www.coe.int/T-CY

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 investigating 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.