Updated version December 2017

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 programme in Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine

Partnership for Good Governance

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

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.

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

[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

which are typically involving multiple participants operating from various countries.

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:

[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

- "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);
- "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

[15] "At the Kiev meeting (October 2013) participating EAP States 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."

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.

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.

[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."

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.

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

[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/

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. 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

Armenia

Law and regulatory aspects

Armenia has signed the Budapest Convention on Cybercrime (ETS 185) on 23 November 2001, ratified the document on 12 October 2006 and it entered into force on 1 February 2007.

Main threats of **cybercrime** reported by the counterparts are hacking, DDOS attacks, malware financial embezzlements, distribution of pornography, misappropriation of computer data. Identity theft and fake invoice-related frauds are continuously growing (such invoices are being distributed via email to consumers).

The **criminal procedure** has three phases: preliminary, investigation and trial. There is no hotline or website for citizens to report cybercrime incidents, instead public usually reports directly to local police units. Police has 10 days from the crime is reported to do the initial investigation before deciding to either: i) close the matter, ii) send it to local police, or iii) hand the matter over to the Investigative Committee. It is possible to extend the 10-day period of the preliminary investigation phase in situations where police is awaiting the results of a forensics analysis such as the examination of a seized computer. The preliminary investigation is concluded with a decision to transfer the case to the court for indictment or termination of the criminal case.

The definition of **electronic evidence** is stated as "information stored in an electronic format". Definitions of categories of data (subscriber, traffic and content) are not defined. Armenian procedural legislation contains the notion of "material evidence" which relates to information about the crime, while ISP information which can be collected in the course of investigation without judicial order is interpreted as "other evidence" or "operational information" and cannot be used as evidence. Evidence cannot be obtained through a voluntary procedure but must be obtained through the legal process for securing evidence.

Procedural powers under Articles 16, 17 and 18 of the Budapest Convention (preservation and limited disclosure of data and production orders), as well as some specific measures related to search and seizure available under Article 19, are not directly implemented. Access to data is predominantly obtained through search and seizure proceedings. While the procedure used to be slow and paper-based taking up to two months to obtain needed evidence, the Memorandum of Understanding described later under the Informal Cooperation section has improved the situation and evidence is now obtained within a day or two. The draft Code of Criminal Procedure of Armenia reportedly includes measures on how to collect and archive electronic evidence, but is still at deliberation stage.

In terms of **safeguards and guarantees**, a judicial warrant is required for initiating investigative actions concerning correspondence, telephonic communication and other communications. Any record registered on electronic or other media which may provide relevant information may be used as evidence in a criminal case. There are also special regulations that require no court order if terror-related urgent investigation is initiated, however, an application for *post factum* court order needs to be filed within 3 days.

Stakeholders' roles and issues

With regard to **cyber security strategies**, on October 23, 2017 the President of the Republic of Armenia approved the order NK-146-A "On Approving the Concept of Provision of Information Security and Information Policy in the Republic of Armenia", which also includes the approaches regulating cyber security in the Republic of Armenia.

Meanwhile, a Cyber Security Strategy of the Republic of Armenia was developed by The Government of the Republic of Armenia and is under discussion, the purpose of which is to define the main directions of the Cyber Security Strategy, the necessary measures for sustainable development of the sector and the terms of their implementation, as well as the approaches to the creation of the Cyber Security Centre.

As an important milestone regarding countrywide strategic aspect, the Committee already developed a program about online gambling and the next one is being discussed to fight child abuse / child pornography. The government is currently developing the Digital Armenia 10-year strategy to promote e-government. The fight against cybercrime will be part of this strategy. Other aspects include the development of a digital National ID embedded in the SIM card of mobile phones. This Digital National ID could also be used potentially for identification in electronic commerce in addition to identification for government services.

The **Ministry of Justice** has a main role in developing the legislative framework and also the organizational tasks within the government sector regarding codification and the legal reforms. The Ministry is also a forum to generate informal cooperation between the public and the private sectors. The Ministry of Economy and the Ministry of Transport are active peers to the Ministry of Justice within the government.

The **Prosecutor General's Office** has the responsibility to control and to supervise the investigative procedures. In practical terms, if any investigative measure is applied unlawfully by the investigating entity, the prosecutor can impose disciplinary actions against the investigator; to date, no ISP has challenged requests for information during an investigation.

Cooperation with all national ISPs was considered good, although it was reported that the Office has issues with international providers only. Prosecutors receive technical support from the team of the Investigative Committee, and may also involve forensics and other experts. Two prosecutors are specifically dedicated to cybercrime cases at the Office.

The **High-Tech Crime Department of the National Police** is a centralized unit which is dedicated to handle cybercrimes with a country wide competency. Police has 10 days to determine the fundamental facts and the legal basis for the investigation itself and then deciding to either: close the matter; send case to local police where evidence or perpetrator is located; or transfer the matter to the Investigative Committee. Thus, the Department is the primary police unit handling cybercrime cases at the preliminary stage (before official investigation is opened by the Investigative Committee) and providing support to local units.

Cooperation with the service providers was reported to be good, primarily because it is almost always based on a judicial order; however, it was underlined that data retention is a problem due to law of regulation in the law and data was being kept for 6 months is merely good practice. There are different format in which informal cooperation between police and service providers takes place, such as working group at the National Assembly, non-regular meetings with the providers and Internet Governance Forum-related meetings.

95% of the criminal cases in Armenia are investigated by the **Investigative Committee**, others handled by specialized units for tax and customs fraud or investigations into public officials. The Committee has 3 investigators on staff dedicated to cybercrime cases. The investigator files the criminal case with the prosecutor and leads the investigative procedure. The Committee does not dispose of a computer forensics laboratory but instead will make use of external expertise for the analysis of electronic evidence.

The **National Communications Regulator** is an independent body, as provided by the Constitution of Armenia. No decision can be approved without the opposition representatives within its board. The Regulator has 55 members on staff. The entity covers television and radio regulation, but has **no role on regulating or supervising the internet**. At the same time, majority of television providers are becoming internet providers as well (the number of providers is beyond 100), thus legislation needs to follow up this tendency of the market.

Regarding the television broadcasting, all providers need to keep their program data for 1 month, with an exception rule at the parliamentary elections when this timeframe is prolonged for 3 months in the campaign period. The Regulator has a close contact and cooperation with the police and the Language Inspectorate, but certain government bodies may also have an effect on providers due to industry specific regulations (e.g. advertisements of pharmaceuticals: Ministry of Health). It is the court's competency to decide on breaches committed by providers (fines are imposed generally, but the license may be revoked as *ultima ratio*).

The **Data Protection Authority** (DPA) is quite new, since it was set up on 9 October 2015 based on the initiative of the Prime Minister. The Commissioner of the Authority is appointed for 5 years by the Ministry of Justice pursuant to a list of candidates established by 5 non-governmental organisations. The decision to choose the Commissioner is made with the

support of the Prime Minister. The Commissioner can only be relieved of his position on predefined exceptional grounds. The DPA has a staff of 10 persons, including a technical expert for any needed forensics investigations, who is undergoing technical training.

Decisions made by the Authority are binding on public and private entities. Commissioner can receive complaints or open an investigation at own initiative. The DPA can receive complaints from the public. Complaints have insofar not concerned the use of personal data by ISPs or law enforcement authorities and instead concern the use of personal data for advertising and marketing purposes without the consent of the data subject. The Authority is entitled to impose fines (in the value of 100€ to 1000€) in cases of breaching the relevant regulations. Sanctions such as the deletion of data can be enforced by court marshals. It also holds regular consultative meetings with the ISPs. Currently it is being debated whether the topic of freedom of expression shall belong to the Commissioner.

Armenian legislation does not include exemptions for the processing of personal data for the prevention, investigation, or prosecution of criminal offenses as included in the CoE Convention 108, article 9 ("the suppression of criminal offences", and "protecting the data subject or the rights and freedoms of others"), or the EU Directive 95/46 article 13.1.(f) "the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions". Not having an explicit exemption could make the processing of personal data with the purpose to reduce cybercrime more burdensome.

The **national CERT** - CERT.AM - is a part of the Internet Society of Armenia, being a non-governmental entity but already has a good and active working relationship with the police. One of the main tasks of the CERT is managing the root of the .AM top-level domain system, and to support the government in case of requests.

The CERT regularly provides Internet Access Providers with information about problems on their networks such as amplification attacks. Response from smaller ISPs compared to the main market representatives (such as Beeline, MTC, Vivacell, Ucom) is better, although the access providers do not take action on the information and not engage with CERT.AM for vulnerability testing of their networks.

Since there were no separate meetings with **Internet Service providers** during the visit, majority of the information about their operation comes from government entities. The data security of the 3 major ISPs is very high according to the Data Protection Authority.

There are over 100 ISPs working in the country including five major landline internet access providers and three major mobile carriers.

An electronic communications license is needed if a new ISP intends to enter the market and plans to build an own system. The license includes a provision requiring ISPs to comply with requests to remove unlawful content. In this respect a tentative business plan and a draft infrastructure model must be presented. The general timeframe to receive such a license is 10-23 days. No such license application was yet rejected. Mobile telecommunication carriers are expressly determined as ISPs.

Data retention is not clearly defined for ISPs: data is generally kept between 6 months – 3 years of time as a matter of good practice (telephony related data is being kept for 5 years). Because of the exhaustion of IP-addresses (type 4 IP addresses) operators are resorting to carrier-grade Network Address Translation for backward compatibility instead of moving new users to an exclusive IPv6 address space. The NAT log files from the ISPs' routers are exhaustive for users on that technology and in those situations, where an IPv4 address was shared amongst up to 255 different customers, it can be difficult to identify the point of communication.

ISPs have a strict and prompt cooperation obligation with law enforcement in case of a terror threats (a post filing of the court order shall be made by the authorities within 3 days).

ISPs don't have responsibility for content management, only in case they become aware of an illegal activity, in which case they have an obligation to report to the law enforcement authorities.

Informal cooperation

On 23 November 2015 the Investigative Committee signed a **Memorandum of Understanding** with ArmenTel, K-Telecom, UCom, Orange Armenia with the intention of workload reduction and human resources saving.

The main intentions of the Memorandum are: to take effective joint measures in the direction of operative transmission of court decisions and transcripts, and to develop the mutual cooperation on introduction of technical capabilities. In this framework, parties agreed to communicate on a standardized manner (including cover letters, electronic signatures) and agreed to cooperate in solving issues as soon as possible in case of such procedures. Furthermore, the signing providers agreed to process electronic transmission of the Investigative Committee within a short period of time and also to execute expeditiously court decisions which are designated as "urgent". A second objective of the Memorandum is to ensure that Internet Access Providers retain traffic data of their users for a period of time. Currently Armenia has no data retention legislation.

The Memorandum was reported by law enforcement stakeholders to be working well, which was also confirmed by the Prosecutor General's Office. Practically a same day request-answer working model is achieved by the Memorandum. It was also noted that this result of the public-private partnership is a key milestone, since the general intention is to develop legislation according to the contents of the Memorandum.

There are no immediate plans to expand the memorandum to include more companies or additional sectors such as payment processors or banks.

In terms of other types of public-private dialogue, private sector stakeholders are invited on an occasional basis to the Parliament's relevant committees in order to provide their inputs. There is no established forum with regular meetings to exchange information on problems in cybersecurity. Instead meetings are organized on a case by case basis.

The Government is interested in working with the private companies, in particular for the Digital Armenia 10-year plan on providing a unified approach to government services. There is interest to work internationally with the private sector abroad because of the international aspects of cybersecurity.

Academic institutions play an active role in **education** on cybercrime; moreover, they also support the work of the police on an occasional basis.

Regarding the education mechanism between the public and the private sector both Microsoft and CISCO are regularly providing cooperation or attending forums to support the authorities with the latest developments in the topic.

Police supports state owned television programs which focus criminal topics also on cybercrime in order to raise public awareness. Private television stations also broadcast programs which are raising awareness on cybercrime. Schools regularly receive education classes by police on the topic.

The cooperation on data has a purpose to remove any friction in obtaining evidence under legal process. It does not seek facilitating the exchange of facts outside of the legal process.

Although factual information related to an investigation can be shared informally, such facts obtained outside the legal process cannot be considered evidence in court. Their use is not unlawful, but is considered "operational information" which may be used to direct the investigation. If the information is needed for prosecution, it must then be obtained through a legal process.

Azerbaijan

Law and regulatory aspects

On 30 June 2008, Azerbaijan signed the Convention on Cybercrime. The country has ratified the Convention on 15 March 2007 and it entered into force on 1 July 2007.

The main categories of **cybercrime** offences detected in the country are DDOS attacks, malware and misappropriation of computer data. Attacks against mobile phones (e.g. Android smart phones) are continuously growing. The annual average number of crimes committed in relation to the cyber sphere is reported to be particularly low: two investigations per year have been reported in some recent years.

In terms of **criminal procedure, t**wo law enforcement entities are appointed to investigate cybercrime related cases: State Security Service and the Police under the Ministry of Interior. As a general rule, no evidence may be requested without a court order; however, in cases where human life or health is endangered (or the procedure is focused on deceased persons), law enforcement investigators may request prompt cooperation from the ISPs and request data from them in an urgent manner based on the high interest the investigation. In such cases a legal safeguard is also implemented, since such data may only be evaluated as evidence in a criminal procedure once prosecutor will applies to the court to approve the legal basis of such urgent action. The approval may be granted by a judge within 48 hours.

No definitions of **electronic evidence,** as well as categories of data (subscriber, traffic and content) are not defined in the criminal procedure or other laws of Azerbaijan.

Procedural powers under Articles 16, 17 and 18 of the Budapest Convention (preservation and limited disclosure of data and production orders), as well as some specific measures related to search and seizure available under Article 19, are not directly implemented. Access to data is predominantly obtained through search and seizure proceedings.

In terms of **safeguards and guarantees**, a judicial warrant is required for all types of evidence gathering relevant in the context of the Budapest Convention. In cases of urgent requests by the law enforcement entities, the court must approve the collection of data to be used as evidence within 48 hours after the request is made, otherwise it may not be used as legitimate evidence in the criminal procedure.

Since spring 2017 authorities of Azerbaijan have been analysing possible amendments to the legislation, in particular Criminal Procedure Code with a view to bring legislation on procedural powers fully in line with the Budapest Convention. Workshop organised by the Council of Europe on procedural powers including definition of electronic evidence, categories of data, data preservation and disclosure, took place in May 2017. Although most of the procedural measures of the Budapest Convention have been implemented, there are still gaps and amendments to legislation are needed. Retention of telecommunications data is not foreseen by the legislation and telecommunication service providers have no obligation to retain data. Although providers keep certain data which are needed for billing purposes and provision of services, it might not be sufficient. Retention of data seems also to be a problem for smaller providers who do not have necessary capacity including technical equipment.

In addition to Criminal Procedure Code, Law on Operative and Detective Activities is often used as a legal basis for procedural measures. As it is not always clear which legislative act should be used as a basis for measure, clarification and necessary amendments could be necessary to bring also conditions and safeguards in line with the requirements of the Criminal Procedure Code. Although more intrusive measures like real-time interception are covered, there are gaps with regard to geo-location or identification of location of persons.

Stakeholders' roles and issues

There is no **dedicated strategy** or other specific policy documents on cybercrime currently available or being developed in Azerbaijan. In terms of cybersecurity, Azerbaijan has an information society strategy which encompasses most aspects of a cybersecurity strategy ("National Strategy of the Republic of Azerbaijan on the Development of the Information Society for the period 2014 -2020"). The corresponding section 5.6 of the Action Plan on

"Ensuring information security" notes regulatory framework review, monitoring of the Internet, ensuring safety of e-government infrastructure, and enhancing cooperation with information security agencies worldwide as main directions of action in this regard. The State Agency for Special Communications and Information Security and the Electronic Security Centre are primary bodies for cybersecurity matters.

The **Ministry of Justice** has main role in developing the legislative framework and also the organizational tasks within the government sector regarding codification and the legal reforms. The Ministry is in cooperation with the State Security Service and the Ministry of Communication and High Technologies in order to continuously evaluate and, where necessary, develop the legislative basis of the fight against cybercrime; no specific ongoing projects related to cybercrime/electronic evidence were reported though.

As the Ministry of Justice is responsible for legislative policy development and drafting new legislation, it cooperates and consults also with private sector. There are different committees and working groups where private sector entities have appointed their representatives. When draft laws are being elaborated, private sector is consulted and debates take place. Draft laws are also publicly accessible at the National Assembly website and private sector has possibility to participate in the process and submit opinions and comments.

The **Prosecutor General's Office** has the responsibility to control and to supervise the investigative procedures. The Office exercises supervisions over law enforcement authorities which are entitled to investigate cybercrimes: the State Security Service and the Police (as a part of the Ministry of Interior). In police investigations, prosecutors are assigned to cases on the basis of regional jurisdictions (no specialized prosecutors for cybercrime cases). In case the State Security Service is investigating, the General Prosecutor's Office has direct supervisory authority.

As there are no specialised prosecutors for cybercrime investigations, this should be considered in the future. Still, basic training on electronic evidence and procedural measures addressing computer data should be made available for every prosecutor.

The **Ministry of Internal Affairs** is supervising the Police which is one of the law enforcement entities entitled to investigate cybercrimes beside the State Security Service. Unfortunately, the division of tasks with the State Security Service is not clear since it is the SSS which is deemed to be the specialized cybercrime investigation agency. Although there is no clear borderline between the competences, the mandate of the Security Service includes fight against serious crime as well as crime against the state. In coming years, the Ministry expects to have more prominent role in investigating cybercrime offences. An internal digital forensic team is supporting the work of the Ministry.

If law enforcement authorities receive information that could be useful for private sector for information security and crime prevention purposes, it is possible to inform relevant private sector entities as well. In certain cases, disclosing information to private sector entities that would enable them to prevent their computer systems and take preventive measures against cyber incidents is mandatory.

Similar obligation is foreseen also for private sector entities, which have obligation to report crime. In case of serious crime, non-reporting would result in criminal liability. Reporting may take place by submitting written reports as well as reporting via website. In addition hotlines have been created to facilitate and encourage reporting of crime.

Although cooperation between public and private sector is considered essential, no periodical consultations, roundtables or joint trainings take place. Even if cybercrime has taken place often private sector entities refrain from reporting. Therefore confidence building or cooperation should be strengthened in order to encourage reporting on one hand and facilitate everyday cooperation and information exchange on the other.

Azerbaijan is also involved in international cooperation. Cooperation takes place mostly with Russian Federation and Turkey. From international organizations there is close cooperation with GUAM.

Cooperation between multinational service providers is considered important as well, however there are problems concerning receiving information from them.

Regarding ISP cooperation, the Ministry regularly has bilateral meetings with the Ministry of Communication and High Technologies in order to seek development opportunities in the field of fighting cybercrime.

The Ministry of **Transport, Communication and High Technologies** is the government entity that is supervising telecommunication, information society, e-government, postal services, radio / television services, and personal data as well. It is also the main driver to in the process of evaluating and adopting legislation to the changing needs of the country and the industry as well. In this framework the Ministry has recently developed draft legislation in order to request ISPs to register for quality assurance and consumer protection reasons.

While its role as a communications regulator was more or less clear, it is yet to be determined what role does the Ministry or its entities have in protection of personal data.

Ministry of Communication and High Technologies has also established cybersecurity board to involve ISPs in legislative process and express opinions on draft texts as well as sharing information about threats and trends related to cybersecurity. Meetings with private sector entities take place occasionally and there is also a mailing lists on points of contact to disseminate information.

The national cybersecurity team **CERT.GOV.AZ** is a government entity that is established under the Ministry of Transport, Communication and High Technologies. It is a member of FIRST and Trusted Introducer. A high level of international cooperation / knowledge sharing was reported with: Iran, Bulgaria, Russia, Ukraine, Kazakhstan and Georgia.

The main role of the CERT is to define / detect cyber threats and to collect / analyse data in order to serve the interests of the public and the private sector as well. CERT is also active in education and presenting threat awareness information on its website (social networks as well) and also offline (flyers, booklets). CERT has a hotline (+1654), which is generally provided for anyone, but applied mostly by private individuals.

Azerbaijan has above 50 **Internet service providers** in total (including wholesale, retail and also mobile providers). No license is needed for ISPs since 2000.

There is an association of ISPs in the country since 2001. Not all providers are members, but above 70% of them are being active in it.

Formal cooperation between the ISPs and the law enforcement is continuous and regular. Practically all requests are properly answered by the ISPs; no issues were reported by the law enforcement. This is primarily due to the fact that ISPs have a responsibility to cooperate in criminal procedures: in this frame the general manager of the ISP may also be held liable under criminal law.

Data retention model is not unfirm: data is stored for 3, 6, 18 or 24 months in various models. Currently it can be stated that subscriber ID sessions and IP fingerprints/artefacts are being stored by the providers. The data retention and preservation model needs legislative clarification in order to support stability and predictability on the market.

ISPs don't have any responsibility regarding the stored / transmitted data and they do not investigate the data about their lawfulness. However, if an ISP finds out that information is illegal on their network, they must report it to the law enforcement. ISPs may only block traffic if a court order is provided to them accordingly.

Informal cooperation

No **cooperation document** is signed or being negotiated between the stakeholders of the public and private sector spheres. In fact, the ISPs are expected to cooperate with the law enforcement on the basis of law and regulations, and informal cooperation is not viewed by the authorities as a necessary or desirable mechanism of cooperation. However, public and private sector stakeholders are reported to be regularly communicating at the Ministry Communications and High Technologies, with responsible Deputy Minister being personally involved in the dialogue. Most stakeholders reported limited to no knowledge of the "Guidelines for the cooperation between law enforcement and internet service providers against cybercrime" (2008).

Although the overall level of cooperation is good, there are still problems due to gaps in legislation, in particular due to the lack of the definition of electronic evidence, definitions for different categories of data and specific procedural measures that would address data preservation and disclosure.

On the other hand, the national cyber security team CERT.AZ covers informal cooperation with ISPs and cooperates with them on initiatives involving regular **education** in schools and providing **information on threats** of social networks (e.g. Facebook). Despite this, no countrywide mass media awareness projects are being reported.

At the moment there are no MoUs concluded with the ISPs. There are plans to introduce them in nearby future.

Belarus

Law and regulatory aspects

Belarus has not signed the Budapest Convention on Cybercrime (ETS 185). Several stakeholders have reported their vision to enter the Convention within 5 years of time (until 2021).

Main threats of **cybercrime** reported by the counterparts are ransomware, DDOS attacks, malware and financial embezzlement. Crimes against children are of a rising concern for criminal investigations. It must also be noted that that foreign country attacks through cyber measures are also reported. The annual average number of crimes related to information technology is 2000; however 2015 showed a significant growth reaching nearly 2400 cases.

The **criminal procedure** has three phases: preliminary, investigation and trial. The judge oversees the full criminal investigation phase and may provide judicial control over the prosecutor as well, who is responsible for controlling of the procedures of the law enforcement bodies in charge with the criminal investigation.

The definition of **electronic evidence** for the purposes of criminal proceedings is not implemented in national law (legislative reform is expected on electronic evidence in 2017). Definitions of categories of data (subscriber, traffic and content) are not defined; however, despite the lack of definitions, it was reported that ISPs must keep data (subscriber, traffic and hosting data; content data is also reported to be stored but could not be verified) in the timeframe of 12 months. ISPs may keep the data for 3 years as a maximum. This is fitted to the statutory limitation period. ISPs are not required to delete data after the prescribed deadlines. There are however exceptions in here as well: traffic data related to telephone conversations (subscriber, invoicing, source and destination numbers, duration) are kept for 12 months, however national provider Beltelekom keeps data for 5 years of time (the company is the main hosting provider as well in the country).

Procedural powers under Articles 16, 17 and 18 of the Budapest Convention (preservation and limited disclosure of data and production orders), as well as some specific measures related to search and seizure available under Article 19, are not directly implemented. Access to data is predominantly obtained through search and seizure proceedings. The Investigation Committee may request data - in the pre-investigative phase - from the ISPs without a court order / judicial warrant (e.g. for identifying an IP address). In such cases, a copy of the request is placed at the General Prosecutor's Office who shall oversee the investigation procedure.

It has to be specifically noted that the most fundamental legal text – in addition the Criminal Code and the Criminal Procedure Code – that regulates law enforcement access to data is order Nr. 60 of the President (Presidential decree) from 2010, which was amended in 2013. Presidential Decrees in Belarus have the same legal standing as an Act of Parliament. The presidential decree obliges ISPs to retain traffic data for one year and subscriber data for 5 years. Presidential edict 129 provides more detail on which data has to be collecting such as all billing information. The basic subscriber information can be accessed by the ministry of interior, the investigative committee, the Operative and analytical center under the president, and the KGB.

In terms of **safeguards and guarantees**, even though some of the elements limiting and controlling the application of more intrusive measures, such as search and seizure, real-time collection of traffic data and content interception, are present, lack of judicial authorisation remains an important concern with regard to highly intrusive procedural powers. Against this background, the secrecy of communication is recognised in the law, which also includes the secrecy of electronic- and telecommunication. From the organizational and application point of view it is the Department of Informatisation at the Ministry of Communications and Informatisation which is supervising data protection in the country. Legislation on data protection is being currently developed and is at the concept stage.

Evidence needs to be obtained through legal process or the judge must reject it and deny it admissibility. Evidence obtained from foreign ISPs are directly admissible in court through Law 103 which allows law enforcement to send requests directly to a foreign ISP if the preliminary information shows that obtaining the information is worthwhile for the investigation. This

legislation has been been used to request information from the company Paypal and the replies received from the company were used in court. In total about 300 requests have been made to entities abroad, 10 replies have been received in total from companies like Apple, Facebook, and Paypal.

Stakeholders' roles and issues

There is are no dedicated **strategies** or other specific policy documents on cybercrime currently available or being developed in Belarus. The National Security Concept of Belarus, approved by Decree No. 575 of the President of Belarus on 9.11.2010, defines information security as a condition to protect the balanced interests of the individual, society and the State from external and internal threats related to information and identifies information security as an independent component of national security. Presidential Decree 98 of 2016 concern network security and is part of national cybersecurity plan.

The **Ministry of Justice** has a main role in overseeing the legislative framework and also the organizational tasks regarding codification and the legal reforms. The Ministry also supervises the expert board which has a key role in evidence and forensic work.

The **Prosecutor General's Office** has the responsibility to control the investigative procedures and at the same time the prosecutor's may issue requests to the ISPs in order to provide them subscriber and traffic information. Prosecutor's Office also has the primary responsibility for international cooperation on cybercrime and production of statistics on crime. Mutual legal assistance procedures are implemented and are applied by the Office. Belarus generally initiates between ~300-400 procedures (mostly subscriber information) and receives ~10 annually from foreign countries. It was reported that mutual legal assistance procedures initiated by Belarus are not considered as efficient in many cases. The prosecutors are looking at the possibility to join an international information exchange forum of hi-tech prosecutors to ensure that they can keep up-to-date with the latest forensics information relevant for prosecutors.

The **Ministry of Internal Affairs** has a dedicated High Tech Crimes Department. The Department has 30 officers specialised in cybercrimes and 3 specialists as well in each of the country's 6 counties. They had about 2000 IT related cases from January to September in 2017 and they expect to have about 2500 cases or more than last year. 70% of the cases concern fraudulent withdrawals of money from ATM machines through forged credit cards which are prosecuted as theft. The remaining cases mostly concern unauthorized access into computer systems through hacking and other types of information security crimes. Due to the fact that there is an active system which is connected via a secure channel (VPN) to the ISPs, law enforcement agencies are able to receive information within 5 minutes if needed. The system is provided on a no cost basis for the authorities. Seizures of computers can be carried out under the law on investigations without a court order from a judge. The Ministry of Internal Affairs manages the pre-investigation phase for 99% of the cases. The pre-investigation phase can last for a maximum of 3 months before the case is passed on to investigation with the investigative committee.

Since 2012 the **Investigative Committee** is an official independent investigative authority of the Government. The Investigative Committee investigates about 99% of all crimes, including cybercrime. The Investigative Committee has a website where citizens can report cybercrime. Although the Investigative Committee sets out which information should be sought, the search orders are generally carried out by the Ministry of Internal Affairs. Good cooperation was established with the US Federal Bureau of Investigation (FBI) and the German Federal Criminal Police Office (Bundeskriminalamt).

The **Ministry of Communications and Informatisation** is the national regulator in charge of developing the relevant legislation. It is their responsibility to put the legislation into practice. It was reported that Ministry's main aim is to develop the regulatory framework with continuous communication with the private sector. The Ministry set up the State program on Informatisation and on "Electronic Belarus" which both played key roles in the cyber domain. Transferring data over the Internet is a regulated activity that is allowed by a license under the supervision of the Ministry.

The Department of Informatisation within the Ministry is currently dedicated to supervise data protection issues. The Ministry also has a dispute resolution role between the ISPs and the

subscribers. The subjects of the disputes generally include tariff related / invoicing- and technological issues and do not relate to law enforcement

The **Inspection on Communication** is a government entity is analysing and gathering the illegal information on the Internet. The Inspection manages and supervises the access of all ISPs in the country (~150) and continuously keeps a list of hackers active in relation to the country.

The **Operational and Analytical Centre** is an institution founded by the President and remains under presidential reporting as well and has mandatory powers to act in its field. The Centre's main role is to organize the cooperation related to ICT within the government sphere and its key focus areas are internet security, the support and supervision of critical infrastructure (both public and private), and the regulation on cryptography. They have cooperation on an international level as well if an attack has a cross border effect, but this is only in reactive mode and not regular. The government cloud project (G-Cloud) is managed in the BeCloud framework.

The **national CERT** under the OAC manages and handles the cyber security threats and incidents which may occur in relation to the public and the private sector users as well. The activity is set up the way that they don't only focus on reactive measures, but also on proactive approaches. The entity has a staff of 12 professionals on board. They are entitled to develop their own by-laws. Their practice on international knowledge sharing is generally done by Ukrainian, Russian, Kazakhs and Polish CERT peers, but Estonian, Canadian and Tajik best practices are also relevant for them.

The CERT has regular private sector oriented cooperation as well: KASPERSKY LAB and SYMANTEC were reported in this respect.

There are about 150 **Internet Service providers** working in the country. It shall be noted that before 2010, servers were generally outside of the country's borders. Based on Presidential Order Nr. 60 ISPs are currently not allowed to provide any services from outside of the country. Now all of the hosting is under the supervision of Beltelekom and all providers are in the system of the United Data Transit Network.

ISPs are liable to store the data for 12 months of time and if they fail to do so, their license may be revoked.

Data transmission is a licensed activity. In case the licensing regulations are breached, the Ministry of Communications and Informatisation may initiate an injunction against the ISP. Further breaches may result an administrative fine which is imposed by the court.

The Technological Association "**InfoPark**" is based on the idea of the academic communities and it was founded by a President with the support of 8 institutions (including the Institute for Informatics). The aim of the Association is not to especially develop own practices, but to implement best practices and standards (e.g. ISO 27000 in 2005). Infopark is highly focused on cryptography, on testing of such products and also on issuing of certificates. The three main objectives are: i) cybersecurity, ii) identifying critical information infrastructure, iii) setting up a CERT. It acts as a platform to discuss problems and to identify joint solutions. It originates from the academic world but they act for the needs of the private sector. One of the projects is working on is the support of the EU IDAS regulation by suggesting harmonization of legislation and uniform standards on information exchange for digital signature certification authorities. Infopark made an analysis of crimes in the country and identified 600 cases of which ¾ were related to malware, mostly ransomware. However, some individual cases had many hundreds of victims.

Informal cooperation

There are no specific informal cooperation m mechanisms directly between the law enforcement and ISPs; the latter are expected to comply with requests from the former, making the concept of informal cooperation somewhat less relevant. It is possible to sanction entities which do not comply with requests and there have been cases where sanctions were applied.

On the other hand, the banking sector, the law enforcement authorities, the Ministry of Interior, the investigation committee and the General Prosecutor's Office regularly organize

round tables and conferences on cybercrime issues, which resulted in a Memorandum of Understanding by the parties related to financial crime.

The Scientific Academy is active in supporting and organizing conferences on cybercrime. Such events are visited by both public and private sector stakeholders.

The Internet Governance Forum was held in Minsk on 17 May 2016, which gave the opportunity to the private sector, the NGOs, the academic era and the public sector representatives to meet and share their views on current trends and challenges. The forum is also supported by ICANN.

Educational sessions are being regularly held by the Academic Society for law enforcement agency members and civil servants as well. Regular education is also being provided in the framework of the Ministry of Interior's Academy and it is also supported by the Minsk University. The next step for educational programs is to focus on the judiciary bodies.

As a related recent development, the Law on Public and Private Cooperation Regarding Infrastructure Development was adopted in 2015. The main principles of this act are rule of law, effectiveness of public-private partnerships, the priority of public interest and publicity. It also focuses on technical resources and infrastructure development.

Although Belarus law enforcement is allowed to request information from foreign entities and use any obtained replies as evidence at trial, the opposite is not possible. Belarusian ISPs, when they receive requests for information from abroad, have to reject these as any evidence provided abroad has to go through the national legal process for disclosure.

Georgia

Law and regulatory aspects

Georgia signed the Budapest Convention on Cybercrime (ETS 185) on 1 April 2008, ratified the document on 6 June 2012 and it entered into force on 1 October 2012.

Main threats of **cybercrime** reported by the counterparts are hacking offences combined with requests for ransom (this type of fraud has been discussed in details at the meeting with the National Communications Commission), phishing, online financial frauds, online distribution of fake invoices, attacks against cloud systems and misappropriation of computer data. Terrorism is dealt by the Security Service. Child abuse has low reported statistics in Georgia: there was only 1 case reported in 2015.

The **criminal procedure** has two phases only: investigation and trial. Judge's role in the investigation process is limited to the authorization of intrusive measures and review of challenges to investigation and prosecution conduct by affected parties; it may also provide judicial control over the prosecutor, who is responsible for control of the procedures of the law enforcement bodies in charge of the criminal investigation. The prosecutor needs to apply for a court warrant in case data is required as evidence for an investigation; notably, the defence has the same rights as prosecution to obtain production warrants from the court. The judge must provide his/her answer on this request within 24 hours of request from the prosecutor. In some cases (such as terror threats) the judicial warrant may also be issued *ex post*, however the filing of the application must be within 24 hours by the prosecutor. There is no need of preservation request in cases of urgency when a local ISP is being addressed. In such cases immediate access can be granted (supported with the above mentioned *ex post* judicial supervision).

The concept of **electronic evidence** for the purposes of criminal proceedings is recognized in the Code of Criminal Procedure as one of the valid forms of evidence (information in electronic format). Definitions of subscriber information and traffic data are implemented in the Georgian CPC, while content data is interpreted to include the content of communications. Despite this, Georgia does not make a distinction between categories of data and procedural powers that apply to them.

Procedural powers under Articles 16 and 17 of the Budapest Convention (preservation and limited disclosure of data), as well as some specific measures related to search and seizure available under Article 19, are not directly implemented. Access to data is still predominantly obtained through search and seizure proceedings.

As of 2017, Georgia is in the process of amending Criminal Procedure Code in order to review the legislation on the procedural measures, in particular production order. Specific workshop on legislation organized by the Council of Europe took place in February 2017.

On March 20, 2017, the Parliament adopted new Operative Technical Agency Act which provides for new rules on **data retention**. Data retention is now possible for 12 months subject to the extension for 3 additional months upon the judicial warrant. The following data can be retained: subscriber information; information indicating the communication's origin, destination, time, date, size, duration and type of underlying service, information identifying or tentatively identifying device, information identifying the location of mobile device.

Data retention is executed by the newly established Operative Technical Agency. The new law has introduced a bunch of independence safeguards for the new agency. However, a new Constitutional litigation has been launched concerning the powers of the agency.

In terms of **safeguards and guarantees**, Articles 137(3) and 138(3) of the Criminal Procedure Code respectively extend the priority of less-intrusive measures rule to the real-time collection of traffic data and content interception powers as well. This applies also in relation to secret/covert investigative measures (Article 143^3 of the Code of Criminal Procedure). Beyond that, under Article 6 of the Code there is an overarching principle of the priority of less intrusive measures which applies to all procedural powers, including search and seizure. However, limitations under article 137.3 and 138.3 are far more specific and demanding.

The Law on Personal Data Protection is in force for the public sector since 2012 and for the private sector since 2014. It is based on the Constitution of Georgia adopted in 1995.

Stakeholders' roles and issues

Georgia has a **Cyber Security Strategy** which was initially developed in 2012 by the Permanent Inter-agency Commission within the framework of the National Security Council. Cybercrime-related provisions that were initially present in the Georgian National Cybersecurity Strategy and Action Plan 2012-2015 are now entirely absent from the recently adopted (13.01.2017) Cybersecurity Strategy and Action Plan for 2017-2018, which focus entirely on cybersecurity research, regulatory framework, capacity building, awareness and international cooperation.

Georgia recently introduced an updated Strategy and Action Plan on Organized Crime 2015-2018, both of which contain separate sections dedicated to cybercrime. Although the titles of these documents would suggest otherwise, the issues therein go beyond organized crime matters and address cybercrime threats and planned responses in general. Sections 20 to 30 of the Organized Crime Action Plan refer to increasing public awareness, development of substantive and procedural law, increasing capacities of state agencies combating cybercrime, public-private partnerships and international cooperation as major areas of activity planned in the short term until 2018.

The **Ministry of Justice** has a main role in developing the legislative framework and also the organizational tasks within the government sector regarding codification and the legal reforms. The Ministry is also a forum to catalyse cooperation between the public and the private sectors; it also had a role in developing the Memorandum of Understanding between the law enforcement authorities and the ISPs in 2009 and 2010.

The **Prosecutor General's Office** has the responsibility to control and to supervise the investigative procedures. Cybercrime related investigations are based on the Criminal Procedural Code, meaning no specific regulation was introduced in this respect. Prosecutors must show probable cause in case of search and seizure. There is only one prosecutor on staff who is especially focused on cybercrime issues. There is a current legislative reform draft about the access of subscriber data only by prosecutors.

Volume of requests sent by the Office to Georgian ISPs is 30 to 40 per month. Some foreign operators do respond to requests, for instance Facebook alone received requests related to 35 users in the sole month of May 2016; however, the patterns of intensity of sending requests to international ISPs change very often. General trend is that the number of requests increases.
It is also of note that Georgia has fairly high disclosure rate of data from foreign providers as compared to global average. E.g. in the second half of 2016, Facebook disclosure rate was over 90% for Georgia whereas the global average was between 60 to 70%.

The Prosecution Service Strategy and Action Plan 2017-2021 prescribes the following strategic actions prescribed in respect of cyber-crime and public-private cooperation:

- Set up of new inter-agency cybercrime policy task force - first meeting held in 2017;
- Review the existing LEA-ISP MOU and introduction of amended one if need be – some initial discussions held in 2017, further works will be continued in 2018;
- Participation in and/or initiating procedural and substantive law reforms on cybercrime and electronic evidence issues – a new legislative initiative has been introduced in 2017, which intends to amend production powers and introduce preservation powers, with Prosecution Service participating in the process; substantive law reform intends to further modernize cybercrime elements and is about to launch and the Service will be one of the key actors in the process;
- Training of prosecution attorneys in cyber related matters (procedural powers, international cooperation, cooperation with service providers) – in 2017, over 90 prosecution service staff participated in 6 international and local trainings/seminars on cybercrime and electronic evidence;
- Introduction of policy guidelines on the cooperation with ISPs - in 2017 a draft of the guidelines has been prepared based on the Council of Europe 2008 Guidelines, with document expected to be approved in 2018.
- Issuance of Manual on the LEA direct cooperation with Multinational Service Providers – the first version of the manual was prepared in March 2017 and has been updated several times.

The **Ministry of Internal Affairs** has a dedicated Cybercrime Unit within the Criminal Police Department. The Cybercrime Unit was founded in 2012 and currently has 14 officers on their staff and their technical support is provided by in-house professionals. Police reported a significant growth of cybercrimes in Georgia: more than 50% increase from 2014 (163 complaints) to 2015 (249 complaints). Investigations are considered successful in 20 to 30% of the cases.

The cyber unit proceeds in an investigation if a certain crime is committed in a digital / online manner or if it is a cybercrime by definition. They are also active in raising awareness on the cyber threats topic: the police provide content for online news, which includes recent developments, new trends (fake invoices sent to companies are a growing concern), case stories and video clips. It was reported that police has an active, daily cooperation with all major providers in Georgia.

The Cybercrime Unit plans to set up a Working Group bringing together the ISPs, the GNCC, LEAs and prosecutors. Topics of discussion will include possible solutions on identifying subscribers, legal framework on retention of traffic data, stricter sanctions for cybercrime and how to better implement the Cybercrime Convention. The working group, which would be driven jointly by the Ministry of Interior and the Ministry of Justice, would be split in two sub-groups, one on norms, the second on operational issues. A key benefit from this initiative would be to avoid implementation issues to happen, as it was the case on the legislation on data retention period which could not be implemented due to lack of capacity of ISPs and lack of discussion with industry in advance.

The **State Security Service** has the following main units regarding cybercrimes: crisis management, digital expertise and technology, furthermore, international relations. The Service has an active role – together with the Crisis Management and Security Council - in developing the new Cyber Security Strategy which shall be approved in this year and shall be effective until the end of 2018. As a main development point of the draft Strategy: it will also include cybercrime. The work is in its final phase, since the action plan and the first draft is already prepared, thus the final version / adoption is expected in June 2016 for implementation from 2016 to 2018.

Public-private cooperation will be discussed and facilitated by a forum, either as a continuation of the Cyber Security Forum launched by the Data Exchange Agency or as a new forum. State Security will be interested in getting input from the CoE as this forum develops. In addition to this updated strategy, a separate strategy is expected to cover organised crime, which will further cover cybercrime.

The **Georgian National Communications Commission** (GNCC) is an independent public administration body, which reports to the parliament on an annual basis. Its annual report is published on its website. With a staff of 120 people, its mandate is to regulate electronic communications and broadcasting sectors of Georgia.

GNCC engages directly with ISPs. The Commission has dedication in order to protect privacy of the users. This concept was also articulated in the negotiations at the Memorandum of Understanding signed by the ISPs and the law enforcement authorities. The Commission has a clear understanding that public awareness about cybercrimes is a key issue: educating the users on the threats are of utmost importance. It was reported however that several companies still don't invest into security until they face damages due to cybercrimes. Content is not being monitored in Georgia, but access is. The Commission has a clear legal obligation to cooperate with law enforcement authorities.

The GNCC expresses a clear interest in Georgia to run awareness campaigns on cybersecurity and against cybercrime, which could include a forum of the various relevant stakeholders (ISPs and authorities).

The **Data Exchange Agency** was established in 2010 as an independent body. Its main aim is to coordinate e-governance and strategy, furthermore international projects and cyber security. It has coordinated and published the Cybersecurity Strategy of Georgia 2012-2015 as well as the new Cyber Security Strategy. In these regards it has a significant effect on development, legislation, international relations and raising awareness (e.g. they are very active in Facebook communication and also provide trainings). The implementation of the ISO 27xxx family is a key project of the Agency. No matter the fact that there are strict rules for

bank secrecy, the Agency was still capable of keeping this interest in focus and at the same time effectively support financial institutions in a major attack against them in 2015.

The Agency has established an incident management system which enables them coordinate and exchange information with critical infrastructure entities. For the critical infrastructure entities consultation and assistance has been provided in order to implement the ISO standards.

The Agency has an extensive cooperation at an international level, namely with the following countries: Moldova, Azerbaijan, Poland, Ukraine, Macedonia, Montenegro, Mongolia and Lithuania. In this frame the Agency regularly participates in knowledge sharing projects and it is also open to cooperate on a daily basis if urgent actions are needed.

The **CERT.GOV.GE** under the Data Exchange Agency is one of two dedicated CSIRTs in Georgia: the government CERT.GOV.GE and the academic CERT. The government CERT was founded in 2011 and it is under the supervision of the Data Exchange Agency of the Ministry of Justice of Georgia. The Law on Information Security defined that the government CERT is responsible for the handling of incidents, providing alerts, raising awareness and educating (e.g. penetration testing). The protection of the Georgian critical infrastructure is a priority task for them.

There is no national CERT operating currently in Georgia, although the CERT.GOV.GE is currently performing these functions.

The **Office of the Personal Data Protection Inspector** is an independent body with an annual reporting obligation to the parliament. The Head inspector of the authority is appointed by the Parliament. The main tasks of the Office are: consulting, handling of citizen complaints, inspections / audits, awareness raising and setting up standards / education, providing recommendations and international relations in the topic.

The Office has a staff of 43 people (from 14 in 2013) and has the following departments: legal, inspection, ICT and international. The Office has regular consultative meetings with the ISPs.

The Office of the Personal Data Protection Inspector was awarded a new function in 2014: the supervision of the covert investigative activities for the purposes of crime prevention and investigation, which resulted in additional staff. The Office receives every court warrant in the subject of interception – due to monitoring / safeguard reasons; the current regulation is in force since 30 March, 2017, which is different from the previous model (from 2014 to March, 2017) which gave the inspector the mandate to give prior approval for commencing the interception. The transmission of such documentation is made via a secure electronic channel to the Office; additionally, the Office receives the paper copies of court warrants. It is the Law enforcement oversight unit which is responsible to evaluate such warrants within the Office. In case of ISP data, the Office has only the right to be informed about the warrant. However, in case of telecommunication data, According to the current legislation, the activities may start without OPDPI's approval but may be suspended if inconsistencies are revealed. The OPDPI has suspended a number of interceptions on different legal grounds, e.g. according to the report of 2016 (presented to the Parliament of Georgia in 2017), in 47 cases inspector blocked the start of interception. The Office has also conducted checks, which resulted in some delays before the warrant could be validly implemented.

There are around 110 **Internet service providers** in the Georgia, 32 having their own IP addresses, and the others being virtual operators. Silknet and Causasus Online are the two largest providers with around 80% market share together. In early 2016, the Small and Medium Telecommunication Operator's Association was established, for the purpose of bringing together the small ISPs, but also cable TV operators, transit and telecom operators. As of May 2016, the association has 35 members.

According to the Law on Electronic Communications telecommunications companies must be licensed before entering the market. All ISPs are obliged to properly identify their subscribers before starting to provide services to them. The identification procedure is also required in case of the .ge domain registrations. It can be stated that ISPs are not providing any data to law enforcement authorities without following the necessary procedures. It is strongly communicated that ISPs may not intervene into the private life of any subscriber.

Providers generally do not have to keep traffic data but they can do it on a voluntary basis. There has been a law prescribing a 2 years' traffic data retention obligation, but it was eventually not implemented as ISPs could not comply with it, mainly due to costs incurred. Indeed, the legislation takes into account the capacity of the ISPs: they do not have to store data when they don't have the capacity to do it. The only obligation ISPs have is to provide colocation of the technical equipment (which is owned and operated by State Security) and transfer of the data. Although the colocation of equipment can raise some practical and cost issues, the main concern of ISPs is competition and their access to the market.

Informal cooperation

Cyber Security Strategy and Strategy on fight against organized crime as well as Digital Georgia Strategy highlight the importance of public private cooperation.

A **Memorandum of Understanding** is in force between the ISPs and the law enforcement authorities since 2010, and has been updated regularly until 2015. The aim of the Memorandum is to settle the fundamental intention of the signing parties to effectively cooperate in battling cybercrimes and at the same time to pay respect to the privacy of the subscribers. The Memorandum was reported as effective by both public and private sector stakeholders, although the private sector was more of an opinion that the documents works to far lesser degree than few years ago.

As the legislation, in particular Criminal Procedure Code has been amended in 2013 and procedural powers and cooperation mechanisms changed, the MoU is not considered effective any more. The MoU and its provisions were more relevant previously, when law enforcement authorities were allowed to cooperate directly with service providers. After 2013, it is not the case anymore and now all the requests need to have a court warrant. As it is more time-consuming and involves more bureaucracy, the text of the MoU should be revisited. For example, direct cooperation and use of contact points can still be useful.

As regards the costs related to preservation of data and disclosure of data, there are no agreements and service providers need to cover all costs by themselves. It does not affect the cooperation with larger providers, with whom the cooperation can be considered good. However the cost issue can be an obstacle for smaller providers and makes getting data from them difficult. For smaller providers, it can be also relatively large burden which forces them to raise prices for their customers.

When new legislation is being drafted, specific working groups are established. Private sector entities can be involved and consulted during the process.

Private sector stakeholders are invited on an occasional basis to the Parliament's relevant committees in order to provide their inputs.

On a daily basis many providers work closely with the law enforcement. In case of cybercrimes providers in most cases report them and in this case it seems to be high level of trust between private sector and public sector.

Foreign service providers are also open for formal cooperation with the public sector in Georgia: cooperation arrangements have been discussed already with Facebook and such negotiations are expected to start in the near future with Google as well.

Georgia hosted the Internet Governance Forum in 2015 on the topic of Human Rights in the Cyberspace, and the event was opened by the National Communication Commission. Topics included internet governance – actors and institutions, human rights protection in the internet space, the standards of freedom of expression in the internet, information security and protection, online journalism in Georgia and the regulation norms in the field of internet.

Data Exchange Agency regularly holds the Cyber Security Forum of Georgia, which was launched in September 2012. It has 3 major tasks: identify leaders in private sector, develop management crisis scenarios and prepare for collaboration in time of crisis. It has also brought together key cyber security experts from public and private sector and has contact points in all participating organizations and other entities.

Moldova

Law and regulatory aspects

Moldova has signed the Budapest Convention on Cybercrime (ETS 185) on 23 November 2001, ratified it on 12 May 2009 and it entered into force on 1 September 2009.

Main threats of **cybercrime** reported by the counterparts are payment frauds including skimming, DDOS attacks and malware, child pornography, furthermore, identity theft is becoming a growing issue. Moldova has not yet defined any laws on cyber terrorism; however, their law on terrorism (including extremism and international threat) is already in force. It must be noted that crimes related to the cyber sphere are investigated in case a financial / damages threshold is reached in the amount of 50,000 Leu (approximately 2,500€) to be a criminal offense. Should the damages be for a lower amount, it is considered a misdemeanour offense instead of criminal offense and the investigative powers are lesser. This can cause problems for those cybercrimes that are small individual cases where each victim only loses a couple of hundred euros, but there are hundreds or thousands of victims, because the legislation does not allow for the aggregation of similar offenses to pass the 50,000 Leu threshold. It shall be noted that no cyber related misdemeanours or administrative code based breaches are codified in Moldova.

The **criminal procedure** has three phases: preliminary, investigation and trial. There is a three-stage approval system for obtaining information / evidence from the ISPs:

- The investigation judge may approve the following: house search, placement and use of any recording equipment / video surveillance / related technical means at certain premises; search and seizure of individuals or their communication, and monitoring the telegraphic and electronic communication; monitoring financial transactions; investigating via tracking and location data systems (GPS); collecting data from electronic / internet service providers.
- The prosecutor may approve: identifying of the subscriber or the owner / user of an electronic communication device; visual monitoring of a person; track / control of financial procedures; controlled deliveries and acquisitions, , undercover investigations, cross border surveillance and visual surveillance (not using recording devices).
- The senior investigation officer as the leader of the investigation team may approve: the collection of data which may support identifying a person.

Regarding **electronic evidence** for the purposes of criminal proceedings, there have been some discussions in Moldova, under the projects run by the Council of Europe Cybercrime Programme Office, whether it is necessary to introduce separate definition of electronic evidence in the criminal procedure. Although it was agreed that the general concepts of evidence could cover computer data, a more precise and separate definition of electronic evidence could simplify both the application of special procedural powers and provide clarity as to rules of admissibility of evidence.

The definition of subscriber information has been implemented in Electronic Communications Law, Article 2, while traffic data is defined under the Moldovan Code of Criminal Procedure; content data is interpreted to include the content of communications. Despite availability of definitions, the inconsistent use of terms across different legal acts ("computer information", web traffic data", etc.) was noted as a potential problem.

Moldova implements all **procedural powers** under Budapest Convention in its law; however, specific measures related to search and seizure available under Article 19 BCC are not directly implemented.

Data retention is regulated by the Law on Electronic Communication. The mentioned legal body also regulates that ISPs (no matter if a legal or non-legal entity / private person) need to keep data ("all available information") for 6 months of time, however the definitions are too broad (which may be interpreted the way that all subscriber, traffic and content data as well), which results in a situation where the relevant public and private sector stakeholders have different understanding of them. Traffic data related to telephone conversations (subscriber, invoicing, source and destination numbers, duration) are kept for 12 months. Preservation orders last up to 180 days, and can be extended by 90 days under the Law on the Prevention and Combating Cybercrime.

In terms of **safeguards and guarantees**, one of the key issues in Moldova is the lack of understanding of the systems of safeguards and guarantees tailored to the standards and requirements of the Convention. Although there are definitions of categories of data (subscriber and traffic), there are no differences in terms of accessing such data, with thresholds and limitations gradually progressing from lightest (subscriber information) to heaviest (content data) types in terms of privacy intrusion. Judicial authorization for each and every procedural power under the Convention does not only (potentially) hinder expeditious access to data, but also undermines the whole purpose of coherent and gradual system of safeguards and guarantees tailored to the level of intrusion into private life of individuals.

Stakeholders' roles and issues

There are no dedicated **strategies/action plans** on cybercrime currently in force in Moldova but one is being drafted. Moreover, since 2015, there is a separate section No. 4 entitled "Preventing and combating cybercrime" in the *draft* national Programme on Ensuring Cybersecurity of the Republic of Moldova and its action plan.

The **Ministry of Justice** has a main role in overseeing the legislative framework and also the organizational tasks regarding codification and the legal reforms.

The **Prosecutor General's Office** has the responsibility to control the investigative procedures and at the same time it may issue warrants as well with a limited scope. Since 2010, an Information Technology and Cyber Crime Investigation Section as an independent structural subdivision of the Prosecutor General's Office directly under the General Prosecutor, is in charge of criminal investigations and prosecutions in cybercrime cases. There are 5 prosecutors in the section, supported by 4 consultants and 2 IT specialists, who are tasked the investigation of the full spectrum of offences provided by Article 2-10 Budapest Convention, as well as related offences against or with use of computer systems and data. The Prosecutor General's Office is responsible for the oversight and control of interception. This task is managed by a separate unit within the office, which prepares a report twice a year to the Parliament and the President.

The **Ministry of Internal Affairs** has a dedicated The Centre for Combating Cybercrime within the General Inspectorate of Police has an active communication bridge with Facebook, Skype (Microsoft), Western Union, Webmoney, Paypal and eBay. The Centre plays an important role in providing their opinion to the Parliament as well on how to reform the relevant laws to battle cybercrimes (e.g. extension regarding the preservation of data). They have a good international cooperation with their professional peers (e.g. with Italy, Estonia, international expert bodies, etc.). A reporting mechanism for citizens and legal entities to report internet crimes is being considered but an implementation project has not yet been decided. It is however possible to report crimes by email.

The **Security and Intelligence Service** has a supporting role in collecting and analysing data related to cybercrime, thus it is not proceeding as an investigative body (they don't perform interrogations, but they may interview persons). The investigations which are supported by the Service are generally undertaken by the Ministry of Interior and the General Prosecutor's Office. They have an active cooperation with their local peers and also on an international level in order to handle cyber threats.

The **Ministry of Information Technology and Communications** is driving the Cyber Security Program in Moldova. The Program consists of 7 main pillars: (1) data processing, storing and access, (2) security and integrity of e-commerce, (3) capabilities (including CERT), (4) prevention / combating cybercrime, (5) strengthening defence, (6) education, (7) international cooperation. As a next step the Ministry is aiming at developing minimum cyber security requirements. Based on it, there will be elaborated legal and institutional framework which gives possibility to audit the entities which are stipulated in the Government Decision draft for approving Minimum requirements for insuring cyber security, based on the minimum cyber security requirements.

There is only one operational CSIRT in the Republic of Moldova – "**Cyber Security Centre CERT-GOV-MD**". It was established in 2010 by Government Decision No. 746 of 2010 "On the approval of the updated Individual Partnership Action Plan the Republic of Moldova - NATO". The team took responsibility for handling of information security incidents and offering other cybersecurity services to public administration authorities of the Republic of Moldova.

However, Due to the lack of national CSIRT and wide national and international cooperation capacities of Cyber Security Centre CERT-GOV-MD the centre became the main point of contact for cybersecurity incidents related to the Republic of Moldova. There are five experts working in CERT-GOV-MD. The CERT-GOV-MD cooperates with law enforcement agency – Centre for Combating Cyber Crimes in the following areas: fighting with cybercrime (by reporting suspected incidents), capacity building (by organizing joint cybersecurity workshops and trainings), awareness raising (by organisation of cyber security conferences). Cooperation with state institutions is mainly based on internal regulation, bilateral agreements and voluntary commitments.

The **National Centre for Personal Data Protection of the Republic of Moldova** was founded in 2009 and it has a new director since April 2016, who was elected by the Parliament. The Centre generally has the right to provide its data protection focused comments to the codification bodies.

The Centre works only with 21 staff members, which makes it practically hard to carry out on site audits and inspections (which are only done in case of complaints are filed). The cooperation with the ISPs is regular.

The court may sentence a data processor for a maximum of EUR 400 in case data processing registration is not made, but suspension (to take corrective measures within 30 days) and also the banning of the activity may also be applied. It can be said that all major ISPs are duly registered; however, there is a room for improvement regarding the smaller ones (they receive an average of 10 applications daily). They receive regular complaints regarding procedural measures by police and prosecutors, but these are ended generally by administrative sanctions.

The **Internet service providers** consider themselves to not be liable under the current legislation either to preserve or to retain the data. All providers are active in commenting the proposed amendments to cybercrime legislation (draft Law 161). They have a clear focus on privacy and freedom of speech. Their main issue is that it is also unclear for them what information shall be stored on their systems. In general, the private sector in Moldova is rather hesitant to work with law enforcement than what is normally expected in the country context.

Public sector stakeholders have unanimously stated that they expect ISPs to initiate any cooperation measures. Orange, Moldcell and Moldtelekom were named the most cooperative ISPs by the public sector stakeholders. It was said that smaller ISPs do not store any data, thus many are non-compliant. Moldtelekom is the incumbent provider on the market and its majority owner remained the state. It only operates fixed networks in the country. The Moldcell company is not related and is part of the TeliaSonera group.

Informal cooperation

There is no general Memorandum of Understanding between the ISPs and the public sector. Such an approach was discussed in 2012-2013, however it never received a mutual recognition and neither did it arrive to a final drafting phase. In 2015 a similar event was held, aimed at co-operation initiated by the National Cybercrime Investigations Centre, which was successful, but not followed up. At the same time, the National Bank – which oversees all banks in Moldova - has concluded a Memorandum of Understanding with the General Prosecutor's Office.

There is a Cross Agency Regulation which was signed by all law enforcement bodies in Moldova. The document is considered as normative. Its existence is public knowledge, but the content of the regulation is classified.

Education is being regularly held for judges at the judicial academy.

An important issue is that any information gathered from private parties following voluntary co-operation can only be used as intelligence. Whilst it can be used to motivate the use of police powers, it cannot be used as evidence. For it to be used as evidence the fact have to be collected through the legal process.

Similarly, a problem is that to receive information from ISPs significant suspicion (reasonable doubt) against a subject is required for the investigative judge to authorise information

gathering. This makes it hard to build cases that require information residing with an ISP and that have yet to arrive at full suspicion against a subject. It was observed that this hinders building cybercrime cases.

The Prosecutor's office has obtained cooperation from foreign ISPs such as Facebook, Microsoft, and VKontakte (Russian-based social networking service). Moreover a cooperation agreement is expected to be signed with Kaspersky Labs for technical assistance on investigations.

Moldovan ISPs cannot provide evidence directly to foreign law enforcement; however law enforcement of Moldova has shared such information with Europol and Interpol and foreign law enforcement on the basis of rogatory letters. Another obstacle to sharing information directly by an ISP to foreign law enforcement is the personal data protection that requires the transfer of personal data abroad to be authorized. However there is good cooperation between the Moldovan Prosecutor's office and foreign law enforcement as both German BKA and American FBI have obtained interception of communications from Moldova through legal cooperation.

Ukraine

Law and regulatory aspects

Ukraine has signed the Budapest Convention on Cybercrime (ETS 185) on 23 November 2001, ratified the document on 10 March 2006 and it entered into force on 1 July 2006.

Main threats of **cybercrime** reported by the counterparts are crimes with financial aspects (e.g. online fraud, pharmaceutical / IPR cases, etc.) as first, except at the state security service where terrorism related crimes were mentioned as the top priorities followed by counter intelligence, considering on-going military hostilities. Stakeholders have only mentioned child abuse and child pornography, in case it was asked, but in case any child abuse or child pornography would occur, reporting to police would be the immediate action taken. In 2017 several large-scale malware and ransomware attacks targeted both public and private sector entities in Ukraine. Many private companies were severely hit by the ransomware attacks and suffered damages.

The **criminal procedure** has three phases: preliminary, investigation and trial. There is no separate regulation in the criminal procedural legislation in respect of cybercrimes. Ukraine has a dedicated law on operative-detective activities, which also defines surveillance and covert operations. The judge oversees the full criminal investigation phase and may provide judicial control over the prosecutor as well, who is responsible for control of the procedures of the law enforcement bodies in charge with the criminal investigation. A judicial warrant is needed in case a law enforcement agency requires data from an ISP. Warrant requests are being sent to the court in paper form; however they are distributed in an electronic system within the court. Decisions on warrant requests are generally made by the judge within 24 hours, but in severe cases this may go down to 6 hours only (criminal procedure provides an exhaustive list on these cases, such as terror threats).

Regarding **electronic evidence** for the purposes of criminal proceedings, the concept of documents is used instead and interpreted to include electronic data in practice. The definitions of subscriber information, traffic and content data compliant with the Budapest Convention are not found in Ukrainian legislation.

Procedural powers under Articles 16, 17 and 18 of the Budapest Convention (preservation and limited disclosure of data and production orders), as well as some specific measures related to search and seizure available under Article 19, are not directly implemented. Access to data is predominantly obtained through search and seizure proceedings.

From September 2016 to May 2017 several workshops and meetings were organized by the Council of Europe to analyse and review the Criminal Procedure Code, Law on Telecommunications and draft laws related to cybercrime. There are many problems at practical level were caused by gaps in legislation in particular lack of definition of electronic evidence, categories of data as well as partial implementation of the provisions of the Budapest Convention. As the legislation does not provide all answers the courts in Ukraine have been developing different interpretations of the law. That has lead to a situation where there is no common understanding and practice on collection of the electronic evidence, storage and analysis as well as admissibility in courts. In order to overcome these problems a report was prepared with possible amendments to the Ukrainian legislation; the legislative process has started on October 5th 2017, when the Verkhovna Rada of Ukraine adopted the Law of Ukraine About the basic principles of providing cyber security in Ukraine. This legislative act reformulates some the issues raised in the paragraph above, especially with regard to ISP obligations to cooperate.

It seems to be the case that several government institutions are working with their own draft laws and there is no central coordination. Instead of drafting a single draft law or package of draft laws on procedural powers, procedures to collect evidence, restrictions, limitations and safeguards the texts are being prepared and sent to parliament separately. This in turn might lead to a situation where there is no clear overview about the overall situation and creates a risk for whether gaps or overlapping provisions in legislation.

There is no clear regulation about what kind of data needs to be retained by an ISP and for what exact amount of time. There are different interpretations concerning existing legislation. According to the Civil Code data should be retained for 3 years. However as the existing

regulation lacks proper clarity and foreseeability, the Civil Code provisions are not supported by the provisions in the Law on Telecommunications, it has been recommended to draft specific and precise provisions on data retention.

In terms of **safeguards and guarantees**, the system of safeguards and guarantees is not implemented in way that encourages application of less intrusive procedural powers before more intrusive options. The absence of clear and enforceable regulations implementing Articles 16-18 Budapest Convention is in itself an obstacle to setting up and implementing a coherent system of safeguards and guarantees which limits intrusion of privacy of individuals. On November 16th 2017 the Verkhovna Rada of Ukraine adopted the Law of Ukraine On Amendments to Certain Legislative Acts on Enforcement of Rights of Participants in Criminal Proceedings and Other Persons by Law Enforcement Agencies during Pre-trial Investigation; this legislative act reportedly remedies some of the issues raised in this regard.

Stakeholders' roles and issues

In terms of **cybercrime strategies,** Section 4.5 of the Cybersecurity Strategy of Ukraine (enacted by Decree 96 of the President of Ukraine of 15 March 2016) addresses the issue of fighting cybercrime. Among the priorities, the following measures are listed: establishing a contact centre for reporting cybercrime and fraud in cyberspace; improving procedural tools for digital forensics; training law enforcement, judges, investigators and prosecutors with regard to handling digital evidence; introducing blocking of information resources (information services) by the court; data retention obligations for operators and providers of telecommunications regulations; enhancing criminal procedure actions with the use of electronic documents and digital signatures; coordination of law enforcement agencies to combat cybercrime; and regulating interception of telecommunications in case of cybercrime investigations.

The Cybersecurity Strategy of Ukraine, beyond cybercrime matters, also addresses the development of safe, sustainable and reliable cyberspace, security of the government information resources, security of critical infrastructure, and development of cybersecurity capacities in the defence sector as strategic priorities. A number of stakeholders, including security, defence, communications and police agencies of Ukraine are tasked with implementing the Strategy.

The Strategy is supplemented by yearly Action Plans that are issued by the Cabinet of Ministers of Ukraine since 2016.
The **Ministry of Justice** has the main role in developing the legislative framework and also the organizational tasks within the government sector regarding codification and the legal reforms. Currently a legal reform is being discussed regarding a more detailed content focused cybercrime initiative for the criminal legislation

The **Prosecutor General's Office** has the responsibility to control and to supervise the investigative procedures. There are plans to introduce specialized prosecutors who would be trained and have necessary experience in cybercrime investigations.

The **National Police** has a dedicated Cyber Police Department. Since its foundation in 2009, the Cyber Police only acts as a specialist force that is supporting investigations from the technological point of view, meaning that they are not performing any core investigations – there are undertaken by investigators based on investigative jurisdiction. The total number of their staff is 39. There are dedicated units within police in the following subjects: e-commerce, online gambling, IPR / pharmacy, financial frauds, credit cards, skimming, online banking intrusions, e-currency frauds and child pornography.. Cooperation was reported as active with Europol and Interpol.

The **State Security Service** provides main focus to secure national security and to protect the country's cyber sphere, Focusing on counteraction to cyberterrorism, protecting state informational resources and critical infrastructure from cyberattacks, fighting with transnational cybercrime, which are the major issues. the Law of Ukraine on Telecommunication` requirement that data should be retained at the term of limitation of actions; the current practice, however, is 90 days.

The investigative and other competences between the police and State Security Service in Ukraine have been clarified with the adoption of the Cybersecurity Strategy of Ukraine(2016) and the Law of Ukraine About the basic principles of providing cyber security in Ukraine

(October 5th 2017). Functions are distributed between the units of the Ministry of Interior and the Security Service of Ukraine on the basis of investigative competence regarding a relevant crime as established by Article 112 of the Criminal Procedural Code of Ukraine. In many cases, the investigative competence on such crimes can vary. Moreover, the distribution of functions is linked to the area of responsibility of the police and Security Service. For the Ministry of Interior, the key focus is to protect rights of people, companies, institutions, organizations, interests of the State and society against unlawful acts. For the State Security Service, the focus is to protect the State, its constitutional order, State security, as well as to conduct counter intelligence activities.

The **National Commission for the State Regulation of Communications and Informatisation** (NCCIR) was established in 2011 and its procedures are based on the Law of Ukraine "On Telecommunications". It is responsible *inter alia* for the licensing, regulation and supervision of the telecom, postal services and ICT sectors. The NCCIR reported around 5000 ISPs in the country. In case of breaching of the relevant regulations an ISP's managing director can be fined. The NCCIR admittedly plays a very modest role in regulating ISPs, specifically regarding ISPs' cooperation with the law enforcement.

The governmental **CERT** within the Special Communications Service provides incident investigation, consultancy (including penetration testing) and monitoring. It is one of their main tasks to support implementation of ISO standards (27xxx). The staff may also proceed as a team of experts at court. It was reported that the cooperation with local ISPs is low. Draft legislation is being debated about setting up further and sector focused CERTs in the country. The CERT has a significant role in drafting the cyber security strategy. It is a member of FIRST since 1 January 2009.

According to the amendments to the Law of Ukraine «On Protection of Personal Data» introduced in 2014 the function of control over observance of the legislation on protection of personal data is assigned to the **Ukrainian Parliament Commissioner for Human Rights:** the Ombudsman's Office.

In order to ensure fulfillment by the Commissioner of the functions of control over the implementation of the legislation on the protection of personal data, the Department for Personal Data Protection was created.

Control over the observance of the legislation on personal data protection by the subjects of inspections shall be carried out by the Department through carrying out inspections: scheduled, unscheduled, field and remote ones. The Department has the right to inspect every controller and processor. The plan of inspections is published on the website of the Commissioner. Scheduled inspections were conducted in the field of IT in 2015. Unscheduled inspections are also carried out on appeals received from citizens.

The Department provides recommendations on practical application of the legislation on protection of personal data, to explain the rights and obligations of the relevant persons upon request, in particular law enforcement and IT companies.

The Department conducts expertise of bills and draft legal acts and analyzes the current laws and legal acts on compliance with their legislation in the field of protection of personal data and prepares proposals on necessary amendments to them.

The Department provides proactive monitoring in order to detect the unlawful dissemination of personal data. Most of the cases are initiated by citizens who file their complaints with the Department (topics include: illegal distribution of personal data over the Internet). According to the legislation the general timeframe in which the Department needs to provide its answers to inquiries is 30 days.

The Department regularly organizes educational trainings for professional and target groups on the practical application of the legislation on personal data protection. At the same time, the Department lacks the technical staff.

Regarding **Internet service providers,** there are about 5,000 business entities in the registry operators of telecommunications (including ISPs) in Ukraine. According to official information from the web site of Ukrainian Internet Association, it consists of 129 active members and 61 associated members, representing mostly large and active entities out of those. The Association is very active on the topics of cooperation with the law enforcement.

The Ukrainian Internet Association has also been involved in legislative process and proposed comments and amendments to draft legislative acts.

The Ukrainian Internet Association has also started cooperation with the Academy of Ministry of Internal Affairs in Kharkiv to provide trainings for future cyber security experts and investigators.

There is no clear regulation on data retention, but it can be stated that ISPs generally keep data for 90 days. It was reported that data preservation is unknown in practice.

ISPs are not actively or not regularly involved in the consultation for legislation. Although there are working groups and committees responsible for drafting legislation, often private sector representatives are not invited to their meetings. There have also been issues with regard to transparency of the process. Even if private sector representatives have been involved and they have submitted their comments and proposals, these are often not taken into account.

As the procedures to gather electronic evidence are not regulated and the practices differ, it would be important to continue with the legislative reform and in parallel start discussing cooperation frameworks and procedures for cooperation which would also include recommendations and guidelines for providers. To respond effectively to cybercrime and cyber incidents, a network of experts from both public and private sector could be established.

Informal cooperation

From the perspective of the Government of Ukraine, there is an ongoing dialogue with ISPs and financial institutions taking place and cooperation agreement has been concluded between police and one ISP (Lifecell) as well as between police and financial institutions. There are also informal cooperation mechanisms that include 24/7 availability for calls and mailing lists between the points of contact. There are also police liaison officers in other government institutions that can also facilitate cooperation and information exchange.

A Memorandum of Understanding approach and a Round Table discussion group already exist, however these are not well communicated in respect of its members/drivers, procedures, responsibilities, functions and most importantly: the next steps. The Memorandum of Understanding and the Round Table are the approaches which can be the common grounds to make a move forward in Ukraine, since all stakeholders struggle from the same issues: (1) unclear legal grounds, (2) inconsequent application of law, (3) no trust towards each other and (4) cybersecurity /crime as a whole is managed differently by each elected government.

Police reported that the cooperation with the major ISPs needs development on the part of the business.

In 2017 following the series of workshops and meetings in Ukraine, the Council of Europe also suggested to both public and private sector representatives to draft a new MoU that would be based on law and that would prescribe cooperation frameworks, procedures to request and disclose data, information exchange channels including contact points and other technical details concerning everyday cooperation to fight cybercrime and ensure cyber security.

Reporting of cybercrime is not mandatory. However, concerning recent malware and ransomware attacks against Ukraine, around 2500 reports were received from private sector. There is an obligation for critical infrastructure objects, identified in the recently adopted Law of Ukraine on basic principles of providing cyber security in Ukraine, to report cyber incidents.

Annex II. Overview of public-private cooperation initiatives in the Eastern Partnership

Prepared by the Cybercrime Programme Office of the Council of Europe (C-PROC)
October-December 2017

Introduction

The current overview of initiatives and projects related to public-private cooperation in the Eastern Partnership is based on the questions and answers conducted with the project country teams and project counterparts in the framework of study visits of Cybercrime Programme Office and the team of experts to all EAP states in October and November 2017. Carried under the project Cybercrime@EAP III and corresponding to one of the expected results/outcomes of the project (*A structured process of public/private cooperation on cybercrime underway*), this short overview is an attempt to map the environment for current and further project implementation, with the potential to identify overlapping or competing efforts but also to search and establish synergies that may contribute to better implementation of all related and relevant initiatives.

The questions were addressed mostly to the law enforcement and government entities represented in the Cybercrime@EAP III project country teams, and involved very time-limited discussions (2-3 minutes per entity) on the past, current and planned initiatives and project that contributed not only to public-private cooperation, but also increase the capacities of specialized cybercrime authorities, as this can be a relevant factor the topic in question.

The current overview thus does not represent an exhaustive inventory of all similar or related efforts but rather summarizes the experience of project counterparts on the topic.

Armenia

The biggest current initiative relevant for cooperation environment is the development of draft Code of Criminal Procedure and all related legislative acts deriving from the draft.

The Working Group on Cyber Security at the Parliament is considered as the initiative developing the standards on the topic.

The training to law enforcement is mostly driven by international actors, such as EC (Taiex Programme), OECD ACN (corruption investigations), OSCE, World Vision (safe Internet, DNS security). Interne Governance Forum is considered as the potential public-private cooperation initiative.

On country-specific initiatives, future cybercrime trainings with FBI are being discussed.

Private sector vendors, namely ISPs, are involved training and capacity building with international partners, mostly coming through headsquares of their parent companies, most frequent topics being abuse management, data protection and information security. The local Interne Governance Forum is viewed as an opportunity for public-private dialogue platform.

Azerbaijan

The projects and initiatives involving Azerbaijani institutions are not implemented in coordinated manner, which could be primarily attributed to the lack of dedicated cyber crime or cyber security strategy and/or action plan.

The major contributors are either states (US, Turkey, Germany in particular) or international organizations (GUAM, OSCE, UNODC, NATO) who offer one-time training sessions on mostly technical issues, such as handing forensics equipment, interception, cyber-security operations and so on; the training is sometimes delivered with the handover of forensics equipment.

The only private-sector contributor mentioned in training and experience sharing was Microsoft.

Belarus

In Belarus, the Cybercrime@EAP projects were specifically mentioned as lead ones on the topics of cybercrime and electronic evidence. An example of joint training with two CSIRT teams in 2017 was held as best practice example.

The law enforcement still receives operational training on the subject through bilateral links, Spain being noted as one such example. Financial Action Task Force 40+ Recommendations were supplemented by training on cooperation between cybercrime units and financial intelligence in the CIS countries.

There are several non-training related initiative relevant for public-private cooperation. The chief among them is the development of information and cyber security strategic documents by the Working Group under the Security Council, also linking this work with the planned amendments to law concerning data protection. The police is also drafting internal guidelines for removal of data from computer systems.

The Scientific and Technological Association Infopark and its events are considered as good example of public-private partnerships based on academic research and participaiotn.

Georgia

Georgia benefits from bilateral training on cybercrime from a multitude of partners, including National Crime Agency of the UK (including participation in Silver Tower exe), Germany, France, Estonia, Israel and the USDOJ and FBI from the United States. The major training courses include investigations and forensics, including mobile forensics, as well as fraud investigations.

From international organizations, IOM delivers training on combating crime; OSCE delivery of trainings on virtual currencies was noted; expert support to increase skills in Police Academy from the EU; and UNODC workshops on electronic evidence, although these are not regular.

Georgian law enforcement and prosecutors actively explore joint training, especially under the umbrella of USDOJ and FBI trainings, which are planned to be expanded with planned appointment of specialized prosecutors working with cybercrime. Prosecution Service has recently adopted its multi-year Action plan, envisaging inter alia specialization of prosecution attorneys and follow up support by training, including cybercrime.

The Data Exchange Agency and its yearly GITI conferences and Cyber Security Forums are considered to be the lead platforms for public-private partnerships.

Moldova

In Moldova, project and initiatives are grouped around several subjects. For example, the Prosecution Service receives Intellectual Property cybercrime related trainings as well as development of guidelines for prosecutors and law enforcement on IP crime. Child sexual abuse online is a subject of dedicated project with the support of the Council of Europe, not only with law enforcement training but also awareness campaign and safe Internet reporting page.

Under the Budgetary Support Matrix project supported by the EU, specifically ERASMUS +, the creation of cyber security faculty in University of Moldova is supported, with delivery of European practice of teaching, study plans for capacity building and coverage of academic institutions in terms of cyber security education.

Law enforcement receives trainings on white hacker training with the support of the Council of Europe and Technical University. Trainings also include data handling, development of codes of conduct and seminars/study visits on the subject.

Data protection issues are important and mostly seen through imminent application of EU GDPR standards; future Twinning project with Germany and Latvia, already signed and in force from 2018, is expected to cover this gap.

Ukraine

Ukraine has been long supporting the idea for the creating of the Cybercrime and Cyber security Excellence Centre for the purposes of serving Ukraine and the rest of the Eastern Partnership. The Government, with support from the law enforcement and led by the Ministry of Foreign Affairs, currently is in discussion with major actors, such as the EU, Council of Europe, and GUAM to launch the initiative.

The EU Advisory Mission in Ukraine has a specific cybercrime advisor who is actively organizing and delivering training on cybercrime to law enforcement; training for prosecutors is also planned. OSCE is another major actor in training of law enforcement in Kyiv and regions of Ukraine in protection of networks and security.

State Security Service benefits from capacity building of the NATO Trust Fund on Cyber Security, which is actively engaged in trainings on the protection of Critical Infrastructure. Council of Europe and its Cybercrime@EAP projects are deemed as major contributor to capacities of the Cyber Police Department of the National Police. The Cyber Police also seeks active involvement with Europol for threat intelligence and countermeasures training.

In terms of private sector involvement, the Internet Association of Ukraine currently works with Kharkov Police Academy to plan and deliver operative trainings to police officers for more effective work on processing and removal of information carriers, to minimize the degree of intrusion into private business activities.

Annex III. Feasibility study on the platform for public-private cooperation in the EAP region

Prepared by the Cybercrime Programme Office of the Council of Europe (C-PROC)
October-December 2017

Introduction

The Octopus Cybercrime Community was set up following Recommendation 18 of the T-CY assessment report on the mutual legal assistance provisions of the Budapest Convention to "explore the possibility of establishing an online resource providing information on laws of Parties on electronic evidence and cybercrime as well as on legal thresholds, and evidentiary and other requirements to be met to obtain the disclosure of stored computer data for use in court proceedings". It is an information resources focused on cybercrime and electronic evidence realised through information sharing and cooperation: prevention/control of cybercrime, securing of electronic evidence, cybercrime policies and strategies, state of implementation of the Budapest Convention on Cybercrime under national legislation, and publishing Council of Europe training materials (such as Electronic Evidence Guide, First responder training pack, Introductory judicial training, Advanced judicial training, Training strategies guidelines), Blog/Calendar of events and news related to cybercrime.

The Octopus Cybercrime Community contains separate section on public-private cooperation on cybercrime and electronic evidence. This tool contains country-specific information on service providers and their requirements to disclose information in response to law enforcement requests, as well as information on States Parties: domestic legal basis to issue production order, request data preservation, emergency situations, data protection safeguards, remedies, and other data.

The Octopus Cybercrime Community section on public-private cooperation falls under partial responsibility of the Cybercrime@EAP III project due to one of the project indicators namely: "An online resource is maintained by the Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania to service [structured process of public/private cooperation], to improve transparency and thus public confidence, and to link up existing initiatives." Namely, the logic of the platform is corresponding to these objectives as follows:

Servicing the process of cooperation

- Status of relevant treaties that have relevance to the topic, reservations
- Legislative acts (criminal justice /communications /data protection) and any explanations, practices or case law applicable to these regulations
- Instructions, manuals, guidelines or operational procedures for accessing data
- Any standard forms or templates used in the process of accessing data
- Information on main stakeholders in the process (government and industry)

Improving transparency and public confidence

- Information structured along the system of safeguards and guarantees (data protection)
- Explanation of applicable requirements and expectations

Linking up existing initiatives

- Information on national/regional/global projects that have relevance to the topic
- Memoranda of cooperation and other arrangements to facilitate cooperation
- Any possibilities for training, membership of associations, etc.

The current feasibility study is based on the questions and answers conducted with the project country teams and project counterparts in the framework of study visits of Cybercrime Programme Office and the team of experts to all EAP states in October and November 2017. Carried under the project Cybercrime@EAP III and corresponding to one of the expected results/outcomes of the project (*A structured process of public/private cooperation on cybercrime underway*), with one of the indicators of this process being the the "feasibility of transforming the process into a more permanent platform in order to sustain the process", the study aims to briefly update the state of the platform as of end of 2017, and contribute to further development of the tool based on country recommendations.

The questions were addressed mostly to the law enforcement and government entities represented in the Cybercrime@EAP III project country teams, and involved discussions on the current use of the online resource, the completeness of information and possibilities contained therein, and suggestion for the best use of the resource in future for the country teams.

Armenia

The counterparts in Armenia stressed their familiarity with the public-private cooperation tool, but reported no particular use of the platform due to lack of information related to service providers, especially multinational ones.

In terms of further expansion of the platform, the counterparts were willing to see more information about the general rules and practices of cooperation in addition to the legal basis. Specific data and statistics indicating the measurement of public-private cooperation would be also appreciated.

It was suggested that the platform should be more functional than current state of providing information. Electronic exchange of information and requests, for example related to tax information and asset recovery cases, would be more feasible. It should also enhance cooperation in mutual legal assistance process by providing, potentially direct access to databases related to criminal cases.

Although the platform showcases the work of the Cybercrime Convention Committee (T-CY) there is an additional need for secure platform for exchange of ideas regarding the improvement of public—private cooperation, including access to evidence in the cloud.

The law enforcement counterparts wished to see the platform to provide some basic functionality for criminal case management in those cases that have an international/foreign cooperation component, modelled as a standalone information technology tool not too dissimilar to Secure Information Exchange Network Application (SIENA) system maintained by Europol.

Azerbaijan

Counterparts in Azerbaijan reported generally no use of the online resource except when asked for contributions to it, also due to lack of information related to service providers, especially multinational ones.

At the same time, there have been several suggestions and recommendations for improvement. With regard to legislation contained on the resource, more focus should be put on legal acts regulation retention of data and access to content, especially concerning the former USSR states since they are frequent counterparts for cooperation. Need for related regulations (beyond criminal procedure laws) on cybercrime and electronic evidence were mentioned, as well as the need to offer specialized training materials, including ones coming from service providers; policies and practices of other states on public-private cooperation, especially standards applicable to the EU states, were also noted as a desirable element.

As to the functionality of the platform, the most frequent request for improvement was the ability to track and process actual requests for data. It was specifically deemed to be very useful in communication with multinational service providers, so that the online tool could become a trusted and effective communications channel with them. One of the counterparts even suggested additional functionality for quick exchange of information on IP addresses involved in cyber incidents/investigations.

Belarus

From the responses of the counterparts in Belarus, the Octopus Community in general is viewed as an opportunity for securing direct access to service providers, especially multinational providers. Long timeframes for official process of mutual legal assistance is a challenge that may be somewhat remedies by the platform providing such access. This is particularly relevant when there are no international agreements between states in question place and the cooperation is ongoing on the basis of reciprocity, which is even a slower process than the mutual legal assistance on the basis of a treaty.

At the same time, it was noted that the potential membership to the Budapest Convention on Cybercrime would be beneficial for Belarus to address the issues of cooperation on reciprocity, but in this case the online resource would still be relevant as a trusted resource of information.

Another potential feature of the Octopus Community was noted – in essence, it has the potential for uniting different professions – investigators, prosecutors, private security experts and so on – on the general theme of combating high-tech crime. Therefore, the idea of specialized discussion forums, such as oversight on criminal investigations, mutual legal assistance, domestic prosecutions and the like - could be undertaken to expand the functionality of the resource. This could be used to provide clarity to its participants related to their functions in relation to the themes under discussion, but it would be worth to keep focus on high-tech crime/cybercrime.

Georgia

Georgian counterparts reported no particular use of the Octopus Cybercrime Community and its public-private cooperation section in relation to real-life cases. However, they have provided the visiting expert team with numerous suggestions for improvement of the resource.

In terms of existing version of the online resource on public-private cooperation, more information about the countries and States parties would be appreciated. This particularly relates to additional information on applicable legislation, as well as practices of cooperation, structure, functions and other information on about on investigative units working on cybercrime, obligatory and optional requisites for request for cooperation, and also information on internal/interagency cooperation practicalities, so that foreign counterparts are more aware to whom to send the cooperation request.

Request processing functionality was suggested as a feature of the online resource. It could improve the transparency of the process and provide necessary statistics of cooperation, as well as possibility of tracking live requests, which would in turn also improve compliance. As it was noted that direct processing of requests requires trusted parties to the process, some solutions have been proposed as well. The request processing portal could use different authorization levels for simple access to information, access to sensitive information, and then to direct request processing. Digipass or tokens could be used to verify higher-level sign-ins, and client/server side applications to make process more secure.

Georgia was one of the few countries that reported experience of limited use of the resource for practical purposes – in this case, updated Google policies for cooperation were accessed (it was not clarified, however, whether the public-private cooperation section was used or other parts of the Octopus Community, such as Cloud Evidence Working Group materials). In this regard, the online resource could be well used as a hub of trusted and verifiable information on provider policies, on the condition, however, that a dedicated effort is made to keep these documents up-to-date, as they change quite often.

Additional functionalities of creating and maintaining the exchange of professional information and advice through discussion forum were also suggested. In this way, the Octopus Community could be the used as a point of reference and initial contact for new or emerging providers, as they would be easier to approach from the Council of Europe than the law enforcement. At the same time, high-level and experienced experts would be more reluctant to post updates and information in such forums, so more integrated social media platforms, such as Facebook Workplace, could be used to steer the dialogue.

Moldova

The Octopus Community section on public-private cooperation was not used for practical purposes, as far as other resources, such as the European Judicial Network, provided useful information for cooperation purposes. As regards the Octopus Community, more integration of other professional communities, such as judiciary, would be of certain benefit, since the prosecutors and judges are often searching for country-specific information and would appreciate the resource geared to their needs. Information on foreign judiciary officers responsible for processing of cooperation requests would be also desirable, as well as more information about legal framework for the execution of requests, standard terms and templates, and the means of transmission of requests.

Other counterparts noted that the Octopus Community should be geared toward establishment and maintenance of partnerships. One such example could be networks of specialized prosecutions and country specific information, advice and support in developing such units. The resource could also support proactive and preventive action in relation for cybercrime by exploring more relationships between applicable legislation and its practical application.

In terms of additional functionality, the possibility to use public chats, feedback and discussion forums would greatly enhance the use of the Octopus Community. The platform also needs the administrator or moderator to supervise such functions, and to maintain private channels of communication for practical purposes.

Ukraine

For counterparts in Ukraine, the Octopus Community and its section on public-private cooperation should be expanded to support relevant investigations not just by information about laws and procedures, but also by facilitating access to methods on investigating crimes, including any applicable manuals, guides or other practice-oriented documents. Providing links to such information, categorized by various categories such as crime or security risks or similar criteria, could improve and expand the resource.

For counterparts related to investigations and security, another feature of the online resource would be specific information on whom to contact for assistance/request purposes and how soon an answer could be expected, as well as what form of request could be used and what are the conditions for receiving information. More focus on substantive law, such as the information on crime qualification in another countries and applicable sentences could be also relevant.

Conclusions and findings

By overall analysis of the responses given to questions and the wishes for the development of the public-private cooperation section of the Octopus Cybercrime Community, it is rather clear that the platform is underused for the purposes of accessing information to the EAP states. This could be due to the fact that the bulk of information was added and further refined in 2017 with the use of questionnaires sent to the EAP states; however, some of the indications for improvement of the resource, in particular related to additional information on legislation, reveal that the countries are not familiar with extensive information on legislation already contained in the resource.

The main suggestions by the country teams related to the existing version of the resource suggest expansion of more interactive elements, and could be potentially grouped into the following major categories:

- Additional functions related to discussion forums and platforms for exchange of ideas and information on various subjects, ranging from application of law to supporting institutional reforms, was among the most frequently requested features of the resource. This could be very relevant in connection with the topic as expansive and as multi-stakeholder as the public-private cooperation on cybercrime, and with proper structuring and/or moderation of discussions, could be well complementary to the work of the Council of Europe in terms of development of the standards for public-private cooperation, including the T-CY Cloud Evidence Working Group;

- The ability to launch and process the requests for cooperation through the online resource was the next most frequently recommended feature of the resource. This could provide particularly useful in the direct communications between the service providers based abroad due to providing a trusted platform for exchange, but hardly useful for the multinational service providers that majority of whom have set up specialized in-house portals for law enforcement requests. Nevertheless, this option could still be pursued in limited manner at least in terms of registering/tracking actual requests for data, as it would increase the transparency of the process.

- The expansion of the resource with additional information was also very frequently noted by almost all counterparts. Judging by their suggestions, perhaps the way forward is to include information that goes beyond and above what other sources and

resources collate in terms of supporting criminal investigations and prosecutions (such as EJN). For the Octopus Community, this means the collation of providers' policies and practices of cooperation, as well as information related to specialized cybercrime units and their *modus operandi*, data on formal or informal arrangements and partnerships necessary for the overall climate of public-private partnerships – in short, the information that would differentiate the online resource on public-private cooperation from other sources of data.

Irrespective of the feasibility to go forward with any or all of the improvement listed above, the way forward for the online resource on public-private cooperation under the Octopus Community would be dependent on the technical limitations of the current platform.