UNODC reference: CU 2016/50/DTA/OCB/CSS

Finland expresses its appreciation to the UNODC for its *note verbale* of 24 February 2016, requesting comments on the draft study being prepared by an open-ended intergovernmental Expert Group on the problem of cybercrime and responses to it.

Finland notes that the study should correctly be referred to as a draft study, as it has yet to be approved by the open-ended intergovernmental Expert Group.

The draft report is an extensive one, and a number of comments can be made. In the following, Finland presents some general comments relating to the draft study, as well as some comments relating to the "key findings" and the "options" presented in draft study. We are also prepared to submit a number of comments regarding matters of detail in the draft study, on request.

General comments relating to the draft study

Finland wishes to begin by welcoming the study on an important and highly topical issue. Finland is in particular pleased that the UNODC has facilitated the conduct of research on an issue before the United Nations Commission on Crime Prevention and Criminal Justice. It is our view that the collection and analysis of data from around the world, the definition of the key concepts, the identification of the key issues, and the tentative identification of possible options, along with their possible costs and benefits, is in keeping with the best tenets of evidence-based policy formulation.

Cybercrime is a rapidly evolving phenomenon, and it has generated its own vocabulary. It is also a highly technical area, requiring its own expertise. The authors of the draft study should in particular be commended for the way they have attempted to clarify the concepts and to present the complex issues and terminology in an informative way. The draft study is well written, and the ample use of tables and graphs help the reader to make sense of the data.

At the same time, however, the way in which the draft study is edited and laid out, and in particular the highlighting against a blue background of what are referred to as "key findings", raises concern. One of the most delicate parts of any study is the drawing of conclusions. Especially when a study is intended for a lay audience, as is the case here (with the primary audience being those participating in sessions of the Crime Commission), considerable caution must be exercised in identifying and formulating what are deemed to be "key findings". On a number of points we question whether the data presented in the draft study does in fact support the drawing of what are referred to as "key findings", and whether these can be formulated in the absolute manner done in the draft study.

The draft study is based on responses received from 69 member states, and reflects the situation as of the beginning of 2012. Finland appreciates that the authors have also used information from the private sector, research and intergovernmental organizations. Given the speed with which the phenomenon of cybercrime and the response to it have evolved, the passing of four years since the writing of the draft study suggests that some of the data, and in particular what are presented as "key findings", would quite likely be different if additional responses were to be collected in order to update the draft study.

Comments relating to the "key findings" and the "options" presented in draft study

As already mentioned, the "key findings" presented throughout the study (against a blue background) and the "options" presented on pp. xiii-xv raise a number of concerns. These are the most important part of the study, and they would require considerable more discussion among the stakeholders: discussion on whether these "key findings" are indeed based on the (limited) data, and on how the "key findings" should be formulated. As already mentioned, many of the key findings seem to be stated in an overly absolute manner, in cases where they should instead be qualified by various cautions and caveats.

As an illustration of our concerns, we find it quite surprising that the key findings and the executive summary (with two exceptions, on pp. xix and xxvi) do not refer to the Council of Europe Convention on Cybercrime. This is a key international instrument that has fundamentally affected legislation, practice and international cooperation in a large number of states around the world. The key findings should emphasize the importance of regional cooperation among stakeholders, and the particular relevance of the Council of Europe Convention, especially when responding to individual cases. Within the framework of the Council of Europe Convention, considerable work has been carried out and continues to be carried out in order to promote the efficacy of international cooperation. A number of Guidance Notes have been adopted, and consideration is being given to the preparation of a protocol to the Council of Europe Convention.

To turn to the six options laid out on pp. xiii – xv of the draft study, for the UN to pursue:

(a) developing international model provisions in criminalization;
(b) developing international model provisions on investigative powers for electronic evidence;
(c) developing model provisions on jurisdiction;
(d) developing model provisions on international cooperation regarding electronic evidence;
(e) developing a multilateral instrument on international cooperation regarding electronic evidence;
(f) developing a comprehensive multilateral instrument on cybercrime;
(g) strengthening international, regional and national partnerships … with a view to delivering enhanced technical assistance.

To begin with some preliminary comments: This list of options can be debated on a number of grounds, such as the feasibility, practicality and added value of the different options indicated. An assessment would be needed of each option in the light of such grounds.

- For example, in respect of criminalization, the study itself indicates that the core cybercrime offences have already been criminalized. The Council of Europe Convention on Cybercrime has had a central role in this work on harmonization.
- Another example: it is, to put it mildly, overly ambitious to suggest that consensus could be reached within the framework of the United Nations on direct access to cross-border data. (Given the comment on p. 220 about trans-border access, this is apparently already recognized in the draft study.) A more realistic and pragmatic approach would be to develop guidance on this issue.
- A third, and significant, point has been made several times in the discussions, but is a fundamental one and should clearly be noted: the negotiation of a completely new instrument, and even of model provisions, would increase fragmentation and legislative differences even more, causing potential conflict between existing instruments. Reaching consensus on difficult issues – even if successful – requires time and resources, which means that if work begins *de novo* on model provisions, much less a new convention, other ongoing work will likely be hampered or even deferred. Scarce time and resources could more productively be placed in technical assistance and support.

- Of the six options given, there is presumably considerable consensus on one key finding: the importance of technical support and assistance. Provision of these does not require any new international instruments or model provisions.

The above preliminary comments notwithstanding, in Finland's view, the most important ground for questioning the list of options is that it is incomplete, even in the light of what is stated elsewhere in the report. The list does not include what in Finland's view is an obvious option, that of strengthening the network of existing international or regional cybercrime instruments. Finland notes that considering the appropriateness of existing multilateral instruments as framework instruments is an option quite distinct from what is contained in option (f), developing a comprehensive multilateral instrument. Furthermore, the action generally called for (harmonising provisions on criminalization, improving international cooperation regarding electronic evidence, improving mutual legal assistance) has already been done, to a considerable extent, on the basis of existing international instruments, and work on this is continuing in particular on the basis of the Council of Europe Convention on Cybercrime.

The absence of an option referring to existing instruments is even more striking, given that the draft report itself provides ample support for such an option. On p. xix of the executive summary, it is noted that "For the more than 40 countries that provided information, the Council of Europe Convention on Cybercrime is the most used multilateral instrument for the development of cybercrime legislation." (It may be noted that "more than 40 countries that provided information" amounts to almost 60% of the responding countries.) Reference is also made on p. 63 to the fact that "A significant amount of cross-fertilization exists between all [existing instruments], including, in particular, concepts and approaches developed in the Council of Europe Cybercrime Convention." (See also figure 3.10 on p. 75.) On p. xii of the draft study, it is noted that "[T]he majority of options suggested" included "accession to existing international or regional cybercrime instruments." We find it quite odd, and a matter of concern, that such fundamental observations are not reflected in the "key findings" or the "options".

In view of this, Finland strongly suggests the inclusion of the following "option":
Using existing multilateral instruments as framework instruments on cybercrime, with a view to strengthening an international approach in the areas of criminalization, procedural powers, jurisdiction, and international cooperation.

At the same time, Finland suggests that several of the options should be reformulated to better reflect what is already happening in international cooperation. For example, options (a) through (d) refer to the possibility of developing international model provisions. However, existing international instruments, in particular the Council of Europe Convention, have already been used by several states as model provisions.

In line with this, option (a) should be reformulated as follows:
(a). Using existing international instruments, in particular the Council of Europe Convention on Cybercrime, as international model provisions on criminalization of core cybercrime acts, with a view to supporting States in eliminating safe havens through the adoption of common offence elements […].

Finland is well aware that reference to the Council of Europe Convention on Cybercrime in this context has been contentious in discussions within the framework of the United Nations Crime Commission and related bodies. The phrase above between commas, "in particular the Council of Europe Convention on Cybercrime", could be left to a footnote. We emphasize nonetheless that

existing international instruments are already being used international model provisions, which calls into question the perceived need to develop new international model provisions.

Options (b), (c) and (d) should be reformulated in a similar manner. Option (g)(i), which also refers to model provisions, should be amended accordingly.