

Japan

Japan, as a Member State which attaches importance to realizing an inclusive, transparent and fair process for the drafting of the forthcoming UN convention on cybercrime, is pleased to provide inputs for the new convention before the formal drafting begins and appreciates the Chair's initiative in providing this opportunity.

Although different States face different cybercrime challenges, Japan recognizes that cybercrime is a constantly evolving and common serious threat for all Member States. In order to combat cybercrime, which easily transcends national borders, it is vital to ensure that each Member State cooperates with one another. Therefore, Japan believes that we should aim to ensure "a free, fair and secure cyberspace" and enhance our capability to prevent and combat cybercrime all over the world by making the substance of the new international convention universal and agreeable for all Member States.

These inputs outline Japan's views on the scope, objectives and structure of the new convention so as to promote discussion within the Ad Hoc Committee established by General Assembly resolution 74/247.

Scope

1. In order to strengthen global measures to combat cybercrime and to establish a universal international framework, the international community should, in the first place, develop a solid framework, focusing on basic and essential provisions of criminal offences, criminal procedure as well as mutual legal assistance and other international cooperation in this field.
2. The acts which the new convention criminalizes should be limited to cybercrime; the offences established in the new convention should foremost cover cyber-dependent crimes, and cyber-enabled crimes should be covered only where it is necessary and there is broad consensus among Member States.
3. The new convention should be firmly based on previous and current discussions in the existing frameworks for combating cybercrime, while taking into account the discussions and works in other fora related to discussions on cybercrime, with the aim of avoiding duplication or undermining of the works.
4. In order to establish a universal international framework which is generally applicable to every kind of usage of information and communication technologies irrespective

of differences between States, and to respond to the future development of technologies, the provisions in the new convention should be formulated in a way that is technology-neutral.

5. Despite the significance of combatting cybercrime, the measures against cybercrimes must not be detrimental to the principle of due process or impose unjustifiable restrictions on human rights. Such safeguards are preconditions for successful international cooperation, and therefore the new convention should include concrete provisions for ensuring due process and human rights.

Objective

6. The primary objective of the new convention should contribute to the safety and security of everyone related to information and communication technologies who should be protected and the protection of their interests. This can be achieved by globally enhancing measures against cybercrime through establishing a universal international framework with the broadest application to cybercrime in its various transnational forms and assisting effective bilateral or multilateral cooperation in criminal investigations and prosecutions.
7. In order to achieve this objective, the new convention should stipulate basic and essential provisions, which could be complied and fulfilled by as many Member States as possible, and thereby raise the worldwide level of measures against cybercrime, strengthening the existing frameworks.

Structure

8. Japan believes that the following basic structure would be effective in organizing the new convention, but supports being flexible regarding a more detailed structure in the upcoming negotiations:
 - Definition of terms
 - List of domestic measures which Member States should adopt
 - Criminalization
 - ◇ Offenses categorized as cyber-dependent crimes
 - ◇ Offenses which should be criminalized among cyber-enabled crimes
 - Procedural provisions regarding the preservation, disclosure, and

production of data

- Safeguards for securing human rights and other interests
- International cooperation in extradition, mutual assistance, and other forms of cooperation
- Final provisions