Provisional Version September 2016
Reviewed at the Second Regional Meeting of the Project
19-20 September 2016

General Report on mapping the current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership

Results of the regional study visit program in Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine

www.coe.int/cybercrime

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

Table of Contents

Abbreviations

CERT – Computer Emergency Response Team
CoE - Council of Europe
Convention – Budapest Convention on Cybercrime
Country Project Team – Combination of public sector experts designated by their country to participate in this project
C-PROC - Cybercrime Programme Office of the Council of Europe
DPA – Data Protection Authority
EAP - Eastern Partnership
FIRST - Forum of Incident Response and Security Teams. FIRST brings together a wide variety of security and incident response teams including especially product security teams from the government, commercial, and academic sectors
GNCC - Georgia National Communications Commission
INHOPE – INHOPE is network of 51 hotlines in 45 countries worldwide, dealing with illegal content and fighting online child sexual abuse (www.inhope.org)
ISP - Internet Service Providers
ITU- International Telecommunication Union
KPI - Key Performance Indicator
LEA - Law Enforcement Agency (police forces and criminal justice authorities)
MLAT - Multilateral Assistance
OSCE – Organization for Security and Co-Operation in Europe.
Parties - the public and the private sector together / in general
Party - the public or the private sector
PGP – Pretty Good Privacy
Program / Project - Program of study on mapping current strengths, weaknesses, opportunities and risks of public/private cooperation on cybercrime in the Eastern Partnership region under the CyberCrime@EAP III project of the Council of Europe
Project Teams –the Country Project Team, the Council of Europe Visiting Team and the Experts together
PPP- public private partnership
Study Team – Combination of CoE Project Team and external experts who performed the Study Visits
Study Visits – Missions in the six EAPIII beneficiary countries done by the Study Team
T-CY - Cybercrime Convention Committee
TLP - traffic light protocol

Introduction

In recent years, the question of public / private cooperation and specifically the issue of criminal justice access to data has become more complex. This is also true for countries participating in the Eastern Partnership project. Often, local and multinational service providers are reluctant to cooperate, criminal justice measures and national security measures are not clearly separated, and trust towards authorities can be 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 cooperation, erodes safeguards and implicates human rights and the rule of law.

The present General Report is prepared under the Cybercrime@EAP III Project, which covers the following countries: Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine (in alphabetical order), and aims to strengthen public / private cooperation on cybercrime and electronic evidence in the Eastern Partnership project.

The Project started with study visits to all countries in focus, where the local Country Project Teams have supported the Project by organizing the meetings - *in cooperation with the Cybercrime Programme Office of CoE* - at various local stakeholders of the public and of the private sector (Study Visits).

The Study Visits were performed by the representatives of the Cybercrime Programme Office of CoE (C-PROC) and by chosen international experts (contracted consultants).

The meetings were held in English language with the support of on-site interpretation organized or performed by the Council of Europe. The local Council of Europe Office Teams have also supported the Study Visits by organization activities and by providing their premises for meetings in some cases.

The local stakeholders included professionals from the following fields:

- Government bodies with coordination focus on legislation / codification, preferably the Ministry of Justice;
- Government bodies and authorities with investigative competence, preferably various law enforcement authorities (which in some cases included operative and cyber specialized units and 24/7 points of contact personnel);
- Prosecution authority representatives with competence regarding cybercrime and electronic evidence;
- Regulatory authorities with info-communication and / or telecommunication competence;
- Institutions of the cybersecurity domain and with the main focus of notification / alerting competence (various CSIRT/CERT bodies or similar entities);
- Non-governmental associations or other forums with Internet organization focus, such as Internet provider associations;
- Internet Service Providers (ISPs);
- Authorities with data protection competence.

The purpose of the present report is to come to an initial assessment on common issues and differences regarding the cooperation between criminal justice authorities and the private sector in the countries in focus. Such cooperation is a paramount factor in securing a proper balance between the interests of investigation and the necessary safeguards, as private sector entities are holding a critical part of data relevant for law enforcement authorities.

The present report aims to discuss applicable international standards for public / private cooperation in cybercrime and electronic evidence, applicable legislative and regulatory issues in the Eastern Partnership countries, main stakeholders and practical issues facilitating or hampering such cooperation, and to offer conclusions and strategic summary as to what can be done in this respect.

The report is based on the country reports, which were prepared in cooperation with the local Country Project Team members and with the Council of Europe Project Team, and are attached to this report as an annex. In these, strengths, weaknesses, opportunities and risks of public/private cooperation are addressed in a country-specific manner.

Council of Europe Cybercrime Programme Office

Name	Details
Giorgi JOKHADZE	Project Manager Giorgi.JOKHADZE@coe.int
Nina BARYSHNIKOVA	Senior Project Officer nina.baryshnikova@coe.int
Alexandra-Adina TRANDAFIR	Project Assistant Alexandra-Adina.TRANDAFIR@coe.int

General Report

Name	Details
Giorgi JOKHADZE	Project Manager
Dr. Gergely DZSINICH, LL.M.	Dr. Dzsinich Law Office gergely@dzsinich.com
Jean-Christophe LE TOQUIN, LL.M.	Managing partner at SOCOGI SAS jcletoquin@socogi.fr
Hein DRIES-ZIEKENHEINER, LL.M.	CEO, VIGILO Consult hein@vigilo.nl

Expert Team in Study Visits

Name	Study Visits
Dr. Gergely DZSINICH, LL.M.	All countries
Hein DRIES-ZIEKENHEINER, LL.M.	Moldova, Ukraine
Jean-Christophe LE TOQUIN, LL.M.	Georgia
Christian AGHROUM, CEO at SOCOA christian.aghroum@socoa.ch	Belarus
Uwe Manuel RASMUSSEN, Attorney at law uwe@rasmussen.eu	Armenia

1. Applicable international standards for public-private cooperation in cybercrime and electronic evidence

This section aims to address the most recognizable of the international standards that have impact on the regulation of public-private cooperation in cybercrime and electronic evidence. While not an exhaustive list by any means, these standards were discussed during the study visits to the countries in question as basic points of departure for addressing public / private cooperation.

1.1 The Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime (the Budapest Convention) is the first and, so far, the only international treaty with a global geographic coverage on crimes committed against and/or by use of computers and computer networks. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

The Convention is the product of four years of collaborative effort by Council of Europe experts, but also by the United States, Canada, Japan and other countries which are not members of the Organization. It has been supplemented by an Additional Protocol on Racism and Xenophobia in 2003, making publication of racist and xenophobic material via computer networks a criminal offence.

Opened for signature in November 2001 in Budapest, the Cybercrime Convention has been steadily gaining membership of different states around the world. As of writing, 48 states were parties to the treaty, and another 18 are signatories or have been invited to accede. Ukraine ratified the Convention in 2006. However, the reach of the Cybercrime Convention is far wider, including also significant number of states that draw on the Convention provisions as the source for developing national legislation on cybercrime.

The Cybercrime Convention Committee (T-CY) represents the State Parties to the Budapest Convention. Its functions, as provided by the Convention, include facilitating the effective use and implementation of the Convention, exchange of information on significant legal, policy or technological developments on the subject, and consideration of possible supplementation or amendments to the Convention.

The Budapest Convention remains the only binding international agreement on cybercrime matters, serving as a guideline and benchmark for the development of national legislation against cybercrime and providing framework for international cooperation between States Parties to the treaty.

All of the countries in focus have signed and ratified the Budapest Convention at the time of the Study Visits, with notable exception of Belarus.

Country	Signed	Entry into force
Armenia	23/11/2001	01/02/2007
Azerbaijan	30/06/2008	01/07/2010
Georgia	01/04/2008	01/10/2012
Moldova	23/11/2001	01/09/2009
Ukraine	23/11/2001	01/07/2006

From the point of view of public-private cooperation under the Budapest Convention on Cybercrime, there is a strong acceptance of the fact that cybercrime – or, even more precisely investigation of criminal cases involving electronic evidence - is different from a traditional criminal investigation. This technical specificity leads to the necessity of updating the traditional procedural methods for capturing and processing evidence in criminal proceedings, and even introducing new powers and actions that are specifically tailored for the production of admissible electronic evidence.

The Budapest Convention on Cybercrime thus provides for a set of special or amended procedural powers that are applicable

- to the offences listed in the Convention itself,
- more generally to the investigation of any crime if it was committed by the means of a computer system
- and even more generally to any investigation in which evidence is kept in any kind of digital record.

Such procedural powers include:

- **Preservation of stored computer data** allows for expeditious preservation of specified computer data, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification (regular deletion of data, limited retention, etc.), and aims to keep integrity and security of the stored data. Such data can be preserved up to a maximum of 90 days, with a view to subsequent disclosure; moreover, persons or entities who are in possession or control such data are obliged to maintain confidentiality regarding the preservation procedures.

- **Traffic data can be preserved in an expedient manner** on the request of law enforcement seeking disclosure of such information. Traffic data is critical in determining the source or destination of a past communication, allowing identification of potential perpetrators. Traffic data may be generated and communicated by several communications providers, making it important to disclose such facts to the requesting authority, and **to disclose sufficient amount of traffic data** to determine the path through which the communication was transmitted.

- **A production order** is a viable alternative to otherwise lengthy, inefficient or even disruptive search and seizure procedure and is aimed at computer data or subscriber information that is in the possession or control of a person or a service provider, meaning physical possession or remote access. The term "subscriber information" which is crucial in this regard basically covers any information that potentially assists in establishing the identity of the person concerned.

- **Search and seizure procedures** for computer data (i.e., electronic evidence) are, in essence, assimilative provisions that aim to harmonize already existing criminal procedural law powers for search and seizure of tangible objects, in terms of their application to computer systems and data. Data search and seizure may involve either direct access to data within a computer system or its part (connected storage device) or independent storage medium (removable storage, etc.). Data may be rendered inaccessible as this may be necessary to minimize harm to victims.

- **Real-time collection of traffic data** is a procedure that is geared toward collection of data generated by computers in the chain of communication in order to route a communication from its origin to its destination, auxiliary to the communication itself ("traffic data"). The categories of traffic data that that can be collected by real-time procedures include: the origin of a communication, its destination, route, time (GMT), date, size, duration and type of underlying service.

- **Interception of content data** (that is, any other data in communication that is different from traffic data) aims to assimilate traditional options for the collection of content data in respect of telecommunications (e.g., telephone wiretapping) into the environment of information technology. In terms of criminal intelligence, it is a useful investigative tool to determine that the communication is of an illegal nature (e.g., the communication constitutes a criminal threat or harassment, a criminal conspiracy or fraudulent misrepresentations). In terms of cybercrime investigations, interception means the acquisition, viewing, capture, or copying of the contents or a portion thereof, of any communication, including content data, through any means or devices capable of such capture.

The use of procedural powers described above, despite their recognized efficiency in tackling cybercrime cases, cannot be without any limitations and safeguards, since most of these measures have direct effect on the privacy of individuals who are, willingly or unwillingly, taking part in these actions. Therefore, Article 15 of the Cybercrime Convention, as a provision of horizontal scope and application, lays down the groundwork for applicable safeguards and guarantees that relate to exercise of all of these procedural powers.

In this regard, several applicable principles can be brought forward in terms of ensuring compliance with Article 15 requirements:

- **Respect for obligations under the international human rights instruments:** As this is a fairly self-explanatory statement, states may be parties to different international treaties and enforcement mechanisms concerning human rights and fundamental freedoms. Therefore, states must adhere to the law and practice of such instruments, as interpreted by national and international courts, in the exercise of procedural powers envisaged by the Cybercrime Convention, and in many cases this would mean an application of analogy with regard to traditional procedural powers that form the basis for these special procedures. E.g. Parties to the European Convention for the Protection of Human Rights and Fundamental Freedoms should take into account the extensive jurisprudence of the Strasbourg Court with regard to wiretapping of phone conversations where provisions of Cybercrime Convention Article 21 (Interception of content data) are being applied;

- **Reliance on grounds justifying application:** As application of any of the procedural powers available under the Cybercrime Convention represents, to one degree or another, interference into the private life of persons, the use of such measures should be sufficiently justified by applicable facts and findings. More importantly, though, such reasons and grounds should be presented and available before the actual exercise of procedural powers, as the necessary justifications are often provided post factum during the court hearings on the admissibility of evidence. This also means that in all cases, application of some more invasive forms of procedural powers (e.g. real-time collection of data or search and seizure) should be only done within the framework of initiated and ongoing criminal case;

- **Adherence to the principle of proportionality:** There is a certain logic to the sequence of procedural powers in the Cybercrime Convention, as they are grouped starting from the least intrusive (preservation of data) to the most intrusive (interception of content) procedures in terms of their interference with privacy of persons. This means that, in case where less intrusive measures can be undertaken instead of search and seizure – e.g. the production order – preference should be given to the less intrusive procedures, unless there is a significant threat to integrity or availability of evidence. In all cases, the choice of the procedural power should be proportional to the nature of the offence and circumstances of the case.

- **Limitation of the duration and scope of the powers:** Any procedural measure provided by the Cybercrime Convention should be limited in time for its application, which does not rule out periodic extension based on the review of duly authorized authorities. In the same manner, application of the most intrusive procedural powers, such as real-time collection of traffic data and interception of content, where privacy of third parties is particularly vulnerable to abuse, should be only undertaken in cases of serious or grave offences;

- **Judicial or other independent supervision:** Judicial supervision is an important safeguard against violations of a right to fair trial, and is particularly applicable to those procedures that effectively intrude into private life and privacy of individuals and businesses. Judicial supervision presupposes a person with the powers of the judge or a magistrate, or comparable authority with sufficient degree of functional – and not formal – independence from the parties to the criminal proceedings. Judges, magistrates, public defenders, data protection authorities, communications regulators, parliamentary or ad hoc commissions all represent just a few examples of such supervision. Last but not least, such supervision should be exercised in relation to the application of the specific procedural power, and not focused on (although this can be also considered) the post factum admissibility of evidence that is collected through such application.

It is also self-evident that other equally important rights and guarantees in criminal proceedings, such as presumption of innocence, prohibition of punishment without law and of double jeopardy, right to liberty and security of a person, and right to fair trial shall be equally respected in all cases, whether concerning cybercrime investigations or otherwise.

Admittedly, Article 15 provides only general guidance that the establishment, implementation and application of the procedural law powers under the Cybercrime Convention should be balanced with adequate protection of human rights and liberties, with specific solutions to

ensure this balance being handed over to the States Parties. These general terms, however, have a very practical impact on cybercrime investigations and criminal proceedings, since non-adherence to the applicable safeguards and guarantees should mean, in principle, inadmissibility of evidence collected as a result of corresponding procedural actions.

1.2 The 2008 Council of Europe Guidelines for Cooperation between Law Enforcement and Internet Service Providers against Cybercrime

The Guidelines for the Cooperation between the Law Enforcement and Internet Service Providers against Cybercrime, adopted by the Global Conference on Cooperation against Cybercrime in 2008, is another example of Council of Europe guidance on the subject that is crucially important for the successful investigation of cybercrime. The Guidelines were adopted at the Octopus global conference for Cooperation against Cybercrime in Strasbourg (1-2 April 2008), which provided an opportunity to set an approach that is a result of the negotiations between the public and the private sphere representatives which took part between 2007 and 2008.

The Guidelines shall serve as a supporting roadmap and a source of practical advisory for the countries which aim at further developing their status in the domain. Moreover, these Guidelines, most interestingly, were directly referenced by the European Court of Human Rights in the case of *K.U. v. Finland*, making this document, at the very least, a recognized source of best practice on the subject.

However, it shall also be stated that reaching the starting point of utilizing the contents of the Guidelines already requires a certain environment where the parties mutually can state that there is a need for a solution – such as the Guidelines - in order to cooperate against the common goal: the effective fight against cybercrimes.

Furthermore, the use of the practical suggestions of the Guidelines can be really beneficial once the parties have realized that their cooperation is or can be based on *trust.* This trust results from statements throughout the negotiations, regular project management with pre-agreed milestones, continuous openness for communication about their real aims. Moreover, it is also key to commonly agree on joint goals.

In the below section the main aspects of the Guidelines are being summarized in order to have a comprehensive view before analysing the countries in this regard.

The Guidelines prescribe the following common approaches for both parties:

- Regular information exchange between the parties regarding cybercrimes;
- A culture of cooperation, including the sharing of best practices and organizing regular meetings;
- A commonly negotiated and agreed written agreement on cooperation rules;
- A constructive and regular feedback system;
- Implementation of guarantees in order to properly respect the rights of the other party;
- Protection of fundamental rights, especially: human rights, fundamental freedoms, civil and political rights and data protection;
- Enforcement of privacy and data protection standards;
- Cost respectful- and effective procedural measures.

The Guidelines specifically suggest the following measures to be taken by the law enforcement, with the intention to ease cooperation with the Internet service providers:

- Assisting of the provider sector in educational seminars and also with the sharing of good practices nationally and internationally (both legal and technical);
- Written requests shall be produced with consequent follow-ups;
- Internal trainings on effective implementation of procedures;
- Obtaining and maintaining the necessary and secure technical resources for information exchange;
- Designated and trained personnel as contact points;
- Defining the exact authorizations in written communication;
- Introducing clearly defined procedures and the authorized personnel;
- Verifying the provided information about communication and contact details;
- Securing the clear method of communication with documentation streamline, standards, format, prioritization and archive;

- Providing of clear specification of the relevant data and the necessary amount of information on the investigation;
- Providing of assistance and explanations to the provider segment in order to support development;
- Acting with a budget efficient focus, applying appropriate deadlines and avoiding of the unnecessary interruption of the provider's normal business procedures;
- Ensuring of the necessary confidentiality regarding the received data;
- Using of contact points only in cases of reasoned urgency;
- Acting appropriately and cooperatively in cases of preservation- and disclosure orders;
- Following the procedures based on international treaties in case of non-domestic providers;
- Ensuring that provisional measures shall be followed by international procedures for mutual legal assistance;
- Setting up of compliant and comprehensive procedures with clear descriptions of programs for the providers;
- Applying a transparent system in order to track statistics and processes in an auditable manner in order to identify strengths and weaknesses (publish reports when applicable).

In order to keep up the balanced approach as the main ideology of cooperation, the Guidelines also set measures for the ISPs about how to proceed in this manner:

- Cooperating with law enforcement in order to minimize illegal activities;
- Reporting of criminal incidents, which may not include the obligation to search for such in an active manner;
- Assisting in education and training;
- Following-up of requests from law enforcement in a reasonable manner;
- Implementing and applying internal policies for diligently processing measures in case of requests;
- Providing internal trainings in respect of such procedural steps;
- Appointing of trained contact points;
- Setting up and continuously operating of an effective emergency contact point;
- Dedicating the necessary resources for stable cooperation procedures;
- Setting up of compliant and comprehensive procedures with clear descriptions for law enforcement;
- Verifying the received information and securing the confidentiality of data management in the processes;
- Applying a transparent system in order to track statistics and processes in an auditable manner;
- Securing the clear method of communication with documentation streamline, standards, formats, prioritization and archive;
- Processing of data with respect of the deadlines, in a timely manner;
- Providing of proper and validated information for requests with explanations if needed;
- Applying a transparent system in order to track statistics and processes in an auditable manner in order to identify strengths and weaknesses (publish reports when applicable).
- Coordinating the cooperation with law enforcement and the sharing of best practices within the provider segment with due respect to industry related legislation (e.g. anti-trust / competition law).

In light of the above it can be stated that the Guidelines aim at providing a structured and balanced way for developing opportunities in cooperation against cybercrime with an approach which outlines effective measures and toolsets that can be adopted for many situations. This approach provides the EAP countries' public and private sector representatives an opportunity to develop their cooperation methodology and milestones in their own individual dynamic. The ability to tailor the set of instruments to be applied is also affected by the given country's history, legal system, government / decision maker willingness, maturity of legislation regarding the cybercrime domain and largely by the current cooperation level between the public and the private sector.

2. Legislation

In order for public-private partnerships to work in the area of fighting cybercrime and generally the use of electronic evidence in criminal proceedings, one has to be aware of the fact that, more often than not, such data is held by private sector entities in the form of subscriber, traffic or content data. Therefore, a central issue to the discussion of the public /

private cooperation against cybercrime and on electronic evidence is access by the criminal justice officials to data held by private entities.

Accordingly, it is without question that the terms, conditions and limitations for such access should be addressed by legal framework of the states in a comprehensive and balanced manner, while recognizing the need for such access to be sufficiently expeditious and efficient due to the volatile nature of such data. In a strictly regulated environment of criminal investigations, clarity and predictability of law represent decisive foundations upon which the government and the industry can be able to build effective and efficient cooperation modalities.

The discussion and analysis below is therefore structured in the following applicable sets of legal regulation:

- Necessary definitions and categories of data and evidence;
- Conditions on storage of and access to data as electronic evidence;
- Implementation of procedural powers under the Cybercrime Convention; and
- Safeguards and guarantees applicable to exercise of such procedural powers.

2.1 Necessary definitions

One of the most important notions in preventing and combating cybercrime, not defined directly by the Cybercrime Convention but noted numerous times in the Convention's text, is the concept of **electronic evidence**. Representing a form of evidence that is similar legally to other "traditional" types of evidence (such as paper document or oral testimony), it may be defined as "any information generated, stored or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceedings."[1]

Electronic evidence can be extracted from the multitude of sources, including computers, computer networks, peripheral devices, data storage, mobile telephones, the Internet and other media. Being an intangible form of evidence, it can be easily manipulated and altered; despite this, electronic evidence is still subject to the same evidentiary standards of integrity and admissibility as the other types of evidence.[2]

Electronic evidence, as a standalone and admissible type of evidence, is not directly defined – excepting a couple of exceptions – in criminal procedure legislation of the Eastern Partnership states. The lack thereof is somewhat compensated by the use of other concepts or types of evidence ("documents", "objects" or "other materials") that can include electronic evidence; moreover, there were no reports that electronic evidence is not accepted either by prosecution or judiciary as valid evidence in the criminal proceedings.

However, the definition of electronic evidence is an important concept that can facilitate application of less intrusive procedural powers in practice, as the standalone nature of the electronic evidence and focus on possibilities on access thereto can provide a viable alternative to often prevalent practice of removing entire computer systems or parts of hardware from the lawful possession of individuals or legal entities.

For the purposes of criminal proceedings involving electronic evidence, the Cybercrime Convention, being the primary source of law on the subject, differentiates between several types of data that can be used as electronic evidence, namely, subscriber information, traffic data and content data.

The term "**subscriber information**", for the purposes of the production order (a procedure discussed in the further section on procedural powers), stands for any information that can potentially lead to identifying several categories of information related to the subscriber (i.e. user) of the electronic communications. Such categories may include the type and technical data of communication service used (including time), the subscriber's identity, address and contact data, and any other information on the site of the installation of communication equipment.[3]

[1] "Electronic Evidence Guide: A basic guide for police officers, prosecutors and judges", developed under the CyberCrime@IPA joint project of the Council of Europe and the European Union on cooperation against cybercrime in South-Eastern Europe, March 2013, p 11.
[2] Ibid., pp. 11-12.
[3] Convention on Cybercrime, Article 18.

The term "**traffic data**" stands for any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.[4]

"**Content data**" is not defined in the Convention but refers to the communication content of the communication; i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication (other than traffic data).[5]

The terms of subscriber information and traffic data can be mostly found in several legislative acts of the EAP states, including criminal procedure legislation and laws on telecommunication or electronic communications. Content data is usually not defined as the interception of such data, as a vehicle to implement the procedural powers provided by Article 21 of the Cybercrime Convention, is implemented either in criminal procedure or laws on operative-detective activity in relation to all types of data.

The major problem in this regard is not the precise definitions of each type of data or general level of compliance with the Cybercrime Convention in relation to terms used, but rather the absence of different approaches to different types of data in terms of applicable procedural powers. In law and practice of EAP states, all types of data are treated in a same manner and subject to same or similar limitations or conditions for access, while a coherent approach from the point of safeguards and guarantees would be to attribute lesser conditions to accessing subscriber information, while access to traffic data should be subject to more stringent limitations, and access to content data should require the most stringent ones.

2.2 Conditions on storage of and access to data

The Cybercrime Convention offers a fairly structured approach to accessing data/electronic evidence necessary for the investigation of cybercrime or other offences. Data preservation and limited disclosure are followed by the production orders as the least intrusive measures of accessing electronic evidence; search and seizure is used a next point of resort or where necessary as production orders cannot serve the purpose; real-time collection or traffic data and interception of content are covert but fairly standalone measures that could be justified by adequate necessity for their use where other measures cannot reliably produce evidence.

Quite often, data retention regulations and practice are thought to be beyond the above-noted structure and overall remit of the Cybercrime Convention, as its Explanatory Report draws distinction between data retention and data preservation: "While sharing similar meanings in common language, they have distinctive meanings in relation to computer usage. To preserve data means to keep data, which already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate. To retain data means to keep data, which is currently being generated, in one's possession into the future. Data retention connotes the accumulation of data in the present and the keeping or possession of it into a future time period. Data retention is the process of storing data. Data preservation, on the other hand, is the activity that keeps that stored data secure and safe."[6]

However, in terms of public / private cooperation against cybercrime and on electronic evidence, availability of data retention possibilities is sometimes a key to dialogue between the government and industry in terms of access to electronic evidence. From this perspective, data retention is a potential –not exclusive - alternative to data preservation that gives both the law enforcement the comfort of access to already stored and readily available subscriber information/traffic data by preservation orders, while the service providers benefit from the safer path of turning over such data instead of being subject to coercive measures that often directly interfere with their legitimate business.

That said, data retention legislation is a problematic area of regulation throughout the Eastern Partnership region. In some countries, the definitions and requirements are unclear, especially those related to time limits for the storage of data or the specific types of data (traffic data) that needs to be stored. Widely different practices of time limits to the data retention are characteristic for the Eastern Partnership region. Data can be kept from 3 months to 5 years, sometimes with different stakeholders in the same jurisdictions reporting entirely different

[4] Article 1 of the Convention on Cybercrime.
[5] Explanatory Report to the Convention on Cybercrime, par. 209.
[6] Explanatory Report to the Convention on Cybercrime, par. 151.

terms for storage, or not kept at all as the obligations to store such data are not sufficiently clear or detailed and are usually not followed due to lack of sanctions for failure to do so.

In some countries, the data is retained for a fairly long period of time but is subject to virtually no supervision or control, which makes the practice problematic from the personal data protection perspective. In at least one country of the region, applicable data retention regime was almost entirely stuck down by the Constitutional Court due to concerns related to equality of arms and proportionality. In another jurisdiction, where data retention is regulated and sufficiently detailed, the issues of trust between the Internet service providers and the law enforcement make the cooperation difficult to follow in practice.

The policy makers in the EAP states are following the recent debate and review of the data retention regulations in the aftermath of the ruling of the European Court of Justice in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*.[7] The Court examined the issues in relation to traffic data (including Internet access related traffic data) and took the view that, by requiring the retention of those data and by allowing the competent national authorities to access such data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data. Furthermore, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate for the persons concerned a feeling that their private lives are the subject of constant surveillance. Needless to say, the widely varying approaches of the EU states in still ongoing implementation of this decision are not, in current conditions, a very convincing case for common approach in the Eastern Partnership states.

In addition, the discussion on data retention regulations is very often delayed or is non-productive due to the disagreement as to the costs that need to be borne by the industry to comply with data retention requirements. Several ISPs, for example, point to the fact that the storage of traffic data as defined by the Cybercrime Convention is far less costly than building and maintaining a system for the preservation of data, which may include content data, for 90 days and beyond; similar concerns are expressed in relation to real-time monitoring and interception capabilities. Thus, the dialogue on costs, including compensation schemes where practicable, is an indispensable part of and, in certain respect, an obstacle for the reform of this important area of law.

2.3 Procedural measures under the Cybercrime Convention

As noted above, the Cybercrime Convention establishes a logical structure of procedural powers applicable to electronic evidence, either in terms of chronology (data preservation followed by other options of retrieval) or level of intrusiveness into the private life of individuals (least intrusive powers giving way to progressively more intrusive options). This structure and direct implementation of all procedural powers has a direct impact on the level of public-private cooperation beyond overall goal of ensuring mere compliance with the Convention, as the availability of least intrusive procedural options increases trust of the service providers in non-intrusion with its lawful business activity, while the "heavier" options at the disposal of the law enforcement represent the possibility to get access to sought data, should lighter measures fail due to various circumstances, including non-cooperation from the providers.

Unfortunately, the implementation of the procedural powers in the Eastern Partnership states leaves a lot to be desired from the point of view of either coherence or practical application:

- With one notable exception, five out of six countries of the Eastern Partnership do not implement the provisions of Articles 16 and 17 of the Cybercrime Convention into their national law. Data preservation powers are usually thought to be effectively replaced by the search and seizure powers that are, while still subject to judicial control and oversight, far less desirable options in terms of expediency that is required by the above-noted provisions of the Convention. Data preservation obligations are very often understood as the exclusive competence of the 24/7 network of the points of contact under the Budapest Convention and are thus very rarely utilized under in national investigations. Lack of effective distinctions between subscriber information and traffic data based on applicable conditions and limitations further limits the proper

[7] http://curia.europa.eu/juris/liste.jsf?num=C-293/12.

understanding and utilization of data preservation/limited disclosure powers by the law enforcement;

- At least in two countries of Eastern Partnership, production orders pursuant to Article 18 of the Convention are available in national criminal procedure legislation; however, in practice this is rarely used due to issues of trust and overall readiness of cooperation, with ISPs requiring judicial orders for any handover of their data; this forces the law enforcement to revert to more intrusive and compulsory measures, such as search and seizure. In the states where production orders are not implemented, absence of production orders as important alternative to search and seizure is also tied to lack of clear regulation of data retention and data preservation powers, which are important pretexts to production (as data needs to be created and stored first to be turned over to the law enforcement as admissible evidence);

- The Eastern Partnership countries report virtually no practical problems in applicability of the base search and seizure provisions of the Article 19 of the Convention to the electronic evidence, as the chain of custody, including forensics process, is being applied to all types of evidence that require such treatment. However, extended search possibilities under Art. 19 par. 2 of the Convention as well as possibilities to render data inaccessible under Art. 19 par. 3(d) of the Convention are not widely implemented, as the practice of seizure of electronic evidence without custody of the corresponding data carriers/related hardware is not prevalent. However, the possibility to engage experts/specialists for support in the search and seizure process (Article 19, par. 4) is widely available and regulated by the criminal procedure in the EAP states;

- The powers under the Article 20 and 21 of the Cybercrime Convention, related to real-time monitoring of traffic data and interception of content, are implemented in all Eastern Partnership states either through criminal procedure laws or laws on operative-detective activity. The limitations as to offences, judicial supervision, purpose limitation, exhaustion of lesser measures and proportionality are, in general, applicable, and practical concerns of costs and availability of direct access to the infrastructure of Internet service providers provide additional safeguards. At the same time, there seems to be limited understanding as to variance of such limitations and safeguards in relation to traffic vs. content data. In half of the EAP states, the interception/monitoring powers are subject to ongoing policy and public debate, while in other three this issue could not be discussed in much detail due to sensitivity of the subject for the industry. Legal interception capabilities were not always made transparent at the country meetings. In some countries, the state requires the operator to relinquish control over their network intercept points to a state service that, in turn, proceeds to intercept individual users without involving the ISP or any other intermediate or supervisory body. This system is, in theory, very prone to abuse and oversight of the use of this police power is hard, if not impossible, due to lack of transparency.

To overcome these concerns, legislative reforms related to the full implementation of the procedural powers under the Cybercrime Convention have been reported to be ongoing in at least five out of six Eastern Partnership states, which is an encouraging development.

2.4 Safeguards and guarantees

Public / private cooperation against cybercrime is not free from the rule of law. Although in some countries, traditionally, help is provided voluntarily by Internet service providers to investigating bodies and authorities, and without thought or question, this practice may lead to questions and does not provide a solid basis for cooperation in matters concerning cybercrime investigations. Indeed, the Cybercrime Convention recognizes in Article 15 that all powers that are implemented by the signatories are "subject to conditions and safeguards provided for under its domestic law which shall provide for the adequate protection of human rights and liberties." These safeguards and guarantees are equally important for the cooperation of law enforcement with industry in the fight against cybercrime as any other legal requirements.

The Cybercrime Convention recognizes this in Article 15 and, in a horizontal manner, links the application and implementation of the procedural provisions of the Convention on Cybercrime to the rule of law, human rights and proportionality considerations:

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

Article 14 of the Cybercrime Convention also serves to provide further guidance in implementing a proportionate system of application of powers. Although it mandates the use of all powers mentioned in the Convention on Cybercrime in the substantive cybercrime cases that are defined therein, it exempts the most intrusive measures (the collection of - real time-traffic data and interception of content) from this obligation and make them subject to further limits defined in national law. Article 15 also implies that safeguards and guarantees are sought to make sure powers mentioned in the Budapest Convention on Cybercrime are implemented in a way that is balanced and takes note of the rights of all parties involved.

The Convention on the Protection of Human Rights and Fundamental Freedoms is by far the most important and practical guidance for the implementation of the Convention in this regard. The most relevant rights and safeguards - at least for the purposes of this report - are the right to liberty and security (Article 5), the right to fair trial (Article 6), the legality principle (no punishment without law; Article 7) and the right to privacy (Article 8). In some cases, freedom of speech and expression (Article 10) may be involved.

The European Court of Human Rights (ECHR) has only provided limited guidance on these articles in relation to the Budapest Convention, however. Only in the case of *K.U. vs. Finland* did the court address this issue. In this case the identity of a user behind a dynamic IP address was crucial to the investigation. The ECHR ruled that in order to receive such data there should be "an explicit legal provision" in order to be able to identify the actual offender. Also, there is a positive obligation to provide remedy to such cases. Finland, lacking a provision to identify the suspect, was therefore required to change its laws.

Irrespective of applicable law and extent of regulation (one has to bear in mind that at least one of the project countries is not a member to the Council of Europe), several issues of concern need to be singled out in the context of the Eastern Partnership, as outlined below.

Countries in the EAP region appear to refer to judicial oversight mechanisms for the various stages of the investigation as a primary safeguard, as judges will normally be fair and impartial supervisors in this process. Judicial warrants in several countries are used as a ground for applying even all of the Convention-related procedural powers irrespective of the data sought. Presumably, this has a negative effect on the expediency requirements for the exercise of such powers, taking into account the volatile nature of electronic evidence.

At the same time, most of the EAP states reported that in practice judiciary will have to produce or decline the judicial order within 24 hours from the application, which is, on one hand, considered adequate for practical purposes, and on the other, as a factor which increases compliance of the private sector vendors against whom such orders may be directed.

Irrespective of the efficiency or adequacy of this approach, this leaves a very little incentive for the development of the public / private cooperation in practice, as the requirement of the judicial warrant for accessing all types of data through all of relevant procedural powers renders effective judicial oversight and system of progressive safeguards and limitations rather pointless.

Throughout the EAP region, it is common in some countries to divide the investigation into preliminary and investigative phases, during which different regimes and even different legal acts may apply. In some countries, the preliminary phase is the prerogative of the police and

cases are investigated on the basis of operative-detective legislation that is, in most cases, fairly limited in terms of judicial oversight and secondly, does not directly produce evidence that is admissible in court, unless converted into admissible evidence through some other procedure (examination of witness, expert's findings, etc.).

Personal data protection regulations are a relative novelty for the region, with the core data protection legislation adopted in the span of last five to ten years; in reality, there is yet very little practice in the region in terms of detailed regulations on the processing of data, including processing of user's data by the Internet service providers. Although most of the EAP states have legislation in place that covers law enforcement processing, there was little evidence, throughout the region, of extensive contacts and awareness on the risks and requirements of public-private cooperation in the field in of both cybersecurity and cybercrime.

At the same time, it should be noted, that data processing was also perceived by some countries as a blocking factor that makes public private cooperation less easy, if not impossible, due to the lack of grounds for processing the data involved. In general, privacy should not be a concern if there are fair and legitimate grounds for processing; however, this could be attributed to the lack of meaningful dialogue and sharing of common values between the law enforcement community and the data protection community, which leads to the need for more guidance on how to achieve efficient public / private cooperation.

The project team is also mindful of the practical consideration that there would be specialized activities under the Cybercrime@EAP III project in 2017 that focus exclusively on the implementation of the Article 15 in the EAP region; given the wealth of the rest of information supplied through the study visits, the above analysis can be seen as only a preview of the most obvious issues related to safeguards and guarantees in the process of public / private cooperation on cybercrime and electronic evidence.

3. Main stakeholders and issues of the public-private cooperation process

This section of the report attempts to bring together the practical issues of public / private cooperation against cybercrime and on electronic evidence that are inherently tied to the main stakeholders in the process of such cooperation.

3.1 Criminal justice authorities

Law enforcement authorities in the Eastern Partnership states are most active and common representatives of the state in the process of public / private cooperation against cybercrime and on electronic evidence. Most commonly, the cybercrime/high-tech/computer crime units at the national police forces are the primary source of requests for access to data, as these units are most specialized in handling of electronic evidence in criminal cases. In two states of the Eastern Partnership, Investigative Committees as central authorities of investigation separate from police forces are handling these cases, while one EAP jurisdiction is in the process of handover of the cybercrime investigation powers from the security services to the national police. The investigative units also rely very often on either internal or external expert capacity in both securing and processing electronic evidence.

Prosecutors in the EAP states play a far more understated role in terms of public / private cooperation, at least in the practical instances of requests for accessing data. While they are primarily the state officials entrusted with the responsibility of introducing and supporting evidence of the state in both pre-trial and trial proceedings, there seems to be less focus on the concerns related to electronic evidence and data held by private vendors from prosecution authorities. Requests for access to data are usually initiated and executed by the law enforcement, while prosecutors would provide an oversight or guidance only in general terms to the investigation. With one notable exception, there are no specialized prosecution units dealing with cybercrime investigations in the legal systems of the Eastern Partnership, which decreases their role and interest in the development of public-private cooperation opportunities.

Judiciary authorities were not part of the study effort and therefore not covered either by the study visits or this report. Nevertheless, their role in providing judicial oversight in terms of safeguards and guarantees, as well as ruling on admissibility of electronic evidence remains undisputed.

At the same time, law enforcement authorities involved in the investigation of cybercrime are also active in the field of anti-terrorism investigations. Police/operative/intelligence powers in these investigations are usually broader and face less scrutiny than powers applied in traditional cybercrimes (such as search and seizure or interception). Although not studied in detail in this particular study, the mixed use of these powers may lead to lack of clarity in the exercise of these powers, especially when criminal charges are investigated based on information gained from powers related to terrorism.

The latter issue is compounded by the fact that many countries in the region still have and rely on the concept of operative-detectives and extensive (police) powers in the preliminary investigations phase. From the context of cooperation this may mean that ISPs, banks and other private sector institutions faced with law enforcement requests pertaining to cybercrime have limited recourse to procedures that would allow them to question the use of these powers in individual cases, eroding their trust and leading to a limited cooperation level and limited possibilities for voluntary cooperation.

At the same time, the Study Team noted that the use of operative-detectives in criminal investigations is still widespread but rather seems to be on the decline throughout the region, with some of the countries abandoning this concept in favour of the criminal procedure regulations on covert investigative activities. From the perspective of cooperation with industry this should lead to more clarity in contacts with law enforcement due to increased foreseeability of law.

The lack of clear, succinct and widely understood working methods - when it comes to requests from law enforcement - may lead to misunderstandings and can easily create tensions between public interests in enforcement and private interests that include privacy and commercial interests. Such concerns can very often be prevented or overcome by cooperation agreements that implement at least some of the recommendations provided by the 2008 Guidelines for the Cooperation between the Law Enforcement and Internet Service Providers against Cybercrime.

Despite the fact that such memoranda of cooperation are concluded in three of the EAP countries between the law enforcement and the Internet industry - with varying degree of coverage as regards the law enforcement representatives in two of them – such cooperation agreements have not been seen yet as decisive factors in day-to-day cooperation; more weight is given yet to the clear and balanced legislative background as a primary source for such cooperation.

The reasons for this are varying, but generally include either general mistrust toward the government from the industry despite the already concluded memorandum (in two such cases, highly disputed legislative amendments in terms of data retention and procedural powers), or such document may have been concluded only very recently to yet bring forward any tangible results. In most countries, there was no practice of operational meetings or other standing body that was capable of bringing together all relevant parties in these cases through discussions.

At the same time, these agreements are recognized from the law enforcement as an important exercise in terms of exchange of working contacts and increase of expediency in terms of compliance with law enforcement requests, and are generally regarded as a first step in the right direction that needs further commitment from both of the sides to such partnerships.

3.2 Internet service providers

The Internet service providers are important players in relation to cybercrime. Their registration of IP addresses, subscriber information logs of traffic data as well as their efforts to ensure security of their networks, are often decisive factors in the success of cybercrime investigations.

In the European Union, businesses and organizations providing Internet access are exempted from liability for content they host, transmit or cache, as long as they meet well defined criteria (such as that they did not select or create the material themselves, and in the case of hosting: they do not have actual knowledge of potentially illegal information that is made available). This regime is laid down in the e-commerce directive (Directive 2001/31/EU) and also provides that no obligation to monitor for illegal content shall exist.

This "safe harbor" regime is an important safeguard to freedom of speech, as it prevents ISPs from becoming liable for the content of their users. In many cases, court orders may still be used to block or delete content – however the independent review of the courts assures industry that any request made to them is indeed related to unlawful activities or illegal content. This provides industry with the certainty that government intervention is neither random nor based on mere self-interest or undue censorship. As such, the regime promotes trust and freedom of speech in a fair and balanced manner.

Throughout the Eastern Partnership region, however, the study team did not always find examples of this legislation, or similar regimes, implemented in either regulation or law. In fact, ISP liability was often understood as the liability of ISPs to unquestioningly cooperate with law enforcement, or the liability that arises if cooperation is lacking. This is indicative of lack of understanding and trust in the region that will be elaborated on later in this report.

This lack of trust and understanding of common, shared goals toward ensuring a safer cyberspace often contributes to varying degrees of general caution and even scepticism of some of the players in the industry toward the law enforcement in general, and possibilities of public-private cooperation in particular. There seem to be various factors at play that are directly influenced by features attributable to different states, but several common trends can be singled out nevertheless:

- The level of cooperation is in direct correlation to the ownership of the ISP in question. State-owned service providers that are sometimes in privileged position are generally more inclined to cooperate and report less problems in their interaction with the law enforcement, while the local subsidiaries of large multinational telecom providers are most reluctant to give law enforcement sought access to data;

- There seems to be very little dialogue between the law enforcement and the ISP sector beyond their daily interaction on the issues that can be of common interest for both communities. The ISPs view the current regime of cooperation as one-way street in terms of information flows, with very little information provided in return from the state;

- The competence of some of the law enforcement officials (usually beyond specialized cybercrime investigation units) dealing with requests to ISPs is often called into question and is a major factor of mistrust and lack of cooperation on the part of the industry players. The lack of expertise and knowledge in terms of accessing data leads to situations where ISPs feel that either too much data or even unnecessary hardware/storage is requested from them in an arbitrary manner;

- In several of the EAP jurisdictions, the requests from law enforcement that are justified by exigent/exceptional circumstances and thus request access to data without effective oversight or even paper trail are reported to become the norm instead of exception. This undermines, in the view of the Internet industry, already limited cooperation as their concerns of protection of their customers from arbitrary interference in their private lives is seen as a part of their business requirements.

Irrespective of these concerns, the ISP community in the Eastern Partnership states seems to be open to dialogue and cooperation in at least seeking more clarity and predictability on the regulations and methods employed by the law enforcement in accessing data. At the same time, from the perspective of ISPs, the Memoranda of cooperation in those countries that concluded them were seen as more of a statement of intent rather than practical documents, with some of the ISPs reporting even no knowledge of the existing arrangements that they were supposed to be part of.

3.3 National communications regulators

National tele- or electronic communications regulators are seen as potential partners in the issues of public-private cooperation on cybercrime and electronic evidence due to the direct involvement of such organizations in the licensing, introduction of regulations, adjudication of disputes between industry players, and most importantly, the focus on the protection of subscriber to the service of the Internet service providers. Communications regulators are usually independent in their policy and decisions making and can provide an independent forum for addressing the issues of cooperation between the government and the industry.

That said, the project team meetings with the communications regulatory authorities of the Eastern Partnership revealed that such institutions, with one notable exception where a national regulator provided a platform for the conclusion of the law enforcement/ISP cooperation memorandum, have not been or do not plan to get involved in the issues of law enforcement access to data held by Internet service providers. The primary related concern of such agencies is cybersecurity, but rather on a policy level than introduction of regulations; similarly, there is little involvement with the much needed reform of the data retention regulations and practices, while protection of customers is mostly driven by hearing of individual complaints. There are also different practices as regard licensing and possible sanctions/remedies in cases where the legal obligations to cooperate with the law enforcement are not followed. In general, the communications regulators seems to distance themselves from the criminal justice response to cybercrime and cybersecurity in both terms of policy or practice.

There may be therefore a need to revise the approach of the Cybercrime@EAP III project in terms of involvement of the national communications regulators, as a follow-up to the initial stage of the project, as partners and players in the overall scheme of cooperation. So far, there seems to be a far more pressing need for building direct partnerships between the law enforcement and the Internet industry in fighting and preventing cybercrime.

3.4 Data protection authorities

The data protection authorities are becoming increasingly important factor in the public-private cooperation in cybercrime and electronic evidence for two primary reasons: first, the mass processing of personal data through data retention regulations and practices that need oversight; and secondly, law enforcement access to such data needs to comply with data protection principles.

Data protection legislation is, as such, present and developed throughout the region. With the exception of Belarus, which expects a personal data protection act to be adopted in 2017, all EAP countries have both a data protection act and an authority that oversees and enforces the legislation. The institutional frameworks are different, however, with only two of the EAP states having a fully independent authority, while in others these functions are combined with various Ministries or Ombudsman's Office.

The institutional framework is, then, also in need of support as most of these institutions have been introduced only fairly recently. The biggest concern is the lack of human resources and a clear need for development of these institutions, including financial resources. Data Protection Authorities generally suffer from lack of staff specialized in information technology and are often understaffed with lawyers as well, especially as the inspections of the public or private entities are needed.

Data protection authorities are often a port of call for individuals and businesses whose (customer) rights are infringed upon, so it is encouraging that in most countries the DPA has oversight over law enforcement processing of data. Only in one states of the EAP region, however, this oversight is enforced through direct technical involvement in the authorisation and control of interception and data access activities of the law enforcement – and in that particular country, this system as well as data retention are under review following a Constitutional Court judgement.

3.5 Cybersecurity community

There is a global trend of increasing interest in cybersecurity and need for a national cybersecurity strategy is recognized by most countries in the region. Most are either working on one, or have one adopted. The process of identifying critical infrastructure and legislation that requires the security of this infrastructure to be adequate is also underway in a number of EAP countries.

In many countries that had adopted a cybersecurity strategy, cybercrime is not specifically mentioned in the strategy however. This may lead to functional separation of the security function from the law enforcement function, and could have the altogether undesirable effect that one incident is reported to one type of authority, but does not reach the other.

In terms of public / private cooperation it may be noted that national CSIRT teams are quite common in the area. Many have been set up either within the government and also some

sectoral CERTs operate in the private sector. In most countries the national CERT is a part of the central government, and is a coordinating node, intended to also co-operate with sectoral CERTs. This may well be a natural axis for cooperation, as most important private industries (such as ISPs, and banks) also have extensive experience in cybersecurity management and may well be able to assist in securing critical information infrastructure.

Another area that requires the attention of the Project is the exchange of data between the public and private sectors, and the exchange of security/CSIRT related data with law enforcement bodies. Traditionally the CSIRT/CERT community uses relatively informal ways of sharing information and the TLP (traffic light protocol) to limit distribution of data. With CERT bodies increasingly being incorporated in security services and regulators that have close ties to law enforcement (as it is the case in almost all of the EAP states where the government CERT acts as a national CERT), the question as to the status and legality of this exchange arises. This is an area where good practices would be invaluable, not only for the EAP region, but for the global security and law enforcement communities.

Although outside the Cybercrime Convention coverage and the issue of criminal justice access to data, there seems to be room for some support in this regard since cybersecurity, quite often, first port of call and a shared interest when it comes to the cooperation between private industry and public entities. In many other countries, successful operational meetings in the context of CSIRT/CERT operations contribute to the successful cooperation (also in cybercrime cases) between public and private organizations. It is often beneficial if the CSIRT/CERT has some independence in carving out its role so that it can broker good relationships without being perceived as a strictly government entity.

4. Conclusions

The current study aims to provide a mapping of current strengths, weaknesses, opportunities and risks of public / private cooperation on cybercrime in the Eastern Partnership region. In this section, the project team will attempt to summarise the main conclusions of the study, which shall serve as a baseline for the CyberCrime@EAPIII Project to address these issues by regional and in-country events.

4.1. Public-private cooperation is a challenge everywhere

It cannot be underestimated how much public-private cooperation is a more challenging concept than it seems at first. Making it a practical and sustainable in reality at national and international levels is even more difficult. Still, the technical complexity of the Internet, the fact that most of the telecommunication infrastructure is owned and managed by the private sector, and the reality that crimes are increasingly using the Internet infrastructure as our societies increasingly rely on technology - all these factors contribute to remind authorities that they absolutely cannot fight cybercrime alone, and they need the assistance from the private sector.

Once authorities understood that it was critical to involve the private sector, they have been tempted in the early 2000's – predominantly in North America and the European Union – to trust the private sector in self-regulating itself. This approach was not providing public authorities with sufficient transfer of knowledge from the private sector, and the private sector did not have enough expertise and resources to understand the priorities of the government. To put it simple, it was not the private sector's role to take care of the general interest. Self-regulation was not a premature concept, it was misguided.

From the adoption of the EU e-commerce Directive in 2000 (2000/31/CE), a first compromise on liability of ISPs was reached, which over the years demonstrated it was providing a workable framework for Internet intermediaries and content owners. A key challenge of the directive though has been whether the protection of ISPs from general monitoring (Article 15) was adequate to protect all parties[8]. Nowadays, the largest ISPs, user generated content platforms and social networks of the western world are still abiding by the principles of the e-commerce directive, but they have developed a number of ways to improve the protection of their service, be it by making easier for content owners to report infringement[9], by developing

[8] Study on the liability of Internet intermediaries, 2007 : http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf

[9] Example of a large scale reporting system for copyright protection, and the controversies it generates (July 2016): http://www.musicbusinessworldwide.com/youtubes-content-id-fails-spot-20-40/

teams who assess and moderate contents[10], by implementing some proactive measures in the field of child protection[11], and by sharing information and reports on infringing activities through a national public-private platform[12].

As of today, 20 years after the Internet started to become available to the public, a lot of progress has been made in understanding the benefits and limitations of public/private cooperation, and existing best practices – including in the EAP region - validate the necessity of including public-private cooperation in any cybercrime strategy.

Still, **public / private cooperation** can be safely described **as a work in progress**, and no region of the world can pretend to have a reach a satisfactory level of maturity in this field.

Continuing with this logic, the result of this study shows that public / private cooperation is a challenge in the Eastern Partnership region, and this is not to be surprising. It also shows that some countries in the EAP region have already implemented initiatives which are essential for the future of any public-private cooperation, such as the adoption of a national cybersecurity strategies or the signature of a Memorandum of Understanding between authorities and ISPs.

The key expected outcome of the study was to assess whether there is a potential for developing such cooperation in the EAP region, whether the key elements necessary for a successful cooperation are present or can be implemented, and what factors could be detrimental to such success. How public / private cooperation can be developed in a sustainable way is the hardest question, and for this reason should be left to the – hopefully – next phase of the Eastern Partnership project(s) focusing public-private cooperation.

4.2 Trust as a general issue

When embarking on the development of public-private cooperation against cybercrime, the key issue is trust.

Trust is key, because almost every component of this cooperation – in this case against cybercrime and on the issues of electronic evidence in criminal cases – is more or less unknown:

- Cooperation and sharing of information among public authorities themselves is required and rarely developed in an initial phase;
- Cooperation and sharing of information among ISPs tend to exist in the field of cybersecurity, to protect from fraud and abuse, and in some countries in the field of business competition (typically when smaller ISPs join forces against the incumbent telecom operator), but it is rarely developed in the field of cybercrime;
- Cooperation between public authorities and ISPs may exist in the field of cybersecurity, but rarely in the field of cybercrime as interactions are typically regulated by laws and other norms;
- Topics for cooperation can only be determined on a case by case basis, through dialogue and sharing of information. Three main themes are most often used for public-private cooperation but they all have their limitations:
    - terrorism is matter of concern across the EAP region, but is better suited for a more traditional type of cooperation where assistance by ISPs is closely regulated by material and procedural laws;
    - combating sexual abuse of children online is well suited for cooperation due to the universal concern for the protection of children, but obtaining evidence of such abuse is not necessarily without cooperation of ISPs or until a landmark case of abuse has created public interest;
    - financial fraud and abuse of online services are likely to be the topic of greatest interest for ISPs, as they have both the technical expertise to detect the offenses and the financial motivation to devote time and resources to stop the abuse. This interest is not necessarily shared by the public authorities, due to the technical nature of the offences, and the complex schemes involved which are typically involving multiple participants operating from various countries.

[10] See an investigation on the situation of these human content moderators (May 2016): http://techcrunch.com/2016/05/31/terminating-abuse/

[11] Large providers such as Facebook and Microsoft have made public that they proactively detect and remove content of sexual child abuse published or distributed on some of their services: https://en.wikipedia.org/wiki/PhotoDNA

[12] See as an example in the field of spam and phishing : https://www.signal-spam.fr/english

Trust is the result of a long process. It starts with parties who do not know each other at the beginning have the willingness to work together for a mutual benefit. Trust may be achieved based on conclusions drawn from facts and results which are reached by similar evaluation of cooperation and experience.

In general terms, trust is developed and nurtured by applying some universal principles such honesty, persistency, transparency, alignment between commitments and actions, and providing to each parties a benefit that exceeds its investment.

Mutual understanding by all parties involved of the benefits they get is of value but not a requirement, as long as at least one organisation from each side (public and private sectors) understand the motivation and the benefits obtained by the other side.

In practice, each country deals with a unique situation in terms of history, law, economy and politics which may or may not provide to its people the opportunity to embark on public/private cooperation.

In the EAP region specifically, the experts found that there is a trust issue between the public and private sector, including in the countries which are already equipped with a Memorandum of Understanding between authorities and the ISPs.

The severity of the trust issue cannot be underestimated in the EAP region as in other parts of the world and will have to be recognised at the outset of the project.

The recognition of this issue may not be easy, but it will catalyse the implementation of the next steps. The next sections will provide a series of recommendations to prepare the ground for a successful cooperation.

4.3 Comprehensive cybercrime strategies as a starting point

The adoption of cybersecurity and cybercrime strategies is the first priority action listed in the "Declaration on Strategic Priorities for Cooperation against Cybercrime" adopted at the Conference on Strategic Priorities under the CyberCrime@EAP project in Kyiv on 31 October 2013[13], and it was among the first activities implemented. A regional workshop was held on this topic in November 2014 and a report on "Cybercrime and cybersecurity strategies in the Eastern Partnership region" was published in May 2015[14].

The signatories of the above-noted Declaration have rightfully highlighted the importance of such strategies in their declaration, and included the need to "Engage in public/private cooperation, including in particular in the cooperation between law enforcement authorities and Internet Service Providers" (page 5).

Three EAP countries have already adopted cybersecurity strategies, which can be used as a reference by the other countries, while no explicitly defined cybercrime strategies have been undertaken yet.

In 2013 at the time of the Kyiv declaration, cybersecurity strategies which had been adopted were motivated primarily by the protection of critical infrastructure from attacks (Estonia in 2008, UK in 2011). Since then, the range of motivations has broadened, from protection national sovereignty (France, 2015) to economic and social development (Gambia, 2016).

For the EAP countries, the development of cybersecurity and cybercrime strategies is therefore an opportunity to engage with the private sector, and develop a multi-stakeholder approach. This recommendation is consistent with those from the abovementioned report, in particular the following ones:

- "The private sector should be involved in elaborating cybersecurity strategies from the twin perspective of cybersecurity consumers and cybersecurity providers; they should respectively focus on major threats and not try to address all issues;" (page 41);

[13] Declaration available at: https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/CyberCrime@EAP/2523_EAP_Strat_Priorities_V7%20ENG.pdf

[14] Report available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803053d2

- "Cyber strategies should be open to insights from third parties with different knowledge and expertise" (page 41);
- "all national stakeholders from the public and private sector should be involved in the development, implementation and enforcement of a cybersecurity strategy. A National Cybersecurity Council, consisting of public sector entities (such as National Security Ministry of Interior, and Telecommunications Agency), private sector entities (banks, ISPs, telecommunication providers, international software and hardware companies) and academics could coordinate cybersecurity, while respecting and observing one another's interests. Such an approach should be supported by a legal framework setting out rights and obligations of all stakeholders, procedures for information exchange and modes of cooperation" (page 43);

Almost all EAP countries lack comprehensive cybercrime strategies, either as standalone document or by means of a section dedicated to cybercrime in a broader national strategy against crime or cyber security. The situation is similar to the one found in 2014 at the time of the report on cybersecurity strategies in the EAP region[15].

This makes possible for those EAP countries which are not equipped with a cybersecurity strategy, to develop a cybercrime strategy in parallel of or as a key pillar of a cybersecurity strategy, as they see fit.

In any case, there is no protection from threats and attacks against critical infrastructure and people without a criminal justice strategy.

4.4 Clear rules and procedures for law enforcement access to data held by private sector

"Establish clear rules and procedures at the domestic level for law enforcement access to data held by ISPs and other private sector entities in line with data protection regulations" is the first of the three recommendations of the "Strategic Priority n°7 : cooperation between law enforcement and Internet service providers" of the Kyiv Declaration of 2013[16].

It is indeed a key element of trust, and a challenge throughout the region, but it is important to be more specific on what "establish" means. Based on the results of the missions to the EAP countries, the finding is that the challenge is not only about the absence of rules, but more broadly about the difficult to be clear about what the rules are.

Before engaging in drafting new rules, the following preliminary work would be useful to consider:

- provide **official translation of the laws and regulations** in force, as it would help the national and regional community in the context of the EAP project to properly evaluate the current circumstances;
- **clarify the key definitions** of electronic evidence and categories of data, as it would help understand the exact harmonization status or opportunities with the Budapest Convention and the Guidelines.

It may be that this work will lead to call for a **legislative reform.** As some degree of legal reform is currently ongoing in all of the EAP states in relation to cybercrime and electronic evidence, the core issues of data retention regulations, implementation of all procedural powers under the Cybercrime Convention, and addressing the issues of safeguards and guarantees in the application of these could be very well taken onboard together with already ongoing efforts.

[15] "At the Kiev meeting (October 2013) participating EAP States93 affirmed their willingness to pursue cybercrime strategies to ensure an effective criminal justice response to offences against and by means of computers as well as to any offence involving electronic evidence. Georgia, the Republic of Moldova and Ukraine affirmed that actions against cybercrime are priorities of the cybersecurity strategy. However, none of the countries reported a specific cybercrime strategy in place. Georgia was the only country to provide information on cybercrime within its Organized Crime Strategy." (page 40)

[16] "**Establish clear rules and procedures at the domestic level for law enforcement access to data** held by ISPs and other private sector entities in line with data protection regulations. A clear legal basis in line with the procedural law provisions and the safeguards and conditions of the Budapest Convention on Cybercrime will help meet human rights and rule of law requirements. Guidelines3 adopted at the Octopus Conference of the Council of Europe in 2008 may help law enforcement and ISPs organise and structure their cooperation. Governments should facilitate the use of the expedited preservation provisions (Articles 16, 17, 29 and 30) of the Budapest Convention taking into account the results of the assessments by the Cybercrime Convention Committee."

Beyond criminal justice institutions, the recent development of data protection regulations and the establishment of privacy authorities shall be further encouraged. Independence, the necessary human resources support (legal and technical) and publicity are fundamental to maintain a **balanced data protection system** in a country.

4.5 Fostering a culture of cooperation between law enforcement and ISPs, including written agreements/memoranda

"Foster a culture of cooperation between law enforcement and ISPs" is the second recommendation of the "Strategic Priority n°7 : cooperation between law enforcement and Internet service providers" of the Kyiv Declaration of 2013[17].

The recommendation rightfully proposes the development of Memoranda of Understanding combined with regional coordination.

The experts found that the MoUs already signed in the EAP region were not readily available to third parties, even with some confidentiality requirements. **Availability of these non-binding MoUs** is an element of trust, especially when they are regularly updated, as it ensures that stakeholders and interested parties know the most recent status of these documents.

Developing and signing a Memorandum of Understanding between ISPs and law enforcement is an obvious way to show activity and produce some tangible deliverables. This being said, it is not the only way to develop cooperation, and it can even be counterproductive, in cases where signing the Memorandum is considered as the conclusion of a process instead of its beginning.

A constant issue, in the EAP region as in other countries, is the lack of **budget and expertise, and the fight for human and financial resources**. As in many other places in the world, in the EAP region the private sector is perceived as providing better salaries to their employees compared to the public sector, which makes difficult for the public authorities to retain experts - however the private sector is also fighting to keep resources.

Companies, ISPs in this case, operate in a competitive environment, and their primary objective is to generate sufficient revenues to pay their staff and retain customers. This struggle for revenue is actually a struggle for life: generating revenue is a constant concern which is not fully appreciated by authorities when they seek cooperation from the ISPs to protect the public interest. Both sides are operating in a completely different environment, and success is being measured in almost opposite ways.

To give a concrete example, a good business model for and ISP can be to sell pre-paid anonymous Internet access, which does not require administrative process and can generate a more comfortable margin. Obviously, anonymous Internet access can become a nightmare for law enforcement authorities as it can prevent the identification of offenders. Therefore, it can be tempting to forbid anonymous Internet access through mandatory regulation, and this can be perceived negatively by the ISPs. But such anonymous access, if it is not complemented by a series of anti-fraud and security checks, can become a gateway for cybercriminals and harm ISPs and their own customers. Ultimately, anonymous Internet access combined with some forms of identification or traceability can prove to be beneficial to all parties, ISPs, customers and authorities.

It is therefore recommended that for all requests between authorities and ISPs, **any decision takes into consideration the broader environment in which the stakeholders operate:** it is not sufficient to consider the immediate technical effectiveness of a given measure against cybercrime, the long term impact on the ability of the ISPs to operate its business must be considered as well. While this process requires more time, especially in an initial phase when both parties have little understanding of each other's constraints, it guarantees a much higher quality of the decisions.

[17] "**Foster a culture of cooperation between law enforcement and ISPs.** Memoranda of understanding between law enforcement and Internet Service Providers are a fundamental tool in this respect. Regional coordination of such MOUs would facilitate the ability of law enforcement authorities to conduct investigations across regional borders, with the knowledge that comparable standards have been adopted in other States. MOUs combined with clear rules and procedures may also facilitate the cooperation with multi-national ISPs and other private sector entities including in the disclosure of data stored in foreign jurisdiction or on cloud servers that are managed by these ISPs."

Regarding the budget limitations and how the private sector can have the capacity to recruit the specialised and trained professionals from the public sector, this trend – which can be seen all over the globe – has it benefits: it ensures that personnel with key skills and intimate knowledge of the public sector moves to the private sector. Over time, if the knowledge of such personnel is properly valued at national level, this trend can contribute to accelerate the mutual understanding between authorities and ISPs.

Last recommendation, **common education / development programs** with the attendance of the public and the private sector representatives may be of key importance, since this may not only facilitate the better understanding of each other's aims, but may also raise the common understanding of obstacles which is a first step for finding the joint solutions to work on: together.

4.6 Way forward: facilitate information sharing, even across borders

"Facilitate private / public information sharing across borders" is the third and last recommendation of the "Strategic Priority n°7: cooperation between law enforcement and Internet service providers" of the Kyiv Declaration of 2013[18].

In this recommendation, there are two elements which are recommended to be dissociated in order to be more easily implemented in practice: the private/public sharing of information, and the regional/international scale of the cooperation.

- Private / public sharing of information

  It may sound provocative in the context of this report, but it can be said that there is no such thing as private-public sharing of information, especially in the context of cybersecurity and even more in the context of cybercrime. The reason is simple: public authorities operate under very strict rules when it comes to the confidentiality of the information they process. Even in cases when they could share information on the cases they operate, they need to be careful and the culture of confidentiality prevents the sharing of information.

  Ultimately, the sharing of information tends to be one way: information flows (or is expected to flow) from the private sector to the public sector. In cases when the private sector has set up a process in place to report offences, as this happens in the field of content of sexual abuse against children, still the sharing of information may be a challenge: the police forces may be able to report back to the ISPs or the hotlines dealing with child abuse online what actions they have taken, but it is typically more challenging for the prosecutors to report back to the police and the private sector if they have initiated prosecutions based on the information which had been reported.

  The success of proven private-public sharing models, such as FIRST in the field of cybersecurity[19], CEOP in the UK in the field of protection against sexual abuse of children online[20], Signal Spam in France in the field of spam and phishing, are not based on symmetric or balanced sharing of information.

  The rationale for participating and the benefits obtained by private and public sectors are not identical, they shall even be of a very different nature: private sector provides data, knowledge, know-how that they have readily available, and the public sector contributes by a more effective response against the threats and guarantees that the cooperation remains focused on the general interest.

- Regional/international scale of the cooperation

  It has been demonstrated during the visits that some international service providers have already implemented cooperation with authorities of some of the EAP countries.

[18] "Facilitate private/public information sharing across borders. Private sector entities hold large amounts of data on cybersecurity incidents. The transborder sharing of such data would help improve the security of the information infrastructure as well as investigate offenders. Governments should consider legislation and the conclusion of agreements allowing for private/public information sharing and encourage the development of guidelines to facilitate the sharing of information intra- and transborder, including procedural, technical, legal and data protection safeguards."

[19] https://www.first.org/

[20] https://www.ceop.police.uk/

The information publicly available provides confirmation of our findings, but apparently to a more limited extent than the actual practice[21].

In the course of the EAP project, further sharing of information among EAP countries on their respective success in collaborating with international ISPs will provide further clarity on international practice vis-à-vis the EAP region. This will have two benefits:

- understand and improve the current practice with these companies, and
- serve as a benchmark for cooperation with ISPs at national and regional level.

- Ways and topics to improve both sharing of information and regional / international scale

In a situation where the trust has yet to be developed, a consequently managed and verified **statistical system on cybercrimes** is key in order to establish a roadmap with the necessary focus points to handle. Developing statistics on crime is not only a minimum requirement of any government, it is also an opportunity to create a virtuous circle in the cooperation between law enforcement agencies and ISPs to measure and combat cybercrime.

Both public and private sectors are familiar with the concept of measuring and producing statistics in order to define their strategies. This experience will provide the necessary common ground to kick off the collaboration. As cybercrime is a complex and multifaceted phenomenon, a public / private cooperation on statistics will enrich both sides on the trends that affect the region.

In terms of topics that are most likely to enable cooperation, it can be reported that **terrorism** is a well and openly focused topic in the region, however **crimes against children** within the cyber sphere must be addressed not only by legislative means, but also with the necessary publicity and awareness in order to reach goals and achieve results. As we mentioned earlier, ISPs are most concerned about **fraud** as it impacts directly their revenues. While strategically fraud may not be a top priority in a given EAP country, developing cooperation on fraud can be tactically an appropriate choice in a starting phase.

[21] Examples include https://www.google.com/transparencyreport/userdatarequests/countries/ and https://govtrequests.facebook.com/

Annex I. Country reports

[to be completed once revised/approved versions are provided by the countries]

Annex II. Repository of public-private cooperation projects in the Eastern Partnership

[to be completed once specific information is provided by the countries]