Japan

Contribution on International Cooperation, Technical Assistance, Preventive Measures, Mechanisms of Implementation, Final Provisions and Preamble

1 International Cooperation

1.1 General Principles

1.1.1 Japan believes that we should strive for "a free, fair and secure cyberspace" and enhance our capability to prevent and combat cybercrime all over the world by making the new international convention universal, practical and agreeable to all Member States. As with other chapters, the provisions on international cooperation should avoid duplication with existing international instruments and established frameworks, and should be discussed in terms of provisions that need to be included in the Convention in the context of combating cybercrime. In addition, the content of the international cooperation provisions is linked to the content of the criminalization provisions, and should be reexamined as future discussions on the criminalization provisions take place. This contribution is without prejudice to any future contributions Japan may make in the course of future discussions, including on the present chapters.

1.1.2[i] A State Party receiving a request for assistance should determine, in as transparent and timely a fashion as possible and respecting the urgency and sensitivity of the request, whether it has the capabilities, capacity and resources to provide the assistance requested, and then respond to the request. It is desirable to stipulate this way of response as a general principle; this is particularly important for combating cybercrime because the extent of damage and destruction of evidence in cybercrimes are much severer than in conventional types of crimes.

1.1.3 We could consider stipulating that States Parties shall cooperate with each other, in accordance with the provisions of the chapter of international cooperation, and through the application of relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible 1) for the purposes of investigations or proceedings concerning criminal offenses related to computer systems and data, or 2) for the collection of evidence in electronic form of a criminal offense.

1.2 Extradition

1.2.1 In order to bridge gaps between Member States in the investigation and prosecution of cybercrimes committed across borders, Japan supports the introduction of provisions allowing extradition for the crimes set out in this Convention.

1.2.2 In order to ensure the effectiveness of the Convention, Japan could support the introduction of a provision on *aut dedere, aut judicare*. However, in order to avoid undue burden on States Parties, the obligation to submit the case to their own competent authorities for prosecution should, at minimum require that: 1) the requested State Party has jurisdiction under its domestic laws and regulations and 2) the requesting State Party has requested that the case be submitted to the competent authorities of the requested State Party for prosecution.

1.3 Mutual Legal Assistance

1.3.1 General Principles

We could consider stipulating that States Parties shall afford one another mutual legal assistance to the widest extent possible 1) for the purpose of investigations or proceedings concerning criminal offenses related to computer systems and data, or 2) for the collection of evidence in electronic form of a criminal offense. This assistance could include: taking evidence or statements from persons; effecting service of judicial documents; executing searches and seizures; examining objects and sites; providing information and evidentiary items; and identifying, freezing, tracing proceeds of crime.

1.3.2 Specific Mutual Legal Assistance

The Ad Hoc Committee can consider including provisions for mutual legal assistance regarding expedited preservation of stored computer data, expedited disclosure of preserved traffic data, accessing of stored computer data, and the real-time collection of traffic data. The Convention may also stipulate that necessary procedures under such mutual legal assistance should be initiated without undue delay, and States Parties shall make reasonable efforts to process the requests within a timeframe set out in the Convention.

1.3.3 Return of Proceeds of Crime

Money laundering using crypto assets and extortion against companies using ransomware and other malware are new phenomena resulting from the development of cyberspace,

while causing great harm to society. International cooperation on the return of proceeds of crime is considered critical to combating those crimes. Consideration could be given to introducing provisions for the recovery of proceeds of crime similar to those of the United Nations Convention against Transnational Organized Crime (UNTOC) and the United Nations Convention against Corruption (UNCAC).

1.3.4 Communications between the Central Authorities

Such mutual legal assistance should be able to be provided directly through the communications between the central authorities of States Parties. Additionally, we could consider stipulating that the central authorities may communicate by means such as email under certain conditions, e.g. when an appropriate level of security and confidentiality is ensured.

1.3.5 Grounds for Refusal

At minimum, a requested State Party, in responding to a request for assistance, should be able to decline to render assistance if there are grounds for refusal similar to those set forth in Article 46, paragraph 9 (b) and paragraph 21 of the UNCAC.

1.3.6 Spontaneous Information

Considering that cybercrimes can be committed transnationally, it is necessary to avoid situations where one State Party has significant information on investigations or proceedings of cybercrimes that are conducted by another State Party, but the latter State Party conducting the investigations or proceedings is not aware of this fact, so that no request for mutual legal assistance is made and the offender escapes punishment. In light of this, it is desirable to stipulate that a State Party may, within the limits of its domestic law and without prior request, forward to another State Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving State Party in initiating or carrying out investigations or proceedings concerning criminal offenses established in accordance with this Convention or might lead to a request for assistance by that State Party under this chapter.

1.4 Transfer of Sentenced Persons

The system of transfer of sentenced persons is not directly related to crime prevention or investigation; its main purpose is to improve the rehabilitation environment for prisoners after the completion of investigation and prosecution procedures. Thus, it is not

appropriate to include the transfer of sentenced persons in this Convention, which is elaborated to combat specific types of crimes. Japan is opposed to the inclusion of such a provision in this Convention.

1.5 Transfer of Prosecution

Given the wide variety of cultural and social conditions and different judicial systems among the Member States, Japan is opposed to the introduction of a system of transfer of prosecution in this Convention, which aims to be concluded by as many countries as possible.

1.6 24/7 Network

1.6.1 It will be beneficial that the Convention stipulates that each State Party shall designate a 24/7 point of contact in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense. With regard to communications between 24/7 contact points, we should consider an effective use of networks based on existing international instruments and other frameworks.

1.6.2 Cybercrimes include those that pose a significant and imminent risk to the life or safety of individuals. Japan believes that a fast track procedure clause, which states that States Parties may request prompt mutual legal assistance if they are of the view that an emergency exists and that the requested State Party must respond to the request as quickly as possible, is necessary to respond to ongoing emergencies caused by a cybercrime.

1.7 Role of the International Criminal Police Organization (INTERPOL) and Other Organizations

The Ad Hoc Committee should consider stipulating provisions that give the International Criminal Police Organization (INTERPOL) and other organizations beneficial roles in investigating and prosecuting cybercrime with regard to international cooperation, without undermining existing efforts.

2 Technical Assistance

2.1 In the fight against transnational cybercrime, it is critical not to create safe havens for cybercrime. In order to increase the effectiveness of the Convention, it would be helpful to introduce a provision that encourages States Parties to cooperate in technical guidance or assistance and support for capacity building.

2.2 Technical assistance could cover, for example, the following areas: 1) developing and implementing domestic laws and regulations on cybercrime investigation and prosecution, and training of law enforcement officials; 2) assisting the implementation of the Convention, including the provision on training for law enforcement officials to facilitate extradition and mutual legal assistance and the establishment of 24/7 contact points; and 3) raising awareness of cybercrime among the private sector and the public.

2.3 The Ad Hoc Committee can consider inserting provisions on the specific roles of the United Nations Office on Drugs and Crime (UNODC), INTERPOL, and other organizations in providing technical assistance. The Committee should consider the details of the provisions so that these provisions will be useful in the fight against cybercrime without undermining existing efforts, listening to the opinions of each organization.

3 Preventive Measures

3.1 The provision of infrastructure and platforms in cyberspace currently relies heavily on the private sector. As the private sector plays an important role in the prevention of cybercrimes, it is worth considering introducing a provision on preventive measures that would encourage States Parties to provide awareness-raising and training for or with the support of the private sector. However, the provision on preventive measures should clearly define the role of States Parties and should not impose obligations on the private sector, nor should Internet governance be addressed under this Convention.

3.2 The Convention, for instance, could provide that each State Party shall take appropriate measures, such as ensuring the public has effective access to information and

undertaking public information activities, within its means and in accordance with fundamental principles of its domestic law, to raise public awareness regarding the threat posed by cybercrime. The Convention could also stipulate that each State Party shall take such measures as may be necessary to encourage, in accordance with its domestic law, cooperation between national investigating authorities and entities of the private sector, in particular Internet service providers and platformers, relating to matters involving the commission of offenses established in accordance with this Convention.

3.3 It would also be effective to promote, through a provision of this Convention, States Parties to consider 1) analyzing, in consultation with the scientific and academic communities, trends in cybercrime in its territory, the circumstances in which cybercrime operates, as well as the professional groups and technologies involved and 2) developing and sharing analytical expertise concerning cybercriminal activities with each other and through international and regional organizations. It is desirable that such analyses consider the different impacts of cybercrime on gender and the impact of cybercrime on vulnerable groups, including children.

4 Mechanisms of Implementation

In order for States Parties to make the best use of their respective resources to combat cybercrime, it is important to avoid duplication of efforts under other international instruments and to consider truly necessary implementation mechanisms. Such mechanisms would enable the following efforts:

- Facilitating the exchange of information among States Parties on patterns and trends in cybercrime and on successful practices for preventing and combating it;
- Establishing a framework for voluntary collection of information on good practices and challenges related to the implementation of the Convention;
- Cooperating with relevant international and regional organizations and non-governmental organizations; and
- Preparing templates for request forms and other documents to facilitate and streamline cooperation within the framework of international cooperation.[ii]

5 Final Provisions

5.1 It can be considered to allow reservations or declarations to the extent necessary to make this Convention acceptable to as many countries as possible. It is also conceivable that the Convention includes a provision on protocols so that the Convention could be supplemented by protocols to be developed in the future on issues that need to wait for international and domestic discussions to mature. It is appropriate that these issues be considered at the final stage of the Ad Hoc Committee's negotiation, as necessary.

5.2 If two or more States Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they should also be entitled to apply that agreement or treaty or to regulate those relations accordingly, to the extent that is not inconsistent with the Convention's objectives and principles.

6 Preamble

Japan believes that the preamble should include the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights and the consideration of existing international instruments and international cooperation frameworks.

****

[i] cf. Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security (A/76/135) para. 53.
[ii] cf. ibid. para. 54.