NEW ZEALAND

Elaboration of a convention on countering the use of information and communications technologies for criminal purposes

New Zealand's view on the objectives, scope and structure

New Zealand is pleased to respond to the invitation from the Chair of the Ad Hoc Committee to member states to submit their views on the scope, objectives and structure of the new convention, with regard to the implementation of UN General Assembly Resolutions 74/247 and 75/282. We welcome the opportunity to share our views and look forward to others' contributions and to discussing a path forward as we work together in a transparent, inclusive manner to elaborate a new convention.

Cybercrime is a transboundary challenge. It follows that global cooperation rooted in an inclusive and multi-stakeholder approach is the only way to ensure that the international community is able to effectively counter this growing threat. International cooperation on cybercrime issues requires consistent, effective cybercrime laws that enable investigation and prosecution of cybercrime across borders. Facilitating this cooperation has never been more important. As work, research and social interactions have shifted online, including over the course of the COVID-19 pandemic, the areas of opportunity for cybercriminals have broadened and we have seen cybercrime incidents increase in both frequency and severity.

International cooperation on cybercrime is particularly essential for Small Island Developing States and it is imperative that these countries are able to engage meaningfully in the work of the Ad Hoc Committee. New Zealand is committed to ensuring that Pacific Island Countries are able to meaningfully participate in the work of the AHC. We support hybrid participation for AHC sessions and emphasise the importance of allowing time for adequate preparation and participation by smaller delegations.

Scope

- The new cybercrime convention must **complement rather than conflict** with existing instruments. All member states have agreed that international law applies to cyberspace which means that this new convention will not exist in a vacuum. It will be most effective if it complements and reinforces existing instruments and the current legal regime which includes tools to address cybercrime such as the UN Convention against Transnational Organisation Crime and the Council of Europe Convention on Cybercrime (the Budapest Convention). This is in line with the mandate provided by Resolution 74/247, which urges the AHC's work to take 'into full consideration existing international instruments and efforts at the national, regional and international levels'.

- For New Zealand it is essential that any instrument **protects human rights and upholds a cyberspace that is multi-stakeholder governed, free and open.** The cybercrime convention must

therefore be consistent with states' obligations to protect and respect human rights online, including the right to freedom of expression and the right not to be subjected to arbitrary and unlawful interference with privacy. Measures to combat cybercrime must be consistent with international human rights law.

- The treaty should be **sharply focused on core cybercrime issues** in order to effectively strengthen cooperation to tackle the threat these pose to individuals, industry and governments. We consider that the treaty should cover cyber-dependent offences, together with cyber-enabled crimes only where the scope, speed and scale of the offence is increased by use of information and communications technologies. We consider that there are two clear candidates for this category of crimes: child sexual exploitation and abuse online, and cyber-enabled fraud and theft including ransomware.

- New Zealand does not consider there is a need to duplicate offences that are covered by other legal instruments such as corruption, trafficking or terrorism simply because these may be completed using information communications technologies. Such an approach risks contradiction and confusion and will not deliver a targeted, practical instrument that can improve our collective ability to tackle cybercrime.

- The mandate for this process clearly articulates that we should focus on developing a **criminal justice instrument to improve the international response to cybercrime**, through actions taken by national law enforcement agencies. This requires defining and sanctioning criminal conduct in cyberspace and for states to implement appropriate processes and legislative tools that enable agencies to access and share digital evidence to effectively disrupt and sanction criminal conduct in cyberspace. It does not require defining norms for non-criminal behaviour online. We consider there is value in learning from other criminal justice treaties which have been successful where they have focused on core criminal issues, alongside broad international cooperation provisions and support to build capacity in all member states.

- The language of an eventual convention must be practical, **technology-neutral and future-proofed** to the extent possible in order to ensure that it stands the test of time and does not require constant revisions. This means we will need to focus on the activity rather than the particular form or method used to carry out that activity.

- It would be premature at this stage to determine what may be required in terms of an **implementation mechanism** for a convention. There are a wide range of models to consider, but this aspect of the treaty can be parked until the scope of the instrument and its objectives are more clearly defined.

Objectives

- The primary purpose of the new instrument should be a **harmonised, modern and effective global framework for cooperation and coordination** between states to tackle the growing threat

posed by cybercrime to individuals, business, critical infrastructure and governments. It should include the provision of support and technical assistance for all states to develop capacity and capability to respond to these challenges. This will increase states' ability to respond effectively to cybercrime nationally, regionally and internationally.

- This means the treaty needs to support **cooperation of national law enforcement, prosecution and judicial agencies bilaterally or multilaterally in preventing, investigating and prosecuting the offences set out in the treaty.** This is critical to combat cybercrime given its transboundary nature means cybercrime often involves perpetrators and victims based in multiple jurisdictions. Common understanding of what constitutes criminal offences in the context of cyberspace, and what offences should be punishable in domestic jurisdictions will help facilitate this, particularly if complemented by consistent frameworks for accessing and sharing digital evidence with international partners with appropriate safeguards.

- The use of powers to investigate and prosecute offences set out in the treaty must be subject to **effective safeguards** in relation to human rights and fundamental freedoms, as set out in existing international treaties. Safeguards must also exist to ensure mutual co-operation powers are used fairly and appropriately, and allow states to refuse cooperation when certain standards are not met. In addition, we consider that the treaty must recognise the independence of national law enforcement and prosecutorial agencies, and that the decision on whether to take action lies solely with those agencies in respective member states.

- Effective international cooperation is best achieved through a **widely-supported** treaty. New Zealand considers that this requires the treaty negotiations to be **inclusive and transparent** with best endeavours made to reach consensus so as to secure the strongest possible mandate for the convention. All member states should be able to share their views and engage meaningfully in negotiations supported by the expertise and perspectives of civil society, industry and other relevant stakeholders. The perspective of indigenous peoples, including Māori in Aotearoa New Zealand, as well as other minority groups should be included, along with the potential impact of cybercrime and efforts to combat it on such groups.

- International cooperation to combat cybercrime is not as effective as it could be. This is not due to a lack of will from member states, but rather from a lack of capacity or expertise. **Technical assistance and capacity building** for law enforcement institutions is a critical requirement and the convention needs to support development of capacity and capability globally.

Structure

- We look forward to hearing the views of other states in relation to the scope and objectives of the Convention through this process and at the first negotiating session in January 2022. Following this we anticipate a clear path forward in terms of structure will emerge rapidly.