Japan’s Response to the Guiding Questions regarding Agenda Item 6

Question 32:
While it is important that not only a state but also the private sector, civil society, and NGOs jointly stand up to cybercrime, the preventive measures under the Convention should be clearly distinguished from measures under criminal procedures, and should clearly define the role of the state. The Convention, for instance, could stipulate that each Party shall take appropriate measures, such as ensuring the general 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 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 relating to matters involving the offenses established in accordance with this Convention. When we consider these measures, it is desirable to take into account the different impacts of cybercrime on gender and the impact of cybercrime on vulnerable groups, including children.

Questions 33 and 34:
Currently, the supply of infrastructure and platforms in cyberspace 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 Parties to provide awareness-raising and training for or with the support of the private sector.

The Convention could also stipulate that each 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 offenses established in accordance with this Convention.

Furthermore, it would also be effective to promote, through this Convention, Parties to consider 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. This Convention is not intended to set standards of security or cybersecurity, and we do not believe that it is appropriate to discuss cyberattacks targeting critical infrastructure in particular at the Ad Hoc Committee. Still, we believe that the points mentioned earlier are
also applicable as preventive measures against such cyberattacks.

**Question 35:**
We oppose including a provision to designate a national authority responsible for preventing cybercrime because the institutions and structures of each Party for the prevention of cybercrime are diverse, and efforts to prevent crime range in different fields. Therefore, it is not appropriate to require to designate such an authority.

**Question 36:**
Our answer to this question is no. Internet governance should not be addressed in this Convention, and we should be cautious in establishing security standards and sanctions for their violations. Whether to impose sanctions on the private sector with respect to security standards and the division of criminal, civil, and administrative roles in such cases should be left to the domestic legislation of each country because these issues need to be considered in light of each Party’s state structure and consistency with the governance in other sectors.

**Question 37:**
As Article 13 of the UNCAC stipulates, the Convention could provide that each Party shall take appropriate measures, such as ensuring the general 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.