Check against delivery

SINGAPORE'S STATEMENT
SECOND SESSION OF THE AD HOC COMMITTEE TO ELABORATE A COMPREHENSIVE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES FOR CRIMINAL PURPOSES
VIENNA, 30 MAY TO 10 JUNE 2022

Agenda Item 4: Provisions on criminalisation

As Singapore and many Member States have highlighted at the first session, the Convention should, first and foremost, focus on cyber-dependent crime. The scope of cyber-enabled crime is broad and can potentially include any type of traditional crime that can be committed through the use of computer systems or online.

The inclusion of cyber-enabled crimes will thus pose implementation challenges, and inevitably dilute the focus on cybercrime. Given the large number of crimes that can qualify as cyber-enabled crimes, we envisage that a large amount of time and effort may need to be spent to reach consensus on the types of such crimes that should be covered by the Convention. This will be a great concern for many Member States.

However, there are certain cyber-enabled crimes, which, given their severity, propensity for amplification through ICT as well as in the public interest, should be included in the Convention and tackled at the international level in a concerted manner. One such example is cyber scams, which could be cyber-dependent or cyber-enabled, and make up a disproportionately high percentage of all fraud in today. Scam syndicates are well-resourced and make use of technology to commit scams across national boundaries and to cover their tracks.

While cyber scams continually evolve in modus operandi, the conduct of such scams, which is by deception for economic benefit or to obtain access credentials or personal information, should be clearly targeted in the Convention. The illegal use or distribution of such credentials or personal information typically following such scams should similarly be marked, given the downstream implications and potential damage to victims.

Singapore has provided drafting suggestions in our written contributions, which we believe form a realistic and reasonable starting point to achieve this.

The inclusion of other types of cyber-enabled crimes would need to be deliberated carefully and should be approached with restraint.

Thank you.