

## Council of Europe/EU PGG Annual Plan of Action 2018: Criminal Justice Action on Cybercrime

<b>Theme</b> <b>Thematic programme</b> <b>Priority Area</b>	
<b>Project title</b>	Cybercrime@Eastern Partnership II (international cooperation) Cybercrime@Eastern Partnership III (public/private cooperation)
<b>Geographical focus</b>	Eastern Partnership region: Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine
<b>Beneficiaries /Partners</b>	Country project teams established by official nominations through PCF/PGG coordinators Criminal justice authorities National communications regulatory authorities Personal data protection authorities Internet service providers (including international providers) Cyber security experts
<b>Contact Person (Council of Europe)</b>	Alexander SEGER
<b>Start - End dates of the project (including inception)</b>	Between 1 January 2018 and 31 December 2018
<b>Relevance for Council of Europe Action Plan and priorities</b>	<a href="#">Armenia 2015-2018</a> <a href="#">Azerbaijan 2014-2016</a> <a href="#">Georgia 2013-2015</a> <a href="#">Georgia 2016-2019</a> <a href="#">Republic of Moldova 2013-2016</a> <a href="#">Republic of Moldova 2017-2020</a> <a href="#">Ukraine 2015-2017</a>
<b>Relevance for the EU strategic documents including 2020 Deliverables</b>	<b>12- Resilience and civilian security:</b> - Budapest Convention fully implemented, particularly as per procedural law for the purpose of domestic investigations, public-private cooperation and international cooperation. - Fully-fledged, operational cybercrime units in law enforcement authorities created.  In this respect, Report on “ <i>Cybercrime strategies, procedural powers and specialised institutions in the Eastern Partnership region – state of play</i> ”, prepared under the Cybercrime@Eastern Partnership projects in June 2017, has noted that further improvements are required in the region concerning:

	<p>1. <i>Strategic approaches and policies on cybercrime and electronic evidence:</i> There is a lack of strategic approaches to countering cybercrime and making use of electronic evidence in criminal proceedings, as reflected in the absence of dedicated policy documents on cybercrime and electronic evidence as mainstream challenges of criminal justice systems. Even where cybercrime-related provisions are found in strategies or action plans, they are placed within an overall framework of organized crime strategies or cybersecurity documents. This hardly addresses the problem of cybercrime as a major criminal justice challenge. In consequence, 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 resource and capacities in terms of <b>fully-fledged, operational cybercrime units in law enforcement authorities</b>.</p> <p>2. <i>Procedural law powers on cybercrime and electronic evidence (major gaps in implementation of Budapest Convention in this respect):</i> 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. As such powers interfere with the rights of individuals, they need to be clearly defined by law. Articles 16 to 21 Budapest Convention provide an accepted international guideline. Against this background, the procedural powers of the Budapest Convention remain to be fully implemented in most of the countries of the Eastern Partnership. While some of the States address more procedural powers in their <b>national legal frameworks</b> than the others, none follow the sequence of the progressive application of these powers as required by Convention – not necessarily in terms of chronology, but also in terms of gradually applicable safeguards and guarantees, which are important preconditions for <b>domestic investigations</b> involving electronic evidence.</p> <p>3. <i>Division of competencies between security services and criminal police:</i> Recurring problem for the Eastern Partnership remains the division of competences between various agencies competent to investigate cybercrime. 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. Beyond the reasons of efficiency and coordination, with cybercrime becoming an increasingly mainstream matter of criminal justice systems, security services do not have sufficient resources or even enough rationale to be dealing with day-to-day investigations of cybercrime offences</p>
--	--

– and, moreover, of traditional offences involving electronic evidence - that should be performed by regular investigative units of the police. In some of EAP jurisdictions, the investigative powers are divided between the police units and special investigative agencies that operate beyond police/Ministry of the Interior structures. While this is primarily a regulatory and policy choice, lack of clarity remains as to the division of competencies between “preliminary” and “full” investigations performed by police forces and investigative agencies respectively. At the same time, responsibilities for international police-to-police cooperation are retained at police units rather than fully-fledged investigators who should be more competent in terms of receiving and processing such requests and have a full suite of procedural powers available to them. 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 - data preservation provisions of the Budapest Convention are not properly implemented in majority of the Eastern Partnership States, and general powers for production, search and seizure are used instead. In some of the Eastern Partnership States, subscriber information is considered to be a part of traffic data and is treated as such, thus making it difficult to obtain it without a court order. 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. Normally, there are no national regulations that expressly prohibit such practice and outgoing requests are usually sent to large multinational providers (primarily social networks and mail services) that would have set up specialized channels or departments for cooperation with law enforcement. **Proper legal regulation is essential** for this process, as foreign/multinational service providers do cooperate on a voluntary basis, where lack of clear and proper basis in national law could be

	one of the major reasons for declining this important aspect of <b>public-private cooperation</b> .
--	---

## 1. State of Play

The two Cybercrime@EAP projects - Cybercrime@Eastern Partnership II (international cooperation) and Cybercrime@Eastern Partnership III (public/private cooperation) contributed to the following:

### International cooperation

- Study on the international cooperation in the EAP was completed at the beginning of the project and used for planning of activities to target challenges identified;
- Increased number of mutual legal assistance requests (data to be confirmed through questionnaires at end 2017);
- Increased number of requests sent/received by 24/7 points of contact (data to be confirmed through questionnaires at end 2017);
- Draft amendments to procedures/rules on MLA in all six countries: process ongoing in five EAP states to reform procedural legislation in line with Budapest Convention.

### Public-private cooperation

- Study on mapping current strengths, weaknesses, opportunities and risks regarding public/private cooperation is completed and will be revised and expanded by end 2017 for future reference;
- Six EAP countries and service providers participated in a structured process of public/private cooperation through regional & country-specific meetings, such as regional project meetings, first ever cyber exercise, national sessions/meetings in all EAP states and attendance of various international events;
- Specific agreements will have been concluded in at least four of the six EAP countries: so far only two EAP states have such memorandum in place, while another one is working on the text to be adopted;
- An online resource on public-private cooperation is established, launched online and verified with project teams;
- The feasibility of transforming the process into a more permanent platform in order to sustain the process will have been established: is scheduled as a study of the EAP states by the end of the project in November 2017;
- Procedural law reforms will have been completed in at least two countries: only one country of the EAP has undergone full parliamentary process to adopt legislative changes. Proposals for reforms in additional countries will be available: is achieved in other 4 EAP jurisdictions where such drafts are being discussed.

A detailed report on “Cybercrime strategies, procedural powers and specialised institutions in the Eastern Partnership region – state of play” has been prepared under the Cybercrime@EAP projects. The draft was shared with the European Commission, discussed with Eastern Partnership countries in a workshop in Tallinn, Estonia, on 5 June 2017, and presented at the 1st meeting of the Eastern Partnership Rule of Law Panel in Brussels on 15-16 June 2017. The report states that while much progress has been made, for example, in terms of operational cybercrime units, bodies for international cooperation or ratification of the Budapest Convention, **further improvements** are required with respect to:

- Strategic approaches and policies on cybercrime and electronic evidence;

- Procedural law powers on cybercrime and electronic evidence (major gaps in implementation of Budapest Convention in this respect);
- Division of competencies between security services and criminal police;
- Problems in international cooperation due to gaps in domestic procedural law;
- Cooperation with multi-national service providers.

## 2. Intervention logic

OVERALL OBJECTIVE(s) [Impact]	OBJECTIVELY VERIFIABLE INDICATORS	BASELINE (VALUE & YEAR)	TARGET (VALUE AND YEAR)	SOURCES OF VERIFICATION	Risks and Assumptions
<p>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.</p> <p>This will contribute to the 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.</p>	<ul style="list-style-type: none"> <li>- Implementation of Budapest Convention in terms of procedural powers into national laws;</li> <li>- International cooperation on cybercrime and electronic evidence improved;</li> <li>- Public-private partnerships between law enforcement and private sector are in place;</li> <li>- Specialized cybercrime units are operational.</li> </ul>	<p><b>International cooperation:</b></p> <ul style="list-style-type: none"> <li>- The EAP countries' authorities responsible for mutual legal assistance have better skills and tools (manual, online resources) for international co-operation on cybercrime and electronic evidence. It is assumed that this will lead to a measurable increase in MLA requests already by the end of the project;</li> <li>- The role of 24/7 points of contact has been strengthened in the six EAP countries. It is assumed that this will lead to a measurable increase in the number of requests sent/received by 24/7 points of contact;</li> <li>- Recommendations for amendments to procedures and rules on mutual legal assistance on cybercrime and electronic evidence are available for the six EAP countries. It is assumed that adoption and implementation of these recommendations will enhance the effectiveness of international co-operation in these matters in the longer term.</li> </ul> <p><b>Public-private cooperation:</b></p> <ul style="list-style-type: none"> <li>- Criminal justice authorities and major service providers participate in a regional process of public/private co-operation;</li> <li>- Specific partnerships or agreements have been established in at least four of the six EAP countries;</li> </ul>	<p><b>As this is a regional project focusing on international co-operation, it is expected all countries participate in all activities. A risk is that not all countries will be prepared to participate in activities depending on the location. Mitigation: regional activities will be organised in locations that are acceptable to all.</b></p> <p><b>The success of the action will depend on a buy-in by the private sector. Mitigation: some key private sector entities will be</b></p>		

		- An online resource on public/private co-operation 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.			contacted at an early stage to ensure their participation so that others will follow. The benefits of the project to the private sector will need to be underlined.
SPECIFIC OBJECTIVE(s) [Outcome]	OBJECTIVELY VERIFIABLE INDICATORS (name of indicator)	BASELINE (VALUE & YEAR)	TARGET (VALUE AND YEAR)	SOURCES OF VERIFICATION	ASSUMPTIONS
1. To enable efficient regional and international co-operation on cybercrime and electronic evidence.	1.1. The number of mutual legal assistance requests on cybercrime and electronic evidence sent/received will have increased in the six countries by month 12.	1.1. Requests sent / received by individual countries – 2017	1.1. Increased numbers of request sent or received by individual countries – 2018	1.1. Report on International cooperation in the EAP/questionnaires	The study and its report rely on correct data provided by the EAP country teams
	1.2. The number of requests sent/received by 24/7 points of contact will have increased in the six countries by month 12.	1.2. Requests sent / received by individual countries – 2017	1.2. Increased numbers of request sent or received by individual countries – 2018	1.2. Report on International cooperation in the EAP/questionnaires	The study and its report rely on correct data provided by the EAP country teams
	1.3. Draft amendments to procedures and rules on mutual legal assistance on cybercrime and electronic evidence are available by month 12 in the six countries.	1.3. Reforms of procedural law initiated and supported by project in 5 EAP	1.3. Support continued to EAP countries to progress further in legal development - 2018	1.3. In-country and regional events focusing on legislative reform	Project counterparts have readiness to pursue with legislative reforms necessary

<b>2. To improve public/private cooperation regarding cybercrime and electronic evidence in the Eastern Partnership region.</b>		countries – 2017			
	2.1 Criminal justice authorities and major service providers participate in a regional process of public/private cooperation.	2.1. Dedicated regional and in-country discussions on the subject is initiated through project activities - 2017	2.1 Combination of regional and country-specific meetings with involvement of the major stakeholders - 2018	2.1 Reports of the meetings	Project country teams and counterparts take direct part in regional and in-country activities of the project; Project counterparts understand the need for such cooperation
	2.2 Specific partnerships or agreements have been established in at least four of the six EAP countries.	2.2. Only two EAP countries have an agreement - 2017	2.2 Four EAP country concluded agreements – 2018	2.2 Text of agreements and reports of events supporting them	Participation in national and regional activities; Basic legal framework for procedural powers is in place; Parties to the dialogue agree to resolve their differences through written agreements

	2.3 An online resource on public/private cooperation data is available and contributes to transparency on criminal justice access to data.	2.3. Online resource on international and public/private cooperation is established - 2017	2.3 Online resource remains operational and is updated with all the relevant information– 2018	2.3 Online resource on public-private cooperation at the Octopus Cybercrime Community website	The submissions by the country teams and other counterparts provide complete, accurate and up-to-date data
	2.4 Reforms of criminal procedure laws will have been completed in at least two of the countries and draft amendments are available in others.	2.4. Two EAP countries commit legal reforms into Parliamentary stage, while four others discuss the drafts through combination of regional and country-specific meetings – 2017	2.4 Support continued to EAP countries to progress further in legal development - 2018	2.4 Legal drafts, reports of the meetings, adopted legislation and assessments	Project counterparts understand the key nature of legal regulation for public-private cooperation; Willingness of counterparts to engaged in legislative process
<b>OUTPUTS</b>	<b>OBJECTIVELY VERIFIABLE INDICATORS</b>	<b>BASELINE (VALUE &amp; YEAR)</b>	<b>TARGET (VALUE AND YEAR)</b>	<b>SOURCES OF VERIFICATION</b>	<b>ASSUMPTIONS</b>



<b>Output 1</b> Authorities responsible for mutual legal assistance have their capacities enhanced with regard to cybercrime and electronic evidence.	1. Further development of online tools and resources with regard to EAP countries.	1. Online resource for international cooperation online – 2017	1. MLA authorities continue to maintain online resource; national meetings on interagency cooperation – 2018	1. Online resource on international cooperation at the Octopus Cybercrime Community site; Reports of in-country meetings	1. Online resource for international cooperation stays operational; Project teams engage in in-country meetings on interagency cooperation.
	2. Use of cooperation templates for BCC Article 29/30 and Article 31 requests.	2. Draft cooperation templates approved at international meetings – 2017	2. Cooperation templates are used in real-life cases for Art. 29/30 and Article 31 requests; Participation in international exercise on the subject - 2018	2. Reporting to project team on the successful use of cooperation templates; Report of international exercise	2. The 24/7 units and mutual legal assistance authorities participate in relevant meetings and exercises; Cooperation templates are accepted as valid documents for processing requests.
<b>Output 2</b> The effectiveness of 24/7 points of contact is enhanced	1. Training and support to networking of 24/7 points of contact.	1. 24/7 points of contact attending and receiving training at international events – 2017	1. 24/7 points of contact receiving targeted regional training; continued attendance at international events – 2018	1. Reports of national, regional and international activities on the subject	1. 24/7 points of contact officers take part in planned activities

	2. Additional regulations on the powers of 24/7 points of contact where necessary.	2. No specific regulation's on 24/7 points of contact in EAP countries – 2017	2. In-country advisory missions on international cooperation between law enforcement to facilitate execution of the mutual legal assistance	2. Reports of in-country workshops; regulations adopted where deemed necessary	2. Country teams engaged in discussions at planned events; Willingness to undertake regulatory drafting where necessary
<b>Output 3</b> Draft amendments to rules and procedures on mutual legal assistance will be available for adoption	1. Completion of reforms of procedural law as basis for domestic investigations and international cooperation.	1. Reforms of procedural law initiated and supported by project in 5 EAP countries – 2017	1. Support continued to EAP countries to progress further in legal development - 2018	1. Legal drafts, reports of the meetings, adopted legislation and assessments	1. Willingness of counterparts to continue to be engaged in legislative process
	2. Related regulations including division of competencies between authorities.	2. No clear regulation on division of competences for domestic investigations and international cooperation in two EAP states – 2017	2. National seminars and meetings on regulations for international cooperation in line with applicable and emerging standards - 2018	2. Drafts of regulations or assessment of existing setups, reports of the seminars/meetings	2. Participation in planned national meetings; Readiness to follow up with adopting necessary regulations; Agreement between investigative agencies in question to delineate competencies
<b>Output 4</b> A structured process of public/private co-operation on cybercrime underway and agreements concluded.	1. Promoting strategic and multi-stakeholder approaches to cybercrime and electronic evidence and assessment of state of play against strategic priorities adopted in Kyiv in October 2014.	1. Cybercrime and cybersecurity strategies not available in 4 EAP countries	1. Study of cybercrime and security trends in states in question; production of	1. Reports of national, regional and international activities on the subject	1. Readiness of country team to engage into report preparation; participation at national, regional and

		– 2017	national and regional reports; in-country workshops to discuss cooperation between CSIRT, law enforcement and private sector; International Conference on Cybercrime Strategies to address decision makers – 2018		international activities on the subject
	2. Cooperation agreements and arrangements between law enforcement and domestic providers as well as multinational service providers.	2. Only two EAP countries have cooperation agreements in force – 2017	2. Facilitate further dialogue through National Cybercrime Cooperation Forums; participation in Regional exercise on communications protocols; Participation and contribution to EuroDIG 2018 – 2018	2. Reports of national, regional and international activities on the subject	2. Participation in national and regional activities; Legal framework for procedural powers in place; Parties to the dialogue agree to resolve their differences through written agreements

	3. Follow up to recommendations of the T-CY Cloud Evidence Group in Eastern Partnership countries.	3. The major guiding documents and studies have been produced by the T-CY – 2017	3. To be discussed through National Cybercrime Cooperation Forums and at Regional meetings under the project – 2018	3. Reports of national and regional activities on the subject	3. Participation of country teams and counterparts in national and regional events on the subject
	4. Enhance use of cooperation tools and platform by EAP countries.	4. Online resource for international cooperation online – 2017	4. In-country workshops in each EAP country to expand, complete and maintain the online tool on public/private cooperation – 2018	4. Reports of workshops; public-private cooperation resource at Octopus Cybercrime Community	4. Readiness of the country teams to take full ownership of the public-private cooperation resource; Information available on the resource is of practical use for both parties (state and private entities)
<b>Output 5</b> Criminal procedure law strengthened.	Completion of reforms of procedural law as basis for domestic investigations and public/private cooperation.	Reforms of procedural law initiated and supported by project in 5 EAP countries – 2017	Support continued to EAP countries to progress further in legal development – 2018	Legal drafts, reports of the meetings, adopted legislation and assessments	Willingness of counterparts to continue to be engaged in legislative process

### 3. Activities

Activities	2018											
	1	2	3	4	5	6	7	8	9	10	11	12
<b>Output 1: Authorities responsible for mutual legal assistance have their capacities enhanced with regard to cybercrime and electronic evidence.</b>												
1.1 Fourth Regional meeting on Improving international cooperation on cybercrime in the Eastern Partnership region (MLA and 24/7 working groups)					3-4 May, Kyiv							
1.2 In-country workshops on interagency cooperation in the context of international cooperation on cybercrime and electronic evidence (Armenia, Azerbaijan, Belarus, Georgia and Ukraine)				17-20 April, Yerevan 24-27 April, Tbilisi 29 May -1 June, Kyiv	15-18 May, Baku 22 -25 May, Minsk							
1.3 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	
1.4 Participation in Underground Economy Conference (organized by iPROCEEDS project)									4-7 September, Strasbourg			
1.5 Final meeting on Improving international cooperation on cybercrime in the Eastern Partnership region (MLA and 24/7 working groups) – Closing conference of the project												12-14 December, TBD
<b>Output 2: The effectiveness of 24/7 points of contact is enhanced.</b>												
2.1 Fourth Regional meeting on improving international cooperation on cybercrime in the Eastern Partnership region (MLA						3-4 May 2018						

[illegible]

standards, including relevant T-CY recommendations <sup>1</sup>		2018, Yerevan (TBC)										
<b>Output 4: A structured process of public/private co-operation on cybercrime underway and agreements concluded.</b>												
4.1 Initiate and conduct study of cybercrime and cybersecurity trends in the EAP, support countries in the preparation of country reports (on request), and prepare a regional report on the subject (to be published at Activity 4.8 below)	15-31 January: Methodology (C-PROC)			Review of data, initial report, C-PROC	Review of data, initial report, C- PROC	Follow- up missions on request, EAP	Follow-up missions on request, EAP		Production of final reports, C- PROC	Production of final reports, C- PROC		
4.2 In-country workshops to discuss cooperation between CSIRT, law enforcement and private sector from the perspective of cybersecurity strategies (all EAP countries)		6-8 February, Yerevan  13-15 February, Baku  20-22 February, Tbilisi	26 February – 2 March, Chisinau  13–15 March, Minsk  20-22 March, Kyiv									
4.3 Cybercrime Cooperation Exercise for law enforcement / CSIRT/private sector communication protocols			27–30 March, Chisinau									
4.4 Prepare terms of reference for National Cybercrime Cooperation Forums					7-11 May, C- PROC							
4.5 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						
4.6 National Cybercrime Cooperation Forums with participation of law enforcement and Internet industry in each EAP country									11-14 September, Yerevan  18-21 September, Baku	2-5 October, Minsk  9-12 October, Tbilisi	6-9 November, Chisinau  13-16 November, Kyiv	
4.7 In-country workshops in each EAP country to expand, complete and maintain the online tool on		8 February, Yerevan	2 March, Chisinau  15									

<sup>1</sup> Two potential activities envisaged, based on country request and/or necessity, following the needs of on-going or planned legal reforms on the subject.

public/private cooperation - combined with National Cybercrime Cooperation Forums		15 February, Baku 22 February, Tbilisi	March, Minsk 22 March, Kyiv									
4.8 International Conference on Cybercrime Strategies: in cooperation with GLACY+, iPROCEEDS and Cyber@South projects										1-2 November, Bucharest		
4.9 Final meeting on improving public/private cooperation on cybercrime in the Eastern Partnership region – closing conference of the project.												4-6 December, TBD
<b>Output 5: Criminal procedure law strengthened.</b>												
5.1 National seminars and meetings to complete the reforms of national procedural law <sup>2</sup>		26-27 February, Chisinau										

<sup>2</sup> Three potential meetings envisaged, based on country request and/or necessity, following the needs of on-going or planned legal reforms on the subject.