

## **Prevention measures and international cooperation to combat Cybercrime:**

**By: Cristina Schulman**

- Role of public and private-sector cooperation in addressing cybercrime
- Importance of international cooperation in the exchange of police information and judicial cooperation
- Importance of establishing an international network of contact points
- Enhancing channels of communication between countries through identifying a focal point in each country

### **1. INTRODUCTION**

One of the most serious challenges in fighting against cybercrime is the international dimension. Computer systems may be accessed in one country, computer data manipulated in another and the consequences felt in a third country. Moreover, the evidence of the cybercrime may be stored on a computer in a different country from where the criminal executed the act. A cybercriminal can hide his identity and route materials over networks in different countries from different continents before reaching the intended recipients.

The ability to move electronically from one network to another and access database on different continents have the result that different sovereignties, jurisdictions, laws and rules are involved, challenging the existing rules of international crime law and making an investigation very difficult.

Cybercrime is a transnational crime and effective fight against this phenomenon requires increased, rapid and well-function international cooperation in criminal matters. Because the international cooperation depends on countries legal systems, lack of

legislation, for example, not clearly defining computer offences in national law or not creating the mechanisms for investigating computer crimes, inapplicability of seizure powers to intangibles, insufficient provisions regarding extradition and mutual legal assistance will prevent that country to adequately respond to an international cooperation request.

These are arguments for the necessity to have a common understanding of which conducts in relation to computer systems and networks should be criminalized and which procedural law provisions should be adopted by countries. Based on such provisions it can be established at international level an efficient framework for cooperation against cybercrime.

## **2. THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME (ETS 185)<sup>1</sup>**

The Convention on Cybercrime of Council of Europe (ETS 185) provides such an instrument. It has been developed by the Council of Europe in cooperation with Canada, Japan, South Africa and the United States of America and it was opened for signature in Budapest in 23.11.2001 and entered into force on 1.07.2004.

One of the aims of the Convention on cybercrime is to set up a fast and effective regime of international co-operation. Therefore the Convention contains provisions that are meant to establish such a framework for a rapid and reliable international cooperation and require parties to provide each other with various forms of assistance

Chapter III of the Convention contains the provisions regarding traditional and computer crime-related mutual assistance and also extradition rules. It has been considered two situations: where between parties there is not other legal basis (treaty, reciprocal legislation, etc.) and Convention applies and where such a basis exists in which case the existing arrangements also apply to assistance under this Convention.

---

<sup>1</sup> Comments and explanations provided in accordance with the text of the Explanatory Report

## 2.1. Section 1 – General principles

According to the general principles relating to international cooperation and extradition set out in Section 1 of Chapter III, Parties should provide extensive cooperation to each other and eliminate the obstacles for a rapid flow of information and evidence.

Co-operation will cover all criminal offences related to computer systems and data as well as the collection of evidence in electronic form of a criminal offence, which means that either where the crime is committed by use of a computer system, or an ordinary crime, which was not committed by use of a computer system but involves electronic evidence, the terms of Chapter III are applicable.

Co-operation will be provided in accordance with the provisions of the Chapter III and applying the relevant international agreements on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws.

Article 24 provides the obligation for extradition between Parties for criminal offenses establish under Articles 2 -11 of the 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 if there is not another arrangement agreed on the basis of uniform reciprocal legislation or an extradition treaty in force.

The offences provided by the Convention are to be deemed extraditable in any extradition treaty between or among Parties and they will be included in future treaties.

Under this article a Party that requires an extradition treaty with the requesting Party may use the Convention itself as a basis for surrendering the person requested.

It is also provided the principle "*aut dedere aut judicare*" (extradite or prosecute).

According to Article 25 of the Convention - General principles relating to mutual assistance – co-operation will be provided "to the widest extent possible." Thus mutual

assistance is in principle to be extensive, and impediments strictly limited. Parties can make urgent requests for co-operation through expedited means of communications, rather than through traditional, much slower transmission of written, sealed documents through diplomatic channels or mail delivery systems and the requested Party has the obligation to use same expedited means to respond.

Article 26 – spontaneous information – provides the possibility for a Party, which possesses valuable information to assist another Party in a criminal investigation or proceeding, and which the Party conducting the investigation or proceeding is not aware that exists to forward that information. In such cases, no request for mutual assistance will be forthcoming.

Under Article 27 - Procedures pertaining to mutual assistance requests in the absence of applicable international agreements - Parties are obliged to apply certain mutual assistance procedures and conditions where there is no mutual assistance treaty or arrangement.

The Article reinforces the general principle that mutual assistance should be carried out through application of relevant treaties and similar arrangements for mutual assistance.

Convention establishes a separate general regime of mutual assistance that would be applied in lieu of other applicable instruments and arrangements, agreeing instead that it would be more practical to rely on existing MLAT regimes and avoiding confusion that may result from the establishment of competing regimes.

It is provided a number of rules for mutual assistance in the absence of an MLAT or arrangement on the basis of uniform or reciprocal legislation, including designating central authorities, imposing of conditions, grounds for and procedures in cases of postponement or refusal, confidentiality of requests, and direct communications.

Assistance may be refused on the grounds provided for in Article 25, paragraph 4.

Under Article 27 the requested Party can postpone a request, rather than refuse, assistance where immediate action on the request would be prejudicial to investigations or

proceedings in the requested Party or instead of refuse or postpone a request to provide assistance subject to conditions.

Central authorities designated shall communicate directly with one another. However, in case of urgency, requests for mutual legal assistance may be sent directly by judges and prosecutors of the requesting Party to the judges and prosecutors of the requested Party. The judge or prosecutor following this procedure must also address a copy of the request made to his own central authority with a view to its transmission to the central authority of the requested Party.

Article 28 - Confidentiality and limitation on use - enable the requested Party to ensure that its use is limited to the scope for which assistance is granted, or to ensure that it is not disseminated beyond law enforcement officials of the requesting Party.

## **2.2. Section 2 – Specific provisions**

Section 2 of Chapter III provides specific measures for taking effective and concerted international action in cases involving computer-related offences and evidence in electronic form, including provisions, which are meant to facilitate the investigation of computer crimes with the help of new forms of mutual assistance.

Article 29 - Expedited preservation of stored computer data - provides for a mechanism at the international level equivalent to that provided in Article 16 at the domestic level. A Party may request for the expeditious preservation of data stored in the territory of the requested Party by means of a computer system, in order that the data not be altered, removed or deleted during the period of time required to execute a request for mutual assistance to obtain the data.

The situations when the requested Party may refuse a request for preservation are limited and each Party has to ensure that data preserved will be held for at least 60 days.

If the requested Party realizes that the custodian of the data is likely to take action that will threaten the confidentiality or prejudice the requesting Party's investigation, it must notified promptly the requesting Party.

This procedure has the advantage of being both rapid and protective of the privacy of the person whom the data concerns.

Article 30 - Expedited disclosure of preserved traffic data. At the request of a Party in which a crime was committed, a requested Party will preserve traffic data regarding a transmission that has traveled through its computers, in order to trace the transmission to its source and identify the perpetrator of the crime, or locate critical evidence.

It was considered that the requested Party may discover that the traffic data found in its territory reveals that the transmission had been routed from a service provider in a third State, or from a provider in the requesting State itself. In such cases, the requested Party must expeditiously provide to the requesting Party a sufficient amount of the traffic data to enable identification of the service provider in the other State.

The requested Party may only refuse to disclose the traffic data, for the same reasons as a request for preservation of stored computer data.

According to Article 31 – Mutual assistance regarding accessing of stored computer data - each Party must have the ability, for the benefit of another Party, to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within its territory.

Such a request must be responded to on an expedited basis where:

(1) there are grounds to believe that relevant data is particularly vulnerable to loss or modification, or

(2) otherwise where such treaties, arrangements or laws so provide.

Article 32 - Transborder access to stored computer data with consent or where publicly available - provides two situations when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance:

- where the data being accessed is publicly available,
- where the Party has accessed or received data located outside of its territory through a computer system in its territory, and it has obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data to the Party through that system.

#### Mutual assistance regarding the real-time collection of traffic data (Article 33)

In many cases, investigators cannot ensure that they are able to trace a communication to its source by following the trail through records of prior transmissions, as key traffic data may have been automatically deleted by a service provider in the chain of transmission before it could be preserved.

It is therefore critical for investigators in each Party to have the ability to obtain traffic data in real time regarding communications passing through a computer system in other Parties.

Under Article 33 each Party is under the obligation to collect traffic data in real time for another Party and such co-operation will be provided according to applicable treaties, arrangements and laws.

Because real time collection of traffic data is at times the only way of identifying the perpetrator of a crime, and because of the lesser intrusiveness of the measure, Parties are encourage to permit as broad assistance as possible, i.e., even in the absence of dual criminality.

#### Mutual assistance regarding the interception of content data (Article 34)

Considering the high degree of intrusiveness of interception, the obligation to provide mutual assistance for interception of content data is restricted. The assistance will be provided to the extent permitted by the Parties' applicable treaties and laws.

As the provision of co-operation for interception of content is an emerging area of mutual assistance practice, it was decided to defer to existing mutual assistance regimes and domestic laws regarding the scope and limitation on the obligation to assist.

Under Article 35 of the Convention each Party has the obligation to designate a point of contact available 24 hours per day, 7 days per week in order to ensure immediate assistance in investigations and proceedings within the scope of Chapter III of the Convention.

It is very important that principles and obligations established by the Chapter III of the Convention, which enable the competent authorities to respond rapid and effectively to mutual assistance requests, to be implemented.

### **3. INTERNATIONAL COOPERATION PROVISIONS UNDER CONVENTION ON CYBERCRIME AND THEIR IMPLEMENTATION IN ROMANIA**

Romania signed the Convention on Cybercrime on 23.11.2001 and ratified the Convention on 12 May 2004 (Law 64/2004).

In order to harmonize the national legislation with the provisions of the Convention it was adopted Title III of the Law 161/2003, which regulates the prevention and combating of cybercrime, by specific measures to prevent, discover and sanction the offences committed through computer systems ensuring adequate protection of human rights and liberties<sup>2</sup>.

Chapter V of the Romanian Law on cybercrime deals with International Cooperation in Articles 60 – 66.

It is also applicable, Law no. 302/2004, which is an extensive law on international judicial co-operation in criminal matters.

---

<sup>2</sup> Title III containing the relevant provisions for preventing, discovering and sanctioning the offences committed through the computer systems are incorporated in the Law 161/2003 on certain measures to ensure transparency in the exercise of public dignity, public office and in the business environment, to prevent and sanction corruption (published in the Official Gazette no 279 from 21 April 2003)

### **Article 23 of the Convention – General principles relating to international co-operation**

Regarding general principles, under articles 60- 61 of the Law on cybercrime, the Romanian competent authorities cooperate directly, under the conditions of the law and by observing the obligations resulting from the international legal instruments of which Romania is party, with the institutions with similar attributions in other states, as well as with the international organisations specialised in the area.

On the territory of Romania common investigations can be performed on the basis of bilateral or multilateral agreements concluded with the competent authorities.

### **Article 24 of the Convention – Extradition**

According to Article 60 of Romania Law no 161/2003, the competent authorities cooperate directly with the institutions with similar attributions in other states, as well as with the international organisations specialised and the cooperation can have as scope among others extradition matters.

Law No. 302/2004 on international judicial co-operation in criminal matters regulates cooperation procedures including on extradition and surrender based on European Arrest Warrant and also covers the provision of the Convention.

### **Article 26 of the Convention – Spontaneous information**

Article 66 provides that the competent Romanian authorities can send, ex-officio, to the competent foreign authorities the information and data necessary for the competent foreign authorities to discover the offences committed by means of a computer system or to solve the cases regarding these crimes.

A similar provision is also provided in Article 166 of the Law no 302/2004 on international judicial co-operation in criminal matters.

### **Article 28 – Confidentiality and limitation on use**

According to Article 12 of Law on international judicial co-operation in criminal matters Romania is obliged to make sure, to the extent possible, upon request from the Requesting State, of the confidentiality of requests sent to it and of any documents attached to such requests.

In the event that it would be impossible to ensure confidentiality, Romania shall notify the foreign State, which shall decide.

### **Article 29 – Expedited preservation of stored computer data**

According to Article 63 of the Romanian Law within the international cooperation, the competent foreign authorities can require from the Service for combating cybercrime the expeditious preservation of the computer data or traffic data existing in a computer system on the territory of Romania.

If, in executing the request for the expeditious preservation a service provider in another state is found to be in possession of the data regarding the traffic data, Cyber-Crime Fighting Service will immediately inform the requesting foreign authority about this, communicating also all the necessary information for the identification of the that service provider.

**Article 32 – Trans-border access to stored computer data** - was transposed in Article 65 of the Romanian Law.

### **Article 35 – 24/7 Network**

The provisions of Article 62 establish the Service for combating cybercrime within the Prosecutor's Office of the High Court of Cassation and Justice.

Currently, the Service for combating cybercrime is operating within the Directorate for Investigating of Organized Crime and Terrorism Offences.

The competences of the Service for combating cybercrime meet the requirements set out in the Convention on Cybercrime on international cooperation being also the contact point available 24/7.

#### **4. Prevention measures**

Some prevention measures have been taken in Romania in order to fight against cybercrime, such as:

- increased public awareness and education about the danger of the computer crimes;
- hotlines allowing citizens who discover online illegal activities to report the conduct to relevant authorities (in Romania: [www.efrauda.ro](http://www.efrauda.ro));
- cooperation between all institutions (at national and international level) and law enforcement agencies in fighting against cybercrime;
- encourage the private sector (including Internet Service Providers) and civil society (including teachers, non-governmental organizations, the media) to report any information they might obtain concerning cybercrime to the appropriate law enforcement or social service authority;
- Internet service providers can also contribute by facilitating the referral of relevant information to law enforcement authorities;
- training for criminal justice professionals (law enforcement, prosecutors and the judges) is a necessary as a part of a comprehensive program designed to fight these crimes. The National Institute of Magistracy from Romania or other programs have provided special training for judges, prosecutors and police officers but still more should be done in this area.

Council of Europe has provided great support including training for judges, prosecutors and police officers in many countries including in Romania.

## **5. CONCLUSIONS**

The effective fight against cybercrime requires increased, rapid and well-function international cooperation in criminal matters.

It is necessary that each country to provide domestic legislation that criminalizes illegal use of computer systems.

The domestic efforts must be complemented by a new level of international cooperation since global networks facilitate the commission of transborder offenses.

Effective combating of crimes committed by means of a computer system and effective collection of evidence in electronic form require a very rapid response.

Therefore countries are encouraged to make a better use of the Council of Europe Convention on Cybercrime including the international co-operation provisions.