Australia – Comments on the Draft Comprehensive Study on Cybercrime

Australia thanks the United Nations Office on Drugs and Crime (UNODC) for preparing the Comprehensive Study on Cybercrime – Draft February 2013 (the Draft Study). The Draft Study captures a snapshot of the global cybercrime situation in 2013. It identifies some of the challenges faced by countries, international organisations and the private sector, and some of the steps being taken in respect of international cooperation, technical assistance and capacity building. Many aspects of the Draft Study will be of assistance to countries in their consideration of the cybercrime challenge.

However, Australia does not support the inclusion in the Draft Study of the various "key findings" and "options". These particular elements of the Draft Study are beyond the mandate given by the open-ended intergovernmental experts group (IEG). The judgements and recommendations contained in these elements inappropriately stray into areas of policy which are properly within the competence of Member States to consider. The Draft Study should be limited to collecting and collating the relevant data. It is for Member States, through the IEG to evaluate the information and examine possible responses.

Furthermore, Australia does not believe that the "key findings" and "options" in the Draft Study provide the right policy prescriptions. The "options" are disproportionately skewed towards new legislative approaches in the form of model laws or a new treaty, at the expense of capacity building and technical assistance. This approach does not accord with Australia's experience of what is currently needed. Not only are new legislative approaches unnecessary given the range of effective multilateral instruments already available, but they divert attention and resources from the more pressing need for practical capacity building and technical assistance.

The Draft Study identifies a number of existing multilateral instruments available to assist countries to respond to cybercrime, including the Council of Europe Convention on Cybercrime (the Budapest Convention). From Australia's experience, the Budapest Convention offers a number of advantages as a model for countries seeking to develop their own national legislative approach to cybercrime, including:

- providing a comprehensive model framework for offences and law enforcement powers in relation to cybercrime, and facilitating cooperation between States Parties;
- providing for the expeditious preservation and sharing of non-content data (including subscriber information) for law enforcement purposes; and
- using technology-neutral language to ensures it remains effective in response to technological changes.

In additional to cybercrime-specific multilateral instruments such as the Budapest Convention, the United Nations Convention against Transnational Organized Crime and the Protocols thereto also provide powerful tools for international legal cooperation to combat transnational crime, including cybercrime.

The Draft Study identifies significant practical difficulties for countries, especially developing countries, in responding to cybercrime, including with respect to law enforcement,

prosecutors and the judiciary. Australia firmly believes that the international community should prioritise the provision of capacity building and technical assistance, especially for developing countries, to strengthen the abilities of national authorities to respond to cybercrime.

Australia is a strong supporter of capacity building and technical assistance in relation to cybercrime. This includes funding to the UNODC's Global Programme on Cybercrime; regional programs working with Pacific island countries and territories on cyber safety and the collection and use of forensic evidence, including electronic evidence; and bilateral partnerships to assist the development of domestic cybercrime legislation. Australia also recognises the important role of the private sector in this regard and encourages public-private sector partnerships as a highly effective tool to combat cybercrime.

Partnerships between Australia and other countries are critical to ensuring there are no safe havens for cyber criminals and allow Australia to work internationally to stop cyber attacks and track down perpetrators. Australia will continue to invest in these relationships and in raising the cyber security capacity of our region.