www.coe.int/cybercrime

Council of Europe / Project on Cybercrime

Discussion paper (draft)

The functioning of 24/7 points of contact for cybercrime

Alexander Seger – Council of Europe – Strasbourg, France – alexander.seger@coe.int

Background

- Convention on Cybercrime: Article 35 - 24/7 Network
- Cybercrime Convention Committee April 2008: Project on Cybercrime to prepare a report on functioning of 24/7 network + checklist for preservation requests for submission to T-CY meeting in March 2009
- Questionnaire to CP of countries that are parties to the CCC in Sep 2008
- Workshop in Ohrid (FYROM) in November 2008
- Discussion at G8 HTCSG meeting Rome (Feb 09)
- Discussion at PC-OC (Feb 09)
- Report to be discussed at T-CY meeting 12-13 March 2009

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.

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.

Draft report: Overall assessment

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

Draft report: 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
- Risk: Proliferation of contact points (G8, CoE, Interpol, SIRENE, EJN etc.)
- One option: National Interpol offices as CP with referral to high-tech crime units?

Draft report: 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

➢In a number of countries, formalised requests for preservation required (see check list)

Checklist - Request for expedited preservation

(to be attached to an email or fax as a "official" document with letter head)

1. Identification and contact information of the requesting 24/7 contact point:
- Name of requesting individual, of requesting contact point
- City and country, Telephone numbers, Fax number, E-mail address, Reference number of the sending contact point
- Date of request

2. Responsible prosecution or law enforcement authority (on behalf of which the request is sent)
- Name, contact details
- Case/file number

3. The offence and related facts
- Criminal offence and related criminal law provisions (including seriousness and penalty provided for by law)
- Summary description of the case (optionally also names of suspects, victim information, damage involved etc)
- Related investigations and preservation requests

4. Purpose of the request (action and evidence requested)
- Type of data required (subscriber information, traffic data, or content data)
- Date and time of the communication(s): provide both local time and Coordinated Universal Time/UTC
- IP address, subscriber and other specified data (eg physical address, type of service used, other email addresses used, mode of payment or similar)
- Account information (such as usernames, screen names, aliases, or other subscriber information related to different types of accounts, such as email, instant messenger or other types of accounts)
- Log files related to IP addresses or email or other types of accounts
- Duration for preservation required

5. Follow up
- Intention regarding mutual legal assistance request/letter rogatory
- Partial disclosure of traffic data
- Feedback on action taken and availability of data

Draft report: 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

Draft report: MLA

➢MLA not sufficiently efficient („Cloud computing")

➢If not CP, who is reponsible for expediting MLA under Article 31 (MLA regarding accessing of stored computer data)?

➢CP to take on powers for MLA?

➢CP to receive copies of MLA requests and facilitate their execution?

➢Exploit opportunities for direct contacts

➢Judges and prosecutors to be trained in international cooperation matters related to cybercrime

➢CP to ensure that preservation requests are followed by MLA requests

➢Separate directory of competent authorities for MLA

Draft report: Conclusions

For the network to become more effective:

➢Contact points need to become more pro-active and in particular make themselves known

➢Contact points need to take on more responsibility to facilitate MLA

➢National regulations to facilitate preservations measures need to be put in place

➢More countries to become party to the Convention on Cybercrime

Draft report: Conclusions

Issues to be addressed:

➢How to organise cooperation between Council of Europe and G8 HTCSG?

➢How to facilitate ownership of the network by non-G8 and non-CoE members?

Council of Europe workshops?
G8 HTCSG training conference?

Thank you

Alexander.seger@coe.int