Japan's Response to the Guiding Questions regarding Agenda Item 4

A. First group of questions

Question 1:

Regarding interception, punishing all interceptions of communications would lead to excessive criminalization, since radio communications can be easily received by anyone. Therefore, it is appropriate to limit the scope of punishment by, for example, requiring that interception be conducted "with dishonest intent."

With regard to illegal access, it should be required that there are no legitimate reasons for access and that there is an awareness of it, in order 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 as a result of an overly broad scope of criminalization.

In addition, granting special protection only to cybersecurity researchers would not only raise the issue of definition but also make it difficult to define the scope of protection, because there may be researchers and technicians in other fields who are eligible for protection as well. Therefore, we should properly define what constitutes the crime, such as dishonest intent, and should not limit the scope to cybersecurity researchers so that no one will be punished unjustly.

Question 2:

In terms of data interference, it is unnecessary to require material damage as a prerequisite for establishing an offense. Although we do not preclude the possibility of making material damage an additional requirement at the discretion of each country, it is appropriate to leave the content of such a requirement to each country's domestic legislation.

Question 3:

The infringement of security measures should be considered as a condition for establishing crimes under the first group. For example, regarding illegal access, many countries have already established domestic laws on hacking, but their scopes and conditions for establishing the crime may vary. In order for the Convention to be ratified by many countries, it should be required that the object of hacking be limited to computer systems that are not intended

for unauthorized access and can be attacked through a network connection. In this way, we could avoid discussions on the definition of hacking, and easily separate it from legal access. In other words, the provisions should allow for the addition of requirements such as "the access was made by infringing security measures," and when an offense is committed in relation to "a computer system that is connected to another computer system."

Question 5:

Japan recognizes the importance of countermeasures against attacks on computer systems of information infrastructures and facilities. However, since these attacks can be considered within the scope of cyber-dependent crimes, we do not have to deal with these offenses as an issue specific to information infrastructures or facilities.

Question 10:

The substantive basis for punishing interference with computer data is to protect the integrity and proper functioning or use of stored computer data or computer programs, thereby ensuring the credibility of the computer data. Therefore, criminalizing copying as a type of interference with computer data is unsupportable because copying has no such basis.

B. Second group of questions

Question 2:

An overly broad scope of criminalization could cause a chilling effect on legitimate operations and activities, such as technology development, or cause an abuse of power by law enforcement authorities. In order to avoid such risks, it should be required that computer forgery be done with the intent to mislead others' operations, so as not to impose absolute liability. Although it is not necessary to require malicious or dishonest intent beyond the intent to mislead, we do not object to a proposal to require such an element.

Granting special protection only to cybersecurity researchers would not only raise the issue of definition, but would also make it difficult to define the scope of protection, as there may be researchers and technicians in other fields who are also eligible for protection. Therefore, we should precisely define what constitutes the crime, such as dishonest intent, not limiting the scope to cybersecurity researchers, so that no one will be punished unjustly.

Question 3:

We should not consider the proposed provisions on "creation and use of digital information to mislead the user" as a form of computer-related forgery. In this context, offenses related to harmful contents should not be criminalized under this Convention, as further careful consideration on whether and how to criminalize such kinds of acts is needed. Japan strongly opposes the criminalization of the creation and use of disinformation, since it is difficult to reach consensus on the definition of disinformation, and its criminalization could lead to the destruction of free speech and journalism through government control of information.

Question 4:

We would like to consider the issue based on specific proposals suggesting elements that constitute identity-related offenses, but in general, it is not necessary to establish separate provisions in this Convention for cases where a crime is committed as a cybercrime, because many cases can be treated as traditional crimes.

Question 5:

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. It would be beneficial to criminalize the infringement of copyright and related rights when such acts are committed willfully, on a commercial scale and by means of a computer system, with reference to existing international instruments on copyright.

C. Third group of questions

Question 1:

From the perspective of protecting children's rights, Japan supports the criminalization of the production and distribution of child sexual abuse materials that visually depict minors engaged in sexually explicit conduct under the Convention.

On that basis, Japan believes that careful consideration should be given to treating materials, which visually depict a person appearing to be a minor engaged in sexually explicit conduct and realistic images representing a non-existing child engaged in sexually explicit conduct as child sexual abuse materials, moreover, criminalizing offenses related to such materials, as we should take into account the fact that an existing minor is not subject to direct abuse as

well as the importance of freedom of expression.

We are aware that the term “child sexual abuse material” has replaced “child pornography” in many fora mainly because “child pornography” implies that the child consented to its production and undermines the nuance that it is sexual exploitation and abuse. With this in mind, Japan uses “child sexual abuse material” in its written contribution. Japan is open to discuss appropriate terminology and is ready to listen to the opinions of Member States, observers and multi-stakeholders.

In addition, restrictions on freedom of expression regarding audio recordings and writings should be minimal, therefore the scope of child sexual abuse material must be examined carefully. In this regard, “pornography” traditionally refers to objects that can be recognized by sight, and whether “child sexual abuse material” includes audio recordings and writings should be carefully considered.

Question 2:
If access to or viewing of child sexual abuse material constitutes a crime, it would be difficult to determine whether or not there is a justifiable reason, and the scope of punishment would become too broad. If that is the case, even unintentional access would be punishable. Therefore, Japan opposes obligatory punishment without, at least, considering the domestic law of each country.

Questions 4-6:
Japan does not support criminalization of offenses that are mentioned in Questions 4-6 in this Convention. For example, sexual extortion and blackmail by threatening to distribute sexual images can be punished as traditional forms of crimes even if they are exchanged via the Internet, and careful consideration is needed as to whether they should be treated under this Convention to avoid a long list of crimes.

D. Fourth group of questions
Questions 1-4:
Some of the offenses addressed in the questions can constitute traditional crimes, even if they are committed via the Internet. Criminalization of these acts should be carefully considered,

so as not to duplicate existing efforts.

Regarding cyber-terrorism, even if the target of cyber-terrorism is the core system of critical infrastructure, the act of cyber-terrorism itself, such as attacking by manipulating a computer, is considered a cyber-dependent crime. Therefore, we do not have to give cyber-terrorism and its relevant acts an independent provision.

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. In order to protect freedom of expression, it is necessary to avoid causing a chilling effect on expressive activities. What is considered harmful content in this context varies depending on the cultural, social, and political background of each country and the people who come into contact with the contents. It is inappropriate to criminalize acts related to harmful content in this Convention, and it should be regulated through domestic legislations of each Member State.

E. Fifth group of questions

Question 2:

Mandating uniform punishment for all 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 in the domestic criminal legislation of individual states. The criminalization of these offenses should be left to the domestic legislation of each Member State.

Question 3:

We support holding legal persons liable, up to a certain extent, when these offenses have been committed by the organization as a whole with regard to their business, under the condition that they are liable either criminally, civilly or administratively according to the legal principles of each Member State.

In the meantime, establishing a provision to hold corporations, their representatives, or software developers liable who are not intentionally involved in cybercrimes themselves may have a chilling effect on legitimate economic activities and inhibit the development of technology.

Question 4:

The Convention could use the wording on the liability of legal persons contained in Article 10 of the UNTOC for guidance. A separate offense punishing the negligence of legal persons in maintaining the necessary security measures would not be needed under this Convention because it would be a matter of cybersecurity and Internet governance and would go beyond the mandate of the Ad Hoc Committee. We should also be aware that criminalizing such an act would have a chilling effect on legitimate economic activities and would impede the development of technology.

Question 5:

Since the new Convention should only provide for criminalization, and leave the legal penalties and sentencing to the discretion of each State Party, the Convention should not provide for grounds for aggravating or mitigating circumstances. However, as in Article 30 paragraph 1 of the UNCAC, a general provision on "sanctions that take into account the gravity of that offense" could be considered.