COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Version 18 August 2009

International Co-operation under the Convention on Cybercrime[1]

Cybercrime has a strong transnational component.[2] Attacks launched by a person in one country or jurisdiction can affect persons in multiple other countries, and even an email communication sent to a person in the same country may generate electronic evidence elsewhere as data may be transmitted through servers in several countries.

At the same time electronic evidence is volatile. Thus urgent measures that are needed to preserve data at the national level are also necessary within the framework of international co-operation.

In short, what is required is international co-operation to the widest extent possible, including urgent measures to preserve data and efficient mutual legal assistance.

Chapter III of the Convention on Cybercrime provides a legal framework for international co-operation with general and specific measures. The following is an overview of some of the provisions of this chapter.

General principles for international co-operation

Article 23 establishes three principles for international co-operation as provided for in Chapter III of the Convention on Cybercrime:

- international co-operation is to be provided among Parties "to the widest extent possible." This principle requires Parties to provide extensive co-operation to each other, and to minimise impediments to the smooth and rapid flow of information and evidence internationally

- co-operation is to be extended to all criminal offences related to computer systems and data as well as to the collection of evidence in electronic form related to any criminal offence. This means that either where the crime is committed by use of a computer system, or where an ordinary crime not committed by use of a computer system (e.g., a murder) involves electronic evidence, the terms of Chapter III are applicable

[1] This document has been prepared under the Project on Cybercrime and is for information only.
[2] Regarding the transnational dimension of Cybercrime see: *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2, page 289 – available at: http://www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf.

Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension - in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 et. seqq. – available at: http://media.hoover.org/documents/0817999825_1.pdf;

- co-operation is to be carried out both "in accordance with the provisions of this Chapter" and "through application of relevant international agreements on international co-operation in criminal matters, arrangements agreed to on the basis of uniform or reciprocal legislation, and domestic laws." The latter clause establishes the general principle that the provisions of Chapter III do not supersede the provisions of international agreements on mutual legal assistance and extradition, reciprocal arrangements as between the parties thereto (described in greater detail in the discussion of Article 27 below), or relevant provisions of domestic law pertaining to international co-operation.

The third point also explains why many European but also other countries make use of the large range of available agreements related to criminal matters when co-operating with each other against cybercrime and not exclusively the Convention on Cybercrime.

> Article 23 – General principles relating to international co-operation
>
> The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes 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.

General principles related to extradition

Principles related to extradition are covered by Article 24 which contains a number of sub-provisions and which requires Parties to make the cybercrime offences of the Convention (articles 2-11) extraditable. At the same time it establishes thresholds so that not every offence is extraditable per se.

Article 24 also refers to other international or bilateral agreements on extradition and stipulates that in cases where an extradition is refused because of the nationality of the offender (many countries do not extradite their own nationals) the principle of "*aut dedere aut judicare*" (extradite or prosecute) applies.

> Article 24 – Extradition
>
> 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.
>
> b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.
>
> 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

General principles related to mutual legal assistance

Article 25 repeats some of the general principles of Article 23, namely that co-operation is to be provided for to the widest extent possible and that the obligation to co-operate not only refers to cybercrimes as such but also to traditional offences involving electronic evidence.

It states that applicable mutual legal assistance treaties, laws and arrangements shall be made use of.

Parties to the Convention furthermore need to establish a national legal basis to carry out the specific measures as foreseen in articles 29 to 35 of the Convention.

Paragraph 3 of this article is aimed at accelerating the process of obtaining a response to a mutual assistance request so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to. It:

- empowers the Parties to make urgent requests for co-operation through expedited means of communications, rather than through traditional, much slower transmission of written, sealed documents through diplomatic pouches or mail delivery systems

- requires the requested Party to use expedited means to respond to requests in such circumstances. Each Party is required to have the ability to apply this measure if its mutual assistance treaties, laws or arrangement do not yet provide so.

Paragraph 4 sets forth the principle that mutual assistance is subject to the terms of applicable mutual assistance treaties (MLATs) and domestic laws. These regimes provide safeguards for the rights of persons located in the requested Party that may become the subject of a request for mutual assistance. For example, an intrusive measure, such as search and seizure, is not executed on behalf of a requesting Party, unless the requested Party's fundamental requirements for such measure applicable in a domestic case have been satisfied. Parties also

may ensure protection of rights of persons in relation to the items seized and provided through mutual legal assistance.

Paragraph 5 is essentially a definition of dual criminality for purposes of mutual assistance under this Chapter. Where the requested Party is permitted to require dual criminality as a condition to the providing of assistance dual criminality shall be deemed present if the conduct underlying the offence for which assistance is sought is also a criminal offence under the requested Party's laws, even if its laws place the offence within a different category of offence or use different terminology in denominating the offence.

Countries that are Parties to the Convention are required to have criminalised the conduct defined in Articles 2 to 11 (illegal access, data interference, child pornography etc.) and thus the condition of dual criminality can therefore be considered as having been met.[3]

Article 25 – General principles relating to mutual assistance

1 The Parties shall afford one another mutual assistance to the widest extent possible 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.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

[3] Of course, some Parties may have made reservations or declarations for some of these articles reservations.

Mutual legal assistance in the absence of applicable international agreements

The previous provisions of the Convention on international co-operation made extensive reference to the use of existing agreements. In fact, European countries dispose of a large number of such treaties as well as bilateral agreements.

However, increasingly non-European countries will become Parties to the Convention on Cybercrime and these are not necessarily acceding to other treaties on co-operation in criminal matters.

In such situations Article 27 provides the basics for mutual legal assistance between countries that have no other legal agreement.

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b The central authorities shall communicate directly with each other;

c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Specific provision: expedited preservation of stored computer data

The expedited preservation of stored computer data is not only necessary at the national (article 16) but also at the international level. This is provided for in Article 29 of the Convention.

A Party receiving a request is obliged to act very quickly in order to have data preserved. The condition of dual criminality only applies in exceptional circumstances. It is important to underline that this is a provisional measure through which data is preserved mostly at the level of the Internet service provider. The actual disclosure of information is a subsequent step that may require a mutual legal assistance request.

Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a the authority seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying the custodian of the stored computer data or the location of the computer system;

e the necessity of the preservation; and

f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Specific provision: expedited disclosure of preserved traffic data

As data often transit several countries, it is not sufficient to order the preservation of traffic data in one country but in all countries or on all servers involved in the chain. Therefore, a service provider must disclose sufficient data so that the path through which a communication was transmitted can be identified and the preservation of further data be ordered. This is provided for in Article 30 of the Convention (which is the equivalent to the partial disclosure provision under Article 17 at the national level).

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

Specific provision: mutual assistance regarding accessing of stored computer data

Article 31 allows a Party to request another Party to access, seize and disclose data stored on a computer system on its territory. This article also provides for expedited responses to requests.

Article 31 – Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Specific provisions: mutual assistance for the interception of data

Two provisions relate to the interception of data, namely, Article 33 which covers the real-time collection of traffic data, and Article 34 which is about the interception of content data. Of course, as the interception of content data represents a high level of intrusion, mutual assistance in this respect is restricted and subject to safeguards, other applicable treaties and domestic law.

> Article 33 – Mutual assistance in the real-time collection of traffic data
>
> 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.
>
> 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.
>
> Article 34 – Mutual assistance regarding the interception of content data
>
> The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Specific provision: the network of 24/7 points of contact

In order to facilitate urgent action, in particular the expedited preservation of data in another country, a network of 24/7 points of contact has been established under Article 35 of the Convention.[4] Each Party is required to establish a point of contact for co-operation in urgent cases. This point of contact supplements and does not replace other existing channels of co-operation.

> Article 35 – 24/7 Network
>
> 1 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.
>
> 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.

[4] This provision is based on the experience of the G8 High-tech Crime Subgroup which established such a network already in 1997.

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.