Cybercrime@EAP

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

Projects 3271 / 3608

Bucharest, 23 June 2017

Cybercrime strategies, procedural powers and specialised institutions in the Eastern Partnership region – state of play

Discussion paper prepared by the
Cybercrime Programme Office
of the Council of Europe (C-PROC)
under the Cybercrime@EAP projects

www.coe.int/cybercrime

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Contact
Cybercrime Programme Office of the Council of Europe (C-PROC)
Email cybercrime@coe.int

Contents

1 Background

The European Union and the Council of Europe have supported capacity building on cybercrime in the Eastern Partnership region, that is, Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine, through several projects.

CyberCrime@EAP from 2011 to 2014 was followed by CyberCrime@EAP II on international cooperation (May 2015 – December 2017) and Cybercrime @EAP III, on public/private cooperation (December 2015 – December 2017). The current Cybercrime@EAP projects are scheduled to end in December 2017. Reflections have commenced regarding capacity building projects beyond this period.

Countries of the Eastern Partnership have committed to implement the Budapest Convention on Cybercrime as a framework for domestic measures and for international cooperation on cybercrime and electronic evidence. All countries – with the exception of Belarus – are Parties to the Budapest Convention and are thus members of the Cybercrime Convention Committee (T-CY).[1]

During the CyberCrime@EAP project, Eastern Partnership countries furthermore identified the strengthening of capacities for international cooperation and public/private partnerships on cybercrime and electronic evidence as strategic priorities for the region.[2] A precondition for international and public/private cooperation is that criminal justice authorities have the necessary powers to investigate cybercrime and secure electronic evidence. Such procedural powers – corresponding to Articles 16 to 21 Budapest Convention – must be clearly defined in domestic criminal law and be subject to conditions and safeguards to meet rule of law requirements.

In December 2016, the European Commission and the European External Action Service established a set of "key priorities and deliverables" to be achieved by 2020 in their cooperation with the Eastern Partnership.

With regard to cybercrime, "milestones" to be discussed at the Eastern Partnership Summit (scheduled for November 2017) are:

- "Action Plans to address cybercrime adopted by Partner Countries."
- "Operational contact points for international police-to-police and judicial cooperation on cybercrime and e-evidence designated."

Targets for 2020 are:

- "Budapest Convention fully implemented, particularly as per procedural law for the purpose of domestic investigations, public-private cooperation and international cooperation."

1 Belarus participates in the T-CY as ad-hoc observer and has expressed its commitment to implement this treaty.

2 This was reconfirmed during the launching events of the CyberCrime@EAP II project in Bucharest in September 2015 and at the launching event of the CyberCrime@EAP III project in Kyiv in April 2016.

Within this context, the purpose of the present report is to facilitate reflections on milestones and targets by summarizing the current situation (as at June 2017) in EAP countries with respect to:

- action plans and strategic documents related to cybercrime;
- procedural law for the purposes of domestic investigations, public-private cooperation and international cooperation;
- operational cybercrime units in law enforcement authorities;
- authorities for international police-to-police and judicial cooperation on cybercrime and e-evidence.

This "state of play" may thus serve as a baseline against which to determine future progress. It should furthermore help design support beyond 2017 through Cybercrime@EAP projects in view of 2020 targets.

2 Country reports

2.1 Armenia

2.1.1 Action plans and strategic documents related to cybercrime

Armenia currently has no dedicated strategy or action plan on cybercrime as such in place or in development.

Although Armenia has not published a formal cybersecurity strategy, the National Security Service (NSS) is responsible for cybersecurity policy and the protection of government websites and networks. Furthermore, a concept for an Information Security Strategy was developed in 2009, which outlines certain activities to be implemented. The Digital Society 2020 Strategy includes certain measures regarding cybersecurity activities and laws in the area of cybersecurity and data protection, and is currently under discussion.

Annex 4 to the draft "Concept of E-Society development in Armenia" (2010) provides for the establishment of cyber-security working group, headed by the National Security Service, was tasked with the development of an action plan with the following elements: risk assessment, cyber security legislation, capacity building, compliance with ITU and ISO standards, sector-specific approaches, development of cybercrime legislation, awareness raising, training and establishment of coordination centre. No further progress has been noted regarding this draft.

2.1.2 Procedural law for the purpose of domestic investigations, public-private cooperation and international cooperation

Armenia signed the Budapest Convention on Cybercrime (ETS 185) on 23 November 2001 and ratified it on 12 October 2006. Armenia is a Party as from 1 February 2007.

The provisions on electronic evidence of the Convention for the purposes of criminal proceedings, as well as important definitions of subscriber information and traffic data, as required by the Convention, are not implemented in national law. An important effect of this is a lack of functional distinction between these categories of data in respect to procedural powers that apply to all categories of data (more specifically, preservation of data under Article 16 and production orders under Article 18.1.a Budapest Convention). The possibility of a lighter regime for access to subscriber information as opposed to traffic data should be explored.

Armenia so far has not implemented provisions on expedited preservation of stored computer data (Article 16 Budapest Convention) and expedited preservation and partial disclosure of traffic data (Article 17) as standalone measures in its procedural legislation. In the context of compliance with international requests for preservation received and processed by the authorities, search and seizure is the option used as an alternative. The Cybercrime Convention Committee (T-CY) has thus assessed Armenia not to be line with the Budapest Convention.[3]

There are also no specific provisions in domestic legislation with the scope and purpose corresponding to Article 18 Budapest Convention (production orders). Instead, it is argued that search and seizure is the default measure used to obtain stored computer data in a person's

[3] Assessment report: Implementation of the preservation provisions of the Budapest Convention on Cybercrime Adopted by the T-CY at its 8th Plenary (5-6 December 2012)
https://rm.coe.int/16802e722e

possession or control. In addition to general rules on search and seizure, investigative authorities are competent to order and withdraw computer (including subscriber data) in accordance with the Law on Operative-Detective Activities, on the basis of a court order.

In terms of search and seizure of stored computer data (Article 19), there are no provisions in the procedural legislation which would provide for a specific, computer-related search and seizure measures. Therefore, traditional powers of search and seizure of tangible objects are used to give effect to Article 19. A general requirement justifying application of the search measure is that there are "sufficient grounds to suspect that in some premises or in some other place or in possession of some person, there are instruments of crime, articles and valuables acquired by criminal way, as well as other items or documents, which can be significant for the case" (Code of Criminal Procedure, Article 225); the term "document" is interpreted broadly enough to cover computer data. From the formal viewpoint, search is executed on the basis of a court order (same Article, par. 3).

Implementation of special provisions in the context of search and seizure provided by Article 19 (search of a connected system; making and retaining a copy of those computer data; maintaining the integrity of the relevant stored computer data; rendering inaccessible or removing those computer data in the accessed computer system) is not provided by the procedural legislation of Armenia. At the same time, provisions related to seizing or similarly securing computer data (p. 3(a)) and assistance of specialists in technical matters (p. 4) are addressed by general regulations on seizure and involvement of specialists and experts in the criminal proceedings.

In Armenian legislation, no distinction is made between the real-time collection of traffic data and interception of content data (Articles 20 and 21 Budapest Convention). The same set of legal rules, conditions and safeguards is used in relation to both of these measures. The Code of Criminal Procedure (Articles 239 and 241) provides for general legal conditions for the execution of these measures, while the Law on Operative-Detective Activity defines, in its Article 26, general measure of wiretapping, also applicable to computer data. Under this Article, it is possible to collect certain categories of data which qualify as traffic data in the terms of Convention using general wiretapping procedure.

In terms of horizontally applicable conditions and safeguards (Article 15 Budapest Convention), although most of the elements limiting and controlling the application of more intrusive measures (search and seizure, real-time collection of traffic data and content interception) are present - such as existence of criminal investigation, judicial order, limitation as to gravity of offences and other conditions – the system of safeguards and guarantees is not implemented in a way that encourages application of less intrusive procedural powers before more intrusive options. The absence of clear 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 the intrusion into privacy of individuals.

Armenia has initiated comprehensive reform of its criminal procedure legislation several years ago (the start of formal process dating back to 2009). The draft Code of Criminal Procedure now seems to be at the final stages of approval by a Working Group of experts at the Ministry of Justice and is expected to be submitted for parliamentary hearings in autumn 2017. The draft Code would lead to closer implementation of the relevant provisions of the Budapest Convention. Council of Europe experts – through the Cybercrime@EAP projects – reviewed the draft in May 2017 and presented recommendations for refining cybercrime-related provisions.

2.1.3 Operational cybercrime units in law enforcement authorities

The Division for Combating High-Tech Crime under the General Department on Combating Organized Crime at the Police of the Republic of Armenia is a centralized unit which is responsible for handling cybercrime with country-wide competency. The police have 10 days to determine the facts and the legal basis for the investigation and then deciding either to close the matter, send the case to local police where evidence or a perpetrator is located, or to transfer the matter to the Investigative Committee. Thus, the Division is the primary police unit handling cybercrime cases at the preliminary stage (before an official investigation is opened by the Investigative Committee) and providing support to local units.

There are 8 officers employed at the Division for Combating High-Tech Crime of Armenian police. There are no specialised local units; where necessary, additional resources of the Organized Crime Department are used (either at the local offices or the headquarters). The Division is competent to investigate offences committed against computer systems such as hacking, attacks on the critical infrastructure, illegal interception and data interference. The Division is also competent to deal with offences involving technology such as computer related fraud, Internet crimes, and offences involving the abuse of children, intellectual property offences as well as racism and xenophobia.

Since the reform of the criminal procedure in 2011, 95% of the criminal cases in Armenia are investigated by the Investigative Committee of the Republic of Armenia, the remaining cases being handled by specialized units for tax and customs fraud or investigations into public officials. The Committee has 6 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 makes use of external expertise for the analysis of electronic evidence.

Where an expert evaluation is necessary, it is performed at specialised centres, in particular the National Bureau of Expert Evaluation that is a state non-commercial centre of Armenia's Academy of Sciences.

On 23 November 2015 the Investigative Committee signed a Memorandum of Understanding with Armenian Internet service providers, such as ArmenTel, K-Telecom, UCom, Orange Armenia, with the intention of reducing workload and saving human resources. The main goals of the Memorandum are to undertake effective joint measures in the direction of operative transmission of court decisions and transcripts, and to develop mutual cooperation on introduction of technical capabilities. Within this framework, parties agreed to communicate in 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 providers agreed to process electronic transmissions from 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 set period of time on a voluntary basis.

2.1.4 Authorities for international police-to-police and judicial cooperation on cybercrime and e-evidence

2.1.4.1 24/7 points of contact and police cooperation

In Armenia, the Division for Combating High-Tech Crime under the General Department on Combating Organized Crime at the Police of the Republic of Armenia, processes requests for police-to-police cooperation under the Budapest Convention and the G7 networks on 24/7 contact

points. It processes only operative and intelligence information (cannot be used as evidence in criminal proceedings) and does not receive and process mutual legal assistance requests. Information received through the 24/7 point of contact is forwarded to competent investigative authorities; if the specific investigative action is required, referral is done through the Prosecutor's Office. Technical assistance and support and advice can be provided by the 24/7 point of contact.

The data preservation process involves a number of distinct steps. Step 1 is to register incoming request, followed by confirmation of receipt by email delivery/email opening report (if requested by sender). At the next stage, a legal review as to the lawfulness of the request and whether the information requested is of operative/intelligence nature is performed. In case of operative-intelligence request being determined, the request is cleared and sent for execution to service provider/person for compliance (no guarantees for response due to lack of legal framework). However, if the request is determined to require investigative actions, the request is sent back with an indication that an MLA process is required. This also applies to all cases concerning content data.

In cases of terrorism or similar offences, urgent measures can be undertaken provided that the approval of the court is received within 24 hours. Particular measures/steps will be decided on a case-by-case basis.

2.1.4.2 Mutual legal assistance authorities

At the stage of pre-trial investigation, the competent authority for MLA is the Department for International Cooperation and Legal Support at the Prosecutor General's Office. According to the authorities, a prerequisite for request at this stage is the Red Notice / Diffusion Notice (circulated by Interpol) Reciprocity is also a prerequisite – written confirmation from the requesting state is necessary.

At the trial stage, the Ministry of Justice (Department for International Legal Assistance) is in charge of the MLA process. A prerequisite for the request is the Red Notice by Interpol / Diffusion Notice (attached to request). Request according to the European Convention on Extradition of 1957 should be supported by documents noted in Article 12 Budapest Convention. In general, an indication of clear legal basis for the request is necessary; otherwise, reciprocity is a prerequisite – in the form of express written assurance of reciprocity from the requesting State.

In the absence of treaties and on the basis of reciprocity, the Ministry of Foreign Affairs (Consular Department) is the channel through which the request is received. The Ministry of Justice is the consenting body for reciprocity. The request has to include assurances of reciprocity. Only the official written request needs to go through the Ministry of Foreign Affairs.

Armenia can provide preliminary consultations on international requests for assistance without limitations concerning the seriousness of offences; email communications are preferred for the consultation process. Following the receipt of the original request in non-electronic form, Armenian competent authority will take the initiative of seeking clarifications where necessary.

For outgoing requests, at the pre-trial stage the General Prosecutor's Office receives communications from investigative agencies and, if there is no specific treaty basis to continue otherwise, the request is translated and sent to the Ministry of Foreign Affairs for processing via diplomatic channels. The process is the same for trial stage and is performed via the Ministry of Justice.

2.2 Azerbaijan

2.2.1 Action plans and strategic documents related to cybercrime

There is are 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 main objective of the strategy is to build an information society and effective use of its capabilities by citizens, society and the State for the sustainable socio-economic, cultural and economic development of the country, including the development of ICT. Section 2.2.9 of the Strategy in particular concerns "ensuring information security through training and awareness raising" (it has to be noted that concepts of information and cyber security are often meant to be the same in the practice of post-Soviet States).

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.

2.2.2 Procedural law for the purpose of domestic investigations, public-private cooperation and international cooperation

Azerbaijan signed the Convention on Cybercrime on 30 June 2008 and ratified it on 15 March 2010 with entry into force on 1 July 2010.

The provisions on electronic evidence of the Convention for the purposes of criminal proceedings, as well as important definitions of subscriber information and traffic data, as required by the Convention, are not implemented in national law. An important effect of this is a lack of functional distinction between these categories of data in respect to procedural powers that apply to all categories of data (more specifically, preservation of data under Article 16 and production orders under Article 18.1.a Budapest Convention). The possibility of a lighter regime for access to subscriber information as opposed to traffic data should be explored.

The Republic of Azerbaijan does not implement expedited preservation of stored computer data (Article 16 Budapest Convention) as a standalone measure. In order to achieve the purpose of this article production order (Article 143, p. 2 of the Criminal Procedure Code) is used, and search and seizure is an available alternative.

As regards expedited preservation and partial disclosure of traffic data (Article 17 Budapest Convention), there is a *sui generis* possibility for its application: in general, while there is no legal obligation for service providers to retain traffic data, on the basis of the Law on Intelligence and Counter-Intelligence Activities (Articles 17 and 39), communication operators are required to establish an "appropriate level of cooperation with [...] authorities", thereby enabling and assisting in the execution of some of the procedural measures in criminal cases. At the same time, a clear implementation of Article 17 as a logical progression from the provisions of Article 16 Budapest Convention is not present in the procedural law of Azerbaijan. Access to data about

communications stored by service providers requires a court order, thus expedited disclosure of traffic data raises concerns.

The general legal framework for production orders (Article 18 Budapest Convention) is established by Article 143 of the Criminal Procedure Code, which, as read in conjunction with Article 135 of the CPC, enables authorities to request production of any type of stored computer data. However, article 143.2 of the CPC provides only for the possibility of *voluntary* production of data and as such does not have to be based on the court order. In the situation when the production of data is refused, the only workable alternative is search and seizure.

There are no specific provisions on search and seizure of stored computer data in Azeri procedural legislation; therefore, the legal framework for traditional search and seizure is applicable. In order for a search measure to be executed, it is necessary that a formal investigation is opened and, as a general rule, search and seizure can be conducted on the basis of a court order (Criminal Procedure Code, Article 243, p. 1). Search orders can be issued when "available evidence or material discovered in a search operation give rise to a suspicion that a residential, service or industrial building or other place contains, or certain persons are in possession of, objects of potential significance to a case".

Implementation of special provisions in the context of search and seizure provided by Article 19 (search of a connected system; making and retaining a copy of those computer data; maintaining the integrity of the relevant stored computer data; rendering inaccessible or removing those computer data in the accessed computer system) is not found in the procedural legislation of Azerbaijan. At the same time, provisions related to seizing or similarly securing computer data (p. 3(a)) and assistance of specialists in technical matters (p. 4) are covered by general regulations on seizure and involvement of specialists and experts in the criminal proceedings.

In general, Azeri legislation does not differentiate between real-time collection of traffic data and interception of content data (Articles 20 and 21 Budapest Convention); therefore, it would appear that the same set of rules is applicable in both cases. However, it was reported that Azeri authorities do not apply real-time collection of traffic data in practice. In any case, should the real-time collection of traffic data be executed in Azerbaijan, it would have to follow the legal framework established for interception of content data.

Article 21 Budapest Convention is implemented in Azeri legislation through an article entitled "Interception of conversations held by telephone and other devices, of information sent by communication media and other technical means, and of other information", which is one of the "investigative procedures" enumerated in Article 177 p.3 of the Criminal Procedure Code and regulated in more details in Article 259 of the same Code. In addition, the subject-matter of article 21 Budapest Convention is also covered by Article 10 of the Law on Operative-Detective Activity, which provides for a list of detective-search actions and includes, *inter alia*, examination of "other correspondence" alongside telephone conversations/telegraph messages. Court order is the main condition for the application of measures of interception of content; the aforementioned actions can only be executed when it is impossible to achieve the goals of the law by other (less invasive) means. Maximum duration of interception is set to six months.

In terms of horizontally applicable conditions and safeguards (Article 15 Budapest Convention), although most 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 – such as existence of a criminal investigation, judicial order, exhaustion of lesser options and other conditions – the system of safeguards and guarantees is not implemented in a 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 into the privacy of individuals.

The authorities of Azerbaijan have recently (April 2017) re-engaged in a dialogue with the Cybercrime Programme Office of the Council of Europe in order to start revising the criminal procedure and related legislation to achieve closer compliance with the Budapest Convention; the first discussions in Baku on the subject were held on 10-12 May 2017 and led to production of the report that highlights specific problems and suggests generic/concept set of provisions to address the above-mentioned gaps in procedural law.

2.2.3 Operational cybercrime units in law enforcement authorities

In Azerbaijan, the State Security Service has a Department of Combating Crimes in Communications and IT within the General Directorate of Combating Organised Transnational Crimes. It has the powers to investigate computer-related crimes, including hacking attacks against computers and vital state infrastructure, illegal interception and interference with data, computer-related fraud, crimes on the Internet, child abuse, and racism. Its activities mainly aim at fighting child pornography, signs of terrorism in the Internet, embezzlement and fraud related to use of IT and Internet. The number of reported and investigated cases is very low, keeping in the single digits for recent years.

There are ongoing discussions since 2016 to establish a dedicated unit to fight cybercrime within the police under the Ministry of the Interior; currently there is a small team of officers designated for the task. However, the police are not yet fully investigating, but currently view their role more of a supportive and advisory body to other units of the police that handle cybercrime and electronic evidence. An internal forensic team is supporting the work of the Ministry in this regard.

There are indications of reform by which more investigative powers would be transferred to the Ministry of the Interior from the State Security Service; in this light, the Ministry of the Interior would have a more prominent role in investigating cybercrime offences and dealing with electronic evidence in the near future.

2.2.4 Authorities for international police-to-police and judicial cooperation on cybercrime and e-evidence

2.2.4.1 24/7 points of contact and police to police cooperation

The authority in charge of the 24/7 contact point is the Department of Combating Crimes in Communications and IT of the General Directorate of Combating Organised Transnational Crimes at the State Security Service of the Republic of Azerbaijan.

With regard to requests, the following steps are involved: confirmation of receipt (if requested); legal review as to national and international requirements (within 3 days); if necessary, sending request back for additional clarifications or, otherwise, proceeding with the request or refusing to comply; if acceptable, sending the request for execution to provider/person.

Follow up is undertaken in cases of urgency or where a specific time for a response was requested and there is no feedback from the provider. Requests should in principle be executed within a 10-day period after receipt, as set by an applicable order of the Prosecutor General (in exceptional cases the execution can be prolonged, but not more than 2 months).

There is no special difference in terms of execution of urgent or regular requests.

2.2.4.2 Mutual legal assistance authorities

The International Relations Department of the Prosecutor General's Office is the central authority at the pre-trial stage. Reciprocity and dual criminality are important pre-requisites for mutual legal assistance; the choice of channels of communication is irrelevant as the General`s Prosecutor Office would be the central recipient in all cases. The preferred means of communication include regular mail, email or fax.

At the stage of trial proceedings, the Ministry of Justice is the competent authority. A clear indication of the legal basis for the request is necessary; otherwise, reciprocity is a prerequisite in the form of express written assurance of reciprocity from the requesting State. Preferred means of communication include regular mail, email or fax.

For outgoing requests, the investigative or judiciary authority decides on the necessity of initiating a request; in such a case, all relevant materials of the case are collected, translated and sent to the competent authority for legal assistance (Ministry of Justice or the Prosecutor General's Office). After check of the request against applicable legal requirements, the request is sent to the requested State through diplomatic channels or directly, whenever the treaty permits this.

2.3 Belarus

2.3.1 Action plans and strategic documents related to cybercrime

There is are no dedicated strategy 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.

2.3.2 Procedural law for the purpose of domestic investigations, public-private cooperation and international cooperation

Belarus has not yet acceded to the Budapest Convention on Cybercrime (ETS 185) but has expressed a strong interest in accession.

The provisions on electronic evidence of the Convention for the purposes of criminal proceedings, as well as important definitions of subscriber information and traffic data, as required by the Convention, are not implemented in national law. An important effect of this is a lack of functional distinction between these categories of data in respect to procedural powers that apply to all categories of data (more specifically, preservation of data under Article 16 and production orders under Article 18.1.a Budapest Convention). The possibility of a lighter regime for access to subscriber information as opposed to traffic data should be explored.

The Decree of the President of the Republic of Belarus No. 60 "On the issues to improve making use of the national segment of Internet" (1 February 2010) covers data retention and some of the issues which are subject-matter of Articles 16 and 17 Budapest Convention, namely, expedited preservation of stored computer data and expedited preservation and partial disclosure of traffic data. This decree mandates that Internet service providers "identify user's terminals when providing services", and "register and store data on the users' terminals and information on Internet services provided". In addition, owners of Internet share points (computer clubs, Internet-cafes, home networks and other locations where public access to the Internet is possible) or persons authorised by them are required to enable identification of their Internet users and store their personal data and information on internet services provided to those users. However, this does not amount to full implementation of Articles 16 and 17, as the retention of data is *not* identical with the scope and purpose of these Articles.

Regarding production orders under Article 18 Budapest Convention, Article 103, p. 2 of the Criminal Procedure Code of Belarus provides only general guidance as to the handover of documents by any person at the request of an investigator, as sanctioned by the prosecutor. Additionally, according to the Law on Agencies of Internal Affairs, internal affairs agencies are authorized to carry out operative investigations and to, inter alia, "request and receive from companies and people data and explanations as to inspected activity; to schedule inventory count and inspections; to request and, where necessary, seize documents" and so on. However, the provisions of the Article 18 Budapest Convention require more specific implementation and clarity than currently is the case.

Article 19 Budapest Convention on the search and seizure of stored computer data is generally implemented in the Belarus legislation via traditional search provisions contained in chapter 24 of the Criminal Procedure Code. According to article 208 of the CPC, searches can be executed when

there is reasonable evidence to believe that the instrument of crime, items, records, and valuables which may be critical for criminal investigation may be kept on specific location or held by specific person. In the similar manner, Article 209 states that "reasonable evidence indicating that certain items or records which are critical for criminal investigations are available, provided that the location and possessor thereof have been clearly identified, constitutes grounds for a seizure". Belarus does not provide for judicial supervision of search and seizure measure, as the order of investigator or prosecutor (or, in special cases, heads of investigative units) is sufficient in this respect (Article 210 of the Code of Criminal Procedure).

Implementation of special provisions in the context of search and seizure provided by Article 19 (search of a connected system; making and retaining a copy of those computer data; maintaining the integrity of the relevant stored computer data; rendering inaccessible or removing those computer data in the accessed computer system) is not found in the procedural legislation of Belarus. At the same time, provisions related to seizing or similarly securing computer data (p. 3(a)) and assistance of specialists in technical matters (p. 4) are covered by general regulations on seizures and involvement of specialists and experts in criminal proceedings.

The real-time collection of traffic data (Article 20 Budapest Convention) is performed on the basis of the Law on Investigation Activities. The relevant provision in this regard is article 11, sub-paragraph 12, which provides for a power to "retrieve information from telecom channels", as well as Article 18, sub-paragraph 12, which provides for a power to "exercise control in electronic communications networks".; no judicial authorization is provided. As the real-time collection of traffic data is considered to be the measure which limits constitutional right to privacy, Article 13 of the said Law stipulates that this measure under Article 12 can only be executed on the basis of prosecutor's warrant, upon a "well-grounded order of a respective agency responsible for operational investigation", while Article 19 of the said Law stipulates that measure under Article 18 can only be executed on the basis of a resolution issued by an authority conducting operational and search activities and sanctioned by the prosecutor or deputy thereof; no judicial authorization is provided in either case. Article 13 additionally provides for certain time-limits of the duration of the power to "retrieve information from telecom channels".

The legal framework for interception of content data (Article 21 Budapest Convention) is established in several sources of law. Article 214 of the Code of Criminal Procedure provides for a general power to monitor and record communications. According to this provision, "communications may be monitored and recorded subject to the warrant issued by the prosecutor or deputy thereof, or, alternatively, subject to the resolution of the Chairman of the Investigative Committee, Chairman of the State Security Committee, or officials acting in their capacity"; no judicial authorization is provided. From the technical perspective, the interception of content data is facilitated by Decree of the President of Belarus of 3 March, 2010, No 129 "On Cooperation between Telecommunication Operators and Authorities conducting Operational and Search Activities".

In terms of horizontally applicable conditions and safeguards (Article 15 Budapest Convention), 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 system of safeguards and guarantees is not implemented in a way that encourages application of less intrusive procedural powers before more intrusive options are applied. The absence of clear and enforceable regulations implementing Articles 16-18 Budapest Convention is another obstacle to a coherent system of safeguards and guarantees which limits intrusion into the privacy of individuals.

2.3.3 Operational cybercrime units in law enforcement authorities

Since 2002, there is a High-Tech Crime Department within the Ministry of Interior of Belarus (Department "K") whose competency is to detect and deal with crimes against information security, embezzlement by means of computers, including that conducted by means of stolen and forged bank cards or their details, and to counter the distribution and advertising of child pornography on the Internet. Besides preliminary investigations, the Department "K" also assists other units across the country in matters of cybercrime and electronic evidence. There are currently 25 officers at the headquarters of Department "K".

In five regional centres of Belarus, territorial units have been established to counter hi-tech crime. The average staffing of units is 7 persons.

Since 2012, there is also a specialised unit within the Investigative Committee of the Republic of Belarus, that is, High Tech Crime and Intellectual Property Department; its function is to initiate criminal proceedings and conduct full investigations of detected criminal activities. It now employs about 30 officers dedicated to cybercrime/high-tech investigations, out of which 10 are located at headquarters.

The roles between police officers and officers of the Investigative Committee are divided as follows: officers of Department "K" of the Ministry of Interior collect information on circumstances that are evidence of cybercrime, register illegal activities and, if there is sufficient data for opening a criminal case, hand over the material collected to the Investigative Committee. Investigators of the Committee make a decision on opening a criminal case and proceed with the investigation. Throughout the investigation, Department "K" and the Investigative Committee cooperate with each other. When the investigation is complete, the criminal case is transmitted to the supervising prosecution office for further hearings in court.

When a more thorough examination of evidence or electronic media is required, an examination by a computer or other specialised expert can be organized. Such expert examination is the competency of qualified experts of the Forensic Centre of the Ministry of Interior of Belarus.

2.3.4 Operational contact points for international police-to-police and judicial cooperation on cybercrime and e-evidence

2.3.4.1 24/7 points of contact and police cooperation

The national authority for the 24/7 point of contact is the High-Tech Crime Department within the Ministry of Interior of Belarus (Department "K") .

The 24/7 contact point does not confirm receipt of data preservation requests. Upon receipt of a preservation request, a legal review as to national and international requirements is performed within 24 hours, another 24 hours is reserved for decision on returning the request for additional clarifications, proceeding with the request or refusing to comply. In case of approval, the request is sent for execution to the relevant provider/person within 24 hours of approval. Providers undertake necessary activities for data preservation during the working hours and within a few days upon the written inquiry.

Urgent procedures are not stipulated in the Criminal Procedure Code of the Republic of Belarus, but in case of need and possible public danger (due justification is important) every kind of legal assistance sought in a criminal case can be rendered within the shortest term.

2.3.4.2 Mutual legal assistance authorities

At the pre-trial stage of criminal proceedings, Office of the Prosecutor General of the Republic of Belarus, International Legal Department is deemed to be central authority for mutual legal assistance in criminal cases based on the principle of reciprocity.

At the trial stage of criminal proceedings, the competent authorities are the International Legal Department of the Office of the Prosecutor General and the Supreme Court of the Republic of Belarus; the latter is competent only for submitting procedural or other documents in criminal cases under trial and execution of sentences (and also in relation to other decisions of the court in criminal proceedings).

In the course of implementation of international cooperation in criminal cases and preparation of the corresponding requests for legal assistance on the basis of a treaty, the Office of the General Prosecutor is always indicated as the central competent authority. In case of a treaty basis, the Republic of Belarus additionally determines national competent authorities specific to the treaty (the following authorities are often mentioned: the Investigative Committee of the Republic of Belarus, the State Security Committee of the Republic of Belarus, the Ministry of Internal Affairs of the Republic of Belarus, the State Control Committee of the Republic of Belarus and others), or may choose to keep the Prosecutor's Office as single authority. This does not apply in the course of implementation of international cooperation based on the principle of reciprocity, where the Office of the Prosecutor General represents the only central competent body.

For outgoing requests, the authority in charge of the criminal case sends a draft of the request to the competent authority that can approve the request or ask for clarifications/corrections. Once cleared, the request and attached materials are sent to the foreign competent authority either through diplomatic channels or directly – in which case the requesting criminal justice authority is notified of progress.

2.4 Georgia

2.4.1 Action plans and strategic documents related to cybercrime

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.

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.

2.4.2 Procedural law for the purpose of domestic investigations, public-private cooperation and international cooperation

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

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 not make a distinction between categories of data and procedural powers apply to them. The possibility of a lighter regime for the production of subscriber information as opposed to traffic or content data should be explored.

Georgia did not implement Article 16 Budapest Convention on expedited preservation of stored computer data as a standalone measure. The production order provisions of Article 136 of the Criminal Procedure Code can be used due to their broad interpretation in practice; alternatively, search and seizure in exigent circumstances can be used to address this issue in a similar manner. Although this is deemed as an acceptable level of implementation, it is recognized that a standalone power of preservation of data would be a preferable and more complete implementation of the Convention requirements.

There is also no direct implementation of the power of expedited preservation and partial disclosure of traffic data (Article 17 Budapest Convention). Similar to Article 16 implementation, due to broad interpretation of production order under Article 136 of the Georgian CPC, it can be used as an alternative; on the other hand, preservation of traffic data is a specific task in the sense that it can require cooperation between several service providers when it is necessary to reconstruct the whole chain of communications. In this regard, Article 136 can be seen as an acceptable but otherwise partial implementation of Article 17 Budapest Convention.

In general, subject-matter of Article 136 of the Georgian CPC is the production order, which is an issue primarily relevant in the context of Article 18 Budapest Convention. The terms of this provision are of open nature and can cover requests directed to any person (ISP, individual or organization). Taking into account the fact that any case of non-compliance could potentially be

treated as tampering with evidence, which is a criminal offence under Georgian law, order based on Article 136 of the CPC creates a significant legal obligation on the part of its addressee. At the same time, several conditions have to be fulfilled: on-going formal investigation is an absolute prerequisite; the need for an investigative action in all cases shall be based upon the probable cause standard; judicial order, issued on a motion of a prosecutor, is needed to apply this measure. Procedure for issuing such an order is regulated extensively in Article 112 of the Georgian CPC.

Georgian legislation does not implement search and seizure of stored computer data under Article 19 Budapest Convention as a specific measure applicable for computer-related search and seizure; instead, traditional measures of search and seizure are applicable also to computer system and data. General rules establishing grounds for search and seizure are contained in article 119 of the Code of Criminal Procedure, which is a procedure driven by a judicial order, unless being performed in exigent circumstances with subsequent authorization from the judge.

Georgia has not implemented special provisions in the context of search and seizure provided by Article 19 (search of a connected system; making and retaining a copy of those computer data; maintaining the integrity of the relevant stored computer data; rendering inaccessible or removing those computer data in the accessed computer system) in its procedural legislation. At the same time, provisions related to seizing or similarly securing computer data (p. 3(a)) and assistance of specialists in technical matters (p. 4) are covered by general regulations on seizure and involvement of specialists and experts in the criminal proceedings.

Article 20 Budapest Convention providing for real-time collection of traffic data is directly implemented in Georgian legislation by Article 137 of the Criminal Procedure Code. Conditions and safeguards used in connection with this measure generally follow the same principles as in cases of other procedural measures required by the Convention (production order and search and seizure). While the on-going formal investigation is an absolute prerequisite for this measure, Article 143^3 of the Code of Criminal Procedure lists additional limitations as to the offences for which it can be applied; this investigative power is also conducted on the basis of a court order.

The interception of content data (Article 21 Budapest Convention) is also directly implemented in Georgian legislation by Article 138 of the Criminal Procedure Code. The necessary conditions and safeguards include on-going formal investigation, probable cause, court order, and limitations in time. Georgian legislation, in particular Article 143^3 of the Code of Criminal Procedure, also limits application of interception measures to "intentionally serious and/or particularly serious offence", as well as detailed list of other offences in respect of which this power may be applied; this reflects the requirement of Article 21 Budapest Convention, which states that measures defined therein should be used "in relation to a range of serious offences to be determined by domestic law".

In terms of horizontally applicable conditions and safeguards (Article 15 Budapest Convention), although most 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 – such as existence of criminal investigation, judicial order, time limitations and other conditions – the system of safeguards and guarantees encourages application of less intrusive procedural powers (before more intrusive options) only in relation to secret/covert investigative measures (Article 143^3 of the Code of Criminal Procedure).

At the time of reporting (May 2017), Georgia has initiated a reform of its procedural legislation to address the issues of data preservation and production orders in line with the Budapest Convention. The Cybercrime Programme Office of the Council of Europe was actively involved by providing expertise and advice to this process.

2.4.3 Operational cybercrime units in law enforcement authorities

The separation of investigative jurisdiction in Georgia is regulated under Decree 178 of the Minister of Justice of Georgia. The document underlines that the investigative jurisdiction in general is vested in the investigative agencies of the Ministry of Internal Affairs, with some exceptions specifically listed in the Decree (such as crimes investigated by Investigative Division of the Ministry of Finance of Georgia).

Cyber Crime Division of the Central Criminal Police Department at the Ministry of Internal Affairs of Georgia was established by the decree of the Minister of the Interior in December 2012. Currently, there are 15 detective-investigators within the Division who are responsible for investigation of cybercrime. The Division is competent to investigate cybercrime offences in narrow sense, in particular crimes provided for in Chapter 15 (Cybercrime) of the Criminal Code of Georgia; however, the Division also provides advice, guidance and technical assistance to other police units across Georgia in investigation of cybercrime and handling of electronic evidence. The forensics team of the Ministry of the Interior handles the forensic examination duties.

Following legislative reform in 2014, the Ministry of State Security has been established separate from the Ministry of the Interior. The Ministry inherited the team of former Operative-Technical Department of the Ministry of the Interior, which now acts as a cybercrime investigation team of within the Ministry.

Since 2010, a Memorandum of cooperation between Internet Service Providers and Law Enforcement Agencies is in force. Ten largest ISPs representing the majority of the Internet industry and the representatives of government agencies, such as Prosecution Service and the Ministry of the Interior, signed the memorandum in January 2010. The Memorandum defines the principles of cooperation between ISPs and law enforcement agencies in the process of investigation of cybercrime and specifies the rights as well as responsibilities of the parties to the memorandum. Among the most important achievements under the document is the creation of specialized contact points within the structure of ISPs and the law enforcement, and significant reduction of time for processing of law enforcement requests.

2.4.4 Authorities for international police-to-police and judicial cooperation on cybercrime and e-evidence

2.4.4.1 24/7 points of contact and police cooperation

The 24/7 National Contact Point is operating at the Cyber Crime Division of the Central Criminal Police Department at the Ministry of Internal Affairs of Georgia.

In case of requests for preservation of data, the request is recorded and receipt is confirmed by email upon delivery/opening report (if requested by sender). The next step is an initial review as to dual criminality for which the judicial cooperation central authority may be consulted. If approved, the relevant ISP is approached and requested to preserve data, and if ISP confirms data preservation, requesting authority will be notified accordingly. If preservation is not available, requesting country is offered urgent MLA procedures.

Given the nature of preservation requests they are all treated as urgent.

2.4.4.2 Mutual legal assistance authorities

Georgia uses a single central authority for MLA requests irrespective of the stage of proceedings, namely, the International Cooperation Unit of the Department of Legal Affairs, Office of the Chief Prosecutor at the Ministry of Justice of Georgia. Although requests can be technically transmitted via 24/7 contact point or Interpol point, they must be addressed to the central authority.

A preliminary consultation is not an obligation but highly recommended as specific restrictions apply to access to electronic data. Hence, prior consultation may prevent waste of costs for requests that have no prospect. Consultation can be provided via designated e-mail. The 24/7 point of contact provides similar consultations at the designated email address but keeping the Prosecutor's Office in copy is advisable. The Georgian Central Authority may also review draft request if asked to do so.

As to outgoing requests, prosecution offices are allowed to draft their requests and submit them to the central authority, while defence attorneys should file a motion with the court which would then initiate the same process of communicating with the central authority. All requests are screened for quality before sending, and foreign countries' legal requirements are checked against a database of requirements kept by the central authority.

2.5 Moldova

2.5.1 Action plans and strategic documents related to cybercrime

So far, there are no dedicated strategies/action plans on cybercrime currently in force in Moldova. However, 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 section focuses on the further development of legislation, training of law enforcement, implementation of Council of Europe recommendations on the subject, accession to the Additional Protocol to the Budapest Convention on Cybercrime, ensuring compliance with the Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention), further regulatory framework study, and further strengthening of capacitates of authorities tasked with preventing and combating cybercrime.

Other sections of the draft Programme on Ensuring Cybersecurity aim to achieve safe processing, storage and access to data; security and integrity of electronic communications networks and services; capacities of prevention and emergency response (CERT); strengthening cyber defence capacities; education and information; and international cooperation and contact. The Cybercrime Programme Office of the Council of Europe was asked to provide corresponding expertise and has engaged the experts to provide comments on the draft Programme in November 2015.

Until the draft Programme is adopted, the Moldovan authorities are guided by the action plan on the implementation of the National Strategy for Information Society Development, Digital Moldova 2020, approved under the Government Decision No 857 of 31 October 2013.

2.5.2 Procedural law for the purpose of domestic investigations, public-private cooperation and international cooperation

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.

A 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. However, although the formal difference between these terms is captured in law, neither functional distinction in terms of applicability to certain procedural powers that cover all types of data (data preservation and production orders being prime examples), nor gradual and coherent applicability of safeguards and guarantees to accessing different types of data through such procedural powers can be found in the legislation of Moldova. Despite availability of definitions, the inconsistent use of terms across different legal acts ("computer information", web traffic data", etc.) is also noted as a potential problem.

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.

Expedited preservation of stored computer data (Article 16 Budapest Convention) is directly implemented by Article 7(c) of the Law on Prevention and Combating Cybercrime of Moldova. However, implementing provision - Article 7 of the said Law - creates obligations for service

providers only; it should be noted that Article 16 Budapest Convention concerns not only traffic data generated by the e-communication service providers but any stored data, i.e. held or processed by other persons or entities.

Expedited preservation and partial disclosure of traffic data under Article 17 Budapest Convention is also directly implemented by Article 7, par. 2 of the Law on Prevention and Combating Cybercrime of Moldova. It follows closely the language Budapest Convention; however, an element of required expediency is missing. Traffic data can also be preserved on the basis of a request by the competent authorities under Article 7 of the said Law.

Production order (Article 18 Budapest Convention) provisions are implemented under Article 7(d) of the Law on Prevention and Combating Cybercrime and are also applicable to service providers – this power is meant to be applied to any person/entity that is in possession or in control of certain computer data. Also the scope of information covered by the text refers only to subscriber information, implementing only the requirements of Article 18.1.b Budapest Convention; provisions of Article 18.1.a are not properly addressed within the Law.

In terms of search and seizure of stored computer data under Article 19 Budapest Convention, the current legislation of Moldova (Articles 125 and 126 of the Code of Criminal Procedure) is tailored mostly to tangible objects to be searched and seized (instruments used for the commission of the crime, objects and valuables resulting from the crime and other objects and documents that may be of interest for the case); all three categories are interpreted broadly in practice to apply to a computer system. Search and seizure is a procedure driven by a judicial order, unless being performed in exigent circumstances with subsequent authorization from the judge.

Special provisions in the context of search and seizure provided by Article 19 (search of a connected system; making and retaining a copy of those computer data; maintaining the integrity of the relevant stored computer data; rendering inaccessible or removing those computer data in the accessed computer system) are not implemented in Moldovan procedural legislation. At the same time, provisions related to seizing or similarly securing computer data (p. 3(a)) and assistance of specialists in technical matters (p. 4) are covered by general regulations on seizure and involvement of specialists and experts in the criminal proceedings.

Implementation of Article 20 Budapest Convention on real-time collection of traffic data can be found in Article 18, p. 1.1(e) of the Law on Operative and Investigative Activity of Moldova. Notably, application of this operative-detective power can produce evidence admissible in criminal proceedings (Art. 24 of the same Law). However, the level of detail and precision in terms of both data and specific procedures that should be defined in law, as required by the Convention and related standards, is not properly addressed.

With regards to the interception of content data Article 21 Budapest Convention, Article 135 of the Code of Criminal Procedure refers to the interception of communications (wiretapping), which can be extended also to computer data. Similar to real-time collection of traffic data, concerns apply to precise definition of the content of communications that should be necessary to properly implement Article 21 Budapest Convention. At the same time, procedures are more detailed compared to real-time collection of traffic data; both of these powers require judicial authorisation.

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.

Moldova initiated a reform of many facets of its criminal procedures in 2014 by introducing draft package of amendments to all of the laws and regulations mentioned above, with one of the purposes being closer implementation of the Budapest Convention and more effective cooperation between law enforcement and the Internet service providers. However, the discussion became controversial, which led to review of the prepared draft amendments by the Venice Commission of the Council of Europe in November-December 2016; two experts were assigned to the task of reviewing the cybercrime/electronic evidence provisions of the proposed amendments, with the support of the Cybercrime Programme Office of the Council of Europe. Despite early availability of the opinion and recommendations, the authorities of Moldova are still awaiting official opinion by the Venice Commission to proceed with further review and legislative process.

2.5.3 Operational cybercrime units in law enforcement authorities

The Centre for Combating Cybercrime at the National Inspectorate for Investigations of the General Inspectorate of Police of the Ministry of the Interior of Moldova is the primary unit for the investigation of cybercrime. The Centre currently employs 29 officers (7 criminal investigative officers and 22 investigative officers) tasked with preliminary investigative and operative-detective activities in terms of cybercrime offences. Similar to other jurisdictions, the Centre is active in providing assistance and guidance to local police units in cybercrime and electronic evidence matters.

The work of the Centre is supported by a cyber lab created within the Technical Criminalist Directorate of the Ministry of Internal Affairs, where technical specialists work on analyses, collection and processing of electronic evidence. The process of forensic examinations takes place in compliance with the provisions of the Criminal Code, Criminal Procedure Code, methodological materials and other applicable standards.

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 currently 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.

Both the Ministry of Interior and the General Prosecutor's Office can receive and process crime reports from individuals, legal entities and state authorities directly. Due to daily interaction between these institutions and supervision by specialized prosecutors of all relevant investigations, coordination is considered to be efficient.

2.5.4 Authorities for international police-to-police and judicial cooperation on cybercrime and e-evidence

2.5.4.1 24/7 points of contact and police cooperation

Moldova employs not one but two competent 24/7 points of contact for the purposes of the Budapest Convention, one at the General Police Inspectorate (Centre for Combating Cybercrime of National Inspectorate for Investigations) of the Ministry of the Interior and another at the Prosecutor General's Office (Information Technology and Cyber Crime Investigation Section).

The 24/7 point of contact at the General Police Inspectorate provides police-to-police cooperation under the Budapest Convention and the network of the G7, processing only operative and intelligence information (cannot be used as evidence in criminal proceedings). It does not receive and process mutual legal assistance requests, but can provide technical assistance and support/advice.

The procedure for data preservation starts with confirmation of receipt, followed by legal review as to national and international requirements. As a result of review, the request is either sent back for additional clarifications, proceeded with or refused. In case the request goes forward, it must be verified by the supervising prosecutor. Then the request is sent for execution to the provider/person in question.

In cases of terrorism or similar offences, urgent measures can be undertaken provided that the sanction of the court in Moldova verifying the request is received within 24 hours. The particular measures/steps will be decided on a case-by-case basis.

2.5.4.2 Mutual legal assistance authorities

The Department for International Legal Assistance of the Prosecutor General's Office of the Republic of Moldova is the designated central authority for the stage of pre-trial investigation. Requests at the stage of trial proceedings or sentence execution are dealt with by the Ministry of Justice, International Legal Cooperation Division. Interpol National Contact Point can receive but not implement the MLA request and has to send it to the competent authority for action.

Preliminary consultations can be provided, and email communications are preferred. No limitation is used as to the seriousness of offences in terms of cases that can benefit from preliminary consultations;. Following the receipt of the original request in non-electronic form, Moldovan competent authority will take the initiative in seeking clarifications where necessary.

For outgoing requests, the requesting authorities (prosecution offices or investigators) have to address all their communications to the central authority, which ensures further processing of requests with foreign competent authorities.

2.6 Ukraine

2.6.1 Action plans and strategic documents related to cybercrime

In terms of cybercrime, 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.

2.6.2 Procedural law for the purpose of domestic investigations, public-private cooperation and international cooperation

Ukraine signed the Budapest Convention on 23 November 2001 and ratified it on 10 March 2006 with entry into on 1 July 2006.

The Code of Criminal Procedure of Ukraine does not contain a definition of electronic evidence**.** According to Article 84(1) of the CPC, evidence is defined broadly, and covers any factual knowledge, obtained in accordance with the Code, by which presence or absence of facts and circumstances which are important for the criminal proceedings can be proved. Sources of such knowledge (evidence) can be testimonies, objects, documents and expert findings. According to Article 99(1) of the same Code, 'document' is "material object, which was created specifically for conservation of information, such object containing fixed by means of written signs, sound, image etc. the knowledge that can be used as evidence of the fact or circumstance which is established during criminal proceedings". It is further stipulated in paragraph 2 that documents might be "materials of photography, sound recording, video recording and other data media (including electronic)".

While several articles of the Code of Criminal Procedure of Ukraine refer to the collection of subscriber information and identification of the subscriber (Articles 162, 248, 263, 268), the notion of subscriber' information is not defined in the procedural legislation. The only definition related to this notion can be found in the Law on Telecommunications, where the term 'subscriber' is explained. However, this definition is not sufficient, due to the narrow scope of the Law (it applies only to telecommunication providers), and also because only the notion of 'subscriber', and not 'subscriber information', is elaborated.

A definition of traffic data is not found in the legislation of Ukraine, while content data is addressed in corresponding investigative power under the Criminal Procedure Code.

In terms of expedited preservation of stored computer data**,** Ukraine did not implement Article 16 Budapest Convention by introducing specific preservation order in its procedural legislation. Chapter 15 of the Criminal Procedure Code foresees some possibility of preserving computer data by using the concept of "provisional access to objects and documents". According to Article 159(1) of the Code of Criminal Procedure, purpose of 'provisional access to objects and documents' is for a party in proceedings to (1) get opportunity to examine objects and documents, (2) make copies thereof and, (3) seize them. However, as the access to data with the use of provisional access to objects and documents requires several steps with the full judicial hearing and authorisation, concerns related to expediency inherent to Article 16 Budapest Convention remain, especially as there are questions as to the applicability of the concept of the "document" to denote all instances of "stored computer data" as required by the Convention.

Similarly, the expedited preservation and partial disclosure of traffic data under Article 17 Budapest Convention is not implemented, as there are no specific provisions that define traffic data, authorize its expedient preservation and disclose the path of communications by the service providers, neither in the procedural nor in telecommunications legislation of Ukraine.

Ukraine did not implement Article 18 Budapest Convention by introducing specific production order provisions. Chapter 15 of the Code of Criminal Procedure, entitled "Provisional access to objects and documents", can be deemed as a relevant alternative. However, the options provided by the said Chapter of the CPC provide only very limited possibilities to order production of data. Firstly, the notion of 'information held by telecommunication operators on … subscribers' is not elaborated in the law, which is not acceptable from the point of certainty and foreseeability of law. Secondly, such information is deemed 'secrets protected by law' and subject to unnecessarily extensive conditions and safeguards. Last but not least, the provisional access to documents is meant to provide only temporary access to information, not fully reflecting the scope and purpose of Article 18 Budapest Convention that aims to produce and hand over evidence that can be used in criminal proceedings.

Search and seizure of stored computer data under Article 19 Budapest Convention can partially be achieved on the basis of Chapter 16 of the Code of Criminal Procedure ('provisional seizure of property'), Articles 234 – 236 of the CPC (search) and 167 ('provisional seizure of property'). However, there are several shortcomings if these provisions are to be applied to search and seizure of computer data. Firstly, these provisions were meant to be used with regard to tangible objects. This is visible firstly from the object of these actions, which is 'property' or 'possessions'. While this includes the notion of 'documents', it is necessary to once again point to the limited scope of that notion in terms of covering all instances of computer data.

Moreover, special provisions in the context of search and seizure provided by Article 19 (search of a connected system; making and retaining a copy of those computer data; maintaining the integrity of the relevant stored computer data; rendering inaccessible or removing those computer data in the accessed computer system) are not implemented. At the same time, provisions related to seizing or similarly securing computer data (p. 3(a)) and assistance of specialists in technical matters (p. 4) are covered by general regulations on seizure and involvement of specialists and experts in the criminal proceedings, although legislation still needs to be improved with regard to the copying of data to make this possibility clearer.

Ukraine implements Articles 20 and 21 Budapest Convention related to real-time collection of traffic data and interception of content data by similar set of provisions.

Article 40(4) of the Law on Telecommunications obliges telecommunication operators to, at their own expense, "install and ensure functioning of the technical means necessary for the

performance by search and investigation bodies and Ukrainian telecommunication networks security monitoring agencies, as well as to promote, within the scope of their competences, search and investigation activities, monitoring performance and prevention from the disclosure of the employed organizational and tactical techniques". It is also stipulated that operators must ensure protection of said technical means from unauthorized access.

In terms of procedural implementation, Articles 258 – 266 of the Code of Criminal Procedure provide legal basis for several covert investigative (detective) actions which interfere with the private communications of the individual. In the context of Articles 20 and 21 Budapest Convention, primarily relevant action is 'collecting information from transport telecommunication networks' (CPC Article 263).

At the same time, the lack of the key definition of traffic data in specialized or procedural legislation makes application of these combined powers less likely to achieve implementation of real-time collection of traffic data as required by Article 20 Budapest Convention.

It is to be noted that, according to Ukrainian Code of Criminal Procedure, these provisions also apply to interception of content data. According to Article 258(4) of the Code, "interference in private communication implies access to the contents of communication under conditions when participants to the communication can reasonably expect that their communication is private". Although the measures referred to above were intended to use for the interception of the telecommunications networks and for the phones and mobile phones, they are applicable also to the computer systems. These measures can only be applied to the investigations of serious criminal offences; other legal safeguards as to duration, purpose limitation and other are also foreseen, as Chapter 21 of the Code describes in detailed manner the grounds for measures, procedures of obtaining the order, the documentation and possibility to use information as evidence, thus putting these provisions in line with the Convention.

In terms of horizontally applicable conditions and safeguards (Article 15 Budapest Convention), although most 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 - such as existence of criminal investigation, judicial order, duration and other conditions – 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.

Since September 2016, the Cybercrime Programme Office of the Council of Europe provides extensive support to Ukraine in order to fully revise and amend the criminal procedure legislation and related legal acts, such as draft Law on Electronic Communications. Numerous drafts and parallel amendments have been analysed and commented on. On 17 May 2017, a team of Council of Europe experts has finalised a model package of amendments with commentaries and explanatory notes to resolve the issues of compliance of Ukraine with the Budapest Convention. With the package of draft amendments handed over to Ukrainian authorities, it is now up to the country to follow this initiative through by passing the relevant legislation.

2.6.3 Operational cybercrime units in law enforcement authorities

Following the reform implemented in 2015, there is now a Cyber Police Department of the National Police of Ukraine, as part of the Ministry of Internal Affairs of Ukraine. There are 25 law enforcement officers and 2 senior specialists in the within the Cyber Police Department of the

Ministry of Interior of Ukraine. In every region of Ukraine there are local cybercrime units; total number of staff being up to 100 members.
Staff of the Cybercrime Department of the Ministry of Interior are competent to detect and clear all crimes committed by means of information technologies and telecommunications, including computer-related fraud, crimes on the Internet, child abuse, and infringement of copyright. According to the regulations of the Ministry, the Department focuses on the following:

- Crimes against information security;
- Crimes in the areas of IT, telecom and copyright;
- Crimes in the areas of payment systems and commercial activities;
- Computer intelligence activities.

Investigators of the Cyber Police Department lead criminal proceedings on such cases.

In order to collect and analyze electronic evidence, the Cyber Police Department engages experts of the Forensic Science Centre of the Ministry of Interior. The experts take part in collecting, seizure, storage, analysis, examination and expert evaluation of digital evidence. Other agencies and units can invite experts of the Centre where it is necessary to collect and analyse digital evidence within investigative proceedings conducted by such other agencies / units.

The Department of counterintelligence protection of state's interests in sphere of information security of the State Security Service of Ukraine is another specialized law enforcement unit in Ukraine. The Department investigates crimes established by Article 359 of the Criminal Code of Ukraine (Illegal use of technical means for covert capture of information). Competencies of the Department also include investigation of crimes committed by means of computers and telecom channels established by articles 361, 361-1, 361-2, 362, 363, 363-1 of the Criminal Code of Ukraine (which correspond to offences under Articles 2-6 of the Budapest Convention).

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.

In practical terms, however, there is an overlap of functions and investigative competencies between the two agencies. Currently, it is not very clear how powers and competences have been divided. Additionally, in order to fight serious crime, including cybercrime, the State Security Service may also use means and measures which are not available for the police. Combining the protection of State security, counter-intelligence and other competences which are unique to security services, together with police powers within one government institution may provide for an effective use of resources; however, it may also pose risk to fundamental rights and freedoms. Therefore, having an authority with competence for both state security and criminal justice requires extra attention to conditions and safeguards.

The Cybercrime Programme Office of the Council of Europe, through its capacity building projects, currently provides support to Ukrainian authorities and the local Association of Internet Service providers in order to develop and conclude a Memorandum of Cooperation that would enhance public-private cooperation in view of more effective access to electronic evidence held by private sector entities.

2.6.4 Authorities for international police-to-police and judicial cooperation on cybercrime and e-evidence

2.6.4.1 24/7 points of contact and police cooperation

The Cyber-Police Department of the National Police of Ukraine, as part of the Ministry of Internal Affairs, performs the functions of the 24/7 point of contact. The 24/7 contact point is executing only police-to-police type of requests related to cybercrime and electronic evidence. It can provide assistance in the investigation of criminal offences connected with computer systems and exchange of operative information (that is not the evidence in criminal proceedings). The central authorities of Ukraine may take into consideration a request that came from the requesting party electronically, by facsimile or other means of communication.

Because of the absence of a mechanism for exchanging messages to/from international law-enforcement agencies between the National Police and Security Service of Ukraine, the possibility of establishing a second 24/7 contact point at the Security Service of Ukraine is being currently discussed. The agreement on creating a separate 24/7 point of contact point was recently (in 2017) reached between the Security Service of Ukraine and National Police of Ukraine; the division of tasks stems from the recent instruction of the usage of the 24/7 point of contact, developed by the National Police of Ukraine and currently under approval process at the Ministry of Justice of Ukraine. The additional 24/7 contact point would be based at the Department of Counterintelligence Protection of State's Interests in Sphere of Information Security, the unit of Security Service of Ukraine tasked with counteracting cyber threats and cyber terrorism.

The 24/7 National contact point according to the national legislation has no competence in executing mutual legal assistance requests. MLA requests can only be executed through the Prosecutor General's Office.

As to the execution of preservation requests, only regular procedures are used, as under Ukrainian legislation there is no separate provision for data preservation. Accordingly, no urgency procedures have been reported to exist.

2.6.4.2 Mutual legal assistance authorities

During the stage of pre-trial investigation, the Prosecutor General's Office (Department for International Legal Cooperation) is the central authority. According to the newly adopted legislation, the National Anticorruption Bureau of Ukraine is also a central authority in execution of the MLA requests at the stage of pre-trial investigation. At the trial stage, the Ministry of Justice (Division on Mutual Legal Assistance in Criminal Matters, International Legal Cooperation Department, Directorate for International Law) is handling MLA requests.

Requests may be sent to a foreign State or received from a foreign State, also through INTERPOL. The NCP INTERPOL cannot implement an MLA request but has to send it to the competent authority (Prosecutor General's Office or the Ministry of Justice of Ukraine) for action. Diplomatic channels are also used in case of absence of an international treaty.

In the absence of treaties and on the basis of reciprocity, Ministry of Foreign Affairs, Directorate General for Consular Service is the channel through which the request is forwarded and received. If received by the above, the request should be transferred to the central authority according to the stage of proceedings. The request has to include assurances of reciprocity. Only the official written request can be accepted by the Ministry of Foreign Affairs.

For outgoing requests, a court, prosecutor or investigator - in consultation with the prosecutor - can send requests for international legal assistance in criminal proceedings to competent central authorities. Central authorities ensure the transmission of requests to foreign counterparts and manage all communications in this respect.

3 Findings

3.1 Strategies and action plans

States of the Eastern Partnership region have been the target of serious cyberattacks and other security incidents in recent years. They thus recognise the growing challenges and threats in cyberspace and the need to respond, among other things, through the means of criminal justice.

At the same time, there is a lack of strategic approaches to countering cybercrime and making use of electronic evidence in criminal proceedings, as reflected in the absence of dedicated policy documents on cybercrime and electronic evidence as mainstream challenges of criminal justice systems. Even where cybercrime-related provisions are found in strategies or action plans, they are placed within an overall framework of organized crime strategies or cybersecurity documents. This hardly addresses the problem of cybercrime as a major criminal justice challenge.[4]

In consequence, criminal justice systems lack resources and capacities to prevent, investigate, prosecute and adjudicate not only cybercrime but the growing number of other offences involving electronic evidence.

Clearer policies, more specific plans and allocation of resources for the criminal justice response to cybercrime and electronic evidence are needed.

3.2 Procedural legislation

Criminal justice authorities need the powers to secure electronic evidence to investigate cybercrime and other offences entailing electronic evidence to bring offenders to justice and maintain the rule of law also in cyberspace. As such powers interfere with the rights of individuals, they need to be clearly defined by law. Articles 16 to 21 Budapest Convention provide an accepted international guideline.

Five Eastern Partnership countries are Parties to the Budapest Convention and Belarus has expressed its interest in this treaty.

And yet, albeit available to a certain degree, the procedural powers of the Budapest Convention remain to be fully implemented in most of these countries.

In order for procedural powers to apply, key definitions need to be addressed first. The overall concept of electronic evidence, even where not incorporated as a standalone type of evidence in criminal procedure, remains addressed in practice through other concepts, such as other materials, intangible objects, or documents. While there are concerns that some of the alternative definitions do not cover all instances of computer data (and thus, electronic evidence), in practice, such differences do not have any reported impact on the criminal investigations.

However, when it comes to another set of definitions related to computer data that can be used as evidence – namely, subscriber information, traffic data and content data – the impact on implementation is far greater. Availability of these concepts under the criminal procedure or related framework (e.g. electronic communications laws) varies greatly from one EAP state to another. The lack of these definitions in some jurisdictions is particularly concerning, as the

[4] Eastern Partnership countries are not unique in this respect. Few States have adopted dedicated cybercrime strategies.

application of some of the procedural powers under the Budapest Convention is directly linked to a specific category of computer data. But even where these definitions or their elements are found in national legal frameworks, implementation remains formal and not functional: no distinctions are drawn between these types of data in terms of applying different treatment, either in terms of procedural power used, level of intrusion into private life, or the level of judicial control.

In the logical hierarchy suggested by the Budapest Convention and related standards, access to subscriber information should attract least obstacles and controls in terms of safeguards and guarantees, which, in turn, guarantees necessary expediency; stricter conditions apply to access to and production of traffic data due to more serious privacy intrusion; while access to content data should be subject to strictest safeguards and controls corresponding to serious nature of privacy infringement.

Against this background, the procedural powers required by the Cybercrime Convention (Articles 16-21) are not fully implemented, with all required elements fully available under national law, in either of the States of the Eastern Partnership. While some of the States address more procedural powers in their national legal frameworks than the others, none follow the sequence of the progressive application of these powers as required by Convention – not necessarily in terms of chronology, but also in terms of gradually applicable safeguards and guarantees.

Preliminary measures under Articles 16 and 17 of the Cybercrime Convention, namely, expedited preservation of stored computer data and expedited preservation and partial disclosure of traffic data, being the powers most tailored to the environment of cybercrime/electronic evidence investigations where expediency of response is crucial, remain most challenging concepts for the Eastern Partnership countries to properly – i.e. directly – implement as standalone measures. Although some of the countries opted for direct implementation of these provisions, with a varying degree of coverage of all necessary elements, in the majority of EAP states the preference is still given to alternatives, such as production order or search and seizure.

This is particularly problematic as the implementation of Articles 16 and 17 has direct impact not only on national investigations and, beyond those, on cooperation with the private sector entities in terms of access to data; it is also crucial for international cooperation between cybercrime units and access to data from foreign/multinational service providers, as the proper implementation of these provisions into national law is a prerequisite for corresponding cross-border requests for preservation and disclosure.

Production orders under Article 18 Budapest Convention benefits from more consistent implementation, although still missing from most EAP jurisdictions as standalone measure for electronic evidence, while being mostly addressed through general obligation of cooperation with law enforcement or by alternative procedural powers. Most concerning, however, is the reliance of Eastern Partnership States, in part due to the legacy of their procedural system, on the search and seizure as a predominant procedural alternative to production orders. Similar to preservation and disclosure, production orders remain an equally important procedural power upon which mutual legal assistance in criminal cases concerning electronic evidence, as well as direct access to data offered by globally present multinational service providers, can be provided.

Taking into account the above, search and seizure of stored computer data remains most consistently implemented and available procedural power when it comes to the Eastern Partnership jurisdictions. Even where most of the implementing provisions do not focus specifically on electronic evidence but rather address search of computer data through traditional search/seizure provisions tailored to tangible objects, use of experts or specialized investigators during the search/seizure process ensures practical focus on electronic evidence – for example, through securing images or copes of data instead of removal of hardware or storage. Safeguards

and guarantees are present (bar one specific example) due to legal traditions and court practice of such measures. There is, however, a problem of over-reliance upon this particular procedural power for reasons of familiarity and comfort for investigation, at the expense of rarely used, less intrusive alternatives such as expedited preservation of data followed by production orders.

More problematic in terms of search and seizure as required by the Budapest Convention is implementation of specific procedural measures related to computer search, such as extension of search to connected computer systems (par. 2 of Article 19) or rendering data inaccessible (par. 3(d)). None of the Eastern Partnership States have implemented these possibilities in their national legislations.

Provisions that give effect to real-time collection of traffic data and interception of content are found in all Eastern Partnership legal frameworks, usually addressed in great detail as to the procedures, safeguards and technical details for such measures. Two major concerns apply to the implementation of these procedural measures. One is the lack of clarity as to the applicable legal regulation, some being addressed by proper criminal procedure legislation and others by the laws on operative-detective activities (which by themselves are far less transparent and subject to less safeguards and guarantees). The second problem is the lack of meaningful differences between these powers in terms of subject matter – namely, traffic data and content data – with more stringent conditions and safeguards applicable for access to content data as being the most protected under the right to privacy.

It is fair to note that, despite all of the concerns raised above in relation to legal frameworks for procedural powers, all five Eastern Partnership States that are Parties to the Budapest Convention are in the process of reforming their legislation or indicated the willingness to do so with the support of the capacity building activities of the Cybercrime Programme Office of the Council of Europe. This means that compliance with the procedural aspects of the Budapest Convention remains work in progress and should remain a priority in the Eastern Partnership.

3.3 Operational units

All Eastern Partnership countries have units specialized in the investigation of cybercrime, and some also have specialized prosecution units or specially assigned prosecutors for cybercrime matters.

However, a recurring problem for the Eastern Partnership remains the division of competences between various agencies competent to investigate cybercrime. Some EAP states have both security service and regular police/Ministry of the Interior units designated as investigative authorities for cybercrime, sometimes with competing and unclear divisions of powers or investigative jurisdiction. Beyond the reasons of efficiency and coordination, with cybercrime becoming an increasingly mainstream matter of criminal justice systems, security services do not have sufficient resources or even enough rationale to be dealing with day-to-day investigations of cybercrime offences – and, moreover, of traditional offences involving electronic evidence - that should be performed by regular investigative units of the police. Moreover, the concerns of safeguards and guarantees are also applicable in terms of procedural powers, as security services usually have a wider array of methods and powers beyond criminal procedure at their disposal, some of which may not be subject to the same or similar system of controls and conditions inherent in mainstream criminal investigations.

In some of EAP jurisdictions, the investigative powers are divided between the police units and special investigative agencies that operate beyond police/Ministry of the Interior structures. While this is primarily a regulatory and policy choice, lack of clarity remains as to the division of competencies between "preliminary" and "full" investigations performed by police forces and

investigative agencies respectively. At the same time, responsibilities for international police-to-police cooperation are retained at police units rather than fully-fledged investigators who should be more competent in terms of receiving and processing such requests and have a full suite of procedural powers available to them.

On the other hand, there is almost uniform understanding of the functions of cybercrime units as supporters of other investigative units/authorities when it comes to issues of electronic evidence. Such units would provide guidance, advise and even technical expertise in cases that require handling of electronic evidence; having, in some of the EAP countries, computer forensics services directly within the structure of the same government agency and readily available to provide expert support to units in question is certainly helpful in this regard.

Some of the investigative units report particularly low number of cybercrime investigations per year (in double or even single digits in some jurisdictions), in contrast to far greater number of cyber security incidents or overall assessment of the scope of the problem, especially when the number of criminal cases with electronic evidence elements is taken into account. This points at the need to focus on greater efficiency of reporting systems and processing of cases by investigative units.

3.4 International cooperation

In terms of police-to-police cooperation, 24/7 points of contact under Article 35 of the Budapest Convention have been set up in all of the States of the Eastern Partnership, including the one that is not a Party to the treaty. In line with accepted practice, these units are part of investigative units that deal with cybercrime and electronic evidence, and serve as international interface for requests to and from similar units of the 24/7 network or other channels for police-to-police cooperation.

Eastern Partnership countries are aware of the legal and practical importance of the preservation of data under the Budapest Convention on Cybercrime, that is, the possibility of "freezing" relevant data in order to allow time for obtaining a court order for the production or seizure of data. Against this understanding, there are obvious gaps in legal regulations as well as practice of preservation. Data preservation provisions of the Budapest Convention are not properly implemented in majority of the Eastern Partnership States, and general powers for production, search and seizure are used instead.

In some of the Eastern Partnership States, subscriber information is considered to be a part of traffic data and is treated as such, thus making it difficult to obtain it without a court order. In one of EAP jurisdictions where distinction was initially available, the legislation was amended due to privacy/data protection concerns, requiring a court order to receive subscriber information. The general understanding of the subscriber information is that the definition applies to both static and dynamic IP addresses.

Incoming or outgoing international preservation requests (Article 29 Budapest Convention) are often not followed by mutual legal assistance requests for the production of data; moreover, there are often no formal modalities for informing States requesting preservation of a necessity of mutual legal assistance request (in the best practice of the states implementing the Convention, such replies can be automated).

The need to accompany the expedited preservation of data (Articles 16 and 29 Budapest Convention) by the partial disclosure of a sufficient amount of traffic data to determine the path of a communication (Articles 17 and 30 Budapest Convention) appears to be problematic for Eastern Partnership countries due to insufficient legal regulations.

As a related concern with regard to production orders under Article 18 Budapest Convention, there is an interest among the states of the region to explore and put into effect the possibilities accorded by Article 18.1.b Budapest Convention, which allows domestic authorities to order the production of subscriber information from foreign/multinational service providers offering a service on the territory of the State in question.[5]

In terms of judicial cooperation, all of the Eastern Partnership States have designated authorities for mutual legal assistance. With one exception where the authority is the same for all stages of proceedings, the Office of the Prosecutor General is usually the central authority at the pre-trial stage of investigation, while the Ministry of Justice is the one for the trial stage. End-to-end procedures for the handling of incoming and outgoing mutual legal assistance requests are rather similar in Eastern Partnership countries. Differences may be due to adversarial, common law inspired criminal proceedings in some states of the region, as well as to provisional steps of compliance checking (e.g. technical pre-screening, applicability of urgency procedures) and additional management steps (e.g. processing of requests through local divisions of justice).

Time-frames for processing and execution of incoming mutual legal assistance requests are reported to be reasonable (ranging mostly from 2 to 6 months for non-expedited proceedings) and delays are experienced mostly due to large requests requiring translation and/or need to clarify ambiguities in cases of incomplete/low-quality requests. Translation of documents and related quality checks are considered particularly problematic among Eastern Partnership States.

Consideration of incoming mutual legal assistance as urgent or as priority, with one exception, is based upon informal criteria and is not uniform in application. Availability of formal and uniform criteria for assigning urgency to specific requests, as well as transparency in making these criteria known to international counterparts, may be considered as possible solution for handling large number of *de minimis* requests which put unnecessary pressure on already limited resources of international cooperation officers.

Direct contact with foreign or multinational service providers is an increasingly important option for all Eastern Partnership States, both for police cooperation units and mutual legal assistance authorities. Normally, there are no national regulations that expressly prohibit such practice and outgoing requests are usually sent to large multinational providers (primarily social networks and mail services) that would have set up specialized channels or departments for cooperation with law enforcement. Proper legal regulation is essential for this process, as foreign/multinational service providers do cooperate on a voluntary basis, where lack of clear and proper basis in national law could be one of the major reasons for declining cooperation.

[5] See Guidance Note on Production Orders adopted by the Cybercrime Convention Committee in February 2017.

3.5 Capacity building

Further support to capacity building in all of these areas will be required in the period 2018 to 2020 to sustain the processes of change initiated.

The Cybercrime@EAP joint projects of the Council of Europe and the European Union under the Partnership for Good Governance in 2018 will thus focus on:

- promoting strategic and multi-stakeholder approaches to cybercrime and electronic evidence and assessment of state of play against strategic priorities adopted in Kyiv in October 2014;
- completion of reforms of procedural law as basis for domestic investigations, public/private and international cooperation;
- related procedural regulations including division of competencies between authorities;
- capacities for mutual legal assistance, including Further development of online tools and resources with regard to EAP countries and use of cooperation templates for requests for data under Article 29/30 and Article 31 Budapest Convention;
- the effectiveness of 24/7 points of contact, including training and support to networking of 24/7 points of contact and additional regulations on the powers of 24/7 points of contact where necessary;
- cooperation agreements/arrangements between law enforcement and domestic providers as well as multinational service providers;
- follow up to recommendations of the T-CY Cloud Evidence Group in Eastern Partnership countries.

However, with substantive criminal law provisions in place, procedural law reforms in progress, and units for investigations and international cooperation on cybercrime and electronic evidence now in place, a major training effort would be required for law enforcement, prosecutors and judges in Eastern Partnership countries between 2018 and 2020 beyond the limited resources available under the current Cybercrime@EAP projects.

3.6 State of play: overview

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Cybercrime strategies and action plans	No	No	No	Yes – as part of cybersecurity and organized crime strategies and action plan	Draft as part of cybersecurity strategy and action plan	Yes - as part of cybersecurity strategy, with yearly action plans since 2016
Procedural law	- No definitions of categories of data - No implementation of Articles 16, 17 and 18 BCC (search and seizure used as alterative); - - Special powers for search and seizure (Art. 19 BCC) not implemented.	- No definitions of categories of data - No implementation of Art. 16 BCC (production order or search/seizure as alternative); - No implementation of Art. 17 BCC (general obligation of ISPs to cooperate); - Partial implementation of Art. 18 BCC (voluntary compliance); - Special powers for search and seizure (Art. 19 BCC) not implemented.	- No implementation of Art. 16 and 17 BCC (general data retention obligation used as alternative); - No implementation of Art. 18 BCC (general powers to receive documents); - Special powers for search and seizure (Art. 19 BCC) not implemented; - No judicial authorization for intrusive powers.	- No implementation of Art. 16 and 17 BCC (production orders used as alternative); - Special powers for search and seizure (Art. 19 BCC) not implemented.	- Partial implementation of Art. 16 BCC (applies only to ISPs); - Partial implementation of Art. 18 BCC (only provisions of Article 18.1.b); - Special powers for search and seizure (Art. 19 BCC) not implemented.	- No definitions of subscriber information and traffic data; - No implementation of Art. 16 BCC – production order or search/seizure as alternative; - No implementation of Art. 17 BCC; - No implementation of Art. 18 BCC – provisional access to objects and documents as alternative; - Special powers for search and seizure (Art. 19 BCC) not implemented; - Partial implementation of Art. 20 BCC – no definition of traffic data.

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Operational cybercrime units	- Division for Combating High-Tech Crime under the General Department on Combating Organized Crime at the Police - Investigative Committee	- Department of Combating Crimes in Communications and IT of the General Directorate of Combating Organised Transnational Crimes at the State Security Service; - Ministry of the Interior (unit being set up)	- High-Tech Crime Department of the Ministry of Interior (Department "K") - High-Tech Crime and Intellectual Property Department of the Investigative Committee	- Cybercrime Division of the Central Criminal Police Department at the Ministry of Internal Affairs - Ministry of State Security	- Centre for Combating Cybercrime at the National Inspectorate for Investigations of the General Inspectorate of Police of the Ministry of the Interior - Information Technology and Cyber Crime Investigation Section of the Prosecutor General's Office	- Cyber Police Department of the National Police under the Ministry of Interior - Department of counterintelligence protection of state's interests in sphere of information security of the State Security Service
Police-to-police cooperation units	- Division for Combating High-Tech Crime under the General Department on Combating Organized Crime at the Police	- Department of Combating Crimes in Communications and IT of the General Directorate of Combating Organised Transnational Crimes at the State Security Service	- High-Tech Crime Department of the Ministry of Interior (Department "K")	- Cybercrime Division of the Central Criminal Police Department at the Ministry of Internal Affairs	- Centre for Combating Cybercrime at the National Inspectorate for Investigations of the General Inspectorate of Police of the Ministry of the Interior - Information Technology and Cyber Crime Investigation Section of the Prosecutor General's Office	- Cyber Police Department of the National Police under the Ministry of Interior - The Department of counterintelligence protection of state's interests in sphere of information security of the Security Service of Ukraine

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Authorities for judicial cooperation	- Department for International Cooperation and Legal Support at the Prosecutor General's Office (pre-trial); - Ministry of Justice, Department for International Legal Assistance (trial stage).	- International Relations Department of the Prosecutor General's Office (pre-trial); - Ministry of Justice (trial stage).	- International Legal Department of the Office of the Prosecutor General; - Other authorities specified on treaty basis; - Supreme Court (limited competence).	- International Cooperation Unit of the Department of Legal Affairs of the Office of the Chief Prosecutor at the Ministry of Justice	- Department for International Legal Assistance and European Integration at the Prosecutor General's Office (pre-trial) - International Legal Cooperation Division of the Ministry of Justice (trial stage)	- Department for International Legal Cooperation of the Prosecutor General's Office (pre-trial) - Division on Mutual Legal Assistance in Criminal Matters, International Legal Cooperation Department, Directorate for International Law, Ministry of Justice (trial stage)