SUMMARY

NEIGHBOURHOOD EAST REGIONAL ACTION PROGRAMME 2018, PART III, TO BE FINANCED FROM THE GENERAL BUDGET OF THE EUROPEAN UNION

1. IDENTIFICATION

Budget line	22.04.02.01
Total cost	EUR 7 000 000 of EU contribution: - EUR 7 000 000 from the general budget of the EU for 2018 Analytical breakdown: - EUR 3 200 000 on Component 1 "Cybersecurity" - EUR 3 800 000 on Component 2 "Cybercrime"
Legal basis	Regulation (EU) No 232/2014 of the European Parliament and of the Council of 11 March 2014 establishing a European Neighbourhood Instrument (ENI)

2. REGIONAL BACKGROUND

The EaP countries are faced with revitalising and diversifying their economies while maintaining fiscal and macroeconomic stability. Most countries are faced with security issues either on their borders or inside the country.

The EU regional approach for assisting these countries can increase confidence among them and promote security, stability, and prosperity in the region.

3. SUMMARY OF THE ACTION PROGRAMME

The European Neighbourhood Policy, including the EaP and the bilateral relations between the EU and each of these countries, guides the EU policy responses to the challenges of the ENI East region.

With a total allocation of EUR 7 000 000, the ENI East Regional Action Programme (RAP) 2018, Part III will address:

1. EU4Digital: Improving Cyber Resilience in the Eastern Partnership Countries

The objective of the Action is to contribute to improving the cyber-resilience and criminal justice response of the Eastern Partnership (EaP) countries and will focus on two key building blocks: cybersecurity and cybercrime.

To this end, this Action will encompass the following two components:

a) The development of technical and cooperation mechanisms that increase cybersecurity and preparedness against cyber-attacks, such as the strengthening the institutional governance and legal framework, developing the critical information infrastructure structure, and increasing the incident management capacities

b) The 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. The Budapest Convention continues to provide the benchmark for an effective framework.

The proposed actions will be implemented, when appropriate, at the regional level, but also at country's and multi-country's level to address specific needs of individual EaP countries according to the differentiated approach of the revised European Neighbourhood Policy and to the specific situation in the countries.

3.1 Neighbourhood-related policy of partner countries

Serious cyberattacks and other security incidents in recent years have targeted countries of the EaP region, as well as transiting through or originating in these countries, ultimately targeting EU Member States. Thus, the growing challenges and threats in the region related to the cyberspace and the need to respond, amongst other things, through the means of law enforcement and judicial authorities, is recognised.
At the last EaP Justice and Home Affairs Ministerial that took place on 7 July 2017 in Tallinn, the ministers of the Partner countries all welcomed the assistance provided so far in the above areas by the EU and called for further support in the field of cyber.

3.2 Consistency with the programming documents:

The RAP 2018 is in line with the ENI East Regional Strategy Paper, the 2015 ENP Review and the Indicative Programme 2017-2020, and Article 7 of the ENI Regulation. RAP 2018 proposed actions are foreseen in the framework of the Regional Indicative Programme 2017-2020.

Action	Priority area	Ref. multiannual indicative programme
Action 1	Strengthening institutions and good governance	ENI Multiannual indicative programme 2017-2020

3.3 Identified actions and expected results

Action Programme:

The **overall objective** of this action is to increase and enhance the cyber-resilience and criminal justice capacities of the EaP Partner countries to better address the challenges of cyber threats and improve their overall security.
The project will also build on a regional, individual and multi-country approach, promoting EU best practice and ensuring compliance with human rights.

The Specific Objectives and corresponding results (outputs) are:

I) Component 1: Cybersecurity

- To strengthen the national cybersecurity governance and legal framework across the EaP countries.
- To strengthen the protection of critical information infrastructure in the EaP countries.
- To increase the operational capacities for cybersecurity incidents management in the EaP countries.

II) Component 2: Cybercrime

- To adopt legislative and policy frameworks compliant to the Budapest Convention.

- To reinforce the capacities of judicial and law enforcement authorities and interagency cooperation.
- To increase efficient international cooperation and trust on criminal justice, cybercrime and electronic evidence, including between service providers and law enforcement.

3.5 Complementary actions/donor coordination

Activities will be coordinated with other EU-funded activities and with other donors' activities. Project implementation is also reported to the EaP platforms and panels. The ENI Committee before their adoption by the European Commission approves all regional programmes.

4. COMMUNICATION AND VISIBILITY

Communication and information activities are an integral part of the support measure 'ENI-East Global Allocation'. Each specific project shall also have its own communication component elaborated in line with the Communication and Visibility Manual for EU External Action[1].

5. COST AND FINANCING

The total costs of the action programme is EUR 7 000 000.

Action	EUR
Action 1 - Budget line: 22.04.02.01	**7 000 000**
Total Amount RAP	**7 000 000**

The Committee is invited to give its opinion on the attached ENI East RAP 2018, Part III.

[1] https://ec.europa.eu/europeaid/funding/communication-and-visibility-manual-eu-external-actions_en

ANNEX

of the Commission Implementing Decision on the ENI Regional East Action Programme 2018 part III

Action Document for EU4Digital: Improving Cyber Resilience in the Eastern Partnership Countries

ANNUAL PROGRAMME
This document constitutes the annual work programme in the sense of Article 110(2) of the Financial Regulation and action programme/measure in the sense of Articles 2 and 3 of Regulation N° 236/2014.

1. Title/basic act/ CRIS number	EU4Digital: Improving Cyber Resilience in the Eastern Partnership countries CRIS number: ENI/2018/041-179 financed under European Neighbourhood Instrument
2. Zone benefiting from the action/location	Eastern Partnership (EaP) countries: Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova and Ukraine The action shall be carried out in the six EaP countries.
3. Programming document	Programming of the European Neighbourhood East Instrument (ENI) – 2014-2020 – Regional East Strategy Paper (2014-2020) and Multiannual Indicative Programme (2017-2020)
4. 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 programme 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			
5. Sector of concentration/ thematic area	Security Strengthening Institutions and Good Governance	DEV. Aid: YES[1]		
6. Amounts concerned	Total estimated cost: EUR 7 380 000 Total amount of EU budget contribution EUR 7 000 000 This action is co-financed in joint co-financing by: - Council of Europe for an amount of EUR 380 000.			
7. Aid modality(ies) and implementation modality(ies)	Project Modality Direct management through: Procurement (component 1) Indirect management with the Council of Europe (component 2)			
8 a) DAC code(s)	15210 Security system management and reform 22040 Information and communication Technology 15130 Legal and judicial development			
b) Main Delivery Channel				
9. Markers (from CRIS DAC form)	**General policy objective**	**Not targeted**	**Significant objective**	**Main objective**
	Participation development/good governance	☐	☐	✓
	Aid to environment	✓	☐	☐
	Gender equality (including Women In Development)	☐	✓	☐
	Trade Development	☐	✓	☐
	Reproductive, Maternal, New born and child health	✓	☐	☐
	RIO Convention markers	**Not**	**Significant**	**Main**

[1] Official Development Aid is administered with the promotion of the economic development and welfare of developing countries as its main objective.

		targeted	**objective**	**objective**
	Biological diversity	✓	☐	☐
	Combat desertification	✓	☐	☐
	Climate change mitigation	✓	☐	☐
	Climate change adaptation	✓	☐	☐
– **10. Global Public Goods and Challenges (GPGC) thematic flagships**	N/A			

SUMMARY

In light of the increased cyber-attacks affecting the EU Member States and the Eastern Partnership (EaP) countries, a need for a regional programme encompassing cybersecurity and cybercrime has been identified.

This new programme will contribute to improving the cyber-resilience and criminal justice response of EaP Partner countries and will focus on two key building blocks. First, the development of technical and cooperation mechanisms that increase cybersecurity and preparedness against cyber-attacks, such as the strengthening the institutional governance and legal framework, developing the critical information infrastructure structure, and increasing the incident management capacities. Second, the 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. The Budapest Convention continues to provide the benchmark for an effective framework.

Consequently, the programme is divided between a cybersecurity (first building block) and a cybercrime (the second building block) component.

The proposed actions will be implemented, when appropriate, at regional level but also at country level to address specific needs of the individual EaP Partners according to the differentiated approach of the revised European Neighbourhood Policy.

1 CONTEXT ANALYSIS

1.1 Context Description

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. 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[2], 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, research and technology development, and education.[3] 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.

A. Cybersecurity

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 promotion of human rights, 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. This ultimately hinders fundamental rights.

Cybersecurity represents the first layer of protection against cybercrime. Law enforcement authorities are ill equipped to respond to high-volume opportunistic crime, which can be effectively prevented through awareness raising and the implementation of basic cybersecurity measures. Therefore, regular outreach and public education campaigns directed to end-users should be considered. Further reinforcing IT security will contribute to effectively strengthening the fight against cybercrime and the prevention of other forms of online crimes and attacks against information systems.

The EU recognized 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.

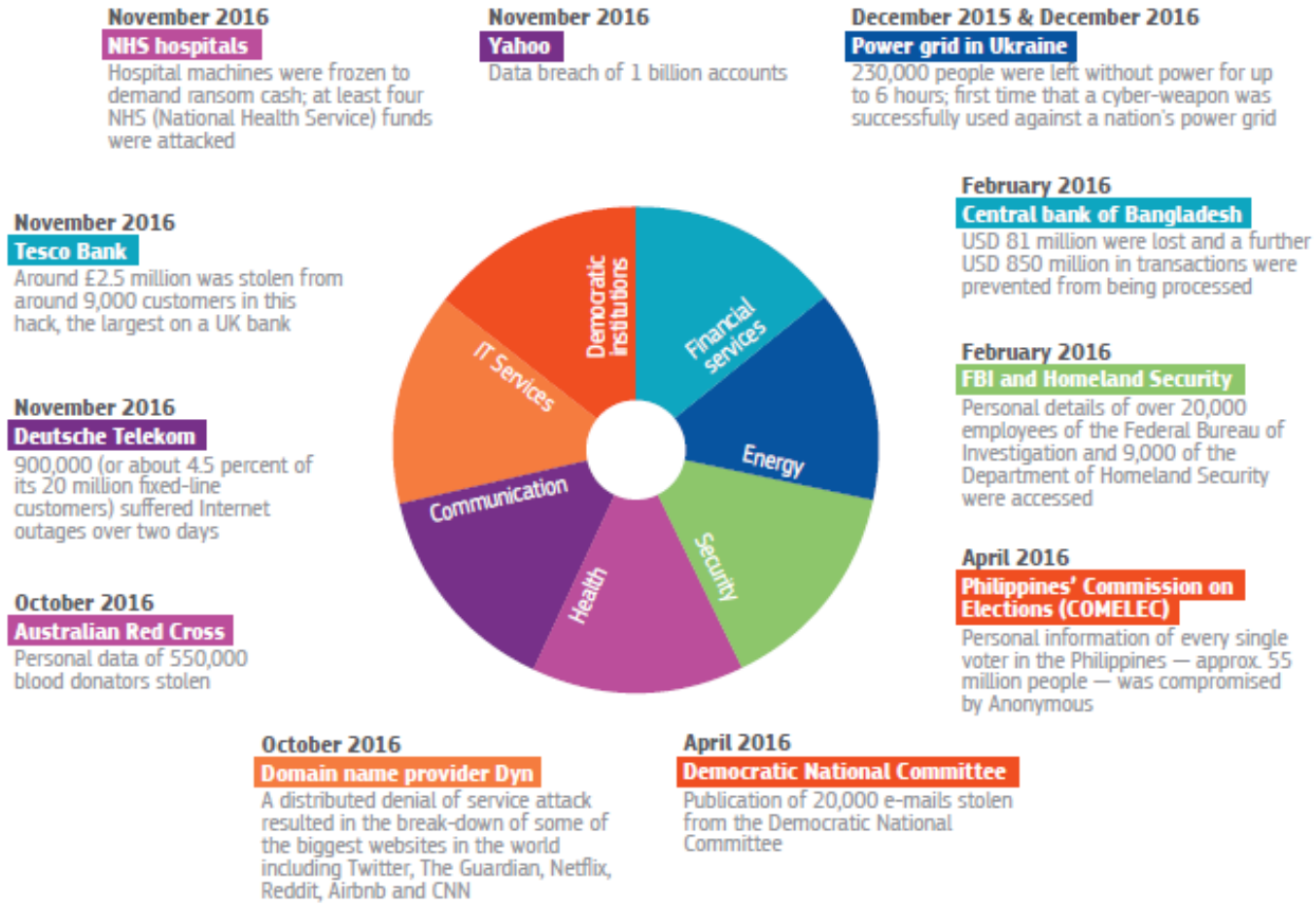
---

2 R. Wainwright, & F. Cilluffo, "Responding to cybercrime at scale", *Europol,* 2017, 10p.

3 H. Tiirmaa-Klaar, "Building national cyber resilience and protecting critical information infrastructure", *Journal of Cyber Policy,* vol. 1, n°.1, 2016, pp.94-106.

Figure 1: No critical sector escapes the cyber threat

This figure features only a small selection of incidents that took place in 2016. Many more attacks occur every day all over the world.



Source: European Political Strategy Centre, based on media reports

B. Cybercrime

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, various forms of online sexual and gender-based violence, 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[4] 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).[5] It is therefore an international obligation for them to 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 (CoE) since 2011 under the umbrella of the EU-CoE Partnership for Good Governance (PGG). As a result, good progress has been made in many respects.

Furthermore, the EaP countries adopted in October 2013 (Kyiv, Ukraine) a Declaration on Strategic Priorities for the Cooperation against Cybercrime in the EaP Region[6]. They committed to pursue the necessary actions in key areas, such as procedural law, safeguards and guarantees, data protection and protection of children against online sexual abuse and exploitation with the objective of adopting an overarching effective framework to combat cybercrime on the basis of the Budapest Convention.

However, despite progress made, the following concerns and challenges have been identified:

- **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 criminal 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.
- **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 (CERTs) 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.

The last four points constitute overriding issues and should be addressed, inter alia, through practical simulation exercise(s) involving relevant stakeholders backed up by guidelines and other tools and best practice.

[4] The Convention on Cybercrime of the Council of Europe (CETS No.185), known as the Budapest Convention: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561
[5] Belarus participates in the T-CY as ad-hoc observer and has expressed its commitment to implement this treaty.
[6] https://rm.coe.int/1680300ad4

1.2 Policy Framework (Global, EU)

Through the **revised European Neighbourhood Policy,** the European Union seeks to enhance its cooperation with the neighbouring countries, especially with the Eastern neighbours in key areas of social and political life. Strengthening democratic processes in the ENP countries, good governance, economic growth and integration, energy security, involving civil society, are among the priorities.

The revised European Neighbourhood Policy introduced **differentiation** among the countries, in accordance with their ambitions in the relationship with the European Union. It also calls for **prioritisation** and for a more focused approach in order to deliver tangible and noticeable results to the citizens, as reflected in the Joint Staff Working document "EaP – Focusing on key priorities and deliverables" identifying a list of 20 deliverables for 2020.

In line with the EU priorities in this field, DG NEAR is engaging deeper in its policy dialogue with its partner countries on cybersecurity, cyber-resilience and countering hybrid threats, protection of critical infrastructures and strategic communication. **Moldova** has already undertaken the hybrid threats risk assessment survey under the Action 18 of the Joint Communication "Joint Framework on countering hybrid threats". This hybrid risk threat assessment has been launched for **Georgia** in February 2017.

Deliverable 12 aims at increasing the resilience of Partner Countries to security threats, through stronger cooperation in the area of **security**. Until 2020, three targets under deliverable 12 are set to strengthen the cyber-resilience of Partners, including through the adoption of Strategies or Action Plans to address cybercrime; the designation of operational contact points for international police-to-police and judicial cooperation on cybercrime and e-evidence; the development of national CERTs[7] and Cybersecurity Strategies (if not in place).

Building on the **European Agenda on Security**, adopted in April 2015, the European Commission put forward a new Communication in April 2016 aimed at paving the way towards an effective and genuine Security Union. The European Directive on Security of Network and Information Systems (**'NIS' Directive**), adopted in July 2016, which was to be implemented by Member States by 9 May 2018 is therefore an integral part of the strategy. The 2015 Digital Single Market Strategy also aims to make the EU a stronger player in digital technologies, while acknowledging the importance of trust and security. The EU must also contribute to building an international framework on cyberspace that helps to strengthen trust among all stakeholders.

On 19 September 2017, the Commission and the High Representative proposed to reinforce the EU's resilience and response to cyber-attacks through a new **Cybersecurity Package.** The wide range of measures included therein build on existing instruments and present new initiatives to further improve EU cyber resilience and provide a response in three key areas:

- Building EU resilience to cyber-attacks and stepping up the EU's cybersecurity capacity;
- Creating an effective criminal law response; and
- Strengthening global stability through international cooperation.

[7] Computer Emergency Response Teams.

As part of the Cybersecurity Package, the EU Council (General Affairs Council) adopted on 26 June 2018 the Council conclusions on EU External Cyber Capacity Building Guidelines8. They aim at offering an overall policy framework for a coherent, holistic and strategic approach to EU external cyber capacity building based on EU values and should help guide and prioritise EU efforts in assisting partner countries and organisations.

A step towards improving the criminal law response to **cyber-attacks** was taken with the adoption of the 2013 Directive on attacks against information systems[9] that sets out minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems and provides for operational measures to improve cooperation amongst authorities. The EU has also adopted legislation to fight effectively other forms of cybercrime such as dissemination of child abuse material and grooming[10], and fraud and counterfeiting of non-cash means of payment[11]. The Commission has also proposed new rules enabling cross-border access to electronic evidence[12].

The Joint SWD '**EaP – 20 Deliverables for 2020**' lists several targets in the areas of fighting cybercrime and enhancing cybersecurity, in particular:

- The full implementation of the Budapest Convention;
- The reinforced protection of critical infrastructure;
- The set-up of fully operational national CERTs;
- The adoption of actionable national cybersecurity Strategies; and
- Enhanced public/private and international cooperation on cybersecurity.
- Developing the capacity to respond to cybersecurity incidents.

The EU and all the EaP Partner countries agreed in the Declaration of the Second EaP Ministerial Meeting on the Digital Economy (October 2017, Tallinn) to:

- Improve the resilience of the critical infrastructure in different key sectors of the economy for the benefit of citizens, businesses and public administrations;
- Launch further actions to promote the development of national cybersecurity strategies and operational national CERTs in line with EU best practices.

By assisting beneficiary countries in focusing on common challenges, a **regional approach** has the potential to increase confidence among partner countries, and thus to promote increased security, stability and prosperity in the region, while **allowing bilateral actions** to address country-specific needs.

[8] http://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf
[9] Directive 2013/40/EU on attacked against information systems.
[10] Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography.
[11] Framework Decision 2001/413/JHA combating fraud and counterfeiting of non-cash means of payment – currently under revision.
[12] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

1.3 Public Policy Analysis of the partner country/region

A. Cybersecurity

Georgia, Moldova and Ukraine have adopted national cybersecurity strategies; however, only Georgia and Ukraine have set up policy department units. Azerbaijan, Belarus and Georgia have threat assessment units. In Azerbaijan, Belarus, Georgia and Ukraine, a point of contact has been identified for international cooperation porpuses.

Regarding baseline security, Belarus, Moldova, Ukraine and to some extent Georgia present some of the key elements connected to cybersecurity.

Critical infrastructure protection is addressed only in Belarus and Georgia. CERTs or similar structures are set up in Azerbaijan, Belarus, Georgia, Moldova and Ukraine.

The table in Annex I presents more details on the level of approximation of the EaP Partner countries to the EU legal and strategic framework – namely the NIS Directive[13].
Against this background, this regional action will focus in further developing the approximation of all EaP Partner countries to the EU basic pillars on cybersecurity. As the previous explanation shows, there is a different level of advancement between the EaP countries. Therefore, beyond the basic pillars, specific activities and objectives will be also be defined to address the specific situation of countries as well as their differing degree of preparedness and willingness to further advance their approximation to the EU relevant legal and strategic framework – i.e. the NIS Directive. Namely, the programme will also specifically engage with the three EaP countries which have signed an Association Agreement with the EU.

B. Cybercrime

Georgia, Ukraine and Moldova have cybercrime strategies and/or action plans as part of other strategies as follows:

In Georgia, cybercrime is covered by the updated National Strategy 2017-2020 for Combating Organised Crime and its Action Plan 2017-2018. For Ukraine as part of the cybersecurity strategy, with yearly action plans since 2016. Since 2015, in Moldova there is a separate section No. 4 entitled “Preventing and combating cybercrime” in the National Programme on Cybersecurity 2016-2020" (adopted by Government Decision n˚811 dd. 29/10/2015). Other sections of the Programme aim to achieve safe processing, storage and access to data; security and integrity of electronic communications networks and services; capacities of prevention and emergency response (CERT); strengthening cyber defence capacities; education and information; and international cooperation and contact. Moldovan authorities are also guided by the action plan on the implementation of the National Strategy for Information Society Development, Digital Moldova 2020, approved under the Government Decision No 857 of 31 October 2013.

[13] As per the information contained in the “Situation Review: Safety and Security of Cyberspace and E-Democracy in the EaP Countries” by the Estonian e-Governance Academy

Azerbaijan, Armenia and Belarus do not have a strategy/action plan to tackle cybercrime nor as part of another strategy.

All countries have designated operational contact points for international police-to-police and judicial cooperation. (For the Contracting Parties to the Budapest Convention on Cybercrime, this is an obligation under the Convention).

The table in Annex II shows further details on the state of implementation of the Budapest Convention in the EaP Partner countries[14].

1.4 Stakeholder analysis

Serious cyberattacks and other security incidents in recent years have targeted countries of the EaP region, as well as transiting through or originating in these countries, ultimately targeting EU Member States. Thus, the growing challenges and threats in the region related to the cyberspace and the need to respond, amongst other things, through the means of law enforcement and judicial authorities, is recognised.

At the last EaP Justice and Home Affairs Ministerial that took place on 7 July 2017 in Tallinn, the ministers of the Partner countries all welcomed the assistance provided so far in the above areas by the EU and called for further support in the field of cyber.

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 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, Infrastructures etc.). They will contribute to the policy-making processes and participate in activities carried out under this action in their area of expertise.

With regard to the **cybercrime component**, 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 programme 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.

[14] Discussion paper prepared by the Cybercrime Programme Office of the Council of Europe (C-PROC) under the Cybercrime@EAP projects,

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.

1.5 Problem analysis/priority areas for support

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

(i) the development of technical and cooperation mechanisms that increase cybersecurity and preparedness to cyber-attacks, such as setting up of functional Computer Emergency Response Teams, organising table-top exercises and improving the general cyber hygiene.

(ii) 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, increasing and enhancing the operational capacities of cybercrime units, as well as strengthening interagency, international and public/private cooperation. The capabilities in this respect were assessed as incomplete at the June 2017 EaP Rule of Law panel devoted to the fight against cybercrime as well as in the report prepared by the Council of Europe in June 2017 in the framework of the Partnership for Good Governance[15].

2 RISKS AND ASSUMPTIONS

Risks	**Risk level (H/M/L)**	**Mitigating measures**
The multifaceted and rapidly evolving target sector of the programme implies that expertise, both at EU and partner country level, might be difficult to find for the implementation phase, namely with regards cybersecurity	M	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.
Regional programmes have sometimes difficulties to be implemented in Belarus due to absence of financing agreement with the government and the need to register all actions. Further to this, Belarus is not a member of the Council of Europe, one of the implementing partners of this	L	Smooth implementation in Belarus will be ensured through early notification to the government (Ministry of Interior, Justice and Defence) about the programme, as well as possibly identifying a local partner to facilitate registration of the programme activities in Belarus. The Government has expressed on several occasions its predisposition to adhere to the greatest

[15] Cybercrime strategies, powers and institutions in the Eastern Partnership region – State of Play

action.		extent possible to the Budapest Convention, to which it is not a Party.
Lack of or insufficient Rights Based Approach in the beneficiary countries in their cybersecurity and cybercrime framework and operations.	M	Mainstreaming Fundamental Rights into the programme activities. This will include focusing on an external and internal oversight mechanism.
Limited interest, trust, and/or stakeholder buy-in	L	The project has been developed in direct response to demands from beneficiary governmental and private sector stakeholders. As such, it is extremely unlikely that EaP partner countries will not remain committed. Even so, any lack of interest, trust and/or buy-in will be overcome through the demonstration of concrete results that can be derived from cooperation. Project activities will be adjusted accordingly should there be limited interest.
Citizens, businesses and administrations do not disclose personal data for the fear of misuse.	M	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.
Share of the list of critical infrastructures per country	M	This risk is only limited, as such lists, considered extremely sensitive, are highly classified and very rarely shared. In the EU, in application of Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, only the number of European Critical Infrastructures (ECIs) and their sector are communicated to EC; all other elements of the identity of such ECIs are kept secret by Member States.

Assumptions
The political and security situation allows for the implementation of project activities and does not deteriorate to an unacceptable level. 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 LESSONS LEARNT, COMPLEMENTARITY AND CROSS-CUTTING ISSUES

3.1 Lessons learnt

3.1.1 Actions undertaken under the EU-Council of Europe Partnership for Good Governance (PGG)

The project aims at improving the cooperation between law enforcement and judicial authorities and service providers in specific criminal investigations and with the necessary rule of law safeguards.

Cybercrime is as one of the priorities of the PGG, managed by the Council of Europe and financially supported by NEAR through its ENI instrument.

The PGG assists the EaP countries in adopting a set of strategic priorities on cybercrime and electronic evidence. EaP countries established specialised units, training programmes, co-operation with private sector entities, and all EaP countries now have cyber security strategies adopted or in draft form with the exception of Belarus. In Georgia, Moldova and Ukraine action against cybercrime is among the priorities of cybersecurity strategies. In Georgia, cybercrime is also reflected in the strategy on organised crime.

During the CyberCrime@EAP project, EaP countries furthermore identified the strengthening of capacities for international cooperation and public/private partnerships on cybercrime and electronic evidence as strategic priorities for the region. A precondition for international and public/private cooperation is that law enforcement and judicial authorities have the necessary powers – legal, institutional and operational – to investigate cybercrime and secure electronic evidence. Such procedural powers – corresponding to Articles 16 to 21 Budapest Convention – must be clearly defined in domestic criminal law and be subject to conditions and safeguards to meet rule of law requirements.

3.1.2 Actions undertaken under the East Police Cooperation Programme (PCP)

Fight against cybercrime was one of the focus areas under the PCP aiming at increasing police cooperation on issues related to cross-border crime between the EU and EaP countries and among EaP countries themselves. There has been a call from beneficiaries to strengthen further the support in this area.

3.1.3 The 'Safety and Security of Cyberspace and E-Democracy in the EaP Countries' situation review

This Situation Review – published by the e-Governance Academy of Estonia in 2017 – provides the current situation of the state of affairs in the field of cyber security and e-democracy in the Eastern Partnership countries

3.1.4 TAIEX and Twining activities

The Technical Assistance and Information Exchange instrument (TAIEX) of the European Commission (DG NEAR), supports public administrations with regard to the approximation, application and enforcement of EU legislation, as well as facilitating the sharing of EU best practices. It is originally demand-driven and delivers appropriate tailor-made expertise to address issues at short notice. In the past two years, we have used this instrument 15 times for cyber-related expert workshop and trainings in the EU accession and neighbouring countries.
For example, in Ukraine alone in 2017 7 TAIEX events were organised in the area of cybersecurity.

3.2 Complementarity, synergy and donor coordination

Synergies shall be sought also with other ongoing and upcoming EU regional initiatives, such as 'EU4Digitial' and the bilateral programmes for example in Moldova and Ukraine. The proposed action on cybersecurity and cybercrime will ensure complementarity with bilateral programmes and provide cross-country added value in the improvement of cyber resilience and criminal justice response. This will be provided through the built-in flexibility of following a multi-country approach tailored to regional and individual needs and priorities.

Ensuring co-ordination with other donors and actors on the ground is vital for the success of the programme.

3.2.1 East Regional Action Programme (RAP 2018): EU4Digital programme

Under the EaP regional programme 'EU4Digital', it was initially envisaged to *"develop a standard set of cybersecurity guidelines for the EaP region based on EU experiences"*, for assessing threats, risks and vulnerabilities of information systems and resources from cyberspace, and provide for appropriate exchanges with EaP partner country counterparts, as well as external/internal oversight, accountability and communication/transparency mechanisms. The guidelines should also cover the specification and certification of minimum competence requirements (duties, functions and obligations) for public and private sector employees in the field of cyber security.

3.2.2 Georgia

The "EU4 Security, Accountability and Fight against Crime in Georgia (SAFE)" program under the Annual Action Programme 2018 (AAP 2018) will contribute to strengthening good governance and the rule of law in Georgia and will ultimately increase the security of citizens. This programme will aim at: (i) consolidating the prevention and fight against crime; (ii) improving civil protection; and (iii) enhancing the oversight over the security sector.
More concretely, it identifies two specific objectives relevant to this regional programme: 1) to strengthen cyber security capacities; and 2) to further improve resilience against cybercrime and other threats against critical infrastructure

3.2.3 Ukraine

The AAP 2018 foresees the support to the consolidation of the legislative framework in the field of cybersecurity in line with EU acquis and building the capacity of Ukrainian institutions to protect critical infrastructure and increase resilience and response to cyber threats.

3.2.4 Moldova

Under AAP 2017, a project (under elaboration) will support the national Centre for Emergency Response Team (CERT) or the Centre for Special Telecommunication (CTS). More details will follow the completion of a need assessment.

Complementarity with the three bilateral programmes will be ensured. The regional programme will help building the foundations of some systems, which may be expanded under the bilateral programmes. The Steering Committee of this action will regularly monitor the complementarity and synergies with the bilateral programmes.

4 DESCRIPTION OF THE ACTION

The implementation of this action, reflected under the below-described objectives, expected results and activities, will follow a sequencing approach for both components. A prioritisation system will be stablished to focus first on the institutional governance and legal and policy framework, and subsequently the technical, operational and cooperation activities.

4.1 Objectives

The **overall objective** of this action is to increase and enhance the cyber-resilience and criminal justice capacities of the EaP Partner countries to better address the challenges of cyber threats and improve their overall security.

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 (SO) 1.1: To strengthen the national cybersecurity governance and legal framework across the EaP countries

Expected results (indicative), where applicable:

- Strengthened regional and international cooperation on cybersecurity.
- National cybersecurity strategies, relevant legal frameworks and implementation documents are developed and tailored in approximation with the EU NIS Directive.
- National frameworks and actor for the internal and external oversight of cybersecurity defined and reinforced.
- Tailored approximation of the legal framework to the EU NIS 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 the development and implementation of cybersecurity policies and measures.
- Increased cyber awareness (Cyber Hygiene) in all EaP partner countries proposed.

SO 1.2: To strengthen the protection of critical information infrastructure in the EaP countries

Expected results (indicative):

- Mapping of the critical information infrastructure in line with the EU NIS Directive.
- Strengthened the management and mitigation of the cybersecurity risks posed to the critical information infrastructure.
- Framework on managing and responding to major cybersecurity incidents relating to critical information infrastructures developed.

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

Expected results (indicative):

- National CSIRTs/CERTs designated and operational capacities for incidents management created and further strengthen taking into account the respective levels of readiness.
- National cooperation between designated National CSIRTs/CERTs and owners of the critical information infrastructure on managing cybersecurity incidents improved.
- Cooperation between designated National CSIRTs/CERTs in EaP partner countries increased.

Component 2: Cybercrime

SO 2.1: To adopt legislative and policy frameworks compliant to the Budapest Convention

Expected results (indicative):

- National action plans or similar strategic documents regarding the criminal justice response to cybercrime and electronic evidence developed.
- Substantive criminal law, if necessary, in line with Articles 2 to 12 of the Budapest Convention revised and improved.
- Procedural law for the purposes of domestic investigations in line with Articles 16 to 21 of the Budapest Convention improved.

SO 2.2: To reinforce the capacities of judicial and law enforcement authorities and interagency cooperation

Expected results (indicative):

- Operational cybercrime units in law enforcement authorities, skills and institutional set-up strengthened.
- Improvement of interagency cooperation of the relevant law enforcement and criminal justice authorities, agencies and bodies including through improved data sharing.
- Internal and external accountability and oversight mechanisms defined and adopted capacities of civil society organisations and oversight bodies reinforced.
- Public communication and transparency on cybercrime-related actions improved.
- Reinforce mechanisms for cooperation and trust with the private sector and citizens.

SO 2.3: To increase efficient international cooperation and trust on criminal justice, cybercrime and electronic evidence, including between service providers and law enforcement

Expected results (indicative):

- Skills set up and competencies of the 24/7 points of contact further strengthened.
- Guidelines and procedures for mutual legal assistance and data requests in place.
- Operational skills for international judicial and police authorities' cooperation on cybercrime strengthened.
- Implementation of existing agreements on public/private cooperation and the conclusion of such agreements in the remaining countries.

4.1.1 Main activities

The indicative activities identified below will be implemented in a country, multi-country and/or regional tailored manner. Activities will include but not be limited to the ones listed here under.

Component 1: Cybersecurity

SO 1.1: To strengthen the national cybersecurity governance and legal framework across the EaP countries

- Capacity building across all the objectives through the provision of legal advice, strategic and operational analysis and institutional set-up guidance, inter alia technical assistance and advice for the definition and implementation of national cybersecurity priorities, incorporating modules on human rights, data protection safeguards and oversight;
- Steer, assist and support the elaboration of amendments to legislation, or to the formulation new legislation proposed, in accordance with the EU legal framework – i.e. NIS Directive;
- National, multi-country and regional training modules and mentoring cycles addressing the concerned stakeholders (also via a train-the-trainers approach) of relevant public officials, inter alia on cyber threats and response, cyber-hygiene, human rights, data protection safeguards and oversight mechanisms;
- Support the revision, update and/or conclusion of cooperation agreements with the private sector service providers through national workshops and regional activities, inter alia the development of procedures for access and/or exchange of data held by private

sector entities, as well as training on the application of standard templates and procedures for access to data through case studies and simulation exercises (national or regional level);
- Public awareness raising campaigns and trainings organised and delivered to inform citizens about cyber threats and to improve their consciousness of individual cyber hygiene.

SO 1.2: To strengthen the protection of critical information infrastructure in the EaP countries

- Technical assistance for the elaboration of national critical information infrastructure and private service providers relevant for cybersecurity purposes mappings;
- Support for the definition of action plans and/or systematic processes for the protection of all critical information infrastructure developed;
-
- Support through technical assistance and training the development of Critical Information Infrastructure Protection systems creating relevant links with CERTs established.

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

- Organisation of joint cyber incident management meetings, table-top exercise(s) and mock operations to simulate a cyber-attack situation and operational meetings, to promote inter-agency and trans-national cooperation, trust, transparency, exchange of information and predictability amongst those EaP Partner countries which manifest an appropriate level of readiness and willingness;
- Support for the organisation of joint cyber operations and investigations;
- Facilitation of operational meetings promoting inter-agency and trans-national cooperation in actual cyber incidents;
- Supporting, promoting and further consolidating existing regional networks.

Component 2: Cybercrime

SO 2.1: Legislative and policy frameworks and compliance with the Budapest Convention

- Assessment of compliance with substantive law provisions of the Budapest Convention on Cybercrime through country assessments;
- Contribution to development/update of cybercrime strategies and action plans through national discussion forums, advisory missions and discussions at regional meetings;
- Continued support to EaP countries in the preparation of country reports on cybercrime and cybersecurity trends and threats and preparation of updated regional report;
- Continued support to reforms of procedural law frameworks and related legislation through national seminars and workshops, based on needs and requests of EaP states;
- High-level regional and as relevant national meetings of criminal justice authorities, policy makers and members of Parliament to assess key issues and design action plans of legislative reform in the Eastern Partnership countries.

SO 2.2: Reinforcement of the capacities of judicial and law enforcement authorities and interagency cooperation

- Assessment – through in-country visits – of the institutional setup, capacities, competencies, training needs as well as interagency cooperation gaps and opportunities for cybercrime units in the Eastern Partnership region;
- Contribution to update and/or development of the training plans for cybercrime units with a view to establishing sustainable knowledge sharing and training frameworks at criminal justice training institutions (through in-country seminars and workshops with regional review);
- Development and implementation of domestic and regional training sessions, case simulation exercises and mock trials on cybercrime investigations, digital forensics for relevant agencies/entities;
- Business analyses and development of agreed procedures for cybercrime/incident reporting and sharing of data by Computer Security Incidents Response Teams (CSIRTs) with criminal justice authorities through country-specific workshops with regional conclusions; Workshops and training to follow up on assessment/business analyses to promote data sharing and integration of data.

SO 2.3: To increase efficient international cooperation and trust on criminal justice, cybercrime and electronic evidence, including between service providers and law enforcement

- Development of standard step-by-step guidelines for drafting and processing of mutual legal assistance requests for criminal cases involving cybercrime and electronic evidence;
- National, regional and international workshop, traininds and hands-on simulations for improvement of the skills, set-up and competencies of 24/7 points of contact;
- National training sessions for cybercrime units and prosecutors on the use of templates for international requests for data preservation and subscriber information;
- Regional/international case simulation exercises developing skills for international cooperation on cybercrime and electronic evidence for judicial and police cooperation authorities.
- Further support, building on previous Cybercrime@EaP projects, to the revision, update and/or conclusion of cooperation agreements between the law enforcement and criminal justice authorities through national workshops and regional activities;
- National workshops for development of standard templates and procedures for access to data held by private sector entities; training to support their implementation including through through case studies and simulation exercises (national or regional level);
- Continued support to public-private dialogue on cooperation through maintenance of the online resource on cooperation and supporting participation in regional and international initiatives and events on public-private cooperation.

4.2 Intervention logic

This action is the first intervention that tackles 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 assess and define their needs and identify roles and responsibilities in a structured manner through a national cybersecurity strategy.

Moreover, EaP countries have shown a limited capacity to monitor and manage incidents in cyberspace. 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.
First, the institutional governance and the legal and policy frameworks will be dealt with. For this, the legislation/regulation of the EaP partner countries will be assessed and modify against the core pillars of the NIS Directive, building on security and trust. The 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. 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.

4.3 Mainstreaming

4.3.1 International security

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.

4.3.2 Rights based approach

All activities under this programme will be designed and implemented in accordance with the principles of good governance and human rights, gender equality, the inclusion of socially or economically deprived groups and environmental sustainability, wherever these issues are of particular relevance to the institutions and beneficiaries to be assisted.

All Critical Information Infrastructure Protection (CIIP) 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 2015 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.

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.

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.

To ensure compliance of the proposed action with the obligations stipulated in Article 10 ("Human rights") of Regulation (EU) No 230/2014, a clear human rights perspective should be incorporated throughout the different stages of the project cycle (project design/formulation; monitoring of implementation; evaluation) on the basis of the operational guidance developed to this end by the European Commission (https://ec.europa.eu/europeaid/operational-human-rights-guidance-eu-external-cooperation-actions-addressing-terrorism-organised_en). Any potential flow-on risk on the respect of human rights should be constantly monitored and mitigating measures need to be foreseen.

4.3.3 Gender equality

Cyber- violence against women and girls (VAWG), is a global problem with serious implications for societies and economies around the world. The statistics pose risks to the peace and prosperity for all enshrined in the Charter of the United Nations, and, in particular, to the goals of inclusive, sustainable development that puts gender equality and the empowerment of women as key to its achievement. The sheer volume of cyber VAWG has severe social and economic implications for women and girls and responses have yet to be fully addressed.

There exist various forms of cyber VAWG, including, but not limited to, online harassment to the desire to inflict physical harm including sexual assaults, murders and suicides, cyber stalking, non-consensual pornography (or 'revenge porn'), 'sextortion', and electronically enabled trafficking.

Research suggests that women are disproportionately the targets of certain forms of cyber violence compared to men. In line with the international human rights legal framework, including the Istanbul Convention[16], this action will accompany the EaP countries to improve institutional responses to cyber VAWG, in order to protect women both online as well as offline.

4.4 Contribution to SDGs

This intervention is relevant for the 2030 Agenda. It contributes primarily to the progressive achievement of SDG 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.

5 IMPLEMENTATION

[16] The Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention), signed by the EU June 2017: https://www.coe.int/en/web/istanbul-convention/home

5.1 Financing agreement

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

5.2 Indicative implementation period

The indicative implementation period for this action, during which the activities described in section 4 will be carried out and the corresponding contracts and agreements implemented, is **50 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 Decision and the relevant contracts and agreements.

5.3 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[17].

5.3.1 Procurement (direct management) (Component 1)

Subject in generic terms	Type (works, supplies, services)	Indicative number of contracts	Indicative trimester of launch of the procedure
Cybersecurity	Services	1	2nd quarter 2019

5.3.2 Indirect management with an international organisation

A part of this action (Component 2 of this action – i.e. Cybercrime) may be implemented in indirect management with the Council of Europe. This implementation entails the continuation of the implementation of the activities of the CyberCrime@EaP projects under the Partnership for Good Governance regional project, whose objectives will now only be covered under this new action. The envisaged entity has been selected due to the Council of Europe's expertise in standard-setting and monitoring tools.

The **Council of Europe** (CoE) is a longstanding strategic partner to the European Commission, both at the policy level and as an implementing partner in the field of rule of law, human rights and democracy. As a key organisation based on legally-binding instruments and convention-based monitoring mechanisms at a pan-European scale, the Council of Europe has been for decades a key partner for the EU in providing support to the Eastern partner

[17] www.sanctionsmap.eu 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.

countries. In this context, the EU has partnered with the Council of Europe (CoE) to promote structured criminal justice reforms in the fight against cybercrime on the basis of the Budapest Convention on Cybercrime that serves as the international legal framework of reference.

Cybercrime is one of the fields of CoE's expertise and the CoE has been supporting capacity building on cybercrime in the EaP region through several projects under the Partnership for Good Governance (PGG): CyberCrime@EAP from 2011 to 2014 was followed by CyberCrime@EAP II on international cooperation on cybercrime and electronic evidence (May 2015 – December 2017) and Cybercrime @EAP III, on public/private cooperation (December 2015 – December 2017). Both Cybercrime@EAP II and Cybercrime@EAP III were extended for one year in 2018 through a joint project Cybercrime@EAP 2018, implemented within the framework of the Partnership for Good Governance (PGG) between the EU and the CoE.

The entrusted entity would carry out the following budget-implementation tasks: running the public procurement, grant award procedures, concluding and managing the resulting contracts, including making of the related payments.

It is envisaged to have activities implemented in coordination with the EU Agency for Law Enforcement Training (CEPOL), Europol and the EU Agency for Network and Information Security (ENISA).

5.3.3 Changes from indirect to direct management mode due to exceptional circumstances

If negotiations with the above-mentioned entity fail, that part of this action may be implemented in direct management in accordance with the implementation modalities identified in section 5.3.1.1.

Subject in generic terms	Type (works, supplies, services)	Indicative number of contracts	Indicative trimester of launch of the procedure
Cybercrime	Services	1	2nd quarter 2019

5.4 Scope of geographical eligibility for procurement and grants

The geographical eligibility in terms of place of establishment for participating in procurement and grant award procedures and in terms of origin of supplies purchased as established in the basic act and set out in the relevant contractual documents shall apply.

The Commission's authorising officer responsible may extend the geographical eligibility in accordance with Article 9(2)(b) of Regulation (EU) No 236/2014 on the basis of urgency or of unavailability of products and services in the markets of the countries concerned, or in other duly substantiated cases where the eligibility rules would make the realisation of this action impossible or exceedingly difficult.

5.5 Indicative budget

	EU contribution (amount in EUR)	**Indicative third party contribution, in currency identified**
5.3.1.1 Procurement (direct management) (Component 1)	EUR 3 200 000	N/A
5.3.1.2 Indirect management with an international organisation (Component 2)	EUR 3 800 000	EUR 380 000
Total	**EUR 7 000 000**	**EUR 380 000**

5.6 Organisational set-up and responsibilities

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

An annual steering committee 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. 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 service provider and the Council of Europe will provide the Secretariat of the Steering Committee for their respective components.

The **European Commission will ensure,** with the support of the Council of Europe, **the coordination and communication** with the interested stakeholders, including relevant Commission Services and EU Delegations. Programme-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 Council of Europe and include representatives of Council of Europe 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 invited as 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 service provider and the Council of Europe. 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 service provider and the Council of Europe, an annual meeting chaired by the Commission will be organised with representatives of the six EaP countries. EU Member States may also be invited.

5.7 Performance and Results monitoring and reporting

Performance measurement will be based on the intervention logic and the log frame matrix, including its indicators.

- Performance measurement will aim at informing the list of indicators that are part of the log frame matrix.
- In certain cases, mainly depending on when the monitoring exercise is launched, contribution to the outcomes will also be part of monitoring and for this to happen indicators defined during planning/programming at the outcome level will be the ones for which a value of measurement will need to be provided.
- In evaluation, the intervention logic will be the basis for the definition of the evaluation questions. Evaluations do mainly focus on the spheres of direct (outcomes) and indirect (impacts) influence. As such, indicators defined for these levels of the intervention logic will be used in evaluation. Depending on the specific purpose and scope of the evaluation exercise, additional indicators will be defined.

Monitoring is a management tool at the disposal of the action. It is expected to give regular and systemic information on where the Action is at any given time (and over time) relative to the different targets. Monitoring activities will aim to identify successes, problems and/or potential risks so that corrective measures are adopted in a timely fashion. Even though it is expected to focus mainly on the actions' inputs, activities and outputs, it is also expected to look at how the outputs can effectively induce, and actually induce, the outcomes that are aimed at.

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.

For component 1, the implementing partner 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 results (outputs and direct outcomes) as measured by corresponding indicators, using as reference the logframe matrix (for project modality) or the partner's strategy, policy or reform action plan list (for budget support). 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.

For component 2, the different responsibilities for this dual internal monitoring are the following:

i. The Council of Europe's monitoring will aim at collecting and analysing data to inform on progress towards planned results' achievement to feed decision-making processes at the action's management level and to report on the use of resources. To this aim, the Council of Europe shall establish a permanent internal, technical and financial monitoring system for the action and elaborate regular progress reports (at least twice a year) 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 results (outputs and direct outcomes) as measured by corresponding agreed indicators (and related targets), included in the logframe matrix (for project modality) or the list of result indicators (for budget support). 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. Reporting should not focus on

activities and inputs' use, unless it allows reporting on actual (and progress towards) results. The final report, narrative and financial, will cover the entire period of the action implementation.

ii. EU operational manager monitoring will aim at complementing implementing partners' monitoring, especially in key moments of the action cycle. It will also aim at ensuring a sound follow-up on external monitoring recommendations and at informing EU management. This monitoring could take different forms (meetings with the Council of Europe, action steering committees, on the spot checks), to be decided based on specific needs and resources at hand. Reporting will be done on the basis of checklists and synthesised in a monitoring note/report.

Both types of internal monitoring are meant to inform and provide support to external monitoring.

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 5.6.

SDGs indicators and, if applicable, any jointly agreed indicators as for instance per Joint Programming document should be taken into account.

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).

Beside the Results Oriented Monitoring (ROM) review, the Commission may undertake action results reporting through independent consultants recruited directly by the Commission (or recruited by the responsible agent contracted by the Commission for implementing such reviews). Their aim would be to identify and check the most relevant results on the action.

5.8 Evaluation

The Commission may, during implementation, decide to undertake an evaluation for duly justified reasons either on its own decision or on the initiative of the partner. Evaluation will give evidence of why intended changes are or are not being achieved.

Where relevant, the provisions of the Financial and Administrative Framework Agreement concluded between the European Union and the selected international organisations shall apply.

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

Having regard to the importance of the action, a final evaluation(s) 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 Commission shall inform the Council of Europe in advance of the dates foreseen for the evaluation missions. The Council of Europe 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 Council of Europe 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.

5.9 Audit

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 audits or expenditure verification assignments for one or several contracts or agreements.

Where relevant, the provisions of the Financial and Administrative Framework Agreement concluded between the European Union and the selected international organisations shall apply.

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

5.10 Communication and visibility

Communication and visibility of the EU is a legal obligation for all external actions funded by the EU.

This action shall contain communication and visibility measures which shall be based on a specific Communication and Visibility Plan of the Action, to be elaborated at the start of implementation.

In terms of legal obligations on communication and visibility, the measures shall be implemented by the Commission, the partner country (for instance, concerning the reforms supported through budget support), contractors, grant beneficiaries and/or entrusted entities. Appropriate contractual obligations shall be included in, respectively, the financing agreement, procurement and grant contracts, and delegation agreements.

The Communication and Visibility Requirements for European Union External Action (or any succeeding document) shall be used to establish the Communication and Visibility Plan of the Action and the appropriate contractual obligations. Additional Visibility Guidelines developed by the Commission (European Neighbourhood Policy and Enlargement Negotiations) will be strictly adhered to.

In particular, the Council of Europe will ensure adequate visibility of EU financing and of the results achieved. The Council of Europe will draft a communication and visibility plan containing communication objectives, target groups, communication tools to be used and an allocated communication budget.

Furthermore, key results will be communicated to all governmental, non-governmental and other stakeholders. All reports and publications produced will be widely disseminated. All activities will adhere to the European Union requirements for visibility on EU-funded activities. This shall include, but not be limited to, press releases and briefings, reports, seminars, workshops, events, publications.

Visibility and communication actions shall demonstrate how the interventions contribute to the agreed programme objectives. Actions shall be aimed at strengthening general public awareness of interventions financed by the EU and the objectives pursued. The actions shall aim at highlighting to the relevant target audiences the added value and impact of the EU's interventions. Visibility actions should also promote transparency and accountability on the use of funds.
With regards to the Neighbourhood East, all EU-supported actions shall be aimed at increasing the awareness level of the target audiences on the connections, the outcome, and the final practical benefits for citizens of EU assistance provided in the framework of this action. Visibility actions should also promote transparency and accountability on the use of funds.

Outreaching/awareness raising activities will play a crucial part in the implementation of the action. The implementation of the communication activities shall be the responsibility of the implementing organisations, and shall be funded from the amounts allocated to the action.

The implementing organisations shall report on its visibility and communication actions, as well as the results of the overall action to the relevant monitoring committees. This action will be communicated externally as part of a wider context of EU support to the country, where

relevant, and the EaP region in order to enhance the effectiveness of communication activities and to reduce fragmentation in the area of EU communication.

The implementing organisation shall coordinate all communication activities with EU Delegations as well as regional communication initiatives funded by the European Commission to the extent possible. All communication strategies developed as part of this action shall ensure they are in line with the priorities and objectives of regional communication initiatives supported by the European Commission, such as "EU4Digital" and in line with the relevant EU Delegation's communication strategy under the "EU4Country" umbrella initiative.

APPENDIX - INDICATIVE LOGFRAME MATRIX:[18]

The activities, the expected outputs and all the indicators, targets and baselines included in the logframe matrix are indicative and may be updated during the implementation of the action, no amendment being required to the financing decision. When it is not possible to determine the outputs of an action at formulation stage, intermediary outcomes should be presented and the outputs defined during inception of the overall programme and its components. The indicative logframe matrix will evolve during the lifetime of the action: new lines will be added for including the activities as well as new columns for intermediary targets (milestones) for the output and outcome indicators whenever it is relevant for monitoring and reporting purposes. Note also that indicators should be disaggregated by sex whenever relevant.

	Results chain	**Indicators**	**Baselines** (incl. reference year)	**Targets** (incl. reference year)	**Sources and means of verification**	**Assumptions**
Impact (Overall objective)	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.					*Not applicable*
Specific objective(s): Outcome(s)	Component 1: <u>Cybersecurity</u> 1. To strengthen the national cybersecurity governance and legal framework across the EaP countries 2. To strengthen the protection of critical information infrastructure in the EaP countries 3. To increase the operational capacities for cybersecurity incidents management in the EaP countries	1. Country position at ITU's Global Cybersecurity and Cyber-wellness Index 2. Country position at the CyberGreen Index 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. Level of involvement of civil society organisations in the	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)	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,	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/	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

[18] Mark indicators aligned with the relevant programming document mark with '*' and indicators aligned to the EU Results Framework with '**'.

		cybersecurity decision making processes.	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 each selected third country (2019)	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 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)	surveillance, freedom of expression online, access to content)	cybersecurity strategies and associated activities does not have an adverse impact on human rights in the target countries
Outputs	1.1 Strengthened regional and international cooperation on cybersecurity. 1.2 National cybersecurity strategies, relevant legal frameworks and implementation documents are developed and tailored in approximation with the EU NIS Directive 1.3 National frameworks and actor for the internal and external oversight	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	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	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.	- Project update reports - National reports from cyber-coordinating Ministries - ENISA reports - Press releases - National CERTs reports - Civil society reports	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

	of cybersecurity defined and reinforced. 1.4 Tailored approximation of the legal framework to the EU NIS 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 the development and implementation of cybersecurity policies and measures. 1.6 Increased cyber awareness (Cyber Hygiene) in all EaP partner countries proposed.	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. 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.	partner for each EaP Partner country at the inception phase. 5. 0 (2019) 6. 0 (2019)	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.	- Regional organisations' reports - National government reports - Press releases	right expertise for the roll out of activities. Translation and interpretation services for the roll out of activities do not create delays.
	2.1 Mapping of the critical information infrastructure in line with the EU NIS Directive. 2.2 Strengthened the management and mitigation of the cybersecurity risks posed to the critical information	1. Number of EaP Partner countries adopting Critical Information Infrastructure Protection policies. 2. Number of countries where the national incident response	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	

	infrastructure 2.3 Framework on managing and responding to major cybersecurity incidents relating to critical information infrastructures developed.	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			- Press releases - National CERTs reports - Civil society reports - Regional organisations' reports - National government reports - Press releases	
	3.1 National CSIRTs/CERTs designated and operational capacities for incidents management created and further strengthen taking into account the respective levels of readiness. 3.2 National cooperation between designated National CSIRTs/CERTs and owners of the critical information infrastructure on managing cybersecurity incidents improved. 3.3 Cooperation between designated National CSIRTs/CERTs in EaP partner countries increased. 3.4 Specific defined for CERTs in the EaP countries. 3.5 Increased international recognition and trust of CERTs in the EaP countries.	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	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

		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 international professional cyber associations.				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
Specific objective(s): Outcome(s)	Component 2: <u>Cybercrime</u> 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	- Number and quality of action plans or similar strategic documents.	- No specific action plans or strategies in Armenia, Azerbaijan	- Action plans or strategies in 5/6 countries.	Project reports.	Legislative amendments to be approved by Parliaments.

	cybercrime and electronic evidence developed. 1.2 Substantive criminal law, if necessary, in line with Articles 2 to 12 of 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.	- Number and quality of legislative amendments.	and Belarus. - Procedural law deficient in 4/6 countries.	- Draft legislative amendments in 5/6 countries approved by Governments.		
	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 cybercrime-related actions improved. 2.5 Reinforce mechanisms for cooperation and trust with the private sector and citizens	- 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.
	3.1 Skills, set up and competencies of the 24/7 points of contact further	- Number of cases handled by 24/7 contact points.	- 24/7 points of contact available in all countries, but limited	- Significant increase in cases handled by 24/7 points of	Project reports.	Sufficient trust by partner countries. Support to

	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.	- Number of cases where templates have been used. - Number of training events, official trained on police-to-police, and judicial cooperation.	use in practice in most countries (few cases handled per year). - No specific templates used for requests. - Limited skills for international cooperation in practice.	contact. - Templates used in practice. - Core staff for police-to-police and judicial cooperation trained in the six EaP countries.		participation in the T-CY and other relevant international events should facilitate this.

ANNEX I: OVERVIEW OF THE STATE OF APPROXIMATION TO THE EU LEGAL AND STRATEGIC FRAMEWORK – NAMELY, THE EU NIS DIRECTIVE

	NIS Directive	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Policy Department	- Policy Department unit (Art. 7)				X		X
	- Cybersecurity strategy (Art. 8)				X	X	X
Threat assessment unit	Art. 7, 9, 10		X	X	X		
International representation	Art. 11, 12, 15		X	X	X		X
Baseline security	- Baseline cybersecurity management unit (Art. 8)			X	X		X
	- Cybersecurity management standards (Art. 19)					X	
	- ICT Sysem accreditation (Art. 16)			X		X	X
	- ICT systems audit (Art. 15, 16, 17)			X		X	X
Critical infrastructure	- Definition in legislation (Art. 5)			X	X		
	- Protection unit with mandate to file […] (Art. 8)			X	X		X
	- Continuity requirements (Art. 14)			X	X		

CERT	- CERT unit (Art 9 and annex 1)		X	X	X	X	X
	- Art. 10, 14, 16, 20			X			X
	- Public private cooperation – PPPs (Art. 7 and annex 1)			X	X		
	- Legislation allowing exchange of information (59)			X	X	X	X
Crisis management	- Crisis management plan						
	- Cyber crisis excercise				X		

ANNEX II: OVERVIEW OF THE STATE OF IMPLEMENTATION OF THE BUDAPEST CONVENTION IN THE EASTERN PARTNERSHIP COUNTRIES

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Cybercrime strategies and action plans	No	No	No	Yes – as part of cybersecurity and organized crime strategies and action plan	Yes – as part of the National Programme on Cyber Security 2016-2020	Yes - as part of cybersecurity strategy, with yearly action plans since 2016
Procedural law	- No definitions of categories of data - No implementation of Articles 16, 17 and 18 BCC (search and seizure used as alterative); - Special powers for search and seizure (Art. 19 BCC) not implemented.	- No definitions of categories of data - No implementation of Art. 16 BCC (production order or search/seizure as alternative); - No implementation of Art. 17 BCC (general obligation of ISPs to cooperate); - Partial implementation of Art. 18 BCC (voluntary compliance); - Special powers for search and seizure (Art. 19 BCC) not implemented.	- No implementation of Art. 16 and 17 BCC (general data retention obligation used as alternative); - No implementation of Art. 18 BCC (general powers to receive documents); - Special powers for search and seizure (Art. 19 BCC) not implemented; - No judicial authorization for intrusive powers.	- No implementation of Art. 16 and 17 BCC (production orders used as alternative); - Special powers for search and seizure (Art. 19 BCC) not implemented.	- Partial implementation of Art. 16 BCC (applies only to ISPs); - Partial implementation of Art. 18 BCC (only provisions of Article 18.1.b); - Special powers for search and seizure (Art. 19 BCC) not implemented.	- No definitions of subscriber information and traffic data; - No implementation of Art. 16 BCC – production order or search/seizure as alternative; - No implementation of Art. 17 BCC; - No implementation of Art. 18 BCC – provisional access to objects and documents as alternative; - Special powers for search and seizure (Art. 19 BCC) not implemented; - Partial implementation of Art. 20 BCC – no definition of traffic data.
Operational cybercrime units	- Division for Combating High-Tech Crime under the General Department on	- Department of Combating Crimes in Communications and IT of the General Directorate of	- High-Tech Crime Department of the Ministry of Interior (Department "K")	- Cybercrime Division of the Central Criminal Police Department at the Ministry of Internal	- Centre for Combating Cybercrime at the National Inspectorate for Investigations of the General	- Cyber Police Department of the National Police under the Ministry of Interior

	Combating Organized Crime at the Police - Investigative Committee	Combating Organised Transnational Crimes at the State Security Service; - Ministry of the Interior (unit being set up)	- High-Tech Crime and Intellectual Property Department of the Investigative Committee	Affairs - Ministry of State Security	Inspectorate of Police of the Ministry of the Interior - Information Technology and Cyber Crime Investigation Section of the Prosecutor General's Office	- Department of counterintelligence protection of state's interests in sphere of information security of the State Security Service
Police-to-police cooperation units	- Division for Combating High-Tech Crime under the General Department on Combating Organized Crime at the Police	- Department of Combating Crimes in Communications and IT of the General Directorate of Combating Organised Transnational Crimes at the State Security Service	- High-Tech Crime Department of the Ministry of Interior (Department "K")	- Cybercrime Division of the Central Criminal Police Department at the Ministry of Internal Affairs	- Centre for Combating Cybercrime at the National Inspectorate for Investigations of the General Inspectorate of Police of the Ministry of the Interior - Information Technology and Cyber Crime Investigation Section of the Prosecutor General's Office	- Cyber Police Department of the National Police under the Ministry of Interior - The Department of counterintelligence protection of state's interests in sphere of information security of the Security Service of Ukraine
Authorities for judicial cooperation	- Department for International Cooperation and Legal Support at the Prosecutor General's Office (pre-trial); - Ministry of Justice, Department for International Legal Assistance (trial stage).	- International Relations Department of the Prosecutor General's Office (pre-trial); - Ministry of Justice (trial stage).	- International Legal Department of the Office of the Prosecutor General; - Other authorities specified on treaty basis; - Supreme Court (limited competence).	- International Cooperation Unit of the Department of Legal Affairs of the Office of the Chief Prosecutor at the Ministry of Justice	- Department for International Legal Assistance and European Integration at the Prosecutor General's Office (pre-trial) - International Legal Cooperation Division of the Ministry of Justice (trial stage)	- Department for International Legal Cooperation of the Prosecutor General's Office (pre-trial) - Division on Mutual Legal Assistance in Criminal Matters, International Legal Cooperation Department, Directorate for International Law, Ministry of Justice (trial stage)