Japan

Contribution on Criminalization, General Provisions, and Procedural Measures and Law Enforcement

1 Criminalization

1.1 Cyber-Dependent Crimes

1.1.1 Japan recognizes that there is general consensus in the Ad Hoc Committee on the criminalization of cyber-dependent crimes, which consist mainly of offences that violate the confidentiality, integrity and availability of computer data and systems. Based on this recognition, Japan supports the criminalization of cyber-dependent crimes.

1.1.2 We believe that many of the acts that need to be criminalized to address today's challenges to which each Member State attaches importance, such as ransomware attacks and attacks on computer systems of critical infrastructure, are in the range of cyber-dependent crimes. Such cyber-dependent crimes could include illegal access, illegal interception, interference with computer data or computer systems, and misuse of devices among others.

1.1.3 Japan recognizes the importance of countermeasures against attacks on the computer systems of information infrastructures and facilities. However, since these attacks, such as theft or alteration of data through hacking, can be considered within the scope of cyber-dependent crimes, there is no need to deal with these offences as issues specific to information infrastructures or facilities. Also, as it is important to make the forthcoming convention applicable for the long-term future, it should be noted that provisions on criminalization will lose its versatility if they are too focused on individual modus operandi. Furthermore, it is important that this new convention stipulates basic and essential provisions that could be complied with and implemented by as many Member States as possible. In light of this, the discussion should start with common cybercrimes such as illegal access. It should be carefully considered whether or not it is necessary to establish a specific provision for attacks on computer systems of information infrastructures and facilities in addition to provisions on common cybercrimes in order to avoid duplication among provisions on criminalization.

1.1.4 In addition, it is necessary to avoid the risk of a chilling effect on legitimate operations and activities, such as technology development, or abuse of power by law enforcement authorities caused by an overly broad scope of criminalization. For example, when criminalizing illegal access, it may be required that there be no legitimate reason for the access and awareness of that in order to avoid imposing absolute liability.

1.1.5 Furthermore, mandating uniform punishment for attempted crimes or aiding and abetting crimes, or mandating punishment at the stage of preparation or conspiracy that is not sufficient to constitute an attempt, would be an excessive interference with the domestic criminal legislation of individual states. The criminalization of these offenses should be left to the national legislation of each Member State. Regarding countermeasures against cybercrimes that have a transnational nature, it is very important not to create a safe haven for cybercrime. Therefore, it is necessary to avoid stipulating such provisions that limit the number of Member States that can conclude the new convention due to differences in the basic legal concepts that inevitably exist among Member States.

1.2 Freedom of Expression

1.2.1 In considering the criminalization of activities in cyberspace, reference should be made to international human rights treaties. In determining what acts can be criminalized as cyber-enabled crimes under the new convention, particularly with regard to the criminalization of acts related to harmful content on the Internet, Member States must not forget the importance of protecting freedom of expression.

1.2.2 For example, article 19, paragraph 2, of the International Covenant on Civil and Political Rights stipulates that freedom of expression “shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.” While keeping in mind that article 19, paragraph 3 provides for certain restrictions to the right, we must ensure that there is room for the development of domestic laws considering the actual situation in each Member State so that the rights and freedoms relating to academic research, cultural and artistic activity, and press are not unjustly infringed upon.

1.2.3 In order to protect freedom of expression, it is necessary to avoid causing a chilling effect on expressive activities. Therefore, criminalization of acts related to harmful content on the Internet should be undertaken only to the extent that all Member States can agree on the definition of such acts, and that there are demonstrable grounds for the need for punishment.

1.2.4 In order to make this convention a treaty that as many Member States as possible can conclude, and to await for the discussions to ripen internationally as well as nationally, we believe that one of the most promising options would be to leave the criminalization of acts pertaining to harmful content to a future additional protocol.

1.3 Conventional Crimes Exploiting Cyberspace

1.3.1 Regarding crimes related to terrorism, firearm-related offences and drug-related offences, they may constitute conventional crimes even when they are committed via the use of the Internet, and existing treaties such as the United Nations Convention against Transnational Organized Crime (UNTOC) may also apply.

1.3.2 Criminalization of these acts should be carefully considered, so as not to duplicate above-mentioned existing efforts. Reference should also be made to the discussions during the process of formulation of existing treaties, so that provisions that were intentionally not included in them will not simply be incorporated in this convention in a different form.

1.4 Possible Cyber-Enabled Crimes to be considered

With regard to cyber-enabled crimes other than those regarding harmful content (See 1.2 above), some cyber-enabled crimes that are recognized as significant to be criminalized as cybercrimes under this convention could be subject to discussion on criminalization, under the premise that all Member States can agree on a definition of such acts and that there are demonstrable grounds for the need for punishment. Such cyber-enabled crimes include those whose scope and speed and scale of damages are increased by the use of computers. These crimes may include offences as follows.

1.4.1 Computer-Related Forgery

It is difficult to detect computer data forgery with the human senses. Moreover, in today's world where many business processes are carried out by computer, the social impact of undermining trust in computer data is significant. Therefore, Japan could support the criminalization of the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data, when committed intentionally and without right.

1.4.2 Computer-Related Fraud

Computer data fraud, when perpetrated through the forgery of computer data or through interference with the functioning of computer systems, is easy to perpetrate against a wide range of targets and can cause serious property damage in many Member States. Therefore, we could support the criminalization of the causing of a loss of property to another person by any input, alteration, deletion or suppression of computer data, or any interference with the functioning of a computer system with fraudulent or dishonest intent of procuring.

1.4.3 Infringements of Copyright

On the Internet, data can be copied and content can be reproduced easily, and such content spreads fast, which can increase the degree of copyright infringement. We believe that it would be beneficial to criminalize the infringement of copyright and related rights where such acts are committed willfully, on a commercial scale and by means of a computer system, with reference to existing international agreements related to copyright.

1.4.4 Child Sexual Abuse and Exploitation

The production and distribution of child sexual abuse materials are extremely malicious acts that have a harmful effect on the mental and physical health of depicted children and seriously infringe upon their human rights. It is difficult to delete child sexual abuse materials once they have been disseminated through the Internet, and they will continue to have a serious impact on the sound upbringing of the children. From the perspective of protecting human rights of children, we support the criminalization of the production and distribution of materials that visually depict a child engaged in sexually explicit conduct.

Nevertheless, we believe that careful consideration should be given to treating realistic images representing a person appearing to be a minor or a non-existing child engaged in sexually explicit conduct as child sexual abuse materials and criminalizing offences related to these images, taking into account that an existing minor is not subject to direct abuse as well as the importance of freedom of expression.

1.5 Liability of Legal Persons

We support stipulating the liability of legal persons to a certain extent in cases where such legal persons organization-widely committed cybercrimes with regard to the business of them under the conditions that the liability may be criminal, civil, or administrative subject to the legal principles of each Member State. The division of roles among criminal,

civil, and administrative matters and the necessity of sanctions are issues that should be left to the domestic legislation of each Member State, as they need to be considered in light of each Member State's national structure and the parity with governance outside the cyber sector in each Member State.

2 General Provisions

2.1 Statement of Purpose

We support the three objectives outlined in the Chair's proposal at the first session of the Ad Hoc Committee: 1) to promote and strengthen measures to prevent and combat cybercrime; 2) to promote, facilitate, and strengthen international cooperation; and 3) to provide practical tools to enhance technical assistance and build the capacity of national authorities.

2.2 Use of Terms

From the viewpoint of creating a convention that will be effectively utilized for a long period of time, the terms used in this convention need to be clearly defined in a technology-neutral manner. For example, it would be inappropriate to establish definitions for technologies that are constantly changing, such as "botnet."

Therefore, definitional provisions should be established in as general and clear manner as possible and to the extent necessary, while referring to existing international instruments such as the UNTOC. We believe that this perspective applies equally to discussions on other parts of this convention, such as provisions on criminalization.

2.3 Scope of Application

2.3.1 The scope of the application of this convention should be clearly stated based on the provisions of UNTOC and United Nations Convention against Corruption (UNCAC).

2.3.2 Cybersecurity and Internet governance should not be addressed in this convention. For example, the following measures would have a chilling effect on legitimate economic activity and would impede the development of technology, and would go beyond the mandate of the Ad Hoc Committee:

- setting security standards under this convention;

- imposing obligations on legal persons and individuals to comply with such standards or imposing penalties for violation of such standards; or
- holding legal persons, their representatives, or software creators who unintentionally engaged in cybercrimes committed by other actors without awareness, accountable.

3 Procedural Measures and Law Enforcement

3.1 Regarding procedural measures for cybercrime investigations, consideration could be given to providing for the expedited preservation, search and seizure of stored computer data, production order, and real-time collection of traffic data.

3.2 We could consider applying these procedural provisions to investigations and criminal proceedings for the criminal offences established in this convention and other criminal offences committed by means of a computer system, and to the collection of evidence in electronic form of a criminal offence.

3.3 In granting the above-mentioned authority to competent authorities of each Member State, it is necessary to establish provisions confirming that each Member State should ensure that the rights arising in accordance with obligations under human rights treaties and others, as well as other human rights and freedoms, are appropriately protected and that domestic legislations which include the principle of proportionality are followed. This convention should confirm this concept in the chapter on procedural measures and law enforcement.

****