UK National Submission on the UN Cybercrime Treaty

Scope

1. The UK believes the new international cybercrime convention should focus on strengthening cooperation to tackle the growing threat posed by criminal activity to citizens, businesses, and governments.

2. There are a number of existing regional and international cybercrime treaties which have already contributed significantly to efforts to tackle cybercrime. It is important to both build on the success of such treaties and also to recognise the relevant provisions of criminal justice treaties such as the UN Convention against Corruption (UNCAC) and the UN Convention against Transnational Organised Crime (UNTOC).

3. The scope of the treaty should be a) the investigation and prosecution of the offences defined in the treaty; b) the development of capacity and capability to allow all UN Member States to be able to tackle these offences, and c) the recognition of an expert forum by which new and emerging threats can be identified.

4. The UN treaty on cybercrime should cover cyber-dependent offences, together with cyber-enabled crimes where the scale, scope and speed of the offence is increased by the use of a computer. Cooperation is effective where the offences included in the treaty are commonly understood and recognised by all legal systems.

5. The offences in the treaty should not undermine the exercise of freedom of expression or opinion.

6. This is a criminal law treaty, and should focus on the activity to be undertaken by national administrations. It should also consider how, through a multi-stakeholder approach, citizens, non-governmental organizations, civil society organizations, academic institutions and the private sector can work together to protect themselves from cybercrime.

7. Any treaty must contain strong safeguards that include respect for privacy and other human rights, as set out in international human rights law and recognised in relevant resolutions adopted by the UN General Assembly and the UN Human Rights Council.

8. The treaty must be developed in an inclusive and transparent manner, respecting the views of all UN Member States and with the active participation of a wide range of stakeholders, including non-governmental organizations, civil society organizations, academic institutions and the private sector. Furthermore, the treaty's provisions should also encourage an inclusive and transparent approach to tackling cybercrime, e.g. on implementation and capacity building.

9. The language should be technology neutral to ensure the treaty stands the test of time and does not require constant updating.

10. The treaty should not replicate work that has already been or should properly be done elsewhere. The treaty should not extend to matters of cybersecurity, which are already addressed by the UN General Assembly's First Committee, or internet governance, which are already are addressed in dedicated multi-stakeholder forums.

Objectives

11. The primary purpose of the treaty should be to support the effective cooperation of national law enforcement and prosecutorial agencies, bilaterally or multilaterally, in investigating and prosecuting the offences set out in the treaty. A treaty which is widely-supported will enable the widest possible international cooperation.

12. To support effective mutual cooperation, there must be options for refusal on the grounds of dual criminality, refusal in respect of political offences, particularly where the alleged offence relates to the exercise of freedom of expression, and refusal of a request made for the purpose of punishing or persecuting the individual on grounds of their race, religion, gender, or other protected characteristics. It would be useful to have minimum standards that the requesting authority must confirm they have met, such as the request being necessary, proportionate, time limited and authorised at a specific level.

13. The use of powers to investigate and prosecute offences set out in the treaty, including those used in bilateral or multilateral cases, must be subject to effective safeguards in relation to human rights and fundamental freedoms, as set out in international human rights law.

14. The treaty must recognise the operational independence of national investigative and prosecutorial agencies, and that the decision on whether to take action lies solely with those agencies.

15. The treaty should support the development of capability globally, and support capacity building.

16. The threats from criminal activity in cyberspace will change, and the treaty should determine an intergovernmental and multi-stakeholder process to identify future threats, without prejudice to whether that process forms part of the treaty.

17. Given that different genders are affected in different ways by cybercrime, the treaty should be gender inclusive in order to help us tackle cybercrime more effectively. Developing a cybercrime treaty that is cognisant of the gendered implications of its provisions will encourage more women to participate at all levels and in all processes. This will result in more diverse, richer and ultimately better solutions. At the Intergovernmental Experts

Group (IEG) meeting in April 2021 all Member States agreed they should promote, in particular, the participation of women experts.

18. The treaty should promote a “whole of society” approach to tackling cybercrime and encourage Member States to work together with actors outside of government, including experts, industry and the general public, on areas like raising awareness, improving education, gender and cybercrime training, and victim support.

Structure

19. The UK believes that the following structure would be an effective means of organising the treaty.

a) General provisions

The general provisions should include the basis and purpose of the treaty, and the definitions that will be used throughout the treaty. The definitions must be commonly understood and agreed by all parties, and must be technology neutral, taking into consideration terminology that has been widely agreed upon in regional instruments and used in national legal frameworks.

b) Core offences

The offences must include cyber-dependent offences (e.g. illegal access), with descriptions and definitions that are acceptable to all parties. Cyber-enabled offences (e.g. Child Sexual Exploitation and Abuse or fraud) should be included where the offence is mainly carried out online, where computers change the scale and speed of the offence, and where the definitions of the offence are commonly understood.

c) Human rights and safeguards

The operation and implementation of the treaty must be underpinned by meaningful procedural safeguards and strong protections for human rights, and reference international human rights law.

d) Preventive measures

As with UNCAC and UNTOC, the treaty should include provisions encouraging states to implement measures to prevent cybercrime, including through working with all relevant stakeholders.

e) Procedural law provisions

The powers to support investigations and prosecutions must allow appropriate authorities to preserve, search and seize electronic evidence for any offence committed by means of a computer or where the evidence

relating to an offence is in electronic form, for both domestic and international investigations.

f) International cooperation

The international cooperation provisions must cover mutual legal assistance and assistance in an emergency, including a requirement on countries to set up 24/7 contact points. Alongside the practical sharing of evidence, the IEG's recommendations in April 2021 made clear that Member States want to continue to share experiences and best practice, and information on new and growing threats.

g) Technical assistance and capacity building

Capacity building should be encouraged, with a significant role for the UN Office on Drugs and Crime, and there should be coordination of such work through existing structures such as the Global Forum on Cyber Expertise (GFCE). The UK notes the large number of recommendations agreed by the IEG in April 2021 which focussed on capacity building, including the provision of specialist and up-to-date training for practitioners on cybercrime investigations, the handling of electronic evidence, chain of custody and forensic analysis.

h) Implementation

There should a clear plan for implementation of the treaty.