Project on Cybercrime
www.coe.int/cybercrime

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

Version
2 April 2009

Discussion paper

The functioning of 24/7 points of contact for cybercrime

Prepared by the Economic Crime Division

This discussion paper has been prepared by the Economic Crime Division 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

Disclaimer:

Contents

1 Background and context

Cybercrime is probably the most transnational of all crime and thus poses particular challenges. Efficient international cooperation is required in order to cope with situations where perpetrators from one country attack victims or computer systems in other countries, where data – including traffic data – is crucial evidence but is volatile and travels through several jurisdictions. Traditional ways of police and judicial cooperation are thus not sufficient.

The Budapest Convention on Cybercrime can help countries meet these challenges:

- The chapter on substantive law ensures a minimum of harmonisation of substantive criminal law of different countries
- The procedural law chapter provides law enforcement with a set of efficient investigative tools that are available in a similar manner in the countries that are implementing the Convention, such as the expedited preservation of computer data
- The chapter on international cooperation contains general measures for international cooperation, but also specific ones such as the expedited preservation of computer data and other investigative measures at the international level
- In order to facilitate immediate, "expedited" or provisional measures the Convention stipulates that each party to the Convention establish a 24/7 point of contact. The provisional measures taken by these contact points (CP) in most cases need to be followed up to by formal requests for legal cooperation.

By December 2008, 22 of the then 23 parties to the Convention had established a CP according to article 35. The text of this article and relevant extracts from the explanatory report to the Convention are reproduced below for ease of reference.

The network of CP of the Convention on Cybercrime is based on the experience of the network created by the G8 High-tech Crime Subgroup in 1997. The list of CP of the Convention and the directory of CP of the G8 are being merged. By December 2008 the combined directory contained some 60 CP from all over the world.

International legal cooperation in cases involving computer systems is also possible under a range of other international agreements on cooperation in criminal matters as well as bi-lateral agreements or on the basis of reciprocity. The same applies to international police cooperation.

In this context Interpol with its network of National Central Reference Points (NCRP) is highly important and available to provide assistance to its more than 110 members on a permanent basis.

Nevertheless, the Convention on Cybercrime is the only specific international treaty in cybercrime matters and provides a framework for international cooperation for those countries that have ratified or acceded to this treaty.

The Cybercrime Convention Committee (T-CY) is meeting at least once every year and follows the implementation of this treaty. At its 3rd meeting (Strasbourg, 3-4 April 2008), it discussed among other things, the question of CP as well as difficulties in international cooperation and requested the Council of Europe's Project on Cybercrime to follow up on the following issues:

16. The T-CY requested the Project on cybercrime to prepare, in co-operation with the Committee of experts on the operation of European Conventions on co-operation in criminal matters (PC-OC) and the G8 Network:

- a report dealing in particular with the nature, role, powers, legal basis and institutional e-mail addresses of contact points and to submit it to the next meeting of the T-CY.

23. One particular difficulty pointed out by the T-CY was the question of the effective follow up to requests for expedited preservation and other preliminary measures through formal requests for mutual legal assistance. It was proposed, among other things, that 24/7 contact points and competent authorities for mutual legal assistance should strengthen their cooperation with each other.

27. The T-CY took note of a proposal by Romania concerning the preparation by the T-CY of a checklist for use between the 24/7 contact points for requests for expedited preservation of computer data and requested the Project on cybercrime to present a draft for consideration by the T-CY at its next meeting.

The Project on Cybercrime has thus been tasked with the preparation of a report on the functioning of 24/7 CP and the preparation of a checklist for requests for expedited preservation.

The present report has been prepared on the basis of replies to a questionnaire received from 14 CP[1] in October 2008 and discussions at a meeting of contact points and competent authorities for judicial cooperation held in Ohrid, "the former Yugoslav Republic of Macedonia", on 18-19 November 2008 under the Project on Cybercrime and the PROSECO Project of the Council of Europe and the European Commission.

In November 2007, the Council of Europe's PC-OC Committee[2] sent a questionnaire to countries which are parties to European conventions on cooperation in criminal matters on mutual legal assistance in computer-related cases. The replies received from 23 countries in the course of 2008 have also been taken into account.

In February 2009, a draft of the present report was presented to the High-tech Crime Subgroup of the G8 in Rome.

The basis for this report is obviously somewhat limited, but nevertheless sufficient to provide food for thought.

The purpose of this report is to provide a short analysis of the functioning of 24/7 points of contact as well as the links to mutual legal assistance. A number of suggestions are made - including a checklist for expedited preservation requests – to make the application of the relevant provisions of the Convention more effective.[3] The report will also help share good practices and provide guidance to countries wishing to establish CP and engage in more efficient international cooperation.

[1] 13 parties to the Convention and Spain.
[2] Committee of Experts on the Operation of European Conventions on Co-operation in Criminal Matters (PC-OC).
[3] The report may also be considered in conjunction with a discussion paper on "the effectiveness of international cooperation against cybercrime – examples of good practice" prepared by Pedro Verdelho (Portugal) under the Project on Cybercrime in April 2008.

Convention on Cybercrime (CETS 185)

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.

Extract from the explanatory report: 24/7 Network (Article 35)

298. As has been previously discussed, effective combating of crimes committed by use of computer systems and effective collection of evidence in electronic form requires very rapid response. Moreover, with a few keystrokes, action may be taken in one part of the world that instantly has consequences many thousands of kilometres and many time zones away. For this reason, existing police co-operation and mutual assistance modalities require supplemental channels to address the challenges of the computer age effectively. The channel established in this Article is based upon the experience gained from an already functioning network created under the auspices of the G8 group of nations. Under this Article, each Party has the obligation to designate a point of contact available 24 hours per day, 7 days per week in order to ensure immediate assistance in investigations and proceedings within the scope of this Chapter, in particular as defined under Article 35, paragraph 1, *litterae a) – c)*. It was agreed that establishment of this network is among the most important means provided by this Convention of ensuring that Parties can respond effectively to the law enforcement challenges posed by computer- or computer-related crime.

299. Each Party's 24/7 point of contact is to either facilitate or directly carry out, *inter alia*, the providing of technical advice, preservation of data, collection of evidence, giving of legal information, and locating of suspects. The term "legal information" in Paragraph 1 means advice to another Party that is seeking co-operation of any legal prerequisites required for providing informal or formal co-operation.

300. Each Party is at liberty to determine where to locate the point of contact within its law enforcement structure. Some Parties may wish to house the 24/7 contact within its central authority for mutual assistance, some may believe that the best location is with a police unit specialised in fighting computer- or computer-related crime, yet other choices may be appropriate for a particular Party, given its governmental structure and legal system. Since the 24/7 contact is to provide both technical advice for stopping or tracing an attack, as well as such international co-operation duties as locating of suspects, there is no one correct answer, and it is anticipated that the structure of the network will evolve over time. In designating the national point of contact, due consideration should be given to the need to communicate with points of contacts using other languages.

301. Paragraph 2 provides that among the critical tasks to be carried out by the 24/7 contact is the ability to facilitate the rapid execution of those functions it does not carry out directly itself. For example, if a Party's 24/7 contact is part of a police unit, it must have the ability to co-ordinate expeditiously with other relevant components within its government, such as the central authority for international extradition or mutual assistance, in order that appropriate action may be taken at any hour of the day or night. Moreover, paragraph 2 requires each Party's 24/7 contact to have the capacity to carry out communications with other members of the network on an expedited basis.

302. Paragraph 3 requires each point of contact in the network to have proper equipment. Up-to-date telephone, fax and computer equipment will be essential to the smooth operation of the network, and other forms of communication and analytical equipment will need to be part of the system as technology advances. Paragraph 3 also requires that personnel participating as part of a Party's team for the network be properly trained regarding computer- or computer-related crime and how to respond to it effectively.

2 Set up, authority and procedures

2.1 Institutional set up of 24/7 points of contact

2.1.1 Institutional setting

In November 1997, the Ministers of Justice and Home Affairs of the G8 agreed on a set of principles to combat high-tech crime, which resulted in the creation of network of CP in March 1998 with the primary purpose of facilitating immediate action to have data preserved in another country. This network soon expanded to non-G8 countries and by 2008 comprises some 50 members. Following the opening for signature of the Budapest Convention on Cybercrime in 2001, parties to this treaty also began to establish CP.

The USA, France and Italy were among the first countries to designate such points of contact already in 1997/1998. In Europe, the most recent additions include Armenia (August 2008) and Bosnia and Herzegovina (July 2008).

From the 14 countries that responded to the questionnaire in October 2008, twelve are police-type bodies and are hierarchically under the Ministry of Interior, the criminal police or the national police. In the USA the CP is a prosecution service under the Department of Justice. Romania has two CP, one prosecution service within the High Court of Cassation and Justice, that is, the prosecutor general's office which has been formally created by law, and a second one within the criminal police. The CP of Norway is a hybrid type in that it is a criminal police body with judicial, prosecutorial functions.

The global picture reflects a similar split: 53 CP are police bodies, six are prosecution services, and two are hybrids:

- Police type points are found in: Albania, Armenia, Australia, Austria, Belgium, Bosnia and Herzegovina, Brazil, Bulgaria, Canada, Chile, Cyprus, Czech Republic, Denmark, Dominican Republic, Estonia, Finland, France, Germany, Hong Kong, Hungary, Iceland, India, Indonesia, Israel, Italy, Jamaica, Japan, Liechtenstein, Lithuania, Luxembourg, Malaysia, Malta, Mauritius, Mexico, Morocco, Namibia, Netherlands, New Zealand, Pakistan, Peru, Philippines, Portugal, Romania, Russian Federation, Serbia, Singapore, Slovakia, Slovenia, Spain, Sweden, Taiwan/Chinese Taipeh, Thailand, Tunisia, United Kingdom

- Prosecution-type CP have been established in: the Republic of Congo, Korea, Romania, South Africa, "the former Yugoslav Republic of Macedonia", and the USA

- CP combining police and prosecutorial functions are found in: Nigeria and Norway.

The following strengths and weakness have been raised during the Ohrid workshop, in the replies to the questionnaire and other discussions:

- Police or prosecution: arguments in favour of police bodies are that they usually have more staff, resources, infrastructure, skills and specialised training. On the other hand, prosecution services may have a stronger capability to follow up through judicial cooperation or execute requests for mutual legal assistance themselves. In the USA, the Computer Crime and Intellectual Property Section (CCIPS) of the Department of Justice is a prosecutorial service. It is a separate office from the Interpol central authority and also from the Criminal Division of the Office of International Affairs that is responsible for mutual legal assistance. All these offices are within the Department of Justice which should facilitate coordination. Armenia and Bosnia and Herzegovina have declared that their newly established police-type CP will also be responsible for mutual legal assistance and extradition. It is unusual to combine all of these powers in one body.

- Police CP with prosecutorial powers: The Norwegian approach of a body with police and prosecutorial powers seems to be a most efficient solution as it combines the advantages of both types, including resources and specialisation and the issuing and execution of requests for legal assistance. However, in other countries such an approach may not be compatible with the criminal justice system. The High-tech Crime Division of the KRIPOS National Criminal Investigation Service of Norway has law enforcement and judicial functions and is not only the CP for G8 and Council of Europe purposes but also the National Office Interpol. This certainly helps prevent coordination problems.

- A police as well as a prosecution CP within one country: Romania has one prosecution and one police CP. This seems to function in a very efficient manner.[4] In Albania, the CP is currently in the police, but thought is given to follow the Romanian approach of having a second CP established within the Office of the Prosecutor General. It seems that this can work very well in some countries and facilitate the cooperation between the police and prosecution service: the police can make use of their own channels and instruments, while the prosecutor can order preservation and is competent for mutual legal assistance. On other hand, this could lead to overlapping requests, conflicts of competence, a proliferation of CP and may be confusing for other parties. Close cooperation between the two (or more) CP is thus required.

- Neither police nor prosecution body: In some countries the question has been raised whether CP should not be located within an intelligence service or a telecom regulatory body or a CERT or another body. However, this seems to be discouraged as a CP is expected to take measures that only a police or prosecution service is authorised to do. Moreover, a police or prosecution service of one country may find it difficult to engage in full cooperation with a different type of body of another country.

- Forensic services: In a few countries, the CP is managed by a cyber-forensic service (such as in Brazil and Namibia). This may have the advantage of highly specialised subject-matter expertise, but also means that the CP is somewhat removed from police operations and thus not necessarily able to initiate immediate action.

- National Interpol office as CP: In some countries the CP is also servicing Interpol or other international networks such as Europol or SIRENE. This is for example the case in Estonia, Finland, Iceland, Netherlands and Norway. This seems to have the advantage of avoiding a proliferation of CP for different purposes, of facilitating coordination and of specialisation in international cooperation matters. But this may also mean a lack of specialisation in cybercrime or high-tech crime matters. It appears that in Italy efforts are currently underway to consolidate the different CP within one agency. In Hungary and Slovakia this problem is resolved in that the Interpol bureau refers an incoming request to the specialised high-tech department of the police.

In conclusion, any of the options is feasible in principle as long as it is a police or prosecution body or a combination.

One important problem experienced in many countries, is that the functions, and sometimes the existence, of **the CP are not known to relevant national authorities**. In one case, the body itself was not aware that it had been declared to be the CP when the country ratified the Convention on Cybercrime.

[4] Examples in this report related to Romania refer to the prosecution CP.

Examples based on the replies to the questionnaire:

	Name	**Year establ.**	**Hierarchically attached to**	**Type of CP**
Armenia	The division of struggle against cyber crimes of the General Department of struggle against organised crime of the Police	August 2008	Police of Armenia	Criminal police
Bosnia and Herzegovina	State Investigation and Protection Agency – SIPA	July 2008	Ministry of Security of Bosnia and Herzegovina.	Criminal police
Bulgaria	Cyber crime Unit Directorate Counter Organized and Serious Crime	2007	Ministry of Interior	Criminal police
Denmark	National High Tech Crime Centre NCB Copenhagen	2002	National Police	Criminal police
France	Office Centrale de Lutte contre la Cybercriminalité (O.C.LC.T.I.C)	1997	Ministry of Interior	Judicial police
Hungary	Response and international Telecommunication Division "NEBEK NIO" National Bureau of Investigation"	2004	International Law Enforcement Cooperation Centre of Hungarian National Police HQ	Criminal police
Italy	Postal and Communication Police Service	1998	Italian National Police	Criminal police
Lithuania	Cyber Crime Unit, Crime investigation Board 2 Communication Centre of the National Unit, SIRENE	2006	Lithuanian Criminal Police Bureau	Criminal Police
Netherlands	National High Tech Crime Unit (KLPD)	2007	National Police Agency (KLPD)	Criminal police
Norway	KRIPOS National Criminal Investigation Service (NCIS Norway) High Tech Crime Division	2002	Part of the National Criminal Investi-gation Service and reports to the Police Directorate	Criminal police with judicial functions
Romania	Service for combating Cyber Criminality Directorate for Investigating Organized Crime and Terrorism Offences	2004	High Court of Cassation and Justice	Prosecution
Slovenia	International Police Division			Police
Spain	Computer Crime Unit	2006	Central Operational Unit of the Guardia Civil	Police
USA	Computer Crime and Intellectual Property Section CCIPS	1998	United States Department of Justice	Prosecution

2.1.2 Resources

Article 35 (3) of the Convention on Cybercrime stipulates that:

> 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Replies to the question as to the resources available, not only show a great variations but also two different types of concepts:

- In some countries, a CP is understood as one to three specific individuals (for example in Bulgaria, Republic of Congo, Croatia, Italy, the prosecution CP of Romania, Spain or "the former Yugoslav Republic of Macedonia")
- In other countries, an office is indicated comprising a much larger number of officers, such as in France (55), Hungary (11), Netherlands (30), Norway (40) or the USA (40).

The first option has the advantage that the persons responsible are clearly identifiable, thus facilitating personal contacts, networking and mutual trust. The downside is that cooperation is less institutionalised and may evaporate if the individual is reassigned to other duties or otherwise becomes unavailable. In some instances CP are hardly contactable as they are very busy with many other tasks.

The second option is less personalised but more institutionalised and having much more staff. Where such offices are high-tech crime units or similar, they can have a high level of specialisation and training, they are more likely to be in a position to have an officer on duty at any time, and they may also have a broader level of language skills. They also risk being more anonymous and less approachable and open for networking.

The G8/Council of Europe directory of CP shows that even where an office on the whole represents the CP, the name of one or several individual may be indicated who can be contacted directly. Countries that only indicate anonymous institutions and not individual persons appear to be much less involved in the network.

Replies to the questionnaire and discussions thus suggest that the most effective, resourced and sustainable option is to have as the CP an office or service specialised in high-tech crime cases within which a few individuals are identified by name.

Information received does not point at particular problem regarding equipment. It seems that the functions of a CP do not require particular investments in infrastructure other than email, fax, telephone, mobile phone, blackberry or similar devices. Some CP have a secure communication system available but do not necessarily use it in this context. A secure system for communication and experience exchange among members of the network may nevertheless help make the network more efficient and involve new members.

Most contact points seem to have found ways to be available 24/7.

One concern raised, however, is that in a number of cases web-based personal email accounts are used. This raises concern including one of security, confidentiality and reliability. Tests have shown that **the email details provided by a number of CP listed in the directory are not correct** and mails bounce back.

It would seem that the most appropriate solution is to **provide a non-personalised institutional office email address as well as a personal institutional email address**.

It is essential, that the contact details of CP are accurate and kept up to date.

Examples based on the replies to the questionnaire:

	Number of staff	**Qualifications**
Armenia	1 (5 planned)	
Bulgaria	2 persons working at the CP	Substantial professional experience in the field of cybercrimes Languages: English, Russian, French Spanish, Portuguese Outstanding participation in plenty of domestic and international trainings, working groups, conferences.
Denmark	2 persons	Languages: English and German Cyber crime investigation training
France	55 persons	Qualified in cybercrime, computer forensic, network, programming. Legal trainings and forensics. National and international judicial and legal ability. Languages: English, Spanish, Romanian, German
Hungary	NINI CSBEO : 11 NEBEK NIO : 11	Languages: English, German Law and police
Italy	2 officers	Long experienced High Tech Crime Investigators Participation in G8 activity and 24/7 Network development
Lithuania	8 persons	Cybercrime investigations Trainings for law enforcement officers investigating in cyber crimes
Netherlands	30 persons	• 24/7 availability • Investigations dedicated to High Tech Crime • Combination of digital and regular investigators • Direct contact with national prosecutor on High Tech Crime • Own research and development available • Own knowledge and expertise desk • Wide international network • Fast response
Norway	40 persons working in the High Tech Crime Division	Highly qualified in cybercrime, computer forensics and international cooperation Languages: Norwegian and English
Romania	5 prosecutors	Prosecutors are specialized and experienced Languages : Romanian, French, Spanish and English
Spain	3 people	
USA	40 attorneys	Combating cybercrime and theft of intellectual property Trainings on the functioning of the 24/7 network and the international cooperation provisions of the Convention. Languages : English

Examples based on the replies to the questionnaire:

CP	Office hours	Arrangements after office hours
Bulgaria	8h20 – 17h30 Monday to Friday	Contact via mail and mobile phones at any time
Denmark	8h– 16h Monday to Friday	NCB Copenhagen mail connection
France	9h – 19h Monday to Friday	Etat major
Hungary	7h30 – 16H Monday to Thursday 07h30 – 13h30 Friday	NEBEK 24/7 duty service
Italy	8h – 18h Monday to Friday	Officers use a smart phone and/or a laptop computer equipped to connect to the internet via a HSPDA/UMTS connection (broad band mobile communication)
Lithuania	24 hours and 7days a week	
Netherlands	7h – 18h Monday to Friday	On call 24/7
Norway	0800 – 1600 Monday thru Friday	Calls will be received at NCIS 24/7 Desk who will contact personnel from the High Tech Crime Department
Romania	8h – 16h Monday to Friday	The chief prosecutor may be reached at any time by mail
Spain	8h – 20h Monday to Friday	Email requests are received at any time of the day
USA	09h00 – 18h Monday to Friday	An attorney on duty can be reached at any time

2.2 Responsibility and authority of the contact point

2.2.1 Legal basis of the contact point

Article 35 of the Convention on Cybercrime states that a CP should be able to ensure

1 …. 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.

The question has been raised whether this implies that a CP requires a specific legal basis or whether these powers are covered by existing regulations.

In Romania, for example, Article 62 of Law 161/2003 designates the Service for combating cybercrime within the Prosecutor's Office as the CP:

> Art. 62 –
> (1) In order to ensure an immediate and permanent international cooperation in the cybercrime area, within the Organised Crime Fighting and Anti-drug Section of the Prosecutor's Office belonging to the Supreme Court, a service for combating cybercrime is established as a contact point permanently available.
> (2) The Service for combating cybercrime has the following attributions:
> a) provides specialised assistance and information on Romanian legislation in the area to similar contact points in other states;
> b) orders 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;
> c) executes or facilitates the execution, according to the law, of letters rogatory in cases of combating cybercrime cooperating with all the competent Romanian authorities. [5]

Information received suggests that if the 24/7 CP functions are entrusted to an existing body with the authority to investigate or prosecute cybercrime and to engage in international law enforcement cooperation no separate legal basis is required.

This seems to be the case in most countries. The law on the ratification of the Convention on Cybercrime and the declarations made with regard to Article 35 may also serve as a legal basis.

On other hand, a specific legal basis would perhaps "responsibilise" CP, make them accountable for results achieved, make them known and facilitate cooperation with authorities at the national level, and give them powers for preservation and possibly MLA.

[5] Following the reorganisation of the Prosecutor's Office, the CP is now within the Directorate for Investigation of the Organized Crime and Terrorism Offences (Law no. 508/2004 on establishing, organising and operating of the Directorate for Investigation of the Organized Crime and Terrorism Offences (amended by Emergency Ordinance of Government no. 131/2006)).

Examples based on the replies to the questionnaire:

CP	Legal basis
Bulgaria	Ministry of Interior Act is the main legal document. The functions of the CP are set in accordance to the Convention on Cybercrime and the responding Protocols. No need to define the mandate of the CP.
Denmark	Part of the National Police with its term and laws.
France	Decree N°2000-405 creating the Office Centrale de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication.
Hungary	Act LIV of 1999 (NEBEK act), Act LXXIX of 2004 (Convention on Cybercrime) 4/2002 BM-PM Ministerial Decree
Italy	CP has been established in accordance to the Convention on Cyber crime Law nr.48 of 18 March 2008.
Netherlands	National Prosecutor is in the lead of investigations
Norway	Part of KRIPOS (NCIS) mandate
Romania	Service for combating Cybercrime has been established in 2003 according to the Law no. 161/2003, article 62
Spain	Law enforcement agencies are allowed to request for personal data involved in a current investigation. There are some specific laws that shelter police to ask for these requests. Police forces can obtain personal data from Spanish Data Protection Agency.
USA	CCIPS is the prosecutorial authority with the Department of Justice that, working with investigative agencies, prevents, investigates and prosecutes computer crimes and intellectual property theft. CCIPS, with other components of the Department of Justice is able to issue or seek any type of legal process that may be relevant to a 24/7 request.

2.2.2 Authority of the contact points in terms of article 35 of the Convention on Cybercrime

As indicated above, according to Article 35 of the Convention on Cybercrime a CP should have the authority to directly or in coordination with another authority provide the following immediate assistance in an expedited manner:

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.

The CP should also have:

… the capacity to carry out communications with the CP of another Party on an expedited basis.

Obviously, the network can function more efficiently if a CP can carry out these measures directly rather than requesting another body to take action or requiring approval from another body.

It would seem that the "provision of technical advice" and the "capacity to communicate with the CP of another Party on an expedited basis" are within the direct authority of most CP and do not pose difficulties.

The same applies to "the provision of legal information", that is, for example advice on legal prerequisites required for providing informal or formal cooperation.

The "location of suspects" can be carried out by the CP directly or through other bodies. It seems that in many countries a formal request from the foreign CP or competent authority is required

before this measure can be initiated. The same is true for the collection of evidence which in addition may also require authorization by a prosecutor or judge.

The most important function of a CP is to order the expedited preservation of data at the request of a foreign CP. Obviously, this measure must be possible under national procedural law. **A country that does not have the possibility for "the expedited preservation of stored computer data" in line with Article 16 of the Convention on Cybercrime and the "expedited preservation and partial disclosure of traffic data" (Article 17) will have great difficulties to participate effectively in the network of 24/7 points of contact.**

CP of countries that have fully implemented the Convention are thus able to directly order the expedited preservation of stored computer data and the expedited disclosure of preserved traffic data in the context of international cooperation according to articles 29 and 30 of this treaty.

However, available information suggests that at least in some countries **a simple email or telephone call is not sufficient to take this measure, but that a CP requires a more formal request with relevant information from a foreign CP that can also stand up to the scrutiny of a prosecutor or possibly a judge.**

The procedure for expedited preservation requests and the format used for such requests will therefore be elaborated on in more detail below.

Examples based on the replies to the questionnaire:

	Does the CP have the authority to directly carry out the following (if not, which institution can be requested to carry out the measure):					
CP	Provide techn. advice	Order preser-vation	Collect evidence (following a MLA request and judicial authorisation)	Provide legal advice and share information	Locate suspects	Communicat e directly with foreign CP
Bulgaria	Y	Y	Y	N	Y	Y
Denmark	Y	Y	Y	Y	Y	Y
France	Y	Y	Y	Y	Y, if an official request is sent	Y
Hungary	Y	Y	Y	Y	Y	Y
Italy	Y	Y	Y	Y	Y	Y
Lithuania	Y	Y	Y	Y	Y	Y
Netherlands	Y	Y	Y	Y	Y	Y
Norway	Y	Y	Y	Y	Y	Y
Romania	Y	Y	Y	Y	Y	Y
Spain	Y	Y	Y	Y	Y	Y
USA	Y	Y, where appro-priate	Y, working with investigative authorities	Y	In appropriate circumstances CCIPS can assist foreign law enforce-ment to coordinate with US law en-forcement in locating suspects)	Y

2.3 Ability to carry out preservation and mutual legal assistance requests

2.3.1 Preservation requests

Electronic evidence is highly volatile. Thus, the possibility to have computer data, in particular traffic data, preserved in another country in an expedited manner is one of the most important tools in the international cooperation against cybercrime. The relevant provisions of the Convention on Cybercrime are articles 29 and 30 which are reproduced here for ease of reference:

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.

"Expedited preservation" is a provisional measure through which not only an Internet service provider but any legal or physical person can be ordered to preserve specified stored computer data which are in his possession or under his control.[6] This does not yet mean that the data is handed over or disclosed to the law enforcement authority (with the exception of data as defined in article 30 (1)). That would be a second set and be subject to a production order or similar.

In some countries, a CP can order an ISP or a person to preserve data directly and without seeking judicial permission, in particular but not only where the CP is a prosecutor. This is the case for example in Bulgaria, Denmark, France, Norway, Spain or the USA. In Romania, this is also true for the CP at the prosecution service while the police CP is required to seek the approval of the prosecution CP.

In a number of other countries, however, even such a provisional measure requires approval by a superior judicial authority (prosecutor or judge), such as in Italy, the Netherlands and now also in Germany.

For the actual collection of preserved data by a CP or law enforcement and for the actual disclosure of such data to the foreign CP in almost all cases a formal request in the form of an international rogatory letter is required.

Discussions and replies to the questionnaire show that while the expedited preservation measure under Article 29 is used often, there is very little experience with the expedited disclosure of preserved traffic data provision.

It also appears that **more than half of the countries that are listed in the directory of CP, do not yet have provisions in their national legislation for the expedited preservation of data. They are therefore not in a position to cooperate with the CP of other countries with regard to the type of expedited preservation measures as defined in articles 29 and 30. This is also true for some countries – in particular in South-eastern Europe – that have ratified the Convention on Cybercrime.**

[6] Preservation is about specified data and not to be confused with the concept of data retention regulations under which an ISP is required to retain all traffic data and subscriber information for a certain period of time.

Examples based on the replies to the questionnaire:

	Expedited preservation of stored computer data (art 29)	**Expedited disclosure of preserved traffic data (art 30)**
Bulgaria	Send official requests to ISPs hosting companies etc. According to the Ministry of Interior Act all the state bodies and private entities are obliged to provide us with the required information.	
Denmark	Contact to ISP or person directly to preserve the data	
France	We can send a simple email to providers (or other companies who store computer data).	
Hungary	Request sent to providers (ISP)	Request sent to providers (ISP)
Italy	A judicial preservation order is requested to competent judicial authority	A disclosure authorisation is requested to judicial authorities
Lithuania	No requests so far	No requests so far
Netherlands	Contact national prosecutor, ask for permission, and carry out request within a few hours	Wait for formal request for legal assistance, approved by our national prosecutor. Carry out request within a few hours after receiving formal request
Norway	We direct the preservation order to the relevant party	We direct the preservation order to the relevant party and ask for disclosure of traffic data
Romania	Verifies the origin of the request and compliance with the Romanian law registers and issues the order according with article 54 Law no.161/2003	
Spain	Directly request the server administration to make the preservation and send a copy of the data	

2.3.2 Mutual legal assistance

The network of 24/7 points of contact is conceived to provide assistance in very urgent matters, and the expedited preservation of data is clearly the primary measure. However, immediate assistance may also comprise a range of other measures, including cases of mutual legal assistance. In most countries other authorities are competent for MLA, but CP may nevertheless play a facilitating role.[7] According to Article 35, CP shall:

> 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.

Relevant provisions in the Convention that may require immediate, expedited assistance include articles 31, 33 and 34:

> Article 31 – Mutual assistance regarding accessing of stored computer data

[7] It should be noted that opinions on the role of CP regarding MLA are controversial. Some argue that CP are designed to handle very urgent requests only and to supplement and not to replace other channels, others favour a stronger involvement of CP in MLA.

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.

Information available suggests that a CP can only take such measures if a formal request for assistance is received from a competent foreign authority and if it is approved by a national judicial authority, in particular if it involves the interception of content data. This underlines the need for efficient cooperation between CP and competent authorities for mutual legal assistance.

A further problem in this context is the so far rather **limited number of countries that are full parties to the Convention on Cybercrime. Only ratification or actual accession will allow a country to make full use of this treaty for the purposes of mutual legal assistance. Once all countries that have already signed the Convention or been invited to accede actually become parties a critical mass of countries will be available to cooperate with each other**.

Examples based on the replies to the questionnaire:

	Mutual assistance regarding accessing of stored computer data (art 31)	**Mutual assistance in the real-time collection of traffic data (art 33)**	**Mutual assistance in the interception of content data (art 34)**
Bulgaria	The responsible state body in question is the Supreme Cassation Prosecution	The responsible state body in question is the Supreme Cassation Prosecution	The responsible state body in question is the Supreme Cassation Prosecution
Denmark	Contact host or person to preserve the data	Contact host or person to preserve the data	Contact host or person to preserve the data
France	An official international request is needed	An official international request is needed	An official international request is needed
Hungary	In line with criminal procedure involve the prosecutorial authorities	In line with criminal procedure involve the prosecutorial authorities	In line with criminal procedure involve the prosecutorial authorities
Italy	The judicial authorities are requested to authorise the measure	The judicial authorities are requested to authorise the interception	The judicial authorities are requested to authorise the interception
Netherlands	Wait for formal request for legal assistance, approved by our national prosecutor. Carry out request, possible within a few hours after receiving formal request	Wait for formal request for legal assistance, approved by our national prosecutor. Carry out request, possible within a few hours after receiving formal request	Contact national prosecutor, ask for permission, carry out request possible within a few hours after request
Norway	Based on a search warrant or a court order we would search and seize data	This requires a court order or a temporary order from the Chief of Police	This requires a court order or a temporary order from the Chief of Police
Romania	A rogatory letter is needed	A rogatory letter is needed	A rogatory letter is needed
Spain	Server administration is contacted and requested to hand in a copy of the data involved in the investigation, then this data can be sent to the corresponding Law enforcement agency to be analysed	The CP gets in touch with administration in order to obtain the data to be sent back to the applicant	The request is brought to court in order to obtain the formal orders that allow us the interception of the data

2.4 Format used for sending/receiving requests

While the preservation of data should take place in an expedited manner and should thus not be subject to too many formalities, a minimum of information is required in order to permit the CP receiving a request to act. Article 29 (expedited preservation of stored computer data) of the Convention lists what a request should contain:

> 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.

Information received and discussions show that some CP are rather pragmatic and do not use or require a particular format and may even be able to act upon a telephone call received from a foreign CP. Others do not use or require a particular format but a minimum set of information. And others finally use and require a formally signed and stamped document. This is particularly the case for many countries of central, eastern and south-eastern European countries and at the Ohrid workshop in November 2008 was underlined as a requirement by countries such as Bosnia and Herzegovina, Bulgaria, Croatia, Montenegro, or "the former Yugoslav Republic of Macedonia". It seems to be also a requirement in other European countries such as Norway and currently Germany. A formalized request is helpful or needed in cases where the CP requires the approval of a prosecutor or another authority before carrying out a particular measure.

Email, scanned documents or fax are means of transmission accepted by most CP as long it can be verified that the sender is genuine. In this context the use of institutional email accounts is encouraged.

These non-formalised approaches are pragmatic, non-bureaucratic and can be efficient on the one hand. But they may also delay the execution of a request if the format and contents do not meet the needs of the receiving CP.

This question was debated at the 3rd meeting of the Cybercrime Convention Committee (T-CY) in April 2008. The T-CY:

> 27. The T-CY took note of a proposal by Romania concerning the preparation by the T-CY of a checklist for use between the 24/7 contact points for requests for expedited preservation of computer data and requested the Project on cybercrime to present a draft for consideration by the T-CY at its next meeting.

The preparation of a "checklist" rather than a "common form" was a compromise between the need to harmonise requests and the risk of over-formalisation.

In their replies to the questionnaire, CP sent their checklists of what they would like to see in a request. That information as well as the "Checklist for Use of the G8 24/7 Network" served as basis for discussion at the Ohrid workshop, where a checklist was proposed for submission to the Cybercrime Convention Committee (T-CY) (see appendix).

Examples based on the replies to the questionnaire:

CP	Format used for sending requests	Information required from requesting authority
Bulgaria	Scanned copy of an official letter authorized by the Director; in urgency matters, we sent emails	Depends on the current case, e.g. if it refers to internet sites containing child abuse images we need IP logs from the administrative access to the site.
Denmark	Word document	Short description and what is requested.
France	Email, open document (.odt), txt	A mutual legal assistance request for data identification but not for preservation
Hungary	Jpg, doc, tif, txt, htm, pdf	Name of the authority, reference number, type if offensive, shortly facts of case, request… (what any other legal act additionally orders)
Italy	Fax or email	Detailed description of the conduct (considered to be a crime in the requested country): Exact date and time when the crime as occurred (possibly in Universal Standard Time); Details of the victim (name, location); entity of the damage/loss. IPO Address or other technical means Identification of involved hardware/network host (telephone or computer).
Lithuania	Fax, email	Depends on cases, but preferable to receive as much information as possible about the specific Telecommunication incident as possible.
Netherlands	Not specified	Formal request signed by prosecutor of the requesting country containing the requests referring to the Convention and offences committed.
Norway	Letter with official letterhead, signature, and official stamp. The letter would be faxed or sent by e-mail	Letter with official letterhead and signature sent from the CP
Romania	Mail/fax	Preservation letters: Name of the requesting authority and case number; Brief presentation of facts that are subject to the criminal investigation and their legal background; Computer data required to be preserved; Any available information, necessary for the identification of the owner of the computer data and the location of the computer system; The intention of the foreign authority to formulate a request of international legal assistance
Spain	Mail, no specified format	Description of the facts. Detailed list of data requested. Clear information about what must be done with the data
USA	Pragmatic. Most useful format	Depends on type of action sought. Ask information regarding the nature of the emergency including details with respect to the source of the activity, the victim and related technical information, the assistance requested and contact details for where to direct the response.

3 Experience

3.1 Requests sent and received

3.1.1 Types of request

In terms of types of request sent and received through the network, as expected most seem to be related to the expedited preservation of stored computer data (Article 29), although some also send and receive MLA requests.

Probably the most often sought and needed urgent information is related to the identification of suspects, that is, linking an IP or email address to a person or location. It could perhaps be argued that providing such information is in the spirit of the Convention ("cooperate with each other to the widest extent possible") and listed in the tasks of CP ("location of suspects"). Such information, however, is protected by national regulations and a CP may be able to provide such information informally on rare occasions only. Usually, a formal request for MLA under article 31 is required.[8]

The CP of some countries (Netherlands, Norway and Spain) also use the network for the expedited disclosure of preserved traffic data (Article 30) and mutual legal assistance to access stored computer data (Article 31).

Examples based on the replies to the questionnaire:

CP	Types of request sent	Types of request received
Bulgaria	Expedited preservation of stored computer data (art 29)	Expedited preservation of stored computer data (art 29)
France	Identification of IP addresses and data preservation.	Identification of IP addresses and data preservation.
Italy	Expedited preservation of stored computer data (art 29) Request for identification of suspects	Expedited preservation of stored computer data (art 29) Request for identification of suspects
Lithuania	Expedited preservation of stored computer data (art 29)	Expedited preservation of stored computer data (art 29)
Netherlands	MLA regarding accessing stored computer data (art 31)	MLA regarding accessing stored computer data (art 31)
Norway	Expedited disclosure of preserved traffic data (art 30) MLA regarding accessing stored computer data (art 31)	Expedited disclosure of preserved traffic data (art 30) MLA regarding accessing stored computer data (art 31)
Romania	Preservation letters (art 29)	Preservation letters (art 29)
Spain	Expedited disclosure of preserved traffic data (art 30)	Expedited preservation of stored computer data (art 29), Expedited disclosure of preserved traffic data (art 30), MLA regarding accessing stored computer data (art 31), Mutual assistance in the real-time collection of traffic data (art 33), Legal assistance, Incident response
USA	Expedited preservation of stored computer data (art 29)	

[8] The question the extent to which subscriber information is or should be covered by privacy rules and whether a type of regulation on the "expedited disclosure of subscriber information" is conceivable may be further discussed.

3.1.2 Numbers of requests sent and received

According to information received from 14 CP that responded to the questionnaire or participated in the Ohrid workshop, some 540 requests were sent and some 480 were received in total in 2007 and the first ten months of 2008.

The USA was certainly the most active CP and contributed more than 80% of all requests sent and more than 50% of requests received. This is not surprising, given the large amount of internet traffic involving the USA in one way or the other. The network is thus very much used and an efficient mechanism for the cooperation of the USA with other countries and vice versa. In Europe, in terms of numbers, Bulgaria and the Netherlands appear to be the most active ones.

The number of requests sent and received by most CP is rather modest and is less than ten per year, even among active members of the network such as France, Italy, Romania or Spain.

A number of CP of countries that have ratified the Convention on Cybercrime have not yet sent or received a single request, such as Albania, Armenia, Bosnia and Herzegovina[9], Slovenia or "the former Yugoslav Republic of Macedonia".

These data may be incomplete and to some extent misleading. A single request may trigger a series of other measures, cases and requests for MLA which are dealt with by other agencies. They do not comprise requests for advice and informal exchanges.

It should also be pointed out that the network should primarily be used for urgent assistance. And the network is not conceived to be the exclusive channel of cooperation, but indeed to supplement other channels. Representatives of Romania mentioned the "1000+100+10" formula: The police exchange information with counterparts in other countries in about 1,000 thousand instances per year. Some 100 formal requests for mutual legal assistance in cybercrime cases are dealt with by the Ministry of Justice or the Office of the Prosecutor General per year. And about ten requests are urgent and are handled by the prosecution CP. Similarly in France where some ten requests per year are handled through the CP and more than 220 cybercrime-related requests through the Interpol National Reference Point.

In terms of numbers it therefore seems that the network of 24/7 CP is used in exceptional, particularly urgent cases only (such as those under articles 29 and 30 of the Convention). The majority of cases are probably considered less urgent and other channels seem to be used.

[9] The CP for Armenia and Bosnia and Herzegovina were only established in the second half of 2008.

Examples based on the replies to the questionnaire:

Number of requests sent and received in 2007 and 2008 (as at October)								
CP	Total sent	Pre-serv-ation (art 29 + 30)	MLA (art 31+ 33+ 34)	To	Total re-ceived	Pre-serv-ation (art 29 + 30)	MLA (art 31+ 33+ 34)	From
Albania	0				0			
Armenia	0				0			
Bosnia and Herzegovina	0				0			
Bulgaria	34	34		USA,Spain, France, UK, Russia, Denmark, Canada, South Africa, Lithuania, The Netherlands	18	18		Romania, UK, USA, Russia, Mexico, Latvia
France	3			Ukraine, Bulgaria	8			UK, Ukraine, Bulgaria, Nigeria, Lithuania
Italy	13 (request for iden-tification of sus-pects) +4=13	4		USA, Germany	8 (request for identific ation suspects)+3=8	3		Russia, USA
Lithuania	6			Hong Kong, UK, USA				
Netherlands	13	0	13	USA, Russia, UK, Germany	31	0	31	USA, Russia, UK, Germany, Australia
Norway	12	8	4	USA	0			
Romania	3			USA	15	13	2	USA
Slovenia	0				0			
Spain	4	4		Italy, Netherlands, Germany, Taiwan	11	4	7	UK, USA, Bulgaria, Chile, Hong Kong
"the former Yugoslav Republic of Macedonia"	0				0			
USA	Ca 450			Germany + many others	Ca 250			Germany + many others
Total	Ca 540				Ca 480			

3.2 Timeliness of requests and responses

In principle, CP are in a position to respond to urgent requests in an expedited manner and within a reasonably short time. Some CP state as a problem that they do not receive answers on time or that the receipt of a request sent by email is not confirmed. Overall, the response time seems to be acceptable with regard to urgent provisional measures such as data preservation. Of course, the response time depends on the level of cooperation with internet service providers.

Delays and difficulties are more often encountered with regard to the follow up through formal mutual legal assistance or urgent measures that require a formal request from a foreign country. This will be discussed below.

Examples based on the replies to the questionnaire:

CP	Time needed to receive answers to requests	Time needed to respond to requests
Bulgaria	High priority: four days	Few days, when it's a matter of national security or serious crime, capable to react within a 24 h
Denmark	Depends on request, 1or 2 weeks	Depends on request, 1or 2 weeks
France	Few hours to few days	Few hours to few days
Hungary	10 minutes (personal data or criminal records) to 2 month (verifying offenders/hardware, IP address	10 minutes (personal dates or criminal records) to 1or 2 days if answerable. 1-2 days to 2 month if forwarded
Italy	Few days to a month	From a few days to a few weeks. If a case is particularly urgent the request might be handled within the same day of the request
Nether-lands	Depends on emergency, few hours is possible	Depends on urgency, few hours is possible
Norway	Preservation of stored computer data – a few hours depending on time of day and the service provider Disclosure of preserved data – a few hours depending on time of day and the service provider Accessing stored data – a few days depending on the service provider	Preservation of stored computer data – 1-3 hours Disclosure of preserved data – 1-3 hours Accessing stored data – 1-3 days depending on various factors as the amount of data
Romania	At least 2 weeks for identification of IP address up to several months for other information such as the preservation letters followed by international judicial request	The preservation letter is executed as urgent as the information sent is verified. Normally, in the same day, the ordinance issued by the prosecutor is sent to the ISP. The ordinance is issued for 90 days. A normal identification of an IP address may take 2 weeks, as well as other information regarding subscriber information
Spain	15 days. If we are requesting data from a small ISP it can be done in one day or two maximum. Bank accounts information requires about a week. And just in case it can be provided, identifying IP users should take no more than 2 weeks	Depending on data requested, if we refer to information available to CP it can be doe in one day maximum. If the request involves other entities it depends on them, but normally, it can be fixed in less than a week. Obviously it also depends on the amount of the data requested
USA	It can be minutes to for an emergency request, or months for a complex request that requires formal legal processes	Depending on the urgency of the request, it may be handled immediately, or it may take several hours or even days, but the CP has someone available 24 hours a day, seven days a week. Every effort is made to notify the requestor when the request has been received

3.3 Follow up through judicial cooperation

3.3.1 The role of CP in the mutual legal assistance process

As indicated previously, the network is primarily used for provisional measures such as expedited preservation requests or the exchange of informal and spontaneous information. This is of crucial importance for an investigation.

In order to actually obtain the preserved data from a foreign ISP or to use information about the identity of a person linked to an IP address as evidence in criminal proceedings or to access stored computer data in another country or to have data collected or intercepted in another country formal mutual legal assistance procedures are required in almost all cases.

Most CP do not have the authority to request MLA of execute MLA requests themselves. Exceptions include Norway where the CP is the competent authority for MLA, and – according to declarations made when ratifying the Convention on Cybercrime – Armenia and Bosnia and Herzegovina – where police services are designated at CP, as well as competent authority for MLA and extradition.

Some CP can be involved in the process but under the authority of a judicial authority. They must therefore seek efficient coordination with the competent authority for MLA. And a few CP appear not to be involved in the MLA process at all. However, this seems not to be in line with the Convention. According to Article 35:

> 2 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.

Moreover, CP need to make sure that preservation requests are followed up to through a request for MLA:

> Article 29 – Expedited preservation of stored computer data
>
> 2 A request for preservation made under paragraph 1 shall specify:
> ….
> 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.

Information received suggests that CP can be involved in the execution of a request but are not necessarily involved ex officio.

The competent authorities for MLA, that is, the international cooperation services of the Ministries of Justice or the Prosecutors General often refer to requests to local or regional judges, prosecutors or police officers without knowledge or role of CP.

One challenge seems to be **to ensure that CP are able to coordinate with competent authorities for MLA in an efficient, "expedited" manner.**

Examples of "competent authorities" according to the replies to the questionnaire and declarations made when ratifying the Convention on Cybercrime:

	Competent authority for judicial cooperation (according to declarations made when ratifying	**Role of CP**

	the Convention)[10]	
Albania	Albania declares that the name and address of 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 is: Ministry of Justice, Bulevardi Zog. I., Tirana	
Armenia	In accordance with Article 24, paragraph 7, Article 27, paragraph 2, and Article 35, paragraph 1, of the Convention on Cybercrime, the Republic of Armenia designated as the national CP for cooperation in combating cybercrime, available on a twenty-four hour, seven-day-a-week basis: Main Department on Combat Against Organized Crime of the Police of the Republic of Armenia	According to this declaration the police CP is also responsible for MLA and extradition
Bosnia and Herzegovina	In accordance with Article 24, paragraph 7, Article 27, paragraph 2, and Article 35, paragraph 1, of the Convention on Cybercrime, Bosnia and Herzegovina designated as the competent authority for the purposes of the Convention : the State Investigation and Protection Agency of Bosnia and Herzegovina. The CP is Mr Jasmin GOGIC, Director of Sarajevo's regional office of the State Investigation and Protection Agency of Bosnia and Herzegovina	According to this declaration the police CP is also responsible for MLA and extradition
Bulgaria	The Republic of Bulgaria declares that it designates the following Central Authorities responsible for sending and answering requests for mutual assistance: - the Supreme Cassation Prosecutor's Office - in respect of requests for mutual assistance at the stage of pre-trial proceeding; - the Ministry of Justice - in respect of requests for mutual assistance at the stage of the trial	The CP has no authority to engage itself in judicial cooperation. In the everyday process the CP cooperates intensively with the Supreme Cassation Prosecution responsible for MLA
Denmark	The Government of the Kingdom of Denmark has designated the Ministry of Justice, Slotsholmsgade 10, DK-1216 Copenhagen K, Denmark, as competent authority	The CP can engage itself in judicial cooperation but with the help of local police
France	France declares that, even in cases of urgency : - requests for mutual assistance from the French judiciary authorities and directed to foreign judiciary authorities are transmitted through the Ministry of Justice (*Ministère de la Justice, 13, Place Vendôme, 75042 Paris Cedex 01*); - requests for mutual assistance from foreign judiciary authorities and directed to the French judiciary authorities are transmitted through diplomatic channel (*Ministère des Affaires étrangères, 37, Quai d'Orsay, 75700 Paris 07 SP*).	The CP is composed of judiciary police officers who can be mandate by a judge to execute a request. The unit in charge of the international request is in permanent contact with the judicial authorities.
Hungary	- The Republic of Hungary communicates that, regarding requests delivered before starting the	

[10] It should be noted that Article 27 refers to MLA in the absence of other applicable agreements. Cooperation on the basis of other bi- or multi-lateral agreements may indicate a different competent authority. For example, under other European treaties sometimes prosecution services are indicated as competent authority rather than ministries of justice during pre-trial proceedings.

	criminal procedure, the designated central authority is the Hungarian National Police International Implementing Co-operation Centre. - Regarding requests delivered after starting the criminal procedure, the designated central authority is the General Prosecutor's Office of the Republic of Hungary	
Italy	The Italian Republic declares that the Minister of Justice of the Italian Republic is designated as the competent authority	No involvement. The CP only replies to urgent request for preservation. The disclosure of this data are managed directly by the points of contact (upon a simple judicial authorization) upon request or through traditional mutual legal assistance channel if they have to used as evidence in court
Lithuania	The Ministry of Justice and the General Prosecutor's Office of the Republic of Lithuania are designated as central authorities to perform the functions mentioned in Article 27	The officers discharching the functions of the CP are at the same time criminal police officers who investigate cyber crimes, therefore they have the authority to engage themselves in the implementation of requests for legal assistance
Netherlands	The central authority designated by the Netherlands is *Landelijk Parket van het openbaar ministerie* (National office of the public prosecution service)	Yes. In cooperation with national prosecutor. Weekly meetings and daily phone call with national prosecutor
Norway	The Norwegian authority designated is the National Criminal Investigation Service (KRIPOS). Direct telephone number for 24/7 (The High Tech Crime Division)	The CP is the competent authority
Romania	Romania declares that the central authorities responsible for sending and answering requests for mutual assistance are : a) the Prosecutor's Office to the High Court of Cassation and Justice for the requests of judicial assistance formulated in pre-trial investigation (address: Blvd. Libertatii nr. 12-14, sector 5, Bucuresti); b) the Ministry of Justice for the requests of judicial assistance formulated during the trial or execution of punishment	Yes. By Law the Service for combating cyber criminality has attributions in this respect. Also the service cooperates closely with the specialized Office established within the DIOCT. Usually the CP asks a copy of the judicial request
USA	The Office of International Affairs, United States Department of Justice, Criminal Division, Washington, D.C., 20530, is designated as the central authority of the United States of America for mutual assistance under the Convention.	CCIPS refers judicial cooperation requests to the Office of International Affairs, but remains available for consultation in cases involving cybercrime, intellectual property or electronic evidence

3.3.2 Difficulties in judicial cooperation

As expected, the main problem is the **duration of the mutual legal assistance process**. It usually takes six months or more to receive a formal response to an MLA request. Considering that Article 16 (2) of the Convention asks countries to enact legislation for the preservation of specified data of up to 90 days (though with the possibility of extension) and that even countries with data retention regulations may require ISPs to keep data for six months only, this poses problems. Reasons include:

- Limitations regarding the **skills, knowledge and training of judges and to some extent prosecutors** appear to have a direct bearing and delay the mutual legal assistance process: they have difficulties understanding cybercrime matters and are thus reluctant to open a case or issue search warrants.
- Furthermore, **insufficient use is made of the possibility in international agreements for direct contacts between judicial authorities in urgent cases and efficient channels of communication** (such as Article 15 of the European Convention for Mutual Legal Assistance in Criminal Matters or Article 4 of the more recent 2nd Additional Protocol to this convention, ETS 182).
- The **involvement of CP in the process may often be too limited**. In fact, it appears that sometimes the competent authorities for MLA are not aware of the existence and role of CP.
- It is to be noted that **not all CP are sufficiently trained, resourced or available to assist competent authorities** and facilitate the process.
- Furthermore, the authorities for MLA of many countries receive a **large volume of requests** and it is not always possible to see why a request related to cybercrime should be given higher priority than other requests.

Another issue is that **preservation requests are not always followed up by MLA requests** at all or not within a reasonable timeframe.[11] This creates major concerns for the requested CP with regard to their interaction with ISPs and their readiness to cooperate in the future.

Examples based on discussions and replies to the questionnaire:

CP	**Which are the main difficulties/challenges regarding judicial cooperation against cybercrime?**
Albania	Skills, technology, lack of training
BiH	Direct cooperation with neighbouring countries on organised crime possible and with good experience
Croatia	Good direct cooperation with countries of the region. Also language no problem
France	The execution of the request takes too long including the time to receiving the original request of the mutual legal assistance. Lack of knowledge of different jurisdictions. Restrictions regarding cooperation with other countries
Germany	Lack of specialisation of prosecutors or judges re cybercrime: thus reluctant to issue search warrant
Italy	Slow process
Lithuania	Responses to requests for legal assistance are received not earlier than after half a year. If, together with these responses, the data on the connections/logins to the Internet is received, quite often there is no possibility to establish the logs of these IP addresses since currently the internet service providers in Lithuania store the data on the connections of their customers only 6 months.
Montenegro	Time is key problem. Have agreement with neighbouring countries for direct cooperation (for police cooperation Interpol works very well. Here CP should be in police directorate and

[11] Article 28 (7) states that: 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.

	use Interpol)
Netherlands	Problem of obtaining fast response
Romania	The period of time necessary to execute an international request, either as a requested country or as a requesting country. Time is the main problem when other countries execute rogatory letters. In Romania there is a central office for this; not in other countries. Judges don't understand. Need training in technologies and in international cooperation.
Spain	Delays in carrying all the necessary procedures to open a new investigation as a consequence of another country request. Need sufficient information for prosecutor or judges to sign investigations
USA	Slow process, hard to obtain data in time because formal judicial cooperation often requires multiple agencies. Huge volume of MLA requests. Judges and prosecutors now much more trained

3.3.3 Solutions proposed

In discussions and replies to the questionnaire a number of solutions were proposed. One proposal is to give CP the authority to take responsibility for mutual legal assistance during pre-trial proceedings, as is already the case in Norway and Romania (for the prosecution CP). In some countries such a role is legally not possible.[12]

Alternatively, CP could systematically receive copies of MLA requests and facilitate their execution. As a minimum, CP may need to become more proactive regarding MLA (eg "provide technical advice" so that judicial authorities make use of the possibility of direct contacts), make themselves and their roles known to competent authorities, and engage in a more frequent dialogue with them.

Examples based on discussions and replies to the questionnaire:

CP	**How could judicial cooperation be made more efficient? How could the 24/7 network be used to speed up judicial cooperation and MLA measures?**
Bulgaria	The establishments of practical ties between Cybercrime Section and the Judicial bodies would enhance the process of strengthening judicial cooperation.
Hungary	Modifying rules, for example, extending the authority of CP in the Convention on Cybercrime
Italy	The points of contact should be composed both by investigators and prosecutors to be able to take responsibility for MLA
Lithuania	Taking into account the fact that requests for legal assistance in Lithuania are sent to other countries through the General Prosecutor's office of the Republic of Lithuania, there's no possibility to speed up judicial cooperation and MLA measures
Netherlands	Secure online availability of CP, sharing best practices
Norway	The CP is responsible for MLA
Romania	In Romania, the CP has attribution in the international judicial cooperation and can be involved in executing any of such requests. The CP can use the network information to obtain information about the executing stage of a request or to intermediate where the law permits, communication between counterparts
Spain	Including prosecutors and judges in the CP of each country may allow CP to communicate directly between themselves in MLA
USA	The 24/7 Network can ensure the availability of data and assist with pinpointing the proper recipient of judicial cooperation or MLA measures-for example by determining which service provider hosts an account of interest and whether the account in fact contains any records. This makes drafting formal requests much easier and can speed up the formal cooperation process. If a matter is particularly urgent, these types of facts can be shared with our office of International Affairs to assist in expediting the formal request

[12] And some CP insist that the role of CP should remain limited to urgent measures only.

4 Overall assessment and recommendations

This report is based on information received from CP of a limited number of countries which are parties to the Convention on Cybercrime.[13] It should nevertheless stimulate further discussions and measures in view of making not only the network of 24/7 points of contact but international cooperation against cybercrime more effective and efficient.

In the understanding of the G8 High-tech Crime Subgroup, which established the network of CP in 1997, and the Convention on Cybercrime (article 35), the main purpose of the network is to facilitate immediate measures, in particular the expedited preservation of data (articles 29 and 30 of the Convention) but also other measures such as the collection of evidence. CP should furthermore coordinate with competent authorities for MLA in an expedited manner. The effectiveness of the network should be assessed against this purpose.

4.1 Lessons learnt and suggestions with regard to set up, authority and procedures

Institutional set up:

- A strength of the network is that it is not very formalised and that every country can designate a CP that best meets its purpose within its existing structure and within the broad parameters of Article 35
- All countries that have established CP either chose a police or a prosecution body or a combination, and any of these options is valid
- It seems that rather than relying on one or two individuals, the most effective, best resourced and most sustainable option is to have as the CP an office or service specialised in high-tech crime within which a few individuals are identified by name
- There is a risk of proliferation of contact points for different purposes (Interpol, Europol, SIRENE, G8, Council of Europe etc.) and possibly the need for consolidation or streamlining. One option is to use national Interpol offices as a gateway from where cybercrime cases are referred to high-tech crime units in an expeditious manner
- The functions of a CP do not require particular investments in infrastructure or technology. Web-based personal email accounts should be avoided and use be made of a combination of non-personalised institutional office email address as well as a personal institutional email address
- In order to facilitate reliable communication between CP, a secure web portal could be established dedicated to the exclusive use of CP for real time communication and exchange of experience
- A major problem is that in many countries CP are not known to their own authorities. They should thus make themselves and their role known to relevant institutions.

Responsibility and authority of the CP:

- Information received suggests that if the 24/7 CP functions are entrusted to an existing body with the authority to investigate or prosecute cybercrime and to engage in international law enforcement cooperation no separate legal basis is required. On other hand, a specific legal basis could "responsibilise" CP, make them accountable for results achieved, make them known and facilitate cooperation with authorities at the national level, and give them powers for preservation and possibly MLA
- It would seem that the "provision of technical advice" and the "capacity to communicate with the CP of another Party on an expedited basis" are within the direct authority of most CP and do not pose difficulties. The same applies to "the provision of legal information", that is, for example advice on legal prerequisites required for providing informal or formal cooperation

[13] A draft of this report was also presented and discussed at the G8 HTCSG meeting in Rome on 10 February 2009.

- The most important function of a CP is to order the expedited preservation of data at the request of a foreign CP. This measure must be possible under national procedural law. However, it appears that more than half of the countries that are listed in the directory of CP do not yet have provisions in their national legislation for the expedited preservation of data. They are therefore not in a position to cooperate with the CP of other countries with regard to the type of expedited preservation measures as defined in articles 29 and 30. This is also true for some countries – in particular in South-eastern Europe – that have ratified the Convention on Cybercrime. These countries will have great difficulties to participate effectively in the Network of 24/7 points of contact. Countries should thus put the necessary legislation in place
- For a CP to order expedited preservation measures in some countries less and in other countries more formalised requests are needed. Often a simple email or telephone call is not sufficient to take this measure, and a CP requires a more formal request with relevant information from a foreign CP that can also stand up to the scrutiny of a prosecutor or possibly a judge. The appendix to this report contains a checklist for the type of information required
- While most CP do not have the authority to send or execute requests for MLA directly, they can facilitate and expedite this process and participate in the execution of a request. In many countries their cooperation with the competent authorities for MLA is rather limited
- A further problem in this context is the so far rather limited number of countries that are full parties to the Convention on Cybercrime. Only ratification or actual accession will allow a country to make full use of this treaty for the purposes of mutual legal assistance. Once all countries that have already signed the Convention or been invited to accede actually become parties a critical mass of countries will be able to cooperate with each other.

4.2 Lessons learnt and suggestions with regard to types of request and numbers

- In terms of types of request sent and received through the network, as expected most seem to be related to the expedited preservation of stored computer data (Article 29)
- Probably the most often sought and needed urgent information is related to the identification of suspects, that is, linking an IP or email address to a person or location. The MLA process is this respect is hardly efficient and options for a more effective procedure ("expedited disclosure of subscriber information") may need to be further discussed
- In terms of timeliness of responses the system appears to function satisfactorily. However, CP should systematically confirm receipt of a request
- Countries may send and receive a large number of requests related to cybercrime through different channels. Only few of these appear to be considered particularly urgent, and for these the network of 24/7 CP is used. Some countries use it more, others less and some CP have yet so sent or receive a request
- The majority of cases seem to be considered less urgent and for these other channels appear to be used.

4.3 Lessons learnt and suggestions regarding mutual legal assistance

The mutual legal assistance process is believed to be not sufficiently efficient to permit effective measures against the transnational phenomenon of cybercrime. Unless sweeping solutions in terms of re-thinking the nature of international criminal matters in the times of "cloud-computing" are found, the following possibilities should be explored to accelerate the process:

- CP could systematically receive copies of MLA requests and facilitate their execution. As a minimum, CP may need to become more pro-active regarding MLA, make themselves and their roles known to competent authorities, and engage in a more frequent dialogue with them

- One option could be – if legally possible – that CP comprise prosecutors and police officers and thus themselves take responsibility for sending, receiving and executing MLA requests, at least for those of an urgent nature
- More use should be made of possibilities for direct contacts and efficient channels of communication that are already available in some international treaties
- Judges and prosecutors should be trained with regard to cybercrime and international cooperation matters
- CP should make sure that preservation requests are followed by MLA requests
- The Council of Europe should establish a separate directory of competent authorities for MLA and involve these authorities in its activities related to international cooperation against cybercrime.

4.4 Issues requiring further discussion

1. Restricted or broader role for CP

Should CP – in addition to handling urgent, exceptional cases – assume a broader role in the international cooperation against cybercrime? Article 35 of the Convention which asks CP to also facilitate the collection of evidence and MLA certainly provides an opening in this respect. It seems that it would be difficult to come to a common understanding on this question at this stage. For the time being it is therefore up to individual CP to define their role beyond expedited preservation measures. Experience and good practices in this respect may then inspire other CP.

2. Broadening ownership and decision making in the network

It would be important to identify ways to give all CP an opportunity to participate actively in the functioning of the network and take ownership. As at January 2009, from the more than 60 CP listed in the directory of contact points, only 26 are represented in the Cybercrime Convention Committee or the G8 HTCSG.

The training conferences of the G8 HTCSG or the workshops under the Council of Europe Project on Cybercrime provide only a partial solution as they are not designed for decision making.

The secure information system that is currently being developed by the Italian CP may help create a sense of community among members of the network.

3. Cooperation between the G8 High-tech Crime Subgroup and the Council of Europe

In order to make the network more effective in line with the suggestions made in this report the G8 HTCSG and the Council of Europe need to organise their cooperation.

The merger of the Directory of Contact Points is an important step. The chair of the G8 HTCSG and the Council of Europe should cooperate on a continued basis in the updating of the Directory.

The Cybercrime Convention Committee (T-CY) could consider inviting the G8 HTCSG as an observer to its meetings. The G8 HTCSG in turn should invite the Council of Europe as an observer to its meetings.

The Council of Europe and the G8 Sub-group should cooperate with each other in the organisation of training and other events related to 24/7 points of contact.

4.5 Recommendations

The drafters of the Convention on Cybercrime had in mind a critical role for the 24/7 network when it:

> "was agreed that establishment of this network is among the most important means provided by this Convention of ensuring that Parties can respond effectively to the law enforcement challenges posed by computer- or computer-related crime".[14]

Clearly, the expedited measures foreseen under articles 29 and 30 would not be workable without such a network. The proposals made in this report provide food for thought and should provoke actions to (a) make the network more effective with regard to these expedited, provisional measures, and (b) enhance the role of the network regarding international cooperation against cybercrime in general.

Key recommendations are:

1. Contact points should become more pro-active and in particular make themselves known. In support of this, the Council of Europe should publish a listing of basic information on contact points (without specific contact details)

2. The T-CY could request Parties to the Convention with less active CP to provide clarification on the functioning of their CP

3. The T-CY may consider the draft checklist for preservation requests and send it to CP and the G8 HTCSG for further comments[15]

4. Contact points should take on more responsibility for facilitating MLA. The Council of Europe could support this by establishing a directory of competent authorities and involve these in training and other activities related to international cooperation against cybercrime

5. Many countries still need to create the legal basis for expedited preservation measures in their national law (see articles 16, 17, 29 and 30 of the Convention). The T-CY could request Parties to the Convention on Cybercrime to provide clarifications in this respect

6. More countries need to become party to the Convention on Cybercrime

7. The Council of Europe and the G8 HTCSG should organise their cooperation and maintain a joint directory of CP. The T-CY may invite the G8 HTCSG to become an observer in the T-CY, and in turn the Council of Europe could become an observer in the G8 HTCSG

8. The T-CY should continue to review the effectiveness of the network of CP.

---

[14] Explanatory report to the Convention on Cybercrime.
[15] The HTCSG is planning a meeting of CP in autumn 2009 where the checklist could be further discussed and validated.

5 Appendix: Proposed checklist for requests for expedited preservation

In their replies to the questionnaire, CP sent their checklists of what they would like to see in a request. That information as well as the "Checklist for Use of the G8 24/7 Network" served as basis for discussion at the Ohrid workshop, where the following checklist was proposed for submission to the Cybercrime Convention Committee (T-CY):

Request for expedited preservation (to be attached to an email or fax as a "official" document with letter head)
1. Identification and contact information of the requesting 24/7 contact point: - Name of requesting individual, of requesting contact point - City and country - Telephone numbers - Fax number - E-mail address - Reference number of the sending contact point - Date of request
2. Responsible prosecution or law enforcement authority (on behalf of which the request is sent) - Name, contact details - case/file number
3. The offence and related facts - Criminal offence and related criminal law provisions (including seriousness and penalty provided for by law) - Summary description of the case (optionally also names of suspects, victim information, damage involved etc) - Related investigations and preservation requests
4. Purpose of the request (action and evidence requested) - Type of data required (subscriber information, traffic data, or content data) - Date and time of the communication(s): provide both local time and Coordinated Universal Time/UTC - IP address, subscriber and other specified data (eg physical address, type of service used, other email addresses used, mode of payment or similar) - Account information (such as usernames, screen names, aliases, or other subscriber information related to different types of accounts, such as email, instant messenger or other types of accounts) - Log files related to IP addresses or email or other types of accounts - Duration for preservation required
5. Follow up - Intention regarding mutual legal assistance request/letter rogatory - Partial disclosure of traffic data - Feedback on action taken and availability of data

Notes:
This checklist is non-binding and for written requests only. Initial contact may be established by phone to ensure that messages are read. Contact points should indicate whether they monitor their email addresses 24/7. Recipients should confirm receipt of request to requesting contact point.
For the meaning of "expedited preservation" and "partial disclosure" see articles 29 and 30 of the Convention on Cybercrime.