Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Project proposal:

CyberEast+ on Enhanced action on cybercrime for cyber resilience in Eastern Partnership States

Version February 2024

Project title / number:	CyberEast+ joint project of the European Union and the Council of Europe on Enhanced action on cybercrime for cyber resilience in Eastern Partnership States
Project area:	Armenia, Azerbaijan, Georgia, Republic of Moldova, Ukraine[1]
Duration:	36 months (1 March 2024 – 28 February 2027)
Budget:	~EURO 3.9 million (EU 90%, COE 10%)
Funding:	European Union and the Council of Europe
Implementation:	Cybercrime Programme Office (C-PROC) of the Council of Europe

BACKGROUND AND JUSTIFICATION

Cybercrime and other offences involving electronic evidence remain major challenges for societies of Eastern Partnership region. The recent COVID-19 pandemic and ongoing security threats and armed conflicts in the region, in particular the aggression of Russia against Ukraine, contribute further to the deterioration of the security and crime situation. This is reflected in increasing cyberattacks, including against critical infrastructure, and other forms of cybercrime. Attacks against and by means of computers targeting or emanating from those countries have an impact on other geographical regions, including EU Member States.

The Russian aggression furthermore underlines once more the need for capacities to secure electronic evidence for use in criminal proceedings not only in relation to cybercrime or cyberattacks but in relation to any offence, including war crime.

Capacity building towards an effective response to the challenges of cybercrime and e-evidence remains highly relevant. Such capacity building on cybercrime needs to be closely linked to the area of cybersecurity. A combination of regional and country-specific measures within a common international framework should be pursued. Armenia, Azerbaijan, Georgia, Moldova and Ukraine are all Parties to the Budapest Convention on Cybercrime. They are thus also able to join and make use of the tools of the new Second Additional Protocol to this treaty on enhanced cooperation and disclosure of electronic evidence that was opened for signature in May 2022. By 9 March 2023, 36 countries had signed it (with one ratification), including Moldova and Ukraine.[2]

[1] Belarus participated in previous project activities until its suspension in August 2020. Should circumstances change, Belarus could be integrated again this project.

[2] The tools of this Protocol include: direct cooperation with service providers in other Parties for the disclosure of subscriber information and with registrars for domain name registration information; government-to-government cooperation for the production of subscriber information and traffic data; expedited disclosure of data and cooperation in emergencies; joint investigation teams and joint investigations; video conferencing. These tools are backed up by data protection and other safeguards that need to be implemented by Parties.

The European Union and the Council of Europe have supported countries of this region (Armenia, Azerbaijan, Georgia, Moldova and Ukraine)[3] through regional joint projects since 2011 within the Eastern Partnership framework.

Under the current CyberEast joint project (2019-2023), much progress was made in terms of legislation implementing the Budapest Convention on Cybercrime, enabling efficient regional and international cooperation, and improving public/private cooperation on cybercrime and electronic evidence in the Eastern Partnership region. This project also featured new themes on enhancing operational capacities of cybercrime units, increasing accountability, oversight and public visibility of action on cybercrime, as well as strengthening interagency cooperation on cybercrime and electronic evidence, by improving information sharing between Computer Security Incident Response Teams (CSIRTs) and criminal justice authorities. Following the onset of the Russian aggression in February 2022, support was provided to Ukraine through CyberEast without delay. The project concluded in December 2023 with adoption of the renewed Declaration on Strategic Priorities for Co-operation on Cybercrime in the Eastern Partnership Region.

A follow up joint project CyberEast+ is proposed to commence in 2024.

CyberEast+ will be aimed at ensuring a more effective criminal justice response to cybercrime and electronic evidence and increased cyber-resilience through a combination of regional actions and actions addressing the specific needs of each country.

While CyberEast+ will build upon or further consolidate achievements of the CyberEast project, the following themes will be added or receive stronger emphasis:

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

The project will be divided into four components (outcomes) on (1) policies and legislation; (2) capacities of criminal justice authorities; (3) enhanced cooperation on the basis of the Second Protocol to the Budapest Convention on Cybercrime, and (4) synergies between criminal justice and cybersecurity responses to cyberthreats. Targeted support to Ukraine will assist the efforts of national authorities in handling electronic evidence of war crimes and related offences through threat research, improvement of legal framework and delivery of specialised training and exercises.

The project management structure will be adjusted to the needs of project countries. While the CyberEast+ management team will again be based at the Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest, some staff may be located in Council of Europe offices in project countries to ensure greater efficiency and responsiveness to needs by counterpart organisations.

[3] And Belarus until August 2020.

OBJECTIVE, EXPECTED OUTPUTS AND ACTIVITIES

Project Objective/ Impact	**To enhance the capacities of Eastern Partnership countries for a more effective criminal justice response to cybercrime and electronic evidence and for increased cyber-resilience** The action will strengthen the criminal justice capacities of project countries on cybercrime and e-evidence in terms of legislation and policies, capacities for investigation, prosecution and adjudication as well as international and public/private cooperation, in line with the Budapest Convention on Cybercrime and its Second Protocol and in line with European Union priorities for the Eastern Partnership region.[4] Objectively verifiable indicators for this action will include: – Level of implementation of Budapest Convention and Second Protocol; – Availability of up-to-date regulatory and policy frameworks on cybercrime and electronic evidence; – Effectiveness of criminal investigations, prosecutions and adjudication of cases of cybercrime and e-evidence; – Availability of sustainable training on cybercrime and electronic evidence for criminal justice authorities; – Level of synergies between policies and measures on cybercrime and cybersecurity.
Outcome 1	**To support legislation and policy frameworks on cybercrime and electronic evidence and achieve stronger compliance with the Budapest Convention and its Second Protocol** Objectively verifiable indicators: – Number of ratifications of the Second Protocol by project countries; – Availability of cybercrime strategies or action plans (drafted/adopted) and extent to which existing cybercrime policy documents have been reviewed/updated or their effectiveness reviewed; – Reforms of legislation and regulations adopted or draft amendments available; – References to national research and studies reflected in policy/strategy documents; – Number of participants involved in discussions and activities.
Output 1.1	Regulatory framework for domestic investigations and international cooperation improved in line with the Budapest Convention and its Second Protocol
Activities	
	Support to legal reforms and review of applicable regulations implementing the provisions of the Second Additional Protocol to the Budapest Convention.
	Continued support to reforms of procedural law frameworks in line with Articles 16 to 21 Budapest Convention and related safeguards and conditions provided by Article 15 Budapest Convention.
	Ukraine: Further work with Ukrainian authorities to improve procedural powers, applicable safeguards and international cooperation in the context of investigating war crimes and gross human rights violations.

[4] EU Recovery, Resilience and Reform: Post-2020 Priorities for an Eastern Partnership that delivers for all https://euneighbourseast.eu/news/publications/recovery-resilience-and-reform-post-2020-priorities-for-an-eastern-partnership-that-delivers-for-all/

Output 1.2	Informed cybercrime policies or strategies supported
Activities	
	Contribution to updates of cybercrime strategies or action plans and review of their effectiveness through supporting research and meetings with stakeholders.
	Series of national studies of cybercrime threats, cybercrime victims, reporting, cybercrime offenders and criminal groups with involvement of national experts and academia/research institutions.
	Regional sessions with civil society stakeholders involved in cybersecurity, cybercrime, criminal justice and Internet governance matters through annual EuroDIG conferences.
	National discussions with service providers, personal data protection authorities, civil society and national communications regulators on responsible reporting and prevention of cyberviolence.
	Ukraine: Prepare and conduct an advanced study on cybercrime threats, criminal groups and trends specific to the context of armed aggression against Ukraine, with possible regional conclusions relevant for other countries of the region.
Outcome 2	**To reinforce capacities of criminal justice authorities through sustainable training frameworks, specialised training and practical exercises** Outcomes/objectively verifiable indicators: – Availability of courses and training plans at national training institutions. – Number of training sessions and participants trained. – Number of exercises held and participants engaged.
Output 2.1	Cybercrime and electronic evidence skills of law enforcement and judicial authorities kept up to date with continuous and specialised training
Activities	
	Setup, integration and delivery of intermediate and advanced cybercrime/e-evidence training programmes for investigators, prosecutors and judges through domestic training institutions, as required.
	Delivery and/or support of advanced training on specialized topics of cybercrime investigations, virtual currency investigations and digital forensics for national partners.
	Support delivery of cybercrime/e-evidence training to defence attorneys with the use of online HELP training courses in national languages.
	Ukraine: Develop and deliver training courses on malware/ransomware investigations, live data forensics, network forensics and investigations, energy sector/SCADA investigations, data preservation, use of OSINT tools and other relevant themes as requested by national partners.
Output 2.2	Improving advanced skills of cybercrime investigation and forensics through national and regional exercises
Activities	
	Yearly Regional Cybercrime Cooperation Exercises for law enforcement, prosecutors, forensic experts, CSIRTs and specialised investigators involving real-time competitive simulation exercises on cybercrime and cybersecurity.
	National or regional simulation exercises and/or mock trials on cybercrime investigations, digital forensics and interagency cooperation for relevant agencies/entities, in cooperation with other C-PROC projects where relevant.
	Delivery of courses on specialised cybercrime investigation and forensic tools, with gradual handover of software licenses for law enforcement partners in the region.

Outcome 3	**To enhance cooperation on the basis of the Second Protocol to the Budapest Convention** Objectively verifiable indicators: – Number of training sessions and participants trained. – Availability of guides, procedures or templates for the application of the provisions of the Second Protocol. – Decreased time for obtaining the disclosure of data across borders.
Output 3.1	Competent criminal justice authorities and 24/7 points of contact are able to apply the tools of the Second Protocol
Activities	
	Practical guides, procedures and templates, and domestic and regional training and exercise on articles 8 (giving effect to production orders), 9 (expedited disclosure in emergencies), 10 (emergency mutual assistance), 11 (video conferencing) and 12 (joint investigation teams and joint investigations) of the Second Protocol.
	Continued support to participation and networking in INTERPOL/EUROPOL/EUROJUST conferences, T-CY/Octopus, UN and other relevant events.
Output 3.2	Increased public/private cooperation across borders on the basis of the Second Protocol
Activities	
	Practical guides, procedures and templates, and domestic and regional training for competent authorities, service provides and registrars on the application of articles 6 (requests for domain name registration information) and 7 (production orders for subscriber information) of the Second Protocol.
	Support to national dialogue with key infrastructure and service providers on preventive reporting, preservation and production of data.
	Ukraine: Cooperation exercises with private sector actors (critical infrastructure and service providers) on the preservation, reporting and handling evidence of war crimes and related offences.
Outcome 4	**To reinforce synergies between criminal justice and cybersecurity responses to cyberthreats** Objectively verifiable indicators: – Extent of implementation of national standard operating procedures for CSIRT/criminal justice cooperation. – Availability of good practice studies and reports on trusted CSIRT/criminal justice cooperation.
Output 4.1	Reinforced mechanisms for trusted cooperation between cybersecurity institutions and criminal justice authorities
Activities	
	Support implementation of national cooperation principles, operative procedures and segregation of duties, developed and agreed under CyberEast project, through national fora involving cybersecurity experts and criminal justice authorities.
	Develop and deliver training sessions based on national standard operating procedures (SOPs) – developed with the support of the CyberSecurity East project – including simulation exercises on critical infrastructure attacks, ransomware attacks and other forms of cybercrime.

	Conduct national reviews on improvement and interoperability of cybercrime/cyber-incident reporting systems in project countries, upon request.
	Ukraine: Training on substantive law elements of the Budapest Convention supporting proper identification and qualification of attacks on civilian targets and critical infrastructure for criminal justice professionals and cybersecurity experts.

CONTACT

European Commission:

Martin MUEHLECK
Ukraine Service
Directorate-General for Neighbourhood
and Enlargement Negotiations (DG NEAR)
European Commission
ec.europa.eu

Council of Europe:

Giorgi JOKHADZE
CyberEast Project Manager
Giorgi.Jokhadze@coe.int

Cybercrime Programme Office of the
Council of Europe (C-PROC)
Bucharest, Romania
www.coe.int/cybercrime