COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Cooperation against cybercrime in Ukraine

Workshop, Kyiv, Ukraine, 29 April 2009

Alexander Seger
Council of Europe,
Strasbourg, France
Tel +33-3-9021-4506
alexander.seger@coe.int

1

Session 1: Cooperation against cybercrime: what are the issues?

Session 4: Law enforcement – Internet service provider cooperation

Session 5: International cooperation and 24/7 contact points

2

2

1 Cooperation against cybercrime: what are the issue?

1.1 Current threats and challenges

1.2 The Convention on Cybercrime and Ukrainian legislation

1.3 Why law enforcement – internet service provider (ISP) cooperation is necessary

1.1 What is cybercrime?

What is cybercrime?

1. Offences against the confidentiality, integrity and availability of computer data and systems
2. Computer-related forgery and fraud
3. Content-related offences (child pornography, xenophobia, racism)
4. Offences related to intellectual property rights and similar rights

Cross-cutting issues and combination of offences

AND: evidence on a computer system

5

5

Investigating, prosecuting, adjudicating cybercrime: challenges

- Electronic evidence
- Volatile evidence
- Transnational crime scene
- Security and rights of users

6

6

Need:

- Criminalise conduct in a harmonised manner
- Procedural tools for law enforcement to preserve electronic evidence
- International cooperation (efficient urgent, preliminary measures + formal cooperation)
- Law enforcement – ISP cooperation
- Protect rights of users

7

7

1.2 The Convention on Cybercrime and Ukrainian legislation

The Budapest Convention on Cybercrime

- Opened for signature in Budapest in November 2001
- Elaborated by the Council of Europe with the participation of Canada, Japan, South Africa and the USA
- CCC common standard: used in 100+ countries world wide
- Ratified by Ukraine in 2006

Contents:

- Substantive criminal law: criminalising conduct (Articles 2 – 12)
- Procedural measures: expedited preservation, production order, search and seizure, interception of data (Articles 14 – 21)
- International cooperation (Articles 23 – 35)

8

8

The Convention on Cybercrime and Ukrainian legislation

Criminalising conduct (substantive law):

	Convention	Ukrainian legislation
Illegal access to a computer system	Art 2	?
Illegal interception	Art 3	362 (2) Criminal Code
Data interference	Art 4	362 (1) Criminal Code
System interference	Art 5	361 (1) Criminal Code 363-1 Criminal Code
Misuse of devices	Art 6	361-1 Criminal Code
Computer-related forgery and fraud	Art 7+8	190 Criminal Code?
Child pornography	Art 9	301 Criminal Code
Infringement of copyright and related rights	Art 10	176 Criminal Code and copyright law

9

9

The Convention on Cybercrime and Ukrainian legislation

Tools for investigation (procedural law):

	Convention	Ukrainian legislation
Expedited preservation of stored computer data	Art 16	? 66 CPC?
Expedited preservation and partial disclosure of traffic data	Art 17	? “
Production order	Art 18	? “
Search and seizure of stored computer data	Art 19	? “
Real-time collection of traffic data	Art 20	? “
Interception of content data	Art 21	? “
Procedural safeguards	Art 15	30+31 Constitution 14-1 CPC

Scope: Do provisions on evidence generally apply to electronic evidence?

10

10

1.3 Why law enforcement – ISP cooperation is necessary

- Information society dependend on ICT - vulnerable to cybercrime - Need to enhance security of ICT
- LEA and ISP play crucial role in a secure Internet
- LEA investigations often not possible without ISP cooperation
- Ensure efficient work of LEA
- Protect ability of ISP to provide services
- Ensure due process
- Protect rights of users
- How to enhance, how to structure cooperation?
- Guidelines for cooperation (Strasbourg, April 2008)

11

11

4 Law enforcement – service provider cooperation in the investigation of cybercrime

Why law enforcement authorities (LEA) / service provider (ISP) cooperation is necessary

- Information society dependent on ICT - vulnerable to cybercrime - Need to enhance security of ICT
- LEA and ISP play crucial role in a secure Internet
- LEA investigations often not possible without ISP cooperation
- Ensure efficient work of LEA
- Protect ability of ISP to provide services
- Ensure due process
- Protect rights of users
- How to enhance, how to structure cooperation?
- Guidelines

12

12

Law enforcement – service provider cooperation in the investigation of cybercrime

Developing guidelines under the Council of Europe Project on Cybercrime (October 2007 – April 2008)

Background study/good practices:

- Formal and informal relationships
- German E-Commerce Association/BKA agreement Nov 2007
- MoUs Microsoft – LEA in different countries
- eBay ELBA (electronic LE request processing system)
- AFA ISP-LEA training
- ECO SpotSpam
- Digital Phishnet
- French Signal Spam project
- MS CETS
- ISP training LEA

13

13

Law enforcement – service provider cooperation in the investigation of cybercrime

Background study/bad practices:

- One request for multiple accounts
- Requests without clear legal basis
- Law enforcement not respecting privacy regulations
- Multiple requests that are LEA fishing expeditions
- LEA request for content without appropriate legal procedure
- Unclear, unspecific requests
- Requests sent to wrong person or provider
- ISP refuse to provide information without clear reason
- LEA receive incomplete responses/information
- Preservation requests not followed by production orders

14

14

Law enforcement – service provider cooperation in the investigation of cybercrime

Guidelines for the cooperation between law enforcement and internet service providers against cybercrime

Adopted at the global Conference on Cooperation against Cybercrime (Council of Europe, Strasbourg, 1-2 April 2008):

- Common measures (including protection of rights and freedoms)
- Measures to be taken by law enforcement
- Measures to be taken by service providers

15

15

Law enforcement – service provider cooperation in the investigation of cybercrime

Common guidelines for LEA and ISP

- Develop a culture of cooperation
- Develop written procedures for cooperation with each other
- Cooperate for the protection of rights and freedoms of individuals
- Respect each others roles, rights and limitations
- Mindful of cost of cooperation
- Etc

16

16

Law enforcement – service provider cooperation in the investigation of cybercrime

Measures to be taken by law enforcement

- Broad and strategic cooperation with ISP
- Procedures for legally binding requests
- Designated and trained personnel for cooperation
- Verification of source of requests
- Standard request format
- Specificity and accuracy of requests
- Follow preservation orders with production/disclosure orders
- Criminal compliance programme
- International requests: 24/7 network and formal mutual legal assistance

17

17

Law enforcement – service provider cooperation in the investigation of cybercrime

Measures to be taken by service providers

- Report criminal incidents
- Assist LEA with training and other support
- Procedures for responding to requests
- Designated and trained personnel for cooperation
- Emergency assistance outside business hours
- Criminal compliance programme
- Verification of source of requests
- Standard response format
- Explanation if information not provided
- Coordination among ISP

18

18

Law enforcement – service provider cooperation in the investigation of cybercrime

Important:

- Guidelines, not binding
- Not substitute for procedural law and other formal regulations
- Based on good practices already available
- Help LEA and ISP in any country to structure their cooperation

19

19

Law enforcement – service provider cooperation in the investigation of cybercrime

Questions:

- What is the current state of law enforcement – ISP cooperation in Ukraine?
- Examples of good practice?
- What are the key problems?
- How can cooperation be improved, structured and organised?

20

20

5 International cooperation

Convention on Cybercrime
Chapter III - International cooperation

Legal and institutional basis for

- Expedited, urgent measures
- Legal cooperation in cybercrime matters

21

International cooperation

Chapter III - International cooperation

Section 1 – General principles

- Art 23 General principles on international cooperation
- Art 24 Principles related to extradition
- Art 25 Principles related to mutual legal assistance
- Art 26 Spontaneous information
- Art 27 MLA in the absence of applicable international instruments
- Art 28 Confidentiality and limitation on use

22

International cooperation

Chapter III - International cooperation...

Section 2 – Specific provisions

- Art 29 - Expedited preservation of stored computer data
- Art 30 - Expedited disclosure of preserved computer data
- Art 31 - Mutual assistance re accessing stored computer data
- Art 32 - Trans-border access to stored computer data
- Art 33 - Mutual assistance in real-time collection of traffic data
- Art 34 - Mutual assistance re interception of content data

- Art 35 - 24/7 network

23

23

International cooperation

Article 35 – 24/7 Network

Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;
b the preservation of data pursuant to Articles 29 and 30;
c the collection of evidence, the provision of legal information, and locating of suspects.

24

24

International cooperation

Article 35 cont'd

2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

25

25

International cooperation

Assessment of existing contact points:

Purpose of 24/7 network:

- Facilitate immediate measures (expedited preservation)
- Facilitate collection of evidence
- Coordinate with MLA authorities in an expedited manner (facilitate MLA)

Overall assessment against this purpose:

As a channel for expedited preservation (art 29 and 30) supplementing other channels of cooperation considered effective by countries with active contact points

26

26

International cooperation

Assessment: Set up, authority, procedures

Re institutional set up

- Different options possible as long as prosecutors or law enforcement CP
- Best option: CP = High-tech crime unit + specific individuals [+ MLA powers?]
- Problem: CP often unknown
- One option: National Interpol offices as CP with referral to high-tech crime units?

27

27

International cooperation

Assessment: Set up, authority, procedures

Re responsibility + authority

- Separate legal basis not necessarily required but: could "responsibilise" CP, make them accountable for results, make them known and facilitate cooperation with authorities at the national level, and give them powers for preservation and possibly MLA
- Problem: Many CP have no legal basis for expedited preservation and cannot effectively participate in the network
- Limited involvement of CP in MLA

28

28

International cooperation

Assessment: Types and number of requests

- Most requests are for expedited preservation (art 29 CCC)
- Countries may send and receive a large number of requests related to cybercrime through different channels. Only few of these appear to be considered particularly urgent, and for these the network of 24/7 CP may be used. Some countries use it more, others less and some CP have yet to sent or receive a request
- The majority of cases seem to be considered less urgent and for these other channels appear to be used

29

29

International cooperation

Ukraine is the only party to the Convention that has not yet established a 24/7 contact point:

- What options are available in Ukraine?
- What steps should be taken?

30

30

Thank you

Alexander.seger@coe.int

31