Partnership for Good Governance

FINAL NARRATIVE REPORT ON PCF/PGG PROJECT IMPLEMENTATION[1]

I. PROJECT DATA

Project title: Criminal Justice action on Cybercrime - Cybercrime@EAP III: Public/Private Co-operation / PGG 2018: Cybercrime@EaP: International and Public/Private Cooperation on Cybercrime and Electronic Evidence in the Eastern Partnership region (*extension*)

Project type: Regional

Target country(ies): Armenia, Azerbaijan, Belarus, Georgia, Republic of Moldova and Ukraine

Project duration: 37 months (1 December 2015 – 31 December 2018)

National partners: Country project teams established by official nominations through PCF/PGG coordinators of six EAP countries; criminal justice authorities (prosecutors, investigators, security services investigating cybercrime); authorities in charge of legislative reforms; national communications regulatory authorities; personal data protection authorities; Internet service providers (including international providers); cyber security agencies and experts

Final beneficiaries and/or target groups[2] (if different): *same as above*

Project manager(s): Giorgi JOKHADZE

Project managers' supervisor(s): Alexander SEGER

[1] Please be concise and analytical. The report should not exceed 8 pages, including 1 page for overall assessment.

[2] "Target groups" are the groups/entities who are directly positively affected by the project and "final beneficiaries" are those who will benefit from the project in the long term.

II. OVERALL ASSESSMENT

In line with expected results under the Cybercrime@EAP III project and continued with Cybercrime@EAP 2018 - identifying challenges to public-private cooperation, enabling a structured process of such cooperation and strengthening of criminal procedure law - the project country teams brought together policy makers/law drafters, criminal justice authorities and communications regulatory authorities, with extension of funding of the project in 2017 allowing also to take onboard representatives of personal data protection community, cyber security experts and Internet industry representatives. The country teams are instrumental to the project: they are the main source of information for the project regarding both challenges and opportunities to improve public-private cooperation, and are, at the same time, parties who develop and maintain such partnerships.

Due to limited information about the state of public-private cooperation, the project, with the support of the country teams, completed several studies on the subject, ranging from state-of-play reports to more complex studies on legal and practical aspects of cooperation, such as legal frameworks, necessary safeguards, cybercrime threats, strategies/policies and others. Findings of these reports were used to plan, inform and deliver activities under the project.

Despite common heritage as to legal systems and practices, each of the countries of the region has unique approach to public-private cooperation and thus requires an individualized approach. This is attested by a number of specific requests beyond the initially agreed work-plan for activities, requesting project to support specific topics or events. This makes achieving one of the main specific outcomes of the project – structured process of public/private cooperation on cybercrime with agreements concluded – a rather challenging task in the context of regional project.

Nevertheless, the project addressed this by focusing on four necessary elements of public-private cooperation, as agreed by the project countries: clear regulatory framework; identified and engaged counterparts; voluntary compliance mechanisms; and efficient access to data beyond national jurisdictions. And to strengthen regional approach, more involved and interactive experiences were offered to the country teams, such as Regional cybercrime cooperation exercises (becoming a trademark of the project), ensuring attendance and contribution to industry-driven international forums and exercises, or by bringing country teams into direct contact with multinational service providers to discuss direct cooperation channels.

The ultimate goal of public-private partnerships on cybercrime and electronic evidence is to ensure effective access by the law enforcement to data held by private entities - mostly Internet service providers – in the context of criminal investigations. Such access, which more often than not requires some degree of intrusion into privacy of individuals, requires clear legal basis to do so; the project thus 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; in Ukraine, the number of activities aimed to introduce new legislation and develop a memorandum of cooperation resulted in separate track of 8 events in 2016 and 2017 designed specifically for that country.

Facilitating adoption of clear legislation based on the Budapest Convention and engaging local service providers in the process of discussion regarding development of law is in itself a trust-

building exercise, with trust being a key element in successful public-private partnerships. To this end, besides the Cybercrime Convention, the project also built upon the principles set by the 2008 Council of Europe Guidelines for cooperation between law enforcement and Internet service providers, as well as followed ongoing work of the Council of Europe, through T-CY and Cloud Evidence Working Group, to secure and further explore direct cooperation opportunities with the global/multinational service providers. To ensure proper feedback, the progress under the project was regularly reported to the Cybercrime Convention Committee.

III. ASSESSMENT OF PROJECT RESULTS

a) Achievements of project outcomes and expected results

Expected results	**Status**	Description
Analysis of current initiatives, challenges and opportunities regarding public/private cooperation in the Eastern Partnership region available.	Achieved	• In March to June 2016, mapping study visits were undertaken to all EAP states to establish necessary partnerships, launch dialogue with country counterparts and study opportunities for cooperation, as well as to identify the issues that are necessary for public-private partnerships to generally work; the findings of these visits have been summarized in the Mapping Report on public-private cooperation in the Eastern Partnership. • The report has been updated through similar series of visits and discussions in EAP states in October-November 2017, with a further view on feasibility of regional approach to public-private partnerships and inventory of public-private initiatives in the Eastern Partnership region. • Two additional regional studies have been completed in July and August 2017, looking into the issues of Liabilities of Internet service providers in the EAP and into Strategies of cooperation with multinational service providers. • The revised study on Article 15 Safeguards and Guarantees, also updated as result of visits to EAP in October-November 2017, was presented and discussed in 2018. • 2015 Study on Cybercrime Strategies in the EAP has been revised and updated in 2018. • As a result of series of national workshops, Regional Study on cybercrime threats in the EAP was produced and completed in 2018.
A structured process of public/private cooperation on cybercrime underway and agreements concluded.	Partially achieved	• Through participation of project country teams and counterparts in Regional meetings under the project, international conferences and discussion forums, and in-country activities tailored to specific country requests or findings of project report, EAP states are actively engaged in the process of public-private cooperation built on four main elements: clear regulatory framework; identified and engaged

		counterparts; voluntary compliance mechanisms; and efficient access to data beyond national jurisdictions. • Two countries of the EAP (Georgia and Armenia) have concluded cooperation agreements that are confirmed as working and applicable. With support of the project, Ukraine has developed a draft memorandum, while Moldova hosted national discussion between criminal justice authorities and service providers on the subject. In the remaining states, the focus is on clear framework regulating day-to-day cooperation.
Criminal procedure law strengthened.	Achieved	• Five out of six EAP states (all except Belarus) are engaged in process of developing legal amendments aimed to implement the Budapest Convention on Cybercrime with the direct support of the project – either in terms of procedural powers or related legislation, including safeguards and guarantees.
Outcome indicators	**Status**	Description
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. A study has been conducted on cybercrime and cybersecurity trends in EAP, supporting countries in the preparation of country reports (on demand).	Achieved Achieved	• In March to June 2016, mapping study visits were undertaken to all EAP states to establish necessary partnerships, launch dialogue with in-country counterparts and study opportunities for cooperation, as well as to identify the issues that are necessary for public-private partnerships to generally work; the findings of these visits have been summarized in the Mapping Report on public-private cooperation in the Eastern Partnership. • The report has been updated through similar series of visits and discussions in EAP states in October-November 2017, with a further view on feasibility of regional approach to public-private partnerships and inventory of public-private initiatives in the Eastern Partnership region. • 2015 Study on Cybercrime Strategies in the EAP has been revised and updated in 2018. While three of EAP countries have already adopted cybersecurity strategies and action plans, all of the countries can benefit from more detailed and precise risk assessments to better inform future policy making. • As a result of series of national workshops, Regional Study on cybercrime threats in the EAP was produced and completed in 2018 for the first time. The report discovered shortcomings observable at a regional level, such as lack of cybercrime reporting / statistics and lack of information about cybersecurity incidents. However, awareness and political will to address these topics is fairly strong and steadily increasing.
Criminal justice authorities of the six EAP countries and service providers will have participated in a	Partially achieved	• The EAP country project teams have participated in four Regional Meetings, several international forums featuring focus on public-private cooperation and two hearings (with service providers and data protection community) organized by the Cybercrime Convention

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.		Committee to discuss and increase awareness of relevant issues of public-private cooperation. Other regional and international platforms for discussion and cooperation, led by EuroDIG, have provided venue for further discussion and training. • In-country activities by the project catered to the needs of countries as identified by Mapping Report or requested by countries themselves. Series of in-country workshops addressed abilities to develop inclusive cybercrime strategies that take into account the views of the private sector, and the need for improved cooperation between the state and the private sector for addressing common cybercrime threats and challenges. The project supported numerous national forums and events by expertise and attendance, these events providing national platforms for discussion of cybercrime and security matters between government and the private sector. In Ukraine and Moldova, project efforts focused to support law drafting/revision and agreement of principles for memorandum of cooperation. • International Cybercrime Cooperation Exercises (held twice in 2017 and 2018) became trademark and flagship events of the project. Real-time technical exercises encourage use of common approaches and methods for processing electronic evidence in both cyber security incident handling and criminal/ financial investigations on the basis of internationally accepted standards, such as the Budapest Convention. The exercises helped to establish closer links between professional communities of cybercrime investigators, cyber security players and private sector in the EaP. • EAP states received training and direct advice from multinational service providers (such as Apple, Facebook, Microsoft and Airbnb) during international events supported by the project, increasing their knowledge and skills for such cooperation. • Two countries of the EAP (Georgia and Armenia) have concluded cooperation agreements that are confirmed as working and applicable. With support of the project, Ukraine is developing such memorandum. At the same time, Azerbaijan and Belarus maintain that there is no need for such agreements due to strong state regulation of the Internet industry and compliance with law enforcement requests is claimed to be already good. • The Octopus Cybercrime Community section related to public-private cooperation has been populated by detailed entries from EAP states in response to questionnaires sent. The feasibility study run by the project identified potential new uses for this platform,

		and listed a number of relevant projects and initiatives in the region with potential for coordination and cooperation. • In-country workshops held in each EAP country in 2018 provided a venue for discussion / feedback to further expand, complete and maintain the online tool on public/private cooperation.
Procedural law reforms will have been completed in at least two countries. Proposals for reforms in additional countries will be available	Partially achieved	• The project directly supported five out of six EAP states (all except Belarus) in on-going process to develop legal amendments aimed to implement the Budapest Convention on Cybercrime – either in terms of procedural powers or related legislation. Applicable safeguards and guarantees under the Article 15 Budapest Convention were used as guidance for law reform. In terms of progress, while selected provisions related to search and seizure passed formal legislative adoption process (Moldova and Ukraine), in Georgia the amendments have been initiated formally, while Ukraine is at the stage of government review before committing the entire draft to Parliamentary process.
Impact on final beneficiaries		Description of the impact to date
Increased understanding of issues important for public-private cooperation on cybercrime and electronic evidence.		• The EAP countries, through studies and discussions under the project, agreed four specific elements to identify working and efficient public-private cooperation: clear regulatory framework; identified and engaged counterparts; voluntary compliance mechanisms; and efficient access to data beyond national jurisdictions.
Better interagency cooperation between government actors.		• Criminal justice, law enforcement, CSIRT community, data protection agencies and communications regulators of the EAP are aware of issues of public-private cooperation and are willing to work together for common goals of better cooperation and more secure cyberspace.
Increasingly meaningful dialogue between the government and private sector to find possibilities for cooperation.		• Bringing private sector and government into dialogue during project events facilitated stronger contacts and understanding of each others' issues in terms of cooperation. This had particularly strong effect in Ukraine and helped start dialogue in Moldova.
Better interaction with multinational service providers.		• EAP states received training and direct advice from multinational service providers (Apple, Facebook, Microsoft and Airbnb) during international events supported by the project, increasing their knowledge and skills for such cooperation.
Resources available to service the process of cooperation.		• The Octopus Cybercrime Community section related to public-private cooperation is populated by detailed entries from EAP states and can be used by them and other states or private entities for information.

Improved procedural legislation and related legislative framework.		• All EAP states now have general recommendations for improving procedural powers and practical aspects of cooperation as required by Council of Europe standards, and five out of six states received recommendations tailored directly to improvement of their national regulatory framework.
Increased visibility of EAP as a region piloting advanced issues of public-private cooperation in cybercrime and electronic evidence.		• Country teams and authorities of the EAP region are more active and visible, as compared to the start of the project, in terms of participation in and contribution to major international events that keep them updated of the latest developments on the subject matter.

b) Mainstreaming and cross-cutting issues

Gender issues have limited relevance in the context of Cybercrime@EAP III project (also extended in 2018), as the project focused on the practical aspects of cooperation between institutions and organizations, namely, criminal justice authorities and Internet industry players on cybercrime and electronic evidence. However, where the issue of preventing and combating child sexual abuse online is discussed as a matter of public-private cooperation, a non-governmental organization "La Strada" from Moldova, also active in the area of rights of women, is usually present and contributes its views to both national and regional meetings held in Chisinau under the project.

Civil society organizations are stakeholders in the public-private cooperation in the extent that they represent interests of the Internet service providers in their interaction with the law enforcement or security services. A particularly active partner for the project in Ukraine is the Internet Association of Ukraine, with the support of which the difficult issues of cooperation in criminal investigations led to agreement on a set of amendments to be introduced into law and principles of cooperation memorandum were agreed. In Moldova, the non-governmental sector is actively involved in the discussions on the draft Law 161 in what concerns the safeguards and guarantees and general trust between state and industry in criminal investigations – both being important topics for the project.

IV. PROJECT GOVERNANCE AND CO-ORDINATION

a) Complementarity and co-operation

The project objectives and priorities are fully aligned with standards of the EU, one of those being the implementation of the Council of Europe Convention on Cybercrime. The EU Council of Ministers conclusions on improving criminal justice in cyberspace directly refer to necessity for enhancing the cooperation with service providers. The Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, also notes cooperation between public authorities on the one hand, and the private sector and civil society on the other, being of great importance in preventing and combating attacks against information systems. And as direct benchmark for the Cybercrime@EAP projects, the EU Joint Staff Working Document "Eastern Partnership - 20 Deliverables for 2020 - Focusing on key priorities and tangible results", directly refers to implementation of the Budapest Convention on

Cybercrime for the purposes of public-private cooperation as a strategic priority for the Eastern Partnership under section 12 on Resilience and Civilian Security.

To ensure coordination and cooperation, the EU Delegations resident in capitals of EAP states are informed in advance and invited to all of the project's events to provide opening address and attend/contribute in other ways; however, many times attendance was not possible due to other commitments of the Delegations. In Ukraine, partnership with the EU Advisory Mission in Ukraine, specifically the Cybercrime Advisor, is pursued by the project in terms of coordinating activities and planning joint initiatives in the future.

b) Communication and visibility

Communication and visibility measures were taken in line with the magnitude of the activities organized, as well as with impact and scope of deliverables achieved.

International and regional events organized under Cybercrime@EAP projects benefited from planned media involvement: press releases were developed and issued ahead of events, disseminated through local Council of Europe Offices as well as through relevant local counterparts involved. Press briefings were organized in the set-up of respective events, commonly in the first day of the meetings, after introductory sessions. During press briefings, project managers and Council of Europe representatives as well as high profile participants amongst local counterparts and visiting experts were interviewed. Visibility materials were produced, such as banners, roll-ups, pens, notebooks with project PCF/PGG logos, as well as short films and live-streaming for three regional meetings.

Visibility was ensured at smaller-scale events specifically through the production of roll-ups and through visual elements such as the Cybercrime-logo folders. Agenda of events were disseminated beforehand with local counterparts. News items were published on the "Action against cybercrime" news section, on a dedicated website of the project. Press expressed interest and was present during some high profile in-country events (especially Ukraine).

Online presence was ensured not only through media coverage, but also through presence on "Action against cybercrime" as well as Cybercrime@EAP project web-pages, containing not only news about project activities, but also deliverables produced, such as studies and reports developed. Quarterly reviews of events as well as calendars of events were disseminated through the Cybercrime@CoE news digest, while most relevant events were publicized through PCF/ PGG pages.

Results achieved and deliverables produced were disseminated online whether through CEAP webpages or Octopus community platform, ranging from information sheets on the CEAP projects to developed studies and reports.

c) Challenges, lessons learned and possible follow-up

Challenges

The project is fairly unique in scope and subject, and has no directly related or comparable efforts in the Eastern Partnership region. At the same time, the variety of topics it brings together is novel for the region and the project is constantly evolving in identifying possible solutions to problems of

public-private cooperation. Despite the differences in the approach of states, one particular topic is of universal concern for the region: criminal justice authorities' access to data held by global/foreign communication service providers. As more data is being sought from such providers, cooperation is considered more challenging, compared to accessing data from private vendors/service providers established within national jurisdictions. Procedural powers to secure electronic evidence and obtain data from private sector service providers remains a challenge.

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. The issue of safeguards and guarantees is an important practical factor in terms of public-private cooperation. Availability, consistency and proportional use of specialized procedural powers by the law enforcement, beyond reasons of efficiency for investigations, contribute to clarity and foreseeability of law as well as protection from arbitrary interference with privacy of individual users and legitimate business of service providers.

Cooperation agreements between the law enforcement and the Internet industry are believed to be the way forward to determine and regulate administrative and operational issues of public-private cooperation; at the same time, the existing arrangements in the region are either too narrow in scope, or not developed further, thus having a diminishing impact on maintaining trust between the parties. There is therefore need for more focus on more comprehensive cooperation agreements with more partners and topics covered, taking into account the underutilized harmonization potential of the 2008 Council of Europe Guidelines for cooperation between law enforcement and Internet service providers. Confidence and trust remain key for interagency, international and public-private cooperation. In particular, sharing of data between Computer Security Incident Response Teams and criminal justice authorities needs to improve.

Despite project's efforts to provide a venue for balanced and inspired dialogue between the government and private service providers, the readiness of the latter to appear at and actively contribute to project activities has proven to be a challenge for the project. Additional funding made available for the project in 2017 has mitigated this by allowing the project to take private sector entities onboard as country team members. This challenge will be further remedied during project extension in 2018 by designing more interactive exercises to encourage more involvement and ensuring that private sector contribution is properly acknowledged.

Lessons learned:

The practice of establishing the project country teams composed main stakeholders has proven successful in the Cybercrime@EAP III, but benefited even more from the mid-term (January 2017) revision of the composition that sought to remove some of the redundant/irrelevant institutions (some communications regulators and several CSIRT representatives), while bringing in new partners who have more stake and role in the process of cooperation, as identified by studies and meetings under the project. The expansion of project country team membership has an advantage of better visibility of Cybercrime@EAP III / 2018 in the national context.

Although issues of public-private cooperation are primarily relevant in national contexts, the regional dimension of the project was an important contributor to results achieved so far. Bringing

the country teams and international experts together not only allowed them to discuss challenges and issues, but also to learn from each other in terms of regulatory or institutional reforms. Peer-to-peer exchange of experience in the complex topic of public-private cooperation is important, since country teams appreciate real-life examples of problem-solving by their direct counterparts rather than having experts offer often excellent, but still rather remote and depersonalized view on the subject.

Given the complexity and multi-stakeholder nature of public-private cooperation on cybercrime and electronic evidence, it was certainly useful to focus strongly on four elements agreed by all stakeholders of the project: clear regulatory framework; identified and engaged counterparts; voluntary compliance mechanisms; and efficient access to data beyond national jurisdictions. Being the work in progress, the project is developing gradual approach to these elements: at the current stage, the project features strong focus on building up proper legislation and regulatory framework; this already enables and will further support identified partners to ensure meaningful contributions to cooperation process on much clearer terms; and the clear cooperation process will encourage voluntary compliance with best standards and practices in the future.

Joining forces with other projects run by the Cybercrime Programme Office of the Council of Europe (C-PROC) was successful in increasing interaction between countries of different regions covered by projects and searching for common solutions across different regions.

Internal coordination within the Council of Europe in terms of coordinating country-specific action by the Organization, as reflected in country Action Plans[3], is another positive experience that works well in terms of uniform response and should be maintained.

Follow-up:

The following priorities and outcomes are expected to continue to have long-term relevance for public-private cooperation on cybercrime and electronic evidence in the Eastern Partnership region:

- Promoting strategic and multi-stakeholder approaches to cybercrime and electronic evidence in line with Declaration of Strategic Priorities adopted in Kyiv in October 2014;
- Completion of reforms of procedural law as basis for domestic investigations and public/private cooperation;
- Pursuing cooperation agreements and arrangements between law enforcement and domestic providers, as well as multinational service providers;
- Follow up to work of the T-CY Cloud Evidence Group and development and opportunities accorded by draft Second Additional Protocol to Budapest Convention;
- Focus on practical skills and procedures to share data and make cooperation between law enforcement, cyber security actors and Internet industry work;
- Enhanced use of cooperation tools and online platform by Eastern Partnership countries.

[3] Action plans for the EaP countries can be found at the following link: https://www.coe.int/en/web/programmes/documents#{%2226530095%22:[]}.

ANNEX

Reports and documentation appended to this Report:[4]

1. Project Summary (Cybercrime@EaP III and Cybercrime@EaP 2018)
2. General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership (initial version 2016)
3. General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership (updated version 2017)
4. Study on Strategy of Cooperation with Multinational Service Providers
5. Study on Liabilities of Internet Service Providers in the Eastern Partnership Region
6. Suggestions for draft amendments to procedural legislation of Armenia concerning cybercrime and electronic evidence
7. Suggestions for draft amendments to procedural legislation of Azerbaijan and other recommendations concerning cybercrime and electronic evidence
8. Georgia: Report on draft legislation supplementing and amending various issues related to cybercrime and electronic evidence
9. Moldova: Joint Opinion of the Venice Commission and of the Directorate General of Human Rights and Rule of Law (DGI) of the Council of Europe on the draft Law No 161 amending and completing Moldovan legislation in the field of cybercrime
10. Ukraine: Report on current legislation and draft laws supplementing and amending various issues related to cybercrime and electronic evidence
11. Suggestions for draft amendments to procedural legislation of Ukraine concerning cybercrime and electronic evidence
12. Conditions and safeguards under Article 15 of the Convention on Cybercrime in the Eastern Partnership (revised report 2018)
13. Cybercrime and cybersecurity strategies in the Eastern Partnership region: Updated report 2018
14. Perception of threats and challenges of cybercrime in the Eastern Partnership

List of activities:

1. Contribution to the Council of Europe Conference on Internet governance/Freedom of expression, 15-16 December 2015, Tbilisi, Georgia

[4] All reports referenced in this section can be downloaded at the following address: https://mycloud.coe.int/s/23y27Rp9iSCZm9M

2. Study visit to develop the Mapping Study on public-private cooperation in the Eastern Partnership region, 30 March - 1 April 2016, Kyiv, Ukraine

3. Launching Conference of the project and Public Hearings on ISP cooperation in Ukraine, 6-7 April 2016 Kyiv, Ukraine

4. Study visit to develop the Mapping Study on public-private cooperation in the Eastern Partnership region, 13-15 April 2016, Yerevan, Armenia

5. Study visit to develop the Mapping Study on public-private cooperation in the Eastern Partnership region, 18-20 April 2016, Tbilisi, Georgia

6. Study visit to develop the Mapping Study on public-private cooperation in the Eastern Partnership region, 11-13 May 2016, Minsk, Belarus

7. Study visit to develop the Mapping Study on public-private cooperation in the Eastern Partnership region, 16-18 May 2016, Chisinau, Moldova

8. Attendance of the Cybercrime Convention Committee sessions and Hearing with Data Protection Community, 23-26 May 2016, Strasbourg, France

9. Study visit to develop the Mapping Study on public-private cooperation in the Eastern Partnership region, 8-10 June 2016, Baku, Azerbaijan

10. Ukraine project: Assessment visit to key organizations on amendments to procedural law assessment, 8-9 September 2016, Ukraine

11. First Regional Meeting: Cooperation Platform between the Law Enforcement and the Internet service providers, 19-20 September 2016, Minsk, Belarus

12. Public-Private cooperation: Workshop on crime and incident reporting framework including national CSIRT, 6-7 October 2016, Chisinau, Moldova

13. Public-Private cooperation: Workshop on cooperation between the law enforcement and ISPs focusing on data preservation, 12-14 October 2016, Azerbaijan

14. Second Regional Meeting: Cooperation with multinational service providers (in cooperation with the IPROCEEDS project), 24-25 October 2016, Dublin, Ireland

15. Participation in GLACY Closing / GLACY+ Launching Conference, 26-28 October 2016, Bucharest, Romania

16. Joint expert mission between DGI and Venice Commission to support assessment of the draft Law 161 of Moldova (cybercrime), 2-3 November 2016, Chisinau, Moldova

17. Ukraine project: Presentation of findings from the Ukraine report, 4 November 2016, Ukraine

18. Public-Private cooperation: Workshop on best models in the EU and other states for public-private cooperation, 7-8 November 2016, Yerevan, Armenia

19. Public-Private cooperation: Solutions for improved sharing of subscriber information and support to Georgian IT Innovations Conference Information Security Day, 9-11 November 2016, Tbilisi, Georgia

20. Ukraine project: Workshop on communication and information sharing with local ISPs and discussion on proposed law amendments, 8–10 February 2017, Kyiv, Ukraine

21. Workshop to support revised package of amendments related to data retention, categories of data and interception/monitoring, 16–17 February 2017, Georgia

22. Public-Private cooperation: Workshop on public-private partnerships in sector-specific approach, 23-24 March 2017, Belarus

23. Research paper on cooperation strategy with multinational service providers, April-August 2017, Eastern Partnership

24. Ukraine project: Workshop on Law reform around the topics of cybercrime procedures and public-private cooperation (continued discussion of amendments), 6-7 April 2017, Kyiv, Ukraine

25. Third Regional meeting: Coordination and Partnership Cyber Exercise (in cooperation with the IPROCEEDS project), 24-28 April 2017, Tbilisi, Georgia

26. Research paper on Liabilities of Internet Service providers in the EAP, May-September 2017, Eastern Partnership

27. Workshop to support revision of the draft Criminal Procedure Code of Armenia (cybercrime and electronic evidence) to ensure compliance with the Budapest Convention, 3-5 May 2017, Yerevan, Armenia

28. Workshop on Law reform to ensure compliance with the Budapest Convention, 10-12 May 2017, Baku, Azerbaijan

29. Ukraine project: Public hearings on final version of legal amendments and development of the principles of the cooperation memorandum, 17-19 May 2017, Kyiv, Ukraine

30. Supporting attendance of the EuroDIG 2017 and Steering Committee / Planning Workshop of the project, 5-7 June 2017, Tallinn, Estonia

31. Attendance and contribution to the EAP Rule of Law Panel Meeting at the EU/DG HOME, 15-16 June 2017, Brussels, Belgium

32. Workshop on legal and practical aspects of cooperation between law enforcement and CSIRT, 5-7 July 2017, Minsk, Belarus

33. Ukraine project: Visits to key organizations to finalize the text of memorandum of cooperation, 7-8 September 2017, Ukraine

34. Ukraine project: Presentation of draft memorandum at Telecom industry meeting, 9-10 September 2017, Odessa, Ukraine

35. Fourth Regional Meeting on safeguards, guarantees and legislation and presentation of two studies prepared under the project, 11-12 September 2017, Chisinau, Moldova

36. Attendance of public hearings on law reform implementing the Joint Opinion of the VC/DGI concerning draft Law 161 of Moldova (cybercrime), 14 September 2017, Chisinau, Moldova

37. Ukraine project: Support to IGF-UA 2017 and presentation of cooperation memorandum to industry stakeholders, 5-6 October 2017, Kyiv, Ukraine

38. Meetings with criminal justice institutions, regulatory authorities and Internet service providers to update Study on Article 15 safeguards and Mapping Report on public-private cooperation in the Eastern Partnership, 12-13 October 2017, Baku, Azerbaijan

39. Supporting participation of Belarusian representative at Council of Europe and OSCE Internet Freedom Conference, 13 October 2017, Vienna, Austria

40. Meetings with criminal justice institutions, regulatory authorities and Internet service providers to update Study on Article 15 safeguards and Mapping Report on public-private cooperation in the Eastern Partnership, 16-17 October 2017, Yerevan, Armenia

41. Meetings with criminal justice institutions, regulatory authorities and Internet service providers to update Study on Article 15 safeguards and Mapping Report on public-private cooperation in the Eastern Partnership, 19-20 October 2017, Tbilisi, Georgia

42. Meetings with criminal justice institutions, regulatory authorities and Internet service providers to update Study on Article 15 safeguards and Mapping Report on public-private cooperation in the Eastern Partnership, 23-24 October 2017, Minsk, Belarus

43. Supporting contribution to IV South East European Regional Forum on Cyber security and Cybercrime, 30-31 October 2017, Sofia, Bulgaria

44. Meetings with criminal justice institutions, regulatory authorities and Internet service providers to update Study on Article 15 safeguards and Mapping Report on public-private cooperation in the Eastern Partnership, 2-3 November 2017, Chisinau, Moldova

45. Workshop on data retention vs. data preservation policy and practice, 6-7 November 2017, Baku, Azerbaijan

46. Meetings with criminal justice institutions, regulatory authorities and Internet service providers to update Study on Article 15 safeguards and Mapping Report on public-private cooperation in the Eastern Partnership, 13-14 November 2017, Kyiv, Ukraine

47. Contribution to Georgian IT Innovations Conference with presentation on law enforcement trust in cyberspace, 16-17 November 2017, Tbilisi, Georgia

48. Workshop on Cybercrime Threats, Strategies and update of the Online Resource, 6-8 February 2018, Yerevan, Armenia

49. Workshop on Cybercrime Threats, Strategies and update of the Online Resource, 13-15 February 2018, Baku, Azerbaijan

50. Workshop on Cybercrime Threats, Strategies and update of the Online Resource, 20-22 February 2018, Tbilisi, Georgia

51. Workshop on Cybercrime Threats, Strategies and update of the Online Resource, 28 February – 2 March 2018, Chisinau, Moldova

52. Workshop on Cybercrime Threats, Strategies and update of the Online Resource, 11-13 April 2018, Kyiv, Ukraine

53. Workshop on Cybercrime Threats, Strategies and update of the Online Resource, 22-24 May 2018, Minsk, Belarus

54. Workshop on legal and technical aspects of LEA/ISP cooperation, 26-27 February 2018, Chisinau, Moldova

55. International Cybercrime Cooperation Exercise on law enforcement / CSIRT / private sector communication protocols, 27-30 March 2018, Chisinau, Moldova

56. Contribution to Cyber Security Festival, 20 April 2018, Tbilisi, Georgia

57. Participation and contribution to EuroDIG 2018 – focus on criminal justice action in cyberspace / combined with Project Planning meeting and Steering Committee, 4-6 June 2018, Tbilisi, Georgia

58. Contribution to Underground Economy Conference, 4-7 September 2018, Strasbourg, France

59. Workshop on practical aspects of CSIRT/LEA cooperation, combined with advisory visit to CERT.GOV.UA and SSU technical division, 24-26 September 2018, Kyiv, Ukraine

60. Support to national forums of discussion: contribution to Youth IGF 2018 and IGF-UA 2018, 27-28 September 2018, Kyiv, Ukraine

61. Support to national forums of discussion: contribution to OSCE Conference on Terrorism in Digital Age, section on public-private cooperation, 9-10 October 2018, Minsk, Belarus

62. Support to national forums of discussion: contribution to Regional Cyber Week & Expo 2018 in Moldova, 29 October – 2 November 2018, Chisinau, Moldova

63. Support to national forums of discussion: contribution to Cyber Security Forum Georgia 2018, 9 November 2018, Kvareli, Georgia

64. Regional Conference on Cybercrime Strategies, combined with Final meeting on improving public/private cooperation on cybercrime in the Eastern Partnership region, 11-13 December 2018, Tbilisi, Georgia