Agenda Item 6: Provisions on preventive measures

With respect to Q32, Singapore suggests that the chapter on preventive measures can broadly cover the following:

a) Development of a National Cybercrime Action Plan to establish and promote best practices and policies aimed at the prevention of cybercrime.

b) Promoting public education and awareness on cybercrimes and cybercrime prevention measures.

c) Fostering international and regional cooperation with other States as well as International Organisations, industry and academia for capability building and sharing of knowledge, best practices and solutions concerning cybercrime.

d) Increasing cybercrime awareness in the private sector and encouraging the private sector to develop capabilities to respond to the latest cyber threats.

On Q33, critical infrastructures perform important functions and provide essential services to government, businesses and citizens. Disruptions to their functions can affect livelihoods, cause widespread instability, and even undermine public trust and confidence. The reality is that cybercrime today can be and is often perpetrated across borders. In addition, as the world becomes increasingly digitalised and connected, there are a growing number of supranational systems that support services critical to the good functioning of the internet, international trade, financial markets, global transport, communications, health or humanitarian action.

While attacks on critical infrastructures are of major concern globally, the question of how to prevent such cyber-attacks suggests establishing and implementing certain security standards, which encroach into the cybersecurity domain. Such cybersecurity concepts should be dealt with in their respective fora.

As the focus of this Convention is on the criminal justice response to cybercrime, we can address this from the angle of deterrence. This Convention could provide for enhanced punishment in cases of cyber-attacks on critical infrastructure.

This Convention can also allow for measures to facilitate urgent cooperation amongst states on criminal activities that target critical infrastructures providing essential services, especially supranational information infrastructures that operate across national borders. These
measures could include commitments to share information in a timely manner to facilitate cross-border law enforcement action, as well as mitigation and remediation action.

On Q34, Singapore is of the view that States parties can take measures to cooperate with civil society, the private sector and academia in the areas of capability building, as well as sharing of knowledge, best practices and solutions concerning cybercrime.

As for Q35, on whether this Convention should provide for the designation of a national authority responsible for preventing and combatting cybercrime, Singapore can be flexible. However, we would like to flag that in many countries, this national authority will likely be a different agency from the Central Authority for MLA and extradition matters. Countries may also have a different agency responsible for cybersecurity. This separation of duties will need to be catered for.

On Q36, Singapore notes that at the first session, there was wide consensus not to impose obligations on the private sector in this Convention. Singapore is and continues to be aligned with this view.

Preventive measures in relation to the private sector under this Convention should instead focus on encouraging and strengthening public-private partnership in the context of capability building, sharing of knowledge, best practices and solutions concerning cybercrime, as well as raising public awareness on cybercrimes. We can also agree to provisions encouraging private sector stakeholders to develop capabilities to protect against and respond to the latest cyber threats.

As for Q37, this Convention can provide for States parties to increase cybercrime awareness in the private sector and encourage private sector stakeholders to develop capabilities to protect against and respond to the latest cyber threats. This Convention can also encourage States to promote public education and awareness on cybercrimes and cybercrime prevention measures.