**Session 1.3**

**International Cooperation in a**

**Global Economy**

***Introduction to exercise case study and group work***

**Procedural tools**

**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.

**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:

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

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

**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.

**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.

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.