NEW ZEALAND
FOREIGN AFFAIRS & TRADE

New Zealand Ministry of
Foreign Affairs and Trade
Manatu Aorere

1. New Zealand is pleased to respond to the invitation from the Chair of the Ad Hoc Committee requesting proposals relating to:

- Provisions on criminalisation;
- General provisions; and
- Provisions on procedural and law enforcement measures.

2. The deadline for submitting proposals was a challenging one to meet. Accordingly, New Zealand's submission focuses primarily on criminalisation provisions. We also provide general comments relating to general provisions and provisions on procedural and law enforcement measures. We look forward to engaging further on all issues during the second and subsequent negotiating sessions.

Striving for consensus: a convention that gains universal acceptance is in all our interests

3. During the first session of the Ad Hoc Committee we heard a diverse, and at times divergent, range of views on what this convention should or could include. We also heard widespread agreement that this process needs to be inclusive, and the outcome needs to gain universal acceptance to ensure it is an effective convention. Further, we have limited time. The roadmap agreed during the first session is an ambitious programme of work. The deadlines for member states to develop positions and respond to proposals is very tight, requiring an immense amount of resource. It will be at times particularly difficult for smaller delegations, including our own, to meet those timeframes.

4. With this context in mind, New Zealand believes we must be sharply focused on areas where we can best hope to achieve comprehensive agreement. Searching for areas of consensus will give us the best chance of building a universal instrument – therefore an effective one – and the best chance of finalising a convention within the mandated timeframes.

Criminalisation provisions

5. During the first session we heard widespread support for, and no opposition to, the inclusion of provisions targeting cybercrime within this convention, particularly cyber dependent crimes and a limited range of cyber enabled crimes.

6. At Annex 1 of this document we propose a list of criminalisation provisions that New Zealand believes have the greatest likelihood of achieving consensus and should therefore be the focus of the Ad Hoc Committee's attention given limited resources and limited time. We also provide some text suggestions to assist with drafting, primarily drawn from other relevant international instruments such as the United Nations Convention against Transnational Organized Crime (UNTOC), the United Nations Convention against Corruption (UNCAC), and the Council of Europe Convention on Cybercrime (Budapest Convention).

7. New Zealand supports including a provision on **jurisdiction** that mirrors, where applicable, existing instruments, such as article 42 of UNCAC, with additional elements requiring states to exercise jurisdiction where the offence or any part of the offence is committed in the territory of the state party, to reflect the reality that cybercrimes may be committed in cyberspace, with the possibility that the perpetrator, victim, data, and computer system used are in different jurisdictions.

General provisions

8. In our view, the general provisions should consist of:

- **Purpose –** Developing an effective treaty will be best served by taking a coherent, realistic, and focused approach in determining our objectives. In New Zealand's view our purpose should be to develop a harmonised, modern and effective global framework for cooperation and coordination between states to tackle the growing threat posed by cybercrime to individuals, businesses and governments. This includes the provision of support and technical assistance for all states to develop capacity and capability to respond to these challenges.
- **Scope of application –** Likewise, the scope of application should be targeted and clearly defined. The chair's proposal in CRP8 provides a good basis for determining the scope of the convention.
- **Agreed definitions** – Definitions should be precise, unambiguous, future proof, and where possible based on relevant existing international and regional instruments.

- A comprehensive instrument must also include a general provision that emphasises the **protection of human rights and fundamental freedoms and respect for the rule of law,** taking into particular account the perspectives of women, children, indigenous peoples, and vulnerable groups.

9. We have also heard from a number of states that the inclusion of a provision relating to **state sovereignty** is important to them. We would note that the application of any such provision in the context of this convention must take into account some critical features that distinguish cyberspace from the physical realm. In particular: i) cyberspace contains a virtual element which has no clear territorial link; ii) cyber activity may involve cyber infrastructure operating simultaneously in multiple territories and diffuse jurisdictions.

Provisions on procedural and law enforcement measures

10. Contingent on the inclusion of comprehensive safeguards to ensure the protection of human rights and fundamental freedoms, respect for the rule of law, and adherence to the principle of proportionality, New Zealand supports including in this convention provisions that would enable swift preservation and access to digital evidence. For example, provisions relating to:

- **Search and seizure of targeted and relevant stored computer data**;
- **Real time collection of targeted and relevant computer data**;
- **Interception of targeted and relevant computer data**;
- **Preservation of targeted and relevant computer data**;
- **Production orders for specified computer data in a person's possession or control, which is stored in a computer system or a computer-data storage medium.**

11. New Zealand would also support the inclusion of provisions which ensure that criminals do not profit from their crimes, such as the **seizure and confiscation of proceeds of crime**, and provisions that would **enhance cooperation with law enforcement authorities**.

Annex 1 – Criminalisation provisions

Illegal access to computer systems

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Illegal interception of computer data

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Interference with computer data

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Interference with the functioning of computer

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Misuse of devices or computer programs

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
   a) the production, sale, procurement for use, import, distribution or otherwise making available of:
      i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with [relevant articles];
      ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with the intent that it be used for the purpose of committing any of the offences established in [relevant articles]; and
   b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in [relevant articles]. A Party may require by law that a number of such items be possessed before criminal liability attaches.
2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with [relevant articles], such as for the authorized testing or protection of a computer system.
3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Criminalisation of cyber-extortion

New Zealand would support the inclusion of a provision that criminalises:
1) The extortion of a user of a computer system to unlock data;
2) The extortion of a user of a computer system with threats of the unauthorised release of data or personal information.

New Zealand looks forward to working with colleagues to develop precise language for this offending.

Computer related Fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a) any input, alteration, deletion or suppression of computer data,
b) any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Computer related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Sexual exploitation of children using computer systems

We look forward to working with colleagues to develop effective and comprehensive criminalisation provisions relating to combating online sexual exploitation and abuse of children.

At a minimum, such offending should include offences relating to the use of a computer system to:

a) produce child sexual exploitation material;
b) offer or make available child sexual exploitation material;
c) distribute or transmit child sexual exploitation material;
d) procure child sexual exploitation material for oneself or for another person;
e) possess child sexual exploitation material.
f) groom children for the purposes of sexual exploitation.

Posting or distributing an intimate visual recording without consent

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law the transfer, sending, publishing, disseminating, or otherwise communicating, by means of a computer system, without reasonable excuse, an intimate visual recording of a victim—
   a) knowing that the victim has not consented to the posting; or
   b) being reckless as to whether the victim has consented to the posting.

For clarity, a child or young person under the age of 16 years cannot consent to the posting of an intimate visual recording of which they are the subject.

Participation and attempt

1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence, in accordance with its domestic law, participation in any capacity such as an accomplice, assistant or instigator in an offence established in accordance with this Convention.
2. Each State Party may adopt such legislative and other measures as may be necessary to establish as a criminal offence, in accordance with its domestic law, any attempt to commit an offence established in accordance with this Convention.
3. Each State Party may adopt such legislative and other measures as may be necessary to establish as a criminal offence, in accordance with its domestic law, the preparation for an offence established in accordance with this Convention.

Liability of legal persons

1. Each State Party shall adopt such measures as may be necessary, consistent with its legal principles, to establish the liability of legal persons for participation in the offences established in accordance with this Convention.
2. Subject to the legal principles of the State Party, the liability of legal persons may be criminal, civil or administrative.
3. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offences.

4. Each State Party shall, in particular, ensure that legal persons held liable in accordance with this article are subject to effective, proportionate and dissuasive criminal or non-criminal sanctions, including monetary sanctions.
5. Legal persons shall be protected from liability for an act done or omitted to be done in good faith—
   a) in the performance or intended performance of a duty imposed by or under this convention; or
   b) in the exercise or intended exercise of a function or power conferred by or under this convention.

Criminalisation of money laundering

1. Each State Party shall adopt, in accordance with fundamental principles of its domestic law, such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally:
   a) (i) The conversion or transfer of property, knowing that such property is the proceeds of cybercrime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her actions;

      (ii) The concealment or disguise of the true nature, source, location, disposition, movement, or ownership of or rights with respect to property, knowing that such property is the proceeds of cybercrime;
   b) Subject to the basic concepts of its legal system:
      (i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of cybercrime;
      (ii) Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.
2. For purposes of implementing or applying paragraph 1 of this article:
   a) Each State Party shall seek to apply paragraph 1 of this article to the widest range of predicate offences;
   b) Each State Party shall include as predicate offences [relevant crimes established in relevant article of this Convention and] the offences established in accordance with [relevant articles] of this Convention. In the case of States Parties whose legislation sets out a list of specific

predicate offences, they shall, at a minimum, include in such list [a comprehensive range of offences associated with cybercrime];

c) For the purposes of subparagraph (b), predicate offences shall include offences committed both within and outside the jurisdiction of the State Party in question. However, offences committed outside the jurisdiction of a State Party shall constitute predicate offences only when the relevant conduct is a criminal offence under the domestic law of the State where it is committed and would be a criminal offence under the domestic law of the State Party implementing or applying this article had it been committed there;

d) Each State Party shall furnish copies of its laws that give effect to this article and of any subsequent changes to such laws or a description thereof to the Secretary-General of the United Nations;

e) If required by fundamental principles of the domestic law of a State Party, it may be provided that the offences set forth in paragraph 1 of this article do not apply to the persons who committed the predicate offence;

f) Knowledge, intent or purpose required as an element of an offence set forth in paragraph 1 of this article may be inferred from objective factual circumstances.

Obstruction of justice

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally:

a) The use of physical force, threats or intimidation or the promise, offering or giving of an undue advantage to induce false testimony or to interfere in the giving of testimony or the production of evidence in a proceeding in relation to the commission of offences covered by this Convention;

b) The use of physical force, threats or intimidation to interfere with the exercise of official duties by a justice or law enforcement official in relation to the commission of offences covered by this Convention. Nothing in this subparagraph shall prejudice the rights of States Parties to have legislation that protects other categories of public officials.

Annex II - Definitions

"computer system" means any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

"computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer to perform such a function.

'child sexual exploitation material' shall mean any material, including in the form of images, video, or live steam, that depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child for primarily sexual purposes.

"property" shall mean assets of every kind, including digital assets, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in, such assets.