EN

THIS ACTION IS FUNDED BY THE EUROPEAN UNION

ANNEX II

to the Commission Implementing Decision on the financing of the multiannual action plan in favour of the NDICI Neighbourhood East Region for 2023-2024

Action Document for Improving Cyber Resilience in the Eastern Partnership countries

MULTIANNUAL ACTION PLAN

This document constitutes the multiannual work programme in the sense of Article 110(2) of the Financial Regulation, and action plan/measure in the sense of Article 23(2) of NDICI-Global Europe Regulation.

1. SYNOPSIS

1.1. Action Summary Table

1. Title OPSYS Basic Act	**Improving Cyber Resilience in the Eastern Partnership countries** Multiannual action plan in favour of the NDICI Neighbourhood East Region for 2023-2025 OPSYS business reference ACT-61842 ABAC Commitment level 1 number: JAD.1164549 and JAD.1164550 Financed under the Neighbourhood, Development and International Cooperation Instrument (NDICI-Global Europe).
2. Economic and Investment Plan (EIP)	Yes Digital
3. EIP Flagship	No
4. Team Europe Initiative	No
5. Beneficiar(y)/(ies) of the action	The action shall be carried out for the benefit of the Eastern Partnership countries (Armenia, Azerbaijan, Belarus[1], Georgia, Republic of Moldova[2], Ukraine).
6. Programming document	Regional Multiannual Indicative Programme Document (MIP) 2021-2027[3]
7. Link with relevant MIP(s) objectives/expected results	**Specific Objective 1** (of priority area 2): Support judicial reforms, the rule of law, prevention and fight against corruption, and economic, organised and serious crime, including trafficking in human beings, drug trafficking, firearms trafficking and cybercrime;

[1] In line with the Council Conclusions of 12 October 2020 and in light of Belarus's involvement in the Russian military aggression against Ukraine, recognised in the European Council Conclusions of February 2022, the EU has stopped engaging with representatives of Belarus public bodies and state-owned enterprises. Should there be a change of the context this may be reconsidered. In the meantime, the EU continues to engage with and, where possible, has stepped up support to non-state, local and regional actors, including within the framework of this regional programme.

[2] Hereinafter referred to as Moldova

[3] C(2021)9370 adopted on 15/12/2021

	Expected result: Improved alignment with EU legal, institutional and policy frameworks on cybercrime, implementation of relevant international cooperation mechanisms to fight cybercrime and access digital evidence **Specific objective 3** (of priority area 4): Align institutional, policy and legislative cybersecurity and cyber-threat frameworks. **Expected results**: • Institutional, policy and legislative cybersecurity frameworks in all Eastern Partnership countries made compatible with EU legislation and guidelines, notably the EU Directive on security of network and information systems and relevant European Union Agency for Cybersecurity (ENISA) guidelines; • Introduction of ENISA's cyber threat landscape methodology in all Eastern Partnership countries.
PRIORITY AREAS AND SECTOR INFORMATION	
8. Priority Area(s), sectors	Priority area 4: Resilient digital transformation Priority area 2: Strengthening Institutions and Good Governance. 15210 Security system management and reform (40%) 22040 Information and communication Technology (40%) 15130 Legal and judicial development (20%)
9. Sustainable Development Goals (SDGs)	Main SDG Goal 16: Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels. In particular, the action will cover: • 16.4 Significantly reduce illicit financial and arms flows, strengthen the recover and return of stolen assets and combat all forms of organized crime; • 16.A Strengthen relevant national institutions, including through international cooperation, for building capacity at all levels, in particular in developing countries, to prevent violence and combat terrorism and crime; It will also contribute to: • 16.3 Promote the rule of law at the national and international levels and ensure equal access to justice for all; • 16.6 Develop effective, accountable and transparent institutions at all levels; • 16.7 Ensure responsive, inclusive, participatory and representative decision-making at all levels; • 16.10 Ensure public access to information and protect fundamental freedoms, in accordance with national legislation and international agreements; • 16.B Promote and enforce non-discriminatory laws and policies for sustainable development
10. DAC code(s)	15210 Security system management and reform (40%) 22040 Information and communication Technology (40%) 15130 Legal and judicial development (20%)
11. Main Delivery Channel	12000 – Recipient government

12. Targets	☐ Migration ☐ Climate ☐ Social inclusion and Human Development ☐ Gender ☐ Biodiversity ☒ Human Rights, Democracy and Governance			
13. Markers (from DAC form)	**General policy objective**	**Not targeted**	**Significant objective**	**Principal objective**
	Participation development/good governance	☐	☐	☒
	Aid to environment	☒	☐	☐
	Gender equality and women's and girl's empowerment	☒	☐	☐
	Reproductive, maternal, new-born and child health	☒	☐	☐
	Disaster Risk Reduction	☒	☐	☐
	Inclusion of persons with Disabilities	☒	☐	☐
	Nutrition	☒	☐	☐
	RIO Convention markers	**Not targeted**	**Significant objective**	**Principal objective**
	Biological diversity	☒	☐	☐
	Combat desertification	☒	☐	☐
	Climate change mitigation	☒	☐	☐
	Climate change adaptation	☒	☐	☐
14. Internal markers and Tags	**Policy objectives**	**Not targeted**	**Significant objective**	**Principal objective**
	EIP	☐	☒	☐
	EIP Flagship	YES ☐		NO ☒
	Tags	YES		NO
	transport	☐		☒
	energy	☐		☒
	environment, climate resilience	☐		☒
	digital	☒		☐
	economic development (incl. private sector, trade and macroeconomic support)	☒		☐
	human development (incl. human capital and youth)	☒		☐
	health resilience	☐		☒
	migration and mobility	☐		☒
	other	☐		☒
	Digitalisation	☐	☐	☒
	Tags	YES		NO
	digital connectivity	☒		☐

	digital governance	☒		☐
	digital entrepreneurship	☒		☐
	digital skills/literacy	☒		☐
	digital services	☒		☐
	Connectivity	☐	☒	☐
	Tags	YES		NO
	digital connectivity	☒		☐
	energy	☐		☒
	transport	☐		☒
	health	☐		☒
	education and research	☐		☒
	Migration	☒	☐	☐
	Reduction of Inequalities	☒	☐	☐
	COVID-19	☒	☐	☐
BUDGET INFORMATION				
14. Amounts concerned	Budget line: BGUE-B2023 14.020111 - C 1 NEAR (Eastern Neighbourhood) BGUE-B2024-14.020111 - C 1 NEAR (Eastern Neighbourhood) Total estimated cost: EUR 7 000 000 Total amount of EU budget contribution EUR 7 000 000 The contribution is for an amount of EUR 2 000 000 from the general budget of the European Union for 2023 and for an amount of EUR 5 000 000 from the general budget of the European Union for 2024, subject to the availability of appropriations for the respective financial years following the adoption of the relevant annual budget, or as provided for in the system of provisional twelfths.			
MANAGEMENT AND IMPLEMENTATION				
15. Implementation modalities (management mode and delivery methods)	Indirect management with pillar assessed entities to be selected in accordance with the criteria set out in section 4.3.1			

1.2. Summary of the Action

In light of the increased cyber-attacks affecting the EU Member States and the countries in the EU's Eastern Neighbourhood, a need to continue to address the challenges related to cybersecurity and cybercrime has been identified. Russia's military aggression against Ukraine was preceded and is being accompanied by a strategy of hostile cyber operations. In 2022, targeting of users in Ukraine increased by 250% compared to 2020. Targeting of users in NATO countries increased over 300% in the same period.[4]

The recent COVID-19 pandemic and ongoing security threats and armed conflicts in the region, in particular the repeated aggression of Russia against Ukraine, contribute further to the deterioration of the security and crime situation. In the weeks immediately before Russia launched its war of aggression against Ukraine on

[4] Google, "Fog of War How the Ukraine Conflict Transformed the Cyber Threat Landscape", February 2023, google_fog_of_war_research_report.pdf.

February 24, 2022, Russia intensified its attacks in cyberspace, with distributed denial-of-service (DDoS) attacks, disruptive wiper malware, etc. Cyber-attacks have been constantly at high level, reflected in increasing cyber-attacks targeting Ukraine and having an impact on other geographical regions, including EU Member States. Combined with disinformation attacks they continue to undermine the trust in the governments and the overall stability.

The EU is currently carrying out action in addressing cybersecurity and cybercrime related challenges in Eastern Partnership region through EU4Digital: Improving cyber resilience in the EaP countries. The project has delivered well in building capacities of the key interlocutors, approximating partner countries legislation and standards with the EU, and created linkages between European key cybersecurity players. Partner countries have expressed strong appreciation for project, and continue requesting capacity building support from the European Union. Members States encourage Commission to enhance the activities to increase cybersecurity in the region. Partners' strengthened capacities to increase cyber resilience is one of the ten targets of Eastern Partnership for 2025.

The follow-up to the ongoing of cybersecurity and cybercrime programme will contribute to improving the cyber resilience and criminal justice response of EaP Partner countries. As the previous programme, the action will focus on two key building blocks – a cybersecurity and a cybercrime component.

First, the development of technical and cooperation mechanisms that increase cybersecurity and preparedness against cyber-attacks, such as strengthening the institutional governance and legal framework in line with the EU acquis, developing the critical information infrastructure structure and increasing the incident management capacities, will be strengthened. This component also foresees a small allocation for the procurement of equipment and licences, if in line with overall capacity building work. The proposed actions will be implemented, when appropriate, at regional level, however different level of aspirations to be associated with the EU, in particular the candidate country status granted to Ukraine and Moldova, and the European perspective of Georgia need to be taken into account when planning the actions. Such a differentiated approach is also in line with the revised European Neighbourhood Policy.

Secondly, full implementation of an effective framework to combat cybercrime, including substantive and procedural criminal legislation, law enforcement and judicial authorities' capacity to investigate, prosecute and adjudicate cases of cybercrime, measures to enable international cooperation and cooperation between public authorities and private entities, will be supported. The Budapest Convention continues to provide the benchmark for an effective framework.

Moreover, the Russian aggression furthermore underlines the need for capacities to secure electronic evidence for use in criminal proceedings not only in relation to cybercrime or cyber-attacks but in relation to any offence, including war crimes committed by Russia in Ukraine. The action would support the implementation of the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (legislation, procedures, guides, templates and practical training exercises). A combination of regional and country-specific measures within a common international framework will be pursued.

1.3. **Beneficiar(y)/(ies) of the action**

Beneficiary countries of the action are Armenia, Azerbaijan, Georgia, Moldova and Ukraine, the countries of the Eastern Partnership region. In the area of cybersecurity, the Representatives from national Governments and institutions of these EaP partner countries are among the key institutional beneficiaries of this Action. Beneficiaries also include private sector and non-governmental organisations. The final beneficiaries of the action are the populations of these EaP partner countries who will benefit from the fact that their countries are more resistant to cyberattacks and cybercrime. Please see further details on beneficiaries in Section 2.2.

2. RATIONALE

2.1. Context

Cybersecurity incidents – theft of commercial trade secrets, business information or disruption generate a significant cost for the global economy and undermine trust in the digital society. According to various reports and studies, the global cost of cyber attacks has been estimated to be in the hundreds of billions of dollars annually. For example, a report by Cybersecurity Ventures estimated that they could cost the global economy EUR 6 trillion annually by 2021, including both direct and indirect costs. With the evolution of cybercrime from a relatively resource-intensive activity reserved for a group of tech-savvy criminals to an affordable crime-as-a-service-based business model that supports the entire cybercrime value chain and drives the digital underground economy, the range of threat vectors has multiplied significantly. At the same time, cyber tools are used to pursue particular political, economic, financial and strategic interests, including through disinformation campaigns or hybrid operations targeting critical financial, energy, or transportation infrastructure.

As cyber threats began to have a stronger societal impact, the understanding of resilience has shifted from a purely technical account (i.e. the capacity of networks to recover) to one that concerns also strategic and operational dimensions across the whole range of policy areas, including home affairs, security and defence, foreign policy, industrial and economic policy, trade, research and technology development, and education. Due to the multi-dimensional nature of threats in cyberspace, they require flexible and adaptable governance models to counter them, accompanied by comprehensive and cross-cutting policies that engage the many levels and with different actors, institutions and individuals involved. Consequently, the focus on risks and vulnerabilities in the context of building cyber resilient states and societies addresses security not merely as an objective in itself but rather as means towards achieving broader developmental objectives.

Information security is paramount to the protection of fundamental rights of citizens as enshrined in the Charter of Fundamental Rights of the EU, as well as the fight against cybercrime and the protection of democracy and the rule of law. Insecure systems may lead to data breaches or identity fraud that could cause real harm and distress to individuals, including a risk to their lives, their privacy, their dignity, or their property.

Cybersecurity has become an important issue of international security all over the world. International relations in cyberspace often mirror the challenges of a multi-polar world reflected also in other domains. The EU recognised in its 2016 Global Strategy that its internal security depends on external security, including security of its geographical neighbour countries. Cyberspace as a global and, to large extent, borderless domain exacerbates risks and vulnerabilities related to interdependencies between states, economies and stakeholders (both public and private). Thus, in its Global Strategy, the EU presented its commitment to increase its focus on cybersecurity and amongst others to invest in cyber capacity building. The Global Strategy also pledged that the EU would strengthen the resilience of states and societies, in particular in the EU's surrounding regions in the East and the South.

The revised EU's Cybersecurity Strategy adopted in 2020 provides for EU's coherent and holistic international cyber policy. Working with its partners at bilateral, regional and international level, the EU promotes a global, open, stable and secure cyberspace guided by EU's core values and grounded in the rule of law. Within the strategy, the EU commits to support third countries in increasing their cyber resilience and ability to tackle cybercrime.

Russia has used cyber-attacks as part of its hybrid war against Ukraine with broader regional impact since the annexation of Crimea and launching the conflict in Donbas in 2014. They include the use of proxies, networks, organised crime and the creation of uncertainties regarding responsibility and blurring the border between state actors, and non-state actors. The most notable attacks include the attacks against elections IT infrastructure in 2014 aimed to present elections as illegitimate and rigged and frame Ukraine as a failed state run and the attacks undermining electricity networks in Western Ukraine in 2015. The impact of some attacks like Not-Petya[5] have caused substantial economic damage globally demonstrating that cyber-attacks do not recognise borders.

Internally in the EU, a robust cybersecurity policy framework has been set up, which is relevant also to the EU Eastern neighbours, particularly to those who would like to become the Member States of the EU. The Network and Information Security (NIS) Directive was the first piece of EU-wide legislation on cybersecurity, with the specific aim to achieve a high common level of cybersecurity across the Member States. To respond to the growing threats posed with digitalisation and the surge in cyber-attacks, the NIS Directive has been revised (NIS 2) by widening the scope, strengthening the security requirements, addressing the security of supply chains, streamlining reporting obligations, and introducing more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU. The NIS2 Directive (Directive (EU) 2022/2555)[6] entered into force in mid-January 2023 and Member States have 21 months at their disposal since that date to transpose the new directive. The expansion of the scope covered by NIS2 to more entities and sectors that have to take cybersecurity risk management measures and are subject to reporting obligations would increase the level of cybersecurity in Europe in the longer term and is therefore highly relevant to Eastern Partnership countries.

As regards the cybersecurity of 5G networks, the EU Toolbox for 5G Cybersecurity recommends a set of measures to mitigate the risks associated with 5G networks, including putting in place restrictions for suppliers considered as high-risk[7].

Eastern Partnership countries have significantly stepped up their capabilities to withstand the attacks. The efforts have been three-fold. First, the improvement of the cybersecurity expertise through daily work defending systems from attacks. Secondly, adoption of the cybersecurity strategies and aligning legislation with the EU legislation, which has contributed in determining the roles and responsibilities across the governments. Thirdly, enhancing cyber resilience hand-in-hand with embracing the possibilities of Internet and digital transformation.

Cybercrime and other cyber-enabled offences involving electronic evidence remain major challenges for societies of the EaP region. Likewise, attacks against and by means of computers emanating from those countries are of concern to other geographical areas including the EU Member States. These crimes consist, inter alia, of the theft of personal data, fraud and other types of financial crime, distributed denial of service attacks or website defacements against media, civil society, individuals or public institutions, as well as attacks against critical infrastructure and others. In this regard, cooperation at all levels is essential.

Countries of the EaP have committed to implement the Budapest Convention on Cybercrime as a framework for domestic measures and for international cooperation on cybercrime and access to electronic evidence. All countries – with the exception of Belarus – are Parties to the Budapest Convention and are thus members of the Cybercrime Convention Committee (T-CY). It is therefore an international obligation for them to

[5] On 27 June 2017, a major global cyberattack called Not-Petya took place. Infections were reported in France, Germany, Italy, Poland, the United Kingdom, and the United States, but that the majority of infections targeted Ukraine (around 80% of infections). Experts believe this was a politically-motivated attack against Ukraine, since it occurred on the eve of the Ukrainian holiday Constitution Day.

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555 .

[7] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, 29 January 2020, https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

implement and comply with it. EaP countries have benefited from several regional projects on cybercrime and electronic evidence financed by the EU and implemented by the Council of Europe since 2011. Ukraine and Moldova have also already signed the Second Additional Protocol on access to e-evidence.

2.2. Problem Analysis

Short problem analysis

This action will contribute to improving the cyber-resilience and cybersecurity of EaP countries and will focus on two key building blocks: cybersecurity and cybercrime.

In terms of cybersecurity, the main challenges of the countries across the Eastern Partnership region are following:

- Gaps in institutional and legal framework- some partner countries do not have national Computer Emergency Response Teams (CERTs), which is a notable gap considering the private ownership of key critical infrastructures;
- Inter-institutional competition and lack of coordination structure that would ensure whole-of-the government approach to cybersecurity;
- Outdated cybersecurity infrastructure/equipment and reliance on post-Soviet software licenses, as well as reliance on potential high-risk suppliers as regards 5G infrastructure and networks[8];
- Capacity building – most cybersecurity experts are self-trained. There is a lack of sustainable solution of providing high-level training to cybersecurity experts in Eastern Partnership countries. Very few cyber experts are certified;
- Awareness - there has been some work on cyber hygiene, but without a political support and not targeted, therefore with minimal impact;
- Information sharing about cyber incidents with private sector – the mechanisms are only being created.

The action will help the development of technical and cooperation mechanisms that increase cybersecurity and preparedness to cyber-attacks, such as building the capacities of functional CERTs and other key players of the cybersecurity ecosystem, organising cyber exercises and improving the general cyber hygiene.

In the cybercrime, despite progress made, the following challenges continue to persist:

- Lack of Criminal procedural law powers to secure electronic evidence and obtain data from private sector service providers. Specific provisions in criminal procedural law enabling the powers for law enforcement and judicial authorities to secure electronic evidence in accordance with rule of law and fundamental rights conditions and safeguards will enhance trust and will contribute to improve public/private and international cooperation;
- Need to build confidence and trust to allow for and enable cooperation between criminal justice authorities and the private sector, as well as between public institutions and between countries;
- Need to improve the operational capacities of specialised cybercrime units;
- Addressing and reducing conflicts of competence; and strengthening interagency, international and public/partnership cooperation. This remains an overriding issue;
- Sharing of relevant data held by Computer Security Incident Response Teams (CSIRTs) on incidents and attacks with all concerned authorities. This information sharing may be most valuable to law enforcement and judicial authorities for follow-up investigation and prosecution purposes. Without this cooperation, it is difficult to determine the scale and trends of cybercrime and threats to cybersecurity and thus to inform cybercrime and cybersecurity strategies in this region.

[8] EU-wide coordinated risk assessment of 5G networks security, 9 October 2019, https://digital-strategy.ec.europa.eu/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security

The action will contribute to national criminal justice authorities' capacities to fight cybercrime and enable access to electronic evidence, including implementation of and compliance with the substantive and procedural law provisions of the Budapest Convention and the Second Additional Protocol, increasing and enhancing the operational capacities of cybercrime units, as well as strengthening interagency, international and public/private cooperation.

In the area of cybersecurity, the Representatives from national Governments and institutions of EaP partner countries will be the direct beneficiaries of the action. The main counterparts will be representatives from the relevant ministries (i.e. Ministries of Digital Transformation, Foreign Affairs, Interior, Defence, Justice, etc.), National Regulatory Authorities and government agencies in charge of cybersecurity. Other key government stakeholders involved will include representatives from other relevant ministries (Telecommunication, Communication and Information Technologies, Infrastructure, Trade, Maritime Affairs etc.). They will contribute to the policy-making processes and participate in activities carried out under this action in their area of expertise.

In the area of cybercrime, all EaP countries have established specialised law enforcement units, 24/7 points of contact and authorities responsible for mutual legal assistance at the level of the General Prosecutor's Offices and Ministries of Justice. Those are the key public sector stakeholders, while service providers are the main private sector stakeholders. Given the crosscutting nature of cybercrime and electronic evidence, a number of other institutions will need to be involved. These include organisations responsible for cybersecurity (including CERTs/CSIRTs) and links between the two components of the action will thus be established. EU Delegations in the EaP Partner countries will play a fundamental role in ensuring that policy support provided through this action is consistent with and complementary to bilateral EU technical assistance programmes. They will also ensure adequate visibility of the European Union as the main donor for this action. The final beneficiaries of this action are the business community and the citizens of the EaP partner countries that would benefit from a more secure cyberspace.

2.3. Lessons Learned

The implementation of the current cybersecurity and cybercrime programme "Improving Cyber Resilience in the Eastern Partnership Countries" (2019-2023) entails number of lessons learnt.

In the area of cybersecurity following lessons have been learned:

- Due to restrictions caused by the COVID-19 pandemic, the Project shifted temporarily to online-only activities. Considering the sensitivity of the subject matter and other limitations of this method of capacity building, it is advisable not to use this for the new action. For best possible results, including technical exercises, multi-country training sessions, regional/international meetings most activities require physical presence.
- The implementation of the current programme has shown that the partner countries are less interested in general cybersecurity training and would like to benefit from much more targeted actions. The action should address those specific needs, including focused training programmes leading to certification, supporting more permanent training structures embedded within the national authorities and organising life-fire cyber exercises. Equipment and licences component should be considered in order to enhance the buy-in by the local interlocutors.
- Overall security situation in the region – Russian war of aggression against Ukraine, one country has suspended its participation in Eastern Partnership in 2021 autumn; two other countries have had bursts of the military conflict with each other has posed a significant challenge for the overall regional approach of the project and led to the focus on those three countries that have expressed interest to benefit from the EU capacity building.
- The candidate country status of Ukraine and Moldova and acknowledgement of Georgia's European perspective have created a new momentum in this regard. The project will have improved possibilities to

facilitate the alignment of the legislation and standards of those countries with the EU. There should be more focus on joint activities with EU cybersecurity institutions, notably the European Union Agency for Cybersecurity (ENISA).

In the area or cybercrime, much progress was made in terms of legislation implementing the Budapest Convention on Cybercrime, enabling efficient regional and international cooperation, and improving public/private cooperation on cybercrime and electronic evidence in the Eastern Partnership region. This project also featured new themes on enhancing operational capacities of cybercrime units, increasing accountability, oversight and public visibility of action on cybercrime, as well as strengthening interagency cooperation on cybercrime and electronic evidence, by improving information sharing between Computer Security Incident Response Teams (CSIRTs) and criminal justice authorities. Following the onset of the Russian aggression in February 2022, support was provided to Ukraine through cybercrime component (CyberEast) of the programme Improving Cyber Resilience in the Eastern Partnership Countries without delay.

It has also become clear that in the area of cybercrime the new action will need enhanced focus on:

- Support to the implementation of the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (legislation, procedures, guides, templates and practical training exercises);
- Practical training exercises at domestic and regional levels (simulation exercises, scenario-based training, table-top exercises, mock trials);
- Fostering synergies between criminal justice and cyber security responses to critical information infrastructure attacks, ransomware offences and other forms of cybercrime;
- Addressing needs regarding cybercrime and electronic evidence under the conditions of armed conflict (Ukraine).

Synergies shall be sought also with other ongoing EU regional initiatives, such as 'EU4Digitial', TOPCOP, 'Fight against Organised Crime in EaP region' and the bilateral programmes for example in Ukraine, Moldova and Georgia. EU4Digital should be particularly highlighted. Launched in 2019, it is a key project that supports digital economy and society in the region and contributes to the implementation of the Economic Investment Plan in the Eastern Partnership countries. It focuses on enabling a stronger economy and stronger governance in the Eastern partner countries through digital transformation.

The proposed action should ensure complementarity with bilateral programmes and provide cross-country added value in the improvement of cyber resilience and criminal justice response. For example, in Ukraine EUR 30 million have been invested into bilateral efforts in cybersecurity and resilient digital transformation. In Moldova, support has been mobilised through Rapid Assistance pillar of the Neighbourhood Development and International Development Cooperation Instrument (NDICI) to strengthen the capacity building of Moldovan stakeholders, enable to compile cybersecurity institutions' legal frameworks, and bring them in line with the EU's approach, standards, and relevant legal and policy framework. The added value of the regional action will be ensured by providing the built-in flexibility of following a multi-country approach tailored to regional and individual needs and priorities. Furthermore, ensuring co-ordination with other donors and actors on the ground is vital for the success of the action.

3. DESCRIPTION OF THE ACTION

3.1. Objectives and Expected Outputs

The overall objective of this action is to increase and enhance the cyber resilience capacities of the EaP Partner countries to better address the challenges of cyber threats and improve their overall security. The action will strengthen the criminal justice capacities of project countries on cybercrime and e-evidence in terms of legislation and policies, capacities for investigation, prosecution and adjudication as well as international and public/private cooperation, in line with the Budapest Convention on Cybercrime and its Second Additional Protocol and in line with European Union priorities for the EaP region.

The action will also build on a regional, individual and multi-country approach, promoting EU best practice and ensuring compliance with human rights.

Component 1: Cybersecurity

Specific objective 1.1: To strengthen the national cybersecurity governance and legal framework across the EaP countries in line with the NIS2Directive core pillars

Specific objective 1.2: To develop critical information infrastructure frameworks in the EaP countries

Specific objective 1.3: To increase the operational capacities for cybersecurity incidents management in the EaP countries

The **Outputs** to be delivered by this component contributing to the corresponding Specific Objectives 1.1.-1.3 are:

Outputs 1.1:

- National cybersecurity strategies, relevant legal frameworks and implementation documents are developed and tailored in approximation with the NIS2 Directive and other relevant EU cybersecurity policies, as well as National competent authorities to oversight cybersecurity are designated.
- Tailored approximation of the legal framework to the NIS2 Directive for the EaP Partner countries with an appropriate level of readiness and interest.
- Increased involvement and participation of the private sector and the civil society in cybersecurity decision-making and implementation including through reinforcing public private partnerships and networks.
- Targeted cyber awareness (Cyber Hygiene) actions are taken.
- Strengthened cooperation with the EU on cyber incident-response mitigation and cybersecurity policy issues, where applicable.

Outputs 1.2:

- Providers of the critical information infrastructure are identified in line with the NIS2 Directive.
- Technical and organisational measures to manage the cybersecurity risks posed to the critical information infrastructure developed and implemented.
- Notification framework on significant cybersecurity incidents in critical information infrastructures developed.

Outputs 1.3:

- National CSIRTs/CERTs designated and operational capacities for incidents management created. In the countries where the structures are still missing, set-up of functional national CERTs based on EU best practice and standards, including tailored-made training programmes. In the countries where they exist
- National cooperation between designated National CSIRTs/CERTs and providers of the critical information infrastructure on managing cybersecurity incidents ensured.
- Where relevant cooperation between designated National CSIRTs/CERTs in EaP partner countries and the EU and its Member States increased.

Component 2: Cybercrime

Specific objective 2.1: To support legislation and policy frameworks on cybercrime and electronic evidence and achieve stronger compliance with the Budapest Convention and its Second Additional Protocol

Specific objective 2.2: To reinforce capacities of criminal justice authorities through sustainable training frameworks, specialised training and practical exercises

Specific objective 2.3: To enhance cooperation on the basis of the Second Additional Protocol to the Budapest Convention

Specific objective 2.4: To reinforce synergies between criminal justice and cybersecurity responses to cyber threats.

The **Outputs** to be delivered by this component contributing to the corresponding Specific Objectives 2.1.-2.4 are:

Output 2.1:

- Regulatory framework for domestic investigations and international cooperation improved in line with the Budapest Convention and its Second Additional Protocol

Output 2.2:

- Informed cybercrime policies or strategies supported
- Improving advanced skills of cybercrime investigation and forensics through national and regional exercises

Output 2.3:

- Competent criminal justice authorities and 24/7 points of contact are able to apply the tools of the Second Protocol
- Increased public/private cooperation across borders on the basis of the Second Protocol

Output 2.4:

- Reinforced mechanisms for trusted cooperation between cybersecurity institutions and criminal justice authorities

3.2. Indicative Activities

Component 1: Cybersecurity

Activities related to Output 1.1:

- Capacity building across all the objectives through the provision of legal advice, strategic and operational analysis and institutional guidance
- Support the elaboration of draft legislation and policy documents in accordance with the EU legal framework – i.e. NIS2 Directive;
- Specific national, multi-country and regional training modules and mentoring cycles addressing the concerned stakeholders potentially leading to certification of cyber experts, where relevant embedded in the national structures
- Support the revision, update and/or conclusion of cooperation agreements with the private sector service providers through national workshops and regional activities, including the development of procedures for access and/or exchange of data held by private sector entities

- Targeted actions improving public awareness about cyber threats and improving cyber hygiene.

Activities related to Output 1.2:

- Technical assistance for the elaboration of national critical information infrastructure and private service providers critical for cybersecurity purposes mappings;
- Support for the definition of action plans and/or systematic processes for the protection of all critical information infrastructure developed;
- Develop comprehensive organisational schemes and mechanisms to create links between the national incident response organizations or CERTs and strengthen the countries' Critical Information Infrastructure Protection systems.
- Limited procurement of equipment and software licences.

Activities related to Output 1.3:

- Organisation of joint cyber incident management meetings, life-fire exercise(s) and mock operations to simulate a cyber-attack situation and operational meetings, to promote inter-agency and trans-national cooperation, particularly with the EU.
- Support for the organisation of joint cyber operations and investigations, where relevant with the EU and its Member States;
- Facilitation of operational meetings promoting inter-agency and trans-national cooperation in actual cyber incidents.

Component 2: Cybercrime

Activities related to Output 2.1:

- Support to legal reforms and review of applicable regulations implementing the provisions of the Second Additional Protocol to the Budapest Convention.
- Continued support to reforms of procedural law frameworks in line with Articles 16 to 21 of the Budapest Convention and related safeguards and conditions provided by Article 15 of the Budapest Convention.
- Further work specifically with Ukrainian authorities to improve procedural powers, applicable safeguards and international cooperation in the context of investigating gross human rights violations (possible war crimes).

Activities related to Output 2.2:

- Contribution to updates of cybercrime strategies or action plans and review of their effectiveness through supporting research and meetings with stakeholders.
- New national public perception surveys (Cyber Barometer reports) to identify threats, trends and reporting of incidents and crime with focus on crime victims and vulnerable groups for improving cybercrime/cybersecurity policies.
- Series of national studies of cybercrime threats, cybercrime offenders and criminal groups with involvement of national experts and academia/research institutions.
- National discussions with service providers, personal data protection authorities, civil society and national communications regulators on responsible reporting and prevention of cyberviolence.
- Prepare and conduct an advanced study on cybercrime threats, criminal groups and trends specific to the context of armed aggression against Ukraine, with possible regional conclusions relevant for other countries of the region.
- Organisation of national cybercrime exercises and mock trials focusing on the tools of the Second Protocol with relevant national partners, including judiciary, prosecutors, law enforcement and defence attorneys.

- Yearly Regional Cybercrime Cooperation Exercises for law enforcement, prosecutors, forensic experts, CSIRTs and specialised investigators involving real-time competitive simulation exercises on cybercrime and cybersecurity.
- Case simulation exercises and mock trials on cybercrime investigations and digital forensics for relevant agencies/entities in cooperation with other C-PROC projects.
- National competitive exercises on facilitating interagency cooperation and coordinated response to cyberattacks.

Activities related to Output 2.3:

- Practical guides, procedures and templates, and domestic and regional training on articles 8 (giving effect to production orders), 9 (expedited disclosure in emergencies), 10 (emergency mutual assistance), 11 (video conferencing) and 12 (joint investigation teams and joint investigations) of the Second Additional Protocol.
- Continued support to participation and networking in INTERPOL/EUROPOL/EUROJUST conferences, T-CY/Octopus, UN and other relevant events.
- Practical guides, procedures and templates, and domestic and regional training for competent authorities, service provides and registrars on the application of articles 6 (requests for domain name registration information) and 7 (production orders for subscriber information) of the Second Additional Protocol.
- Support to national dialogue with key infrastructure and service providers on preventive reporting, preservation and production of data.

Activities related to Output 2.4:

- Support implementation of national cooperation principles, operative procedures and segregation of duties, developed and agreed under CyberEast project, through national fora involving cybersecurity experts and criminal justice authorities.
- Develop and deliver training sessions based on national standard operating procedures (SOPs) – developed with the support of the CyberEast project – including simulation exercises on critical infrastructure attacks, ransomware attacks and other forms of cybercrime.
- Continue supporting improvement and interoperability of cybercrime/cyber-incident reporting systems in project countries, upon request.

3.3. Mainstreaming

Environmental Protection, Climate Change and Biodiversity

Not applicable for this action.

Outcomes of the Environmental Impact Assessment (EIA) screening

Not applicable for this action

Outcome of the Climate Risk Assessment (CRA) screening

Not relevant for this action

Gender equality and empowerment of women and girls

All activities under this action will be designed and implemented in accordance with the principle gender equality, wherever this issues are of particular relevance to the institutions and beneficiaries to be assisted.

Human Rights

All Critical Information Infrastructure Protection issues, also in relation to capacity building, involve a wide range of stakeholders including from national security and law enforcement agencies. Therefore, particular focus should be placed in the incorporation of safeguards in the proposed action in relation to human rights, data protection and good governance, in line with the EU Cybersecurity Strategy, the EU Strategic Framework and Action Plan on Human Rights and Democracy, and the EU Human Rights Guidelines on Freedom of Expression Online and Offline. The EU Council Conclusions on Cyber Diplomacy reaffirm the need to "foster open and prosperous societies through cyber capacity building measures in third countries that enhances the promotion and protection of the right to freedom of expression and access to information and that enables citizens to fully enjoy the social, cultural and economic benefits of cyberspace, including by promoting more secure digital infrastructures".

Strengthening domestic security and prosecution capacity, whilst strongly integrating human rights, may help mitigate the risk of "*cultures of impunity*" becoming entrenched. In this light, all assistance and training aspects must include precautionary measures to assure international human rights standards and norms are met. The issues that must be balanced are therefore to safeguard access and openness, to respect, protect and fulfil human rights online, and to maintain the reliability, resilience and interoperability of the Internet and other ICTs.

Disability

Not applicable for this action.

Democracy

All activities under this action will be designed and implemented in accordance with the principles of good governance. In providing technical assistance and capacity building, the issue of corruption will be carefully considered. To mitigate the challenges posed by corruption, anti-corruption actions will be comprehensively integrated into the training and awareness raising activities.

Conflict sensitivity, peace and resilience

The EU's international cybersecurity policy is designed to address the continuously evolving challenge of promoting global cyber-stability, as well as contributing to Europe's strategic autonomy and security in cyberspace, always guided by the EU's core values and fundamental rights. The EU will prioritise the establishment of a strategic framework for conflict prevention and stability in cyberspace in its bilateral, regional, multi-stakeholder and multilateral engagements. As part of the strategic framework for conflict prevention, the EU promotes the application of international law, and in particular the United Nations Charter, in cyberspace. The EU further supports the development of non-binding voluntary norms of state behaviour and cyber-confidence building measures.

Disaster Risk Reduction

Not applicable for this action.

3.4. Risks and Assumptions

Category	Risks	Likelihood (High/ Medium/ Low)	Impact (High/ Medium/ Low)	Mitigating measures
1- External environment	Continued Russian war of aggression against Ukraine does not allow to carry out the activities related to the action, particularly in the countries most impacted by this (Ukraine and Moldova)	High	High	Full support to Ukraine's territorial integrity and sovereignty through raising the cost of aggression to Russia including stepping up the sanctions. A detailed assessment needs to be made of the situation on the ground as regards the needs and possibilities for mitigating security risks and ensuring the sustainability of activities and investments and planning for contingencies.
1- External environment	Political instability in the region, including changes in government, military and other conflicts presenting an obstacle to project implementation and planned reform efforts. The hostilities in and around Nagorno-Karabakh may flare up again	Medium	Medium	Support the dialogue and peace process between involved parties.
1- External environment	The multifaceted and rapidly evolving target sector of the action implies that expertise, both at EU and partner country level, might be difficult to find for the implementation phase, namely with regards cybersecurity	Medium	High	All possible channels of communication will be used to reach out to the EU Member States (i.e. Council Horizontal Working Party on Cyber Issues) and the private sector since the early stages of the identification phase to raise awareness and interest.
2- Planning, processes and systems	Limited planning capacity and unwillingness of key cyber security interlocutors to engage in genuine all across government coordination	Medium	Medium	Support coordination capacities in institutions. Maintain a dialogue with the Government over plans and priorities.
3-People and the organisations	Limited interest, trust, and/or stakeholder buy-in	Medium	High	The project will adjust to demands from beneficiary governmental and private sector stakeholders. Possible lack of interest, trust and/or buy-in will be overcome through the demonstration of concrete results that can be derived from cooperation.

3-People and the organisations	High staff turnover and integrity issues	Medium	High	Putting in place a retention policy for knowledge and staff as well as enhanced transparency and oversight over the action as mitigating measures.
3- People and the organisations	Citizens, businesses and administrations do not disclose personal data for the fear of misuse.	Medium	Medium	The project will support the development and implementation of roadmaps based on Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) and in full compliance with the EU acquis, notably the principles related to citizens' fundamental rights, data protection, security, confidentiality, and the General Data Protection Regulation, as well as the Police Directive (EU) 2016/680. However, a sufficient national data protection regime will need to be established in the EaP partners, prior to developing any cross-border platform/pilot.

External Assumptions

- The political and security situation allows for the implementation of project activities and does not deteriorate to an unacceptable level, in particular no deterioration of the situation in and due to the Russia's war of aggression against Ukraine.
- National government partners remain committed and support project implementation.
- Trust is built among stakeholders.
- Partner countries will demonstrate national ownership, which is requisite for sustainability of the project deliverables.

3.5. Intervention Logic

Follow up to the current programme Improving Cyber Resilience in the Eastern Partnership Countries, it is the only EU level regional action that will tackle cybercrime and cybersecurity at the same time in the EaP region.

The rationale in the definition of the above-described cybersecurity result areas is based on the fact that these three dimensions (institutional/legal, technical and co/operational) are the tenet of any comprehensive cybersecurity conceptual framework. From the outset, setting up the necessary strategic frameworks at national level is fundamental in allowing third countries to identify roles and responsibilities in a structured manner through a national cybersecurity strategy and align with the EU legislation and institutional set-up, where relevant.

EaP countries have shown some capacity to monitor and manage incidents in cyberspace, the situation differs from country to country. To build this capacity, the introduction of both technological and organisational measures for better incident management is key. The minimum requirements are needed for setting up the national Computer Emergency Response Teams (CERTs), including specialised training and exchange of best practice within the international professional CERT networks. Effective cybersecurity capacity building needs a functioning national CERT, which is the centre of the coordination efforts, feeds information to law enforcement, and acts as an interface between the government agencies and the private sector. National CERTs, private sector and information security networks need to be brought together for long-term sustainable incident response and monitoring system.

In addition, the fostering of a community of trust amongst countries at a regional, trans-regional and international level in order to share information and cooperate in incident response handling is a prerequisite for effective cooperation.

Likewise, the rationale of the cybercrime result areas reflects that four dimensions (policy and legal frameworks, operational capacities of law enforcement and judiciary –i.e. across the criminal justice chain– and cooperation at inter-agency, public-private and international level) are the pillars of any basic conceptual framework in addressing cybercrime.

Against this background, the action is built around two components:

Component 1 will be fully dedicated to cybersecurity. The main outcome is to develop and implement technical and cooperation mechanisms that increase cybersecurity and preparedness to cyber-attacks, in line with the EU best practice and standards. Following up previous programme, the actions will be taken in parallel - institutional governance and the legal and policy frameworks will be dealt simultaneously with technical, operational and cooperation dimensions will follow, addressing the main issues related to critical information infrastructure protection and cyber-incidents management.

Component 2 will address cybercrime and electronic evidence to strengthen the criminal justice capacities in the six EaP countries from three main strands of action. Firstly, the legal and policy framework, with a specific focus on the implementation of the Budapest Convention and its Second Additional Protocol. Secondly, the reinforcement of operational capacities of law enforcement and judicial authorities. Thirdly, the cooperation at interagency, public/private and international levels will be addressed.
Links between the two components will be established. For example, the cybercrime component will comprise outcomes and activities aimed at improving information sharing between CERTs/CSIRTs and criminal justice authorities. CERTs/CSIRTs may also participate in some of the national and regional simulation exercises.

3.6. Indicative Logical Framework Matrix

	Results chain	Indicators	Baselines (incl. reference year)	Targets	Sources of data	Assumptions
Overall objective: Impact	To support the EaP partner countries in increasing and enhancing their cyber-resilience and criminal justice capacities to better address the challenges of cyber threats and improve their overall security.					
Specific objective(s): Outcome(s)	Component 1: Cybersecurity 1. To strengthen the national cybersecurity governance and legal framework across the EaP countries in line with the NIS2 Directive core pillars 2. To develop critical information infrastructure frameworks in the EaP countries 3. To increase the operational capacities for cybersecurity incidents management in the EaP countries	4. Country position at ITU's Global Cybersecurity and Cyber-wellness Index 5. Country position at the CyberGreen Index 6. Country position at the Digital Evolution Index (Fletcher School, Tufts University, 2019) 7. Country position at the Freedom House's Freedom on the Net report (2019) 8. Level of involvement of civil society organisations in the cybersecurity decision making processes.	1. Country position at ITU's Global Cybersecurity and Cyber-wellness Index (i.e. at the start of the action) 2. Country position at CyberGreen Index (2019) 3. Country position at the Digital Evolution Index (Fletcher School, Tufts University, 2019) 4. Country position at the Freedom House's Freedom on the Net report (2019) 5. Marginal civil society involvement in decision making in EaP Partner countries - to be verified/determined by the implementing partner at the inception phase for	1. Improvement of country position at ITU's Global Cybersecurity and Cyber-wellness Index by at least 4 places (2022) 2. Improvement of country position in the CyberGreen Index by at least 4 places (2022) 3. Improvement of country position at the Digital Evolution Index by at least 4 places (Fletcher School, Tufts University, 2022) 4. Improvement (or non-deterioration) of country position at the Freedom House's Freedom on the Net report by at least 3 places (2022) 5. Establishment of informal or formal	1. Global Cybersecurity Index 2. CyberGreen Index 3. Digital Evolution Index 4. Freedom on the Net Report 5. Civil society scrutiny reports on oversight of national cybersecurity policies and executive measures (privacy/ surveillance, freedom of expression online, access to content)	The action is not disrupted by adverse events, such as a fragile security situation, natural hazards, and public health crises. Political stability in the target countries The allocated budget is sufficient both for the full duration and for the full scope of the action. The application of new cybersecurity strategies and associated activities does not have an adverse impact on human rights in the target countries

			each selected third country (2019)	consultation structures between the government and civil society in relation to cybersecurity in all selected third countries - to be confirmed by the implementing partner at the inception phase (2022)		
Outputs	1.1 EaP regional cybersecurity guidelines based on EU experiences and standards developed and endorsed 1.2 Strengthened regional and international cooperation on cyber incident-response mitigation and cybersecurity policy issues, where applicable. 1.3 National cybersecurity strategies, relevant legal frameworks and implementation documents are developed and tailored in approximation with the NIS2 Directive and other relevant EU cybersecurity policies, as well as National competent authorities to oversight cybersecurity are designated.	1. Number of EaP Partner countries adopting national cyber strategies and/or Action Plans in line with the EU best practice and standards. 2. Number of key private sector entities (especially from critical infrastructure/services) and civil society (including women representatives) participating in the development and/or implementation of the national cyber strategies. 3. Number of cooperation MoUs signed between national governments and private sector stakeholders. 4. Number of formal or informal cyber information sharing networks created and/or enhanced, that facilitate incident report sharing/early warning/mitigation of serious cyber incidents.	1. 3 (2019) 2. To be determined by the implementing partner for each EaP Partner country at the inception phase 3. To be determined by the implementing partner for each EaP Partner country at the inception phase. 4. To be determined by the implementing partner for each EaP Partner country at the inception phase. 5. 0 (2019) 6. 0 (2019)	1. 6 (2022) 2. To be determined by the implementing partner for each EaP Partner country at the inception phase, depending on the local industry configuration/maturity and civil society environment. 3. To be determined by the implementing partner for each EaP Partner country at the inception phase 4. To be determined by the implementing partner for each EaP Partner country at the inception phase 5. At least 1 per year 6. To be determined by the implementing partner at the inception phase.	- Project update reports - National reports from cyber-coordinating Ministries - ENISA reports - Press releases - National CERTs reports - Civil society reports - Regional organisations' reports - National government reports - Press releases	Good cooperation amongst Ministries and Agencies. National governments actively seek the involvement of the private sector and civil society. Ability of the implementing partner to mobilise timely the right expertise for the roll out of activities. Translation and interpretation services for the roll out of activities do not create delays.

	1.4 Tailored approximation of the legal framework to the NIS2 Directive for the EaP Partner countries with an appropriate level of readiness and interest. 1.5 Increased involvement and participation of the private sector and the civil society in cybersecurity decision-making and implementation including through reinforcing public private partnerships and networks. 1.6 Cyber awareness (Cyber Hygiene) framework for all EaP partner countries proposed.	5. Number of operational meetings promoting inter-agency and trans-national cooperation in actual cyber incidents. 6. Number of joint cyber operations and investigations. 7. To increase cyber-hygiene awareness.				
	2.1 Mapping of national critical information infrastructure and private service providers critical for cybersecurity purposes. 2.2 Action plans and/or systematic processes for the protection of all critical information infrastructure developed. 2.3 Links between the national incident response organizations	1. Number of EaP Partner countries adopting Critical Information Infrastructure Protection policies. 2. Number of countries where the national incident response organizations or CERTs are organizationally linked to the country's Critical Infrastructure Protection system, and there is an elected/political/democratic oversight on the activities of this technical organisation	1. 2 (2019) 2. To be determined by the implementing partner for each EaP Partner country at the inception phase.	1. At least 4 (2022) 2. At least 3 (2022)	- Project update reports - National reports from cyber-coordinating Ministries - ENISA reports - Press releases - National CERTs reports - Civil society reports - Regional organisations' reports	

	or CERTs and the countries' Critical Information Infrastructure Protection systems strengthened.				- National government reports - Press releases	
	1.1 National CSIRTs/CERTs designated and operational capacities for incidents management created. In the EaP countries with an appropriate level of readiness and interest, set-up of functional national CERTs based on EU best practice and standards, including tailored-made training programmes. 1.2 National cooperation between designated National CSIRTs/CERTs and providers of the critical information infrastructure on managing cybersecurity incidents ensured. 1.3 Cooperation between designated National CSIRTs/CERTs in EaP partner countries increased.	1. Number of incident response organisations and CSIRTs/CERTs established and/or functional in the EaP Partner countries 2. Number of CSIRTs/CERTs that are recognized by the private sector and key government agencies as national and international focal points for cyber incidents 3. Number of incident management/response cases monitored and handled by national computer emergency response teams (CERTs) 4. Number of national incident response organisation or CERTs that have a training programme in place and are part of the international professional cyber associations (e.g. FIRST, Trusted Introducer) 5. Number of table-top exercises and mock operations undertaken within the project framework. 6. Number of countries gaining membership to	1. 5 (2019) 2. To be determined by the implementing partner for each EaP Partner country at the inception phase. 3. To be determined by the implementing partner for each EaP Partner country at the inception phase. 4. To be determined by the implementing partner for each EaP Partner country at the inception phase. 5. 0 (2019)	1. 6 (2022) 2. At least 3 (2022) 3. Increase by 50% (2022) 4. At least 4 (2022) 5. At least 4 (2022) 6. At least 3 (2022)	- Project update reports - National government reports, including Statistical Office (NSO) progress reports - National CERTs reports/ website - Security Incident Management Maturity Model 3 (SIM3) Assessment Results - FIRST - Trusted Introducer	National legislative process for the establishment of CERTs is not blocked Allocation of funding from the national budget for the minimum CERT set up and staff recruitment is approved Good cooperation amongst Ministries and Agencies Required software and hardware is available Trained staff remain within their institutions beyond the capacity building exercise Ability of the implementing partner to mobilise timely the right

	1.4 Specific defined for CERTs in the EaP countries. 1.5 Increased international recognition and trust of CERTs in the EaP countries.	international professional cyber associations.				expertise for the roll out of activities Translation and interpretation services for the roll out of activities do not create delays
Specific objective(s): Outcome(s)	Component 2: Cybercrime 1. To adopt legislative and policy frameworks compliant to the Budapest Convention. 2. To reinforce the capacities of judicial and law enforcement authorities and interagency cooperation 3. To increase efficient international cooperation and trust on criminal justice, cybercrime and electronic evidence, including between service providers and law enforcement	- Availability of action plans or strategies on cybercrime. - Compliance of procedural law with the Budapest Convention. - Level of interagency, public/private and international cooperation.	As of 2018, limited: - Compliance with the procedural law provisions of the Budapest Convention. - Interagency, international and public/private cooperation. - Action plans or strategies on cybercrime.	By 2022, increased: - Compliance with the procedural law provisions of the Budapest Convention. - Interagency, international and public/private cooperation - Action plans or strategies on cybercrime.	Project reports and assessments by the Cybercrime Convention Committee (T-CY).	Components on cyber-security and cybercrime are connected.
Outputs	1.1 National action plans or similar strategic documents regarding the criminal justice response to cybercrime and electronic evidence developed. 1.2 Substantive criminal law, if necessary, in line with Articles 2 to 12 of	- Number and quality of action plans or similar strategic documents. - Number and quality of legislative amendments.	- No specific action plans or strategies in Armenia, Azerbaijan and Belarus. - Procedural law deficient in 4/6 countries.	- Action plans or strategies in 5/6 countries. - Draft legislative amendments in 5/6 countries approved by Governments.	Project reports.	Legislative amendments to be approved by Parliaments.

	the Budapest Convention revised and improved. 1.3 Procedural law for the purposes of domestic investigations in line with Articles 16 to 21 of the Budapest Convention improved.					
	2.1 Operational cybercrime units in law enforcement authorities' skills and institutional set up strengthened. 2.2 Improvement of interagency cooperation of the relevant law enforcement and criminal justice authorities, agencies and bodies including through improved data sharing. 2.3 Internal and external accountability and oversight mechanisms defined and adopted capacities of civil society organisations and oversight bodies reinforced. 2.4 Public communication and transparency on	- Extent to which the capacities and competencies of cybercrime units are improved. - Availability of training plans. - Number of training and simulation exercises and officials trained. - Availability of procedures on CERTs/CSIRT – law enforcement data sharing.	- Specialised units in place but with no clear competencies, nor division of tasks. - Limited interagency cooperation. - No specific training plans. - Limited CERT/CSIRT-LEA information sharing.	- Competencies and division of tasks of specialised units clarified. - Improved interagency cooperation. - Training plans available. - Improved CERT/CSIRT – LEA information sharing.	Project reports.	Readiness and willingness by agencies to cooperate with each other.

	cybercrime-related actions improved. 2.5 Reinforce mechanisms for cooperation and trust with the private sector and citizens 2.6 .					
	3.1 Skills, set up and competencies of the 24/7 points of contact further strengthened. 3.2 Guidelines and procedures for mutual legal assistance and data requests in place. 3.3 Operational skills for international judicial and police authorities cooperation on cybercrime strengthened. 3.4 Implementation of existing agreements on public/private cooperation and the conclusion of such agreements in the remaining countries. 3.5	- Number of cases handled by 24/7 contact points. - Number of cases where templates have been used. - Number of training events, official trained on police-to-police, and judicial cooperation.	- 24/7 points of contact available in all countries, but limited use in practice in most countries (few cases handled per year). - No specific templates used for requests. - Limited skills for international cooperation in practice.	- Significant increase in cases handled by 24/7 points of contact. - Templates used in practice. - Core staff for police-to-police and judicial cooperation trained in the six EaP countries.	Project reports.	Sufficient trust by partner countries. Support to participation in the T-CY and other relevant international events should facilitate this.
	4. Improved cooperation and trust between law enforcement and service providers regarding	- Number and quality of cooperation agreements between service providers and criminal justice authorities.	- Cooperation agreements or arrangements in place in 2/6 countries.	- Cooperation agreements or arrangements in place in 5/6 countries.	Project reports.	Improved service provider/law enforcement cooperation will need to rely largely

	criminal justice access to electronic evidence: 4.1 Implementation of existing agreements on public/private cooperation and conclusion of such agreements in the remaining countries. 4.2 Procedures and templates for requests for data agreed upon public and private sector authorities trained in their application through domestic and regional workshops and simulation exercises.	- Number and quality of procedures and templates and of staff trained to operationalize these agreements.	- Limited procedures and trained staff in place to implement agreements.	- Procedures and trained staff in place in 5/6 countries.		on improved procedural law.

4. IMPLEMENTATION ARRANGEMENTS

4.1. Financing Agreement

In order to implement this action, it is not foreseen to conclude a financing agreement with the partner countries.

4.2. Indicative Implementation Period

The indicative operational implementation period of this action, during which the activities described in section 3.1 will be carried out and the corresponding contracts and agreements implemented, is 72 months from the date of adoption by the Commission of this financing Decision.

Extensions of the implementation period may be agreed by the Commission's responsible authorising officer by amending this financing Decision and the relevant contracts and agreements.

4.3. Implementation Modalities

The Commission will ensure that the EU appropriate rules and procedures for providing financing to third parties are respected, including review procedures, where appropriate, and compliance of the action with EU restrictive measures[9].

4.3.1. Indirect Management with pillar-assessed entities

This action may be implemented in indirect management with pillar-assessed entities which will be selected by the Commission's services using the following criteria:

Component 1 of this action (cybersecurity) will be implemented in indirect management with a pillar assessed entity from the EU Member States based on the following criteria:

- Track record of management of EU funds in Eastern Partnership region
- Availability of cybersecurity expertise
- Solid experience of managing project related to security or governance in Eastern Partnership region, experience of implementing EU funds in the region
- Ability to link with the EU cybersecurity and Member States government's cybersecurity institutions

Component 2 of this action (cybercrime) will be implemented in indirect management with a pillar-assessed international organisation based on-the following criteria:

- Longstanding strategic partnership with European Commission, both at the policy level and as an implementing partner in the field of rule of law, human rights and democracy
- Organisation that is based on legally-binding instruments and convention-based monitoring mechanisms at a pan-European scale
- Solid experience in providing support to the Eastern partner countries and in promotion of structured criminal justice reforms in the fight against based on internationally agreed legal framework of reference

[9] EU Sanctions Map. Please note that the sanctions map is an IT tool for identifying the sanctions regimes. The source of the sanctions stems from legal acts published in the Official Journal (OJ). In case of discrepancy between the published legal acts and the updates on the website it is the OJ version that prevails.

[1] Please find the Twinning Fiche template as Annex C1 of the Twinning Manual available in English at this link.

- Ability to carry out budget-implementation tasks: running the public procurement, grant award procedures, concluding and managing the resulting contracts, including making of the related payments

4.3.2. Changes from indirect to direct management mode due to exceptional circumstances

If the implementation modality under **indirect management** as defined in section 4.3.1 cannot be implemented due to circumstances beyond the control of the Commission or in case no compliant pillar assessed entity can be identified, these parts of the action may be implemented through **grants under direct management**.

Objectives of the grants: The grants shall contribute to achieving the objectives identified in the intervention logic of this Action Document.

Criteria of the grant: The selection criteria will be the ones defined above for the selection of pillar-assessed entities in section 4.3.1 and aligned with article 195 (f) FR.

4.4. Indicative Budget

	EU contribution (amount in EUR)	**Indicative third party contribution, in currency identified**
Component 1 (Cybersecurity): Indirect management with pillar assessed entity from EU Member State	EUR 3 500 000	N/A
Component 2 (Cybercrime): Indirect management with an international organisation	EUR 3 500 000	
Evaluation (Section 5.2)	Will be covered by another Decision	
Audit (Section 5.3)	Will be covered by another Decision	
Strategic Communication and Public diplomacy	Will be covered by another Decision	
Total	EUR 7 000 000	

4.5. Organisational Set-up and Responsibilities

The responsibility of the action lies with the Commission. The steering of the project will be led by Directorate-General for Neighbourhood and Enlargement Negotiations.

At least one annual steering committee meeting separately for the two components will be led by Commission services for reviewing the three results of the project and guide the way forward with main stakeholders. If it is deemed relevant the steering committee meetings can take place more often. Other Commission services (such as Directorate-General for Communications Networks, Content and Technology and Directorate-General for Migration and Home Affairs) and the European External Action Service will be closely associated as relevant.

The implementers will provide the Secretariat of the Steering Committee for their respective components.

The European Commission will ensure, with the support of the implementers, the coordination and communication with the interested stakeholders, including relevant Commission Services and EU Delegations. Specific contact points shall be nominated at headquarters, in EU Delegations and in field offices to ensure coordinated internal and external communication.

The Steering Committee will be chaired by the Commission for the cybersecurity component, while for the cybercrime component, it will be co-chaired by the Commission and the implementing partner and include representatives of operational entities, and where relevant of the European External Action Service and of any other concerned Directorate-General of the Commission. ENISA and Europol will be observers in both Steering Committees. The Steering Committee is responsible for monitoring the implementation of the "EU4Digital: Improving Cyber Resilience in the Eastern Partnership countries" on the basis of activity reports presented by the implementing partners. The Steering Committee shall meet at least twice a year to be updated on the annual activities and for the monitoring of the implementation. With the support of the implementing partners, an annual meeting chaired by the Commission will be organised with representatives of the five EaP countries. EU Member States may also be invited.

5. PERFORMANCE MEASUREMENT

5.1. Monitoring and Reporting

The day-to-day technical and financial monitoring of the implementation of this action will be a continuous process, and part of the implementing partner's responsibilities. To this aim, the implementing partners shall establish a permanent internal, technical and financial monitoring system for the action and elaborate regular progress reports (not less than annual) and final reports. Every report shall provide an accurate account of implementation of the action, difficulties encountered, changes introduced, as well as the degree of achievement of its Outputs and contribution to the achievement of its Outcomes, and if possible at the time of reporting, contribution to the achievement of its Impacts, as measured by corresponding indicators, using as reference the logframe matrix. The report shall be laid out in such a way as to allow monitoring of the means envisaged and employed and of the budget details for the action. The final report, narrative and financial, will cover the entire period of the action implementation.

The Commission may undertake additional project monitoring visits both through its own staff and through independent consultants recruited directly by the Commission for independent monitoring reviews (or recruited by the responsible agent contracted by the Commission for implementing such reviews).

Further, implementation of the projects and their contribution to EaP deliverables shall be closely monitored by the Steering Committee, as referred to above in section 5.5.

5.2. Evaluation

Having regard to the importance of the action, a final evaluation will be carried out for this action or its components via independent consultants contracted by the Commission.

The independent final evaluation will be carried out for accountability and learning purposes at various levels taking into account in particular the tangible results of the action and the impact achieved for citizens, the visibility of the action, internal and external communication, and the lessons learnt of the enhanced cooperation between the Commission and the Council of Europe leading to visible and quantifiable improvements in the scope, width and depth of joint Commission and Council of Europe activities and impacts on reforms in the partner countries.

The independent final evaluation will be carried out for accountability and learning purposes at various levels taking into account in particular the tangible results of the action and the impact achieved for citizens, the visibility of the action, internal and external communication, and the lessons learnt of the enhanced cooperation between the Commission and the Council of Europe leading to visible and quantifiable improvements in the scope, width and depth of joint Commission and Council of Europe activities and impacts on reforms in the partner countries.

The Commission shall inform the implementing partners in advance of the dates foreseen for the evaluation missions. The implementing partners shall collaborate efficiently and effectively with the evaluation experts, and inter alia provide them with all necessary information and documentation, as well as access to the project premises and activities.

The evaluation reports shall be shared with the partner countries and other key stakeholders. The implementing partner and the Commission shall analyse the conclusions and recommendations of the evaluations and, where appropriate, in agreement with the partner country, jointly decide on the follow-up actions to be taken and any adjustments necessary, including, if indicated, the reorientation of the project.

The Commission shall form a Reference Group (RG) composed by representatives from the main stakeholders at both EU and implementing partners levels. The RG will especially have the following responsibilities:

- **Steering the evaluation exercise in all key phases** to comply with quality standards: preparation and/or provision of comments to the Terms of reference; selection of the evaluation team; consultation; inception/desk, field, synthesis and reporting phases.
  The EU programme manager steers the RG and is supported in its function by RG members
- **Providing input and information** to the evaluation team. Mobilise the institutional, thematic, and methodological knowledge available in the various stakeholders that are interested in the evaluation
- **Providing quality control** on the different draft deliverables. The EU programme manager, as lead of the RG, consolidates the comments to be sent to the evaluation team and endorses the deliverables.
- **Ensuring a proper follow-up** after completion of the evaluation

The financing of the evaluation shall be covered by another measure constituting a financing decision.

5.3. Audit and Verifications

Without prejudice to the obligations applicable to contracts concluded for the implementation of this action, the Commission may, on the basis of a risk assessment, contract independent audit or verification assignments for one or several contracts or agreements.

6. STRATEGIC COMMUNICATION AND PUBLIC DIPLOMACY

All entities implementing EU-funded external actions have the contractual obligation to inform the relevant audiences of the Union's support for their work by displaying the EU emblem and a short funding statement as appropriate on all communication materials related to the actions concerned. To that end they must comply with the instructions given in the 2022 guidance document *Communicating and raising EU visibility: Guidance for external actions* (or any successor document).

This obligation will apply equally, regardless of whether the actions concerned are implemented by the Commission, the partner country, service providers, grant beneficiaries or entrusted or delegated entities such as UN agencies, international financial institutions and agencies of EU Member States. In each case, a reference to the relevant contractual obligations must be included in the respective financing agreement, procurement and grant contracts, and delegation agreements.

For the purpose of enhancing the visibility of the EU and its contribution to this action, the Commission may sign or enter into joint declarations or statements, as part of its prerogative of budget implementation and to safeguard the financial interests of the Union. Visibility and communication measures should also promote transparency and accountability on the use of funds. Effectiveness of communication activities on awareness about the action and its objectives as well as on EU funding of the action should be measured.

Implementing partners shall keep the Commission and the EU Delegation fully informed of the planning and implementation of specific visibility and communication activities before the implementation. Implementing partners will ensure adequate visibility of EU financing and will report on visibility and communication actions as well as the results of the overall action to the relevant monitoring committees.

Appendix 1: IDENTIFICATION OF THE PRIMARY INTERVENTION LEVEL FOR REPORTING IN OPSYS

A Primary intervention[10] (project/programme) is a coherent set of results structured in a logical framework aiming at delivering development change or progress. Identifying the level of the primary intervention will allow for:

- ✓ Differentiating these Actions or Contracts from those that do not produce direct reportable development results, defined as support entities (i.e. audits, evaluations);
- ✓ Articulating Actions and/or Contracts according to an expected common chain of results and therefore allowing them to ensure a more efficient and aggregated monitoring and reporting of performance;
- ✓ Having a complete and exhaustive mapping of all results-bearing Actions and Contracts.

The present Action identifies as

Action level (i.e. Budget support, Blending)		
□	Single action	Present action: all contracts in the present action
Group of actions level (i.e: i) top-up cases, ii) second, third, etc. phases of a programme)		
□	Group of actions	Actions reference (CRIS#/OPSYS#): <Present action> <Other actions>
Contract level (i.e. Grants, Contribution Agreements, any case in which foreseen individual legal commitments identified in the budget will have different log frames, even if part of the same Action Document)		
□	Single Contract 1	<foreseen individual legal commitment (or contract)>
□	Single Contract 2	<foreseen individual legal commitment (or contract)>
□	Single Contract 3	<foreseen individual legal commitment (or contract)>
	(…)	
Group of contracts level (i.e: i) series of programme estimates, ii) cases in which an Action Document foresees many foreseen individual legal commitments (for instance four contracts and one of them being a Technical Assistance) and two of them, a technical assistance contract and a contribution agreement, aim at the same objectives and complement each other, iii) follow up contracts that share the same log frame of the original contract)		
□	Group of contracts	<foreseen individual legal commitment (or contract) 1> <foreseen individual legal commitment (or contract) 2> <foreseen individual legal commitment (or contract) #>