PROSECUTING CYBERCRIME : THE SINGAPORE EXPERIENCE

Speech by Attorney-General of the Republic of Singapore, Lucien Wong, S.C.

11th China-ASEAN Prosecutors-General Conference
Brunei Darussalam, 14 August 2018

It is my honour and privilege to share with you about Singapore's experience – and especially, the experience of our Attorney-General's Chambers – in combating cybercrime.

2 Singapore is an extremely 'wired' nation, with many of our citizens and residents making heavy use of technology and the Internet in their daily lives, including their transactions with Government agencies. In fact, statistics suggest that many Singaporeans even live part of their lives online – a recent study showed that 70% of Singaporeans are active social media users, more than double the global average of 34%. Singapore also has the sixth highest Internet penetration rate in Asia, at 83.6%, although we trail behind our hosts Brunei, who are top in Asia with 93.6%!

3 Against that backdrop, it would be no surprise that cybercrime is a matter of great concern in Singapore. Just last month, it was announced that SingHealth, Singapore's largest group of healthcare institutions, had been hacked. The hackers succeeded in stealing the personal particulars and other information belonging to 1.5 million patients – including our Prime Minister, Mr Lee Hsien Loong. This is by far the

largest hacking incident to have taken place in Singapore, and a Committee of Inquiry has been convened.

4 However, while the SingHealth hack may grab the headlines, it is only the tip of the cybercrime iceberg. According to figures released by our Cyber Security Agency, cybercrime in Singapore has increased over the last three years. In 2014, 7.9% of all crimes in Singapore were cybercrimes, but by 2017 that proportion had more than doubled, to 16.6% of all crimes. In other words, one in six crimes committed in Singapore is a cybercrime.

5 Despite this worrying trend, we know that we must keep moving forward in our embrace of technology. One of Singapore's national objectives is to become a 'Smart Nation', in order to improve the lives of our people, and create greater economic opportunities. It is thus imperative that we equip ourselves to combat cybercrime, and our Attorney-General's Chambers has always striven to be at the forefront of that fight.

6 I would like to share with you two key pillars of our Chambers' approach to dealing with cybercrime: *legislation* and *specialisation*. These two things go hand-in-hand. Our legislative frameworks provide the foundation for our specialist prosecutors, equipped with the necessary expertise and experience, to robustly and effectively prosecute cybercriminals.

7 First, *legislation*. Without the necessary legislative frameworks in place, our police and prosecutors may well not have the procedural tools with which to effectively investigate and prosecute cybercrimes. Indeed, there may also be situations where clearly objectionable conduct might not even constitute an offence, in the absence of appropriate offence-creating provisions and legal definitions.

8 In Singapore, we have endeavoured to keep our laws up-to-date, to keep pace with technology's changing and growing role in society. As far back as 2006, numerous amendments were made to our Penal Code, to ensure that traditional crimes such as forgery would also encompass the 'electronic' mode of committing such offences. For example, the definitions of 'document' and 'writing' were amended to explicitly include electronic documents and modes of writing. Another round of amendments to the Penal Code is in the pipeline, which will include more updates to ensure our criminal laws are in line with technological advances.

9 More recently, in 2017, the Computer Misuse and Cybersecurity Act was amended, to introduce new offences for dealing in hacked personal information, and for possessing hacking tools. The extraterritoriality provision of the Act was also expanded, in recognition of the fact that computer hacking offences committed entirely overseas can cause, or create a significant risk of, harm in Singapore.

10 In recent years, entirely new laws have also been introduced, to ensure that offending conduct online can be prosecuted and punished. For example, the Remote Gambling Act was introduced in 2014 to specifically deal with online gambling, in response to the 'modernisation' of traditional illegal gambling syndicates.

11 In the same year, the Protection From Harassment Act was also introduced. Prior to its enactment, our harassment offences only applied to acts in the real world, but with the growing use of social media and other online methods of communications, a pressing need was identified to extend harassment offences to cyberspace. A new offence of stalking – unfortunately, something that has become increasingly frequent online – was also introduced.

12 Our procedural laws have also been updated. The Evidence Act was amended in 2012, to do away with outdated and cumbersome requirements for admitting computer output as evidence, and to replace these with presumptions regarding the authenticity of electronic records. More recently, just this year, amendments were passed to our Criminal Procedure Code, to lay the legislative groundwork for empowering police to require production of evidence in machine-readable formats, which can be more readily analysed by investigators and prosecutors; and to clearly define police investigators' powers to access computer data remotely, as well as to compel relevant persons to assist in accessing computer data.

13 At the same time, existing traditional criminal laws have also had to be employed to deal with new forms of offending behaviour online, especially *content crime* involving the publishing of objectionable material online. In recent cases, offenders have been prosecuted for online postings that incited violence against foreigners and public servants. In another high-profile case in 2015, a husband-and-wife couple were convicted and jailed for eight and ten months, respectively, for offences under the Sedition Act, which dates from before Singapore's independence. They had published xenophobic and untrue content on a website that they operated, that promoted hostility between different races in Singapore. Investigations revealed that their motive was simply to make money, by attracting readers to their website with their inflammatory and fabricated articles. In short, our Chambers already had to deal with 'fake news', four years ago.

14 In fact, depending on what is recommended in a Parliamentary Select Committee report that is to be released later this year, on deliberate online falsehoods and their impact on society, legislation to deal with 'fake news' may well be something that Singapore considers in the future.

15 The second key pillar is *specialisation*. Since the earliest cybercrime prosecutions in the 1990s, our Chambers has always sought to identify prosecutors with the particular aptitude and interest in technology that makes them suitable for handling

cybercrime cases. However, such officers were ‘ad hoc’ specialists, who would be called into action as and when they were needed.

16 Then, in 2012, we formalised that specialisation, with the formation of the Technology Crime Unit (TCU). Today, the TCU is part of the Financial and Technology Crime Division. It is headed by two Senior Directors who collectively have over 40 years of experience in handling cybercrime, and who lead a team of 14 prosecutors. Officers in the TCU are given special training, including training in digital forensics and other technical areas, and also regularly attend conferences and workshops on cybercrime and cybersecurity, to keep abreast of the latest developments and trends.

17 Besides handling cybercrime cases, the officers of the TCU also employ their specialised knowledge of cybercrime, and information technology in general, in rendering advice to law enforcement agencies on technological issues. This includes legal issues arising from the use of technology in investigative processes, such as the proposed replacement of police investigators’ traditional pocket diaries with tablet devices. TCU officers also serve as resource persons for the rest of the prosecutors in our Chambers, providing advice and guidance when, for example, issues concerning the admissibility and reliability of digital evidence arise in the course of prosecutions.

18 Our TCU officers have also had the privilege and honour of conducting training in countries in ASEAN and elsewhere, in conjunction with foreign counterparts such as

the United States Department of Justice or the Crown Prosecution Service, or with international organisations such as the Commonwealth Secretariat and the United Nations Office on Drugs and Crime. We also collaborate with INTERPOL, who established their Global Complex for Innovation in Singapore, in 2015, which has a particular focus on cybercrime research.

19 The TCU has also built up a strong working relationship with their counterparts in the Singapore Police Force's Technology Crime Branch, as well as a good network of contacts with foreign law enforcement and the technology industry.

20 We have found our approach of having a specialised team of prosecutors dealing with cybercrime and technology-related issues to be extremely effective. Their cumulative experience and expertise allows them to quickly come to grips with the technical details of cases that come their way, especially given that cybercriminals are unceasingly 'innovative' in finding new ways to commit crimes.

21 Indeed, almost immediately after the formation of the TCU in 2012, their officers were tested by a high-profile case involving a hacker who called himself 'The Messiah'. Claiming to be a member of the hacker collective 'Anonymous', 'The Messiah' released a YouTube video, declaring his intention to wage 'cyberwar' on the Singapore Government. He had also hacked into the websites of other organisations, including the main local newspaper and a bank. He was ascertained to be a fugitive Singaporean

hiding in Kuala Lumpur, Malaysia. With the assistance of the Royal Malaysian Police, he was apprehended and brought back to Singapore. Our TCU prosecutors worked closely with police investigators to build the case against him. He eventually pleaded guilty to multiple charges under our Computer Misuse and Cybersecurity Act, and was sentenced to four years and eight months in prison.

22 A crucial factor in apprehending 'The Messiah' was our prosecutors' use of 'open source intelligence' or 'online reconnaissance'. This refers to using the offender's own online footprints to trace and identify him. In 'The Messiah's' case, we were able to find online posts that he had made, boasting about his criminal activities and even offering his services as a hacker-for-hire. Although he always used pseudonyms, we were able to build a compelling case linking him to such content, confirming that he was the perpetrator.

23 In another recent case, our prosecutors used Facebook searches to prove that a foreign accused person, who claimed to be too ill to return to Singapore for his appeal to be heard, was actually perfectly well and sailing the high seas, in his job as a ship captain. From a photo he posted online, we were even able to establish that he had been on a particular ship that passed near Singapore, at a time when he was supposedly recovering at home in Greece! His lawyer was most surprised when we produced this information, which his client had kept from him.

24 Our TCU prosecutors' expertise also feeds back into strengthening our legislation. TCU played a key role in ensuring that legislation such as the Computer Misuse and Cybersecurity Act and Protection From Harassment Act would be effective in dealing with cybercrime. For example, during the drafting of the Protection from Harassment Act, our TCU prosecutors stress-tested the new provisions against real-life scenarios to ensure their effectiveness against online harassment.

25 Having shared with you about our two key pillars of *legislation* and *specialisation*, I would like to end by emphasising the importance of a third key pillar in combating cybercrime: *cooperation*.

26 Given the borderless nature of cyberspace, it is inevitable that much cybercrime takes place across national boundaries. However, unlike the cybercriminals, all of us – as domestic prosecutors – must respect one another's national sovereignty. It is thus vital that we continue to develop close relationships through meetings such as this one, so that we can effectively fight cybercrime together when it cuts across our borders.

27 In particular, time is of the essence when dealing with cybercriminals, who can commit crimes almost instantaneously over computer networks, and just as quickly delete their digital trails. Cooperation between law enforcement and prosecution agencies must be capable of moving just as fast. The identification of 24/7 contact

persons for cybercrime in our respective agencies would, I suggest, be a good step forward.

28 The sharing of best practices and mutual development of cybercrime-fighting capabilities is another aspect of the cooperation that is required to deal with our mutual challenges. It is in furtherance of such cooperation that our Chambers has, for the past two years, hosted the ASEAN Cybercrime Prosecutors' Roundtable Meeting, as part of the annual Singapore International Cyber Week. These closed door meetings have brought together prosecutors from almost all the ASEAN countries, to share their expertise and experiences in dealing with cybercrime. This year's Singapore International Cyber Week, including the third Roundtable Meeting, is to be held on 18-20 September 2018, and we have already sent the invitations to your respective agencies. We look forward to welcoming your delegates to Singapore!