Federal Ministry of Justice and Consumer Protection

17 August 2016

German Comments on the

Comprehensive Study on Cybercrime

(Draft – February 2013)

The United Nations Office on Drugs and Crime (UNODC) invited the member states to provide the open-ended Intergovernmental Expert Group (IEG) with comments on the draft Comprehensive Study on Cybercrime of February 2013.

1. General remarks

The 12th UN Crime Congress (Salvador, Brazil, April 2010) discussed "recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime". The Congress came to the conclusion that further studies in the field of cybercrime were necessary and proposed to set up the Open-ended Intergovernmental Expert Group (IEG). As a result the UN General Assembly in her 71st plenary meeting on 21 December 2010 recommended in No. 9 of Resolution 65/230 that the Commission on Crime Prevention and Criminal Justice (CCPCJ) should establish such an Expert Group, which should conduct a "comprehensive study of the problem of cybercrime" and "examine options to strengthen existing and to propose new national and international legal or other responses to cybercrime". Since its establishment the IEG had only two meetings (January 2011 and February 2013). Four weeks prior to the second meeting, an "executive summary" of the Draft Study was made available to the participating States. The complete Draft Study was made available just two weeks prior to the IEG´s meeting. Until today the study was not adopted. The 13th UN CCPCJ in April 2015 just invited IEG to continue its work. In February 2016 the Draft Study was made available in the six official UN-languages and states are invited to provide comments until 31 August 2016. Before the next meeting of the IEG, it is not sufficient that the States merely have the opportunity to give their comments to the IEG. Rather, it is also necessary that the states have an opportunity to review the responses of the other states in detail. **Therefore a meeting in fall or winter 2016 would be clearly too early.**

2. Key findings

The eight chapters of the Comprehensive Study dealing with all dimensions of the phenomenon of cybercrime (connectivity and cybercrime; the global picture; legislation and framework; criminalization; law enforcement and investigations; electronic evidence and criminal justice; international cooperation; prevention) open out into **six key findings** which are mainly convincing. In that sense it is correct that the diversity of cybercrime laws worldwide and multiple instruments lead to the emergence of country cooperation "clusters". Furthermore the formal international cooperation is not really able to secure electronic evidence in a timely manner. There also is a need to re-conceptualize location in the context of cloud computing, a need for technical assistance and a need for prevention and holistic approaches.

By contrast, **key finding d. is not conclusive**, insofar as it claims that due to the different national legal frameworks harmonization of the cybercrime offences is insufficient. Especially through the Budapest Convention on Cybercrime of the Council of Europe (CoE-Treaty No. 185; Cybercrime Convention), its Additional Protocol concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (CoE-Treaty No. 189) and the European Union Directive on attacks against information systems (2013/40/EU) a far-reaching harmonization of criminal law in the field of cybercrime has been reached. These successes at the level of European Union and the Council of Europe are not recognized by the key findings. In Particular the Cybercrime Convention had a meaningful impact on cybercrime legislation worldwide. There has been much progress since 2006 towards greater harmonization of legislation worldwide and fostering as well as accelerating mutual legal assistance, using this treaty as a core or "guideline" (more details also see below). Furthermore, the EU-Directive on attacks against information systems harmonized substantive criminal law across the 28 European member states in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions. Thus also indirectly the mutual legal assistance in Europe has been simplified and made more effective.

3. Observations regarding "Options"

As a conclusion derived from the mentioned key findings the Study finds that options to strengthen existing and to propose new national and international legal or other responses to cybercrime may include **model provisions** (key findings a. – d.) on

- core cybercrime acts
- investigative powers for electronic evidence

- jurisdiction
- international cooperation regarding electronic evidence

and/or the development of a **multilateral instrument** (key findings e. – f.)

- on international cooperation regarding electronic evidence
- on cybercrime, with a view to establishing an international approach in the areas of criminalization, procedural powers, jurisdiction and international cooperation.

From the German point of view United Nations model provisions as well as new multilateral instruments cannot be supported. Both would mean a step back behind the already achieved standards on the level of the European Union and the Council of Europe. At the level of the European Union the Directive on attacks against information systems (2013/40/EU) is in place, whereby the criminal law in the field of cybercrime within the European Union was harmonized. With the Cybercrime Convention an effective treaty and guideline is already in place and functioning.

The efforts of the United Nation in the field of cybercrime should focus on strengthening of **international, national** and **regional partnerships**, including with the private sector and academic institutions, to support matters of **technical assistance** and **capacity building** for prevention and combating of cybercrime in developing countries (key finding g.).

The comprehensive study proposes options, which refer to the establishment of new model provisions and/or multilateral instruments as a response to cybercrime. In that respect, Germany has the following general objections:

1. There is a **lack of consensus on the need for model provisions and/or multilateral instruments** on cybercrime. The possibility of such solutions has been discussed since the 11th UN Congress on Crime Prevention and Criminal Justice in 2005. The debate on that topic continued over years, without any consensus to establish model provisions and/or multilateral instruments. The topic was also on the agenda of 12th UN Crime Congress and it was concluded to set up the open-ended intergovernmental Expert Group which should be tasked with further studies. Since then, there were only two meetings of the Expert Group on cybercrime (last meeting in February 2013), but the Expert Group has the study not yet accepted. Also the 13th UN Crime Congress only concluded to invite the Expert Group to continue its work. Thus, there is also no prospect of an required substantive consensus in the nearer future.

2. There is **no need for (additional) model provisions and/or multilateral instruments** at the level of the United Nations in addition to the Cybercrime Convention. According to Article 37 of the Cybercrime Convention states which are not a member of the Council of Europe can accede to the Convention. At the moment the total number of ratifications of the Cybercrime Convention is 49 states. Another six states signed the Convention and another eleven states were invited to accede; additional accession requests are being processed. At least a huge number of other States worldwide had already used this treaty as a guideline or at least as a source of inspiration for the development of domestic legislation. By adopting Guidance Notes and Additional Protocols the Budapest Convention keeps evolving and up to date. This applies especially to the area of provisions on investigative powers regarding electronic evidence, international cooperation and other current problems. To get these issues under control the Cybercrime Convention Committee inter alia

    - assessed the implementation of the preservation provisions of the Convention
    - assessed the mutual legal assistance provisions of the Convention in general
    - examined the problem of emergency requests for the immediate disclosure of data stored in another jurisdiction through mutual legal assistance channels or through direct requests to service providers
    - established the Cloud Evidence Group (CEG – which works on the criminal justice access to electronic evidence in the cloud, by cooperation with "foreign" internet service providers and with data protection organizations)
    - drew up a Guidance Note on Terrorism
    - drew up a Guidance Note on Production Notes

3. The development of model provisions and/or multilateral instruments on Cybercrime would inevitably lead to a **lowering of already achieved standards**. Considering diverging views on the need for and potential scope of new model provisions/multilateral instruments in general, such instruments would in all likelihood be rather basic in scope and depth. That would be a fatal signal, which would be sent out by the UN. Especially developing countries would base their regulations on such UN-provisions. The standards laid down e.g. in the Cybercrime Convention and in the EU-Directive on attacks against information systems would be undermined in this way. Moreover, a broad scope of such a Treaty on the level of the UN is not feasible because there is no consensus about the scope of such a treaty. While some proponents of a new treaty favor an instrument covering not only cybercrime but also

"cyberterrorism" and "cyber warfare", others appear to be opposed to including terrorism or state-to-state matters.

4. A lot of **reforms underway would be disrupted** through negotiations of model provisions and/or multilateral instruments at the level of the UN. A big majority of States worldwide has undertaken or is in the process of undertaking reforms of legislation on cybercrime and electronic evidence (e.g. with the aim to accede the Cybercrime Convention). To negotiate a new treaty would lead to a disruption of the reform efforts. States that have gone through complex reforms maybe are unlikely to repeat the process and States in the process of reforms cannot afford to wait for several years for the completion of a UN treaty.

4. Conclusions

These arguments (3.1 to 3.4) lead to the following conclusion:

- Germany opposes the development of international model provision on criminalization of core cybercrime acts (option a.) or the development of a comprehensive multilateral instrument on cybercrime (option f.).
- We also refuse the development of international model provisions on investigative powers regarding electronic evidence (option b.), on jurisdiction (option c.), on international cooperation regarding electronic evidence (option d.) as well as the development of a multilateral instrument on international cooperation regarding electronic evidence in criminal matters (option e.)
- From the German point of view it would be much more effective to promote the Budapest Convention on UN-level as a guideline or "model law".
- UN should furthermore focus on the strengthening of international, regional and national partnerships, with a view to delivering enhanced technical assistance for the prevention and combating of cybercrime in developing countries. For this purpose technical assistance should be delivered based on standards of the Cybercrime Convention. Also technical assistance should be delivered through a focus on multi-stakeholder delivery, including representatives from the private sector and academia.
- In order to give all the states the opportunity to review the responses of the other states in detail the next meeting of the Expert Group should take place at the earliest in 2017.