity Measures**	-	-	**01/2012-01/2014 –** Trainings on e-Governance and ICT solutions for representatives of Belarusian civil society – improving the knowledge of Belarusian civil servants of e-governance, the use of ICT and cyber defense.	**11/2012-08/2014 –** Promote the strengthening ***e***-Governance in Georgia – strengthening the capacities of Data Exchange Agency to consequently implement the best and the most suitable e-policies. **09/2015-06/2017 –** Strengthening e-Governance in Georgia II **-** strengthening the institutional set up of the Data Exchange Agency and enhancing the necessary skills and knowledge of the Agency's staff.	**03/2015-10/2015 –** Development of a National Cyber Security Index – developing a national cybersecurity assessment methodology and implementing it.	**4-8/11/2019 –** CyberEast: Pilot Judicial Training in Ukraine – training for 30 judges from across Ukraine through introductory cybercrime, electronic evidence and online crime proceeds course.
Cooperation Mechanism **Cybersecurity Culture** **Data Protection**	**08/2012-12/2014 –** Transactional e-Governance Development in Armenia – strengthening the public sector reform in Armenia, making government operations more efficient and	-	-	**11/2012-11/2014 –** EU-Georgia e-Governance Facility – implementation of the Registry of Registers and developing the Computer Emergency Response Team (CERT).	**03/2018-02/2020 –** Trusted and secure digital society for Moldova –development of Moldova's institutional capacity in the digital security area (e.g. awareness-raising on the EU's new data protection regulation,	**12/2014-06/2014 –** NATO Trust Fund - Cyber Defense – developing CSIRT-type technical capabilities including laboratories to investigate cybersecurity incidents;

Area/Domain	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
	transparent; developing e-governance initiatives.				development of cybersecurity framework)**.**	cyber defense exercises and trainings.
Cooperation Mechanism **Cybersecurity Culture**	-	-	-	-	**09/2014-02/2017 –** Cyber Security Capacity in Moldova – building the country's capacity for efficiently managing cyber incidents and cooperating internally and internationally; holding a cybersecurity exercise and seminar for IT specialists.	-
Cybersecurity Legislation	-	-	-	-	**10/2012-12/2013 –** Digital Information Security for Better Governance and Public Services – capacity-building for digital information security for Moldovan Government Institutions	-

Source: Developed by EU4Digital Facility

Table 14: The programmes or projects common for all Eastern Partner countries and the domains which they address

Area/Domain	Eastern Partner countries
Cybercrime	**Cybercrime@EAP projects:** **2011-2014 –** CyberCrime@EaP I – strengthening the capacities of Eastern Partner countries to cooperate effectively against cybercrime. **2015-2017 –** CyberCrime@EAP II – to optimise the regional and international cooperation on cybercrime and electronic evidence (the improvement of mutual legal assistance for the international cooperation on cybercrime and electronic evidence; to strengthen the role of 24/7 contact points). **2015-2017 –** CyberCrime@EAP III – improving the cooperation between criminal justice authorities and service providers in specific criminal investigations and with the necessary rule of law safeguards. **2018-2019 –** CyberCrime@EAP 18 – International and public/private cooperation. **2019-2022 –** CyberEast: Action on Cybercrime for Cyber Resilience in the Eastern Partner Region – adopting legislative and policy frameworks compliant to the Budapest Convention on Cybercrime and related instruments, reinforcing the capacities of judicial and law enforcement authorities. **2019-2022 –** EU4Digital: Improving Cyber Resilience in the Eastern Partner Countries – to increase and enhance the cyber-resilience and criminal justice capacities of the Eastern Partner countries to better address the challenges of cyber threats and improve their overall security; the aim of the second stream of the programme is the full implementation of an effective framework to combat cybercrime.
Cooperation Mechanism **Cybersecurity Culture**	**2015-2019 –** EaP Connect – establishing and operating a high-capacity broadband internet network for research and education (R&E) across EaP countries. **2019-2022 –** EU4Digital: Improving Cyber Resilience in the Eastern Partner Countries – to increase and enhance the cyber-resilience and criminal justice capacities of the Eastern Partner countries to better address the challenges of cyber threats and improve their overall security; the aim of the second stream of the programme is development of technical and cooperation mechanisms that increase cybersecurity and preparedness against cyber-attacks.
Cybersecurity Legislation	**2015-2016 –** Participatory Democracy, Open Governance & Efficient eGovernment Services project" (PADOS) – the overall objective was to enhance the transparency and openness of decision-making and governance in Eastern Partner countries**.**

Source: Developed by EU4Digital Facility

Annex 1. Detailed cybersecurity maturity assessment methodology description

Table 15: Domain of Cybersecurity Legislation

Initial	Managed	Defined
1. There are some policies related to cybersecurity, but they need to be updated. 2. The NC Strategy is not developed yet. 3. There are no dedicated entities responsible for the initiating and developing cybersecurity policy and regulation.	1. Different policies related to cybersecurity, but they do not cover all aspects. 2. Some additional regulations should be implemented as well in order to improve the cybersecurity.	1. Strong legislation is developed and implemented in the area of cybersecurity, including national cybersecurity strategy and action plan. 2. Regulatory measures are applied in different sectors, the roles and responsibilities of existing public agencies mandated to deal with cybersecurity policies. 3. Regulations and operations are established. 4. NC Strategy is based on the risk management regime.

Source: Developed by EU4Digital Facility

Table 16: Domain of Cybersecurity Measures

Initial	Managed	Defined
1. Baseline cybersecurity measures are implemented, but they do not cover all aspects, or they are an internal policy in organisations. 2. There is no distinction into technical and organisational measures. 3. The obligation of using measures is voluntary. 4. There is no dedicated authority responsible for verifying the level of implementation of security measures.	1. Requirements for cybersecurity measures are based on existing security standards (i.e. the ISO 27,000 Series of Standards) or frameworks and good practices, and should be defined at the national level to be understood in the same way. 2. Cybersecurity measures are obligatory only for limited stakeholders, but the information about baseline cybersecurity measures should be shared among different industry sectors. 3. Technical and organisational measures are described and obligatory among selected institutions and organisations 4. There is no obligation to conduct audits on the implementation of security measures.	1. Implementation of cybersecurity measures is mandatory in both private and public sectors without any exceptions, but organisation can use their own measures as long as they fulfil the national requirements. 2. National authority is responsible for monitoring the implementation of measures and for conducting audits on the implementation of these measures in public and private entities, audits may also be delegated to accredited organisations in accordance with the implemented rules. 4. Special guidelines for the implementation of the cybersecurity measures should be provided to the organisations. 5. Audits are obligatory and reports after audits should serve as a base for updating the requirements of baseline cybersecurity measures.

Source: Developed by EU4Digital Facility

Table 17: Domain of essential services and Critical Information Infrastructure

Initial	Managed	Defined
1. There is a legislation for CI operators, but it is not relevant for CII operators. 2. Obligation for CII operators can be found in another legislation (i.e., requirements for electronic communication infrastructure). 2. There is no specific distinction between the CI and CII operators. 3. Relevant private and public stakeholders have been involved in the process of identification of CII.	1. Legal steps have been taken to sanction the status of CII operators. 2. Entities responsible for selection of CII have been designated. 3. CII is defined and identified at the national level. 4. A comprehensive methodology for identifying CII operators is conducted. 5. Essential services have been determined on the basis of CII assets.	1. Approach to cooperation with CII operators is established by law. 2. Roles and responsibilities of operators and public institutions are defined. 3. CII operators are obliged to conduct cyber risk assessment. 4. Special certification requirements for people applying for position in CII object are established. 5. Regulatory measures are applied. 6. Security polices for each of critical sectors have been implemented.

Source: Developed by EU4Digital Facility

Table 18: Domain of National Risk Assessment

Initial	Managed	Defined
1. There are some policies and standards related to risk assessment, but they need to be updated. 2. National Risk Assessment is not developed yet. 3. There are no dedicated entities responsible for developing national risk assessment methodology. 4. There is no obligation to conduct risk assessment by private and public institutions.	1. National risk assessment addresses cyber threats, but it does not cover all aspects. 2. Obligation to conduct risk assessment is limited to selected institutions. 3. Entities responsible for developing and implementing risk assessment are designated.	1. Approach to risk identification is sanctioned by the law and available for use by organisations and institutions. 2. Cyber risk assessment has been established at the national level and is mandatory for both private and public entities, but it is possible to use own cyber risk assessment if it fulfils the state requirements. 3. Establishing a sectorial risk assessment allows considering more sector-specific risks to critical infrastructure and service providers.

Source: Developed by EU4Digital Facility

Table 19: Domain of reporting mechanism and incident management

Initial	Managed	Defined
1. There are some policies pointing the basic requirements for reporting incidents, but there is no formal mechanism established at the national level. 2. There are no dedicated entities responsible for developing reporting mechanism. 3. There is no obligation to report cyber security incidents. 4. There is no formal scheme of reporting established. 5. There are no requirements for developing a Cyber Contingency Plans.	1. Reporting mechanism is established at the national level and the scheme of incident management is also provided. 2. A single contact point or platform for reporting the incidents is established, but it does not cover all aspects, there is a template for reporting incidents. 3. Classification of types of incidents to be reported is identified and provided and the reporting requirements are outlined. 4. Reporting cyber incidents is limited, not all entities are obliged to report.	1. National CERT and serves as a national contact point for incident reporting are established. Oher governmental and sectoral CERT's are established and collaborate with each other. 2. Creation of SOC teams among the public and private entities. 3. Cooperation with partners abroad has been established and the exchange of information on cyber incidents is developing. 4. Building trust with the participants and the private stakeholders is one of the main goals to achieve for the proper functioning of reporting mechanism. This can be accomplished by developing good practice and training programmes. 5. The requirement to report incidents is mandatory for all. 6. Cyber Contingency Plans (CCP) are developed, main entities responsible for their implementation are dedicated, a policy for verifying the implementation of CCP is established.

Source: Developed by EU4Digital Facility

Table 20: Domain of cooperation mechanism

Initial	Managed	Defined
1. There are some policies related to cooperation mechanism, but no formal mechanism for information sharing and cross sector information exchange is implemented. 2. There are no dedicated entities responsible for developing reporting mechanism and cross sector information exchange. 3. No international cooperation on cyber security has been established. 4. Public-private partnership is at the early stage.	1. Formal mechanism for information sharing and cross sector information exchange is implemented and the responsibilities for national authorities are established. 2. Participation in mechanism for information sharing is voluntary or limited to some entities. 3. Public-private partnership is developed, but the number of participants is limited. 4. Series of cooperation agreements with other countries was established.	1. Strong legislation for cooperation mechanism refers to both national and international partners. 2. Public-private partnerships cover a range of issues and engage number of public and private stakeholders. 3. International cooperation mechanism covers a number of signed or ratified international treaties or conventions, national public agencies involved in international cooperation schemes and cyber security exercise that have taken place. 4. The scope of information exchange between national cyber security authorities is established.

Source: Developed by EU4Digital Facility

Table 21: Domain of data protection

Initial	Managed	Defined
1. There are some policies related to data protection, but they need to be updated. 2. The law on Data Protection is not developed yet. 3. There are no dedicated entities responsible for the initiating and developing regulation of data protection. 4. Reporting on data protection breaches is not mandatory and there are no penalties for violations.	1. Different policies related to data protection, but they do not cover all aspects. 2. Some additional regulations should be implemented as well in order to improve the security of data protection. 3. Reporting on data protection breaches is limited to chosen entities as well as penalties for violations.	1. Strong legislation is developed and implemented in the area of data protection, including requirements contained in General Data Protection Regulation. 2. National authority responsible for data protection is established; the degree of involvement of the national data protection authority in cybersecurity-related issue areas should also be described. 3. Reporting on data protection breaches is mandatory and there are concrete penalties for violations. 4. Organisations and institutions processing the data are obliged to implement technical and operational measures to protect personal data.

Source: Developed by EU4Digital Facility

Table 22: Domain of awareness-raising activities

Initial	Managed	Defined
1. There is no national regulation determining how to implement awareness-raising activities among society. 2. There are no dedicated entities responsible for the initiating and developing regulation in this field. 3. Some of the initiatives may be set up ad hoc in response to specific cyberthreats.	1. Different policies related to awareness-raising activities have been taken, but still there is no clear mechanism for them. 2. National authority responsible for building cybersecurity culture has been established, however no clear action plan has been announced. 3. The state participates in various social actions in this field, but does not organise exercises itself and doesn't participate in international exercises. 5. Budget for awareness-raising campaign has not been established, institutions are organising funds for such events within their own budgets. 4. Cooperation in international information security initiatives has been undertaken but is not strictly followed.	1. Clear and strong policy for cybersecurity culture has been established, a number of initiatives in this area (i.e. workshops, conferences, trainings, exercises) are set up and planned in advance. 2. Special budget for awareness-raising campaigns and training programmes has been established at the national level. 3. Cybersecurity awareness-raising campaigns are developed for society, both at school and university level and among all adult citizens. 4. Awareness-raising activities involve both public and private entities, a mechanism for the exchange of information on cyberthreats is established and promoted. 5. Trainings and awareness-raising campaigns are created in order to deal with identified risks. 6. Special cybersecurity programmes have been developed for students. 7. The state joins and supports international information security initiatives and campaigns.

Source: Developed by EU4Digital Facility

Table 23: Domain of cybercrime defence

Initial	Managed	Defined
1. There are some policies related to cybercrime legislation, but they need to be updated . 2. The law on cybercrime is not developed yet. 3. No action has been taken to set up a cybercrime unit, as a result, there are no accepted rules for classifying and identifying incidents commonly regarded as cybercrime.	1. There are national regulations for cybercrime, but they do not cover all issues and are scattered across different laws. 2. Action should be taken to create a coherent cybercrime law, taking into account international norms and standards. 3. Some initiatives in the field of cybercrime defense have been taken, however there is no clear mechanism for reporting cybercrime and there is no provision for penalties for such an offence. 4. A cybercrime unit has been set up, but its responsibilities have not been indicated yet.	1. A coherent policy on cybercrime has been put in place, created legislation takes account of international regulations. 2. International conventions have been ratified and adapted to national legislation. 3. The law regulates the definition of cybercrime, determines the penalties for committing it and provides for a reporting mechanism. 4. Specialized national cybercrime units have been established, one in charge of developing and verifying compliance/ compatibility with cybercrime legislation and the other as a judicial authority. 5. A framework for cooperation with public and private stakeholders has been established to identify and tackle with cybercrimes. There are also international initiatives for cybercrime defense.

Source: Developed by EU4Digital Facility

Table 24: Domain of funding mechanism

Initial	Managed	Defined
1. There are some policies related to funding mechanism, but they are not detailed. 2. There are no dedicated entities responsible for implementation of regulation related to the funding mechanism.	1. There are policies that define the budget for research and development but cover a wide range of issues. They are not established only for cybersecurity projects. 2. Clear rules on budget spending for R&D in cybersecurity were not adopted. 3. There is lack of market intelligence in the creation of contracts for specific research in the cyber field.	1. Research funds for cybersecurity activities have been launched. 2. The financial mechanism is policy-driven and publicly available. 3. A special national unit has been established, its main task is to coordinate the allocation of funds and to verify the fulfilment of tasks in this area. 4. The public entity in charge of allocating funds identifies the market for those reliant on cyber services and creates appropriate R&D contracts. 5. Joint international initiatives on cyber security research are being taken up.

Source: Developed by EU4Digital Facility