http://www.coe.int/tcj/

Strasbourg, 18 February 2009
[PC-OC Docs2009/(2009) 05 sum replies]

PC-OC (2009) 05

EUROPEAN COMMITTEE ON CRIME PROBLEMS
(CDPC)

Committee of Experts on the
Operation of European Conventions on Co-Operation in Criminal Matters
(PC-OC)

Summary of the replies to the questionnaire on Mutual Legal Assistance in Computer-Related Cases

Background information:

At its 2nd meeting (Strasbourg, 13-14 June 2007), the Cybercrime Convention Committee (T-CY) discussed difficulties relating to mutual legal assistance under the Convention on Cybercrime. The T-CY agreed that timeliness of co-operation between States Parties is a crucial factor for combating cybercrime successfully. Among other matters, it was stressed that the Convention is applicable to offences committed with terrorist intent and in this respect the short period for data retention creates serious practical problems for responsible authorities.

The T-CY noted that offenders use all possibilities of cyberspace and that cybercrime cases often involve more than two States, which makes work of law enforcement authorities more difficult as. It was emphasised that when investigating crimes committed through the Internet the traditional methods of mutual legal assistance, in particular the time limits, could not always serve the purpose of this Convention. In computer related crimes computer data, intended to be used as evidence, can be destroyed/lost instantly.

Following a request from T-CY for guidance concerning best practices for mutual legal assistance in computer-related cases (in particular in urgent cases), the CDPC instructed the PC-OC to provide the requested practical guidance as well as to consider questions relating to operational matters such as Article 32b of the Convention. This Article provides that:

> "A Party may, without the authorisation of another Party […] access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system."

The PC-OC adopted a questionnaire on this issue, which it addressed to all member and observer States of the Council of Europe.

21 member States have replied to the questionnaire, as well as Canada and Japan. These replies are set out in the document PC-OC (2008) 08 Rev, available on the PCOC website (www.coe.int/tcj).

The following is a summary of the replies to this questionnaire. The Appendix contains the chart of signatures and ratifications of the Convention on Cybercrime.

Question 1:

Please describe methods, means and tools used by your competent authorities for rendering mutual legal assistance to authorities of other States in urgent cases (the channels of communication, translation etc.). Please provide examples of good practices or any guidelines for an effective mutual legal assistance in urgent cases, in particular computer-related cases (cybercrime).

Not all responding States provided specific information about channels of communication which can be used for requesting legal assistance in computer-related cases. A number of States explicitly referred to the possibility for the competent authorities of the requesting State to transmit MLA requests directly to their counterparts in the requested State. This possibility is foreseen in the internal legislation of some States (for example, Bulgaria and the Czech Republic). 4 States[1] mentioned that direct contact between competent authorities are possible, provided that the contact details of the competent requested authority are available and that there is a relevant treaty basis (in particular, the Convention on Mutual Assistance in Criminal Matters between the member States of the EU or the 2nd Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters), as well as reciprocity. In Luxembourg, a direct request for legal assistance to judicial authorities, while not foreseen by internal legislation, is nonetheless admitted in practice, in particular where there is urgency.

Requests have to be submitted to a central authority in some member States[2]. Bosnia and Herzegovina stated that it submits its requests for mutual legal assistance through diplomatic channels. Japan requires the use of diplomatic channels where it is the requested country, except when there is a bilateral MLA treaty.

The majority of responding member States[3] stated that in urgent cases their competent authorities essentially use the police and judicial communication networks (such as INTERPOL, Europol, Eurojust, the European Judicial Network, or the PC-OC). 6 member States[4] referred to the 24/7 Network set up under Article 35 of the Convention on Cybercrime, whereas Latvia and Slovakia pointed to the I-24/7 Network of the INTERPOL. Japan made reference to the 24/7 network of contact points established on the basis of the G8 Action Plan to combat High-Tech Crime.

As regards means of communication, all member States who provided details about this aspect of co-operation, as well as Canada and Japan, stated that modern means of communication which leave a written record, such as fax and e-mail, are acceptable, at least in urgent cases.

The majority of responding States did not provide any information concerning linguistic requirements. Some States[5] require translation into their official language(s) or into English. Whereas Swedish legislation requires a request for legal assistance and enclosed documents to be translated into Swedish, Danish or Norwegian, the competent authority may waive this requirement. Japan also replied that, while it requires a Japanese translation along with the request, it accepts requests in English in urgent circumstances.

Germany and Lithuania were of the view that translation into a widely used and acceptable language in the requested State, even where it is not obligatory, speeded up execution. Poland stated that, in practice, urgent requests are transmitted between competent authorities with translation.

---

1 Poland, Slovakia, Slovenia, Sweden.

2 Bosnia and Herzegovina, Malta (the Attorney General's Office), Turkey (Ministry of Justice, General Directorate of International Law and Foreign Relations), Ukraine (Ministry of Justice for requests of courts, the General Prosecutor's Office for requests of pretrial bodies).

3 Armenia, Czech Republic, Finland, Greece, Hungary, Latvia, Lithuania, Malta, Poland, Portugal, Romania, Slovakia, Turkey, Ukraine.

4 Armenia, Finland, Hungary, Latvia, Lithuania, Romania.

5 Bulgaria (either of the official languages of the Council of Europe), Finland (requests in other languages acceptable, but cause delays), Luxembourg, Switzerland.

As regards examples of other good practices or guidelines concerning urgent computer-related cases, most responding States did not provide particular comments. Armenia and Slovenia stated that they have no experience on co-operation in urgent computer-related cases, based on the Convention on Cybercrime or other treaties.

Bosnia and Herzegovina referred to the prosecution of two persons having committed internet frauds, as well as inspection of IP addresses, following data received through the INTERPOL Office in Wiesbaden.

Latvia was of the view that the use of the I-24/7 communication system of the INTERPOL was the optimal solution, and referred to two cases of successful co-operation on the basis of requests made through the US INTERPOL Bureau. Slovakia also stated that the I-24/7 Network of the INTERPOL and Slovakia's system of judges and prosecutors on duty provide an effective framework for dealing with urgent cases.

Lithuania pointed out that best results were achieved when, among other measures, the responsible officers had the opportunity to discuss the execution plan, process, as well as legal and practical issues relating to a request directly in co-ordination meetings.

Poland referred to the fact that its judicial authorities are encouraged to transmit MLA requests directly to their counterparts, wherever possible.

In its very comprehensive answer to the questionnaire, Romania referred to a number of practical cases to illustrate certain problems. It notably mentioned a case, concerning multiple offences affecting 12 countries in three continents, which demonstrated great divergence in the urgency and attention with which Romania's requests were treated by different countries. Romania stated that, at the trial stage, the majority of MLA requests concerned the service of summons or documents, followed by requests for hearing of witnesses. One of the difficulties encountered was the fact that, where expedited means of communication were used in urgent cases, many countries refused to execute requests without certified copies. As potential guidelines, Romania suggested the following:

- possibility of direct requests between competent authorities and the possibility of using modern means of communication;
- importance of networks in fostering human contacts, essential in urgent cases, and necessity of having easy access to full contact details;
- possibility of creating a global network for victims support (allowing representation of victims from another State, thus avoiding delays in servicing documents);
- need for States, where the victim resides, to treat all cybercrime cases with urgency, regardless of the damages involved.

Canada, like Romania, pointed to the importance of having a clearly defined and easily reachable central authority available at all times. It considered that States should resort, where possible, to liaison magistrates posted abroad who can provide early guidance. It also drew attention to the need for providing focused requests, which contain all necessary elements, including grounds for urgency and priorities; as well as the names of persons, such as police officers, already contacted in connection with the case. In this respect, Canada stressed the value of informal police co-operation.

Question 2:

If your State is a Party to Convention on Cybercrime, please describe how Article 32 b of the Cybercrime Convention is applied or is intended to be applied in practice within your jurisdiction. How do your competent authorities interpret the provisions of the mentioned Article in legislation and/or in practice?

All responding States (except Turkey) are signatory to the Convention on Cybercrime, out of which 11 States[6] have already ratified the Convention. It appears that, in the experience of these States, the Convention on Cybercrime, and in particular the provisions of its Chapter III on international co-operation, have never been used as an exclusive legal basis for transmitting a request for legal assistance in computer-related cases. In the opinion of Romania, this is possibly due to the provisions of the Convention itself, and in particular its Article 25, paragraph 4, which provides that "mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties". The main treaties mentioned in this respect are the European Convention on Mutual Assistance in Criminal Matters, and in so far as EU members are concerned, the Convention on Mutual Assistance in Criminal Matters between the member States of the EU, followed by bilateral treaties and the United Nations Convention against Transnational Organised Crime.

None of the responding States had any concrete experience in relation to the application of Article 32 b of the Convention, nor did they feel a need to reform their legislation in the light of this Article. Armenia saw no need to implement this provision immediately, concentrating instead on the "opportunities of the 24/7 contact points". While Greece has prepared a draft law on the ratification and implementation of the Convention, the text in question does not deal with this provision.

Bulgaria and Slovenia referred to the fact that the Convention was directly applicable in their internal system, and that Article 32 b would accordingly be interpreted and applied in the light of the Explanatory Report and the spirit of the Convention, as well as "national and international law on data protection".

Only 5 States[7] provided comments on the substance and interpretation of Article 32 b, with significantly diverging views.

For Finland, Germany and Latvia, this provision provides for trans-border access without the involvement of the authorities of the country where computer data are located, although their interpretations differ as to when this is permissible.

Germany, while not Party to the Convention, interprets this provision as allowing the authorities of country A to access not publicly available data that are located in country B, without addressing a request for mutual legal assistance, provided that a person within country B, who would have lawful authority to pass such data to domestic authorities, has given lawful and voluntary consent to such access. This "sovereign act" is compatible with German criminal procedure, and is not considered an exception to formal mutual legal assistance.

Latvia considers that the owner or operator of a computer system may provide stored computer data directly to the competent authorities of a foreign State, if it has received written consent of the user or subscriber to that effect.

Finland has a more restrictive interpretation. In its view, Article 32 b gives permission "to access e.g. e-mail of the person concerned if he/she has given a lawful authorisation", without the other Party's active role/involvement/assistance. However, Finland considers that this does not apply where it is a service provider (like Google) who provides this information, in which case ordinary MLA channels would have to be used.

---

6 Armenia, Bosnia and Herzegovina, Bulgaria, Finland, Hungary, Latvia, Lithuania, Romania, Slovakia, Slovenia, Ukraine.

7 Finland, Germany, Latvia, Slovakia, Ukraine.

By contrast, Slovakia and Ukraine have a more restrictive interpretation of this provision (Slovakia sees it as one of the most progressive and difficult provisions of the Convention).

According to Slovakia, the approval of a competent judicial authority of the Party where the computer data are located (which Slovakia considered a “quasi-requested State”) would be necessary in all cases.

Ukraine considered that implementation of Article 32 b is only possible, if the data concerned are transmitted by the authorities of the country where they are located. It was of the view that trans-border access to such data without the knowledge or consent of the owner of the data would constitute a breach of law in that country.

Appendix

Convention on Cybercrime (ETS No.: 185): Chart of Signatures and Ratifications

(Status as of: 17/2/2009)

Member States of the Council of Europe

States	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Albania	23/11/2001	20/6/2002	1/7/2004				X			
Andorra										
Armenia	23/11/2001	12/10/2006	1/2/2007				X			
Austria	23/11/2001									
Azerbaijan	30/6/2008				X	X	X	X		
Belgium	23/11/2001									
Bosnia and Herzegovina	9/2/2005	19/5/2006	1/9/2006				X			
Bulgaria	23/11/2001	7/4/2005	1/8/2005		X	X	X			
Croatia	23/11/2001	17/10/2002	1/7/2004				X			
Cyprus	23/11/2001	19/1/2005	1/5/2005							
Czech Republic	9/2/2005									
Denmark	22/4/2003	21/6/2005	1/10/2005		X		X	X		
Estonia	23/11/2001	12/5/2003	1/7/2004				X			
Finland	23/11/2001	24/5/2007	1/9/2007		X	X	X			
France	23/11/2001	10/1/2006	1/5/2006		X	X	X			
Georgia	1/4/2008									
Germany	23/11/2001									
Greece	23/11/2001									
Hungary	23/11/2001	4/12/2003	1/7/2004		X	X	X			
Iceland	30/11/2001	29/1/2007	1/5/2007		X		X			
Ireland	28/2/2002									
Italy	23/11/2001	5/6/2008	1/10/2008				X			
Latvia	5/5/2004	14/2/2007	1/6/2007		X		X			
Liechtenstein	17/11/2008									
Lithuania	23/6/2003	18/3/2004	1/7/2004		X	X	X			
Luxembourg	28/1/2003									
Malta	17/1/2002									
Moldova	23/11/2001									
Monaco										
Montenegro	7/4/2005			55						
Netherlands	23/11/2001	16/11/2006	1/3/2007				X	X		
Norway	23/11/2001	30/6/2006	1/10/2006		X	X	X			
Poland	23/11/2001									
Portugal	23/11/2001									
Romania	23/11/2001	12/5/2004	1/9/2004				X			
Russia										
San Marino										
Serbia	7/4/2005			55						
Slovakia	4/2/2005	8/1/2008	1/5/2008		X	X	X			

Slovenia	24/7/2002	8/9/2004	1/1/2005				X			
Spain	23/11/2001 r									
Sweden	23/11/2001									
Switzerland	23/11/2001									
the former Yugoslav Republic of Macedonia	23/11/2001	15/9/2004	1/1/2005				X			
Turkey										
Ukraine	23/11/2001	10/3/2006	1/7/2006		X		X			
United Kingdom	23/11/2001									

Non-member States of the Council of Europe

States	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Canada	23/11/2001									
Costa Rica										
Dominican Republic										
Japan	23/11/2001									
Mexico										
Philippines										
South Africa	23/11/2001									
United States	23/11/2001	29/9/2006	1/1/2007		X	X	X			

Total number of signatures not followed by ratifications:	23
Total number of ratifications/accessions:	23