Project Cybercrime@EAP III
Public/private cooperation

Արեւելյան Գործընկերություն
Східне партнерство Eastern
Partnership აღმოსავლეთ
პარტნიორობა Parteneriatul Estic
Şərq tərəfdaşlığı Parteneriat
Oriental Усходняе Партнёрства

Project summary

Update

Project title / number:	Cybercrime@EAP III (2015/DGI/JP/3608)
Project area:	Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova, Ukraine
Duration:	25 months (1 December 2015 – 31 December 2017)
Budget:	EURO 1,200,000
Funding:	European Union and Council of Europe Partnership for Good Governance (formerly Programmatic Cooperation Framework for 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. A follow up project, CyberCrime@EAP II, was launched in May 2015 with a focus on international cooperation 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).

The project CyberCrime@EAP III will be aimed at promoting public/private cooperation. It will follow up to CyberCrime@EAP I and complement the CyberCrime@EAP II project which will be carried out in parallel. It will furthermore support EAP countries in the implementation of recommendations of the T-CY.

Cooperation between criminal justice authorities and private sector entities, including in particular service providers, is essential to protect society against crime, as underlined by the European Court of Human Rights in the case of K.U. versus Finland. Such cooperation concerns primarily access by police and prosecution services to data held by service providers for criminal justice purposes, but also the sharing of information and experience, as well as training.

In 2008, the Council of Europe's Octopus Conference adopted a set of "Guidelines for the cooperation between law enforcement and internet service providers in the investigation of cybercrime". These were subsequently supported in the EU Council Conclusions on a concerted work strategy and practical measures against cybercrime of November 2008. The Guidelines helped shape public/private cooperation regarding cybercrime and electronic evidence in a number of countries. Within the Eastern Partnership region one of such examples is Georgia, where the Guidelines were used as a template for public-private Memorandum of Cooperation on Cybercrime concluded in 2010.

Partnership for Good Governance

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

In recent years, the question of public/private cooperation and specifically the issue of criminal justice access to data has become more complex. Reasons include that:

– cybercrime is increasing and involving more data, devices, platforms, persons, providers and States;
– data are increasingly held by cloud service providers in foreign or unknown or multiple jurisdictions;
– the questions of cybercrime and of cybersecurity are increasingly intertwined;
– reports on mass surveillance and other national security activities undermine public confidence and trust, and, in consequence, more stringent data protection standards are put in place also with respect to criminal investigations.

There is a pressing need to reconcile the obligation of governments to protect society and individuals against crime while respecting the principles of rule of law and protecting the privacy , freedom of expression and all human rights of individuals.

This is also true for countries participating in the Eastern Partnership. Often, local and multinational service providers are reluctant to cooperate, criminal justice measures and national security measures are not clearly separated, there is lack of transparency and re-dress mechanisms, and public trust is limited. Moreover, law enforcement powers such as those foreseen in the Budapest Convention on Cybercrime are not always clearly defined in criminal procedure law, and this adversely affects law enforcement/service provider cooperation as well as human rights and the rule of law.

During CyberCrime@EAP I, Eastern Partnership countries concluded that public/private cooperation in particular with regard to access to electronic evidence for criminal justice purposes was a strategic priority.

This was reconfirmed during the launching event of the CyberCrime@EAP II project in September 2015. Public/private cooperation at domestic levels is a pre-condition for effective international cooperation. International mutual legal assistance requests on cybercrime as well as requests for data preservation through 24/7 points of contact require the cooperation of service providers. In Eastern Partnership countries this is considered to be one of the main obstacles to international cooperation and the ability of governments to counter the threat of cybercrime in line with rule of law and human rights requirements.

APPROACH

The present project will address these issues. It will be managed hand in hand with the CyberCrime@EAP II project by the Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania.

The project will commence with an inventory and analysis of public/private initiatives already underway in EAP countries (Result 1). This phase of the project will not only help document good practices as well weaknesses and problems encountered but also identify private sector stakeholders and engage them in the project.

The project will subsequently support a process of public/private cooperation (Result 2). It will initially focus on the cooperation between law enforcement and Internet service providers as well as social media platforms as this is the most pressing concern. It is expected that over time other stakeholders will become involved such as the financial sector, business associations and computer emergency response teams (CERTs).

Activities will include:

– International/regional meetings between criminal justice authorities, service providers and other stakeholders in order to share information and experience, strengthen rule of law and human rights safeguards and to promote confidence and trust.

- Workshops, training events and advice at national levels in order to support the conclusion of cooperation agreements between criminal justice authorities and service providers.
- The creation of an online resource (on policies and transparency reports of private sector entities, relevant legislation, good practices available, training opportunities, initiatives already underway, etc.)

The project will furthermore support reforms of the criminal procedure law (Result 3). It is essential that law enforcement powers to order data preservation or the production of data or other measures that interfere with the rights of individuals are clearly defined by law and follow international standards; otherwise private sector entities – including multi-national service providers – may not be prepared to cooperate.

The project will support a process of public/private cooperation that on the one hand should produce concrete deliverables during the lifetime of the project. On the other hand, such a process will be open-ended. Therefore, the feasibility of continuing the activities of the project as a platform hosted by the Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest should be assessed. This would help ensure the sustainability of project results.

The mandate of C-PROC includes establishing partnerships with public and private sector organisations. The specific scope, membership and management structure would need to be discussed in more detail in the course of the project. It could start as an initiative for the Eastern Partnership region but could then expand to cover other countries and regions.

OBJECTIVE, EXPECTED RESULTS AND ACTIVITIES

Project objective	**To improve public/private cooperation regarding cybercrime and electronic evidence in the Eastern Partnership region.** Outcome 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. –	
Result 1	**Analysis of current initiatives, challenges and opportunities regarding public/private cooperation in the Eastern Partnership region available.** Indicator: By month 7, a study is available that is mapping current strengths, weaknesses, opportunities and risks regarding public/private and specifically law enforcement/service provider cooperation in the Eastern Partnership region and that documents good practices and initiatives already underway.	
Activities:		
1.1	Organise a regional meeting of criminal justice authorities, telecommunications regulators and major service providers to initiate the project and identify key issues as well as current initiatives regarding public/private cooperation in the Eastern Partnership region. This (and other) meetings are to ensure the engagement of stakeholders through a participatory process.	6-7 April, Kiev, Ukraine

1.2	Prepare the study.	Study visits: 30 March - 1 April 2016 - Ukraine 13-15 April 2016 - Armenia 18-20 April 2016 - Azerbaijan 21-23 April 2016 - Georgia 10-12 May 2016 - Belarus 16-18 May 2016 - Moldova June 2016: study report produced
1.3	Update the study by the end of 2017.	Follow-up visits (2.5 day visits): Oct 2017 Armenia Nov 2017 Georgia Nov 2017 Azerbaijan Nov 2017 Belarus Nov 2017 Moldova Nov 2017 Ukraine December 2017: updated report produced
1.4	Research paper on strategy of communication and cooperation with multinational service providers	January-March 2017
1.5	Study on the liability of Internet service providers in the EAP region	June-September 2017
Result 2	**A structured process of public/private cooperation on cybercrime underway and agreements concluded.** Indicator: By month 25, criminal justice authorities of the six EAP countries and service providers will have participated in a structured process of public/private cooperation through a combination of regional and country-specific meetings. Specific agreements will have been concluded in at least four of the six EAP countries. An online resource is maintained by the Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania to service this process, to improve transparency and thus public confidence, and to link up existing initiatives. The feasibility of transforming this process into a more permanent platform in order to sustain the process will have been established.	
Activities:		
2.1	Organise 3 regional meetings of criminal justice authorities, major service providers, regulators and other stakeholders to address specific problems of cooperation and carry out training and simulation exercises.	
	2.1.1 Belarus: Regional Meeting on LEA/ISP Cooperation Platform	19-21 September 2016
	2.1.2 Georgia: Regional coordination and partnership exercise involving a wide array of stakeholders (possibly in cooperation with GLACY+ or i-Proceeds)	24-28 April 2017
	2.1.3 Regional meeting: Meeting with multinational service providers in Ireland	24-25 November 2016
2.2	Organise country-level workshops for criminal justice authorities and service providers in	

	order to promote cooperation agreements.	
	2.2.1 Armenia: Workshop on best models in the EU and other states for public-private cooperation	7-8 November 2016
	2.2.2 Azerbaijan: Workshop on cooperation between the law enforcement and ISPs, focusing on preservation	12-14 October 2016
	2.2.3 Belarus: Public-private partnerships in sector-specific approach (banking etc.)	9-11 Jan 2017
	2.2.4 Georgia: Solutions for improved sharing of subscriber information (possibly combine with annual GITI Conference and Cyber Security Forum)	9-11 November 2016
	2.2.5 Moldova: Workshop on crime and incident reporting framework including national CERT	6-7 October 2016
	2.2.6 Ukraine: Communication and information sharing with local ISPs	18-20 Jan 2017
2.3	Establish an online resource to share information on public/private cooperation and to enhance transparency.	
2.4	Evaluate the possibility of establishing a public/private cooperation platform to sustain the process of cooperation.	
2.5	Participation in GLACY+ joint training for prosecution central authorities and cybercrime units on obtaining electronic evidence from foreign jurisdictions and mutual legal assistance issues combined with International workshops on cooperation with Internet service providers	INTERPOL (Singapore), 27 Feb-1 March 2017
2.6	Training of the law enforcement and project counterparts (including private sector) in the policies and practices of direct cooperation with multinational service providers – combined with CEAP II trainings on international cooperation 9-10 February - Armenia 23-24 February – Georgia 16-17 March – Azerbaijan 23-24 March - Belarus 30 March – 1 April – Moldova 6-7 April - Ukraine	
2.7	Participation in GLACY+ International workshop for cybercrime units and law enforcement training institutions on training strategies (technical level) and access to ECTEG training materials (4 members of each country team)	Europol (the Hague), May 2017
2.8	Participation in international event on European Dialogue on Internet Governance in Estonia	June 2017
2.9	International event: Public-private cooperation conference in cooperation with International Cyber Investigation Training Academy	Bulgaria, October 2017
Result 3	**Criminal procedure law strengthened.** Indicator: By month 25, procedural law reforms will have been completed in at least two countries. Proposals for reforms in additional countries will be available.	
Activities:		
3.1	Organise a regional meeting to review the status of criminal procedure law and of reforms underway.	
	Moldova: Regional Meeting on safeguards and guarantees in the context of cybercrime procedures and public-private cooperation	11-12 Sept 2017
3.2	Provide advice to domestic working groups in view of accelerating the completion of reforms of criminal procedure laws including conditions and safeguards.	
	3.2.1 Armenia: Workshop on amendments to the Criminal Code and Criminal Procedure Code (cybercrime and electronic evidence)	3-5 May 2017
	3.2.2 Azerbaijan: Workshop on Law reform around the topics of	10-12 May 2017

	cybercrime procedures and public-private cooperation	
	3.2.3 Belarus: Workshop on legal and practical aspects of CERT cooperation	July 2017
	3.2.4 Georgia: Workshop on Law reform around the topics of cybercrime procedures and public-private cooperation	16-17 February 2017
	3.2.5 Moldova: Workshop on Law reform around the topics of cybercrime procedures and public-private cooperation)	14 September 2017
	3.2.6 Ukraine: Workshop on Law reform around the topics of cybercrime procedures and public-private cooperation	6-7 April 2017
	3.2.7 Ukraine: Public hearings of the legal amendments	17-19 May 2017
	3.2.8 Ukraine: Seminar on memorandum of cooperation: agreement of principles and finalization of text	7-8 Septembers 2017
	3.2.9 Ukraine: Seminar on memorandum of cooperation: visibility at Internet industry event	5-6 October 2017
3.3	Review conditions and safeguards in law and practice and prepare an update of the study on Article 15 safeguards in EAP countries (October 2013). (updated as a results of visits under p 1.3 on Mapping Study update)	

CONTACT
Alexander Seger
Head of Cybercrime Division, Council of Europe
alexander.seger@coe.int

www.coe.int/cybercrime

Programmatic Cooperation Framework for
Armenia, Azerbaijan, Georgia, Republic of Moldova, Ukraine and Belarus

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