New Legal instruments for Cross-border Crime Investigation in EU

Prof.dr. Borka Jerman Blažič
Institut Jožef Stefan and University of Ljubljana
SLOVENIA
Internet Society Slovenia, chair
The new European approach

October is CyberSecMonth!

- **WEEK 1**: Cyber Security Training for Employees
- **WEEK 2**: Creating a Culture of Cyber Security at Work
- **WEEK 3**: Code Week for All
- **WEEK 4**: Understanding Cloud Solutions for All
- **WEEK 5**: Digital Single Market for All

Cyber Security is a Shared Responsibility

238 Activities across 32 Countries

Building together a Joint EU advocacy campaign on Cyber Security topics!
Outlines

CyberCrime globalisation

Main Challenges

Trace Communication Route and Obtain Related Data

Cross border evidences

Conclusion
What do we have today? Converged ICT Communication

- **Internet D**
- **Cross Border**
- **IT Network**
- **Telecom Network A**
- **Internet E**
- **Global Gateway**
- **Fixed Network B**
- **Mobile C**
- **Illegal Transfer**
**The crime is globalised**

Borderless Internet makes crime behavior fully globalized. Through the Internet and cloud computing, communication in swindler group can be enhanced and anonymous. Because of limitation of state authority and anonymity, it is really hard for state prosecutors and police to take investigation on the entire crime activities.
THE MAJOR PROBLEM IS? WHO IS THE „THIEF“?

A bad guy from China with an English name is attacking a French web shop selling Japanese products, their customers are paying to the Russian web based paying system, led by a Latvian manager with Swedish registration of his domain but registered by Brazilian register, with hosted Web page on some Thai server with a web pointer pointing to Iceland and using an Indonesian mail server for mailing.

Identified by EUROPOL HIGH TECH. CENTRE
With mobile, Internet, IP phone, mobile Internet access or other value-added telecom services, crime actors commit more crimes easily; However, by whatever advanced technology and tool they use, the nature of their crimes always stays all the same. Most of the data are in electronic form.
Challenges
Hard to Identify Criminal
● By new technologies (like IP phones), it is hard to intercept their calls with existing equipment.

Hard to get Cross-border data
● Looking for cross border cooperation or other related clues if no cooperation exist, no crime and crime actors are prosecuted

Proxise and other Anonymizing technics make the problem more difficult
● VPN, Foreign Proxy as Jump Board for criminals may be hidden behind deeper in Internet
The task is „Trace Communication Route and Obtain Related Data
for Cyber Crime Investigation
What are the elements for efficient crime investigation?

1) Law and regulations, understand what the target is and what the key evidence should be and how to get it and

2) Ensure cooperation with service providers and telecoms, as they are aware of information, data, ID and location of suspects.
ICT technology and crime investigation

Use advanced ICT technologies is evident, but **HUMAN is the key of every crime**

From viewpoint of investigation, horizontal coordination among all relevant entities is required.

From tactical viewpoint, international, cross-strait cooperation to combat cross-border global crime is obvious.
Why electronic evidences are important?

Effective and timely access to electronic evidence can save lives or prevent serious damage.

(For example, in terrorism cases with hostages or in ongoing child sexual abuse situations, the time that law enforcement requires to get to the victims can determine whether they survive or not).

After the crime has been committed: electronic evidence is volatile and can be transmitted, altered or deleted easily.

Public authorities therefore need effective and timely access to be able to prosecute criminals and prevent future crimes.

How to ensure this? What kind of legal instruments we have?
The only international document signed by 43 countries for mutual Cooperation in collecting e-evidence is the Budapest Convention On Cyber Crime and the later document known as Guidance Note published in 2017 with information what and how e-evidences can be collected in a cross-border.
The Council of Europe’s **Convention on Cybercrime Act** is known as **Budapest Convention – CCC**.

This document is a result of the efforts dedicated to solving the problem of cyber-based crime by the members of the Council of Europe (CoE), Interpol, Europol, the Organization for Economic Cooperation and Development, the G8 Group of States, Commonwealth and the United Nations (UN).

The document of the Council of Europe entered into force **in July 2004**. The document was ratified by 43 out of 47 Members (until August 2018) of the Council of Europe (San Marino, Ireland, Russia, and Sweden have not yet ratified it) and by Argentina, Australia, Cabo Verde, Canada, Chile, Costa Rica, the Dominican Republic, Israel, Japan, Mauritius, Morocco, Panama, Paraguay, the Philippines, Senegal, Sri Lanka, Tonga, and the United States of America.

The CCC is not limited to matters of cybercrime only as it embraces investigatory measures concerning **“the collection of evidence in electronic form”** for any **form of offence where such electronic evidence may be relevant**.
The problems with CCC and Guidance Note

Article 18 (1) of the CCC defines “production order” for collecting e-evidences as action of issuing production orders by law enforcement bodies to foreign established service providers or persons.

The mutual agreement (MLA) of the cooperating states does not allow the order to be classified as consent to the extraterritorial enforcement of domestic production orders for e-evidence collection.

Production order that addresses foreign-based service providers storing data on foreign territory is not considered to be an exercise of state power in the territory of another state and the answers depends on the service provider policy.
Production order for e-evidence in cross-border is still an issue!

The Guidance Note for CCC provide an extension of the scope of Article 18 of the CCC but it challenges the principle of territoriality and sovereignty of cooperating countries as well.

Exact information what is subscriber of information services is missing. This information is of tremendous importance to the evaluation of the impact regarding the production orders issued according to Article 18 (1) (b) CCC.

Another gap in the Guidance Note is the neglected clarification of a dynamic IP address (whether this data can be considered as subscriber information, or does it fall into the category of traffic data and is consequently outside the scope of Article 18 of the CCC).

This may lead to misunderstandings between the requesting authority and executing authority or the service provider addressed.
Other problems

There are no mandatory data retention rules for e-evidences in the US (where some of the most important service providers are based).

In EU Data Retention Directive was declared invalid by the European Court of Justice in 2014. At the same time, data the minimisation requirements force service providers to delete data more quickly.

This contributes to the volatility of e-evidence and reinforces public authorities' need for timely access in criminal investigations.
Some recent data (2018)

Requests for access to e-evidence within the EU are comparatively fulfilled more easily than with non-EU countries, regardless of the type of data, but the received answers are less than 50% in the last 5 years.

<table>
<thead>
<tr>
<th></th>
<th>Within the EU</th>
<th>With non-EU countries</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Judicial</td>
<td>Direct</td>
</tr>
<tr>
<td>Non-content data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subscriber data</td>
<td>75%</td>
<td>55%</td>
</tr>
<tr>
<td>Metadata</td>
<td>60%</td>
<td>45%</td>
</tr>
<tr>
<td>Content data</td>
<td>55%</td>
<td>N/A</td>
</tr>
</tbody>
</table>
The situation is improving, but very slowly

Requests answered in EU

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage</td>
<td>46%</td>
<td>45%</td>
<td>45%</td>
<td>44%</td>
<td>44%</td>
<td>48%</td>
<td>53%</td>
<td>58%</td>
</tr>
</tbody>
</table>

100%  | 50%  | 0%
Why data are not provided on time or not provided at all?

- Missing of data cause disappearance of other leads in the investigation

<table>
<thead>
<tr>
<th>Cause</th>
<th>Within the EU</th>
<th></th>
<th>With non-EU countries</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Judicial</td>
<td>Direct</td>
<td>Judicial</td>
<td>Direct</td>
</tr>
<tr>
<td>Lack of timely access</td>
<td>35%</td>
<td>25%</td>
<td>45%</td>
<td>15%</td>
</tr>
<tr>
<td>Lack of access (access denied)</td>
<td>25%</td>
<td>25%</td>
<td>25%</td>
<td>15%</td>
</tr>
<tr>
<td>Other</td>
<td>15%</td>
<td>5%</td>
<td>15%</td>
<td>10%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>75%</strong></td>
<td><strong>55%</strong></td>
<td><strong>85%</strong></td>
<td><strong>40%</strong></td>
</tr>
</tbody>
</table>
The new legal instruments proposed in EU – Preservation and Production order regulation to be adopted as EU Directive

*legislative measures for direct cooperation with service providers*

<table>
<thead>
<tr>
<th>Sub-option</th>
<th>Content</th>
<th>Non content</th>
</tr>
</thead>
<tbody>
<tr>
<td>European Production Order (EPO)</td>
<td>Order</td>
<td>Order</td>
</tr>
<tr>
<td>European Production Request (EPR)</td>
<td>Request</td>
<td>Request</td>
</tr>
<tr>
<td>European Production Request and Order (EPRO)</td>
<td>Request</td>
<td>Order</td>
</tr>
</tbody>
</table>
### The NEW REGULATION - main OBJECTIVES

<table>
<thead>
<tr>
<th>Problem drivers</th>
<th>Specific objectives</th>
<th>General objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. It takes <strong>too long</strong> to access e-evidence across borders under existing <strong>judicial cooperation</strong> procedures, rendering investigations and prosecutions less effective</td>
<td>1. <strong>Reduce delays</strong> in cross-border access to electronic evidence</td>
<td>Ensure effective investigation and prosecution of crimes in the EU by <strong>improving cross-border access to electronic evidence</strong> through <strong>enhanced judicial cooperation</strong> in criminal matters and an <strong>approximation</strong> of rules and procedures</td>
</tr>
<tr>
<td>2. Inefficiencies in <strong>public-private cooperation</strong> between service providers and public authorities hamper effective investigations and prosecutions</td>
<td>2. <strong>Ensure</strong> cross-border access to electronic evidence where it is currently missing</td>
<td></td>
</tr>
<tr>
<td>3. Shortcomings in defining <strong>jurisdiction</strong> can hinder effective cross-border investigation and prosecution</td>
<td>3. <strong>Improve legal certainty, protection of fundamental rights, transparency and accountability</strong></td>
<td></td>
</tr>
</tbody>
</table>
How it will work?

Serving a European Production Order

1. Designated legal representative
   - Validated order sent
   - Order forwarded to service provider

2. Corporate entity of same group

3. Other legal representative

Law enforcement

Service provider
The type of data that can be requested

- **Non-content data:**
  - **Subscriber data,** which allows the identification of a subscriber to a service. Examples: subscriber’s name, address, telephone number.
  - **Metadata,** which relates to the provision of services and includes “electronic communication metadata”. Examples: data relative to the connection, traffic or location of the communication.
  - **Access logs,** which record the time and date an individual has accessed a service, and the IP address from which the service was accessed;
  - **Transaction logs,** which identify products or services an individual has obtained from a provider or a third party (e.g. purchase of cloud storage space).
- **Content data.** Examples: text, voice, videos, images, and sound stored in in a digital format, other than subscriber or metadata
Stored vs intercept data:

- All the data in the previous slide refers to electronically stored **data that already exists**.
- Intercept data (i.e. data from real-time interception of telecommunications) is **out of the scope** of this initiative as there are specific and significantly different rules that determine access to that data.
- This initiative concerns cross-border access to e-evidence in the framework of criminal investigations or criminal proceedings for concrete criminal offences.

- Other situations not linked to a concrete investigation, such as intelligence or mass surveillance, are **out of scope**.

- The initiative is **not limited to serious crimes**, as the problem of cross-border access to e-evidence in criminal investigations is relevant for all crimes.
Providers of the following services (personal scope):
- electronic communications services as defined in the proposal for a Directive establishing the European Electronic Communications Code.

This are: traditional telecommunication services (example: voice telephony, SMS, internet access service) as well as new internet-based services enabling inter-personal communications such as voice over IP, instant messaging and web-based email services (Over-the-Top communications services, 'OTTs'). These OTTs are in general not subject to the current EU electronic communications framework (i.e.
- information society services that store data at the individual request of a recipient of a service; this includes a variety of known services providers such as social networks (e.g. Facebook and Twitter), cloud services (e.g. Microsoft, Dropbox or Amazon Web Services), online marketplaces (e.g. eBay or Amazon marketplace) or other hosting service providers (e.g. Bluehost).
- internet infrastructure services such as IP address providers and domain name registries and registrars and associated privacy and proxy services (e.g. GoDaddy).
Simplified procedure may apply

1. Draft order sent for validation
2. Validated where conditions are met
3. Validated order sent
4. Legal representative receives order
5. Order forwarded to service provider
6. Service provider executes order
7. Evidence (where available) transferred back via legal representative or directly

Judicial authority (including public prosecutor where applicable)

Law enforcement
Final message

It will apply to all EU MSs as a part of the legal, law enforcement systems, so faster and on time e-evidences are expected to be produced. Cooperation with USA and other countries is approached in the regulation and mechanisms suggested.