Cybercrime@EAP 2018
International cooperation
Public/private cooperation

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

Summary and workplan

Updated version 6 September 2018

Project title / number:	PGG 2018: Cybercrime@EAP (2018/DGI/JP/PMM 1963)
Project area:	Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, Ukraine
Duration:	12 months (1 January – 31 December 2018)
Budget:	EURO 980,000
Funding:	European Union and Council of Europe Partnership for Good Governance for the Eastern Partnership countries
Implementation:	Cybercrime Programme Office (C-PROC) of the Council of Europe

BACKGROUND AND JUSTIFICATION

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. 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).

Despite progress achieved under these two projects, the Report on "*Cybercrime strategies, procedural powers and specialised institutions in the Eastern Partnership region – state of play*", prepared under the Cybercrime@Eastern Partnership projects in June 2017, has noted that further improvements are required in the region concerning:

1. *Strategic approaches and policies on cybercrime and electronic evidence*: There is a lack of strategic approach to countering cybercrime and making use of electronic evidence in criminal proceedings. Criminal justice systems lack resources and capacities to prevent, investigate, prosecute and adjudicate not only cybercrime but the growing number of other offences involving electronic evidence – that is, lacking resources and capacities in terms of fully-fledged, operational cybercrime units in law enforcement authorities.

2. *Procedural law powers on cybercrime and electronic evidence (major gaps in implementation of Budapest Convention in this respect):* Criminal justice authorities need the powers to secure electronic evidence to investigate cybercrime and other offences entailing electronic evidence to bring offenders to justice and maintain the rule of law also in cyberspace. The procedural powers of the Budapest Convention remain to be fully implemented in most of the countries of the Eastern Partnership, which are important preconditions for domestic investigations involving electronic evidence but also for international and public-private cooperation.

3. *Division of competencies between security services and criminal police*: Some EAP states have both security service and regular police/Ministry of the Interior units designated as investigative authorities for cybercrime, sometimes with competing and unclear divisions of powers or investigative jurisdiction. Cybercrime investigative powers are often divided between the police units and special

investigative agencies that operate beyond police/Ministry of the Interior structures. These instances of uncertainty contribute directly to lack of efficiency expected of fully-fledged, operational cybercrime units in law enforcement authorities.

4. *Problems in international cooperation due to gaps in domestic procedural law:* There are obvious gaps in legal regulations as well as practice of preservation, definitions of subscriber information vs. traffic data; incoming or outgoing international preservation requests (Article 29 Budapest Convention) are often not followed by mutual legal assistance requests for the production of data; moreover, there are often no formal modalities for informing States requesting preservation of a necessity of mutual legal assistance request. This contributes delays and inefficiency of international cooperation on cybercrime and electronic evidence;

5. *Cooperation with multi-national service providers:* Direct contact with foreign or multinational service providers is an increasingly important option for all Eastern Partnership States, both for police cooperation units and mutual legal assistance authorities. Proper legal regulation is essential for this process, since foreign/multinational service providers do mostly cooperate on a voluntary basis and lack of clear and proper basis in national law could be one of the major reasons influencing this important aspect of public-private cooperation.

APPROACH

CyberCrime@EAP 2018 project is a direct follow-up to the previous capacity building efforts in the Eastern Partnership and continues to focus on the same subjects - enabling efficient regional and international co-operation on cybercrime and electronic evidence, and improving public/private cooperation regarding cybercrime and electronic evidence in the Eastern Partnership region. It will be managed by the Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania.

The project will continue to contribute both to improving regional and international co-operation on cybercrime and electronic evidence (Result/Outcome 1) as well as step up effort to improve public/private cooperation regarding cybercrime and electronic evidence in the Eastern Partnership region (Result/Outcome 2).

The project will engage both mutual legal assistance authorities and 24/7 points of contact in international, regional and country-specific activities that increase their skills for handling international cooperation requests, and will also contribute to better regulatory/legal environment for international cooperation to function.

The public-private cooperation element will be further reinforced by region-wide studies on Cybercrime Strategies and Threats, by engaging identified project counterparts and partners into training and exercises with focus on cooperation aspects, and by continuing efforts to improve procedural legislation and to conclude/update the cooperation agreements between the state authorities and internet service providers.

For both dimensions of the project, further support and development of tools and resources of cooperation, maintained by the Council of Europe, will be offered.

OBJECTIVE, EXPECTED OUTPUTS AND ACTIVITIES

Project Objective/ Impact	**Criminal justice authorities in countries participating in the Eastern Partnership are able to enforce stronger action on cybercrime and electronic evidence on the basis of the Budapest Convention on Cybercrime.** This will contribute to relevant EU 2020 Milestones, that is, full implementation of the

	Budapest Convention, particularly as per procedural law for the purpose of domestic investigations, public-private cooperation and international cooperation, and fully-fledged, operational cybercrime units in law enforcement authorities created. Outcomes/objectively verifiable indicators: – Implementation of Budapest Convention in terms of procedural powers into national laws; – International cooperation on cybercrime and electronic evidence improved; – Public-private partnerships between law enforcement and private sector are in place; – Specialized cybercrime units are operational.	
Result/Outcome 1	**To enable efficient regional and international co-operation on cybercrime and electronic evidence.** Outcomes/objectively verifiable indicators: – The number of mutual legal assistance requests on cybercrime and electronic evidence sent/received will have increased in the six countries by month 12; – The number of requests sent/received by 24/7 points of contact will have increased in the six countries by month 12; – Draft amendments to procedures and rules on mutual legal assistance on cybercrime and electronic evidence are available by month 12 in the six countries.	
Output 1	**Authorities responsible for mutual legal assistance have their capacities enhanced with regard to cybercrime and electronic evidence.**	
Activities		
1.1	Meeting with Eurojust on international cooperation	7-8 March, the Hague
1.2	Contribution to UN Intergovernmental Expert Group on Cybercrime	3-5 April, Vienna, Austria
1.3	Fourth Regional meeting on Improving international cooperation on cybercrime in the Eastern Partnership region (MLA and 24/7 working groups)	3-4 May, Kyiv, Ukraine
1.4	Participation at UN Commission on Crime Prevention and Criminal Justice (CCPCJ)	14-18 May, Vienna, Austria
1.5	Participation in Cybercrime Convention Committee (T-CY) and Octopus conference for sharing experience and reinforcing cooperation with the authorities of other States.	9-13 July, Strasbourg 27-29 November, Strasbourg
1.6	Participation in Underground Economy Conference (organized by iPROCEEDS project)	4-7 September, Strasbourg
1.7	In-country workshops/Table top exercises on interagency cooperation in the context of international cooperation on cybercrime and electronic evidence (Armenia, Azerbaijan, Belarus, Georgia and Ukraine)	September-October 2018
1.8	Introductory judicial training with focus on international cooperation	13-15 November 2018, Kyiv, Ukraine
1.9	Regional Conference on Cybercrime Strategies, combined with Final meeting on Improving international cooperation on cybercrime in the Eastern Partnership region – Closing conference of the project	11-13 December, Tbilisi, Georgia
Output 2	**The effectiveness of 24/7 points of contact is enhanced.**	

Activities		
2.1	Attendance at Pompidou Group Annual Meeting on Cybercrime	18-19 April, Dublin, Ireland
2.2	Fourth Regional meeting on improving international cooperation on cybercrime in the Eastern Partnership region (MLA and 24/7 working groups)	3-4 May, Kyiv, Ukraine
2.3	Joint training of 24/7 points of contact and other designated points of contact from investigative agencies with the use of ECTEG materials (Armenia, Belarus, Moldova)	1-5 October 2018, Yerevan, Armenia
2.4	Joint training of 24/7 points of contact and other designated points of contact from investigative agencies with the use of ECTEG materials (Azerbaijan, Georgia, Ukraine)	22-26 October, Baku, Azerbaijan
2.5	Participation in Cybercrime Convention Committee (T-CY) and Octopus conference for sharing experience and reinforcing cooperation with the authorities of other States.	9-13 July, Strasbourg 27-29 November, Strasbourg
2.6	Participation in Underground Economy Conference (organized by iPROCEEDS project)	4-7 September, Strasbourg
2.7	Participation in Europol-INTERPOL Annual Cybercrime Conference 2018	18-20 September, Singapore
2.8	Regional Conference on Cybercrime Strategies, combined with Final meeting on Improving international cooperation on cybercrime in the Eastern Partnership region – Closing conference of the project	11-13 December, Tbilisi, Georgia
Output 3	**Draft amendments to rules and procedures on mutual legal assistance will be available for adoption.**	
Activities		
3.1	Advisory mission on regulations and functions of 24/7 point of contact	25-26 April, Yerevan, Armenia
3.2	Advisory mission on international cooperation by use of 24/7 point of contact and mutual legal assistance	19-21 June, Baku, Azerbaijan
3.3	Advisory mission on international cooperation by use of 24/7 point of contact and mutual legal assistance	6-8 November, Kyiv, Ukraine
Result/Outcome 2	**To improve public/private cooperation regarding cybercrime and electronic evidence in the Eastern Partnership region.** Outcomes/objectively verifiable indicators: – Criminal justice authorities and major service providers participate in a regional process of public/private cooperation. – Specific partnerships or agreements have been established in at least four of the six EAP countries. – An online resource on public/private cooperation data is available and contributes to transparency on criminal justice access to data. – Reforms of criminal procedure laws will have been completed in at least two of the countries and draft amendments are available in others.	
Output 4	**A structured process of public/private co-operation on cybercrime underway and agreements concluded.**	
Activities		
4.1	Initiate and conduct study of cybercrime and cybersecurity trends in	February-

	the EAP, support countries in the preparation of country reports (on request), and prepare a regional report on the subject	December 2018, all EaP countries
4.2	In-country workshops to discuss cooperation between CSIRT, law enforcement and private sector from the perspective of cybersecurity strategies	February-May 2018, all EaP countries
4.3	In-country workshops in each EAP country to expand, complete and maintain the online tool on public/private cooperation - combined with National Cybercrime Cooperation Forums	February-May 2018, all EaP countries
4.4	International Cybercrime Cooperation Exercise for law enforcement / CSIRT / private sector communication protocols	27-30 March 2018, Chisinau, Moldova
4.5	Contribution to Cyber Security Festival	20 April, Tbilisi, Georgia
4.6	Participation and contribution to EuroDIG 2018 – focus on criminal justice action in cyberspace / combined with Project Planning meeting and Steering Committee	4-6 June, Tbilisi, Georgia
4.7	Workshop on practical aspects of CSIRT/LEA cooperation, combined with advisory visit to CERT.GOV.UA and SSU technical division	24-26 September, Kyiv, Ukraine
4.8	Support to national forums of discussion: contribution to Youth IGF 2018 and IGF-UA 2018	27-28 September, Kyiv, Ukraine
4.9	Support to national forums of discussion: contribution to OSCE Conference on Terrorism in Digital Age, section on public-private cooperation	9-10 October, Minsk, Belarus
4.10	Support to national forums of discussion: contribution to Regional Cyber Week & Expo 2018 in Moldova	29 October – 2 November, Chisinau, Moldova
4.10	Support to national forums of discussion: contribution to Georgian IT Innovations Conference 2018 with participation of project country team of Armenia	15-16 November, Tbilisi, Georgia
4.11	Support to national forums of discussion: contribution to IGF Azerbaijan during BakuTEL Expro 2018	6-7 December, Baku, Azerbaijan
4.12	Regional Conference on Cybercrime Strategies, combined with Final meeting on improving public/private cooperation on cybercrime in the Eastern Partnership region	11-13 December, Tbilisi, Georgia
Output 5	**Criminal procedure law strengthened.**	
Activities		
5.1	Workshop on legal and technical aspects of LEA/ISP cooperation	26-27 February 2018, Chisinau, Moldova

CONTACT

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

www.coe.int/cybercrime