# Comments on the Draft Second Protocol to the Convention on Cybercrime (Budapest Convention)

February 20, 2019

**The Centre for Internet and Society, India**

Template designed by Saumyaa Naidu, shared under the **Creative Commons Attribution 4.0 International license**

Following consultations with data protection, civil society, industry and others, during the Cybercrime Convention Committee (T-CY) meeting from 29 November 2018 onwards, the Cybercrime Convention Committee has sought additional contributions regarding the provisional draft text for a Second Additional Protocol to the Budapest Convention on Cybercrime ("Budapest Convention").

The Centre for Internet and Society, ("CIS"), is a non-profit organisation that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives. The areas of focus include digital accessibility for persons with diverse abilities, access to knowledge, intellectual property rights, openness (including open data, free and open source software, open standards, and open access), internet governance, telecommunication reform, digital privacy, artificial intelligence, freedom of expression, and cyber-security. This submission is consistent with CIS' commitment to safeguarding general public interest, and the rights of stakeholders. CIS is thankful to the Cybercrime Convention Committee for this opportunity to provide feedback to the Draft.

The draft text addresses three issues viz. language of requests, emergency multilateral cooperation and taking statements through video conferencing. Below are the comments from the Centre for Internet and Society on the proposals:

1. **Language for requests**

    a. The clause requires that requests should be made in a language acceptable to the Requested Party or to be accompanied by a translation into a language acceptable by the Requested Party. However there should be an exception carved out for emergency situations such as those contained in the second provision of the Protocol. The provision for emergency requests envisages a 24/7 dedicated person for receiving requests, but this provision may be defeated if the requests have to be translated into the language acceptable to the Requested Party since translators may not be available at all times of day and night in the Requesting Party and even if they are available, translations themselves may take time.

b. The Explanatory Report proposes an informal survey to be carried out by T-CY every year regarding the acceptable languages for requests which it envisages giving Parties more leeway in terms of what languages would be acceptable for different types of assistances. This process should be contained in the main text of the Protocol so that the process is formalised and Parties cannot refuse requests on technicalities such as language of the request.

2. **Emergency Mutual Assistance**

a. The emergency clause in the proposal creates an expedited process of requesting information to the appropriate authority in the Requested Party and passing on the information by the appropriate authority to the Requesting Party once it is received. However once the initial expedited request is received, there may be a long process for retrieving the information by the Requested Party as the request may have to go through a number of authorities such as the enforcement authorities, the judicial courts, the data companies, etc. Even if the appropriate authority designates a person to receive emergency requests 24/7 this would not necessarily ensure that all the other departments would also treat the request on an expedited basis.

b. The proposal talks about accepting an emergency request in electronic form with the appropriate levels of security and authentication. With regard to the security requirements the Explanatory Report provides that Parties may decide among themselves whether there is a need for special security protections (including encryption) that may be necessary in a particularly sensitive case. This seems to suggest that Parties need to undertake one-on-one discussions with regard to each case. It is not clear whether this means that the Parties need to specify the appropriate security and authentication procedures for each request once its received or whether they need to have discussions in advance and anticipate all the different situations and have procedures in place for all such cases. Either situation could lead to delays and may defeat the purpose of the expediting

provision. It is suggested that mechanisms for security protections which should be acceptable to all parties can be discussed with the Parties and included in the Additional Protocol itself.

3. **Video Conferencing**

   a. The use of the word "may" in the first paragraph indicates that the provision is not mandatory and the requested party has the option to refuse assistance at the outset. Although the Explanatory Report gives the example of a situation where the Requested Party may refuse because the information requested may be provided in a better manner through some other means, the protocol does not clarify that the Requested Party has to give any reasons for refusing a request for video conferencing. Defining broad standards for refusing a request for video conferencing can help in protecting against giving the Requested Party blanket discretion in this regard.

   b. One rationale of including such a discretionary provision may have been that the provision lays down a procedure to be followed so that protracted negotiations may be avoided every time a request for video conferencing is made. However the provision falls short even on this count as most of the thorny issues such as "which Party shall preside; the authorities and persons that shall be present; whether one or both Parties shall administer particular oaths, warnings or instructions to the witness or expert; the manner of questioning of the witness or expert; the treatment of claims of privilege or immunity, etc." are to be decided between the Parties on a case to case basis.