Project CyberEast

Action on Cybercrime for Cyber Resilience in the Eastern Partnership region

Արևելյան Գործընկերություն
Східне партнерство
Eastern Partnership
აღმოსავლეთ პარტნიორობა
Parteneriatul Estic
Şərq tərəfdaşlığı
Partenariat Oriental

Summary and workplan

27 June 2019

Project title / number:	CyberEast - Action on Cybercrime for Cyber Resilience in the Eastern Partnership region (PMM 2088)
Project area:	Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, Ukraine
Duration:	36 months (20 June 2019 – 20 June 2022)
Budget:	EURO 4.222.222
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 cyber-enabled offences involving electronic evidence remain major challenges for societies of the EaP region. Likewise, attacks against and by means of computers emanating from those countries are of concern to other geographical areas including the EU Member States.

These crimes consist, *inter alia*, of the theft of personal data, fraud and other types of financial crime, distributed denial of service attacks or website defacements against media, civil society, individuals or public institutions, as well as attacks against critical infrastructure and others. In this regard, cooperation at all levels is essential.

Countries of the EaP have committed to implement the Budapest Convention on Cybercrime as a framework for domestic measures and for international cooperation on cybercrime and access to electronic evidence. All countries – with the exception of Belarus – are Parties to the Budapest Convention on Cybercrime and are thus members of the Cybercrime Convention Committee (T-CY).[1] It is therefore an international obligation for them to implement and comply with it.

Furthermore, the EaP countries adopted in October 2013 (Kyiv, Ukraine) a Declaration on Strategic Priorities for the Cooperation against Cybercrime in the EaP Region. 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.

The European Union and the Council of Europe supported Eastern Partnership countries between 2011 and 2014 through the CyberCrime@EaP I project. Two follow up projects, CyberCrime@EaP II and CyberCrime@EaP III, were launched in May and December 2015, with focus respectively on international cooperation and public-private partnerships on cybercrime and electronic evidence. CyberCrime@EaP 2018 project, launched in January 2018 as one-year extension Cybercrime@EaP II

[1] Belarus participates in the T-CY as ad-hoc observer and has expressed its commitment to implement this treaty.

and III projects, focused on the same subjects of international and public-private cooperation on cybercrime and electronic evidence.

The projects implemented helped the EaP countries mutual legal assistance and police cooperation authorities to significantly increase their capabilities to deal with the cybercrime and electronic evidence-related requests for cooperation; all cooperation authorities received international cooperation training tailored directly to their needs to increase and make uniform relevant skills and knowledge across the region; they are now able to utilize the tools developed with their own input during the project, such as the International Cooperation advanced information sections under the Octopus Cybercrime Community, international cooperation training materials developed under the project, and standard templates for Article 29-30 (data preservation) and Article 31 (MLA requests for subscriber information) requests under the Budapest Convention.

To launch and maintain public-private cooperation between the law enforcement and Internet service providers for efficient access to data, capacity building efforts focused on four necessary elements of public-private cooperation: clear regulatory framework; identified and engaged counterparts; voluntary compliance mechanisms; and efficient access to data beyond national jurisdictions. The project pursued strong focus on legislation, managing to engage five out of six EAP states in review of their procedural and related legislation - namely, introduction of less intrusive procedural powers required by the Budapest Convention on Cybercrime while ensuring compliance with safeguards and guarantees requirements under Article 15 of the treaty. To strengthen trust and engage partners, technical cybercrime exercises, contribution industry-driven international forums of discussion and bringing country teams into direct contact with multinational service providers was practiced. A number of regional studies on various aspects of cooperation support EaP countries in improving the public-private cooperation frameworks.

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. Improving trust is an overriding theme for the project.

- Need to improve the operational capacities of specialised cybercrime units.

- Addressing and reducing conflicts of competence; and strengthening interagency, international and public/partnership cooperation.

- Sharing of relevant data held by Computer Security Incident Response Teams (CSIRTs) on incidents and attacks with all concerned authorities. This information sharing may be most valuable to law enforcement and judicial authorities for follow-up investigation and prosecution purposes. Without this cooperation, it is difficult to determine the scale and trends of cybercrime and threats to cybersecurity and thus to inform cybercrime and cybersecurity strategies in this region.

Thus, further capacity building efforts are necessary to remedy these problems in the region.

APPROACH

CyberEast project is a direct follow-up to previous capacity building efforts in the Eastern Partnership and continues to build upon similar themes – strong legislative framework implementing the Budapest Convention on Cybercrime, enabling efficient regional and international cooperation, and improving public/private cooperation regarding cybercrime and electronic evidence in the Eastern Partnership region. However, the project also features new and strong focus on enhancing the 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, in particular by improving information sharing between Computer Security Incident Response Teams (CSIRTs) on incidents and attacks with all concerned authorities.

Immediate Outcome 1 of the project aims at adoption and further improvement of legislative and policy frameworks compliant to the Budapest Convention as well as rerlated standards, such as Istanbul and Lanzarote Conventions. The Outputs under this Outcome focus on the development of national action plans or similar strategic documents regarding the criminal justice response to cybercrime and electronic evidence; revision and improvement of substantive criminal law (where necessary) in line with Articles 2 to 12 of the Budapest Convention with additional focus on Istanbul and Lanzarote Conventions; and improvement of procedural law for the purposes of domestic investigations in line with Articles 16 to 21 of the Budapest Convention. Human rights and rule of law approach is ensured, primarily but not exclusively, by supporting reform of regulatory framework on the basis of updated Study on Article 15 Safeguards in the Eastern Partnership region.

Immediate Outcome 2 of the project seeks to reinforce the capacities of judicial and law enforcement authorities and interagency cooperation, seeking to encompass all criminal justice stakeholders in the EaP countries into coherent, sustainable and skills-oriented experience sharing and training framework. To achieve this, the Outputs under this Outcome aim at strengthening skills and institutional setup of operational cybercrime units in law enforcement authorities, as well as improving interagency cooperation of relevant law enforcement and criminal justice authorities, agencies and bodies including through improved data sharing. Being a new and administratively complex element of the project different from previous activities in scope and reach, an inception period will be allocated at the beginning of the project to assess and plan action under this Outcome accordingly.

Immediate Outcome 3 of the Project pursues the increase of efficient international cooperation and trust on criminal justice, cybercrime and electronic evidence, as well as trust between criminal justice and private entities. As a continuation of the previous capacity building efforts in the EaP on international and public/private cooperation, the Outputs under this outcome strive to further strengthen skills, set up and competencies of the 24/7 points of contact, putting in place guidelines and procedures for mutual legal assistance and data requests, strengthening operational skills for international judicial and police authorities cooperation on cybercrime, and implementing existing agreements on public/private cooperation while concluding such agreements in the remaining countries. This Outcome overall seeks to increase the capacity of state authorities, tasked with cooperation in criminal cases, to effectively handle increased workload and complexity of cases related to cybercrime and electronic evidence. Human rights and rule of law component is addressed through continued public-private dialogue, work with ISP regulators and data protection authorities, and review of cybercrime reporting systems in terms of their focus on citizens' security.

The project will be managed by the Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania by the project team involving a core group of project staff from previous Cybercrime@EaP projects, aided by two new staff members (second Senior Project Officer and a Communications Officer) responding to increased scope and volume of the project.

OBJECTIVE, EXPECTED OUTPUTS AND ACTIVITIES

Project Objective/ Impact	**To increase and enhance the cyber-resilience and criminal justice capacities of the Eastern Partnership countries to better address the challenges of cyber threats and improve their overall security.** The action will strengthen criminal justice capacities of Eastern Partnership countries on cybercrime and electronic 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 the EU 20 Deliverables for 2020. Overall outcomes/objectively verifiable indicators for this action will include: – Level of implementation of Budapest Convention in terms of substantive law and procedural powers into national laws; – Revised and adopted strategies and action plans related to cybercrime; – Stronger and operational specialized cybercrime units; – Better interagency cooperation and information sharing; – Improved civic participation, oversight and visibility of action on cybercrime; – International cooperation on cybercrime and electronic evidence improved; – Public-private partnerships between law enforcement / private sector are in place.	
Result/ Outcome 1	**To adopt legislative and policy frameworks compliant to the Budapest Convention and related instruments.** Outcomes/objectively verifiable indicators: – Availability of cybercrime strategies or action plans (drafted/adopted) and extent to which existing cybercrime policy documents have been reviewed/updated; – Level of compliance with all three regulatory pillars (substantive, procedural and international cooperation) of the Budapest Convention and with relevant provisions of the Lanzarote and Istanbul Conventions. – Reforms of criminal procedure laws completed, draft amendments available. – Level of reforms implemented for the regulatory framework to address issues of Article 15 Budapest Convention.	
Output 1.1	**National action plans or similar strategic documents regarding criminal justice response to cybercrime and electronic evidence developed.**	
Activities		
	High-level Regional Meeting of criminal justice authorities, policy makers and members of Parliament to assess key issues and design action plans of legislative reform in the EaP countries, prepared on basis of background research and policy documents.	Autumn 2020[2]
	Support to EaP countries in the preparation of country reports on cybercrime and cybersecurity trends and threats in cooperation with Europol and contribution to the yearly iOCTA report.	2020-2022
	Contribution to development/update of cybercrime strategies or action plans through national discussion forums, advisory missions and discussions at regional meetings (where necessary), involving national policy makers and MPs, aiming to increase visibility and transparency of strategic process on cybercrime.	2019-2022

[2] All dates indicated are preliminary and subject to approval of the project Steering Committee.

Output 1.2	**Substantive criminal law, if necessary, in line with Articles 2 to 12 of the Budapest Convention and selected provisions of the Istanbul and Lanzarote Conventions revised and improved.**	
Activities		
	Assessment of compliance with substantive law provisions of Articles 2 to 12 of the Budapest Convention on Cybercrime as well as Articles 18 to 23 of the Lanzarote Convention and Articles 34 (Stalking) and 40 (Sexual harassment) of the Istanbul Convention.	Spring 2020
	Support to reforms of substantive law frameworks in line with Articles 2 to 12 of the Budapest Convention on Cybercrime as well as Articles 18 to 23 of the Lanzarote Convention and Articles 34 (Stalking) and 40 (Sexual harassment) of the Istanbul Convention, where necessary.	2020-2022
Output 1.3	**Procedural law for the purposes of domestic investigations in line with Articles 16 to 21 of the Budapest Convention improved.**	
Activities		
	Continued support to reforms of procedural law frameworks in line with Articles 16 to 21 Budapest Convention and related legislation through national seminars and workshops, and regional Working Groups of experts (including national experts), based on needs and requests of EaP states, and with particular view of possible adoption of Protocol II to the Convention.	2019-2022
	Further advice and reform of regulatory framework in line with findings of the updated Study on Article 15 Safeguards in the Eastern Partnership region as a pre-requisite for application of procedural powers under Articles 16 to 21 Budapest Convention.	2019-2022
Result/ Outcome 2	**To reinforce the capacities of judicial and law enforcement authorities and interagency cooperation.** Outcomes/objectively verifiable indicators: – Extent to which the capacities and competencies of cybercrime units (law enforcement and criminal justice authorities) are improved; – Availability of training plans; – Number of training and simulation exercises and participants trained; – Availability of procedures on CERTs/CSIRT – law enforcement cooperation on data sharing; – Extent to which the capacities of data protection and oversight mechanisms exist; – Cybercrime-centric public communication campaign on-going; – Availability of procedures and practices serving to assure trust with general public and private entities.	
Output 2.1	**Skills and institutional setup of operational cybercrime units in law enforcement authorities' and judicial authorities dealing with cybercrime and electronic evidence strengthened.**	
Activities		
	Assessment of EaP countries institutional setup, capacities, competencies, training needs as well as interagency cooperation gaps and opportunities for cybercrime units in the Eastern Partnership region, with regional report.	Sepetmber-October 2019

	National seminars/advisory missions to update and/or develop training plans for cybercrime and electronic evidence and to include into the curricula with a view to establishing sustainable knowledge sharing and training frameworks at criminal justice training institutions.	2019-2020
	Design and delivery of revised first responder courses for the EaP.	2020-2021
	Design and delivery of introductory judicial training courses for the EaP.	2020-2021
	Design and delivery of advanced judicial training courses for the EaP.	2021-2022
	Participation in Cybercrime Masters Programme at established academic institution by supporting enrolment of specialized cybercrime investigators from the EaP.	2019-2022
Output 2.2	**Improvement of interagency cooperation of the relevant law enforcement and criminal justice authorities, agencies and bodies including through improved data sharing.**	
Activities		
	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.	2020
	Support to cooperation forums and meetings for networking between cybercrime and cybersecurity professional communities.	2019-2022
	Support to national cyber exercises on the basis of cybercrime/cybersecurity institutions.	2019-2022
	Yearly Regional Cyber exercises to improve interaction between CSIRTs and law enforcement agencies in real-time environment.	2019-2022
	Case simulation exercises and mock trials on cybercrime investigations (specific topics, such as virtual currencies/Darknet, etc.) and digital forensics for relevant agencies/entities, with major focus on ECTEG materials and in possible cooperation with other C-PROC projects.	2020-2022
	"Effective access to data" Programme: training section on open-source incident and crime reporting systems that can be set up between industry and CSIRT/CERT/law enforcement (including incident handling on the basis of the EU NIS Directive); training on open-source image creation and copying toolkits that would help less intrusion into the regular business process; training on basic parameters and use of hardware/software for retention and access to traffic data, including ideas for shared management for distributed storage systems and public configuration protocols.	2020-2022
	In-country workshops, with elements of training and interagency cooperation exercises (where requested and necessary) for cybercrime units, economic crime units, financial investigators, FIUs and specialised prosecutors on virtual currencies, Darknet and similar topics focusing on public-private cooperation.	2020-2022

Output 2.3	**Internal and external accountability and oversight including role of civil society organisations reinforced.**	
Activities		
	Organize and support workshops/sessions on liaising with civil society organisations involved in cybersecurity, cybercrime, criminal justice and Internet governance through annual EuroDIG conferences.	2019-2022
	Organise meetings between criminal justice authorities, civil society and the private sector in view of enhanced transparency of law enforcement action on cybercrime and electronic evidence.	2019-2022
	Prepare an assessment on data protection in the law enforcement sector in EaP countries.	2020
	Cooperate with personal data protection authorities and national communications regulators to increase their role in ensuring trust and cooperation between public and private sector in terms of access to data in criminal cases.	2020-2022
Output 2.4	**Improved public communication and transparency on cybercrime actions.**	
Activities		
	Cybercrime-centric public communication campaign jointly organized with local counterparts and donors on the occasion of important national and, where possible, at regional/international events under the project.	2019-2022
Output 2.5	**Reinforce mechanisms for trusted cooperation between the private sector, citizens and criminal justice authorities.**	
Activities		
	Direct support to organization of national and regional Internet industry and technology events in EaP countries with focus on increasing trust between the public, the state and the private sector in ensuring security of cyberspace.	2019-2022
	Discussion roundtables on cybercrime/e-evidence aspects with defence attorneys, with a view to ensuring further participation in project activities (e.g. mock trials).	2020-2022
	Assessment of efficiency of cybercrime reporting systems (both public and industry-based) through in-country visits and advisory missions, with experience sourced from other capacity building projects run by the Council of Europe, with regional conclusions	Late 2020
Result/ Outcome 3	**To increase efficient international cooperation and trust on criminal justice, cybercrime and electronic evidence, including between service providers and law enforcement.** Outcomes/objectively verifiable indicators: – Number of requests handled by 24/7 contact points; – Time needed for processing MLA requests related to cybercrime/e-evidence; – Number of cases where templates have been used; – Number of training events and participants trained; – Availability of cooperation agreements concluded and extent to which the existing ones have been revised.	

Output 3.1	**Skills, set up and competencies of the 24/7 points of contact further strengthened.**	
Activities		
	National, regional and international workshops, trainings and hands-on simulations for improvement of the skills, set-up and competencies of 24/7 points of contact.	2020-2022
	Regional/international case simulation exercises developing skills for international cooperation on cybercrime and electronic evidence for judicial and police cooperation authorities, focusing also on multinational service providers (MSPs), using and testing their platforms for cooperation.	February 2020
Output 3.2	**Guidelines and procedures for mutual legal assistance and data requests in place.**	
Activities		
	Development of standard step-by-step guidelines for drafting and processing of mutual legal assistance requests for criminal cases involving cybercrime and electronic evidence; adoption of guidelines in a regional meeting.	2020
	National training sessions for cybercrime units and prosecutors on the use of templates for international requests for data preservation and subscriber information.	2010-2021
	Continued support to reforms of procedural law frameworks and related legislation through national seminars and workshops, based on needs and requests of EaP states, and with particular view of possible adoption of II Additional Protocol to the Convention.	2019-2022
Output 3.3	**Operational skills for international judicial and police authorities cooperation on cybercrime strengthened.**	
Activities		
	Continued support for participation at INTERPOL/Europol conferences, T-CY/Octopus, Pompidou Group, Eurojust and other relevant events (including UN sessions).	2019-2022
	Continued support to development of cooperation tools through maintenance of the online resource on international cooperation.	2019-2022
	Support to organization or participation in operational meetings for the EaP law enforcement for high-profile cases involving the EU states and/or EaP countries (on request and where necessary).	2020-2022
Output 3.4	**Implementation of existing agreements on public/private cooperation and conclusion of such agreements in the remaining countries.**	
Activities		
	Further support, building on previous Cybercrime@EaP projects, to the revision, update and/or conclusion of cooperation agreements between the law enforcement and Internet service providers through national workshops.	2019-2022
	Continued support to public-private dialogue on cooperation through maintenance of the dedicated online resource.	2019-2022
	National workshops for development of standard templates and procedures for access to data held by private sector entities, with additional focus on multinational/foreign service providers and	2020-2021

	direct channels of cooperation.	
	Training to support implementation of data request templates through case studies and simulation exercises (national or regional level).	2020-2022

CONTACT

Giorgi.Jokhadze@coe.int
Cybercrime Programme Office
of the Council of Europe (C-PROC)

www.coe.int/cybercrime