www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 28 November 2011 T-CY (2011) 10 E

Cybercrime Convention Committee (T-CY)

Sixth Plenary

Strasbourg, 23-24 November 2011

Abridged meeting report

The T-CY Committee, meeting in Strasbourg on 23 and 24 November 2011, chaired by Markko Künnapu, decided:

Agenda item 3: By-election of Bureau Members

- To elect Mr. Branko Stamenkovic (Serbia) and Mr. Justin Millar (United Kingdom) to the Bureau of the T-CY for the remainder of the terms of office in line with Article 1.3 of the Rules of Procedure for the Bureau (T-CY(2010)04E).

Agenda item 4: Priorities and workplan of the T-CY for the period 1 January 2012 – 31 December 2013

- To review and adopt document T-CY(2011)4E on "the way forward: Plan for the period 1 January 2012 – 31 December 2013" (as attached in Appendix 2).

- To take note that full implementation of this plan is subject to funding and that for some activities co-funding is to be ensured through Phase 3 of the Global Project on Cybercrime (document T-CY(2011)9E as attached in Appendix 5).

Agenda item 5: Establishment of an ad-hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows

- To adopt the terms of reference of the ad-hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows (T-CY(2011)5E as attached in Appendix 3).

- To appoint as members of the ad-hoc group: Ioana Albani (Romania), Andrea Candrian (Switzerland), Markko Künnapu (Estonia), Vladimir Miloseski ("The former Yugoslav Republic of Macedonia", Erik Planken (Netherlands), Betty Shave (USA), Branko Stamenkovic (Serbia) and Pedro Verdelho (Portugal).

Agenda item 6: Accession criteria and procedure under Article 37 of the Convention on Cybercrime

- To review and adopt the Opinion on accession criteria and procedure to be followed, in conformity with Article 37 of the Convention, as regards accession of non-member States (document T-CY(2011)3E rev as attached in Appendix 4).

- To instruct the Secretariat to share it with the CDPC in view of further consultations.

- To request the Bureau to subsequently finalise the opinion, and to instruct the Secretariat to submit it, thereafter, to the Committee of Ministers.

Agenda item 7: State of ratification, signatures and accession to the Convention and its Protocol

- To take note of the recent ratification of the Convention on Cybercrime by Switzerland and the United Kingdom.

- To take note of the recent ratification of the Protocol CETS 189 by Finland and Germany, and of its signature by Italy.

- To note with appreciation that Senegal was invited to accede to the Convention on Cybercrime in line with Article 37.

- To encourage other States that are signatories or have been invited to accede to become Parties to the Convention and its Protocol as soon as possible.

Agenda item 8: Compliance by Parties with Article 35 of the Convention on 24/7 points of contact

- To take note that all Parties have established 24/7 points of contact in line with Article 35, but that some contact points are yet to become fully functional.

- To instruct the Secretariat to maintain an up-to-date list of contact points established under the Convention on Cybercrime, and to share it on a regular basis with the contact points. To request the Secretariat to liaise with the G 8 High-tech Crime Subgroup.

- To encourage Parties to ensure the effectiveness of contact points (Action 3.2 of the Plan) and to provide the Secretariat with detailed up-to-date information on contact points.

- To instruct the Secretariat to provide additional information on the use of the restricted website.

Agenda item 9: Review of the effective implementation of the Budapest Convention by the Parties: provisions to be reviewed in 2012

- To review at the first Plenary in 2012 the implementation by the Parties of articles 16, 17, 29 and 30 (Action 3.1 of the Plan), and to encourage Parties to cooperate with the Bureau and the Secretariat in this respect.

- To take note of the interest by Parties in the review of other international cooperation provisions, and therefore to start reviewing also additional international cooperation provisions.

Agenda item 10: Results from technical assistance/capacity building programmes

- To take note of the results achieved under the technical assistance programme, including the joint projects of the Council of Europe and the European Union on cybercrime.

- To take note of the planned Phase 3 of the Global Project on Cybercrime and its link to the plan of activities of the T-CY, and to encourage Parties to consider voluntary contributions to this project (Action 6.3 of the Plan).

Agenda item 11: Follow up to the Octopus Conference and 10th anniversary Session of the Budapest Convention on Cybercrime (Strasbourg, 21 – 23 November 2011)

- To note with appreciation the Octopus conference and the special session on the occasion of the 10th anniversary of the Convention on Cybercrime held prior to the T-CY Plenary.

Agenda item 12: Any other business

– To request Parties that have not yet done so, to confirm members of their official T-CY delegation to the Secretariat.

Agenda item 13: Next meeting of the Cybercrime Convention Committee

– To hold two Plenary Sessions in 2012 and to request the Bureau to establish a suitable date for the first meeting in the period May/June 2012.

Appendix 1

Annotated agenda

Wednesday, 23 November, 15h00 – Thursday, 24 November 17h30

(Please note that agenda items marked with * are for decision by the members representing contracting Parties to the Budapest Convention)

1. Opening of the meeting	
2. Adoption of the agenda	T-CY (2011)7 E
3. By-election of Bureau Members* In line with Article 1.3 of the Rules of Procedure for the Bureau, the T-CY is invited to elect two Bureau Members to fill seats that have become vacant for the remainder of the term of office.	T-CY (2010)04 E
4. Priorities and workplan of the T-CY for the 1 January 2012 – 31 December 2013* The T-CY is invited to review, in view of adoption, the "Priorities and workplan of the T-CY for the 1 January 2012 – 31 December 2013.	T-CY (2011) 4 E
5. Establishment of an ad-hoc sub-group of the T-CY on jurisdiction and transborder access to data and data flows* The T-CY is invited to adopt a decision on the establishment of this ad-hoc sub-group. Delegations are invited to propose members with the necessary sub-subject matter expertise.	T-CY (2011) 5 E
6. Accession criteria and procedure under Article 37 of the Convention on Cybercrime* The T-CY is to review, with a view to adoption, the draft "opinion on accession criteria and procedure to be followed, in conformity with Article 37 of the Convention, as regards accession of non-members of the Council of Europe to the Budapest Convention". The T-CY is invited to take into account the CDPC Opinion on Criteria and Procedure for Accession by Non-Member States to Council of Europe Criminal Law Conventions (CDPC(2011)7). The T-CY is furthermore invited to take note that the CDPC Bureau (having met on 20 and 21 October 2011) is concerned that the proposed "procedure" (paragraphs 10 - 20 of the T-CY opinion) should be exactly the same as the one set out in the CDPC opinion, and hence suggests that the opinion of the T-CY, in as far as "procedure" is concerned, should only make a general reference to the opinion of the CDPC on criteria and procedure for accession by non-member states to Council of Europe criminal law conventions".	T-CY (2011) 3 E rev CDPC (2011) 7E

7. State of ratification, signatures and accession to the Convention and its Protocol The T-CY is invited to take note of the information provided by the Secretariat. Members representing states that are not yet parties to the Budapest Convention or its additional protocol are invited to provide information about ongoing ratification or accession procedures.	Treaty office list
8. Compliance by Parties with Article 35 of the Convention on 24/7 points of contact The T-CY is invited to discuss the current state of the establishment of 24/7 points of contact.	
9. Review of the effective implementation of the Budapest Convention by the Parties: provisions to be reviewed in 2012* The T-CY is invited to agree on the provisions of the Budapest Convention to be reviewed in 2012.	Action 3.1 of document T-CY (2011) 4 E
10. Results from technical assistance/capacity building programmes The T-CY is invited to take note of information provided by the Secretariat about ongoing technical assistance projects, as well as the proposed Phase 3 of the Global Project on Cybercrime.	Presentations by Programme on Cybercrime T-CY (2011) 9 E
11. Follow up to the Octopus Conference and 10th anniversary Session of the Budapest Convention on Cybercrime (Strasbourg, 21 – 23 November 2011) The T-CY is invited to take note of information provided by the Secretariat.	
12. Any other business	
13. Next meeting of the Cybercrime Convention Committee	

Appendix 2

www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 24 November 2011 T-CY (2011) 4 E fin

T-CY: The way forward

Plan for the period

1 January 2012 – 31 December 2013

1. Article 46 of Budapest Convention provides for "*Consultations of the Parties*". According to this provision, the Parties of the Convention "*shall consult periodically*". These "*consultations*" are envisaged to facilitate the "*effective use and implementation of the Convention*", the exchange of information and the "*consideration of possible supplementation or amendment of the Convention*". Regarding the "*use and implementation*" of the Convention the Parties can, within the framework of the consultations, identify "*any problems thereof, as well as the effects of any declaration or reservation made under this Convention*" – Article 46, 1, a, b and c.

2. The Cybercrime Convention Committee (T-CY) is the mechanism enabling the Consultations of the Parties. Article 46 is the legal framework of the activities of the T-CY.

3. According to the Explanatory Report of the Convention, the "*consultations*" shall in particular examine issues that have arisen in the use and implementation of the Convention, including the effects of declarations and reservations.

4. These consultations are to be governed by a "flexible" procedure, leaving it to the Parties to decide how and when to convene. This flexibility was believed, according to the Explanatory Report, to be necessary "*to ensure that all Parties to the Convention, including non-member states of the Council of Europe, could be involved - on an equal footing - in any follow-up mechanis*m". "*Given the needs of effective prevention and prosecution of cyber-crime and the associated privacy issues, the potential impact on business activities, and other relevant factors, the views of interested parties, including law enforcement, non-governmental and private sector organisations, may be useful to these consultations*".

5. The increased number of parties, signatories and invitees, and the increased interest in the Budapest Convention worldwide require a more pro-active role of the TC-Y and effective use of resources.

6. In 2011, the United Nations created an Intergovernmental Expert Group to discuss, among other things, the role of the United Nations Office on Drugs and Crime regarding cybercrime. The possibility of drafting a new convention on this matter was not excluded.

7. The Budapest Convention is intended to be a global legal instrument, involving the largest possible number of countries from all over the world. This particular characteristic is at the same time one of its great advantages and also one of the challenges to its effective success.

8. For the time being, adherence to the Convention in terms of ratifications or accessions, in particular outside Europe, is not yet at the level required. Four non-European states have signed the text and one of them ratified it. However, there are good reasons to believe that other countries, in addition to those which have signed, will accede to the Convention in the near future. A number of states have already been invited to accede, particularly as a result of the efforts of the Global Project on Cybercrime of the Council of Europe. Moreover, many other countries have adopted legislation in line with the Budapest Convention and are implementing its principles.

9. These circumstances require from T-CY a programme of activities and timetable for future work – as indicated in the Rules of Procedures of the Bureau (article 4 d) – that help the T-CY to assume its proper role within an international context.

10. In the future, and in order to achieve its objectives, the T-CY will hold two plenary sessions per year (one open to observers and one restricted to the Parties). The plenary sessions will be followed by Bureau meetings.

11. The T-CY will give, in the period of 2012/2013, priority to the following objectives:

1 Support ratification of and accession to the Convention;
2 Review the functioning of the accession procedure for non-member States of the Council of Europe;
3 Review the effective implementation of the Convention by the Parties;
4 Continue to give consideration to possible future standard-setting work, taking into account all options as regards the exact choice of instrument (amendment of the Convention, additional protocol to the Convention or a "soft law" instrument);
5 Ensure closer coordination between the Parties and ensure representation of the T-CY in future discussions on cybercrime in international *fora*;
6 Ensure close cooperation and coordination with other projects or programmes (including the Global Project) on cybercrime developed by the Council of Europe regarding the previous points and, in particular, 1, 2, 3 and 7;
7 Exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form; and
8 Review the financial resourcing of the Committee.

12. The workplan will include the following:

Objective 1	**Support the ratification of and accession to the Convention**
Action 1.1	Engage in policy dialogue with CoE member States that have not signed or ratified it yet: – Not yet signed: Andorra, Monaco, Russian Federation, San Marino – Signed but not yet ratified: Austria, Belgium, Czech Republic, Georgia, Greece, Ireland, Liechtenstein, Luxembourg, Malta, Poland, Sweden, Turkey Policy dialogue is to include T-CY missions to these countries.
Action 1.2	Engage in policy dialogue with – and encourage technical assistance if necessary to – third countries that have signed but not yet ratified it and with those countries that were invited to accede and have not yet completed the accession process: – Argentina, Australia, Canada, Chile, Costa Rica, Dominican Republic, Japan, Mexico, Philippines, Senegal, South Africa Policy dialogue to include T-CY missions to these countries.
Action 1.3	Support accession by the largest possible number of non-member states: – Parties to the Convention to participate actively in the assessment of requests for accession under the new procedure/criteria – In order to encourage accession, Parties to propose for assessment of states that may be interested in acceding – Parties to the Convention and the Council of Europe to provide or facilitate targeted technical assistance if necessary to help meet minimum requirements – T-CY missions to countries.

Objective 2	**Review the functioning of the accession procedure for non-member States of the Council of Europe**
Action 2.1	Within one year following the agreement to the new accession procedure by the Committee of Ministers review the functioning of the procedure
Objective 3	**Review the effective implementation of the Budapest Convention by the Parties**
Action 3.1	Review the implementation (in terms of domestic legislation and practices) of specific provisions of the Convention: – T-CY Plenary to agree which provisions to review in the forthcoming session – Bureau to prepare questionnaire on these provisions to be sent to all Parties – The Bureau with the support of other T-CY members to compile replies and draft a report – Plenary will engage in peer review/discussion and adopt recommendations (one day per Plenary to be foreseen) – Final report to help share and disseminate good practices and lessons learnt
Action 3.2	Ensure compliance by Parties with Article 35 (24-7 points of contact)
Objective 4	**Continue to give consideration to possible future standard-setting work, taking into account all options as regards the exact choice of instrument (amendment of the Convention, additional protocol to the Convention or a "soft law" instrument)**
Action 4.1	Establish an ad hoc sub-group to prepare a draft instrument to further regulate the transborder access to data and data flows, as well as the use of transborder investigative measures on the Internet and related issues for submission to the T-CY Plenary in the second half of 2012
Action 4.2	T-CY Plenary to discuss and decide on the way ahead in the second half of 2012
Objective 5	**Ensure closer coordination between the Parties and ensure representation of the T-CY in future discussions on cybercrime in international *fora***
Action 5.1	Prior to international meetings, consult within the Bureau in view of facilitating common positions of the Parties – Email Bureau members and set up a conference call – Share proposed common position with all Parties
Action 5.2	Encourage Parties to attend the international meeting and support common position
Action 5.3	Coordinate between Parties during international meetings – Set up side-meetings/coordination meetings in the course of the international meetings
Action 5.4	Ensure representation of T-CY in international fora
Objective 6	**Ensure close cooperation and coordination with the technical cooperation programme on cybercrime of the Council of Europe (including the Global Project on Cybercrime) developed by the Council of Europe regarding the previous points and, in particular, 1, 2, 3 and 7**

Action 6.1	T-CY representatives to participate in project activities
Action 6.2	At least one T-CY Plenary to be held in conjunction with the annual Octopus Conference
Action 6.3	The technical cooperation programme on cybercrime to support the work of the T-CY (subject to the availability of funds) – Parties are encouraged to provide voluntary special purpose contributions to allow for this
Action 6.4	Results of technical cooperation activities to be presented to the T-CY
Objective 7	**Exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form**
Action 7.1	T-CY in cooperation with the technical cooperation programme to maintain a database on cybercrime legislation in countries worldwide
Action 7.2	T-CY to contribute to the organisation of the Octopus conferences
Objective 8	**Review the financial resourcing of the Committee**
Action 8.1	Discussion at first T-CY plenary 2012 (7th Plenary)

Appendix

Article 46 – Consultations of the Parties

1 The Parties shall, as appropriate, consult periodically with a view to facilitating:

a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;

c consideration of possible supplementation or amendment of the Convention.

2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.

4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.

5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Appendix 3

www.coe.int/T-CY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 24 November 2011 T-CY (2011) 5 E

Ad hoc sub-group of the T-CY on

jurisdiction and transborder access to data and data flows

Terms of Reference

The Cybercrime Convention Committee (T-CY),

Having regard to:

a. Article 46 (1) (a) and (c), of the Convention on Cybercrime (ETS No. 185);
b. the decision of the fifth meeting of the Cybercrime Convention Committee to instruct the Bureau to *"prepare terms of reference for its future standard-setting work on jurisdiction and transborder access to data and data flows and submit it to the Committee with a road map for implementation, at the earliest convenience"*.

Having considered that:

a. During the last 25 years, which includes the decade since the "birth" of the Budapest Cybercrime in 2001, there has been a significant evolution of information and communication technologies and specifically of the role of the Internet in our societies. We have moved from a real to a virtual or digital world which is borderless by nature. The development of ICT brings much positive innovation. At the same time, ICT have also become highly attractive to criminals. In general terms, criminality evolved from traditional crime with the aid of computers to high tech crime originating from and targeted at ICT. The internet provides criminals with a high degree of anonymity. The Internet allows criminals to target potential victims from anywhere in the world, and enables mass victimisation with relative ease. Attacks against "cloudstorage" systems of ISPs would affect computer data and systems of a large number of end-users.

b. Increasingly data is stored on computer systems in locations and jurisdictions other than the physical location of the suspect or of his or her computer. Often, the precise location of data stored in the "cloud" is unknown to law enforcement lawfully investigation an offence or even to the user. The evolution towards cloud computing thus impedes the securing of electronic evidence or the rapid pursuit and prosecution of offenders.

c. An important issue to be addressed is to find a proportional and practicable balance between privacy, data protection and other fundamental rights of users on the one hand and on the other hand the need for law enforcement action that is sufficiently efficient to allow criminal justice authorities to meet their obligation of protecting users.

d. Whilst cyberspace itself is borderless, the authority of law enforcement is in general bound to a specific jurisdiction. At the same time, trans-border investigations are necessary and are often carried out already. However, it is important to develop clearer rules as to what is and what is not allowed in each jurisdiction with regard to trans-border investigations and cross-border co-operation. This would enhance the effectiveness of the fight against cybercrime in line with human rights and rule of law principles.

e. The existing text of Article 32 of the Budapest Convention was a compromise solution adopted in 2001. At that time, there was a lack of concrete experience at the international level regarding such trans-border situations, and this prevented rules going further than the provision of Article 32b. The wording of paragraph 293 of the explanatory report of the Convention makes it clear that Article 32 must be understood as a minimum text to which all parties, at the time, agreed. The Explanatory Report leaves it open to countries to go beyond

this provision: "Other situations [than mentioned in article 32] are neither authorised, nor precluded." Article 39.3 of the Convention states that "Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party".

f. Reaching an agreement on additional procedures and powers allowing for more direct and effective trans-border investigations by law enforcement with the necessary conditions and safeguards is a major challenge. The Cybercrime Convention Committee is nevertheless prepared to address this challenge.

Has decided:

a. To set up, from among its members, an ad hoc sub-group to examine the following issues:

   i. the use of Article 32 (b), of the Convention on Cybercrime;
   ii. the use of transborder investigative measures on the Internet;
   iii. the challenges to transborder investigations on the Internet posed by applicable international law on jurisdiction and state sovereignty.

b. To instruct the ad hoc sub-group to develop an instrument – such as an amendment to the Convention, a Protocol or Recommendation – to further regulate the transborder access to data and data flows, as well as the use of transborder investigative measures on the Internet and related issues, and to present a report containing its findings to the Committee.

c. To instruct the ad hoc sub-group to take into account the questionnaire, replies and debates in T-CY plenary sessions since 2009.

d. To instruct the ad hoc sub-group to submit a report to the second T-CY plenary of 2012.

e. That the ad hoc sub-group shall be composed of no more than 10 members of the Committee with the necessary subject-matter expertise. The defrayal of expenses is subject to the availability of funds. The ad hoc group may draw upon external expertise.

f. To propose that the European Committee on Crime Problems (CDPC) may send a representative to meetings of the ad hoc sub-group, without the right to vote and at the charge of the corresponding Council of Europe budget sub-head.

g. That the Secretariat shall be provided by the Council of Europe.

h. That these Terms of Reference will expire on 31 December 2012.

Appendix 4

Agenda item 6: Accession criteria and procedure under Article 37 of the Convention on Cybercrime

The T-CY decided:

- To review and adopt the Opinion of the Cybercrime Convention Committee (T-CY) on accession criteria and procedure to be followed, in conformity with Article 37 of the Convention, as regards accession of non-member States (document T-CY(2011)3E rev).
- To instruct the Secretariat to share it with the CDPC in view of further consultations.
- To request the Bureau to subsequently finalise the opinion, and to instruct the Secretariat to submit it, thereafter, to the Committee of Ministers.

Explanatory note:

The T-CY had consulted the CDPC and reviewed the suggestion of the CDPC Bureau (having met on 20 and 21 October 2011), namely to replace the procedure proposed in the draft T-CY opinion (paragraphs 10 to 20) and instead to make a general reference to the procedure set out in the CDPC opinion on criteria and procedure for accession by non-member states to Council of Europe Criminal Law Conventions (document CDPC (2011)7E).

The T-CY shares the overall objectives of the CDPC opinion of facilitating accession by non-member states to certain criminal law conventions through a more transparent procedure. However, with regard to the Convention on Cybercrime, the T-CY:

- considered that a review of a request for accession to the Convention on Cybercrime against certain criteria was a step in the accession procedure which must, therefore, operate within the framework set by Article 37 on Accession to the Convention on Cybercrime;

- is doubtful as to whether the proposed formal role and mandatory hearing of the CDPC in the accession procedure is compatible with Article 37 which only foresees a formal role for the Contracting States and the Committee of Ministers. The Contracting States – including non-member States of the Council of Europe – are represented in the Cybercrime Convention Committee (T-CY);

- is concerned that a dual review by both the T-CY and the CDPC would make the accession procedure less transparent and thus risks deterring accession;

- believes that it disposes of the technical expertise required to carry out a review, and that, therefore, a dual review by the T-CY as well as the CDPC was not necessary;

- agrees that the CDPC should be kept informed of accession requests and of reviews underway by the T-CY so that the CDPC is able to advise the Committee of Ministers case by case if necessary.

Consideration could be given to the option of removing the Convention on Cybercrime from the appendix of the CDPC opinion. It could be argued that the Convention on Cybercrime was a "core" treaty of the Council of Europe as noted in Parliamentary Assembly Recommendation 1920 (2010) on reinforcing the effectiveness of Council of Europe treaty law (and Reply from the Committee of Ministers adopted at the 1114th meeting of the

Ministers' Deputies (25 May 2011)).[1] The T-CY proposes holding further consultations with the CDPC on this matter.

The T-CY recommends that pending a solution the current procedure be maintained so that new accession requests are not delayed.

[1] http://www.assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta10/EREC1920.htm
http://assembly.coe.int/Main.asp?link=/Documents/WorkingDocs/Doc10/EDOC12175.htm
http://assembly.coe.int/Documents/WorkingDocs/Doc11/EDOC12621.pdf

www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 24 November 2011 T-CY (2011) 3 E rev

Draft Opinion of the Cybercrime Convention Committee (T-CY)

Accession criteria and procedure

to be followed, in conformity with Article 37 of the Convention on Cybercrime (ETS No. 185), as regards accession of non-members of the Council of Europe to the Convention

1. The Committee of Ministers (Deputies), at its 1095th meeting on 13 October 2010, decided:

> *"to mandate the T-CY, in close co-operation with the European Committee on Crime Problems (CDPC), to provide advice to the Committee of Ministers on the criteria and procedure to be followed, in conformity with Article 37 of the Convention, as regards the accession of non-members of the Council of Europe to the Budapest Convention."*

2. Given the potential global application of the Convention, the T-CY considers the issue of how best to assess and process requests for accession by non-member states to be of the highest importance, and consequently the T-CY welcomes the above invitation from the Committee of Ministers.

3. The T-CY is of the opinion, that the broadest possible implementation of the Budapest Convention, including accession by non-member states, will serve the aim of effective international cooperation against cybercrime. Accession by countries meeting the minimum requirements of the Convention should therefore be facilitated. The purpose of the criteria and procedure proposed below is to make the accession process more transparent and predictable, and to encourage States that are committed to implement the Budapest Convention and to cooperate against cybercrime to seek accession.

4. The T-CY sees it as its primary task to provide the Committee of Ministers and the Parties to the Convention with a technical assessment by cybercrime experts regarding the ability of a non-member state requesting accession to fully co-operate with the other Parties under the Budapest Convention, including whether the aims of the Convention would be served by the requesting non-member state acceding to it.

5. The T-CY is furthermore of the opinion that an invitation to accede will encourage further legislative reforms and institution building in the country invited, and facilitate technical assistance if necessary.

6. Under this procedure, the T-CY is tasked by the Committee of Ministers to assess all requests for accession to the Budapest Convention, and make a recommendation on the basis of this assessment.

7. On the basis of such a recommendation and technical assessment, the Committee of Ministers can then complete the procedure foreseen by Article 37 of the Convention.

Criteria

8. Given that the Budapest Convention has always been open, accession by states meeting the minimum requirements of the Convention will be welcomed and facilitated. An assessment in the light of these criteria is meant to build mutual trust and ensure effective implementation of the Convention.

9. The T-CY, having consulted the European Committee on Crime Problems (CDPC), believes that a state that meets the minimum requirements of the Budapest Convention and that is committed to cooperate with the other Parties should be invited to accede. The assessment of the request will be based on the following criteria:

a. The requesting non-member state has the necessary legal framework in place to apply the minimum standards of the Convention or has expressed its firm commitment to have in place such a framework by the time of accession. Indicators may include, for example:

   - the enactment of legal provisions and/or administrative guidelines implementing the Convention in domestic law.

b. The requestor ensures in its domestic law that the procedural law powers and procedures provided for in Section 2 of Chapter II of the Budapest Convention are subject to safeguards and conditions which shall provide for the adequate protection of human rights and liberties as stipulated by Article 15 of the Convention.

c. The requestor has expressed its firm commitment to put in place the mechanisms necessary to enforce the Convention and co-operate with other Parties to the widest extent possible. Indicators may include, for example:

   - the existence of efficient administrative infrastructures;
   - the availability of trained staff; or
   - the requestor has indicated its willingness to work with other Parties and/or the Council of Europe on training of its staff.

d. The requestor is committed to participate actively in the Consultations of the Parties in line with Article 46 of the Convention, and thus to realise the aims of the Convention. Indicators may include, for example:

   - the commitment to contribute actively to the international cooperation under the Convention is expressed firmly in the request for accession; or
   - the requestor has a record of co-operation relevant for the fight against cybercrime with one or more Parties to the Convention; or
   - the requestor has received technical assistance from the Council of Europe and/or from other Parties.

Procedure

10. In terms of procedure, the T-CY recommends the following pursuant to Article 37. This procedure shall establish a transparent framework and replace the current practice of informal consultations:

11. When approached by a non-member state with a request to be invited to accede to the Budapest Convention, the Secretary General shall simultaneously inform the Committee of Ministers and the T-CY, consisting of the representatives of the Parties to the Convention, about the request.

12. The Secretariat shall provide the T-CY with all information relevant for the assessment of the request and seek additional information from the requesting state, if necessary.

13. On receipt of a request, the T-CY will assess the request according to the criteria. If a T-CY member does not give its opinion within 60 days, it shall be deemed to not to object to a T-CY recommendation in favour of accession.

14. The T-CY shall provide the Committee of Ministers with its assessment and recommendation as soon as possible, and not later than three months after the receipt of the request.

15. Where the T-CY unanimously supports the request, it will recommend to the Committee of Ministers to invite this state to accede to the Convention.

16. Where an agreement could not be reached in the T-CY on the request, the opinion of the T-CY shall set out the views of the majority, as well as the dissenting views.

17. The assessment by the T-CY should omit any reference to the position taken by individual Parties or member states.

18. The T-CY recommends that the aforesaid list of criteria is made available through the Secretariat to non-member states requesting to be invited to accede in order to improve the level of transparency as regards the assessment of requests for accession.

19. If a Party is aware that a non-member State may be in interested in acceding, the Party may ask for an assessment for that State. Should this assessment be positive, the T-CY may invite the Secretary General to encourage the non-member state in question to seek accession to the Budapest Convention.

20. The request by the non-member state will be examined, in the light of the T-CY recommendation, by the Committee of Ministers or, where appropriate, by one of its rapporteur groups. Once the Committee of Ministers and the Parties to the convention that are not members of the Council of Europe have agreed to give a positive reply to the request, the decision to invite the non-member State in question shall become definitive. An invitation to accede to the instrument in question will be sent to the State concerned by the Secretary General.

****

Appendix 5

Document T-CY(2011)9E

Global Project on Cybercrime (Phase 3)

Project proposal

Version 5 November 2011

Project title	Global Project on Cybercrime, Phase 3 (DGHL/2571)
Project area	A global project aimed at supporting the implementation of the Budapest Convention on Cybercrime and related standards and practices
Budget	Up to EURO 1 million
Funding	Voluntary contributions from public and private sectors
Implementation	Data Protection and Cybercrime Division (Directorate General of Human Rights and Rule of Law, Council of Europe)
Duration	24 months (1 January 2012 – 31 December 2013)

BACKGROUND AND JUSTIFICATION

While the reliance of societies worldwide on computer systems and other information and communication technologies and thus their vulnerability to threats such as cybercrime increase day by day, cybercrime is not a new type of crime anymore. The Budapest Convention was opened for signature ten years ago (November 2001) and a wide range of measures against cybercrime has been taken before and since then.

Relevant standards, tools, good practices and experience are thus available. However, these are not always readily documented and shared between countries and between the public and private sector. The proposed project will address this problem by:

1. Documenting and sharing experience and good practices related to measures against cybercrime with regard to cybercrime strategies and policies, legislation, high-tech crime and other specialised units, law enforcement training, judicial training, financial investigations, public-private cooperation, criminal law measures related to the sexual exploitation and abuse of children, international police and judicial cooperation and other measures. This includes organising the annual global Octopus Conferences on cooperation against cybercrime and developing an online tool.
2. Providing assistance to countries in the implementation of the Budapest Convention and related standards and good practices. The project will organise a number of in-country and regional workshops, support relevant events organised by other organisations, and provide direct legislative and other advice to countries worldwide.
3. In order to determine the state of measures against cybercrime in a given country as well as worldwide, the project will prepare assessments of specific countries but also a report on the global state of measures against cybercrime.

The proposed project will build on the more than 250 activities carried out under phases 1 and 2 of the Global Project on Cybercrime since 2006 as well as the regional joint projects of the European Union and the Council of Europe on cybercrime (CyberCrime@IPA and Cybercrime@EAP). It will allow the continuation of the annual Octopus conferences on cooperation against cybercrime that have been organised since 2004.

The Cybercrime Convention Committee (T-CY) of the Council of Europe is responsible for following the implementation of the Budapest Convention. The present project will closely cooperate with the T-CY and support it in its tasks. It will allow in particular observer states to participate in the work of this Committee.

OBJECTIVE, EXPECTED OUTPUTS AND ACTIVITIES

Project objective	**To promote broad implementation of the Budapest Convention on Cybercrime (CETS 185) and related standards and tools**
Output 1	**Experience exchange: Good practices related to measures against cybercrime documented and shared**
Activity	Prepare or (if already available) update good practice studies on: ▪ Cybercrime strategies and policies ▪ Cybercrime legislation ▪ High-tech crime and other specialised units ▪ Law enforcement training ▪ Judicial training ▪ Financial investigations ▪ Public-private cooperation ▪ Criminal law measures related to the sexual exploitation and abuse of children ▪ International police and judicial cooperation
Activity	Develop an online tool for the sharing of experience and good practices
Activity	Organise two global Octopus conferences on cooperation against cybercrime
Activity	Support the participation of observer states and experts in the meetings of the Cybercrime Convention Committee (T-CY)
Output 2	**Assistance: Countries assisted in the implementation of the Budapest Convention and related standards and good practices**
Activity	Support the organisation of up to 30 in-country or regional workshops
Activity	Contribute to up to 50 events organised by other organisations
Activity	Provide legislative and other advice to countries worldwide
Output 3	**Assessment of measures against cybercrime available**
Activity	Prepare an assessment report on measures taken globally against cybercrime
Activity	Support the Cybercrime Convention Committee (T-CY) in the review of the implementation of the Budapest Convention by the Parties and in the assessment of accession requests

CONTACT

Data Protection and Cybercrime Division
Directorate General of Human Rights and Rule of Law
Council of Europe, F-67075 Strasbourg Cedex (France)

Tel +33 3 9021 4506
Fax +33 3 8841 3955
Email alexander.seger@coe.int

Appendix 6

LIST OF PARTICIPANTS

BUREAU MEMBERS / MEMBRES DU BUREAU

Chair of the Committee/Président du Comité:

Mr Markko KÜNNAPU
Adviser, Criminal Police Department, Ministry of Justice, Estonia

Vice Chair of the Committee / Vice Présidente du Comité:

Mr. Erik PLANKEN
Law Enforcement Department, Ministry of Security and Justice, Netherlands

Members/Membres:

Ms Ioana ALBANI
Chief Prosecutor, Head of the Cybercrime Unit, Prosecutor's Office attached to the High Court of Cassation and Justice, Directorate for the Investigation of Organised Crime and Terrorism offences, Romania

Mr Justin MILLAR
Head of Cyber Crime Policy, Home Office, United Kingdom

Ms Betty SHAVE (apologized/excusée)
Computer Crime and Intellectual Property Section, Department of Justice, United States of America

Mr Branko STAMENKOVIC
Head of the Special Department for High-Tech Crime of HPPO Belgrade, Office of the Public Prosecutor of Serbia

Mr Pedro VERDELHO
Public Prosecutor, General Prosecutor's Office of Lisbon, Procuradoria Geral da Republica, Portugal

PARTIES TO THE CONVENTION ON CYBERCRIME
PARTIES A LA CONVENTION SUR LA CYBERCRIMINALITE

ALBANIA/ALBANIE

Mr Gentijan JAHJOLLI (Representative in the T-CY)
Specialist on Cybercrime issues, Directorate of Foreign Relations, Ministry of Justice, Tirana, Albania

Mr Arqilea KOÇA
Prosecutor, General Prosecutor’s Office, Tirana, Albania,

ARMENIA/ARMENIE

Mr Samvel HOVSEPYAN (Representative in the T-CY)
Head of Division, Police of the Republic of Armenia, General Department on Struggle Against Organized Crime, Armenia

Mr Arsen SAYADYAN
Officer, National Security Office of the Republic of Armenia

Mr Andrey YASHCHYAN
Officer of High Tech Crime Division, Main Department of Combat against Organised Crime

AZERBAIJAN/AZERBAIDJAN

Mr Samir MUKHTARZADE (Representative in the T-CY)
Senior Detective Officer, Cybercrime unit 2, Ministry of National Security, Baku

Mr Mir Kamran HUSEYNOV
24/7 Contact Point, Head of Division, Ministry of National Security, Baku

BOSNIA AND HERZEGOVINA/BOSNIE-HERZEGOVINE

Mr Tomislav ĆURIĆ (Representative in the T-CY)
Expert Adviser, Department for Combating Organized Crime and Corruption, Ministry of Security, Sarajevo

Mr Jovo MARKOVIĆ
Head of the High-Tech Crime Department, Ministry of Interior, Republika Srpska, Banja Luka

Mr Nedzad DILBEROVIĆ
24/7 Point of Contact, Expert Associate for Economic Crime, Ministry of Security of Bosnia and Herzegovina

BULGARIA/BULGARIE

CROATIA/CROATIE

Mr Dubravko PALIJAŠ (Representative in the T-CY)
Deputy to the Chief State Prosecutor, State Prosecutor's Office, Zagreb

Ms Kristina POSAVEC
Chief Police Inspector, Ministry of Interior

CYPRUS/CHYPRE

DENMARK/DANEMARK

ESTONIA/ESTONIE

Mr Markko KÜNNAPU (Representative in the T-CY/Chair of the Committee)
Adviser, Criminal Police Department, Ministry of Justice

FINLAND/FINLANDE

Mr Jani JUKKA (Representative in the T-CY)
District Prosecutor, Key Prosecutor (Computer Crime), Prosecutor's Office of Länsi-Uusimaa, Vitikka

FRANCE

Ms Delphine GAY (Representative in the T-CY)
Capitaine de Police, OCLCTIC, Ministère de l'Intérieur

Mr Christophe RENAUD
Administrative attaché in charge of the Administrative Management Unit, Ministry of Interior, SCTIP

GERMANY/ALLEMAGNE

TBC (Representative in the T-CY)

Dr Alexander DÖRRBECKER
Attorney at Law (N.Y.), Federal Ministry of Justice

HUNGARY/HONGRIE

Ms Rita LISZKAI (Representative in the T-CY)
Legal Expert, Department of Codification and Coordination, Ministry of Interior

ICELAND/ISLANDE

ITALY/ITALIE apologized/ excusée

LATVIA/LETTONIE

Mr Aleksandrs BUKO (Representative in the T-CY)
Head of Cybercrime Enforcement Unit

LITHUANIA/LITHUANIE

Mr Žilvinas SIDERAVIČIUS (Representative in the T-CY)
Chief Investigator, Police Department under the Ministry of the Interior of the Republic of Lithuania, Criminal Police Board

MOLDOVA/MOLDAVIE

Mr Veaceslav SOLTAN (Representative in the T-CY)
Chief Prosecutor, Head of Section of Informational Technologies and Investigation of informational Crime, General Prosecutor Office

Mr Octavian BUSUIOC
Specialist of prevention of IT crimes, Division for Fight against Cybercrime, Ministry of Internal Affairs

Mr Victor ENACHI
Deputy Head of Law Division, Security and Intelligence Service

MONTENEGRO

Mr Vladimir VUJOTIĆ (Representative in the T-CY)
Adviser, Ministry of Justice

Mr Jaksa BACKOVIĆ
Police Directorate of Montenegro, Chief Inspector for Fighting Cybercrime

Mr Zarko PAJKOVIĆ
Deputy basic state prosecutor, Basic State Prosecutor Office

NETHERLANDS/PAYS-BAS

Mr Erik PLANKEN (Representative in the T-CY/Vice chair of the Committee)
Ministry of Security and Justice, Law Enforcement Department

Mr Jean Luc LUIJS
Ministry of Security and Justice, Law Enforcement Department

Ms Wieteke KOORN
National Public Prosecutors Office, Senior-Legal Officer, High Tech Crime and Telecom

Ms Eileen MONSMA
Adviser National High Tech Crime Unit, National Crime Squad of the Netherlands Police Agency

NORWAY/NORVEGE

Mr Eirik TRØNNES HANSEN (Representative in the T-CY)
Police Prosecutor, National Criminal Investigation Service, Cyber Crime Investigation Section, High-Tech Crime Department

PORTUGAL

Mr Pedro VERDELHO (Representative in the T-CY/member of the Bureau)
Public Prosecutor, General Prosecutor's Office of Lisbon, Procuradoria Geral da Republica

ROMANIA/ROUMANIE

Ms Raluca Nicoleta SIMION (Representative in the T-CY)
Legal Adviser, Directorate International Law and Judicial Cooperation

Ms Ioana BOGDANA ALBANI (member of the T-CY Bureau)
Chief Prosecutor, Head of the Cybercrime Unit, Prosecutor's Office attached to the High Court of Cassation and Justice, Directorate for the Investigation of Organised Crime and Terrorism Offences, 24/7 contact point

Mr Virgil SPIRIDON
Head of Cybercrime Unit, Romanian National Police, 24/7 contact point

SERBIA/SERBIE

Mr Branko STAMENKOVIĆ (Representative in the T-CY/ member of the Bureau)
Head of the Special Department for High-Tech Crime of HPPO Belgrade, Office of the Public Prosecutor of Serbia

Ms Bojana PAUNOVIĆ
Judge, Court of Appeals, Criminal and Cybercrime Department

Mr Ljuban PETROVIĆ
Police Inspector, Ministry of Interior, Service for Combating Organised Crime, Cyber Crime Department, 24/7 Contact point for Serbia

SLOVAKIA/SLOVAQUIE

SLOVENIA/SLOVENIE

Mr Toni KASTELIĆ (Representative in the T-CY)
Head of Computer Investigation Centre, Criminal Police Directorate

SPAIN/ESPAGNE

Mr Antonio ROMA VALDÉS (Representative in the T-CY)
Public Prosecutor, Prosecutor's Office, Santiago

SWITZERLAND/SUISSE

Mr Andrea CANDRIAN (Representative in the T-CY)
Département Fédéral de Justice et Pólice, Office Fédéral de la Justice, Unité Droit Pénal International

"THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA" / "L'EX-REPUBLIQUE YUGOSLAVE DE MACEDOINE"

TBC (Representative in the T-CY)

Mr Vladimir MILOSHESKI
Public Prosecutor, Basic Public Prosecutor's Office in Skopje

Ms Marina PESEVSKA
Senior Inspector, Cybercrime Unit, Ministry of Interior

Mr Marjan STOILKOVSKI
Head of Cybercrime Unit, Section of Financial Crime, Centre for Repression of Organized and Serious Crime

Mr Marko ZVRLEVSKI
24/7 Contact point, Public Prosecutor, Head of Basic Public Prosecutors Office in Skopje

UKRAINE

Mr Valentyn PETROV (Representative in the T-CY)
Expert, Security Service of Ukraine

Mr Mykola DANILYUK
Deputy Chief of Computer Intelligence Unit, Division for Combating Cybercrime and Human Trafficking, Criminal Police Department, Ministry of Interior

UNITED KINGDOM/ROYUAME-UNI

Mr Justin MILLAR (Representative in the T-CY/member of the Bureau) Head of Cyber Crime Policy, Home Office

UNITED STATES OF AMERICA/ETATS-UNIS D'AMERIQUE

Betty SHAVE (Representative in the T-CY/member of the Bureau) apologized/excusée
Computer Crime and Intellectual Property Section, Department of Justice

Mr Kenneth HARRIS
Office of International Affairs, Criminal Division, Department of Justice

OBSERVERS/OBSERVATEURS

ANDORRA/ANDORRE

ARGENTINA/ARGENTINE

Mr Gabriel CASAL
Jefe de Gabinete de Asesores, Jefatura de Gabinete de Ministros,

Mr Roberto FRONTINI
Subsecretaria de Política Criminal del Ministerio de Justicia, Seguridad y Derechos Humanos

AUSTRIA/AUTRICHE

BELGIUM/BELGIQUE

CANADA

Gareth SANSOM (Representative in the T-CY) apologized/excusée
Department of Justice

Ms Lucie ANGERS
General Counsel and Director, External Relations, Criminal Law Policy Section, Department of Justice

CHILE/CHILI

COSTA RICA

Mr Francisco SALAS RUIZ
Informatic Law Prosecutor and Director of the Law in Effect System (Procuraduría General de la República) General Prosecutor Office

Mr José Adalid MEDRANO MELARA
Cybercrime Attorney & Consultant

CZECH REPUBLIC/REPUBLIQUE TCHEQUE

Mr Tomáš HUDEČEK
Legal expert, Ministry of Justice

DOMINICAN REPUBLIC/REPUBLIQUE DOMINICAINE

GEORGIA/GEORGIE

Mr Giorgi JOKHADZE
Lawyer, Data Exchange Agency, Ministry of Justice of Georgia

Mr Shalva KVINIKHIDZE
Head of International Relations Main Division, Ministry of Internal Affairs

GREECE/GRECE

IRELAND/IRLANDE

JAPAN/JAPON

Mr Hideaki GUNJI (Representative in the T-CY
Consul (Attorney) Consulate-General of Japan in Strasbourg

LIECHTENSTEIN

Ms Isabelle FROMMELT
First Secretary, Ministry of Foreign Affairs

LUXEMBOURG

MALTA/MALTE

MEXICO/MEXIQUE apologized/ excusée

MONACO

PHILIPPINES

Mr Geronimo SY (Representative in the T-CY)
Assistant Secretary, Department of Justice

POLAND/POLOGNE

RUSSIAN FEDERATION/FEDERATION DE RUSSIE

Mr Ernest CHERNUKHIN
First Secretary Ministry of Foreign Affairs

Mr Alexander GERMOGENOV
Russian Telecom

SAN MARINO/SAINT MARIN

SOUTH AFRICA/AFRIQUE DU SUD

SWEDEN/SUEDE

TURKEY/TURQUIE

Mr Bilal SEN
Superintendent of Police, Turkish National Police - Cyber Crime Unit,

EUROPEAN COMMISSION/COMMISSION EUROPEENNE apologized/ excusée

EUROPEAN COMMITTEE ON CRIME PROBLEMS/ COMITE EUROPEEN POR LES PROBLEMES CRIMINELS (CDPC)

EUROPOL apologized/ excusée

G8 HIGH-TECH CRIME SUBGROUP apologized/ excusée

INTERNAL TELECOMMUNICATION UNION (ITU)/UNION INTERNATIONALE DES TELECOMMUNICATIONS (UTI)

INTERPOL

Mr Michael MORAN
Acting Assistant Director of Cyber Security and Crime / Global Complex Innovation (IGC), Interpol

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT / ORGANISATION DE COOPERATION ET DE DEVELOPPMENT ECONOMIQUES
apologized/ excusée

ORGANISATION FOR SECURITY AND CO-OPERATION IN EUROPE (OSCE)/ORGANISATION POUR LA SECURITE ET LA COOPERATION EN EUROPE (OSCE)

Mr Ben HILLER
Programme Officer, Action against Terrorism Unit

Ms Margaret LAZYAN
OSCE Politico-Military Senior Assistant, Armenia

STEERING COMMITTEE ON THE MEDIA AND NEW COMMUNICATION SERVICES/COMITE DIRECTEUR SUR LES MEDIAS ET LES NOUVEAUX SERVICES DE COMMUNICATION (CDMC)

Ms Bisera Zankova

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC)/OFFICE DES NATIONS UNIES CONTRE LA DROGUE ET LE CRIME (UNODC)

Mr Steven MALBY
Drug control and crime prevention officer, Conference support section, Division for treaty affairs, United Nations Office on Drugs and Crime, Vienna International Centre

Ms Gillian MURRAY
Chief Focal point for Cybercrime, Conference support section, Division for treaty affairs, United Nations Office on Drugs and Crime, Vienna International Centre

SPEAKERS/INTERVENANTS

Mr Henrik KASPERSEN
Professor Emeritius, Former Chair of the Cybercrime Convention Committee (T-CY),

SECRETARIAT OF THE COUNCIL OF EUROPE / SECRETARIAT DU CONSEIL DE L'EUROPE

Council of Europe – DG I- Directorate General of Human Rights and Rule of Law
Conseil del'Europe- Direction des Droits de l'Homme et Etat de Droit:

Mr Alexander SEGER, Secretary of the T-CY, Head of the Data Protection and Cybercrime Division

Ms Cristina SCHULMAN, Head of the Cybercrime Unit, Data Protection and Cybercrime Division

Mr Mustafa FERATI, Programme Officer, Data Protection and Cybercrime Division

Mr Gergo NEMETH, Programme Officer, Data Protection and Cybercrime Division

Ms Elisabeth MAETZ, Assistant, Data Protection and Cybercrime Division