

Note 23/16

The Permanent Mission of the United Kingdom of Great Britain and Northern Ireland presents its compliments to the Secretariat of the United Nations Office on Drugs and Crime and has the honour to respond to your communication CU 2016/50/DTA/OCB/CSS, and thereby officially give our comments on the 2013 Draft Study on Cybercrime.

**General comments on the Study and its options:**

- The UK Government appreciates the UNODC's work in carrying out the study which identifies key challenges for the international community, particularly in terms of international cooperation, information sharing and capacity building. We recognise many of the concerns identified in the report. The lack of appropriate legislation, the limited ability of law enforcement to investigate the offences, and the low level of awareness of the threat to the public and to business are all areas which the UK has been seeking to address, and to encourage other countries to do so.
- However, six of the seven options put forward to address the problems identified in the executive summary relate to the perceived need for a new legislative approach, whether a model law or a full treaty. Only one option relates to capacity building, and it is clear from the text that this is secondary to those relating to legislation. Moreover, we maintain that it is the prerogative of Member States to make policy recommendations of this nature through the appropriate international bodies, within their mandates.

**International instruments:**

- Our international policy objectives on cybercrime are driven by our desire to raise the cost, raise the risk, and reduce the reward to cyber criminals. While we must harden the UK against cyber attacks and reduce vulnerabilities, we must also focus relentlessly on pursuing the transnational organised criminals who continue to target the UK.
- We believe that there are already various multilateral instruments available to us in order to foster and develop international cooperation to counter these threats – including the Council of Europe Convention. Cybercrime is a global problem and the Convention, which took many years to develop, has withstood the test of time in dealing with the problem. In our interconnected cyber-world, every nation needs assistance from other countries to fight cybercrime; the Convention, being a treaty open to any qualified country, provides an instrument of choice for doing so. We believe that the Budapest Convention is the best model for countries seeking to develop their own national legislative approach. The Convention is an effective template that allows countries to identify what they need to put in place to be able to work effectively with other countries.
- Most countries are already motivated to have, and will establish comprehensive legislation that supports effective international cooperation and will use, as their guides, the Budapest Convention or its derivatives: the Commonwealth Model Law on Computer and Computer-related Crime and the ITU cybercrime toolkit. While some of the other instruments are comparatively weaker, most are still based on the principles and content of the Budapest Convention, which we class as the gold standard of cyber legislation.
- We also support the ratification and effective implementation of the United Nations Convention against Transnational Organized Crime (UNTOC) and the Protocols thereto, and to use the UNTOC as a practical tool for mutual legal assistance, joint law enforcement investigation, and other forms of international cooperation in relevant cases to address emerging transnational crimes, particularly cybercrime.

**Addressing gaps**

- From the evidence presented in the study, there appears to be a greater need to address shortcomings in the practical response to cybercrime. Training for law enforcement and the

judiciary, public awareness, and working with industry are all areas where there could be significant improvement, and we believe that these are the areas that we should focus on.

- The key crime type missing in the 2013 study is ransomware which is a significant cyber threat now and the nature of the threat evolves so quickly that this can only be viewed as a snapshot in time and therefore options could not be based on that.
- On capacity building, we are strong supporters of the UNODC's capacity building and technical assistance programmes on cybercrime. We believe that UNODC is well placed to deliver this work in light of its unique reach and expertise. We recommend that UNODC continue, in cooperation with relevant international organizations and the private sector, to place a priority on providing long-term and sustainable technical assistance and capacity building, especially for developing countries, in order to strengthen the ability of national authorities to deal with cybercrime, including the prevention, detection, investigation, and prosecution of such crime in all its forms, and to enhance the security of computer networks.

The Permanent Mission of the United Kingdom of Great Britain and Northern Ireland avails itself of this opportunity to renew to the Secretariat of the United Nations Office on Drugs and Crime the assurances of its highest consideration.

