Cybercrime and Cybersecurity in Singapore

I. Introduction

1. The cybercrime situation in Singapore is generally under control, and the primary concerns of law enforcement and legislation are computer-facilitated crimes and content crimes. The first deals with offences such as identity theft, fraud, online gambling, etc. The latter deals with offences such as online harassment, hate speech, etc.

2. There are several pieces of domestic legislation that deal with the above, from traditional penal statutes such as the Penal Code, to the more recently enacted Remote Gambling Act. However, the primary statute used is the Computer Misuse and Cybersecurity Act (“CMCA”).

II. The Computer Misuse and Cybersecurity Act

3. The CMCA was most recently amended in 2013, having been initially adapted from United Kingdom (“UK”) and Australian legislation when first enacted. The law’s main focus is on computer integrity crimes, where the criminal behaviour is largely premised on the lack of authority to access or modify. However, there are provisions that deal with crimes that have been facilitated by computers.

Authority

4. The bulk of the offences under the CMCA are based on the lack of authority of an offender. For example, section 3 of the CMCA criminalises unauthorised access, while section 5 criminalises unauthorised modification. Section 4 criminalises accessing a computer in order to facilitate specified offences.

5. “Authority” is narrowly defined by the section 2(5) of the CMCA, which states:

For the purposes of this Act, access of any kind by any person to any program or data held in a computer is unauthorised or done without authority if —

(a) he is not himself entitled to control access of the kind in question to the program or data; and

(b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled

6. Similar to the UK position, the Singapore Courts have also taken a narrow reading of “authority”, where an unauthorised user can be found guilty of an offence if he abuses that access for an unauthorised purpose.
7. Section 11 of the CMCA allows for extra-territorial effect, where offences are made out as long as the target computer or the accused person is located in Singapore.

8. There are stiff penalties in place for CMCA offences, especially for section 4, which deals with computer-facilitated crime. Notably, if the offences involve “protected computers” such as computers related to national security, public infrastructure, etc, there would be enhanced penalties as provided for by section 9.

Limitations

9. The CMCA focuses on the acts performed to cause computers to perform functions, and emphasises on the individual process and accesses. It also does not allow the amalgamation of multiple acts into a single charge, which makes it not entirely suitable for offences committed over a span of time or involving many computers, e.g. Botnet cases.

10. Currently, the powers of search and seizure are limited to Singapore. However, many computer crimes are cross-border in nature. Also, some evidence required may not be stored locally, but in the cloud. The transnational nature of cybercrime makes international cooperation and mutual assistance an important element in any cybersecurity framework.

III. Other Legislation

11. Even with the prevalence of computer related and facilitated crime, the Prosecution utilises traditional laws as far as possible if they are suitable, even if the offence was computer-facilitated. There have also been recent amendments to existing statutes such as the Penal Code, Criminal Procedure Code and the Evidence Act to provide for the seizure and admissibility of electronic evidence or the commission of offences via electronic means or using digital documents.

12. Despite these changes, there are cases that traditional law cannot cover, such as offences which require the appropriation of physical and moveable property, or require deception of a person as opposed to a computer system. The challenge is in utilising other offences to address such situations and the need for legislative review as new offences surface. As the volume of digital evidence increases, there is also a need for proper procedures in identifying, preserving and understanding such potential evidence.