Project on Cybercrime
www.coe.int/cybercrime

Economic Crime Division
Directorate General of
Human Rights and Legal Affairs
Strasbourg, France

Version 12 March 2008

Discussion paper (draft)

The effectiveness of international co-operation against cybercrime: examples of good practice

prepared by
Pedro Verdelho, Portugal

This report has been prepared within the framework of the Project on Cybercrime of the Council of Europe.

Contact

For further information please contact:

Economic Crime Division
Directorate General of Human Rights and Legal Affairs
Council of Europe
Strasbourg, France

Tel: +33-3-9021-4506
Fax: +33-3-9021-5650
Email: alexander.seger@coe.int

Contents

1 Introduction 4
1.1 Background – general remarks 4
1.2 A case study 5

2 Implementation of international co-operation tools against cybercrime 7
2.1 Council of Europe Convention on Cybercrime 7
2.1.1 The Convention on Cybercrime 7
2.1.2 1959 European Convention on Mutual Assistance in Criminal Matters 7
2.1.3 Schengen and Mutual Legal Assistance 8
2.1.4 Countries which ratified the Convention on Cybercrime 8
2.1.5 Countries which have signed but not ratified the Convention 10
2.1.6 Other countries 11
2.1.7 General overview 11
2.2 24/7 Contact Points (G8/CoE) 12
2.2.1 The genesis of the network 12
2.2.2 The network 13
2.2.3 The G8 network and the Council of Europe network 14
2.2.4 European Union initiatives 14
2.2.5 General overview 15
2.3 Interpol, Europol and Eurojust 19
2.3.1 Interpol 19
2.3.2 Europol 19

3 Country studies of good practices 20
3.1 France, Romania and Estonia: general background 20
3.2 Legal basis for international co-operation in the three countries 21
3.2.1 France 21
3.2.2 Romania 22
3.2.3 Estonia 23
3.3 Application of specific provisions in the three countries 24
3.3.1 Jurisdiction (Article 22) 24
3.3.2 Extradition (Article 24) 25
3.3.3 MLA principles and procedures (Articles 25, 26, 27, 28) 26
3.3.4 Expedited preservation and disclosure (Articles 29 and 30) 29
3.3.5 Trans-border access (Article 32) 31
3.3.6 Mutual assistance regarding accessing stored computer data (Article 31), the real-time collection of traffic data (Article 33) and the interception of content data (Article 34) 32
3.3.7 24/7 Contact Points (Article 35) 33
3.4 Beyond the Convention: other tools for international co-operation in the three countries 35
3.4.1 Police co-operation 35
3.4.2 Other channels and international co-operation instruments 36

4 Conclusions 37

1 Introduction

1.1 Background – general remarks

> "There is a revolution going on in criminal activity. The revolution lies in the ways that networked computers permit crimes to be committed remotely. A criminal no longer needs to be at the actual scene of the crime to prey on his victim".
> Michael A. Sussmann[1]

> "Cybercrime is international crime which implies the need for efficient and immediate international co-operation to preserve volatile evidence across borders."
> *June 2007 Octopus Conference Interface Summary*[2]

It is obvious nowadays that cybercrime is a phenomenon with a global dimension, typically with multiple territorial connections. The perpetrator is based in a certain country's jurisdiction, but his or her actions can reach computers and victims in many other countries. This is a characteristic common also to other modern forms of criminality, but concerning cybercrime, it is inherent to its nature. Due to the expansion of communication networks, particularly the Internet, it is impossible for any country in the world to act alone against this crime problem. As use of the Internet increases, it gives more possibilities to criminals, and more criminals have new opportunities to commit crimes remotely.

Modern societies depend on information technologies. More than 200 different countries or territorial jurisdictions are currently connected to the Internet. The only adequate approach to address the borderless nature of global networks is a common approach, where domestic efforts are complemented by specific forms and channels of international co-operation that can face the issue of crime being facilitated globally, with potential consequences in any part of the world.

While cybercrime is the most transnational of all crimes (evidence for which may disappear if not preserved within minutes), law enforcement must respect borders.

They must follow proper legal channels to request assistance in criminal investigations; they face perpetrators in this field over whom they do not have specific power or jurisdiction; sometimes they live in a very distant country with a different language and culture; probably this country has a very different legal tradition and criminal law framework. Because of the nature of the communications networks, it is likely that more than one country will often be able to assert jurisdiction over a criminal offence. The first barrier to law enforcement may be the language. The perpetrator probably will focus his or her activity in countries with different languages. This can be problematic if there is a need for speed in exchanging information or in gathering data or evidence.

In such a context, international co-operation between law enforcement agencies – within police or between prosecution services - is crucial to achieve results in criminal investigations.

International organisations are dealing with this question. The United Nations General Assembly adopted resolutions on *Combating the Criminal Misuse of Information Technologies* (Resolutions 55/63 and 56/121) which underline the need to ensure that each Member State adapts its law and practise to eliminate "safe heavens". On the other hand, United Nations'

[1] 'The Critical Challenges from International High-Tech and Computer Related Crime at the Millennium', *Duke Journal of Comparative & International Law*, Vol 9:451.
[2] www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_technical_co-operation/cyber/567%20IF%202007-d-sumconclusions1g%20Provisional.pdf

resolutions refer to the need to exchange information between States and to have co-operation and co-ordination among all the States related to some concrete criminal investigation on an international case of criminal misuse of information technologies.

The Organisation for Economic Co-operation and Development (OECD) had a different approach, with the same intent. Since 1983, the OECD studied the existing need for national cybercrime laws and made recommendations, so that on an international level the same facts could be qualified within similar criminal frameworks.

The approach of the Group of Eight, the G8, goes some steps further. As it will be said below, the G8 created a Contact Points Network that has become a reference in the international co-operation scenario. Essentially, it is a directory of names that can be reached and facilitate immediate action where needed.

The European Union also adopted legal instruments referring to cybercrime and international co-operation in this field, as it will be described below.

Finally, the Organization for Security and Co-operation in Europe (OSCE) recommended, by its Decision No. 7/06, that participating States consider becoming a party to the Convention on Cybercrime. This decision also encouraged participating States to join the G8 24/7 Computer Crime Network and to nominate an appropriate contact point for the purpose of streamlining international law enforcement co-operation on combating the criminal misuse of cyberspace and in criminal cases that involve electronic evidence.

The scope of this study is to help countries to make better use of the international co-operation provisions of the Council of Europe Convention on Cybercrime, including Article 35 on 24/7 points of contact. It will describe the new possibilities for international co-operation and its environment. Concrete case studies will be discussed regarding the application of the general principles of the Convention into domestic laws with a view to determining good practices. These are Estonia, France and Romania.

1.2 A case study

The following is not a typical "cybercrime case". Nevertheless, in the concrete case some international co-operation tools on cybercrime matters were used so that it could come to an end. It is described here as an introduction to the main subject of this study.

In the beginning of 2005, a Norwegian citizen (let's call him A.T.) attacked a bank in Oslo. He intended to steal money and he did so effectively. During his action, a police officer was killed. A.T. ran away and could not be found in Norway. Some days later, police found and searched his home and computer and discovered that A.T. was the owner of an email account from a provider in the United Kingdom. International co-operation was required from British authorities which asked the provider to put this email account under surveillance. One day, A.T. used his email account to send an email message. In the United Kingdom, police asked the ISP information about the IP address where the communication came from and it was found that it came from Spain.

British and Spanish authorities installed an alert system whose objective was to know, each time that A.T. used his email account, where he was. Thus, each time A.T. used his account, British police obtained the IP address of the computer in the origin of the communication and provided it immediately to Spanish police. Then, Spanish police asked the Spanish ISPs about the owner or user of the IP address. All the connexions were made from cybercafés in Madrid. Even proceeding to that area very quickly, during a long period of time it was not possible to arrive at those places before A.T. was gone.

Later, A.T. began to use his email account from a cybercafé in Malaga. This is a smaller town than Madrid and there it was possible to put all the cybercafés from a certain area permanently under physical surveillance. After some days of surveillance, British police announced that A.T. was online, using his email account, and provided the IP address. Very rapidly, the Spanish ISP informed Spanish police from the concrete location of the cybercafé, what allowed the officers in the street to identify and arrest A.T. in place.

A.T. was extradited to Norway and prosecuted[3].

[3] The details about this concrete case were provided by Mr. Juan Salom, from *Grupo de Delitos Telematicos* of the Spanish *Guardia Civil*.

2 Implementation of international co-operation tools against cybercrime

Previous Council of Europe reports state that

> "Difficulties have been encountered in the co-operation between Member States of the Council of Europe and non Member States. For example, classical MLA-procedures for the transfer of the requested material in general take a relatively long term which may jeopardize the investigation and prosecution of the crime involved. In addition, it was brought forward that it may be difficult to determine the physical location of a computer server, which prevents law enforcement to request for mutual assistance".

As a first approach, there is a general impression that a considerable number of international instruments exist nowadays concerning the fight against criminality over the information networks. Beginning with the Council of Europe Convention on Cybercrime, the United Nations Convention on the Rights of Children is still in force and, on a regional level, some European Union directives and framework decisions. In spite of the fact that all those instruments are in place, it seems that they are still not adequately implemented and international co-operation is not benefiting from them. Without proper implementation, it will be difficult to improve international co-operation.

On the other hand, there is also a general impression that there is a great need to increase awareness of existing instruments for international co-operation, so that they can be used properly by national authorities.

2.1 Council of Europe Convention on Cybercrime

2.1.1 The Convention on Cybercrime

The Convention on Cybercrime from Council of Europe (ETS 185) was opened for signature on 21 November 2001. At the time of writing, 43 States have signed the Convention. Four of those 43 States (Canada, Japan, South Africa and the United States) are not members of the Council of Europe. 22 of these Sates had ratified it (the United States were the only one of them outside Europe).

So, most of the 47 Council of Europe Members have already signed the Convention. A number of them have ratified it. All the European Union Member States have signed the Convention, but only 12 of them (Bulgaria, Cyprus, Denmark, Estonia, Finland, France, Hungary, Latvia, Lithuania, the Netherlands, Romania and Slovenia) have ratified it.

Nevertheless, the Convention on Cybercrime does not seek to be the only binding international instrument on international co-operation. It is assumed by the Convention, in Article 23, that the Convention itself will be applicable in the framework of other existing relevant instruments on international co-operation in criminal matters. Consequently, Article 27 describes the general principles that should be observed in the absence of applicable international conventions or treaties.

2.1.2 1959 European Convention on Mutual Assistance in Criminal Matters

The background to the Convention on Cybercrime is the European Convention on Mutual Assistance in Criminal Matters of the Council of Europe from 1959. All the Council of Europe members (with the exception of San Marino) ratified this Convention. It means that, for the time being, from all the Parties of the Convention on Cybercrime, the only non-member Party of the 1959 Convention is the United States.

This single fact attests the added value of the Convention on Cybercrime: it creates, for the first time, a common legal framework for international police and judicial co-operation between most European States and the United States. This is a particularly important aspect because Article 14 says on No. 2 that the procedures on international co-operation of the Convention shall apply, in addition to the criminal offences established in accordance with Articles 2 through 11 of the Convention, as well as to other criminal offences committed by means of a computer system and to the collection of evidence in electronic form of any other criminal offence.

On the other hand, it must be underlined that the rules introduced by the articles of the Convention create new co-operation tools and channels between the Parties that were not allowed by any previous instrument.

2.1.3 Schengen and Mutual Legal Assistance

A large number of countries which have ratified the Convention are also party to the European Union Mutual Legal Agreement of 2000 (MLA). All the European Union Member States are a party of this international agreement since December 2007.

The 2000 MLA provides a large number of international co-operation tools, mainly the possibility of direct contacts between judicial authorities from each party. According to this possibility, each judge or prosecutor can make a request directly to another judge or prosecutor from any 2000 MLA State.

2.1.4 Countries which ratified the Convention on Cybercrime

Albania and Croatia ratified the Convention during 2002. Estonia and Hungary ratified it in 2003. Lithuania, Romania, Slovenia and "the former Yugoslav Republic of Macedonia" ratified it in 2004. Bulgaria, Cyprus and Denmark ratified the Convention in 2005. Armenia, Bosnia and Herzegovina, France, Netherlands, Norway, Ukraine and the United States of America ratified it in 2006. Finally, Finland, Iceland and Latvia ratified the Convention in 2007.

Nonetheless, Albania did not adopt any internal law concerning international co-operation, according to the Convention. The only legal framework available relates to extradition in a general approach. For the 24/7 contact point within the Convention framework, Albania designated the Police of the State under the Ministry of Interior.

Armenia which ratified the Convention in 2006 has still to adopt any domestic law on international co-operation in matters of cybercrime. Armenia has not yet joined any contact point network and has not even indicated who will be the 24/7 contact point within the Convention framework.

Bosnia and Herzegovina which also ratified the Convention, has not yet designated the national contact point for the purposes of Article 35 of the Convention. However, in a *note verbale* from its Permanent Representation in Strasbourg, it declared that it will deposit the declaration by which the competent authorities for the purposes of the Convention will be designated as soon as possible.

Bulgaria has internal rules referring to international co-operation on the Penal Procedure Code and on the Law on Extradition and European Arrest Warrant. In certain cases, the Convention is directly applicable, according to Bulgarian Constitution. In implementation of Article 35 of the Convention, a 24/7 contact point was established and empowered with all relevant competences in conformity with the provisions of the Convention. The Article 35 contact point is the National Service for Combating Organized Crime under, the Ministry of Interior.

Croatia adopted the provisions of the Convention within its domestic legal system by the Law concerning International Legal and Criminal Matters. The Economic Crime and Corruption Department of the General Police Directorate serves as the 24/7 contact point, as described in Article 35 of the Convention. Croatia also joined the G8 network.

Cyprus introduced some provisions on cybercrime into its national law, mainly on substantive criminal law, jurisdiction and extradition. The International Legal Co-operation Unit of the Ministry of Justice and Public Order is the designated 24/7 contact point.

Denmark designated, as a contact point for the purposes of Article 35 of the Convention, the Danish National Police, Police Department. Pursuant to Article 38 of the Convention, Denmark declared also that the Convention will not apply to the Faeroe Islands and Greenland.

Estonia also designated a contact point within the framework of the Convention, in the Central Criminal Police. All the provisions of the Convention were adopted in internal Estonian law, namely within the Penal Code and Penal Procedure Code.

Finland designated, pursuant to Article 35 of the Convention, as its contact point, the National Bureau of Investigation, Criminal Intelligence Division/Communications Centre.

France foresees in its law the provisions on international co-operation of the Convention, mainly in the *Code de Procédure Pénale*. In addition, as required by Article 35 of the Convention, it designated, the *Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication* as its 24/7 contact point. It must be noted that France made a reservation according to Article 22 of the Convention, concerning jurisdiction. In fact, France reserves itself the right not to establish jurisdiction when the offence is committed outside the territorial jurisdiction of any State. Moreover, France declared that whenever the offence is punishable under criminal law where it has been committed, proceedings shall be instituted only upon request from the public prosecutor and must be preceded by a complaint from the victim or by an official complaint from the authorities of the State where the act was committed.

Hungary adopted a law respecting International Co-operation with Criminal Authorities in Criminal Matters (Law No. 54/2002) in 2002. A law concerning Co-operation with European Union Member States in Criminal Matters (Law 130/2003) was adopted in 2003. These two legal instruments transpose the provisions on international co-operation of the Convention on Cybercrime to the Hungarian legal system. Hungary designated the Hungarian National Police International Implementing Co-operation Centre as the 24/7 contact point.

Iceland designated its contact point, in accordance with Article 35 of the Convention, as the National Commissioner of the Icelandic Police (*Ríkislögreglustjórinn*).

Latvia designated as the point of contact, within the framework of the Convention, the International Co-operation Department of Central Criminal Police Department of State Police.

In Lithuania, according to the national legal system, the Convention integrates itself into the domestic Law. It has not adopted any specific regulation to comply with the provisions of the Convention, but some articles of the Criminal Code and of the Code of Criminal Procedure are applicable. In addition, Lithuania designated as its contact point, for the purpose of Article 35 of the Convention, the Police Department under the Ministry of the Interior.

"The former Yugoslav Republic of Macedonia" ratified the Convention. However, it has not adopted any specific legislation concerning international co-operation on cybercrime matters. In some cases, general rules of the Macedonian Criminal Code are applicable. "The former Yugoslav Republic of Macedonia" designed as the 24/7 contact point, in the context of Article

35 of the Convention, a Deputy Public Prosecutor, from the Department for Fight Against Crime and Corruption, in the Office of Public Prosecutor.

The Netherlands declared that, in accordance with Article 35 of the Convention, the point of contact is the National Office of the Public Prosecution Service (*Landlijk Parket van het Openbaar Ministerie*). The Netherlands also declared that, in accordance with Article 38 of the Convention, it accepts the Convention for the Kingdom, in Europe.

Norway provided a direct contact to the parties of the Convention, suitable for the purposes of Article 35 of the Convention, available 24 hours a day, seven days a week, in the High Tech Crime Division of the National Criminal Investigation Service (*KRIPOS*).

Romania mainly transposed the provisions of the Convention into Law No. 161/2003 specifically related to cybercrime issues. Law No. 302/2004 provides the general legal framework for international judicial co-operation on criminal matters implementing the relevant instruments on MLA and extradition of the Council of Europe and European Union. This law does not contain specific provisions on cybercrime although the general provisions on extradition and MLA are applicable. Besides, Romania designated a contact point, in accordance with Article 35 of the Convention (in case, the Service for Combating Cybercrime within the Directorate for the Investigation of Organized Crime and Terrorism).

Slovenia designated the Ministry of the Interior, Criminal Investigation Police Directorate, International Police Co-operation Section as point of contact, in accordance to Article 35 of the Convention, available on 24 hours, seven days a week basis.

Ukraine ratified the Convention but, by the time of writing, had still not joined any contact point network and had not even indicated who will be the 24/7 contact point within the Convention framework.

The United States of America ratified the Convention during 2006 and pursuant to Article 35 of the Convention, designated as point of contact the Computer Crime and Intellectual Property Section of the United States Department of Justice, Criminal Division.

2.1.5 Countries which have signed but not ratified the Convention

Besides the above mentioned countries which have already ratified, some others signed the Convention on 23 November 2001: Austria, Belgium, Germany, Greece, Italy, Moldova, Poland, Portugal, Spain, Sweden, Switzerland, United Kingdom, Canada, Japan and South Africa. Ireland and Malta signed in 2002 and Luxembourg signed the Convention in 2003. The Czech Republic, Slovakia, Serbia and Montenegro (nowadays the two independent countries of Montenegro and Serbia) signed in 2005. None of these countries had ratified the Convention by the time of writing.

Austria has not ratified the Convention but has already established a 24/7 contact point which belongs to the Federal Ministry of the Interior (Federal Office of Criminal Investigation, Department for Computer and Cybercrime). This contact point is reachable on a permanent basis, twenty four hours a day, seven days a week. In addition, Austria has already adopted provisions on international co-operation in its internal law: in the Austrian Penal Code, in the Extradition and Mutual Legal Assistance Act and in the Austrian Code of Criminal Procedure. It must be underlined that according to Austrian law, the Convention will be directly applicable upon its ratification by Austria.

Moldova has not ratified the Convention, nor has it transposed the provisions on co-operation into its domestic laws. National law only includes general principles relating to mutual assistance and provisions on extradition.

Serbia has in its domestic legislation some provisions on international co-operation (mainly in the Criminal Procedure Code). However, it has not adopted any specific law according to the Convention on Cybercrime. Serbia has not yet designated the 24/7 contact point.

Slovakia adopted rules on international co-operation in the Code of Criminal Procedure Act (Act No. 301/2005). There are no specific articles on cybercrime co-operation and a 24/7 contact point does not exist yet.

The Czech Republic already has some provisions on substantive law and on procedural law in its legal framework, referring to the provisions of the Convention. With regard to international co-operation on cybercrime matters, there are not yet any specific provisions in the domestic law. There is also no 24/7 contact point.

Germany signed the Convention but has not yet ratified it. Nevertheless, most of the provisions from the Convention are already covered by German internal law. With respect to international co-operation rules, they are covered by the Act on International Legal Assistance in Criminal Matters (*Gesetz über die internationale Rechtshilfe in Strafsachen, IRG*) and by the German Code of Criminal Procedure (*Strafprozessordnung, StPO*). With regard to the 24/7 contact point, Germany is already part of the G8 network and is also listed in the Interpol contact points.

Portugal signed the Convention, but has not yet ratified it. Furthermore, the country did not introduce the international co-operation provisions from the Convention into its internal law. Portugal has not joined any contact point network, except Interpol.

2.1.6 Other countries

Other non-Member States of the Council of Europe also showed their intention to sign and ratify the Convention on Cybercrime. Some of them joined the G8 contact point network and some others follow the meetings of the Cybercrime Convention Committee (TC-Y) of the Council of Europe. Their legal profiles are available on the Council of Europe Cybercrime webpage.

In Argentina there is a general law related to international co-operation and procedures and there are several bilateral agreements with other countries, but none of them specifically on cybercrime. Argentina is not yet a G8 contact point network member.

Brazil has not adopted any legislative measure concerning international co-operation on cybercrime matters. However, some of the provisions of the Code of Penal Procedure are applicable. Brazil is listed in the G8 network.

The Dominican Republic is also listed in the G8 network. At the domestic level, a law adopted during 2007 (53/07) implemented some of the provisions of the Convention but none of them regarding international co-operation.

Mexico does not yet have any specific regulation regarding international co-operation on cybercrime. However, Mexico is listed in the G8 contact point's network.

Morocco is also listed in the G8 network. Nevertheless, it has not adopted any specific legislation regarding international co-operation on cybercrime matters.

2.1.7 General overview

From the declarations contained in the instruments of ratification deposited by the Parties of the Convention, it can be concluded that most of the contact points are police contact points. Only four countries ("the former Yugoslav Republic of Macedonia", Romania, the Netherlands

and the United States of America) designed Prosecution Services as contact points. This practical question must be analysed from the perspective of each country's internal law and on the specific procedural competence to preserve data and other procedural urgent measures.

In addition, three states (Armenia, Bosnia and Herzegovina and Ukraine) from the 21 countries which have already ratified the Convention have not yet designated a 24/7 contact point, according to Article 35 of the Convention.

It is relevant to consider that only two Parties of the Convention made declarations upon Article 38 (Territorial application). As said before, Denmark declared that the Convention will not apply to the Faeroe Islands and Greenland. The Netherlands declared that, in accordance with Article 38 of the Convention, it accepts the Convention for the Kingdom, in Europe.

In terms of jurisdiction, two Parties made reservations. France made a reservation concerning jurisdiction. As it was described above, France reserves the right not to establish jurisdiction when the offence is committed outside the territorial jurisdiction of any State. In addition, France declared that whenever the offence is punishable under criminal law where it has been committed, proceedings shall be instituted only upon request from the public prosecutor and must be preceded by a complaint from the victim or by an official complaint from the authorities of the State where the act was committed.

The United States of America also made a reservation regarding jurisdiction: it reserves the right not to provide for plenary jurisdiction on offences which are committed outside the United States territory by its citizens, or on-board ships flying its flag or aircrafts registered under its law.

2.2 24/7 Contact Points (G8/CoE)

2.2.1 The genesis of the network

The existing 24/7 contact points network idea, in the context of Article 35 from the Cybercrime Convention, was born from the "G8 High-Tech Crime Subgroup".

The G8 (Group of Eight) is an informal group of the world's major industrial nations, including Canada, France, Germany, Italy, Japan, Russia, the United Kingdom and the United States of America. The G8 address a wide range of international economic, political and security issues, mainly within its heads of state annual meetings. During 1995, a group of experts was organised to look for better ways to fight transnational crime. Inside this group, the G8's Subgroup on High-Tech Crime was created in 1996. This working group made some proposals to G8 Ministers of Justice.

During the G8 meeting of Ministers of Justice and Home Affairs, on 9 and 10 November 1997, general principles to combat high-tech crimes were established and an action plan was defined. This was the first time that a group of representatives of several countries in the world agreed upon principles and rules that could be used to fight cybercrime.

Amongst the principles, it was defined that there must be no safe havens for those who abuse information technologies and that it was important that investigation and prosecution of international high-tech crimes were coordinated among all concerned States, regardless of where harm had occurred. This declaration would make it necessary to establish a mutual legal assistance system that could ensure the timely gathering and exchange of evidence in such cases and also a transborder electronic access by law enforcement to publicly available information. This means that if an investigation needs open source information there is no requirement of authorisation from the State where the data resides. So, the most important guideline from this position was the need to improve measures to facilitate mutual legal

assistance among the members of the G8. The action plan supporting the principles pointed, as the final goal of such a plan, to ensure that criminals would not receive a safe place to perpetrate their offences anywhere in the world.

Thus, the action plan included, among other aspects, the need to develop protocols for international co-operation, both on a procedural and operational level. Next, the principles concerning national points of contact of a wide network of points of contact, for the purpose of combating high-tech crime, were defined.

In the action plan the G8 welcomed countries from outside the G8 to join the network. Since the beginning, it was expected that this network could expand to other countries, building a global network, which could be of a great advantage: in concrete and real investigations, only a widely expanded network could provide the expectancy of efficiently obtaining sufficient evidence to be used to investigate and prosecute suspects. The emphasis was then put on conserving evidence in environments where information can be quickly lost, as traditional urgent investigative measures were not able to be taken at the international level. As most of the investigations jumped from local to global level, the available channels for co-operation were too slow and could ruin the possibility to investigate cyber crimes in due time. Such a network, as proposed by the G8 action plan, was the response to the need to ensure that in urgent cases relating to high-tech crime, mutual assistance could be provided rapidly by expedited means of communication. In fact, the Ministers of Justice from the G8 were aware that cyber criminals must be tracked and identified or located very quickly, otherwise their trail may be impossible to trace once communication has terminated. Further, when a communication travels through several countries, law enforcement agents must obtain a preservation or seizure order from the court in its country. Only after such information is disclosed will the next country be determined; and a new cycle will begin in this country. This procedure can be very long, if contacts between law enforcement and judicial authorities are not expeditious.

2.2.2 The network

This operational network of experts on high-tech criminality was designed to assist other experts, from other countries or jurisdictions, in criminal investigations with international connexions. It wants to face the new challenges caused by the new fast-paced high-tech criminalities. Sometimes, computer crime investigations need to rapidly preserve electronic data, so that it can be possible to locate and prosecute suspects. This new need cannot be satisfied by any traditional channel of international co-operation. That is the added value of this network: it can provide help and co-operation very quickly even if a formal co-operation request must follow this informal way.

Since March 1998, a real and effective contact points network was established among G8 States. This contact points network includes one single point of contact for each country represented, available 24 hours a day, 7 days a week. This means that if someone wants to contact the competent authorities from some other country, e.g. to request an urgent preservation of data, it can do so using this quick means, by a phone call or an email message. Later, the formal request will be sent. There are direct communications between the points, to make it easier. It is also supposed to provide, through this network, expertise on cyber matters and on the legal procedure of each country. This network was mainly planned to provide the possibility to immediately preserve traffic data and other stored data worldwide.

If a law enforcement agent wants to seek assistance from a foreign country, he or she must contact his or her own country's contact point, asking for a contact to the foreign contact point. It is supposed that the foreign contact point makes his or her best efforts to ensure that the request is satisfied as quickly as possible. If needed, the requested contact point must ask for help or legal authorisations from the national competent authorities.

Each contact point must be technically trained to understand the specificities of computer crime and computer crime investigations. Moreover, it must have an understanding of local laws concerning, in particular, preservation or collection of electronic evidence. And finally, as English is the most widely spoken language, each contact point must have English speaking available.

Forty-nine countries were listed in the directory of the members of G8 network in December 2007. This directory is compiled and maintained by the G8 Subgroup on High-Tech Crime, currently chaired by the United States.

The members of the network were, in December 2007: Austria, Belgium, Brazil, Bulgaria, Canada, Chile, Croatia, the Czech Republic, Denmark, Dominican Republic, Estonia, Finland, France, Germany, Hong Kong, Hungary, India, Indonesia, Israel, Italy, Jamaica, Japan, Republic of Korea, Lithuania, Luxembourg, Malaysia, Malta, Mauritius, Mexico, Morocco, Namibia, the Netherlands, New Zealand, Nigeria, Norway, Pakistan, Peru, the Philippines, Romania, Russia, Singapore, South Africa, Spain, Sweden, Taiwan, Thailand, Tunisia, United Kingdom and the United States of America[4].

According to the G8 Subgroup on High-Tech Crime, to date, the number of requests made by the 24/7 network has been small. However, in some very important cases, the network provided crucial assistance.

2.2.3 The G8 network and the Council of Europe network

In general terms, the G8 network can be considered a good model network: it provides direct contact between authorities, on a permanent basis.

The merge between the G8 network and the Convention network can clarify the role of the previous informal structure. It can give confidence to non G8 members to become new members of the network. On the other hand, the association with the network described on Article 35 of the Convention gives a legal framework to the G8 network.

2.2.4 European Union initiatives

Since 2005, the European Union adopted a binding instrument concerning the 24/7 contact point network. The Council Framework Decision 2005/222/JHA of 24 February 2005[5] on attacks against information systems includes, in particular, rules referring to the "existing contact points network". The Article 11, No. 1 of the Framework Decision states that all European Union Member States "shall ensure that they make use of the existing network of operational points of contact available 24 hours a day and seven days a week". This is a provision respecting "exchange of information" relating to some listed offences (illegal access to information systems, illegal system interference, illegal data interference and instigation, aiding and abetting and attempt referred to the other).

According to Article 12, each Member State should take the necessary measures to comply with the provisions of the framework decision. Among them, each Member State should inform the General Secretariat of the Council and the Commission of its appointed point of contact.

It is not said in the articles of the framework decision, but is quite clear to the interpreter that the *existing network* is the G8/Council of Europe network. On the one hand, it is said in

[4] This information was provided by Ms. Betty Shave, Assistant Deputy Chief for International Computer Crime, from Computer Crime and Intellectual Property Section of the US Department of Justice (which chairs the G8 Subgroup on High-Tech Crime).
[5] Official Journal of the European Union L 69/67, from 16.3.2005.

the preliminary considerations of the text (Whereas 7) that one of the scopes of the framework decision is to "complement the work performed by international organisations, in particular the Council of Europe's work on approximating criminal law and the G8´s work on transnational co-operation in the area of high tech crime". On the other hand, this document (Whereas 16) recalls the Council Recommendation of 25 June 2001 on contact points maintaining a 24-hour service for combating high tech crime[6].

This last European document, from 2001, recommended to all European Union Member States that had not yet done so, to join the G8 network of contact points.

2.2.5 General overview

In general terms, it can be noted that for the time being, there is still no coincidence among those countries which are a party on the Council of Europe Convention on Cybercrime and the countries listed in G8 24/7 contact points network.

As mentioned previously, not all the countries which ratified the Convention designated a 24/7 contact point. Not all of those which designated such a contact point joined the G8 network. In fact, nine from the twenty one countries which ratified it have not yet joined the G8 network (Albania, Armenia, Bosnia and Herzegovina, Cyprus, Iceland, Latvia, Slovenia, "the former Yugoslav Republic of Macedonia" and Ukraine). As it was said before, three of them have not even designated a 24/7 contact point at all.

So, in the circle of countries listed in the G8 network, only 12 of them ratified the Convention on Cybercrime. Nevertheless, from the group of countries that did not ratify but have already signed the Convention, twelve of them are listed on the G8 network. This G8 list of contact point includes 24 countries which have not signed or ratified the Convention. Only one of them (Russia) is a G8 member and a Council of Europe Member State.

In spite of the European Union Council's recommendation from 25 June 2001, which recommended to all European Union Member States to join the G8 network, eight of the 27 European Union Member States have not yet joined the network (Cyprus, Greece, Ireland, Latvia, Poland, Portugal, Slovakia and Slovenia).

[6] Official Journal C 187/5, from 3.7.2001.

Table 1: 24/7 contact point in countries that have ratified the Convention on Cybercrime

Country	Contact point	Member of G8 network
Albania	Ministry of Interior/Organised and Financial Crime Unit (Police of the State)	No
Armenia	Not established	No
Bosnia and Herzegovina	Not yet established	No
Bulgaria	National Service for Combating Organized Crime under, the Ministry of Interior	Yes
Croatia	Economic Crime and Corruption Department of the General Police Directorate	Yes
Cyprus	International Legal Cooperation Unit of the Ministry of Justice and Public Order	No
Denmark	Danish National Police, Police Department	Yes
Estonia	Criminal Intelligence Department, Estonian Central Criminal Police	Yes
Finland	National Bureau of Investigation, Criminal Intelligence Division / Communications Centre	Yes
France	*Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) Ministry of Interior* *Central Direction of Judiciary Police (DCPJ)*	Yes
Hungary	Hungarian National Police International Implementing Co-operation Centre	Yes
Iceland	National Commissioner of the Icelandic Police (*Ríkislögreglustjórinn*)	No
Latvia	International Co-operation Department of Central Criminal Police Department of State Police	No
Lithuania	Police Department under the Ministry of the Interior	Yes
"The former Yugoslav Republic of Macedonia"	A Deputy Public Prosecutor, from the Department for Fight Against Crime and Corruption, in the Office of Public Prosecutor	No
The Netherlands	National Office of the Public Prosecution Service (*Landlijk Parket van het Openbar Ministerie*)	Yes
Norway	High Tech Crime Division of the National Criminal Investigation Service (*KRIPOS*)	Yes
Romania	Service of Combating Cybercrime within the Directorate for the Investigation of Organised Crime and Terrorism to the High Court of Cassation and Justice	Yes
Slovenia	Ministry of the Interior, Criminal Investigation Police Directorate, International Police Co-operation Section	No
Ukraine	Not established	No
The United States of America	Computer Crime and Intellectual Property Section of the United States Department of Justice, Criminal Division	Yes

Table 2: Countries that have ratified the Convention on Cybercrime and countries that are listed in the G8 contact point network

Country	Ratified the Convention	Contact Point within Article 35	Member of G8 network
Albania	Yes	Ministry of Interior/Organised and Financial Crime Unit (Police of the State)	No
Armenia	Yes	Not established	No
Austria	No	Federal Ministry of the Interior (Federal Office of Criminal Investigation, Department for Computer and Cybercrime)	Yes
Belgium	No		Yes
Bosnia and Herzegovina	Yes	Not yet established	No
Brazil	No		Yes
Bulgaria	Yes	National Service for Combating Organized Crime under, the Ministry of Interior	Yes
Canada	No		Yes
Chile	No		Yes
Croatia	Yes	Economic Crime and Corruption Department of the General Police Directorate	Yes
Cyprus	Yes	International Legal Cooperation Unit of the Ministry of Justice and Public Order	No
The Czech Republic	No		Yes
Denmark	Yes	Danish National Police, Police Department	Yes
The Dominican Republic	No		Yes
Estonia	Yes	Criminal Intelligence Department, Estonian Central Criminal Police	Yes
Finland	Yes	National Bureau of Investigation, Criminal Intelligence Division / Communications Centre	Yes
"The former Yugoslav Republic of Macedonia	Yes	A Deputy Public Prosecutor, from the Department for Fight Against Crime and Corruption, in the Office of Public Prosecutor	No
France	Yes	*Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication* (OCLCTIC) Ministry of Interior Central Direction of Judiciary Police (DCPJ)	Yes
Germany	No		Yes
Hong Kong	No		Yes
Hungary	Yes	Hungarian National Police International Implementing Co-operation Centre	Yes
Iceland	Yes	National Commissioner of the Icelandic Police (*Ríkislögreglustjórinn*)	No
India	No		Yes
Indonesia	No		Yes
Israel	No		Yes
Italy	No		Yes
Jamaica	No		Yes

Japan	No		Yes
Korea	No		Yes
Latvia	Yes	International Co-operation Department of Central Criminal Police Department of State Police	No
Lithuania	Yes	Police Department under the Ministry of the Interior	Yes
Luxembourg	No		Yes
Malaysia	No		Yes
Malta	No		Yes
Mauritius	No		Yes
Mexico	No		Yes
Morocco	No		Yes
Namibia	No		Yes
The Netherlands	Yes	National Office of the Public Prosecution Service (*Landlijk Parket van het Openbar Ministerie*)	Yes
New Zealand	No		Yes
Nigeria	No		Yes
Norway	Yes	High Tech Crime Division of the National Criminal Investigation Service (*KRIPOS*)	Yes
Pakistan	No		Yes
Peru	No		Yes
Romania	Yes	Service of Combating Cybercrime within the Directorate for the Investigation of Organised Crime and Terrorism to the High Court of Cassation and Justice	Yes
Russia	No		Yes
Singapore	No		Yes
Slovenia	Yes	Ministry of the Interior, Criminal Investigation Police Directorate, International Police Co-operation Section	No
South Africa,	No		Yes
Spain	No		Yes
Sweden	No		Yes
Taiwan	No		Yes
Thailand	No		Yes
The Philippines	No		Yes
Tunisia	No		Yes
Ukraine	Yes	Not established	No
United Kingdom	No		Yes
The United States of America	Yes	Computer Crime and Intellectual Property Section of the United States Department of Justice, Criminal Division	Yes

2.3 Interpol, Europol and Eurojust

2.3.1 Interpol

Interpol is an international organisation, whose members are law enforcement bodies from all over the world. At the time of the writing, Interpol counted 184 members from the five continents. The objective of Interpol is to enhance and facilitate cross-border police co-operation. Interpol maintains a global police communication system and develops specific databases and police information analyses.

Interpol was one of the first international institutions to organise meetings of experts on cybercrime: its first cyber-conference took place in Lyon, France, in 1995. Since then, Interpol has developed efforts to help police corporations around the world to strengthen their ability to combat cybercrime. Reaching that goal, Interpol built a contact point network (Interpol National Central Reference Points - NCRP), which seeks to provide assistance to its members, on a permanent basis. NCRP has currently (December 2007) 111 reference point all over the world. These reference points adopted the layout of the 24/7 contact points of the Convention on Cybercrime. In some of the countries that are Parties of the Convention on Cybercrime, the Interpol reference point was also appointed as the G8 contact point. The G8 contact points were included into this network. The objective of this structure was to enable police to immediately identify experts in other countries and obtain immediate assistance in computer-related investigations and evidence collection.

The network should be available 24 hours a day, seven days a week, to face the extremely time-sensitive nature of such subjects. However, this does not always happen with all the contact points. Sometimes it depends on the communications centres from each national Interpol bureau. In other cases, it is assumed by a special police unit, specialised in computer crime. In many countries, the Interpol referenced points are the same as listed within the G8 24/7 network; in some other cases these points are not the same. The same can be said concerning the contact points network referred to under Article 35 of the Convention on Cybercrime.

Thus, this network is directed to provide and exchange police information to its members and to provide technical and operational support. In fact, the main purpose of NCRP is to ensure that typical police information can be exchanged as soon as possible, through specific and appropriate Interpol channels; this includes information on suspected terrorists, wanted persons, fingerprints, DNA profiles, lost or stolen travel documents, stolen motor vehicles, stolen works of art, etc. This type of potentially important information provided by Interpol is surely very useful to concrete investigations. However, precisely because of the scope of the network, it cannot be used to urgently request, for instance, preservation of computer data, or preservation of traffic data, or any kind of measure in order to obtain or conserve evidence. In other words, the kind of co-operation that can be provided by this specific Interpol network is based on the same principles that are otherwise applied to the general Interpol co-operation.

2.3.2 Europol

Europol is a European Union organisation, whose role is to improve the effectiveness of co-operation between law enforcement authorities from each EU member state. It is operational since 1999. Its activities include facilitating the analysis of criminal information and the sharing of data between Member States. It can be used by those Parties of the Convention that are also EU Member States, mainly to increase the efficiency of the provisions of Article 26 of the Convention (spontaneous information).

3 Country studies of good practices

3.1 France, Romania and Estonia: general background

France is an old Member State of the Council of Europe. It is also party to many of the Council of Europe Conventions on criminal matters and on international co-operation. Since 2006, France is also a party on the Convention on Cybercrime. Yet French legislation has been concerned about these subjects for many years and some laws on criminal matters and on international co-operation were adopted. The introduction of the Convention into the French legislative system did not mean a great revolution, because the country had already, previously, adopted many of its provisions.

Romania ratified the Convention on Cybercrime in 2004. The country then transposed its provisions to the domestic level, simply transcribing into national law many of the provisions of the Convention. Thus, Romanian law on cybercrime and on international co-operation on cybercrime matters is quite similar to the text of the Convention.

Estonia ratified the Convention on Cybercrime in 2003. In fact, it was one of the first countries to do so. Moreover, it is one of the most intensive Internet user's countries in the world: a large percentage of the population is an everyday Internet user and every public service or private company is online. Estonia suffered a very important distributed denial of service (DDoS) attack in April and May of 2007, with very extensive consequences. Such attacks caused important disturbances to the everyday life of people and to the government: web pages were defaced, the servers have been saturated and several attacks using botnets were executed. Estonian websites were not available for some days. However, despite the fact that a lot of suspect IP addresses were identified, only one person was prosecuted and convicted. He was the only Estonian citizen that could be identified. All the other suspects used foreign IP addresses.

These are the reasons why these countries were selected for this study. So that they could be analysed in more detail, meetings were held and national experts were contacted[7].

[7] In Nanterre, France, a meeting was held on 17 December 2007, being present Ms. Maud Morel-Coujard, *Vice-Procureur, Chef de La Section S2 aux du Tribunal de Grand Instance de Paris*, Ms. Adeline Champagnat, *Commissaire de Police, Adjoint au Chef de l'Office Central Pour la Répression des Violences aux Personnes* (from *Police Judiciaire*), Ms. Myriam Quemener, *Substitut Général aux Parquet Général de la Cour d'Appel de Versailles* and Mr. Fabien Lang, *Commissaire de Police, Adjoint au Chef de l'Office Central de Lutte Contre la Criminalité Liée aux Technologies de l'Information et de la Communication* (from *Police Judiciaire*).
In Bucharest, meetings were held with Ms. Laura Ceh, *Procuror* and Mr. Virgil Spiridon, Head of Cybercrime Unit of General Inspectorate of Romanian Police on 19 December 2007 and with Ms. Ioana Albani, *Procuror* in the Prosecutor's General Office Attached to the High Court of Cassation and Justice, Ms Cristina Schulmann, Legal adviser in the Department for International Law and Treaties of the Ministry of Justice of Romania and Mr. Florin Razvan Radu, Director of the Directorate of International Law and Treaties of the Ministry of Justice of Romania, on 20 December 2007.
Finally, in Tallinn, a meeting took place on 4 of February 2008, being present Ms. Anneli Poolkase, Attaché at the Security Policy Division from the Estonian Ministry of Foreign Affairs, Mr Ivo Kolk, *Vanemkomissar* from *Keskkriminaalpolitsei*, the Central Criminal Police, Mr. Dimitri Rudakiv, *politseijutivinspektor* from the Criminal Intelligence Department of the *Keskkriminaalpolitsei* and 24/7 contact point person, Mr. Margus Kurm, Chief State Prosecutor, Ms Kalmer, from the Judicial Co-operation Unit of the Estonian Ministry of Justice and Mr. Markko Künnapu, from the Criminal Policy Adviser, within Estonian Ministry of Justice.

3.2 Legal basis for international co-operation in the three countries

3.2.1 France

3.2.1.1 French law

French law received the provisions of the Convention by the introduction of new rules in the *Code de Procédure Pénale*, even before the Convention was ratified by the country. In fact, France ratified the Convention on 10 January 2006, entering in force into French law on the 1 May 2006. However, since 9 March 2004, by the *Loi nº* 2004/204 (*Journal Officiel* from 10th March), internal law already had provisions applying the obligations from the Convention. It has not created a new autonomous regulation: all the alterations were made by new articles, added to the *Code de Procédure Pénale*. On the other hand, the new provisions did not specifically concern cybercrime, instead covering all kinds of international co-operation requests. Provisions were created on general rules concerning transmission and execution of co-operation requests (Articles 694, 694-1, 694-2, 694-3, 694-4 and 694-9), on co-operation with European Union Member States (Article 695-1, 695-10, 695-18, 695-19, 696-20 and 695-21), on interception of communications by the means of telecommunications (Article 706-95) and on extradition (Article 696-1, 696-2, 696-3, 696-4, 696-5, 696-6 and 696-7).

3.2.1.2 French contact points

With regard to contact points, France has a multiple link system, in the context of the Convention. Pursuant to Article 27, the central authority designed by France to make requests from the French judiciary authorities directed to foreign judiciary authorities is the *Ministère de la Justice*. The central authority designed to receive requests for mutual assistance from foreign judiciary authorities directed to the French judiciary authorities is the *Ministère des Affaires Étrangères* and the requests must be transmitted through diplomatic channels. These are the rules respecting procedures pertaining to mutual assistance, in the absence of applicable international agreements.

The *Ministère des Affaires Étrangères* is also the authority responsible for making or receiving requests for extradition in the absence of a treaty for the purpose of Article 24 (extradition). In this last case, all local and territorially competent prosecutors are also indicated as contact points in cases of provisional arrest.

On the matter of the 24/7 network, France designated as point of contact the *Office Central de Lutte contre la Criminalité liée aux technologies de l'information et de la communication (OCLTIC)*. It is a police department, created in 2000 within the *Police Judiciaire*.

Nevertheless, this is a general definition. In fact, France integrates the Schengen space and France is a Party on European Union MLA Convention from 2000. Because of that, international co-operation with authorities of countries belonging to this agreement can follow specific channels – manly direct contacts between judicial authorities. In addition, multiple contacts can be made through Europol or Eurojust.

In France, action on cybercrime is carried out by national police departments, with jurisdiction in the whole national territory: the *Office Central de Lutte Contre la Criminalité Liée aux Technologies de l'Information et de la Communication* and the *Office Central Pour la Répression des Violences aux Personnes*. Both of them belong to *Police Judiciaire*. The first one investigates all cybercrime offences, except paedo-pornography on the Internet, which is carried out by the second department.

At the prosecution service level, there is a special section within the *Tribunal de Grand Instance de Paris (Section S2*), where all offences respecting computer fraud and attacks against computer systems are investigated and prosecuted. It is an autonomous section from the *Parquet* and has jurisdiction over Paris and some surrounding areas.

3.2.2 Romania

3.2.2.1 Romanian law

The first reported cyber fraud cases in Romania were investigated at the end of the last century and the beginning of the new millennium. They were not a success due to the lack of resources. Then, during 2000, it was decided to create a specialised office for the investigation of computer-related crime, within the Prosecutor's General Office attached to the High Court of Cassation and Justice.

Later, in 2002, there was a boom in information and communication technology, followed by a boom in complaints about fraud committed by Romanians on the Internet. That pushed Romania to adopt in 2003 the internal law on cybercrime and in 2004 to ratify the Convention on Cybercrime. In the same period, the first specialised police body responsible for the investigation of cyber crime offences was created within the General Inspectorate of the Romanian Police.

In Romania the internal law received, *qua tale*, most of the provisions of the Convention. In Romania the internal law received, *qua tale*, most of the provisions of the Convention. They were included in Law no. 161/2003 (Title III), which regulates the combating and prevention of cybercrime by implementing specific measures to prevent, discover, and punish the offences committed through computer systems.
Law No. 302/2004 is an extensive law on international judicial co-operation in criminal matters, which provides international cooperation procedures including on extradition and surrender based on European Arrest Warrant and also covers some of the provisions of the Convention.

International co-operation provisions are described in Articles 60 to 66 of Law 161/2003. Spontaneous information (Article 26 of the Convention) is transposed to Article 66 of Law 161/2003 and also to Article 166 of Law 302/2004. Confidentiality and limitation on use (Article 28 of the Convention) is referred to in Article 12 of Law No. 302/2004. Finally, provisions of Article 27 of the Convention are described in Article 12 of Law 64/2004 that ratified the Council of Europe Convention on Cybercrime.

Thus, Romania has a very extensive legal framework on cybercrime and on co-operation on cybercrime matters. Besides, according to Article 11 paragraphs 2 of Romanian Constitution "*treaties ratified by the Parliament, according to the law, are part of national law".*

The country has a significant amount of cybercrime cases, around 800/900 per year. To face this emerging criminal phenomenon, Law nr 508/2004 established that on cybercrime cases the investigation will always be carried out by the Public Prosecution Service (in other cases, the prosecutors only supervise the investigation prepared under the responsibility of police officers). For that purpose a special independent unit was designed: the Service of Combating Cybercrime within the Section for Combating Organised Crime and Drugs Trafficking to the High Court of Cassation and Justice.

3.2.2.2 Romanian contact points

For the purpose of Article 24 of the Convention, the central authority designated by Romania, responsible for making or receiving requests for extradition or provisional arrest, is the Ministry of Justice.

The central authority responsible for sending and answering requests for mutual assistance, in accordance with Article 27 of the Convention, depending on the moment of the proceedings, are the Prosecutor's Office to the High Court of Cassation and Justice for requests of judicial assistance formulated in pre-trial investigation and the Ministry of Justice for the requests of judicial assistance formulated during the trial or execution of punishment.

As said before, Romania designated as its contact point, in accordance with Article 35 of the Convention, the Service for Combating Cybercrime within the Directorate for the Investigation of Organized Crime and Terrorism. The competence to investigate organized crime, cybercrime, crimes of terrorism etc. belongs exclusively to the prosecutor who is leading the preliminary investigation of the prosecutorial stage and is entitled to indict an offender based on the pre-trial evidence.

This contact point is covered by legal statute, under Article 62 of Romanian Law No. 161/2003, that describes in detail the attributions of this contact point, stating that "within the international co-operation, the competent foreign authorities can require from the Cyber-Crime Fighting Service the expeditious preservation of the computer data or of the data regarding the traffic existing within a computer system on the territory of Romania". This rule supposes that this informal request will be followed by a request for international legal assistance in criminal matters. Article 62 also describes the content that the formal request would include and finally underlines that "the preservation request is executed for a period of 60 days at least and is valid until a decision is taken by the Romanian competent authorities, regarding the request of international legal assistance in criminal matters".

There are therefore two international co-operation structures: one of them, the Service of Combating Cybercrime within the Directorate for the Investigation of Organized Crime and Terrorism, which focuses on cybercrime and above all on urgent matters; the other one, within the Ministry of Justice, is responsible for all general co-operation requests.

About 30% of all mutual assistance international requests received by Romania concern cybercrime, particularly internet fraud and credit card fraud.

3.2.3 Estonia

3.2.3.1 Estonian law

As it was said before, Estonia was one of the first countries to ratify the Convention on Cybercrime in May 2003. The country belongs to the small group of countries where the Convention has been in force since 1 July 2004.

Internal law makes provisions according to the provisions of the Convention, namely in the Penal Code and in the Penal Procedure Code. Those provisions were adopted even before the ratification of the Convention, because the country had already placed great emphasis on cybercrime. Nevertheless, at that time there was limited experience in this field.

On 21 February 2008, the Estonian Parliament adopted some new amendments related to cybercrime in the Penal Code and the President declared them new law on 6 March 2008.

3.2.3.2 Estonian contact points

For the purpose of Article 24 of the Convention (extradition), Estonia designated the Ministry of Justice, in the absence of an extradition treaty, as the authority responsible for making or receiving requests for extradition or provisional arrest. The same Ministry of Justice was designated, on the other hand, pursuant to Article 27 of the Convention, as the central authority responsible for sending and answering requests for mutual assistance, the

execution of such requests or their transmission to the authorities competent for their execution.

Finally, Estonia designated the Central Criminal Police as a contact point within the framework of the Convention. An officer from Estonian Central Criminal Police was personally nominated as the point of contact for the network 24/7, pursuant to Article 35 of the Convention. Nevertheless, a legal provision describing this contact point was included within the law that ratified the Cybercrime Convention.

This officer, who belongs to the Criminal Intelligence Department of the Central Criminal Police, is also the contact point within the Interpol network and to Europol. In fact, he coordinates all international relations from the police side, in Estonia. In such a way, he concentrates information, so that efforts can be coordinated when a request proceeds from more than one channel. On the other hand, as he is a police officer and is bestowed with common police powers, he can directly satisfy most of the received requests, such as preservation of data, for example.

In practical terms, Estonia does not receive many requests, and all of them follow classic general channels: until now, nothing has been requested from Estonia through the 24/7 network. Likewise, it has never needed to send such a request abroad. Normally, in other cases, the requests are received and sent by Interpol or Europol channels.

3.3 Application of specific provisions in the three countries

3.3.1 Jurisdiction (Article 22)

Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
   a in its territory; or
   b on board a ship flying the flag of that Party; or
   c on board an aircraft registered under the laws of that Party; or
   d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Some aspects mentioned both in Romania and in France related to jurisdiction. Difficulties were referred to in some cases to find the right jurisdiction and the power to know the facts and to investigate and prosecute the case. It could be the place where the crime was committed or the place where the crime produced its results. This was not underlined as a specific problem of international co-operation, but in this context the problem becomes wider.

Estonia recognised this issue, which can be a daily problem above all at the domestic level, but underlined that there were never problems with it in court. Normally, Estonia does not open an investigation if the perpetrator of the offence seems to be outside the country. However, investigations are opened in some cases, even if the suspect comes from abroad, for example if an Estonian bank account is used to commit the crime. In cases where the victim is an Estonian, the complaint is collected and sent to the competent authority in the country where the criminal action is supposed to have been performed. These authorities never refused those complaints. Some cases were noted where investigations were really made (in the United Kingdom and in Germany).

In certain situations, a revision of the general criteria was suggested, for example providing jurisdiction to the place or the country where the victim lives.

It was also emphasised that a very relevant number of cases on cybercrime were international cases, with investigations covering more then one country. In such cases, it was remarked that the different types of incrimination, the different proceedings and the different jurisdiction rules among all the possible related countries create difficulties for international co-operation.

In order to tackle this problem, it was suggested to create centralisation rules that permit law enforcement and other authorities to agree about the country or jurisdiction with better conditions to investigate and prosecute.

In Romania it was noted that the country provides universal jurisdiction in these matters if the perpetrator is found on its territory.

3.3.2 Extradition (Article 24)

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.

7 a 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 name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

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

Not one of the analysed countries had specific provisions regarding extradition on cybercrime matters. Three of them only have extradition general rules concerning all the types of criminality. Even in cybercrime cases, general agreements or treaties were applied to require extradition or to extradite someone. There were no remarks on this respect. Nevertheless, the importance of the European Arrest Warrant was emphasised, within the European Union Member States.

Estonia reported that the country has had until now a small number of international requests for extradition, most of them to Russia. In a concrete case, from April 2007, the extradition was not possible because the person in question was a Russian citizen and Russia refused the request. The concrete investigation concerned an offence committed via computer means and the Internet. Estonia then issued a European Arrest Warrant, which was sent to the system, so that it could be executed if the suspect enters the European Union at any time. In the concrete case, Interpol refused to co-operate, because it classified the case as a political case (the facts concerned an article published on the Internet against the Estonian State).

3.3.3 MLA principles and procedures (Articles 25, 26, 27, 28)

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.

Article 26 – Spontaneous information

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

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

(…)

Article 28 – Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions 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 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

Article 60 of Romanian Law 161/2003 states that "Romanian legal authorities co-operate directly (…) with the institutions with similar attributions in other states, as well as with the international organizations specialized in the domain". This direct co-operation will be provided "under the conditions of the law and by observing the obligations resulting from the international legal instruments Romania is part of".

Such a kind of co-operation can have as its scope, where appropriate, international legal assistance in criminal matters, extradition, the identification, blocking, seizing or confiscating of the products and instruments of the criminal offence, carrying out common investigations, exchange of information, technical assistance or of any other nature for the collection of information, specialised personnel training, as well as other such activities.

Estonia did not refer to any type of specific rule concerning international co-operation on cybercrime. It was underlined that in Estonia, as in the rest of Europe, the effective basis for all co-operation is the Council of Europe Convention from 1959 and, within the European Union, the MLA Convention from 2000. Estonia held bilateral agreements with some other countries outside the European Union and Council of Europe.

For what concerns formal procedure, a difference was found between France and Romania: in France, each time a request is received, for instance intending to gather evidence, a formal file is opened so that the evidence can be gathered; in Romania the only needed file in such a case is the rogatory letter. This is valuable both to police co-operation and to judicial co-operation. If any Romanian authority needs further information to justify the gathering of evidence, it can ask it to the competent authority of the requesting State.

In both cases, France and Romania (as well as in Estonia), national law allows law enforcement to do within international co-operation everything which can be done in a domestic investigation.

In Romanian Law 161/2003, there is a special provision on spontaneous information, in Article 66, stating that "the competent Romanian authorities can send, ex-officio, to the competent foreign authorities, observing the legal provisions regarding the personal data protection, the information and data owned, necessary for the competent foreign authorities to discover the crimes committed by/through means of information systems or to solve the causes regarding these crimes" (art.26 of the Convention).

In addition, Article 166 of the Romanian Law 302/2004, on international judicial co-operation in criminal matters, describes "spontaneous transmission of information" (according to Article 26 of the Convention), stating that "Romanian judicial authorities may, without prior request, forward to the competent authorities of a foreign State information obtained within the framework of their own investigations, when they consider that the disclosure of such information might assist the receiving State in initiating criminal proceedings, or might lead to a request for judicial assistance by that State".

French authorities stated that spontaneous information is a useful tool, which they use in both directions, receiving and sending information from and to other countries' authorities. Romanian authorities expressed a very similar point of view; they have used this tool in both directions. Romanian authorities emphasised that in more than one case this kind of exchange of information, above all to and from the United States, was the origin of concrete investigations, mainly regarding "phishing" schemes, "skimming" and "vishing". In one particular case, information sent from Romania to Germany was the beginning of an investigation where some people were arrested, within a credit card fraud scheme.

French and Romanian authorities referred to some difficulties with international requests in certain countries, caused by important differences between legal systems. In some countries, for example, some kinds of offences are prosecuted only if there is a certain amount of damages. If the damages are lower than that, co-operation is refused.

Some other difficulties were underlined, concerning the bureaucratic side of international mutual assistance. Some cases were referred to in which, pursuant to Article 29 of the Convention, mutual assistance was required and expedited preservation of data was made. Later, for some reason, the formal request never arrived to the requested state.

3.3.4 Expedited preservation and disclosure (Articles 29 and 30)

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:

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.

Under Romanian Law 161/2003, Article 63, within the international co-operation, expeditious preservation of the computer data or of the data regarding the traffic data existing within a computer system can be required by foreign authorities.

On the other hand, according to Article 64, if the preserved data reveals that a service provider in another state is found to be in possession of the data regarding the traffic data, the requesting foreign authority can be immediately informed about this, communicating also all the necessary information for the identification of the respective service provider.

In addition, Article 171 of the Romanian Law 302/2004, on international judicial co-operation in criminal matters, describes the conditions under which interception and recording of conversations and communications can be made, prior to a request from the competent authorities from a foreign state, in view of solving a criminal case, where the prosecuted

person is in the territory of the requesting State and the latter needs technical assistance to intercept communications from the target, or is in Romanian territory, in the event that the communications from the target can be intercepted by Romania, or is in the territory of a third State, which has been informed and if the requesting State needs technical assistance for intercepting communications from the target. The judicial assistance may consist of the interception of telecommunications and their immediate transmission to the requesting State, or in the interception of the recording and of the subsequent transmission of the recording of telecommunications to the requesting State.

In Estonia, these methods of gathering evidence, in domestic cases or in case of international co-operation, are covered by general police powers. There are not specific rules regarding cybercrime. The European Directive on data retention was referred to in this context, which Estonia adopted at the domestic level. The used method to implement this type of gathering of evidence is, in Estonia, the search (and seizure). Police asks to the owner of the data to preserve them and later performs a search to seize those data.

A concrete case of judicial co-operation was reported, following a request from Sweden which asked for the preservation of data. Those data were preserved and seized by an order from the prosecutor and were later sent to the requesting country. However, this concrete co-operation followed the proceedings from the European Union MLA.

Article 29 of the Convention on Cybercrime is probably one of the most widely used tools of the Convention. The French and Romanian authorities interviewed referred to the fact that on some occasions they required or have been required to preserve traffic data. On most of the occasions, this kind of request was made through the 24/7 network of contact points. It was emphasised that many of these requests, were made to the United States, in which territory a large amount of email-account subscriber data are located.

Problems concerning the possibility of refusing the co-operation based in the requirement of dual criminality as a request for mutual assistance were not referred to. In the same way, no mention was made of any refusal due to the consideration that the concrete offence was a political offence and to the consideration that execution of the request was likely to prejudice the sovereignty, security, *ordre public* or other essential interests of the requested State.

However, it was stated that the lack of time in provision of No. 7 of Article 29, concerning the obligation of preservation of data for a period not less than 60 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, was too short.

In some cases, State bureaucracy takes much more than 60 days to issue and transmit the formal request of mutual assistance. In Romania it was mentioned that national law allows this provisional preservation for 90 days and even in this case some requiring States do not make a formal request on time. In France it was said that this procedure can sometimes take one year.

It was not underlined as a legal problem that France transposed to internal law the European Union Framework Decision on data retention and decided to impose the obligation of preservation of data for one year to ISP and other operators. The same solution will be adopted in Romania: previously as a draft law, and now under study in the Ministry of Justice, highlights the obligation of preservation for 12 months.

It was also emphasised that, in some cases, contact points of the 24/7 network did not reply to the informal requests made to them. This could be due to the non-effectiveness of the contact point or, mainly, to the difference between legal systems and the consequent difference from legal requirements to preservation of data.

No experience was collected from cases of real application of Article 30 of the Convention. Nevertheless, in France it was stated that such a kind of assistance would require, according to its domestic law, the opening of a specific internal criminal investigation, under the direction of a judge, because only in this case could the co-operation be provided.

In Romania there is also no experience respecting the co-operation under this article. However, it was mentioned that this is the type of information which can be obtained in the police exchange of information.

Regarding the points of the preservation of data and latter disclosure after a formal request is made; a case was briefly presented by the Romanian authorities which was successfully handled although still under investigation and justice secrecy. In spite of that, it could be said that a massive amount of fraudulent transactions using stolen credit cards was detected in Romania, taking place within the "Western Union" system in several Romanian counties. Then, a bank notified Romanian authorities that it had been the target of "phishing" attacks, proceeding from webmail accounts provided by an ISP based in the USA. Romanian authorities asked for co-operation from the United States, requiring information about subscriber data and traffic data from some email-account owners, using ISPs based in the United States. There was a good response from the United States and the data were immediately preserved and the email accounts were monitored. IP addresses from Romania were detected and this information was given to the Romanian authorities. This information allowed for the opening of an investigation under the Romanian Prosecution Service. 21 searches were performed in Romania and 11 suspects were arrested and charged for belonging to an organised crime group, computer fraud and fraudulent use of electronic payment instruments.

3.3.5 Trans-border access (Article 32)

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

According to Romanian Law No. 161/2003 (Article 65), "a competent foreign authority can have access to public Romanian sources of computer data without the necessary of formulating a request in this sense to the Romanian authorities". Moreover, a foreign authority can have access to computer data stored in Romania, "if it has the approval of the authorized person, under the conditions of the law, to make them available by means of a computer system", without requesting the Romanian authorities.

In the same way, Romanian authorities are allowed to collect open source information as suitable evidence.

In France, the existence of some cases in this context was mentioned. France incorporates into its internal law the principle of free evidence obtaining, meaning that all the evidences can be gathered within a criminal procedure, if it is not forbidden by law. Thus, Article 32 of the Convention is completely reflected into the French national law.

Nevertheless, this was not pointed out as a great advantage by the French authorities. They stated that they tried to obtain, under this legal possibility, subscriber information stored by webmail servers in small fraud cases and in offences against honour and consideration cases,

where international co-operation is not merited. They were not successful because the ISP always refused to provide such information, even if it was not classified as confidential.

Estonia stated that it has no specific regulation on this subject because it does not need it. Obtaining open information on the Internet is something inside general police powers and is permitted by law. An example was given of the case of the information relating to the IP addresses owner. It is publicly available on the Internet and is sometimes essential to begin an investigation.

3.3.6 Mutual assistance regarding accessing stored computer data (Article 31), the real-time collection of traffic data (Article 33) and the interception of content data (Article 34)

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 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.

In Romania, Article 57 of the Law 161/2003 provides some general provisions on access to a computer system, as well as the interception or recording of communications carried out by means of computer systems. However, the applicable provisions regarding audio and video interception and recording of conversations or communications by telephone or by any other electronic means of communication are provided by Article 911 (Section V1) of the Criminal Procedure Code.

There is no experience, in Romania, on international co-operation with respect to requests for the interception of communications and for real-time collection of traffic data in electronic communications, but one case concerning the interception of telephone communications was mentioned. There were no problems mentioned in this respect.

Some requests were also made to Romania for search and seizure of computers and computer data. They were accomplished and the rogatory letters sent back to the requesting countries without any legal or operational issues.

With regard to Estonia, the Penal Procedure Code contains rules concerning telephone interceptions, which are also valid to all other communications. The same can be said if international co-operation is required. In the case of computer stored data, normally the practical method is to perform a search of the owner of the data and formally seize those data, by a prosecutor order.

International co-operation to intercept computer data was never required to Estonia but sometimes telephone interceptions are requested. The same can be said regarding international requests made by Estonia to other countries (requests of telephone interceptions have been made, namely to Finland, Spain, Poland, Sweden and Germany).

Content interception of computer communications can be made in Estonia, legally (with a judge order, according to general rules, from the Penal Procedure Code) and technically. However, it is not very frequent. Estonia never made such a request to other countries, but some requests were already made by other countries. At the domestic level, content interceptions are made seldom, and only in very important cases.

In France, no references were made to this topic.

3.3.7 24/7 Contact Points (Article 35)

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.

In Romania, the designated contact point, in accordance with Article 35 of the Convention, is the Service of Combating Cybercrime within the Directorate for the Investigation of Organized Crime and Terrorism. As it was said before, this contact point is referred to in Article 62 of Romanian Law No. 161/2003 that describes, in detail, the attributions of this contact point (providing specialised assistance and giving information on the Romanian legislation to similar contact points in other states; ordering the expeditious preservation of data, as well as the seizure of the objects containing computer data or the data regarding the data traffic required by a competent foreign authority and execution; or facilitating of the execution of letters rogatory in cases of cybercrime).

Under this section, by the means of the contact point network, Romania receives around 10 requests each year and requires two or three from abroad. In both cases the majority are to and come from the United States.

It was stated that normally this contact point is only used to ask for preservation of traffic data. Sometimes, this channel is used by police to exchange information and intelligence, which can be crucial in criminal investigation.

Such a kind of exchange of information happens above all with contact points having a good relationship with Romania and Romanian police officers. In general, it was emphasised, personal relations are very much helpful.

It was also mentioned that it is not quite clear what are the real functions of 24/7 network and what can really be asked and provided by this channel. Clarification could stimulate more countries to join the network and to use it.

Romanian authorities underlined that not all the requests they have made to some of the 24/7 contact points received a reply. On the other hand, not all the countries are aware of all the possibilities permitted by the network. Some more information about it would help to increase its use and expansion.

In the case of France the designated 24/7 network point of contact is the *Office Central de Lutte contre la Criminalité liée aux technologies de l'information et de la communication*, which is a police department, within the *Police Judiciaire*.

It was mentioned that the 24/7 network is only used to request preservation of traffic data. All other kinds of request are made by formal international co-operation requests, mainly by the means of rogatory letters. Nevertheless, it was recognised that by this kind of contact point, relationships between authorities became much more informal, which was seen as an advantage. In spite of that, however, it was pointed out that the informality could also be a negative aspect, because there are no guarantees of proper reply from all the points of contact.

French authorities described 10 to 20 requests received per year by the 24/7 contact point, mainly proceeding from European Union Member States and the United States of America. By these informal contacts, other country authorities request above all technical support and preservation of traffic data. Sometimes, they report "phishing" or other illegal content sites, asking for shut down. All other kind of mutual assistance requests are sent to France by the classic means of international co-operation and sometimes by Interpol.

Still regarding France, it was said that the informality of each contact of this nature created a legal obligation for French law enforcement authorities to open a formal case in France, so as they have legal ground to all the activities of gathering evidence.

It was also stated that there is a regular and efficient update of contact points' information by email within the network.

A case was described, relating to some threatening messages that a French family received by email. Someone was blackmailing the family, from a webmail account belonging to an American ISP. France asked for co-operation from the United States and an IP address was very quickly identified, in California. In the United States, an investigation was opened and the perpetrators were identified. In this case, it was stated, the 24/7 mechanism was really very useful and efficient.

As previously mentioned, Estonia designated a contact point within the framework of the Convention, available 24 hours, 7 days a week, pursuant to Article 35 of the Convention. It is a police contact point, within the Central Intelligence Department of the Central Criminal Police, which is also contact point in the Interpol network and to Europol.

However, Estonia has never been contacted through the 24/7 network contact point and did not feel the need to send such a kind of request abroad through this network.

3.4 Beyond the Convention: other tools for international co-operation in the three countries

3.4.1 Police co-operation

It was stated by French authorities that besides all police channels, mainly through Interpol, there is not much more legal ground to exchange information and police co-operation on cybercrime matters. French police only can provide police information to foreign police agents. If any gathering of evidence is required, the intervention of the prosecution service is mandatory.

It was also referred by French prosecutors that police contact points normally do not reply to theirs requests, even in the framework of 24/7 contact point network. That situation requires the prosecutor to make a formal judicial assistance request.

As an alternative to 24/7 G8 contact point network, it was mentioned by French authorities that they very often use Europol and Interpol, which present to them the advantage of language: within the G8 network the official language is English (and only English) and that can be a problem, it was mentioned.

Europol and Interpol are also the normal channels used by law enforcement to exchange police information. Sometimes these channels are also the used channels to transmit rogatory letters, as an alternative to the classic diplomatic channels.

These two bodies, Europol and Interpol, have personal contact points in charge and liaison officers. This is considered very positive by French authorities, because it increases efficiency.

Something similar was said in Romania. The great advantage represented by the existence of legal *attachés* from other countries in Bucharest was also mentioned (this mainly related to the legal *attaché* from the Federal Bureau of Investigation, of the United States of America).

The same comment was heard from Estonia: liaison officers are very useful when police information is required and, even if they are not an alternative to the official channels, normally they are able to speed up the international co-operation procedure. Estonia has liaison officers in Finland and Russia, besides Europol. There are liaison officers in Estonia from France, Germany (even based in Latvia), Finland and the United States.

A case was described in this context: data preservation was required through the contact point of the 24/7 network, by Romania to the United States. The request was not accomplished until the FBI legal *attaché* in Bucharest intervened in the procedure. By its means, the required information was obtained in the United States and sent to Romania, based on informal requests.

Romanian authorities stated that they receive about 700 international requests for mutual assistance per year, by rogatory letters, through the Ministry of Justice. Most of them, of course, are requests for gathering of evidence. Some of them require telephone interceptions and searches. Romania also receives European Arrest Warrants.

In addition, about 300 to 400 informal requests are received per year, asking for police information, such as identification of numbers and other identification data from someone, or telephone numbers. These kinds of requests have police treatment, following police traditional channels – Interpol, Europol or *liaison* officer. They never relate to evidence, but to police information and intelligence. If evidence is requested, then a formal request must be fulfilled.

In Romania, the Service for combating cyber criminality within the General Inspectorate of the Romanian Police is the contact point in the G8 Network responsible for police exchange of information regarding cybercrime, besides the National Centre for Police Co-operation which is the main responsible institution for international police co-operation. The SCCC is the police unit supporting the prosecutors (DIOCT-SCCC) in investigating cybercrime cases.

The preference for the 24/7 network was underlined by Romanian judicial authorities, instead of classic channels such as Interpol, because it facilitates the direct contact between prosecutors from different countries. The importance of having liaison magistrates in different countries was also mentioned – Romania already has a liaison magistrate in Italy and will have another, probably soon. These magistrates can be helpful when an international request is being prepared. They can explain the terms under which rogatory letters must be redacted and to whom it should be sent.

As it was said before, in Estonia, not many international co-operation requests concerning cybercrime matters were received. Furthermore, they are generally conveyed through Interpol or Europol channels. That is also, in general, the way chosen by Estonian Police to request co-operation from other countries. Even in the case of judicial co-operation, Estonian prosecutors send requests informally via the Interpol channels, even if they need to send them officially by the proper judicial channels.

3.4.2 Other channels and international co-operation instruments

As said before, in Romania, the Convention on Cybercrime is seen as a useful tool to international co-operation if it is needed to quickly preserve computer data and to forward to other countries information obtained within the framework of its own investigations. However the framework of the Convention was never used to ask for co-operation on interceptions of communications and such a request from any other Party was never received.

Estonia so far has not made use of the 24/7 network, as mentioned previously.

In France, the network is also mainly used to exchange police information and to request expedited preservation of date.

For other kinds of international co-operation measures, Romania prefers, rather than the Convention, the framework of European Union 2000 MLA, in force in all European countries and in Romania and Bulgaria since December 2007. The advantage of this international agreement is to facilitate direct contacts between judicial authorities from different Member States from the European Union.

The great added value of the establishment of personal contacts between officers from different law enforcement agencies was emphasised. This is particularly important when informal assistance is needed, in some particular cases. Romanian authorities referred to the great progress they made, since Romania's entry to the European Union – they did not feel a such great advance when the country entered the Council of Europe.

With regard to non-EU Member States, all the three countries stated that the Council of Europe Convention from 1959 is still in force, and the two additional protocols, on co-operation on criminal matters. Outside Europe, some bilateral treaties allow international co-operation. Romania referred to treaties with the United States, Canada, Egypt, Cuba and Algeria. Estonia mentioned Russia, Ukraine and the United States. All the countries underlined that a significant number of the co-operation requests follow the proceedings of this framework.

4 Conclusions

Computer crime creates new challenges for law enforcement around the globe, as crimes can be committed remotely and critical evidence is volatile and may vanish rapidly.

Cybercrime is the most transnational of all crimes. Investigating cybercrime needs efficient international co-operation. Without such co-operation, investigations are unlikely to succeed.

The Council of Europe Convention on Cybercrime provides many useful tools regarding international co-operation, including in particular the network of 24/7 contact points under Article 35 of the Convention.

Not all the countries that have ratified the Convention on Cybercrime have yet established functioning contact points as required. And some of the countries that have ratified and established the 24/7 contact points have not yet joined the G8 High-Tech Crime Sub-Group 24/7 network. Countries should make urgent efforts in this respect.

In Romania and in France, the Convention on Cybercrime is seen as a useful tool and effectively used for international co-operation in order to rapidly preserve computer data and to forward information obtained within the framework of its own investigations to other countries. Until now, the framework of the Convention has not been used by France and Romania to ask for co-operation regarding the interception of communications, and these countries have not yet received such requests from any other Party of the Convention.

In Estonia, the Convention framework is not much used yet, and other channels are preferred. The common framework that the Convention creates is considered an advantage, mainly in that it defines the types of crime and with regard to international co-operation. However, the small number of countries that have so far ratified the Convention is seen as a problem. In the concrete case of the attacks suffered by Estonia in April and May 2007, it would have been useful for the investigation had Russia been a party to the Convention and able to co-operate under this framework. As it was not possible and most of the attacking IP addresses identified appeared to be located in the Russian Federation, only one person was prosecuted. All the other perpetrators remained unpunished.