SINGAPORE

CONTRIBUTION ON GENERAL PROVISIONS, CRIMINALISATION, AND PROCEDURAL MEASURES AND LAW ENFORCEMENT

1. This written contribution sets out Singapore's views and drafting suggestions on the general provisions, criminalisation and law enforcement, and procedural measures and law enforcement, and is without prejudice to any future contributions that Singapore may make during the course of negotiations.

GENERAL PROVISIONS

Terminology and definitions

2. The definitions of terms to be used in the Convention should be made clear at the outset. In particular, there are two key terms which have been proposed to describe the subject matter of the Convention, namely 'cybercrime' and 'use of ICTs for criminal purposes'. The term 'cybercrime' is widely accepted to include cyber-dependent and cyber-enabled crime. The second term 'use of ICTs for criminal purposes' would cover a wide spectrum of communication technology-related issues beyond the scope of 'cybercrime'.

3. Singapore is of the view that the Convention should be based on the term 'cybercrime', as it is a widely-accepted term that covers the current and emerging cybercrime threats that Member States are facing. This will sharpen the focus of the Convention on the crimes which are specific to or enabled by cyberspace, and will enable a more pragmatic approach to dealing with these threats.

4. There were also deliberations in the first session on whether 'prevent and combat' or 'counter' should be used in the Convention. Singapore prefers to use "prevent and combat", which has been used in previous instruments, including United Nations Convention Against Transnational Organised Crime ("UNTOC").

Data Privacy

5. Data privacy considerations should be balanced against the need to ensure public safety, including combatting cybercrimes to ensure online safety, and allowing enforcement agencies to take necessary action to combat cybercrime quickly and effectively.

CRIMINALISATION AND LAW ENFORCEMENT

6. The Convention should also include cyber scams (which are cyber-dependent or cyber-enabled) as these make up a disproportionate percentage of all fraud in today's world. In Singapore alone, victims of scams lost at least S$633.3 million in 2021, with scam cases increasing by 52.9 per cent from the year before and making up more than half of all crimes. Scam syndicates are well-resourced and make use of technology to commit scams across national boundaries and to cover their tracks.

7. Singapore's drafting suggestions are set out in in Table 1 below. We believe that these suggestions form a realistic and reasonable starting point on how key cyber scams can be targeted in this Convention.

Table 1

Illegal access 1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, the access to the whole or any part of a computer system without right.

2. A State Party may require that the offence be committed by infringing a security measure, with the intent of obtaining computer data or other dishonest intent, such as to assume the identity of another person, or in relation to a computer system that is connected to another computer system.

Cyber fraud
Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally and without right, the causing of a loss of property to another person or an entity by:

(a) any input, alteration, deletion or suppression of computer data,
(b) any interference with the functioning of a computer system,
(c) using a computer system to deceive or induce another person or an entity to do or omit to do anything which the person or entity would not otherwise do or omit to do,

with fraudulent or dishonest intent of procuring for oneself or for another person, without right,

(i) an economic benefit; and/ or
(ii) computer data or personal information that would not otherwise be made available to the perpetrator.

Illegal access to passwords and credentials
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 procurement, obtaining, receiving or distribution of passwords or access credentials to a computer system or computer data without right.

PROCEDURAL MEASURES AND LAW ENFORCEMENT

Preservation, collection, obtaining and sharing of electronic evidence and data

8. On the preservation, collection, obtaining and sharing of electronic evidence and data, we would like to make three points:

    i) With more data being stored in the cloud and more transactions being carried out digitally, criminal investigations, especially in relation to cybercrime, predominantly involve digital evidence. Investigations and prosecutions will be hindered if digital evidence is not preserved, collected and obtained in a timely manner.

    ii) Requests via existing channels for digital evidence, such as via Mutual Legal Assistance Treaties ("MLAT"), involve lengthy processes. If digital evidence is not preserved, collected and obtained in a timely manner, there is a high likelihood that such evidence will be overwritten by the time countries decide to accede to the MLAT request. We thus support the need for measures on lawful requests for the expedited preservation of data.

    iii) Cybercrime is transnational in nature. Technological advancements have enabled criminals to carry out their activities remotely and across national borders. Provisions for cross-border sharing of electronic evidence and data will allow our law enforcement agencies to obtain actionable leads for their investigations, as well as facilitate the successful apprehension and subsequent prosecution of criminals and the recovery of assets. The Convention should allow Parties the option to reject requests if the execution of the request is likely to prejudice the sovereignty, security, public order or other essential interests of the requested Party.

9. In addition, we note that Member States have different legal systems and circumstances which could ultimately affect their ability to implement procedural measures, especially those related to the real-time collection and interception of data. We note that in most cases of cybercrime, the inclusion of measures to preserve, collect, obtain and share electronic evidence and data would already significantly benefit investigation processes, particularly in a multilateral treaty that has broad support from States. We should thus avoid being too prescriptive in terms of operational processes so that the provisions of the Convention are applicable for most

States, thus allowing for wider accession/ratification. This can then allow us to tackle cybercrime more effectively in a concerted manner globally.

Asset Recovery

10. Singapore has heard from many Member States on the need for an Asset Recovery mechanism. We support this. Cybercrime groups run sophisticated transnational operations which are not easy to detect or dismantle. They are well-resourced and adept at using technology to cover their tracks. When criminal proceeds have already been transferred out of a country, recovery is often very difficult.

11. This Convention therefore provides the opportunity to implement concrete, timely, efficient and concerted global measures to recover assets, since any country's ability to recover criminal proceeds that have already been moved out of their jurisdiction would depend on the cooperation from overseas law enforcement agencies. It is important that countries work together on asset recovery so that criminal organisations do not benefit from their criminal proceeds and grow in capability, capacity and sophistication.