Speech by SJ at plenary session of 13th China-ASEAN Prosecutors-General Conference in Vietnam (English only) (with photos)

Following is the speech by the Secretary for Justice, Mr Paul Lam, SC, at the plenary session of the 13th China-ASEAN Prosecutors-General Conference in Vietnam today (December 6):

Mr Chairman, Your Excellencies, distinguished guests, ladies and gentlemen,

I am very honoured to have been invited to attend the 13th China-ASEAN Prosecutors-General Conference as a member of the Chinese delegation and also the head of the delegation of the Hong Kong Special Administrative Region (HKSAR) of the People's Republic of China. It gives me great pleasure to address this distinguished audience on the important and timely topic of strengthening international co-operation in the prevention and fight against cybercrimes and transnational crimes.

Before I do so, may I thank Your Excellency Mr Le Minh Tri, Prosecutor General, Supreme People's Procuracy of the Socialist Republic of Vietnam, for the generous hospitality and assistance that have been provided to the Hong Kong delegation since our arrival. I must also congratulate Your Excellency on the arrangements which have been made to ensure the success of this important conference.

The changing face of crime in the 21st century

Technology is advancing at an unprecedented pace. And in recent years we have seen a sharp increase in the number of crimes featuring a technological dimension. In Hong Kong alone, the number of reported cybercrime cases has increased four times over the past six years, from around 5 500 in 2017 to over 22 000 in 2022. The amount of financial loss resulting from such cases has also increased, from around HK$1,393 million in 2017 to a staggering HK$3,215 million in 2022.

Apart from inflicting economic loss and causing substantial harm to individuals and businesses, technological or high-tech crimes pose a real and serious threat to national security. The cyberspace presents risks of unauthorised access and organised attacks on national information systems, and may be exploited as a means through which political agendas endangering national security may be pursued.

Technology has enabled crimes to transcend jurisdictional boundaries. A cyber-criminal in one jurisdiction may cause criminal acts to be committed in multiple jurisdictions. Evidence may be stored on computers or electronic devices in jurisdictions other than the one in which the illegal act is

committed. In addition, the Internet allows communications to circle the globe instantaneously and often anonymously.

Challenges brought about by transnational technology crimes

In my view, there are four principal challenges brought about by the transnational high-tech crimes.

First, high-tech crimes call into question the adequacy of existing criminal laws in this respect. Existing laws may be inadequate in terms of both the substance and the extraterritorial effect. Offences currently enforced under the existing criminal laws may be inadequate in criminalising the wide spectrum of cyber-related misconduct. And the existing offences may also lack extraterritorial effect, the enforcement of which would require laws of different jurisdictions to maintain a proper balance between complying with public international law principles and ensuring the effective sanction of transnational crime. The absence of extraterritorial application of existing cybercrime offences are liable to make them ineffective in combatting high-tech crimes which involve a transnational character.

The second challenge brought about by high-tech crimes is that they are very often much more difficult to detect than traditional crimes. Cyber-criminals are very good at using a variety of techniques to avoid detection. Coupled with the ease with which they can hide their identities in the virtual world, law enforcement agencies often face considerable challenges in detecting high-tech crimes and identifying the true criminals. Furthermore, investigations are easily hindered in case where evidence is scattered across multiple jurisdictions, or where there is inadequate or a lack of timely information and intelligence exchange.

Third, cases of transnational technology crimes often involve evidence from overseas witnesses. Therefore, we need to ensure the evidence obtained from overseas jurisdictions will be admissible and acceptable in the court of law. And even where all the necessary evidence has been successfully gathered, witnesses may not be prepared to testify against the defendant, in particular where to do so would necessitate physical attendance in overseas criminal proceedings.

Fourth, high-tech crimes may involve specialised knowledge such as cloud computing, the metaverse, and the Dark Web – areas which are also under constant development and changes. And our investigators and prosecutors may lack sufficient knowledge to catch up with the latest developments in this area in order to handle such cases competently and efficiently.

Building an international co-operative network for effectively fighting transnational technology crimes

In the light of these challenges, closer cross-jurisdictional co-operation between law enforcement and prosecutorial agencies in fighting transnational high-tech crimes is of crucial importance.

I would venture to suggest and highlight four corresponding aspects on

which we should focus our joint efforts.

Comprehensive legal frameworks criminalising cyber-related conduct

First, the establishment of a comprehensive legal framework to criminalise cyber-related misconduct. Up-to-date legal framework is an indispensable pre-requisite for successfully fighting technology crimes. We should consider to enact new laws to criminalise cyber-related misconduct and to make appropriate amendments to our existing substantive and procedural laws. Concerted effort should be made to ensure that our laws will have extraterritorial application to cater or tackle cyber offences insofar as necessary.

In this regard, experience sharing among jurisdictions will be beneficial and conducive to the development of a more updated and comprehensive legal framework.

In 2022, the Law Reform Commission of Hong Kong, following a comprehensive study of the laws of seven jurisdictions, recommended an enactment of a piece of bespoke legislation on cybercrime, which will introduce five new offences criminalising conduct such as illegal access to computer programmes and interception of computer systems. To allow for sufficient deterrent effect, a maximum sentence of 14 years' imprisonment is recommended. Extraterritorial application of Hong Kong law on high-tech crimes is proposed in cases where the crime has connections to or has caused serious damage to Hong Kong.

In addition, the Prosecutions Division of the Department of Justice of Hong Kong has recently established the new Technology Crime Sub-Division – a dedicated team of prosecutors who specialise in handling and prosecuting technology crime cases. These prosecutors work closely with cyber and forensic experts and the Police's Cyber Security and Technology Crime Bureau. At present, the prosecutors from the Sub-Division are in the course of reviewing the adequacy and effectiveness of existing laws in combatting high-tech crimes.

International co-operation by law enforcement agencies

Second, international co-operation by law enforcement agencies. We must work to strengthen international co-operation among law enforcement agencies of different jurisdictions. Multilateral information sharing and intelligence exchange relating to the identity and whereabouts of suspects, the movement of crime proceeds, trends and patterns of criminal activities, and the operation of criminal groups are of valuable assistance in the detection and investigation of technological crimes, in particular where they have an international dimension. Timely information and intelligence exchange may be achieved by arranging overseas postings of law enforcement officers to other jurisdictions, and making multilateral co-operative arrangements. To this end, insofar as Hong Kong is concerned, existing arrangements are in place for external co-operation with law enforcement agencies, including the Hong Kong Police Force, the Independent Commission Against Corruption, and the Customs and Excise Department.

Cross-jurisdictional measures facilitating effective prosecution

Third, cross-jurisdictional measures to facilitate effective prosecution. Efforts should be made to ensure, insofar as possible, the implementation of cross-jurisdictional measures to facilitate effective prosecution. They will include mutual legal co-operation arrangements between jurisdictions, including mutual legal assistance in criminal matters (MLA) and surrender of fugitive offenders.

The importance of MLA regimes in enabling efficient and effective investigations cannot be overemphasised. MLA arrangements are particularly pertinent to cases of transnational high-tech crimes, as they involve evidence located in more than one jurisdiction. To ensure timely preservation of relevant evidence, jurisdictions should jointly liaise and communicate, as far as possible, to ensure operational efficiency in the rendering of MLA, whether pursuant to formal MLA agreements or informal arrangements between jurisdictions on an ad hoc basis.

In this regard, we must not allow geopolitical considerations to hinder international co-operation. It is most unfortunate that since the enactment of the Law of the People's Republic of China on Safeguarding National Security in the HKSAR, a number of western countries have suspended MLA arrangements with Hong Kong. Such acts are against the common interests of the HKSAR and those other jurisdictions, and will limit our collective capacities to fight transnational crime.

Efforts should also be made to devise specific mechanisms to enable the taking of oral testimony from witnesses located abroad. Such mechanisms are instrumental in cases where witnesses are not prepared to travel overseas to give evidence. For Hong Kong, there is a provision in our criminal procedural law empowering criminal Courts to, in appropriate cases, grant permission for witnesses to give evidence by way of a live television link from a place outside Hong Kong.

Robust training and development initiatives

Fourth, robust training and development initiatives. In order to successfully fight transnational high-tech crimes, we must equip ourselves with sufficient knowledge of the subject matters involved.

Joint training programmes on topics related to high-tech crimes, which may be delivered either in person or virtually, or both, would facilitate knowledge and experience exchanges. Insights can also be gained by these activities by exploring how law enforcement and prosecutorial agencies can better organise their institutional structures and daily operations to maximise capacity, resources, and the ability to tackle emerging high-tech crimes.

Regular international conferences and symposiums, such as the present conference, along with meetings and working groups may also be organised.

The Government of the HKSAR is committed to safeguarding the digital

world and promoting the prevention of high-tech crimes. In September this year, Hong Kong held the International Symposium on Cyber Policing, bringing together more than 100 leaders of law enforcement agencies from around 40 jurisdictions, as well as academics and experts in digital communications, finance, innovation technology, and cyber security. Looking ahead, the HKSAR will host the 11th Asia and Pacific Regional Conference of the International Association of Prosecutors in November 2024, to discuss pertinent issues relating to the prosecution of technological crimes. I look forward to welcoming you all, and to further exchanging ideas on how we can strengthen our efforts to combat technology crimes on an international level.

Concluding remarks

In conclusion, the fight against transnational high-tech crimes is bound to be very challenging. The fight can only be won if governments join hands to take effective measures locally, regionally, and globally, to strengthen co-operation at all levels and among all relevant agencies. As the saying goes, "Alone we can do so little, together we can do so much". On the part of the HKSAR, I am sure and I would undertake that all branches of our Government will continue to promote international co-operation to combat high-tech crimes in all ways possible. We shall ensure that our world, whether physical or virtual, will not become a safe haven for cyber-criminals.

On this note, may I once again congratulate the Supreme People's Procuracy of the Socialist Republic of Vietnam for holding this important conference. My gratitude also goes to all the distinguished speakers for sharing their valuable insights and experience. Thank you very much.