Action of the European Union and the Council of Europe on Cybercrime and Electronic Evidence

Approach and action in the Eastern Partnership region

10 YEARS EaP Eastern Partnership

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

Legislation:
Council of Europe approach to cybercrime and electronic evidence

Scope of the Budapest Convention

Criminalising conduct

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

Procedural tools

- Expedited preservation
- Search/seizure
- Production orders
- Monitoring/interception of computer data

+

International cooperation

- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- 24/7 points of contact

Harmonisation

Need to regulate: Substantive law & definitions

- Offences against and by means of computer systems and data
- Any other offences that may be “on the edge”: e.g. CSIRT taxonomies
- Content-related offences (e.g. CSAM, cyberviolence, etc.)
- Sufficiently dissuasive sanctions (Art. 13)
- Definitions :
  - Computer system;
  - Computer data/electronic evidence;
  - Service provider;
  - Subscriber information, traffic data, etc.

Need to regulate: Procedural powers

- Data preservation & expedited disclosure
- Production orders
- Search and seizure
- Real-time monitoring and interception
- Need to balance procedural powers with Article 15 guarantees
- Balance between operative/detective powers and criminal procedure
- Investigative competencies division

Need to regulate: International cooperation

- Enabling environment for mutual legal assistance for cases of cybercrime and electronic evidence
- Regulations to make all procedural powers work in international cooperation context
- Spontaneous information
- Transborder access to data
- Operation of the 24/7 points of contact network
- National regulations: efficiency, coordination, quality

Need to regulate: Less obvious considerations

- ISP liabilities and specifically data retention regulations
- Data protection oversight and efficiency
- Security and intelligence operations and limits
- Cyber security framework and critical infrastructure regulations
- Increased role of Computer Emergency Response Teams
- Financial intelligence and source of data for investigations
- Interagency cooperation and data exchange/reporting

International cooperation on cybercrime and electronic evidence in the context of the Eastern Partnership

International cooperation in the EaP: state of play

- An update of the initial report of Cybercrime@EAP II project, discussed at the Launching event of the Project (Bucharest, September 2015), through questionnaires sent in the end of 2017
- No significant changes in state of play (institutions and procedures)
- Some additional data and differences:
  - In terms of offences, additional focus on dissemination of malware and social engineering/identity theft;
  - Statistics: little variation in terms of received overall MLAs (fluctuations within 20%), but very significant increase year-on-year in sent MLAs (+255.5%), and even stronger increase of cybercrime-related MLAs (+579% for received and +959.5% for sent)
  - 24/7 request numbers: less data but still 22% to 76% increase in most EaP states, and in Azerbaijan went from 0 to 15/25 requests overall.
  - New standards have being developed and adopted meanwhile (e.g. Art. 18 Guidance Note, work on the II Additional Protocol)

Challenges

Powers to secure electronic evidence to investigate cybercrime and other offences entailing electronic evidence: all procedural powers of the Budapest Convention remain to be fully implemented in all of the countries of the Eastern Partnership.

Recurring problem is the **division of competences** between various agencies competent to investigate cybercrime.

Gaps in legal **regulations** and **practice**:

- subscriber information vs. traffic data;
- preservation requests not followed by mutual legal assistance requests for the production of data;
- no formal modalities for informing States requesting preservation of a necessity of mutual legal assistance request; etc.

Direct contact with **foreign** or **multinational service providers**: an increasingly important factor - cooperation on a voluntary basis, where lack of clear and proper basis in national law could be obstacles.

Recommendations

With regard to legal requirements:

- Legal review of regulations for 24/7 points of contact authority, functions and operations;

- Legislative review on specific provisions on obtaining subscriber information (as opposed to traffic data), including possibilities under Article 18.1.b of the Convention on Cybercrime;

- Comprehensive legal review of the both substantive and procedural law for introduction of uniform concepts and definitions (underlying offences, electronic evidence), full array of procedural powers under the Convention (especially preservation provisions and production orders), and removing obstacles to expedited processing of MLA requests (e.g. reduced requirements for originals of documents);

- Use of legal requirements and grounds for refusal to MLA requests can be at least partially remedied by public availability of best practice guides or handbooks on the subject.

Recommendations

With regard to communications:

- Facilitate use of standard [multi-language] templates and forms for 24/7 communications and mutual legal assistance, developed by the Cybercrime@EAP projects and adopted by the T-CY, which would assist in the timely processing of the assistance requests;

- Further support and expansion of dedicated online resource, maintained by the Council of Europe, for international cooperation in cybercrime cases/electronic evidence;

- Better coordination between 24/7 points of contact and competent authorities for mutual legal assistance by sharing information and ensuring follow-up of incoming/outgoing cases;

- Continued training of investigators, prosecutors, judicial personnel, international cooperation officers tasked and representatives of national points of contact on more advanced matters of international cooperation in cybercrime/electronic evidence cases.

Recommendations

In terms of management:

- Development and publication of guidelines on 24/7 points of contact based on best practices and experience;

- Encouraging formal cooperation between the law enforcement agencies and Internet service providers based on the Council of Europe Guidelines for cooperation between the law enforcement and Internet service providers on cybercrime;

- Efficient use of human resources and communications available for processing international cooperation, with focus on police-to-police communications that can produce admissible evidence and be utilized more efficiently, as well as agreed modalities for direct access to foreign service providers in communications and banking sector for available evidence;

- Formal urgency/priority processing for incoming mutual assistance requests based on formally agreed criteria and case-by-case examination or using advanced features of national legislation;

- Better integration of the core data on MLA requests into available criminal case management systems and more efficient follow-up and monitoring of requests that undergo execution by local criminal justice authorities.

Recommendations

In terms of quality of mutual legal assistance requests:

- Capacity building activities aimed at both criminal justice professionals and international cooperation officers at competent authorities, with focus on compact and informative writing skills;

- Use of standard templates and/or handbooks for reaching an acceptable standard for outgoing mutual legal assistance requests;

- In cases of direct judicial cooperation, centralized reporting, periodic follow-up and consultation from the central authorities should be sought, aiming to improve overall quality of requested and rendered legal assistance.

Conclusions for the EaP

Despite efforts by through capacity building projects:

- targeting legal framework,
- increasing skills and knowledge of cooperation officers,
- development and use of online tools and standard templates,
- ensuring access to development of standards and best practices,

cooperation on cybercrime and electronic evidence is still a **work in progress**

- Improvement of cooperation in criminal matters, including cybercrime and electronic evidence, is a long-term process: e. g. specific need for revising and reforming applicable legislation, but with ownership of states in question

- More streamlined and efficient mutual legal assistance process through revision of legal/regulatory framework and application of practical solutions and tools

- Stronger action of 24/7 points of contact through development of advanced skills, proper division of investigative competences and increased coordination with MLA authorities

- Eastern Partnership context: EU standards and solutions, cooperation with specialized institutions such as Eurojust and Europol.

Public/private cooperation on cybercrime and electronic evidence in the context of the Eastern Partnership

The context of public/private cooperation

- Need to respond to challenges of cyberspace in terms of criminal justice action, including protection of infrastructure;

- Electronic evidence is volatile and difficult to access and preserve and difficult to trace down to the source/offender;

- More often than not, data/evidence is held and processed by private sector entities in the form of **subscriber, traffic or content data**;

- Therefore, a central issue to the discussion of the public / private cooperation on cybercrime and electronic evidence is:

  ✓ **Access by the criminal justice officers to data held by private entities (e.g. Internet service providers)**

Four agreed elements of cooperation

- **Law**
  - Criminal law/procedure in place (definitions, powers, cooperation, related)
  - ISP liability regime present (mere conduit, etc.)
  - International standards: Budapest Convention and 2008 Guidelines

- **Stakeholder readiness/information exchange**
  - Defined and active communities (LEA, CSIRT, DPA, security, etc.)
  - Knowledge, expertise and specialization
  - Regular operational meetings

- **Compliance**
  - Issues of trust / general compliance / voluntary co-operation level
  - Cooperation agreements

- **Ability to cooperate beyond borders**
  - Level of co-operation with multinational companies

Thank you for your attention

1949.2019

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Giorgi Jokhadze
Project Manager
Cybercrime Programme Office
Council of Europe - Conseil de l'Europe
Bucharest, Romania
Giorgi.Jokhadze@coe.int