THE LAW REFORM COMMISSION OF HONG KONG

SUB-COMMITTEE ON CYBERCRIME

CONSULTATION PAPER

CYBER-DEPENDENT CRIMES AND JURISDICTIONAL ISSUES

This consultation paper can be found on the internet at:
<http://www.hkreform.gov.hk>

June 2022

This Consultation Paper has been prepared by the Sub-committee on Cybercrime of the Law Reform Commission. It does not represent the final views of either the Sub-committee or the Law Reform Commission, and is circulated for comment and discussion only.

The Sub-committee would be grateful for comments on this Consultation Paper by 19 October 2022. All correspondence should be addressed to:

The Secretary
Sub-committee on Cybercrime
The Law Reform Commission
4th Floor, East Wing, Justice Place
18 Lower Albert Road
Central
Hong Kong

Telephone: (852) 3918 4097

Fax: (852) 3918 4096

E-mail: hklrc@hkreform.gov.hk

It may be helpful for the Commission and the Sub-committee, either in discussion with others or in any subsequent report, to be able to refer to and attribute comments submitted in response to this Consultation Paper. Any request to treat all or part of a response in confidence will, of course, be respected, but if no such request is made, the Commission will assume that the response is not intended to be confidential.

It is the Commission's usual practice to acknowledge by name in the final report anyone who responds to a consultation paper. If you do not wish such an acknowledgment, please say so in your response.

THE LAW REFORM COMMISSION OF HONG KONG

SUB-COMMITTEE ON CYBERCRIME

CONSULTATION PAPER

CYBER-DEPENDENT CRIMES AND JURISDICTIONAL ISSUES

CONTENTS

Chapter	*Page*
Defined Terms	1
Preface	4
Introduction	4
Terms of Reference	4
Membership of the Sub-committee	5
The scope of the study	6
Three planned parts of the project	7
Methodology adopted for the Sub-committee's study	8
Five cyber-dependent offences to study in Part One	8
Comparative study	8
Guiding principles behind the recommendations	8
Format of this Consultation Paper	9
1. Categorisation of cybercrime	10
Introduction	10
Categorisation at the United Nations' level	10
Categorisation under the Budapest Convention	11
Offences prescribed by the Budapest Convention	11
Model Law on Computer and Computer Related Crime	12
Degree of alignment of the laws in other jurisdictions	12
Latest developments in the United Nations	14
2. Illegal access to program or data	16
Introduction	16
Current Hong Kong law	17

Chapter ***Page***

Crimes Ordinance (Cap 200) 17
Telecommunications Ordinance (Cap 106) 19
Standard of criminalisation under the Budapest Convention 21
Statutory regimes in other jurisdictions 23
Australia 23
Canada 26
England and Wales 28
Mainland China 35
New Zealand 40
Singapore 44
USA 46
The Sub-committee's views 49
Bespoke cybercrime legislation preferable 49
Definition of key terms 49
Outlawing mere unauthorised access 51
Unauthorised nature of an access 53
Access to program or data 53
Defence of reasonable excuse 54
Aggravated offence 55
Model for Hong Kong legislation 55
Recommendation 1 55
Unauthorised access for cybersecurity purposes 56
Recommendation 2 61
Limitation period in summary cases 62
Recommendation 3 62
Criminal liability of officers of a corporate offender 63

3. Illegal interception of computer data 64

Introduction 64
Current Hong Kong law 64
Basic Law 64
Hong Kong Bill of Rights 65
Interception of Communications and Surveillance Ordinance (Cap 589) 65
Telecommunications Ordinance (Cap 106) 67
Standard of criminalisation under the Budapest Convention 69
Two special cases of data at rest 71
"Data at rest" versus "data in motion" 71
Data momentarily at rest during transmission 71
Data stored in a communication system 72
Statutory regimes in other jurisdictions 74
Australia 74
Canada 76
England and Wales 78
Mainland China 81
New Zealand 81

Chapter	*Page*
Singapore	86
USA	89
The Sub-committee's views	95
Outlawing unauthorised interception of computer data	95
Interception for a dishonest or criminal purpose	96
Offence not to be restricted to private communication	96
Offence to cover all data including metadata	97
Offence to apply to data throughout its transmission	98
Model for Hong Kong legislation	98
Recommendation 4	99
Conduct which society may regard as proper investigations	99
Interception by genuine businesses	100
Recommendation 5	102
4. Illegal interference of computer data	103
Introduction	103
Current Hong Kong law	104
Crimes Ordinance (Cap 200)	104
Telecommunications Ordinance (Cap 106)	107
Standard of criminalisation under the Budapest Convention	108
Statutory regimes in other jurisdictions	109
Australia	109
Canada	114
England and Wales	116
Mainland China	121
New Zealand	122
Singapore	126
USA	129
The Sub-committee's views	132
Prohibiting intentional and unauthorised data interference	132
Actus reus	133
Mens rea	134
Lawful excuses	134
Aggravated offence	135
Transposing the offence to the new legislation	135
Recommendation 6	136
5. Illegal interference of computer system	137
Introduction	137
Current Hong Kong law	138
Crimes Ordinance (Cap 200)	138
Standard of criminalisation under the Budapest Convention	141
Statutory regimes in other jurisdictions	142
Australia	142

Chapter ***Page***

Canada 145
England and Wales 147
Mainland China 151
New Zealand 152
Singapore 154
USA 157
The Sub-committee's views 160
Tackling data and system interference consistently 160
New legislation should adopt the existing provisions 161
Possible clarification of "misuse of a computer" 161
Scope of application of the proposed offence 161
Recommendation 7 162
Lawful excuse 163
Recommendation 8 164

6. Making available or possessing a device or data for committing a crime 165

Introduction 165
Current Hong Kong law 166
Crimes Ordinance (Cap 200) 166
Telecommunications Ordinance (Cap 106) 169
Standard of criminalisation under the Budapest Convention 169
Statutory regimes in other jurisdictions 172
Australia 172
Canada 174
England and Wales 176
Mainland China 181
New Zealand 183
Singapore 184
USA 187
The Sub-committee's views 189
New offence with a basic form and an aggravated form should be enacted 189
Devices and data to which the proposed offence should apply 190
Actus reus 192
Mens rea 192
Proposed statutory defence of reasonable excuse 193
Model for the proposed provisions 193
Recommendation 9 194
Possession of data with only harmful use 196
Recommendation 10 197

Chapter *Page*

7. Criteria for the Hong Kong court to assume jurisdiction 198

Introduction 198
General principles on jurisdiction 198
Common law approach 198
Hong Kong legislation prescribing jurisdictional rules 201
Generally accepted bases of extra-territorial jurisdiction 203
Jurisdictional issues associated with cybercrime 203
Challenges presented by cybercrime 203
Judicial recognition of challenges in cybercrime 204
Jurisdictional rules under the Budapest Convention 206
Statutory regimes in other jurisdictions 209
Australia 209
Canada 213
England and Wales 215
Mainland China 217
New Zealand 219
Singapore 221
USA 223
The Sub-committee's views 225
Preliminary considerations 225
Illegal access to program or data 227
Recommendation 11 230
Illegal interception of computer data 230
Recommendation 12 232
Illegal interference of computer data 232
Recommendation 13 233
Illegal interference of computer system 234
Recommendation 14 234
Making available or possessing a device or data for committing a crime 235
Recommendation 15 236

8. Sentencing 237

Introduction 237
Views of Hong Kong court towards cybercrime 237
Current laws in Hong Kong and other jurisdictions 241
The Sub-committee's views 241
The relatively serious proposed offences 241
The proposed summary offence of illegal access to program or data 244
The proposed aggravated offences of illegal interference of computer data and computer system 245
The proposed basic offence of making available or possessing a device or data for committing a crime 245
Recommendation 16 246

Chapter *Page*

9. Consolidated recommendations and consultation questions 248

Introduction 248
Illegal access to program or data 248
Recommendations 248
Consultation questions 249
Illegal interception of computer data 250
Recommendations 250
Consultation questions 251
Illegal interference of computer data 252
Recommendations 252
Illegal interference of computer system 253
Recommendations 253
Consultation questions 254
Making available or possessing a device or data for committing a crime 255
Recommendations 255
Consultation questions 257
Limitation period for summary proceedings 257
Recommendation 257

Appendix 258

Defined Terms

Abbreviation	Definition
Budapest Convention	Council of Europe's Convention on Cybercrime
CCP system	Certified Cyber Professional assured service
Cheng Ka Yee	*Secretary for Justice v Cheng Ka Yee (鄭嘉儀)* (2019) 22 HKCFAR 97, [2019] HKCFA 9
Chu Tsun Wai	*HKSAR v Chu Tsun Wai (朱峻瑋)* (2019) 22 HKCFAR 30, [2019] HKCFA 3
CJO	Criminal Jurisdiction Ordinance (Cap 461)
CMA-EW	Computer Misuse Act 1990 (England and Wales)
CMA-SG	Computer Misuse Act 1993 (Singapore)
DDOS	Distributed denial of service
DNS	Domain name system
Ex parte United States	*R v Bow Street Metropolitan Stipendiary Magistrate, Ex parte United States (No 2)* [2000] 2 AC 216
Explanatory Report	Explanatory Report to the Budapest Convention
Hong Kong	Hong Kong Special Administrative Region
IAF	International Accreditation Forum
ICSO	Interception of Communications and Surveillance Ordinance (Cap 589)

Interpretation No 19/2011	The Interpretation of the Supreme People's Court and the Supreme People's Procuratorate of Several Issues on the Application of Law in the Handling of Criminal Cases about Endangering the Security of Computer Information Systems
IPA	Investigatory Powers Act 2016 (England and Wales)
MCCOC Report	Model Criminal Code Officers Committee, *Report, Chapter 4, Damage and Computer Offences and Amendments to Chapter 2: Jurisdiction* (2001)
Model Law	Model Law on Computer and Computer Related Crime
National Security Law	The Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region
New Zealand Act	Crimes Act 1961 (New Zealand)
NPCSC	The Standing Committee of the National People's Congress
OCMFA	Office of the Commissioner of the Ministry of Foreign Affairs of the People's Republic of China in Hong Kong
PRC	People's Republic of China
PRC Criminal Law	Criminal Law of the People's Republic of China
Russian Convention	*Draft United Nations Convention on Cooperation in Combating Cybercrime* submitted by the Russian Federation to the United Nations on 11 October 2017
SPP's Guiding Cases	Guiding cases issued by the Supreme People's Procuratorate of the PRC
S161	Section 161, Crimes Ordinance (Cap 200)

S27A	Section 27A, Telecommunications Ordinance (Cap 106)
TIAA	Telecommunications (Interception and Access) Act 1979 (Cth) (Australia)
UK	United Kingdom
UNODC	United Nations Office on Drugs and Crime
USA	United States of America
Wong Tak Keung	*HKSAR v Wong Tak Keung* (2015) 18 HKCFAR 62, FACC 8/2014
WTA	Wireless Telegraphy Act 2006 (England and Wales)

Preface

Introduction

1. For many people in the world, information technology, the computer and the internet permeate numerous aspects of their daily life. As we enjoy the convenience brought by technological advances, criminals also utilise them for illicit purposes. In terms of how the criminal law should respond to such abuses, the prevailing view at a global level appears to be that legislation specifically targeted at cyberspace can complement generally applicable legislation.

2. In 2000, the Hong Kong Special Administrative Region Government convened an Inter-departmental Working Group on Computer Related Crime, which conducted the most recent official study of cybercrime in the Hong Kong Special Administrative Region ("**Hong Kong**") to date. With the significant technological and societal developments in the last two decades, the time is ripe for another review of the topic. Against this background, the Chief Justice and the Secretary for Justice referred the topic of cybercrime to the Law Reform Commission of Hong Kong in 2019 for consideration. The Sub-committee on Cybercrime was appointed to examine the current state of the law and to make recommendations.

3. After the Sub-committee had started its deliberations on the topic, the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region ("**National Security Law**") was enacted and applied, as a national law, to Hong Kong by promulgation on 30 June 2020. The duty of Hong Kong to safeguard national security reaffirmed the need for reform of cybercrime laws in Hong Kong[1] and the Sub-committee has taken this into consideration in its pursuit of the cybercrime project.

Terms of Reference

4. The Sub-committee on Cybercrime commenced its study on this topic in January 2019 with the following Terms of Reference:

> *"Having regard to the rapid developments associated with information technology, the computer and internet, and the potential for them to be exploited for carrying out criminal activities, to —*

[1] In addition to the general principles set out in Article 3, Article 9 of the National Security Law provides, in particular, that the Hong Kong Special Administrative Region Government shall take necessary measures to strengthen regulation over matters concerning national security, including the internet.

(a) identify, from a criminal law point of view, the challenges to protection of individuals' rights and law enforcement arising from such developments;

(b) review existing legislation and other relevant measures dealing with the challenges identified in (a) above;

(c) examine relevant developments in other jurisdictions; and

(d) make recommendations on possible law reforms to address the above matters."

Membership of the Sub-committee

5. Composition of the Sub-committee chaired by Mr Allan Leung is as follows:

Mr Allan Leung ***(Chairman)***	Senior Consultant, Dentons Hong Kong LLP
Mr Derek Chan, SC	Senior Counsel
Ms Chan Shuk Yi, Christal	Assistant Director of Public Prosecutions, Department of Justice
Dr Cheng Chung Ngam, Rocky (from 12 January 2022)	Chief Information Officer, Bank of China (Hong Kong) Limited
Ms Cheng Lai Ki, Kelly (from 3 May 2022)	Chief Superintendent, Cyber Security and Technology Crime Bureau, Hong Kong Police Force
Dr K P Chow	Associate Professor, Department of Computer Science, University of Hong Kong
Ms Chui Shih Yen, Joceline (from 12 August 2019)	Principal Assistant Secretary for Security, Security Bureau
Mr Fong Wing Kai, Guy (from 13 December 2018 to 13 September 2020)	Former Group Head (Intellectual Property Investigation (Operations)), Customs and Excise Department

Ms Clara Ho (from 13 December 2018 to 20 December 2020)	Former Head of Resilience Risk, Asia Pacific, The Hongkong and Shanghai Banking Corporation Limited
Dr Michael Kwan	Chief Executive Officer, Asia Pacific Internet Centre
Mr Law Shiu Kai, Andrew (from 13 December 2018 to 13 July 2020)	Former Partner, Robinsons, Lawyers
Dr Law Yuet Wing, Frank (from 13 December 2018 to 12 April 2022)	Regional Commander (Kowloon East), Hong Kong Police Force
Mr Raymond Tang (from 11 January 2021 to 11 January 2022)	Head of Operational and Resilience Risk, Hong Kong and Macau Region, The Hongkong and Shanghai Banking Corporation Limited
Mr Tong Chi-chung, Eddy	Deputy Chief Executive, Consumer Council
Mr Tsang Yue Tung, Andrew (from 13 December 2018 to 9 August 2019)	Former Principal Assistant Secretary for Security, Security Bureau
Miss Wong Pui-kei, Maggie, SC	Senior Counsel
Ms Wong Wai-chuen, Phoebe (from 14 September 2020)	Group Head (Intellectual Property Investigation (Operations)), Customs and Excise Department
Mr Yip Yuk Fai, Lento	Chairman, Hong Kong Internet Service Providers Association

6. The Sub-committee has met regularly since its formation. Miss Cindy Cheuk, Senior Government Counsel in the Secretariat of the Law Reform Commission, is the Secretary to the Sub-committee. Mr Terence Lee, Government Counsel, is also assisting the Sub-committee. Mr Edmund Ma, then Senior Government Counsel, was the Secretary to the Sub-committee until May 2021.

The scope of the study

7. From the early stage of our deliberation, we realise that no

categorisation of cybercrime is universally accepted.

8. Chapter 1 of this Consultation Paper describes how cybercrime has been variously categorised. For the purpose of this Consultation Paper, we have adopted the terminology used by the United Nations Office on Drugs and Crime ("**UNODC**"), which distinguishes between crimes that are "cyber-dependent" and "cyber-enabled" in nature. The following elaboration of the United Kingdom ("**UK**") Government is instructive:[2]

(a) *"cyber-dependent crimes"* are *"crimes that can be committed only through the use of Information and Communications Technology (ICT) devices, where the devices are both the tool for committing the crime, and the target of the crime"*; and

(b) *"cyber-enabled crimes"* are *"traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT"*.

Three planned parts of the project

9. Given the breadth of the Sub-committee's Terms of Reference, as well as the fast-moving international landscape of cybercrime regulation, we have decided to address in stages the issues that arise from this topic. In particular:

(a) Part One of the project addresses cyber-dependent crimes and jurisdictional issues;

(b) Part Two, subject to further discussion in due course on its scope, will cover cyber-enabled crimes and attempt to address the macro challenges in the digital age, including data sovereignty (also known as cyber, digital or technological sovereignty). The essence of data sovereignty is that a place should be able to take autonomous actions and decisions regarding its digital infrastructures and technology deployment. It also relates to efforts in ensuring the security of digital infrastructures and their authority regarding digital communication matters pertaining to their territories and citizens;[3] and

(c) Part Three will deal with evidentiary issues and enforcement (procedural) issues.

---

2 Cabinet Office, National security and intelligence, HM Treasury, and The Rt Hon Philip Hammond MP, *National Cyber Security Strategy 2016-2021* (UK Government, 2016) at para 3.2, available at https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (accessed on 3 May 2022).

3 Julia Pohle & Thorsten Thiel, "Digital Sovereignty", Internet Policy Review: Journal on internet regulation (2020), Vol 9, Issue 4, at 8.

Methodology adopted for the Sub-committee's study

Five cyber-dependent offences to study in Part One

10. This Consultation Paper relates to Part One of the project. Drawing on the Council of Europe's Convention on Cybercrime ("**Budapest Convention**") and the Russian Federation's "*Draft United Nations Convention on Cooperation in Combating Cybercrime*",[4] we focus on the following five cyber-dependent offences which are the core species of cybercrime recognised globally that should be addressed:

(a) illegal access to program or data;

(b) illegal interception of computer data;

(c) illegal interference of computer data;

(d) illegal interference of computer system; and

(e) making available or possessing a device or data for committing a crime.

Comparative study

11. We examine these offences and their associated jurisdictional issues having regard to (a) the requirements under the Budapest Convention, as well as (b) the laws of Hong Kong and seven jurisdictions, namely Australia, Canada, England and Wales, Mainland China, New Zealand, Singapore and the United States of America ("**USA**").[5] Among these jurisdictions, four of them (namely, Australia, Canada, England and Wales, and the USA) are parties to the Budapest Convention whereas four of them (namely, Hong Kong, Mainland China, New Zealand and Singapore) are not.

Guiding principles behind the recommendations

12. We appreciate the need and importance to take into account various stakeholders' different interests and perspectives when we devise our recommendations. Our guiding principles are to balance:

(a) the right of netizens and interests of persons in the information technology industry; and

(b) protection of the public's interest and right not to be disturbed or attacked when using and operating their computer system.

---

4 Details of the Budapest Convention and the "Draft United Nations Convention on Cooperation in Combating Cybercrime" appear in Chapter 1.

5 Federal legislation in the cases of Australia, Canada and the USA.

Format of this Consultation Paper

13. This Consultation Paper consists of the following chapters:

(a) Chapter 1 sets the scene by describing the ways in which international organisations and initiatives have categorised cybercrime.

(b) Chapter 2 starts off with the first of the five cyber-dependent offences falling within Part One of our project, ie illegal access to program or data.

(c) Chapter 3 focuses on the second cyber-dependent offence, ie illegal interception of computer data.

(d) Chapter 4 covers the third cyber-dependent offence, ie illegal interference of computer data.

(e) Chapter 5 moves on to the fourth cyber-dependent offence, ie illegal interference of computer system.

(f) Chapter 6 deals with the fifth cyber-dependent offence, ie making available or possessing a device or data for committing a crime.

(g) Chapter 7 turns to the criteria for the Hong Kong court to assume jurisdiction.

(h) Chapter 8 tackles the issue of sentencing in respect of the cyber-dependent offences above.

(i) Chapter 9 lists our consolidated recommendations and consultation questions.

14. In this consultation exercise, the Sub-committee seeks to consult the public as to whether reform of the criminal law is needed taking into account various offence-creating and other relevant provisions applicable to cybercrime under existing legislation; and if so, what kind of reform is preferable. We seek to engage as much of the public as possible in this consultation exercise and are keen to hear the different voices from all quarters of society. We hope this Consultation Paper would be useful in prompting and facilitating public discussion on the issues raised. We also welcome any views, comments and suggestions on the issues presented in this Consultation Paper. These will greatly assist the Sub-committee's fulfilment of the objectives pursuant to its Terms of Reference.

Chapter 1

Categorisation of cybercrime

Introduction

1.1 As the UNODC observed in its Comprehensive Study on Cybercrime:

> *"… the ubiquity of the internet and personal computer devices means that computer systems or computer data can be ancillary – at least in developed countries – to almost any criminal offence."*[1]

1.2 In other words, there can be no definitive or exhaustive list of cybercrime. Moreover, multiple ways to categorise cybercrime and multiple sets of terminologies for such categorisation exist in the literature. On different occasions or in different publications, an author may not be consistent in terms of the categorisation and the terminology.

Categorisation at the United Nations' level

1.3 At a workshop devoted to the issue of crimes related to computer networks during the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, cybercrime was divided into two categories and defined as follows:

> *"(a) Cyber crime in a narrow sense ('computer crime'): any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them;*
>
> *(b) Cyber crime in a broader sense ('computer-related crime'): any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network."*[2]

---

1 UNODC, *Comprehensive Study on Cybercrime* (Feb 2013), at 16, available at https://www.unodc.org/documents/commissions/CCPCJ/CCPCJ_Sessions/CCPCJ_22/_E-CN15-2013-CRP05/Comprehensive_study_on_cybercrime.pdf.

2 United Nations, "Crime related to computer networks - Background paper for the workshop on crimes related to the computer network" (A/CONF.187/10, 3 Feb 2000), at para 14, available at https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks.pdf.

1.4 The UNODC Global Programme on Cybercrime, which commenced in 2013, differentiates between "*cyber-dependent offences, cyber-enabled offences and, as a specific crime-type, online child sexual exploitation and abuse*".[3] As mentioned in the Preface, we use the terms "cyber-dependent crimes" and "cyber-enabled crimes" in this Consultation Paper.

1.5 Examples of cyber-dependent crimes include hacking, distribution of computer virus, and distributed denial of service ("**DDOS**") attack. Examples of cyber-enabled crimes include online dissemination of child pornography, setting up of a phishing website, and online doxxing (ie unauthorised disclosure on the internet of an individual's private or identifying information).

Categorisation under the Budapest Convention

Offences prescribed by the Budapest Convention

1.6 The Budapest Convention was opened for signature on 23 November 2001 and entered into force on 1 July 2004.[4] Supplemented by an Additional Protocol which entered into force on 1 March 2006,[5] the Budapest Convention appears to be the first multi-national agreement for regulating cyberspace.[6] As at 16 March 2020, 65 states had ratified or acceded to the Budapest Convention.[7]

1.7 The purpose of section 1 of the Budapest Convention (Articles 2 to 13) is to improve the means to prevent and suppress computer or computer-related crime by establishing a common minimum standard of relevant offences.[8] The Budapest Convention requires each party state to "*adopt such legislative and other measures as may be necessary*" to provide for criminal offences under its domestic law in relation to the following subject matters (with compliance apparently on a "substance over form" basis):

---

3 UNODC, "Global Programme on Cybercrime", available at https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html (accessed on 3 May 2022).

4 Its text is available on the website of the Council of Europe, at https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185 (accessed on 3 May 2022).

5 The complete title is the "Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems". Its text is available on the website of the Council of Europe, at https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189 (accessed on 3 May 2022).

6 There are other regional initiatives apart from the Budapest Convention. See, for example: UNODC, "International and regional instruments", available at https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/international-and-regional-instruments.html (accessed on 3 May 2022).

7 Council of Europe, "Colombia joined the Budapest Convention on Cybercrime" (16 Mar 2020), available at https://www.coe.int/en/web/cybercrime/-/colombia-joined-the-budapest-convention-on-cybercrime (accessed on 3 May 2022).

8 Council of Europe, *Explanatory Report to the Convention on Cybercrime* (ETS No 185, 23 Nov 2001) ("**Explanatory Report**"), at para 33, available at https://rm.coe.int/16800cce5b (accessed on 3 May 2022).

(a) offences against the confidentiality, integrity and availability of computer data and systems (including illegal access to computer system, illegal interception of non-public transmissions of computer data, illegal interference with computer data, illegal interference with computer system, and misuse of device or data for committing cybercrime);

(b) computer-related offences (including computer-related forgery and computer-related fraud);

(c) content-related offences (including offences related to child pornography, and dissemination of racist and xenophobic material through computer systems); and

(d) offences relating to infringements of copyright and related rights.

Model Law on Computer and Computer Related Crime

1.8 The Secretariat of the Commonwealth of Nations is an observer to the Cybercrime Convention Committee of the Council of Europe. The Commonwealth has developed a Model Law on Computer and Computer Related Crime[9] ("**Model Law**") taking into account the Budapest Convention. The Model Law was adopted in 2002 and under consideration for review as of July 2017.[10]

1.9 The Commonwealth Secretariat stated in a news article of 22 April 2016 that the Model Law had been used by 22 Commonwealth countries as the basis of their national cybercrime laws.[11]

Degree of alignment of the laws in other jurisdictions

1.10 We stated in the Preface that the comparative study in this Consultation Paper covers the laws of seven jurisdictions, namely Australia, Canada, England and Wales, Mainland China, New Zealand, Singapore and the USA. Regarding the extent to which those laws are consistent with the requirements under the Budapest Convention, the following account provides a historical context:

---

9 Its text is available on the website of the Commonwealth of Nations, at http://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf (accessed on 3 May 2022).

10 The Commonwealth Cyber Declaration was signed at the Commonwealth Heads of Government Meeting in London in 2018. A programme has since been launched in order to implement the commitments of the Cyber Declaration across the Commonwealth. .

11 Commonwealth Secretariat, "Commonwealth model law promises co-ordinated cybercrime response" (22 Apr 2016), available at https://thecommonwealth.org/media/news/commonwealth-model-law-promises-co-ordinated-cybercrime-response (accessed on 3 May 2022).

(a) In Canada, the Supreme Court's 1980 decision in *R v McLaughlin*[12] prompted reform of the Criminal Code to address problems of computer misuse.[13] The Criminal Law Amendment Act 1985 and the Criminal Law Improvement Act 1996 added a number of cybercrime provisions into the Criminal Code, such as section 342.1[14] and section 430(1.1),[15] before April 1997 when negotiations started on what would become the Budapest Convention[16] (which Canada signed in 2001).

(b) In the USA, the key federal legislation on cybercrime is the Computer Fraud and Abuse Act enacted in 1986 and codified at 18 USC 1030. The history of amendments to 18 USC 1030 (on nine occasions from 1986 to 2008) does not suggest any direct influence of the Budapest Convention notwithstanding that the USA became a signatory in 2001.[17]

(c) The Law Commission of England and Wales recommended in 1989[18] the enactment of a new piece of legislation eventually passed as the Computer Misuse Act 1990 ("**CMA-EW**"). The CMA-EW has been amended several times but its overall framework has remained largely the same even after the UK signed the Budapest Convention in 2001.

(d) The Computer Misuse Act 1993 ("**CMA-SG**") in Singapore was enacted in 1993. Its offence provisions are based primarily on the CMA-EW, though with some divergences.[19]

(e) In Mainland China, cybercrime provisions were introduced into Articles 285 and 286 of the Criminal Law of the People's Republic of China ("**PRC Criminal Law**") in 1997,[20] ie before the Budapest Convention entered into force in 2004. In 2009, further provisions were added to Article 285 to extend the application of cybercrime.[21]

---

12 [1980] 2 SCR 331.

13 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015), at 52 to 53.

14 This was initially s 301.2(1) and now renumbered. The section heading reads "*Unauthorized use of computer*".

15 This was initially s 387(1.1) and now renumbered. The section heading reads "*Mischief in relation to computer data*".

16 Explanatory Report, at para 12.

17 Recounted in the book: H Marshall Jarrett, Michael W Bailie, Ed Hagen and Scott Eltringham, *Prosecuting Computer Crimes* (Office of Legal Education, Executive Office for United States Attorneys, 2nd edition, 2010), at 1 to 3, available at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (accessed on 3 May 2022).

18 Law Commission, *Criminal Law: Computer Misuse* (1989), Law Com No 186, available at https://www.lawcom.gov.uk/project/criminal-law-computer-misuse/ (accessed on 3 May 2022).

19 Gregor Urbas, "An Overview of Cybercrime Legislation and Cases in Singapore" (ASLI Working Paper No 001, Dec 2008), at 1, available at https://law.nus.edu.sg/asli/pdf/WPS001.pdf (accessed on 3 May 2022).

20 The amendments to the PRC Criminal Law came into operation on 1 Oct 1997.

21 Article 285(2) and (3) was added into the PRC Criminal Law. As a result of these amendments that came into operation on 28 Feb 2009, the offence of illegal access to program or data also applies to

(f) Following the recommendation by the Law Commission of New Zealand in 1999,[22] the current provisions on cybercrime (sections 248 to 252) were added to its Crimes Act 1961 in 2003. It appears from the legislative background described in the Law Commission's Report that the Budapest Convention did not materially influence the drafting of the New Zealand legislation, if at all.

(g) The origin of the cybercrime provisions in the Criminal Code (Cth) in Australia is a Report issued by the Model Criminal Code Officers Committee ("**MCCOC Report**") in 2001.[23] A parliamentary paper in respect of the relevant Cybercrime Bill 2001[24] suggested that the MCCOC Report was "*significantly influenced*" by the CMA-EW in terms of the approach, and also took account of the draft Budapest Convention at that time. Having said that, and although Australia ratified the Budapest Convention in 2012,[25] the legislative language defining the offences in Australia has, since enactment in 2001, remained rather different from that of the CMA-EW and, indeed, the Model Law which is directly based on the Budapest Convention.

Latest developments in the United Nations

1.11 The international landscape of cybercrime regulation is evolving rapidly. Two developments in the United Nations are potentially influential and deserve close attention:

(a) The Russian Federation submitted a "*Draft United Nations Convention on Cooperation in Combating Cybercrime*" to the United Nations on 11 October 2017 ("**Russian Convention**"). The relevant Resolution of the United Nations General Assembly did not record any agreed follow-up.[26]

---

computer information systems in general, and the offence of making available or possessing a device or data for committing a crime was enacted.

22 New Zealand Law Commission, *Computer Misuse* (1999), Report 54, available at https://www.lawcom.govt.nz/our-projects/computer-crime?id=814 (accessed on 3 May 2022).

23 Model Criminal Code Officers Committee, *Report, Chapter 4, Damage and Computer Offences and Amendments to Chapter 2: Jurisdiction* (Jan 2001). An archived copy of the Report, previously available on the website of the Attorney-General's Department, can be obtained through the "Wayback Machine" (the relevant part is Part 4.2 in Chapter 4) at https://web.archive.org/web/20060920231025/http://www.ag.gov.au/agd/WWW/rwpattach.nsf/viewasattachmentPersonal/(0AFA115E182148C186311CED66C0728D)~modelcode_ch4_Computer_offences_report.pdf/$file/modelcode_ch4_Computer_offences_report.pdf (accessed on 3 May 2022).

24 Department of the Parliamentary Library, *Bills Digest No 48 2001-02* (2001), available at https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd0102/02bd048 (accessed on 3 May 2022).

25 The long title of the Cybercrime Legislation Amendment Act 2012 (Cth) describes it as "*[a]n Act to implement the Council of Europe Budapest Convention on Cybercrime, and for other purposes*", see https://www.legislation.gov.au/Details/C2012A00120 (accessed on 3 May 2022).

26 United Nations General Assembly, *Resolution 72/196* (A/RES/72/196, 19 Dec 2017).

(b) More recently, however, in its Resolution 74/247 adopted on 27 December 2019,[27] the General Assembly decided:

> *"… to establish an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, taking into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes, in particular the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime".*[28]

1.12 If and when a treaty on cybercrime is developed within the United Nations' framework, the categorisation and terminology adopted by it may conceivably become authoritative in time.

---

27 United Nations General Assembly, *Resolution 74/247* (A/RES/74/247, 27 Dec 2019).

28 At para 3. In May 2021, the ad hoc committee elected its officers and discussed an outline and modalities for its further activities at its organisational session. See https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (accessed on 3 May 2022). However, the first session of the committee was postponed to 28 February to 11 March 2022 due to the ongoing COVID-19 pandemic. See: UNODC, "First session of the Ad Hoc Committee", available at https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html (accessed on 3 May 2022).

Chapter 2

Illegal access to program or data

Introduction

2.1 In this Chapter, we will examine the first of the five core species of cyber-dependent offences: illegal access to program or data in a computer. This is to be distinguished from the subject of illegal interception of computer data which will be the focus of the next chapter. Broadly speaking, an offence in respect of illegal access to program or data in a computer would seek generally to:

(a) address dangerous threats to, and attacks against, the security of computer systems; and

(b) thereby protect people's right to manage, operate and control their computer system in an undisturbed and uninhibited manner.

2.2 Hacking is probably the quintessential example of this offence. Apart from that, at least in some jurisdictions,[1] it may be an offence for a person who is authorised to access a computer (eg an employee operating the employer's computer) to act outside the scope of authorisation.

2.3 In considering the offence of illegal access to program or data, we are mindful of the unique nature of cyberspace. As a starting point, a possible analogy to unauthorised access to computer (or the program or data held in it) in the physical world is where a stranger enters an area (eg someone's home) without permission.

2.4 The determination of criminal liability for intrusion in the physical world is more straightforward because the concept of unauthorised access is relatively well-defined as boundaries to physical space are tangible. For example, if a stranger "accesses" another person's residence, he or she has at least physically set foot on the latter's residence and his or her act is clearly objectionable. Also, it is relatively easy for a victim to stop an intruder in the physical world.

2.5 The cyberspace, on the other hand, is a totally different scenario. The characteristics inherent in the design and functioning of, and the practice conducted in, the virtual space mean that in certain widely accepted circumstances, authorisation to access program or data is implicitly granted by

[1] For example, Hong Kong, Australia and the USA (see paras 2.9, 2.23 to 2.26, and 2.83 to 2.88).

an online user. In practice, by connecting a device to the internet or using an internet service, a person has in some way acquiesced to a (reasonable) degree of interaction with other online users in that, for instance, an online user is not generally expected to ask for prior express authorisation of the intended recipient before sending him or her, being another online user, an email or displaying an advertisement on a webpage, especially when this is not done in bad faith. Another example is the scanning of the internet by search engines[2] at various internet protocol addresses in order to find out whether they have a webpage server and index the webpages found. Therefore, in the realm of cyberspace, the concept of "unauthorised" access should be understood against the above background.

Current Hong Kong law

Crimes Ordinance (Cap 200)

Section 161

2.6 Section 161 of the Crimes Ordinance (Cap 200) ("*Access to computer with criminal or dishonest intent*") ("**S161**") provides as follows:

> *"(1) Any person who obtains access to a computer—*
>
> *(a) with intent to commit an offence;*
>
> *(b) with a dishonest intent to deceive;*
>
> *(c) with a view to dishonest gain for himself or another; or*
>
> *(d) with a dishonest intent to cause loss to another,*
>
> *whether on the same occasion as he obtains such access or on any future occasion, commits an offence and is liable on conviction upon indictment to imprisonment for 5 years.*
>
> *(2) For the purposes of subsection (1) gain (獲益) and loss (損失) are to be construed as extending not only to gain or loss in money or other property, but as extending to any such gain or loss whether temporary or permanent; and—*
>
> *(a) gain (獲益) includes a gain by keeping what one has, as well as a gain by getting what one has not; and*

[2] Specifically, search engines regularly test ports 80 and 443, which are ports generally associated with access to websites. Port 80 is designated for "HTTP" for transmission of webpages. Port 443 is designated for "HTTPS" for transmission of webpages securely over Transport Layer Security or Secure Sockets Layer. See https://isc.sans.edu/forums/diary/Cyber+Security+Awareness+Month+Day+25+Port+80+and+443/7450/ (accessed on 3 May 2022).

(b) loss (損失) includes a loss by not getting what one might get, as well as a loss by parting with what one has."

Actus reus under S161

2.7 The leading authority on S161 is *Secretary for Justice v Cheng Ka Yee (鄭嘉儀)*[3] ("***Cheng Ka Yee***"). The Court of Final Appeal construed the provision in light of its text, context and purpose, and had the following observation on the *actus reus* ("obtains access"):

> *" 'Obtain' … is not a word which sits easily with the use by a person of their own device. Nor is the word "access" … As a matter of language one always 'obtains' access to something to which one did not have access before."*[4]

2.8 It was held that "*s.161(1)(c) on its proper construction does not apply to the use by a person of his or her own computer, not involving access to another's computer*".[5] Logic supports the same conclusion with regard to the other limbs in S161(1). Therefore, S161 does not apply to, for instance:

(a) The use of one's *own* computer to set up a phishing website; and

(b) Upskirting using one's *own* smartphone.[6]

Unauthorised nature of an access

2.9 S161 does not, on its face, require that an access in question must be unauthorised. Yet, the courts appear to have read in such a requirement.[7] In this regard, cases involving lack of authorisation simpliciter are relatively straightforward. Contentious issues have tended to arise in various jurisdictions in cases of a perpetrator (say, an employee) acting in excess of authorisation. A Hong Kong authority on point is

---

3 (2019) 22 HKCFAR 97, [2019] HKCFA 9.

4 Same as above, at para 38.

5 Same as above, at para 48.

6 S161 does not define a "computer". In *律政司司長 訴 王嘉業* [2013] 4 HKLRD 588, HCMA 77/2013 (date of judgment: 29 Apr 2013, with the English translation of the judgment reported as *Secretary for Justice v Wong Ka Yip Ken* [2013] 4 HKLRD 604), a magistracy appeal to the Court of First Instance which predated *Cheng Ka Yee*, Barnabas Fung J held that a smartphone capable of, among others, recording video clips amounted to a "computer" for the purposes of a prosecution under S161. The learned judge did not adopt the definition of "computer" in s 22A(12) of the Evidence Ordinance (Cap 8), s 26A of the Inland Revenue Ordinance (Cap 112) and s 19 of the Business Registration Ordinance (Cap 310), ie "*any device for storing, processing or retrieving information*". Instead, the definition of the word given by the Online Oxford Dictionary was adopted:
"*an electronic device, which is capable of receiving information (data) in a particular form and of performing a sequence of operations in accordance with a predetermined but variable set of procedural instructions (program) to produce a result in the form of information or signals*".

7 See fn 3 above, at para 38.

HKSAR v Tsun Shui Lun,[8] in which Chan CJHC held as follows:

> *"For the purpose of a s.161 offence, I do not think that there is or should be any difference between gaining access without authority and gaining access in excess of authority. The section makes no distinction between the two."*[9]

Scope of the "gain" under S161

2.10 The Chief Judge in *HKSAR v Tsun Shui Lun* further construed the word "gain" in S161 as "*not confined to financial or proprietary benefits, but … wide enough to cover intangible benefits*", which can be "*transient as opposed to permanent*".[10] This wide interpretation suggests that the offence applies to a person obtaining, from a computer, information to which the person previously had no access.[11] For instance, the "gain" in that case was a patient's medical records stored in the computer system of a hospital where the offender worked.

Telecommunications Ordinance (Cap 106)

Section 27A

2.11 Another provision relevant to this Chapter is section 27A of the Telecommunications Ordinance (Cap 106) ("*Unauthorized access to computer by telecommunications*") ("**S27A**"):

> *"(1) Any person who, by telecommunications, knowingly causes a computer to perform any function to obtain unauthorized access to any program or data held in a computer commits an offence and is liable on conviction to a fine at level 4.*
>
> *(2) For the purposes of subsection (1)—*
>
> *(a) the intent of the person need not be directed at—*
>
> *(i) any particular program or data;*
>
> *(ii) a program or data of a particular kind; or*
>
> *(iii) a program or data held in a particular computer;*
>
> *(b) access of any kind by a person to any program or data held in a computer is unauthorized if he is not*

---

8 [1999] 3 HKLRD 215, HCMA 723/1998 (date of judgment: 15 Jan 1999), a magistracy appeal to the Court of First Instance cited with approval in *HKSAR v Au Yeung Ka Man Yuniko* [2018] HKCFA 23.

9 [1999] 3 HKLRD 215, at 223D (para 22).

10 Same as above, at 223G (para 24).

11 Same as above, at 223J (para 25).

entitled to control access of the kind in question to the program or data held in the computer and—

(i) he has not been authorized to obtain access of the kind in question to the program or data held in the computer by any person who is so entitled;

(ii) he does not believe that he has been so authorized; and

(iii) he does not believe that he would have been so authorized if he had applied for the appropriate authority.

(3) Subsection (1) has effect without prejudice to any law relating to powers of inspection, search or seizure.

(4) Notwithstanding section 26 of the Magistrates Ordinance (Cap. 227), proceedings for an offence under this section may be brought at any time within 3 years of the commission of the offence or within 6 months of the discovery of the offence by the prosecutor, whichever period expires first."

Comparison between S161 and S27A

2.12 In *HKSAR v Tsun Shui Lun*, Chan CJHC compared S161 and S27A as follows:

> *"In one respect, s.161 has a wider application than that under s.27A of the Telecommunication Ordinance since an offence under s.161 can be committed whether the access is obtained by telecommunication or not. On the other hand, a s.161 offence requires proof of a specific criminal or dishonest intent or purpose and is more serious (as can be reflected from the maximum penalty specified in the provision). It follows that not every kind of access into a computer constitutes an offence under s.161."*[12]

2.13 As the Chief Judge remarked, a perpetrator must have obtained access "by telecommunications" for S27A to apply. This suggests the use of a telecommunications device (eg another computer) to obtain access, in addition to the target computer. Consistently, S27A was characterised in *Cheng Ka Yee* as "*[t]he 'hacking' offence*" which is "*clearly directed at a computer other than the offender's own*".[13]

---

12 Same as above, at 222B-C.

13 See fn 3 above, at para 41.

2.14 Despite such characterisation, case law shows that incidents of hacking tend to be prosecuted under S161 rather than S27A.[14] An example is *HKSAR v Tam Hei Lun & Ors*,[15] where the offender used a program called Back Orifice to access computers of other internet users and obtain their login names and passwords. Another authority involving the offender's use of a separate computer for hacking is *HKSAR v Tse Man Lai*,[16] where the offender directed attacks from his computer to the server for the "HKEXnews" website on two occasions and obtained three still images and video footage.

Apparent difficulties to prove the offence under S27A

2.15 A reason for prosecuting cases of hacking under S161 rather than S27A may be the apparent difficulty for the prosecution to prove the *mens rea* under S27A, which has two aspects – both expressed in the negative – namely the defendant:

(a) *"does not believe that he has been … authorized"* to obtain access of the kind in question; and

(b) *"does not believe that he would have been so authorized if he had applied for the appropriate authority"*.

2.16 In comparison, depending on the facts, it may sometimes be easier to prove a defendant's intent to commit an offence, or dishonesty, as required by S161. Moreover, as noted above, S27A is inapplicable if the defendant did not obtain access "by telecommunications".

2.17 In circumstances where both S161 and S27A can be invoked, the choice is potentially material because of the disparity in the maximum sentences (a fine at level 4 under S27A[17] and imprisonment for five years on conviction upon indictment under S161).

Standard of criminalisation under the Budapest Convention

2.18 The focus of this Chapter corresponds to Article 2 in Title 1 under section 1 of the Budapest Convention:[18]

---

14 To date, there appears to be no reported decision in which S27A was invoked against hacking. A successful prosecution in 1996 under S27A is discussed in the article, Rynson W H Lau, Kwok-Yan Lam and Siu-Leung Cheung, "The Failure of Anti-Hacking Legislation: a Hong Kong Perspective" (Invited Paper in Proceedings of ACM Conference on Computer and Communications Security, March 1996), at 62-67. However, no written decision can be located.

15 [2000] 3 HKC 745, HCMA 385/2000 (date of judgment: 9 Oct 2000).

16 [2013] 3 HKLRD 691 (this authority should now be read subject to *Cheng Ka Yee*), CACC 455/2012 (date of judgment: 18 Jun 2013).

17 Currently $25,000 under Schedule 8 to the Criminal Procedure Ordinance (Cap 221).

18 See para 11 of the Preface and paras 1.6 to 1.10 of Chapter 1 for background information regarding the Budapest Convention.

"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system."

2.19 The Explanatory Report comments on Article 2 as follows:

"44. 'Illegal access' covers the basic offence of dangerous threats to and attacks against the security ... of computer systems and data. The need for protection reflects the interests of organisations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner. The mere unauthorised intrusion ... should in principle be illegal in itself. It may lead to impediments to legitimate users of systems and data and may cause alteration or destruction with high costs for reconstruction. Such intrusions may give access to confidential data ... and secrets, to the use of the system without payment or even encourage hackers to commit more dangerous forms of computer-related offences, like computer-related fraud or forgery.

…

46. 'Access' comprises the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data). However, it does not include the mere sending of an e-mail message or file to that system. 'Access' includes the entering of another computer system ... or to a computer system on the same network ... The method of communication ... does not matter.

47. The act must also be committed 'without right' ... there is no criminalisation of the access authorised by the owner or other right holder of the system or part of it ... there is no criminalisation for accessing a computer system that permits free and open access by the public ...

48. The application of specific technical tools may result in an access under Article 2, such as the access of a web page ... The application of such tools per se is not 'without right'. The maintenance of a public web site implies consent by the web site-owner that it can be accessed by any other web-user ...

…

50. Parties can take the wide approach and criminalise mere hacking in accordance with the first sentence of Article 2. Alternatively, Parties can attach any or all of the qualifying elements listed in the second sentence: infringing security measures, special intent to obtain computer data, other dishonest intent that justifies criminal culpability, or the requirement that the offence is committed in relation to a computer system that is connected remotely to another computer system.[19] *The last option allows Parties to exclude the situation where a person physically accesses a stand-alone computer without any use of another computer system. They may restrict the offence to illegal access to networked computer systems ...* "[20]

Statutory regimes in other jurisdictions

Australia

Sections 477.1 and 478.1, Criminal Code (Cth)

2.20 In Australia, section 478.1 of the Criminal Code (Cth) ("*Unauthorised access to, or modification of, restricted data*") provides as follows:

> *"(1) A person commits an offence if:*
>
> *(a) the person causes any unauthorised access to, or modification of, restricted data; and*
>
> *(b) the person intends to cause the access or modification; and*
>
> *(c) the person knows that the access or modification is unauthorised.*

---

[19] The Explanatory Report discusses the term "computer system" as follows at paras 23 and 24:
"*23. A computer system under the Convention is a device consisting of hardware and software developed for automatic processing of digital data. It may include input, output, and storage facilities. It may stand alone or be connected in a network with other similar devices. 'Automatic' means without direct human intervention, 'processing of data' means that data in the computer system is operated by executing a computer program. A 'computer program' is a set of instructions that can be executed by the computer to achieve the intended result. A computer can run different programs. A computer system usually consists of different devices, to be distinguished as the processor or central processing unit, and peripherals. A 'peripheral' is a device that performs certain specific functions in interaction with the processing unit, such as a printer, video screen, CD reader/writer or other storage device.*
24. A network is an interconnection between two or more computer systems. The connections may be earthbound (e.g., wire or cable), wireless (e.g., radio, infrared, or satellite), or both. A network may be geographically limited to a small area (local area networks) or may span a large area (wide area networks), and such networks may themselves be interconnected. The Internet is a global network consisting of many interconnected networks, all using the same protocols. Other types of networks exist, whether or not connected to the Internet, able to communicate computer data among computer systems. Computer systems may be connected to the network as endpoints or as a means to assist in communication on the network. What is essential is that data is exchanged over the network."

[20] Explanatory Report, at paras 44, 46 to 48 and 50.

Penalty: 2 years imprisonment.

(3) In this section:

***restricted data** means data:*

(a) held in a computer; and

(b) to which access is restricted by an access control system associated with a function of the computer."

2.21 In addition, section 477.1 of the Criminal Code (Cth) ("*Unauthorised access, modification or impairment with intent to commit a serious offence*") is effectively an aggravated offence with respect to unauthorised access to computer data, which is one of the three kinds of wrongful conduct outlawed by that provision:

"Intention to commit a serious Commonwealth, State or Territory offence

(1) A person commits an offence if:

(a) the person causes:

(i) any unauthorised access to data held in a computer; or

(ii) any unauthorised modification of data held in a computer; or

(iii) any unauthorised impairment of electronic communication to or from a computer; and

(c) the person knows the access, modification or impairment is unauthorised; and

(d) the person intends to commit, or facilitate the commission of, a serious offence against a law of the Commonwealth, a State or a Territory (whether by that person or another person) by the access, modification or impairment.

(3) In a prosecution for an offence against subsection (1), it is not necessary to prove that the defendant knew that the offence was:

(a) an offence against a law of the Commonwealth, a State or a Territory; or

(b) a serious offence.

Penalty

(6) A person who commits an offence against this section is punishable, on conviction, by a penalty not exceeding the penalty applicable to the serious offence.

Impossibility

(7) A person may be found guilty of an offence against this section even if committing the serious offence is impossible.

No offence of attempt

(8) It is not an offence to attempt to commit an offence against this section.

Meaning of serious offence

(9) In this section:

***Serious offence** means an offence that is punishable by imprisonment for life or a period of 5 or more years."*

Unsuccessful attempts to access

2.22 Section 477.1 is unique among the statutory provisions examined in this Chapter, with section 477.1(8) expressly excluding attempts to commit the offence from criminal liability. It is clear that section 477.1 only applies to successful attempts.

Unauthorised nature of an access

2.23 As regards the unauthorised nature of an access, the MCCOC Report (which formed the basis of the cybercrime provisions in the Criminal Code (Cth)) commented thus:

"Should individuals who are authorised for one purpose be guilty of an offence under this Part if they act for another, ulterior purpose? Liability should certainly be imposed if the original authorisation was obtained by deception as to the offender's purposes. It does not follow, however, that liability should be imposed when authorisation was obtained without fraud and the defendant misuses the authorisation. The issue is clearly

contentious ..."[21]

2.24 The subsequently enacted section 476.2(1) and (2) of the Criminal Code (Cth) provides that:

(a) *"access to data held in a computer ... by a person is unauthorised if the person is not entitled to cause that access"*; but

(b) *"[a]ny such access ... caused by the person is not unauthorised merely because he or she has an ulterior purpose for causing it"*.

2.25 The decision of the New South Wales Court of Appeal in *Salter v DPP (NSW)*[22] gives a hint of how one should understand the above provisions. In that case, the court interpreted section 308B(2) of the Crimes Act 1900 (NSW), the equivalent of section 476.2(2) of the Criminal Code (Cth) in state legislation, as follows:

> *"The object of s 308B(2) is to protect an officer [in that case, a police officer] who has a legitimate entitlement to access particular data but who may also have an ulterior purpose for that access. Accordingly, if there is a legitimate purpose even though there is also an ulterior purpose, the officer will not breach the Act ... That subsection has the purpose of ensuring that when a person accesses the [computer] system exercising their authority they will not commit an offence 'merely' because they have in addition some ulterior purpose."*[23]

2.26 In the end, the court upheld the offender's conviction because "*[t]he access which she obtained was [merely] for a personal purpose having no relationship with any function she performed on behalf of the police*".[24]

Canada

Sections 326(1)(b) and 342.1(1), Criminal Code 1985

2.27 There are two relevant provisions in the Criminal Code 1985 in Canada. The first is section 326(1)(b) ("*Theft of telecommunication service*"), under which:

---

21 MCCOC Report, Chapter 4, Damage and Computer Offences and Amendments to Chapter 2: Jurisdiction (2001), at 141.

22 [2011] NSWCA 190.

23 Same as above, at paras 19 and 25 (McClellan CJ).

24 Same as above, at para 24 (McClellan CJ).

"Every one commits theft who fraudulently, maliciously, or without colour of right[25] *… uses any telecommunication facility or obtains any telecommunication service."*

2.28 The second is section 342.1(1) ("*Unauthorized use of computer*"):

"Everyone is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years, or is guilty of an offence punishable on summary conviction who, fraudulently and without colour of right,

(a) obtains, directly or indirectly, any computer service;

(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system;

(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or under section 430 in relation to computer data or a computer system; or

(d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c)."

Actus reus

2.29 Both provisions define the *actus reus* by reference to, among other things, a defendant's "use" of a telecommunication facility or computer system. Some academics favour the term "use" over "access". For instance, a commentator has compared them as follows:

"Convergence of technology, the use of ADSL[26] *and broadband, wireless internet and the imprecise nature of networks all create an environment in which it is more accurate to describe 'use' of a computer rather than access to a computer. Adopting a broad definition helps to avoid technical and often arbitrary arguments about what constitutes access, and appropriately focuses on the remaining elements. It is these elements that determine the*

---

25 The term "colour of right" denotes "*an honest belief in a state of facts which, if it actually existed would at law justify or excuse the act done*" (*R v DeMarco* (1973) 13 CCC (2d) 369, at 372 (Martin JA), cited with approval in *R v Simpson* [2015] 2 SCR 827).

26 ADSL stands for "asymmetric digital subscriber line". Utilising the technology, copper wires used to link up telephones in the past can now support an internet connection.

criminality of the conduct and help avoid over-breadth."[27]

2.30 As things stand, however, the Canadian Criminal Code does not define "use". There may be scope for dispute as to whether it only means the effective use of a computer system, or would extend to any use of it without practical utility (including unsuccessful attempts to gain access).

Statutory definitions of key terms

2.31 The word "computer" is also undefined in that Code. However, section 342.1(2) of the Code does define terms such as "computer data", "computer password", "computer program", "computer service", "computer system" and "function".

2.32 In particular, "function" is broadly and non-exhaustively defined to include "*logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer system*". This gives the term "computer system" (the statutory definition of which is set out below) a wide coverage:

> *"**computer system** means a device that, or a group of interconnected or related devices one or more of which,*
>
> *(a) contains computer programs or other computer data, and*
>
> *(b) by means of computer programs,*
>
> *(i) performs logic and control, and*
>
> *(ii) may perform any other function".*

England and Wales

Section 1 of the CMA-EW

2.33 In England and Wales, section 1 of the CMA-EW ("*Unauthorised access to computer material*") provides as follows:

> *"(1) A person is guilty of an offence if—*
>
> *(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured;*

[27] Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015), at 79. This passage appears in the author's discussion of the law in the USA, but his observations apply equally to Canadian law which refers to "use" of computer system.

(b) the access he intends to secure, or to enable to be secured, is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) […]

(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both."

Meaning of "computer"

2.34 Same as the Australian and Canadian legislation, the CMA-EW leaves "computer" undefined. The Crown Prosecution Service noted as follows on its website:

> *"The [CMA-EW] does not provide a definition of a computer because rapid changes in technology would mean any definition would soon become out of date.*
>
> *Definition is therefore left to the Courts, who are expected to adopt the contemporary meaning of the word. In DPP v McKeown, DPP v Jones ([1997] 2 Cr App R 155, HL, at page 163), Lord Hoffman defined a computer as 'a device for storing, processing and retrieving information.' "*[28]

[28] Crown Prosecution Service, "Legal Guidance, Computer Misuse Act", available at https://www.cps.gov.uk/legal-guidance/computer-misuse-act (accessed on 3 May 2022).

Actus reus

2.35 The *actus reus* under section 1(1)(a) is to cause a computer to perform any function. The Law Commission – in its Report which led to the CMA-EW's enactment – preferred this formulation to one referring to the concept of access, because the former:

> *"... covers any manipulation of a computer that is performed with the appropriate nefarious intent and is not ... expressed in terms that technological developments might later render obsolete. It excludes mere physical access, and mere scrutiny of data, without interaction with the operation of the computer."* [29] (emphases in original)

2.36 The above *actus reus* refers to "a computer", and section 1(1)(a) goes on to define the *mens rea* with reference to any program or data held in "any computer". The statutory language obviously covers cases involving two computers, ie one used by the perpetrator as the tool, and the other holding the program or data.

2.37 In addition, the English Court of Appeal held in *Attorney-General's Reference (No 1 of 1991)* [30] that the term "any computer" in the provision included the computer which the defendant had caused to perform any function. Put differently, the provision also applies to the one-computer scenario.[31]

Unsuccessful attempts to access

2.38 The *actus reus* is actually so broadly defined in section 1(1)(a) of the CMA-EW that merely switching on a computer, or trying different passwords in an attempt to access its program or data, would apparently suffice to constitute the *actus reus* [32] irrespective of whether or not the attempt succeeded in the end. The standard of criminalisation under the Budapest Convention[33] aside, it is not generally accepted that mere unauthorised access (which would involve a successful attempt to access) should be an offence.[34]

---

29 Law Commission, *Criminal Law: Computer Misuse* (1989), Law Com No 186, at para 3.26.

30 [1993] QB 94.

31 For comparison, as noted above, parties to the Budapest Convention may choose to exclude from criminal liability "*the situation where a person physically accesses a stand-alone computer without any use of another computer system*" (Explanatory Report, at para 50).

32 Law Commission, *Criminal Law: Computer Misuse* (1989), Law Com No 186, at paras 3.20 and 3.26.

33 "*The mere unauthorised intrusion ... should in principle be illegal in itself*" (Explanatory Report, at para 44).

34 The Explanatory Report made this point in para 49.
Also see, for example, Neil MacEwan, "The Computer Misuse Act 1990: lessons from its past and predictions for its future" [2008] Crim LR 955, at 956:
"*When the [CMA-EW] arrived, some had already questioned why the unauthorised access of confidential information held on a computer should be an offence where if the same information were held on card index no offence would be committed*".
In Australia, the MCCOC Report stated as follows at 135:
"*By contrast with existing law in a number of jurisdictions, mere unauthorised access will not amount to a [Model Criminal] Code offence. The Committee does propose, however, a summary offence of unauthorised access to restricted data.*"

One may argue that the case for criminalising unsuccessful attempts is even weaker.

2.39 The English authority *R v Brown*[35] was concerned with the different context of the (now repealed) Data Protection Act 1984, but illustrates a similar point.[36] In that case, the House of Lords held by a 3:2 majority that the mere retrieval of information from a computer database (say, in the form of a display on a screen, or of a printout) was insufficient to amount to "use" under section 5(2)(b) of that Act;[37] "*it was necessary to do something to the data, and not merely to access it*".[38] The minority took the contrary view.

Access to program or data, not access to computer

2.40 The House of Lords held in *R v Bow Street Metropolitan Stipendiary Magistrate, Ex parte United States (No 2)*[39] ("***Ex parte United States***") that the Divisional Court erred in confining section 1 of the CMA-EW to the "hacking" of computer systems, as opposed to the use of a computer to secure unauthorised access to programs or data.[40] Section 17(6) of the CMA-EW clarifies the relationship between "program or data" on the one hand, and "computer" on the other, in the following terms:

> *"References to any program or data held in a computer include references to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium."*

2.41 With the above clarification, it appears to be an offence under section 1 of the CMA-EW if, for example, someone ("**Person A**") takes another person's thumb drive and connects it to his or her (Person A's) own computer, intending to access the data held in it without authorisation.

2.42 In the above hypothetical scenario, Person A's target is the data held in the thumb drive. Legislation against unauthorised access to data would be apt to deal with such cases. In some other cases, the perpetrator's

---

Similarly, US federal law does not criminalize mere unauthorized access, see Ian Walden, Computer Crimes and Digital Investigations (Oxford University Press, 2007), at para 3.240.

Notwithstanding the above, it is noted that in some jurisdictions, such as Hong Kong, England and Wales, New Zealand and Singapore, mere unauthorised access constitutes an offence.

35 [1996] AC 543.

36 In that case, the defendant was a police officer and entitled to use the police national computer database for the registered purpose of policing as an agent of his chief constable, who was a registered user under the Data Protection Act 1984. The prosecution alleged that the defendant used personal data in that database other than for policing. While the defendant could not be charged under the CMA-EW because the relevant facts took place before that Act came into effect, counsel for the defendant referred to it in argument. If the same facts happen today, the defendant would likely be charged under the CMA-EW.

37 "*A person in respect of whom such an entry is contained in the register [of data users] shall not ... (b) hold any such data, or use any such data held by him, for any purpose other than the purpose or purposes described in the entry*".

38 See fn 35 above, at 548D (Lord Goff of Chieveley).

39 [2000] 2 AC 216.

40 Same as above, at 226E (Lord Hobhouse of Woodborough).

focus may be on a computer or a computer system. Such perpetrator may have a fair point if he or she contends that a charge of unauthorised access to data (rather than computer or computer system) is inappropriate, even though it is probably true that access to a computer would necessarily involve access to data as a matter of technology.

Unauthorised nature of an access

2.43 In this regard, section 17(5) of the CMA-EW provides as follows:

> *"Access of any kind by any person to any program or data held in a computer is unauthorised 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 …"*

2.44 The English Divisional Court in *DPP v Bignell*,[41] based on its interpretation of section 17(5), accepted that "*[a] person who is authorised to secure access to a program or data does not commit an offence under section 1 of the [CMA-EW] if he accesses the computer at the authorised level*"[42] even though the access was for an unauthorised purpose. The ruling generated much criticism.

2.45 This interpretation of section 17(5) in *DPP v Bignell* was subsequently disapproved of by the House of Lords in *Ex parte United States*[43]. The House of Lords pointed out (among other things) that section 17(5) did not introduce the concept of different levels of access to the relevant computer.[44] It was therefore an "*extraneous idea*" to speak of "*an authorised level*" of access.[45] The House of Lords summarised the effect of section 17(5) as follows:

> *"It simply identifies the two ways in which authority may be acquired—by being oneself the person entitled to authorise and by being a person who has been authorised by a person entitled to authorise. It also makes clear that the authority must relate not simply to the data or programme but also to the actual kind of access secured."*[46]

---

41 [1998] 1 Cr App R 1.
42 Same as above, at 13 (Astill J).
43 [2000] 2 AC 216.
44 Same as above, at 225C-F (Lord Hobhouse of Woodborough).
45 Same as above, at 226E (Lord Hobhouse of Woodborough).
46 Same as above, at 224C-D (Lord Hobhouse of Woodborough).

2.46 On the facts in *Ex parte United States*, the House of Lords held that an employee with limited authorisation to access data on a computer might commit an offence under section 1 of the CMA-EW by acting in excess of the authorisation. Section 17(5) did not assist the employee.

2.47 Also relevant to the issue of authorisation is section 17(8) of the CMA-EW, inserted by the Police and Justice Act 2006:

> *"An act done in relation to a computer is unauthorised if the person doing the act (or causing it to be done)—*
>
> *(a) is not himself a person who has responsibility for the computer and is entitled to determine whether the act may be done; and*
>
> *(b) does not have consent to the act from any such person.*
>
> *In this subsection 'act' includes a series of acts."*

Mens rea

2.48 The *mens rea* under section 1(1) of the CMA-EW includes the perpetrator's:

> (a) intent to secure access to any program or data held in any computer, or to enable such access to be secured; and
>
> (b) knowledge at the time of the *actus reus* that such intended access is unauthorised.

2.49 The references to the perpetrator's intent and knowledge appear to connote a subjective test. Questions such as whether those states of mind have any objective element, and what evidentiary burden they entail, are relevant to all aspects of criminal law. For instance, section 8 of the Criminal Justice Act 1967 in England and Wales (set out below) is of general application:

> *"A court or jury, in determining whether a person has committed an offence,—*
>
> *(a) shall not be bound in law to infer that he intended or foresaw a result of his actions by reason only of its being a natural and probable consequence of those actions; but*
>
> *(b) shall decide whether he did intend or foresee that result by reference to all the evidence, drawing such inferences*

from the evidence as appear proper in the circumstances."[47]

Aggravated offence

2.50 If a person commits the offence under section 1 of the CMA-EW with intent to commit (or facilitate commission of) an offence specified in section 2(2), that would constitute an aggravated form of the offence under section 2 ("*Unauthorised access with intent to commit or facilitate commission of further offences*") with higher maximum sentence:

> *"(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ('the unauthorised access offence') with intent—*
>
> *(a) to commit an offence to which this section applies; or*
>
> *(b) to facilitate the commission of such an offence (whether by himself or by any other person);*
>
> *and the offence he intends to commit or facilitate is referred to below in this section as the further offence.*
>
> *(2) This section applies to offences—*
>
> *(a) for which the sentence is fixed by law; or*
>
> *(b) for which a person who has attained the age of twenty-one years (eighteen in relation to England and Wales) and has no previous convictions may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the Magistrates' Courts Act 1980).*
>
> *(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.*
>
> *(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.*

[47] The equivalent in Hong Kong is s 65A(1) of the Criminal Procedure Ordinance (Cap 221). The only difference is that it refers to the person's "acts or omissions" whereas the legislation in England and Wales refers to the person's "actions".

(5) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) […]

(c) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both."

Section 125 of the Communications Act 2003

2.51 For completeness, a provision in England and Wales which is comparable to section 326(1)(b) of the Criminal Code 1985 in Canada (cited above) is section 125 of the Communications Act 2003 ("*Dishonestly obtaining electronic communications services*"):

"(1) A person who—

(a) dishonestly obtains an electronic communications service, and

(b) does so with intent to avoid payment of a charge applicable to the provision of that service,

is guilty of an offence.

(2) […]

(3) A person guilty of an offence under this section shall be liable—

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both;

(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine, or to both."

Mainland China

2.52 It is apposite to first explain the elements that are common to all the five cyber-dependent offences in the mainland of the People's Republic of China ("**PRC**").

Mens rea

2.53 Articles 14 to 16 of the PRC Criminal Law set out the general principles concerning the *mens rea* of the offences under the PRC Criminal Law (which included the five cyber-dependent offences). The Articles provide that a perpetrator will be criminally liable for (i) intentional crimes, or (ii) negligent crimes when the law so provides:

> *"Article 14 An intentional crime refers to an act committed by a person who clearly knows that his act will entail harmful consequences to society but who wishes or allows such consequences to occur, thus constituting a crime.*
>
> *Criminal responsibility shall be borne for intentional crimes.*
>
> *Article 15 A negligent crime refers to an act committed by a person who should have foreseen that his act would possibly entail harmful consequences to society but who fails to do so through his negligence or, having foreseen the consequences, readily believes that they can be avoided, so that the consequences do occur.*
>
> *Criminal responsibility shall be borne for negligent crimes only when the law so provides.*
>
> *Article 16 An act is not a crime if it objectively results in harmful consequences due to irresistible or unforeseeable causes rather than intent or negligence."*[48]
>
> (emphasis added)

2.54 As Articles 285 and 286 of the PRC Criminal Law do not explicitly provide for any negligent crimes, it appears that the *mens rea* of the five cyber-dependent crimes in Mainland China includes intent (as defined in Article 14) and other mental elements specified in Articles 285 and 286 discussed below (if any).

---

[48] The English translation of Articles 14 to 16 is the official version published by the Legislative Affairs Commission of the Standing Committee of the National People's Congress ("**NPCSC**") in 1997. Articles 14 to 16 of《中華人民共和國刑法》state that:

"*第十四條 明知自己的行為會發生危害社會的結果，並且希望或者放任這種結果發生，因而構成犯罪的，是故意犯罪。*

故意犯罪，應當負刑事責任。

第十五條 應當預見自己的行為可能發生危害社會的結果，因為疏忽大意而沒有預見，或者已經預見而輕信能夠避免，以致發生這種結果的，是過失犯罪。

過失犯罪，法律有規定的才負刑事責任。

第十六條 行為在客觀上雖然造成了損害結果，但是不是出於故意或者過失，而是由於不能抗拒或者不能預見的原因所引起的，不是犯罪。"

"in violation of State regulations"

2.55 Common to all the relevant offences in Articles 285 and 286 of the PRC Criminal Law is a requirement that the perpetrator has done the acts "in violation of State regulations". Article 96 of the PRC Criminal Law explains that "violation of State regulations" means:

> *"violation of the laws enacted or decisions made by the National People's Congress or its Standing Committee and the administrative rules and regulations formulated, the administrative measures adopted and the decisions or orders promulgated by the State Council."*[49]

2.56 No official source in Mainland China exhaustively sets out all relevant State regulations. This Consultation Paper highlights the State regulations that appear to be the most relevant.

2.57 According to Article 27 of the Cybersecurity Law of the PRC:

> *"Individuals or organizations shall not engage in the activities endangering cybersecurity such as illegally invading others' cyberspaces, disturbing the normal function of others' cyberspaces or stealing cyber data; they shall not provide the programs or instruments used specially for engaging in the activities endangering cybersecurity such as invading others' cyberspaces, disturbing the normal function of others' cyberspaces or stealing cyber data; if they know that any individual or organization engages in activities endangering cybersecurity, they shall not provide technical support, advertising and promotion, payment settlement or any other assistance to such individual or organization."*[50]
>
> (emphasis added)

2.58 Pursuant to Article 7 of the Regulations of the PRC for Safety Protection of Computer Information Systems:

> *"No organization or individual may make use of computer information systems to engage in activities harmful to the interests of the State or collectives, or the legitimate rights of the*

---

49 The English translation of Article 96 is the official version published by the Legislative Affairs Commission of the NPCSC in 1997. Article 96 reads "*本法所稱違反國家規定，是指違反全國人民代表大會及其常務委員會制定的法律和決定，國務院制定的行政法規、規定的行政措施、發佈的決定和命令。*"

50 The English translation of Article 27 of the Cybersecurity Law is based on the version published by Westlaw China. Article 27 of 《中華人民共和國網絡安全法》 states that "*任何個人和組織不得從事非法侵入他人網絡、干擾他人網絡正常功能、竊取網絡數據等危害網絡安全的活動；不得提供專門用於從事侵入網絡、干擾網絡正常功能及防護措施、竊取網絡數據等危害網絡安全活動的程序、工具；明知他人從事危害網絡安全的活動的，不得為其提供技術支持、廣告推廣、支付結算等幫助。*"

citizens, nor endanger the safety of computer information systems."[51]

(emphasis added)

2.59 Article 6 of the Measures for Security Protection Administration of the International Networking of Computer Information Networks also provides that:

"No unit or individual shall engage in the following activities endangering the security of computer information networks:

(1) accessing to computer information networks or using computer information network resources without permission;

(2) cancelling, altering or increasing computer information network functions without permission;

(3) cancelling, altering or increasing the data and application program stored in, or processed or transmitted by computer information networks without permission;

(4) intentionally creating or spreading destructive programs such as computer viruses;

(5) other activities that endanger computer information network security."[52]

(emphasis added)

Article 285 of the PRC Criminal Law

2.60 Article 285(1) of the PRC Criminal Law provides as follows:

---

[51] The English translation of Article 7 of the Regulations of the PRC for Safety Protection of Computer Information Systems is based on the version published by Westlaw China. Article 7 of 《中華人民共和國計算機信息系統安全保護條例》provides that "*任何組織或者個人，不得利用計算機信息系統從事危害國家利益、集體利益和公民合法利益的活動，不得危害計算機信息系統的安全。*"

[52] The English translation of Article 6 of the Measures for Security Protection Administration of the International Networking of Computer Information Networks is based on the version published at http://www.lawinfochina.com/display.aspx?lib=law&id=6247&CGid (accessed on 3 May 2022). Article 6 of 《計算機信息網絡國際聯網安全保護管理辦法》reads "*任何單位和個人不得從事下列危害計算機信息網絡安全的活動：*

（一）未經允許，進入計算機信息網絡或者使用計算機信息網絡資源的；

（二）未經允許，對計算機信息網絡功能進行刪除、修改或者增加的；

（三）未經允許，對計算機信息網絡中存儲、處理或者傳輸的數據和應用程序進行刪除、修改或者增加的；

（四）故意製作、傳播計算機病毒等破壞性程序的；

（五）其他危害計算機信息網絡安全的。"

"Whoever, in violation of State regulations, invades the computer information system in the fields of State affairs, national defence construction or sophisticated science and technology shall be sentenced to fixed-term imprisonment of not more than three years or criminal detention."[53]

(emphasis added)

2.61 Article 285(2) of the PRC Criminal Law further states that:

"Any person who, in violation of the State regulations, invades computer information systems other than the systems prescribed in the preceding paragraph, or uses other technological means to obtain data stored in, or processed or transmitted by that computer information system, or conducts illegal control of that computer information system shall, if the circumstances are serious, be sentenced to a fixed term of imprisonment of not more than three years or criminal detention and be concurrently imposed with a fine, or shall be imposed with a fine alone; if the circumstances are especially serious, such person shall be sentenced to a fixed term of imprisonment of not less than three years but not more than seven years and be concurrently imposed with a fine."[54]

(emphasis added)

Meaning of "computer"

2.62 The Interpretation of the Supreme People's Court and the Supreme People's Procuratorate of Several Issues on the Application of Law in the Handling of Criminal Cases about Endangering the Security of Computer Information Systems ("**Interpretation No 19/2011**") issued in August 2011 directs that the term "computer information system" means a system having the function of automatic data processing, and includes computer, internet equipment, communication equipment, automatic control equipment, etc.[55]

Actus reus

2.63 Under Article 285(1), mere unauthorised access to the specified

---

53 The English translation of Article 285 is the official version published by the Legislative Affairs Commission of the NPCSC in 1997. Article 285(1) reads: "*違反國家規定，侵入國家事務、國防建設、尖端科學技術領域的計算機信息系統的，處三年以下有期徒刑或者拘役。*"

54 Article 285(2) reads: "*違反國家規定，侵入前款規定以外的計算機信息系統或者採用其他技術手段，獲取該計算機信息系統中存儲、處理或者傳輸的數據，或者對該計算機信息系統實施非法控制，情節嚴重的，處三年以下有期徒刑或者拘役，並處或者單處罰金；情節特別嚴重的，處三年以上七年以下有期徒刑，並處罰金。*"

55 The English translation of Interpretation No 19/2011 is based on the version published by Westlaw China. Article 11 of《最高人民法院、最高人民檢察院關於辦理危害計算機信息系統安全刑事案件應用法律若干問題的解釋》provides that "'*計算機信息系統*'和'*計算機系統*'，*是指具備自動處理數據功能的系統，包括計算機、網絡設備、通信設備、自動化控制設備等。*"

types [56] of computer information systems would constitute an offence. For other types of computer information systems, Article 285(2) provides that the perpetrator must, in addition to mere unauthorised access, obtain the data stored in or handled by that computer information system in order to incur criminal liability.

Unauthorised nature of an access

2.64 According to case number 36 in the 9th batch of guiding cases issued by the Supreme People's Procuratorate of the PRC ("**SPP's Guiding Cases**")[57], the term "invade" in Article 285(1) means the act of illegal access to a computer information system without the victim's consent. It includes access to a computer information system by breaking the defence system using technical means, gaining access without authority, and gaining access in excess of authority.[58]

New Zealand

Sections 249 and 252 of the Crimes Act 1961

2.65 The Crimes Act 1961 in New Zealand ("**New Zealand Act**") provides for three offences relevant to this Chapter, with maximum sentences of different severity. Among them, the offence under section 252 ("*Accessing computer system without authorisation*") has the lightest maximum sentence:

> *"(1) Every one is liable to imprisonment for a term not exceeding 2 years who intentionally accesses, directly or indirectly, any computer system without authorisation, knowing that he or she is not authorised to access that computer system, or being reckless as to whether or not he or she is authorised to access that computer system.*
>
> *(2) To avoid doubt, subsection (1) does not apply if a person who is authorised to access a computer system accesses that computer system for a purpose other than the one for which that person was given access."*

---

56 See para 2.60 above.

57 According to Article 15 of the Provisions of the Supreme People's Procuratorate on Case Guidance Work (《最高人民檢察院關於案例指導工作的規定》), the people's procuratorates may quote relevant guiding cases as the basis for law interpretation and argumentation (but shall not use them to replace laws or judicial interpretations as the direct legal basis).

58 《最高人民檢察院公佈第九批指導性案例》, case number 36 (衛夢龍、龔旭、薛東東非法獲取計算機信息系統數據案), where the directive significance of the case points out that "*非法獲取計算機信息系統數據罪中的"侵入"，是指違背被害人意願、非法進入計算機信息系統的行為。其表現形式既包括採用技術手段破壞系統防護進入計算機信息系統，也包括未取得被害人授權擅自進入計算機信息系統，還包括超出被害人授權範圍進入計算機信息系統。*"

2.66 The other two offences appear in section 249 of the New Zealand Act ("*Accessing computer system for dishonest purpose*"):

> *"(1) Every one is liable to imprisonment for a term not exceeding 7 years who, directly or indirectly, accesses any computer system and thereby, dishonestly or by deception, and without claim of right,—*
>
> *(a) obtains any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or*
>
> *(b) causes loss to any other person.*
>
> *(2) Every one is liable to imprisonment for a term not exceeding 5 years who, directly or indirectly, accesses any computer system with intent, dishonestly or by deception, and without claim of right,—*
>
> *(a) to obtain any property, privilege, service, pecuniary advantage, benefit, or valuable consideration; or*
>
> *(b) to cause loss to any other person.*
>
> *(3) In this section,* ***deception*** *has the same meaning as in section 240(2)."*[59]

2.67 It would be noted that section 249(1) and (2) is phrased similarly. The key difference is that:

(a) the former requires a defendant to have obtained property, privilege, etc, or caused loss; whereas

(b) the latter only requires a defendant to have acted with intent to obtain property, privilege, etc, or cause loss.

Such difference explains the disparity in the maximum sentences of the two offences stipulated by section 249(1) and (2).

Meaning of "computer system" and "computer"

2.68 Under section 248 of the New Zealand Act, the term "computer system":

---

[59] S 240(2) defines deception to mean the following:
"*(a) a false representation, whether oral, documentary, or by conduct, where the person making the representation intends to deceive any other person and—*
(i) knows that it is false in a material particular; or
(ii) is reckless as to whether it is false in a material particular; or
(b) an omission to disclose a material particular, with intent to deceive any person, in circumstances where there is a duty to disclose it; or
(c) a fraudulent device, trick, or stratagem used with intent to deceive any person."

"(a) means—

(i) a computer; or

(ii) 2 or more interconnected computers; or

(iii) any communication links between computers or to remote terminals or another device; or

(iv) 2 or more interconnected computers combined with any communication links between computers or to remote terminals or any other device; and

(b) includes any part of the items described in paragraph (a) and all related input, output, processing, storage, software, or communication facilities, and stored data."

2.69 The New Zealand Act does not define what a computer is. While this approach prevents technological advances rendering the law outdated, there may be cases in which a defendant's guilt or innocence hinges on whether the device used by him or her amounts to a computer at law[60] (an issue far removed from the question whether the defendant's conduct – factually and morally – deserves criminal sanctions).

2.70 A New Zealand authority on this issue is *Pacific Software Technology Ltd v Perry Group Ltd*,[61] which concerned a copyright dispute over computer programs. The New Zealand Court of Appeal characterised digital computer and computer program as follows:

> *"Digital computers rest on five functional elements: (i) input; (ii) storage of that input by a memory system; (iii) a control unit which receives data from memory and gives instructions for the necessary arithmetic; (iv) an arithmetic which carries out the control commands; and (v) an output capacity.*
>
> *A computer program is simply a set of instructions to the computer. Most programs accept and process user-supplied data. The fundamental processes utilised by a programmer are algorithms (simply, mechanical computational procedures) which lie at the heart of the program. These algorithms must be developed by the human creativity of the programmer. The program cannot therefore contain any algorithms not already considered by human beings. The advantage of the computer is simply that it can execute these algorithms faster and more accurately than any human being could."*[62]

---

60 This happened in Hong Kong in *律政司司長 訴 王嘉業* [2013] 4 HKLRD 588, HCMA 77/2013 (date of judgment: 29 Apr 2013, with the English translation of the judgment reported as *Secretary for Justice v Wong Ka Yip Ken* [2013] 4 HKLRD 604), cited above when discussing S161.

61 [2004] 1 NZLR 164.

62 Same as above, at 168, paras 25 and 26.

Unauthorised nature of an access

2.71 Section 252(1) explicitly requires an access to be without authorisation, and requires the perpetrator's knowledge or recklessness in that regard, for criminal liability to arise. Section 252(2) goes on, however, to immediately disapply section 252(1) "*if a person who is authorised to access a computer system accesses that computer system for a purpose other than the one for which that person was given access*".

2.72 The New Zealand Court of Appeal in *Watchorn v R* [63] acknowledged that "*the effect of s 252(2) is to exclude access by an employee for an unauthorised purpose from the ambit of that provision.*"[64] In other words, such access does not constitute an offence under section 252. This position seems more lenient than that in Australia. As discussed above, a person who accessed computer data for an ulterior purpose may escape criminal liability under the Australian provision only if a legitimate purpose existed as well.

2.73 The position in New Zealand also appears more forgiving than that under the CMA-EW as elaborated in *Ex parte United States*. As discussed above, the House of Lords in that case rejected the proposition (from *DPP v Bignell*) that a person authorised to access program or data does not breach section 1 of the CMA-EW if the person accesses the computer at the authorised level even though the access was for an unauthorised purpose.

Construction of section 249

2.74 Section 249 of the New Zealand Act does not refer to the concept of authorisation.

2.75 The New Zealand Court of Appeal in *Watchorn v R*[65] remarked as follows concerning the elements of the offence under section 249(1) of the New Zealand Act:

> *"In our view, it is incorrect to describe s 249(1) as requiring that there must be a dishonest purpose for obtaining a benefit. Although the heading to s 249 is 'Accessing computer system for dishonest purpose', that is not an accurate summary of the offence created by s 249(1). The ingredients of s 249(1) do not include a dishonest purpose. The Crown must prove that the defendant accessed a computer system and thereby dishonestly or by deception and without claim of right obtained a benefit.*

---

63 [2014] NZCA 493.

64 Same as above, at para 79. At the same time, fn 33 to the judgment hinted that the exclusion of employees by s 252(2) might not have corresponded to the original intent.

65 See fn 63 above.

[On the facts] … it was not necessary for the Crown to prove what [the defendant's] purpose in making the download [of certain data from his employer's computer system] was. Rather, the Crown was required to prove that he had obtained a benefit, and that he had done so dishonestly and without claim of right."[66]

2.76 The Court also held that while (according to earlier authority) the computer data in question was not "property" within the meaning of section 249(1)(a),[67] "benefit" in the same provision covered "*anything that is of advantage to the person concerned*" rather than limited to financial advantage.[68] It was therefore arguable that the defendant's "*possession and control of, and therefore opportunity to use, the downloaded files constituted a 'benefit' for the purposes of s 249(1)(a).*"[69]

Singapore

Sections 3 and 4 of the CMA-SG

2.77 As pointed out in the Preface, the offences under the CMA-SG are based primarily on the CMA-EW. Just as the CMA-EW outlaws unauthorised access to computer material in section 1, and then provides for an aggravated offence in section 2, the CMA-SG adopts a two-tiered approach. Section 3 of the CMA-SG ("*Unauthorised access to computer material*") is in these terms:

> *"(1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall be liable on conviction —*
>
> *(a) to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both; and*
>
> *(b) in the case of a second or subsequent conviction, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both.*
>
> *(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.*

66 Same as above, at paras 26 and 42.
67 Same as above, at para 22.
68 Same as above, at para 81.
69 Same as above, at para 83.

(3) For the purposes of this section, it is immaterial that the act in question is not directed at —

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer."

2.78 Section 4 of the CMA-SG ("*Access with intent to commit or facilitate commission of offence*") creates the following aggravated offence:

"(1) Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in any computer with intent to commit an offence to which this section applies shall be guilty of an offence.

(2) This section applies to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years.

(3) Any person guilty of an offence under this section shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both.

(4) For the purposes of this section, it is immaterial whether —

(a) the access mentioned in subsection (1) is authorised or unauthorised;

(b) the offence to which this section applies is committed at the same time when the access is secured or at any other time."

Statutory definition of "computer"

2.79 Notwithstanding the similarities between sections 3 and 4 of the CMA-SG on the one hand, and their equivalents in the CMA-EW on the other, it is noteworthy that "computer" is undefined in the CMA-EW but defined in section 2(1) of the CMA-SG to mean the following:

"an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not

include —

(a) an automated typewriter or typesetter;

(b) a portable hand-held calculator;

(c) a similar device which is non-programmable or which does not contain any data storage facility; or

(d) such other device as the Minister may, by notification in the Gazette, prescribe".

2.80 Much of the above definition resembles the statutory language at 18 USC 1030(e)(1)[70] in the USA. A commentator aptly observed that the exclusion of typewriters, typesetters, calculators, etc "*immediately dates the provision and perfectly illustrates the dangers of technically specific language*".[71] With such a topic as cybercrime, the case for legislation to adopt technology neutral language is particularly strong.

USA

Computer Fraud and Abuse Act (18 USC 1030)

2.81 In the USA, whoever carried out the acts relating to any of the various scenarios set out in 18 USC 1030(a) is punishable as provided in section 1030(c). Among those scenarios, the ones relevant to this Chapter are where a person:

"(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined … to require protection against unauthorized disclosure … or any restricted data … with reason to believe that such information … could be used to the injury of the United States [etc] willfully communicates [etc] the same to any person not entitled to receive it [etc];

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

---

70 "*As used in this section … the term 'computer' means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device*".

71 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015), at 65.

(A) information contained in a financial record of a financial institution [etc];

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency …

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value …

(5) (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss."[72]

Unsuccessful attempts to access

2.82 Under section 1030(b), "*[w]hoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.*" This provision and section 477.1(8) of the Criminal Code (Cth) in Australia (which, as stated above, excludes attempts from criminal liability) are diametrically opposed to each other.

Unauthorised nature of an access

2.83 The structure and style of 18 USC 1030 are quite different from those of the legislation in Hong Kong and the jurisdictions considered above. In terms of what Hong Kong can draw on the USA's jurisprudence, one aspect is their courts' detailed analysis of the distinction between an access of a computer "*without authorization*" and an access in a manner "*exceeding authorized access*" as referred to in 18 USC 1030(a).

---

72 18 USC 1030(a)(1)-(5).

2.84 In particular, despite the explanation at 18 USC 1030(e)(6) that "*the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter*", there have been a number of authorities from different circuits on the meaning of the two phrases "*without authorization*" and "*exceeding authorized access*".

2.85 For example, the Court of Appeals for the Second Circuit in *United States v Valle*[73] described the following key issue as one "*that has sharply divided our sister circuits*":

> *"... whether an individual 'exceeds authorized access' to a computer when, with an improper purpose, he accesses a computer to obtain or alter information that he is otherwise authorized to access, or if he 'exceeds authorized access' only when he obtains or alters information that he does not have authorization to access for any purpose which is located on a computer that he is otherwise authorized to access."*

That court, having concluded that both constructions were permissible, was "*required to apply the rule of lenity and adopt the latter construction*".

2.86 *United States v Valle*[74] was in line with the *en banc* decision[75] of the Court of Appeals for the Ninth Circuit in *United States v Nosal*[76] in 2012, which has sparked much academic debate. Adding to the legal uncertainty, the same court in *United States v Nosal*[77] construed "*without authorization*" less favourably to the defendant in a subsequent majority decision.[78] The majority essentially held that only a computer system's owner could authorise a person's access to it, whereas the minority took the view that either the system owner or a legitimate account holder could provide authorisation.

2.87 Soon afterwards, a differently constituted Court of Appeals for the Ninth Circuit in *Facebook, Inc v Power Ventures, Inc*[79] adopted the approach in the second decision in *United States v Nosal*[80] and set forth "*two general rules in analyzing authorization under the CFAA*", ie the Computer Fraud and

---

73 807 F 3d 508 (2d Cir 2015), 3 Dec 2015.

74 Same as above.

75 Rule 35(a) of the Federal Rules of Appellate Procedure states as follows:
"*A majority of the circuit judges who are in regular active service and who are not disqualified may order that an appeal or other proceeding be heard or reheard by the court of appeals en banc. An en banc hearing or rehearing is not favored and ordinarily will not be ordered unless:*
(1) en banc consideration is necessary to secure or maintain uniformity of the court's decisions; or
(2) the proceeding involves a question of exceptional importance."
Under 28 USC 46(c), "*[a] court in banc shall consist of all circuit judges in regular active service, or such number of judges as may be prescribed …*".

76 676 F 3d 854 (9th Cir 2012), Opinion filed on 10 Apr 2012.

77 844 F 3d 1024 (9th Cir 2016), Opinion filed on 5 Jul 2016 and amended on 8 Dec 2016.

78 Same as above.

79 844 F 3d 1058 (9th Cir 2016), Opinion filed on 12 Jul 2016 and amended on 9 Dec 2016.

80 See fn 77 above.

Abuse Act (18 USC 1030):

> *"First, a defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly. Once permission has been revoked, technological gamesmanship or the enlisting of a third party to aid in access will not excuse liability. Second, a violation of the terms of use of a website — without more — cannot establish liability under the CFAA."*

2.88 The Supreme Court on 10 October 2017 declined the opportunity to clarify the constructional approach when it denied certiorari[81] (ie refused to hear intended appeals) in *United States v Nosal* and *Facebook, Inc v Power Ventures, Inc*.

The Sub-committee's views

Bespoke cybercrime legislation preferable

2.89 At present, the legislation in Hong Kong does not have an ordinance applicable to cybercrime specifically. Different offences are covered in various Ordinances, some of which are outdated. In comparison, most of the other jurisdictions discussed above either have bespoke cybercrime legislation, or have a part of their codified law dedicated to cybercrime. We are attracted by those jurisdictions' approach because it helps ensure uniformity, comprehensiveness and consistency, eg as regards the definitions of the key concepts in this area.

2.90 We therefore propose a wholesale reform of the current law by enacting a piece of bespoke legislation on cybercrime that will include the offences proposed in this and subsequent Chapters. That said, we are mindful of the importance of existing provisions such as S161 in combatting cybercrime. Although any overlap of offences is best avoided, we propose retaining the existing provisions before it is clear that the new legislation suffices to replace them.

Definition of key terms

2.91 We observe that nowadays, many devices are fitted with a microprocessor and have purpose-specific processing power. The current definition of "computer" in the Oxford English Dictionary, which already reflects the modern state of technology, reads as follows:

---

[81] USA Supreme Court, *Journal of the Supreme Court of the United States* (Oct Term 2017), at 149, available at https://www.supremecourt.gov/orders/journal/Jnl17.pdf (accessed on 3 May 2022).

> "*an electronic device (or system of devices) which is used to store, manipulate, and communicate information, perform complex calculations, or control or regulate other devices or machines, and is capable of receiving information (data) and of processing it in accordance with variable procedural instructions (programs or software); esp. a small, self-contained one for individual use in the home or workplace, used esp. for handling text, images, music, and video, accessing and using the internet, communicating with other people (e.g. by means of email), and playing games*."[82]
>
> (emphasis added)

2.92 A legal definition for "computer" was added to the Evidence Ordinance (Cap 8) in 1984. In the context of admitting documentary evidence in criminal proceedings, a "computer" is defined as "*any device for storing, processing or retrieving information*".[83] Some examples of the devices covered by the expansive dictionary definition (or a literal reading of the statutory definition in the Ordinance quoted above) are thumb drives with encryption feature, rice cookers with fuzzy logic, intelligent lighting systems, webcams, and smart televisions.

2.93 We are also aware of the alternative terminologies adopted in the Russian Convention, which defines "information and communications technology (ICT)" and "ICT device" respectively. "Information and communications technology (ICT)" means "*an assemblage of methods, processes, hardware and software that have been interconnected for the purpose of generating, transforming, transmitting, utilizing and storing information*".[84] Similarly, "ICT device" means "*an assemblage (grouping) of hardware components used / designed for automatic processing and storage of electronic information*".[85] In our view, despite the advances in digital technology, the term "computer", as compared with "ICT device", remains a clear concept that is well understood by the public and widely used in the legislation of the jurisdictions cited in our comparative study.

2.94 We have further considered whether "computer" should be given a statutory definition with reference to the meaning of "ICT device" as adopted in the Russian Convention. In this connection, we remind ourselves of the judgment of the Court of First Instance in *律政司司長 訴 王嘉業*[86]:

> *"69. … the reason why the Legislative Council had left the term 'computer' undefined in s.161 of the Crimes Ordinance was because, with rapid developments in scientific technology, the definition of 'computer' is broad, evolving and non-exhaustive.*

---

82 Oxford English Dictionary (Mar 2022).
83 Evidence Ordinance, s 22A(12).
84 Article 4(f).
85 Article 4(o).
86 [2013] 4 HKLRD 588, HCMA 77/2013 (date of judgment: 29 Apr 2013, with the English translation of the judgment reported as *Secretary for Justice v Wong Ka Yip Ken* [2013] 4 HKLRD 604).

…

> *73. … In construing provisions involving science and technology, a statute should be taken as 'always speaking', and a broad interpretation should be given according to its language, applying to the changing situation subsequent to the enactment, unless it goes beyond the natural meaning of the statutory language, or the result is absurd or manifestly unjust."* [87]

2.95 We reason that the court's view applies to our proposed offences as well. A criminal can intrude any device with processing power for illegitimate purposes, eg forming a botnet for launching a DDOS attack. With the advent of the internet of things, criminals can potentially target more and more devices in the coming few years and it is possible that even the general definition of "ICT device" may fall behind the inexorable development and advancement of information technology at some stage. We acknowledge that the absence of a definition may render it unclear at first glance whether a device deploying relatively novel technology constitutes a "computer". We are, however, also mindful of the difficulties to apply a statutory definition (however well articulated, such as one for "ICT device" as given in the Russian Convention) in practice as defendants may, especially as time passes since the introduction of such statutory definition, attempt to make every technical argument to assert that the "device" in question does not legally constitute a "computer" as originally intended by the legislature. This is even though we can place our trust on the courts to construe, as far as the text permits, any definition added to a bespoke cybercrime legislation flexibly in light of advances in technology to best reflect the true legislative intent. All things considered, we are, on balance, in favour of leaving terms such as "computer" and "computer system" undefined. In any case, this issue may be further explored by the law draftsman during the legislative stage should our recommendations be implemented by the Government.

Outlawing mere unauthorised access

2.96 We deliberated whether the new legislation should prohibit mere unauthorised access against the following legal and practical considerations:

(a) Mere unauthorised access is already an offence in Hong Kong under S27A, although it only applies where a perpetrator obtained the access "*by telecommunications*" and a conviction only results in a fine. Some other jurisdictions (eg England and Wales, and New Zealand) also outlaw mere unauthorised access, albeit with relatively light maximum sentences typically.

---

[87] Same as above, at 621-622 (Barnabas Fung J).

(b) The Explanatory Report comments that "*mere unauthorised intrusion*" into computer systems and data "*should in principle be illegal in itself.*"[88]

(c) Unauthorised access to computer / program or data, such as port scanning (which we discuss in more detail below),[89] happens every moment on the internet for a myriad of reasons, both legitimate and potentially illegitimate. It is not necessarily a human being who accesses (say) a website; robots can crawl unprotected websites as well. Moreover, a layperson would likely have little clue as to whether his or her computer was accessed by someone with or without malice.

(d) In practice, allowing an online user to grant a person a blanket authorisation to scan the user's program or data (so that exemptions for unauthorised scanning does not need to be provided) may not be useful in addressing real-world situations. Apart from the difficulties in defining the perimeter for the scanning, the person so authorised may abuse such authority and use the accessed program or data to such person's advantage, ie for purposes other than cybersecurity. There are also situations where the online user and the operator may not practically be able to enter into a contractual relationship before the scanning happens. For instance, it is not practical for some form of satisfactory contractual relationship to have been first established with every website before a search engine starts crawling through the internet.

2.97 The Sub-committee had some lengthy discussions on (a) the extent to which unauthorised access to computer/program or data is analogous to the scenario in the physical world where a stranger enters an area (eg someone's home) without permission, and (b) whether mere unauthorised access deserves criminal consequences. In the physical world, if a person enters another's home without permission and informs the latter that his door lock is not good enough, the entry itself is wrong, irrespective of whether the intruder stops immediately after passing the main door. We find it difficult to justify the permission of certain conduct in cyberspace which is prohibited in the physical world. We therefore take the view that mere unauthorised access to a computer / program or data should be an offence.

2.98 In the context of such unauthorised access, confusion could arise as to the point at which such access should be outlawed (eg whether it should be outlawed at the point of access, or the point at which the intruder commits further wrongful acts upon access). As it is important for the law to be certain, our majority view is that mere unauthorised access to a computer / program or

---

88 Explanatory Report, at para 44 (cited above at para 2.19).

89 A port is a virtual point where network connections start and end. Ports are software-based and managed by a computer system. Each internet service is associated with a port, eg web access is associated with ports 80 and 443. See also fn 2 in para 2.5.

data should be criminalised as a summary offence, which does not require malice to be an element of the offence, subject to the statutory defence of reasonable excuse.

Unauthorised nature of an access

2.99 As mentioned above,[90] the unauthorised nature of an access is an element of the offence under S27A, but is only read into S161 by the courts.

2.100 In our opinion, the new legislation should explicitly require an access to be unauthorised so as to provide guidance to obviate unnecessary dispute. Having looked at the other jurisdictions' statutes canvassed above, which illustrate various ways to describe the unauthorised nature of an access, we favour section 17(5) and (8) of the CMA-EW as elaborated in *Ex parte United States*.[91] In this connection, we wish to reiterate that the customary practices (of not seeking prior express authorisation for access to the level we have given examples of) that are already generally accepted in daily life when entering the cyberspace should continue to be tolerated for the reason we gave earlier when explaining the concept of "unauthorised" access.[92] It is on this basis that we propose that mere unauthorised access to program or data constitutes an offence. Whether there is implied authorisation for access in a particular case would depend on the facts and circumstances as disclosed in the evidence.

2.101 We further believe that it is fair for our proposed offence to be premised on a person's knowledge that his or her access is unauthorised. We anticipate that the court will likely draw inferences regarding such knowledge based on circumstantial evidence. People should know, by common sense, whether entering a certain place is permissible. In that respect, two contrasting analogies are entering a department store during business hours and going into a bank's vault with its door opened. We are convinced that the same common sense approach would apply in cyberspace. Thus, for example, even if a person's computer device or system is not protected by any password or other security measures, it is our view that the person should not be taken to have consented to every access to the program or data concerned, and that liability for unauthorised access should arise if the access amounts to an intrusion which goes beyond what would ordinarily be accepted in the general usage of cyberspace (eg hacking another person's WhatsApp).

Access to program or data

2.102 Our comparative study reveals that different jurisdictions have

---

90 Paras 2.9 and 2.11.
91 See paras 2.43 to 2.47.
92 See para 2.5.

different preferences in this regard. S27A, section 1 of the CMA-EW and section 3 of the CMA-SG refer to access to program or data, whereas S161 and sections 249 and 252 of the New Zealand Act refer to access to computer and computer system respectively.

2.103 While the meaning of "computer" is rapidly evolving, the terms "program" and "data" are, however, relatively well-defined and static. A "program" is "*a series of coded instructions and definitions which when fed into a computer automatically directs its operation in performing a particular task*",[93] whereas "data" means "*the quantities, characters, or symbols on which operations are performed by a computer, considered collectively*".[94] In non-technical contexts, "data" also means "*information in digital form*".[95] We lean towards referring to access to program or data because that is clearer and can prevent unnecessary association of the offence with any physical device. A computer is only a tool or device. It is the materials it stores, mainly data and program, which are important and the target of any unauthorised access. We consider that referring to access to computer may seem too restrictive.

Defence of reasonable excuse

2.104 We discussed whether to recommend a number of defences applicable to specific circumstances, a catch-all defence based on (say) reasonable excuse for an access, or a mix of them.

2.105 Under the first approach, it is not straightforward to be comprehensive and to devise the criteria for each tailor-made defence. For instance, we analysed whether a defence should be available to particular types of access (eg testing a computer system for a known vulnerability, such as a webcam with a default password, or a computer running an unpatched operating system) or to particular categories of persons (eg cybersecurity practitioners accredited by a recognised professional body). It proved challenging for us to formulate a defence with criteria that both accords with culture and reality, and will not easily give rise to factual disputes from a technological perspective.

2.106 We concluded that a generic defence based on reasonable excuse can better incorporate public interest considerations, cater for unforeseen circumstances and give the court discretion and flexibility in deciding if the accused should be exculpated. We recommend this approach accordingly. The risk of the defence being abused appears to be not a concern because all will depend on the evidence and circumstances of the case. To illustrate this point, even though a defendant's accreditation as a cybersecurity practitioner may be a weighty factor, it will not necessarily

---

93 Oxford English Dictionary (Mar 2022).
94 Same as above.
95 Same as above.

exonerate the defendant in relation to an unauthorised access.

Aggravated offence

2.107 When resolving to propose the summary offence described above, we were alive to the potentially serious harm that an offender may further cause after accessing the program or data in question. For instance, an offender may try to install spyware in the target computer, or may intend to blackmail the victim. The proposed summary offence alone will be an insufficient legislative response to such threat to society.

2.108 Inspired by the legislation of some jurisdictions surveyed above, we propose that unauthorised access with intent to carry out further criminal activity should constitute an aggravated form of the offence under the new legislation. As to what further criminal activity will trigger the aggravated offence, the formulation in section 2(2) of the CMA-EW[96] appeals to us as a starting point.

Model for Hong Kong legislation

2.109 We recommend that the proposed provisions be modelled on sections 1, 2 and 17 of the CMA-EW. Good drafting in other jurisdictions' legislation can be taken into account as appropriate.

Recommendation 1

The Sub-committee recommends that:

(a) Subject to a statutory defence of reasonable excuse, unauthorised access to program or data should be a summary offence under the new legislation.

(b) Unauthorised access to program or data with intent to carry out further criminal activity should constitute an aggravated form of the offence attracting a higher sentence under the new legislation.

(c) The proposed provisions of the new legislation should be modelled on sections 1, 2 and 17 of the CMA-EW.

[96] Quoted above at para 2.50.

Unauthorised access for cybersecurity purposes

2.110 Readers might have noticed our repeated references to cybersecurity practitioners in the discussion above on what defence to our proposed offence should be provided for. This reflects our extensive debates on the notion of unauthorised access for cybersecurity purposes.

2.111 We think it would be helpful to articulate the meaning of "cybersecurity" at the outset. In the definitions given by technology companies and cybersecurity organisations in other jurisdictions,[97] the concept of "cybersecurity" is consistently grounded on the practices of protecting computer systems from digital attacks. The following academic text succinctly captures the essence of "cybersecurity" for the purposes of this Consultation Paper:

> "*Cybersecurity refers to the procedures that are taken to protect computers, networks and programs from a cyberattack or acts of cybercrime (e.g., viruses, malware or ransomware). It is also referred to as information technology security.*"[98]

2.112 It was against the following background that we proceeded to consider the issues surrounding unauthorised access for cybersecurity purposes:

(a) At a global level, there are always some people in cyberspace who are testing others' computers, often without securing the latter's authorisation beforehand. The tools for testing computer data or system are readily available and widely used.

(b) A common form of such test, for instance, is known as port scanning.[99] Even if it only causes the scanned computer to generate log record, but not any adverse impact, any unusual increase in network activity may nonetheless alert the computer's administrator or owner to incur time and expenses in investigating whether the computer has been compromised.

(c) From a technological perspective, whether port scanning already constitutes access to the target computer is debatable.

---

97 For example, the National Cyber Security Centre of the Government of the United Kingdom describes cybersecurity as "*how individuals and organisations reduce the risk of cyber attack"* and refers to the core function of cybersecurity as protecting *"the devices we all use (smartphones, laptops, tablets and computers), and the services we access – both online and at work – from theft or damage*". Similarly, the Cybersecurity and Infrastructure Security Agency of the Government of the United States of America defines cybersecurity as "*the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information*." See https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security and https://www.cisa.gov/uscert/ncas/tips/ST04-001#:~:text=Cybersecurity%20is%20the%20art%20of,integrity%2C%20and%20availability%20of%20information respectively (accessed on 3 May 2022).

98 Marion and Twede, *Cybercrime: An Encyclopedia of Digital Crime* (ABC-CLIO, 2020), at 92.

99 See fn 89 above.

Having said that, it seems a broadly drafted offence of unauthorised access (eg the offence under section 1 of the CMA-EW with "access" as explained by section 17(2)) may apply to port scanning conceptually.

(d) People may test others' computers for benevolent, commercial or malicious purposes. By way of illustration:

(i) During the WannaCry incident in 2017,[100] some cybersecurity experts ran tests and warned computer users if their computer required patching to guard against infection. Those experts' work apparently benefitted society.

(ii) A person may conduct port scanning in order to see whether a computer is updated with the latest patches, which port number of a server is open for connection, etc. The person may charge an exorbitant sum to fix any problem identified. The information can also facilitate further criminal activity, eg infection of the computer with malware.

In the case of port scanning, the log record alone would not reveal a person's intent behind conducting the scan. Computer users who are not technologically savvy may not even know that his or her computer has been scanned.

(e) Some cybersecurity companies scan the internet continuously for common vulnerabilities in webcams, web servers, etc. Those companies may offer to fix any vulnerabilities identified in return for payment. Their clients can also subscribe for information of the vulnerabilities identified which may relate to internet protocol addresses used by a client itself, and possibly also those used by others.

(f) Cybersecurity is a dynamic area. The accreditation landscape keeps changing. Multiple industry organisations are active in Hong Kong and globally among cybersecurity practitioners; no industry organisation is regarded as the sole authority.[101]

---

[100] WannaCry was a piece of ransomware that would scan for computers with an unpatched Microsoft Windows vulnerability over the internet and attempt to infect them. Many computer users across the world, including Hong Kong, were affected. See, for example, the press release issued by the Hong Kong Computer Emergency Response Team Coordination Centre of the Hong Kong Productivity Council on 13 May 2017 at https://www.hkcert.org/my_url/en/articles/17051301 (accessed on 3 May 2022).

[101] Some examples of cybersecurity bodies in Hong Kong are the Professional Information Security Association and the Information Security and Forensics Society. Other bodies affiliated with Hong Kong information technology professionals include the Hong Kong Computer Society, the Hong Kong

(g) At least in Hong Kong, many cybersecurity practitioners have hands-on experience but are not formally accredited. Some years ago, the Hong Kong Monetary Authority acknowledged that there was a limited number of accredited cybersecurity professionals operating here when it undertook the Cybersecurity Fortification Initiative to enhance the cyber resilience of the banking industry.[102]

(h) Preventive cybersecurity service is apparently not very popular in the business sector in Hong Kong. Businesses tend to seek help for remedial action and reinforcement of their computer system only after the occurrence of a cybersecurity incident.

(i) While Hong Kong can choose to enact a new offence that prohibits all kinds of unauthorised testing of a computer, in reality, such offence will not preclude scanning from other jurisdictions of computer systems in Hong Kong.

(j) At any rate, criminals typically use their own networks to scan the internet for vulnerabilities, rather than relying on cybersecurity companies. Prohibiting all kinds of unauthorised testing will affect cybersecurity companies without stopping criminals from identifying the vulnerabilities.

2.113 In the premises, there appears to be scope for different opinions on where to draw the line between permissible access and impermissible access. Some may think that our proposed offence will be too broad if all kinds of unauthorised testing of a computer can lead to criminal liability irrespective of the reasons and whether damage is caused.

2.114 We therefore considered whether the new legislation should allow a defence or exemption for unauthorised access for cybersecurity purposes. It is noted that under the existing law in the data protection context, for example, there is a "news activity" exemption under section 61 of the Personal Data (Privacy) Ordinance (Cap 486).[103] Appreciating the difficulties in balancing the

---

Information Technology Federation, the Hong Kong Information Technology Joint Council and the Hong Kong Internet Service Providers Association.

102 See the Keynote Address of the then Chief Executive of the Hong Kong Monetary Authority at the Cyber Security Summit on 18 May 2016, at para 8, available at https://www.hkma.gov.hk/eng/news-and-media/speeches/2016/05/20160518-2/.

103 "*(1) Personal data held by a data user—*
(a) whose business, or part of whose business, consists of a news activity; and
(b) solely for the purpose of that activity (or any directly related activity),
is exempt from the provisions of—
(i) data protection principle 6 and sections 18(1)(b) and 38(i) unless and until the data is published or broadcast (wherever and by whatever means);
(ii) sections 36 and 38(b).
(2) Personal data is exempt from the provisions of data protection principle 3 in any case in which—
(a) the use of the data consists of disclosing the data to a data user referred to in subsection (1); and

conflicting arguments for and against the proscription of unauthorised access even for cybersecurity purposes, we do not propose to settle on a position at this stage. Instead, we welcome public feedback on the consultation questions set out in Recommendation 2(a) below.

2.115 We wish to point out that if our law should accord any defence or exemption to professionals in the cybersecurity industry (which is a question to be settled only after we have received the public's views), a fundamental issue that has to be addressed is how the identity of such professionals can be ascertained or verified. As mentioned above,[104] at present, cybersecurity practitioners in Hong Kong are not formally recognised by any accrediting or professional body. Thus, one possible solution is to develop some form of accreditation regime to provide a mechanism for certifying cybersecurity professionals, who may then be identified with ease if any proposed defences or exemptions are to be relied on. To help the public give informed opinions for our charting the way forward, the following paragraphs give a broad overview of the mechanisms adopted by other jurisdictions in certifying or otherwise identifying cybersecurity practitioners.

2.116 In the United Kingdom, the "Certified Cyber Professional assured service" ("**CCP system**") has been developed by the National Cyber Security Centre in an effort to build a community of recognised cybersecurity professionals.[105] To acquire certification under the CCP system, applicants must provide proof of breadth of application of cybersecurity foundational knowledge by holding certain qualifications or memberships. Recognition may then be awarded in specialised areas of practice in cybersecurity.[106] In Mainland China, the China Cybersecurity Review Technology and Certification Centre is responsible for accrediting cybersecurity practitioners under the mandate of the Cybersecurity Law of the PRC.[107] We also note that

---

(b) such disclosure is made by a person who has reasonable grounds to believe (and reasonably believes) that the publishing or broadcasting (wherever and by whatever means) of the data (and whether or not it is published or broadcast) is in the public interest.

(3) In this section—

***news activity** (新聞活動) means any journalistic activity and includes—*

(a) the—

(i) gathering of news;

(ii) preparation or compiling of articles or programmes concerning news; or

(iii) observations on news or current affairs,

for the purpose of dissemination to the public; or

(b) the dissemination to the public of—

(i) any article or programme of or concerning news; or

(ii) observations on news or current affairs."

104 Para 2.112(f) and (g).

105 See https://www.ncsc.gov.uk/information/certified-cyber-professional-assured-service (accessed on 3 May 2022). The National Cyber Security Centre is the UK's national technical authority for cybersecurity.

106 Same as above.

107 See https://www.isccc.gov.cn/zxjs/zxjs/index.shtml#intro (accessed on 3 May 2022). The China Cybersecurity Review Technology and Certification Centre (中國網絡安全審查技術與認證中心) was established in 2006. Article 17 of the Cybersecurity Law provides that: "*The State shall facilitate the construction of socialized cyber system for security service and encourage relevant enterprises and institutions to carry out such security services as cybersecurity certification, testing and risk evaluation.*" This English translation is based on the version published by Westlaw China. The Chinese version reads

the Cyber Security Agency of Singapore has put in place a programme to train and upskill cybersecurity professionals with formal requirements on their qualifications and working experiences in information and communication technology.[108]

2.117 On the other hand, we understand that jurisdictions without any accreditation or certification system may lean on international standards, such as those prescribed by the International Accreditation Forum ("**IAF**"),[109] for identifying competent cybersecurity personnel.

2.118 If the public prefers that the law should provide defences or exemptions for cybersecurity practitioners and an accreditation regime for Hong Kong is to be established for this purpose, then we shall consider how the regime should work in practice. Some preliminary thoughts are that an accreditation body may be statutory or administrative in nature, tasked with maintaining an accessible list of cybersecurity professionals. We invite the public to respond to the questions set out under Recommendation 2(a)(i) and (ii) to provide their views on the manner and method of accreditation (eg the criteria for accreditation and any possible continuing education requirements), as well as the operational details of an accreditation regime (eg whether the accreditation body may remove an accredited person or refuse to renew his accreditation if the person fails to satisfy any continuing education requirements, and whether any persons outside the accreditation body should have access to the list of accredited persons).

2.119 If it is felt, nonetheless, that the constantly evolving accreditation landscape[110] poses hindrance to a formal accreditation framework, then we tend to think that the bespoke cybercrime legislation may prescribe the requirements that a person should fulfil in order to come within the defence or exemption that the law allows for unauthorised access for cybersecurity purposes. Some basic requirements may pertain to a person's training qualifications, working experience and integrity (eg whether the person is a fit and proper person). Having said that, for any statutorily prescribed criteria to apply well in practice, it would appear that some reliable means to ascertain whether any given cybersecurity practitioner satisfies the requirements is necessary. We welcome the public's view on any possible alternatives that may equally serve the purpose of having an accreditation regime (ie to make cybersecurity professionals who may benefit from the proposed defence or exemption identifiable), as set out in our questions in Recommendation 2(a)(iii) below.

"國家推進網絡安全社會化服務體系建設，鼓勵有關企業、機構開展網絡安全認證、檢測和風險評估等安全服務。"

108 See the website of the Cyber Security Agency of Singapore, available at https://www.csa.gov.sg/Programmes/CSAT (accessed on 3 May 2022).

109 The IAF is a worldwide association of accreditation bodies and other bodies interested in conformity assessment in the fields of management systems, products, services and, most importantly, personnel. See https://iaf.nu/en/about/ (accessed on 3 May 2022). We understand that certifications accredited by the IAF are widely accepted by governments around the world.

110 Para 2.112(f).

2.120 Last but not least, we are aware that non-security professionals may also engage in the act of illegal access to program or data. Such illegal access denotes the initial stage of an intrusion into a computer system. As we will explain in Chapter 5, subsequent interference with the computer system may constitute an offence and we invite the public's view as to whether there should be any lawful excuse to that offence for non-security professionals.[111] Given the close relationship between the offences proposed in Chapters 2 and 5, we likewise seek public feedback in this regard for the offence of illegal access to program or data (see Recommendation 2(b) below).

Recommendation 2

The Sub-committee invites submissions on whether there should be any specific defence or exemption for unauthorised access:

(a) If the answer is yes for cybersecurity purposes, in what terms? For example:

(i) should the defence or exemption apply only to a person who is accredited by a recognised professional or accreditation body?

(ii) if the answer to subparagraph (i) is yes, how should the accreditation regime work, eg what are the criteria for such accreditation? Should the accredited persons be subject to any continuing education requirements? Should Hong Kong establish an accreditation body (say, under the new cybercrime legislation or otherwise created administratively) that maintains a list of cybersecurity professionals so that, for instance, accredited persons who fail to satisfy the continuing education requirements may be removed from the list or not be allowed to renew their accreditation? Who outside the accreditation body (if any) should also have access to the list?

(iii) alternatively, if an accreditation regime is not preferred, should the new bespoke cybercrime legislation prescribe the requirements for putative cybersecurity professionals to invoke the proposed defence or exemption for cybersecurity purposes? If so, what should these requirements be?

[111] Recommendation 8(b) in Chapter 5.

(b) Should the defence or exemption apply to non-security professionals (please see the examples in Recommendation 8(b))[112]?

Limitation period in summary cases

2.121 Under section 26 of the Magistrates Ordinance (Cap 227), the limitation period for summary offences is generally six months from the time when the matter arose unless the relevant legislation prescribes otherwise. An example is S27A(4)[113] which extends the limitation period to "*3 years of the commission of the offence or within 6 months of the discovery of the offence by the prosecutor, whichever period expires first*".

2.122 We understand that the default limitation period under the Magistrates Ordinance (Cap 227) may be insufficient for investigating a case of cybercrime. A victim may only report a case to the Police two to three months after it occurs or, worse still, by the time when an incident is discovered, the limitation period of six months has already lapsed. It may take another period of two to three months for the Police to obtain log records from an internet service provider. Analysis of the log records may require yet another period of two to three months. Further time to reach a prosecutorial decision must be factored in.

2.123 In light of the above, we recommend extending the limitation period for our proposed offence to two years after discovery of the matter while maintaining its summary nature, ie varying section 26 of the Magistrates Ordinance (Cap 227) for the purpose of that offence. Logically, the same extended limitation period ought to apply to a charge by way of summary proceedings for any of the offences we propose in this Consultation Paper.

Recommendation 3

The Sub-committee recommends that the limitation period applicable to a charge for any of the proposed offences by way of summary proceedings should be two years after discovery of any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence, notwithstanding section 26 of the Magistrates Ordinance (Cap 227).

---

112 The examples in Recommendation 8(b) are web scraping by robots or web crawlers initiated by internet information collection tools (eg search engines) to collect data from servers without authorisation, as well as scanning a service provider's system for identifying vulnerability or ensuring the security and integrity of an Application Programming Interface.

113 Quoted above at para 2.11.

Criminal liability of officers of a corporate offender

2.124 We are cognisant of the fact that cybercrime can be committed by a body corporate with the consent or connivance of its directors or other similar officers. Accordingly, we have considered whether any express provision should be added in the new legislation so that criminal liability can be directly attributed to relevant office bearers in certain circumstances.[114]

2.125 At present, there is a general provision on the liability of directors and other officers of a company under Part VI of the Criminal Procedure Ordinance (Cap 221).[115] We take the view that this general provision is sufficient in the context of cybercrime. Moreover, we trust that further consideration may be given more specifically whether express provisions on the liability of directors and persons in a managerial capacity are needed during the legislative process if our recommendations to create the proposed offence of unauthorised access to program or data are accepted.[116] We have therefore drawn the conclusion that specific recommendation on this issue is not necessary at this stage. We take a similar position towards the other offences proposed in Chapters 3 to 6 of this Consultation Paper.

---

114 For example, s 125(1) of the Copyright Ordinance (Cap 528) provides that "*Where a body corporate commits an offence under this Ordinance in respect of any act which is shown to have been committed with the consent or connivance of, or to be attributable to any act on the part of, any director, manager, secretary or other similar officer of the body corporate or any person purporting to act in any such capacity he, as well as the body corporate, commits the offence.*" There are numerous similar provisions in other legislation of Hong Kong.

115 S 101E of the Criminal Procedure Ordinance (Cap 221) provides that "*Where a person by whom an offence under any Ordinance has been committed is a company and it is proved that the offence was committed with the consent or connivance of a director or other officer concerned in the management of the company, or any person purporting to act as such director or officer, the director or other officer shall be guilty of the like offence.*"

116 Drafting Legislation in Hong Kong - A Guide to Styles and Practices (Department of Justice, 2012), at para 6.2.12.

Chapter 3

Illegal interception of computer data

Introduction

3.1 In this Chapter, we examine the second cyber-dependent offence, ie illegal interception of computer data. Broadly speaking, an offence in respect of this subject matter would seek more specifically to:

(a) outlaw interception of computer data that is analogous to traditional tapping and recording of telephone conversations, and not carried out pursuant to legal authority (eg in a law enforcement context); and

(b) thereby protect people's right to privacy of data communication.

3.2 In today's world, interception of computer data can happen anywhere[1] without requiring any special equipment or advanced knowledge in information technology. For example, it is easy for a person to set up a bogus Wi-Fi hotspot maliciously in order to capture data transmitted from a victim's connected device. More sophisticated means to intercept data may involve creating a "backdoor"[2] or installing a spyware.

Current Hong Kong law

Basic Law

3.3 In general terms, offences that prohibit illegal access and illegal interception are concerned with "data at rest" and "data in motion" respectively. If the former merits protection by law, the latter should be no different.

3.4 Moreover, the concepts of "data in motion" and "communication" are inextricable. It is apposite to start this Chapter by quoting Articles 27 and 30 of the Basic Law, which apply to communication in general:

---

1 Data would leave footprints during its transmission through various devices, which may even retain a copy of the data. A person who controls any of those devices may be able to analyse the data being transmitted.

2 A backdoor is *"[a] feature or defect of a computer system that allows surreptitious unauthorized access to data*." See Oxford University Press, "Lexico.com" (2021) at https://www.lexico.com/definition/back_door (accessed on 3 May 2022).

(a) *"Hong Kong residents shall have freedom of speech ..."*[3]

(b) *"The freedom and privacy of communication of Hong Kong residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communication of residents except that the relevant authorities may inspect communication in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences."*[4]

Hong Kong Bill of Rights

3.5 Articles 14 ("*Protection of privacy, family, home, correspondence, honour and reputation*") and 16(2) ("*Freedom of opinion and expression*") of the Hong Kong Bill of Rights[5] are also on point:

(a) *"No one shall be subjected to arbitrary or unlawful interference with his privacy ... or correspondence ... Everyone has the right to the protection of the law against such interference or attacks."*[6]

(b) *"Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds ..."*[7]

Interception of Communications and Surveillance Ordinance (Cap 589)

Purpose of the Ordinance

3.6 The above Articles in the Basic Law and the Hong Kong Bill of Rights are supplemented by the Interception of Communications and Surveillance Ordinance (Cap 589) ("**ICSO**"), which:

"… provides a statutory regime for the authorisation and regulation of interception of communications and covert surveillance conducted by law enforcement agencies to prevent or detect serious crime and protect public security."[8]

---

3 Article 27.
4 Article 30.
5 Hong Kong Bill of Rights Ordinance (Cap 383), s 8.
6 Article 14.
7 Article 16(2).
8 Website of the Secretariat, Commissioner on Interception of Communications and Surveillance, at https://www.sciocs.gov.hk/en/ordinance.htm (accessed on 3 May 2022).

3.7 The ICSO's emphasis is to regulate when and how law enforcement agencies ("**public officers**") can lawfully encroach on a person's right to private communication, eg by obtaining a "prescribed authorization"[9] for an intended interception of a communication or an intended covert surveillance.

Communication "in the course of its transmission"

3.8 Only the first type of action, ie interception of communication, is relevant for the purposes of this Chapter. Under section 2(1) of the ICSO:

> *" '**intercepting act**' (截取作為), in relation to any communication, means the inspection of some or all of the contents of the communication, in the course of its transmission by a postal service or by a telecommunications system, by a person other than its sender or intended recipient;*
>
> *'**communication**' (通訊) means—*
>
> *(a) any communication transmitted by a postal service; or*
>
> *(b) any communication transmitted by a telecommunications system".*

3.9 So defined, the ICSO only regulates the interception of a communication "*in the course of its transmission*". Section 2(5)(b) explains when a transmission ends (in other words, at which moment the ICSO ceases to apply to the communication in question) in these terms:

> *"For the purposes of this Ordinance ... a communication transmitted by a telecommunications system is not regarded as being in the course of the transmission if it has been received by the intended recipient of the communication or by an information system or facility under his control or to which he may have access, whether or not he has actually read or listened to the contents of the communication."*

Subject of an "intercepting act"

3.10 As stated above, the subject of an "intercepting act" is defined as "*some or all of the contents of [a] communication*". Under section 2(6) of the ICSO:

> *"… the contents of any communication transmitted by a telecommunications system include any data produced in*

[9] Interception of Communications and Surveillance Ordinance, s 2.

association with the communication."

3.11 It appears that such data is essentially metadata, ie information about a communication as opposed to the content or substance of the communication. An example of metadata in cyberspace is information about an email's sender and recipient, which is transmitted together with the email's content. The Code of Practice in respect of the ICSO elaborates as follows:

> *"The capture of such information*[10] *without accessing the actual message of the communication during the course of transmission would still be regarded as interception. However, the obtaining of records, eg call records and telephone bills, after the communication has been transmitted, is not an intercepting act. Records of this type of information may be obtained by search warrant."*[11]

Telecommunications Ordinance (Cap 106)

Damaging telecommunications installation with intent - section 27(b)

3.12 The ICSO only applies to public officers. Outside the context of law enforcement, it is possible for *any person* to commit the following offence under section 27 of the Telecommunications Ordinance (Cap 106):

> *"Any person who damages, removes or interferes in any way whatsoever with a telecommunications installation with intent to —*
>
> *(a) prevent or obstruct the transmission or delivery of a message; or*
>
> *(b) intercept or discover the contents of a message,*
>
> *shall be guilty of an offence and shall be liable on summary conviction to a fine at level 4 and to imprisonment for 2 years."*

---

10 The Ordinance and the Code of Practice refer to "data" and "information" respectively. While it seems unnecessary for present purposes to distinguish between the two terms, they are technically different. The International Organization for Standardization defines "data" and "information" as "*a reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing*" and "*knowledge concerning objects, such as facts, events, things, processes, or ideas, including concepts, that within a certain context has a particular meaning*" respectively. See the definitions at https://www.iso.org/obp/ui/#iso:std:iso:10782:-1:ed-1:v1:en (accessed on 3 May 2022).

11 Secretary for Security, Code of Practice Issued Pursuant to Section 63 of the Interception of Communications and Surveillance Ordinance (Cap 589) (Jun 2016), at para 10.

Potential application to cyberspace

3.13 This Ordinance, which came into force in 1963, may well have used "telecommunications" and related expressions initially with reference to telephones in the 1960s. Yet, those expressions are broadly defined and technology has greatly advanced in recent decades.[12] Arguably, a computer can now amount to a "telecommunications installation"[13] so that section 27(b) applies to the damage or removal of such a computer, or interference with it, with intent to "*intercept or discover the contents of a message*".

Not bespoke provision against cybercrime

3.14 Despite what is mentioned above, the fact remains that section 27(b) is not a bespoke provision against interception of computer data. The statutory language and definitions presuppose a telecommunications context and do not apply well to cyberspace. The following examples would serve to illustrate the point:

> *"**interference** (干擾) means the effect of unwanted energy due to any, or a combination of, emission, radiation or induction upon reception in a telecommunications network, system or installation manifested by any performance degradation, misinterpretation or loss of information which could be extracted from that telecommunications network, system or installation in the absence of such unwanted energy;*
>
> ***message** (訊息) means any communication sent or received by telecommunications or given to a telecommunications officer to be sent by telecommunications or to be delivered".*[14]

3.15 Given the above statutory definitions, if, for example, a person is charged under section 27(b) for, say, interference with a computer with the requisite intent, the prosecution may need to adduce expert evidence in order to establish that (a) the computer amounts to a telecommunications installation, and (b) the defendant's conduct constitutes interference as defined.

3.16 In addition, the subject of an intended interception under section 27(b) is limited to "the contents of a message". This phrase apparently does not cover metadata because section 2(6) of the ICSO (cited above) has

---

12 For example, utilising the technology known as asymmetric digital subscriber line, copper wires used to link up telephones in the past can now support an internet connection.

13 S 2(1) defines "telecommunications installation" to mean "*apparatus or equipment maintained for or in connection with a telecommunications network, telecommunications system or telecommunications service*".
While the Supreme Court of Canada held in *R v McLaughlin* [1980] 2 SCR 331 that a computer system was not a "telecommunication facility" within the meaning of s 287 of the then Criminal Code, that decision was premised on computer technology and usage of the bygone era. One should carefully assess its persuasiveness as an authority nowadays.

14 Telecommunications Ordinance (Cap 106), s 2(1).

no equivalent in the Telecommunications Ordinance (Cap 106). Metadata does not seem to be protected by section 27(b) even though it can be as important as "the contents of a message" and potentially valuable in the eyes of a non-party to a communication in question.

Standard of criminalisation under the Budapest Convention

3.17 Article 3 in Title 1 under section 1 of the Budapest Convention[15] (quoted below) addresses the subject matter of this Chapter:

> *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system."*

3.18 The Explanatory Report comments on Article 3 as follows:

> *"51. This provision aims to protect the right of privacy of data communication. The offence represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons. The right to privacy of correspondence is enshrined in Article 8 of the European Convention on Human Rights. The offence established under Article 3 applies this principle to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer.*
>
> *…*
>
> *53. Interception by 'technical means' relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes. The requirement of using technical means is a restrictive*

[15] See para 11 of the Preface and paras 1.6 to 1.10 of Chapter 1 for background information regarding the Budapest Convention.

qualification to avoid over-criminalisation.

54. The offence applies to 'non-public' transmissions of computer data. The term 'non-public' qualifies the nature of the transmission (communication) process and not the nature of the data transmitted. The data communicated may be publicly available information, but the parties wish to communicate confidentially. Or data may be kept secret for commercial purposes until the service is paid, as in Pay-TV. Therefore, the term 'non-public' does not per se exclude communications via public networks. Communications of employees, whether or not for business purposes, which constitute 'non-public transmissions of computer data' are also protected against interception without right under Article 3 ...

55. The communication in the form of transmission of computer data can take place inside a single computer system (flowing from CPU to screen or printer, for example), between two computer systems belonging to the same person, two computers communicating with one another, or a computer and a person (eg through the keyboard). Nonetheless, Parties may require as an additional element that the communication be transmitted between computer systems remotely connected.

56. It should be noted that the fact that the notion of 'computer system' may also encompass radio connections does not mean that a Party is under an obligation to criminalise the interception of any radio transmission which, even though 'non-public', takes place in a relatively open and easily accessible manner and therefore can be intercepted, for example by radio amateurs.

…

58. For criminal liability to attach, the illegal interception must be committed 'intentionally', and 'without right'. The act is justified, for example, if the intercepting person has the right to do so, if he acts on the instructions or by authorisation of the participants of the transmission (including authorised testing or protection activities agreed to by the participants), or if surveillance is lawfully authorised in the interests of national security or the detection of offences by investigating authorities. It was also understood that the use of common commercial practices, such as employing 'cookies', is not intended to be criminalised as such, as not being an interception 'without right'. With respect to non-public communications of employees protected under Article 3 (see above paragraph 54), domestic law may provide a ground for legitimate interception of such communications. Under Article 3, interception in such circumstances would be considered as undertaken 'with right'.

59. In some countries, interception may be closely related to the offence of unauthorised access to a computer system. In order to ensure consistency of the prohibition and application of the law, countries that require dishonest intent, or that the offence be committed in relation to a computer system that is connected to another computer system in accordance with Article 2, may also require similar qualifying elements to attach criminal liability in this article. These elements should be interpreted and applied in conjunction with the other elements of the offence, such as 'intentionally' and 'without right'."[16]

Two special cases of data at rest

"Data at rest" versus "data in motion"

3.19 We observed above that broadly speaking, offences that prohibit illegal access and illegal interception are concerned with "data at rest" and "data in motion" respectively. These are both contrasting and, as hinted in paragraphs 46 and 59 of the Explanatory Report,[17] interrelated concepts.

3.20 Apart from the obvious case of data saved in a computer user's storage media, data may be at rest in two circumstances. We will discuss these below and (by way of illustration) briefly look at how they are handled by legislation in certain jurisdictions, before we embark on a comparative study with regard to the topic of illegal interception of computer data.

Data momentarily at rest during transmission

3.21 The first special case arises due to the technology used in some types of internet-based communications. The mechanism, known as "store and forward" delivery, is such that a communication may be temporarily stored multiple times on a network while *en route* to its destination.[18]

3.22 The question is whether the interception offence should apply to data at the sliver of time when it is momentarily at rest during transmission. While not all jurisdictions deal with this question in their legislation, Australian law answers it affirmatively through the deeming provision in section 5F of the Telecommunications (Interception and Access) Act 1979 (Cth) ("**TIAA**") which reads:

---

16 Explanatory Report, at paras 51, 53 to 56, 58 and 59.
17 Quoted in Chapter 1 and earlier in this Chapter respectively.
18 "Store and forward" delivery can be contrasted with streaming media, such as online video clips.

"For the purposes of this Act, a communication:

(a) is taken to start passing over a telecommunications system when it is sent or transmitted by the person sending the communication; and

(b) is taken to continue to pass over the system until it becomes accessible to the intended recipient of the communication."

3.23 Under this provision, the interception offence would apply to a communication throughout its transmission, irrespective of whether the data constituting it happened to be momentarily at rest or in motion when it was allegedly intercepted.

3.24 Without such a provision, highly technical evidence may be required for the prosecution to prove the elements of the offence. For example, a person charged with the interception offence may dispute the factual issue of whether the data obtained by him or her was in motion at the material time (on the basis that a charge for illegal access is more appropriate in principle if the data was then momentarily at rest). Proving this beyond reasonable doubt may not be straightforward.

Data stored in a communication system

3.25 The second special case involves data at rest in a communication system (after reaching the end point of a communication) and accessible by the intended recipient. Everyday examples include messages stored in a mobile phone user's voice mailbox[19] and emails stored in the server of a web-based email service provider. Such data is apparently not subject to the ICSO, which ceases to apply to a communication:

"… if it has been received by the intended recipient of the communication or by an information system or facility under his control or to which he may have access, whether or not he has actually read or listened to the contents of the communication."[20]

3.26 The relevant concept in Australia is "stored communication", which is defined in section 5 of the TIAA to mean:

"… a communication that:

(a) is not passing over a telecommunications system; and

---

19 *R v Coulson (Andrew)* [2013] 2 Cr App R 32.

20 ICSO, s 2(5)(b) (cited above).

(b) is held on equipment that is operated by, and is in the possession of, a carrier; and

(c) cannot be accessed on that equipment, by a person who is not a party to the communication, without the assistance of an employee of the carrier."

3.27 From the perspective of the categorisation of offences under the Budapest Convention, data in this state should be the focus of the prohibition of illegal access rather than illegal interception. However, different jurisdictions criminalise illegal interception under statutes of a different nature, not necessarily in legislation dedicated to cybercrime.

3.28 For instance, the Investigatory Powers Act 2016 in England and Wales ("**IPA**") prescribes, among other things, the circumstances in which an interception of communication is lawful, as well as the circumstances in which it is unlawful to do so. In this regard, whether the data constituting the communication is static or in motion should hardly make any conceptual difference.

3.29 Accordingly, for the purposes of the IPA, the term "interception" is not necessarily used in contradistinction to the concept of "access" in cybercrime legislation (ie the CMA-EW). On the basis that "interception" in the IPA can be understood in the general sense of obtaining the data that constitutes a communication, no conceptual incongruity arises even if the data in question is static.

3.30 This puts in context section 4(4)[21] and (5)[22] of the IPA, which has the practical effect of applying the interception offence under section 3(1) to what would be regarded as a "stored communication" in Australia. Such concept is significant because:

> *"… the increasing use of web-based email services means that it is increasingly likely that the accessed copy will be that which is stored on the carrier's*[23] *equipment, rather than downloaded to the recipient's computer."*[24]

---

21 "*In this section 'relevant time', in relation to a communication transmitted by means of a telecommunication system, means—*
(a) any time while the communication is being transmitted, and
(b) any time when the communication is stored in or by the system (whether before or after its transmission)."

22 "*For the purposes of this section, the cases in which any content of a communication is to be taken to be made available to a person at a relevant time include any case in which any of the communication is diverted or recorded at a relevant time so as to make any content of the communication available to a person after that time.*"

23 The carrier is the provider of the service of carrying communications. That would typically be the operator of a telecommunications network.

24 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015), at 187.

3.31 Conceptually, when a communication has been downloaded or saved on the recipient's computer (ie no longer remaining in any communication system), any illegal access to the data constituting the communication would be subject to the offences of illegal access to program or data reviewed in Chapter 2.

Statutory regimes in other jurisdictions

Australia

Criminal Code (Cth) irrelevant

3.32 In Australia, Part 10.7 of the Criminal Code (Cth) deals with computer offences. As mentioned in Chapter 2, the main kinds of conduct outlawed under that Part are unauthorised access to computer data, unauthorised modification of computer data, and unauthorised impairment of electronic communication. Pursuant to section 476.1(1):

> *"**impairment of electronic communication to or from a computer** includes:*
>
> *(a) the prevention of any such communication; or*
>
> *(b) the impairment of any such communication on an electronic link or network used by the computer;*
>
> *but does not include a mere interception of any such communication."*

3.33 The proviso above suggests that the Criminal Code (Cth) is irrelevant for the purposes of this Chapter.

Interception offence under the TIAA

3.34 Instead, the TIAA's provisions are relevant. Under section 7(1), unless any exception applies:

> *"A person shall not:*
>
> *(a) intercept;*
>
> *(b) authorize, suffer or permit another person to intercept; or*

(c) do any act or thing that will enable him or her or another person to intercept;

a communication passing over a telecommunications system."

3.35 Section 7(2) to (10) then sets out detailed exceptions. Section 105 of the TIAA stipulates that contravention of section 7(1) is an indictable offence punishable by imprisonment for up to two years.

3.36 Section 7(1) operates in conjunction with section 5F, which (as we mentioned above when considering data momentarily at rest during transmission) effectively applies section 7(1) to a communication throughout its transmission, irrespective of whether the data constituting it happened to be momentarily at rest or in motion.

Stored communication

3.37 Once a communication becomes accessible to the recipient, it is regulated by Chapter 3 of the TIAA as a "stored communication".[25] We discussed this term's statutory definition in paragraph 3.26 above when examining data stored in a communication system.

Metadata

3.38 Unless any exception applies, Chapter 4 of the TIAA generally prohibits access to "telecommunications data" which is essentially metadata:

> *"Telecommunications data is information about a telecommunication, but does not include the content or substance of the communication … In relation to internet based applications, telecommunications data includes the Internet Protocol (IP) address used for the session, the websites visited, and the start and finish time of each session."*[26]

Potential limitation of the TIAA

3.39 As with section 27(b) of the Telecommunications Ordinance (Cap 106) in Hong Kong, the TIAA's references to "telecommunications" potentially restrict its application. As a commentator has observed:

---

[25] Subject to prescribed exceptions, s 108 of the TIAA prohibits access to a stored communication where the access is unknown to its sender or intended recipient.

[26] Parliament of the Commonwealth of Australia, House of Representatives, Explanatory Memorandum for the Telecommunications (Interception and Access) Amendment Bill 2007, available at https://www.legislation.gov.au/Details/C2007B00124/Explanatory%20Memorandum/Text (accessed on 3 May 2022).

> *"Offences concerned with the unauthorised interception of communications are not new and are found in each jurisdiction. Such offences have generally evolved from provisions concerned with interception of telephone calls over public telecommunication networks, and many of the challenges which arise have been associated with their application to digital communications."*[27]

Canada

Section 342.1(1)(b) of the Criminal Code 1985

3.40 In Chapter 2, we referred to section 342.1(1) of the Criminal Code 1985 in Canada. Among that provision's four limbs, the most relevant one to this Chapter is paragraph (b) under which a person who, fraudulently and without colour of right, by means of an electro-magnetic, acoustic, mechanical or other device, intercepts "*any function of a computer system*" or causes it to be intercepted is guilty of an offence and liable to imprisonment for up to ten years if convicted on indictment.

3.41 We also saw in Chapter 2 the expansive definitions of "function" and "computer system" in section 342.1(2) of the Criminal Code 1985. Specifically, "function" includes (but is not limited to) "*communication or telecommunications to, from or within a computer system*". On its face, the *actus reus* of the offence under section 342.1(1)(b) covers many possible scenarios.

3.42 The *mens rea* of the offence ("*fraudulently and without colour of right*") is relatively specific. For example, mere knowledge (of a person that he or she has intercepted "any function of a computer system" or caused its interception) or recklessness would not suffice.

Section 184(1) of the Criminal Code 1985

3.43 Section 184(1) in Part VI ("*Invasion of Privacy*") of the Criminal Code 1985 creates another offence that is relevant to this Chapter:

> *"Every person who, by means of any electro-magnetic, acoustic, mechanical or other device, knowingly intercepts*[28] *a private communication*[29] *is guilty of*

---

27 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015), at 149.

28 S 183 of the Criminal Code 1985 defines "intercept" to include "*listen to, record or acquire a communication or acquire the substance, meaning or purport thereof*".

29 S 183 of the Criminal Code 1985 defines "private communication" to mean:
"*any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based*

(a) an indictable offence and liable to imprisonment for a term of not more than five years; or

(b) an offence punishable on summary conviction."

3.44 Section 184(2) and (3) then sets out certain exclusions. For instance, section 184(2)(c) provides that section 184(1) does not apply to:

> *"a person engaged in providing a telephone, telegraph or other communication service to the public who intercepts a private communication,*
>
> *(i) if the interception is necessary for the purpose of providing the service,*
>
> *(ii) in the course of service observing or random monitoring necessary for the purpose of mechanical or service quality control checks, or*
>
> *(iii) if the interception is necessary to protect the person's rights or property directly related to providing the service".*

Comparison between sections 342.1(1)(b) and 184(1)

3.45 The offences under sections 342.1(1)(b) and 184(1) are committed by substantially the same means, ie interception "by means of [an/any] electro-magnetic, acoustic, mechanical or other device". Apparently, the respective *actus reus* under both sections can cover an interception targeted at a computer system. It would be open for the prosecuting authority to justify laying a charge against a person carrying out such interception so targeted under section 342.1(1)(b) on the ground that it is the more specific provision and only when the requisite *mens rea* of "fraudulently and without colour of right" is alleged.

3.46 At the same time, a person who carried out an interception not targeted at a computer system can only be charged under section 184(1),[30] and would not be subject to the heavier maximum sentence under section 342.1(1)(b),[31] even if the person acted fraudulently and without colour of right. One may say the involvement or otherwise of a computer system is

---

telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it".

30 "*Every person who, by means of any electro-magnetic, acoustic, mechanical or other device, knowingly intercepts a private communication is guilty of*
(a) an indictable offence and liable to imprisonment for a term of not more than five years; or
(b) an offence punishable on summary conviction."

31 "*Everyone is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years, or is guilty of an offence punishable on summary conviction who, fraudulently and without colour of right … (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system*".

not a sufficiently cogent factor to explain the different maximum sentences under the two provisions.

England and Wales

Section 3(1) of the IPA

3.47 In England and Wales, the legislation dedicated to cybercrime (the CMA-EW) does not prohibit interception of computer data. Rather, the pertinent statute is section 3(1) of the IPA ("*Offence of unlawful interception*"). Quoting the first two of its seven subsections is sufficient here:

> *"(1) A person commits an offence if—*
>
> *(a) the person intentionally intercepts a communication*[32] *in the course of its transmission by means of—*
>
> *(i) a public telecommunication system,*
>
> *(ii) a private telecommunication system,*[33] *or*
>
> *(iii) a public postal service,*
>
> *(b) the interception is carried out in the United Kingdom, and*
>
> *(c) the person does not have lawful authority to carry out the interception.*
>
> *(2) But it is not an offence under subsection (1) for a person to intercept a communication in the course of its transmission by means of a private telecommunication system if the person—*
>
> *(a) is a person with a right to control the operation or use of the system, or*

---

32 Under s 261(2) of the IPA:
" *'Communication', in relation to a telecommunications operator, telecommunications service or telecommunication system, includes—*
(a) anything comprising speech, music, sounds, visual images or data of any description, and
(b) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus."

33 The definitions of "public telecommunication system" and "private telecommunication system" in s 261 of the Act are not particularly illuminating. That said, the Act apparently presupposes that computer data can be transmitted by means of a telecommunication system. For example, s 62(7) defines an "internet connection record" to mean:
"*… communications data which may be used to identify … a telecommunications service to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program …*".

(b) has the express or implied consent of such a person to carry out the interception."

3.48 Sections 4, 5 and 6 of the IPA explain the meaning of "interception", when interception is to be regarded as carried out in the UK, and when a person has lawful authority to carry out an interception.

Stored communication

3.49 As we remarked above when addressing the treatment of data stored in a communication system, section 4(4) and (5) of the IPA in effect applies the interception offence under section 3(1) to what would be regarded as a "stored communication" in Australia.

Metadata

3.50 In cases involving a telecommunication system, in contrast with a public postal service, section 4(1) of the IPA (set out below) effectively restricts the offence under section 3(1) to interception of the "content" of a communication:

> *"For the purposes of this Act, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if—*
>
> *(a) the person does a relevant act in relation to the system, and*
>
> *(b) the effect of the relevant act is to make any content of the communication available, at a relevant time, to a person who is not the sender or intended recipient of the communication.*
>
> *For the meaning of 'content' in relation to a communication, see section 261(6)."*

3.51 Section 261(6) of the IPA is in these terms:

> *" 'Content' … means any element of the communication, or any data attached to or logically associated with the communication, which reveals anything of what might reasonably be considered to be the meaning (if any) of the communication, but—*
>
> *(a) any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be disregarded, and*

(b) anything which is systems data[34] *is not content."*

3.52 In short, it seems that "content" of a communication does not include metadata, for which the term "communications data" is used in the IPA. This term is elaborately defined in section 261(5) and essentially covers "entity data" and "events data" as defined in section 261(3) and (4) respectively. Under section 11(1) of the IPA:

> *"A relevant person who, without lawful authority, knowingly or recklessly obtains communications data from a telecommunications operator or a postal operator is guilty of an offence."*

3.53 Section 11(2) defines a "relevant person" to mean "*a person who holds an office, rank or position with a relevant public authority (within the meaning of Part 3)*" of the IPA. This suggests that section 11(1) only offers limited protection to "communications data" because it does not apply to interception by the general public at large.

*Section 48(1)(a) of the Wireless Telegraphy Act 2006 ("**WTA**")*

3.54 Separately, section 48 of the WTA ("*Interception and disclosure of messages*") should be mentioned. A person commits an offence under section 48(1)(a):

> *"… if, without lawful authority … he uses wireless telegraphy apparatus*[35] *with intent to obtain information as to the contents, sender or addressee of a message (whether sent by means of wireless telegraphy or not) of which neither he nor a person on whose behalf he is acting is an intended recipient".*

3.55 It seems that there could be conduct liable to prosecution under both section 48(1)(a) of the WTA and section 3(1) of the IPA. Section 48(3A) acknowledges this by stipulating, in effect, that the IPA takes precedence over

---

[34] S 263(4) of the IPA defines "systems data" to mean:
"*… any data that enables or facilitates, or identifies or describes anything connected with enabling or facilitating, the functioning of any of the following—*
(a) a postal service;
(b) a telecommunication system (including any apparatus forming part of the system);
(c) any telecommunications service provided by means of a telecommunication system;
(d) a relevant system (including any apparatus forming part of the system);
(e) any service provided by means of a relevant system."

[35] Ss 116(2) and 117(1) of the WTA define "wireless telegraphy apparatus" to mean apparatus for the emitting or receiving, over paths that are not provided by any material substance constructed or arranged for the purpose, of electromagnetic energy (of a prescribed range of frequency) that:
(a) serves for conveying messages, sound or visual images (whether or not the messages, sound or images are actually received by anyone), or for operating or controlling machinery or apparatus; or
(b) is used in connection with determining position, bearing or distance, or for gaining information as to the presence, absence, position or motion of an object or of a class of objects.
So defined, the term appears to include, among other things, devices such as a Wi-Fi router and a smartphone with Bluetooth or NFC (near-field communication) connectivity.

the WTA:

> *"A person does not commit an offence under this section consisting in any conduct if the conduct—*
>
> *(a) constitutes an offence under section 3(1) of the Investigatory Powers Act 2016 (offence of unlawful interception), or*
>
> *(b) would do so in the absence of any lawful authority (within the meaning of section 6 of that Act)."*

Mainland China

Article 285(2) of the PRC Criminal Law

3.56 Article 285(2) makes it an offence if "*any person who, in violation of the State regulations, invades computer information systems other than the systems [in the fields of State affairs, national defence construction or sophisticated science and technology], … to obtain data stored in, or processed or transmitted by that computer information system*".

(emphasis added)

Subject of an interception

3.57 Article 285(2) refers generally to data transmitted by the invaded computer information system. It does not distinguish between contents of a communication and metadata. As such, it appears that Article 285(2) would apply to metadata.

3.58 Furthermore, since Article 285(2) also protects the data stored in and handled by the computer information system, the offence also applies to data at rest, eg data momentarily at rest during transmission and data stored in a communication system.

New Zealand

Section 216B of the New Zealand Act

3.59 The relevant statutory provision is section 216B of the New Zealand Act ("*Prohibition on use of interception devices*"). It is located in Part 9A of the New Zealand Act concerning crimes against personal privacy, and not among sections 248 to 252 which deal with crimes involving computers. Section 216B reads as follows:

"(1) Subject to subsections (2) to (5), every one is liable to imprisonment for a term not exceeding 2 years who intentionally intercepts any private communication by means of an interception device.

(2) Subsection (1) does not apply where the person intercepting the private communication—

(a) is a party to that private communication; or

(b) does so pursuant to, and in accordance with the terms of, any authority conferred on him or her by or under—

(i) the Search and Surveillance Act 2012; or

(ii) Part 4 of the Intelligence and Security Act 2017; or

(iii) the International Terrorism (Emergency Powers) Act 1987.

(3) [Repealed]

(4) Subsection (1) does not apply to any monitoring of a prisoner call under section 113 of the Corrections Act 2004 or any interception of a private communication if the interception is authorised under section 189B of that Act.

(5) Subsection (1) does not apply to the interception of private communications by any interception device operated by a person engaged in providing an Internet or other communication service to the public if—

(a) the interception is carried out by an employee of the person providing that Internet or other communication service to the public in the course of that person's duties; and

(b) the interception is carried out for the purpose of maintaining that Internet or other communication service; and

(c) the interception is necessary for the purpose of maintaining the Internet or other communication service; and

(d) the interception is only used for the purpose of maintaining the Internet or other communication service.

(6) Information obtained under subsection (5) must be destroyed immediately if it is no longer needed for the purpose of maintaining the Internet or other communication service.

(7) Any information held by any person that was obtained while assisting with the execution of a surveillance device warrant issued under the Search and Surveillance Act 2012 must, upon expiry of the warrant, be—

(a) destroyed immediately; or

(b) given to the agency executing the warrant."

3.60 Sections 216C to 216F of the New Zealand Act go on to prescribe related matters, such as prohibitions on disclosure of private communications unlawfully intercepted and on dealing with interception devices.

Statutory definitions of key terms

3.61 Section 216A(1) defines broadly three terms used in section 216B:

*"**intercept**, in relation to a private communication, includes hear, listen to, record, monitor, acquire, or receive the communication either—*

(a) while it is taking place; or

(b) while it is in transit

***interception device**—*

(a) means any electronic, mechanical, electromagnetic, optical, or electro-optical instrument, apparatus, equipment, or other device that is used or is capable of being used to intercept a private communication; but

(b) does not include—

(i) a hearing aid or similar device … ; or

(ii) a device exempted from the provisions of this Part by the Governor-General by Order in Council …

***private communication**—*

(a) means a communication (whether in oral or written form or otherwise) made under circumstances that may

reasonably be taken to indicate that any party to the communication desires it to be confined to the parties to the communication; but

(b) does not include such a communication occurring in circumstances in which any party ought reasonably to expect that the communication may be intercepted by some other person not having the express or implied consent of any party to do so."

3.62 The word "communication" is not separately defined. In any event, the subject of an interception is a private communication that is "taking place" or "in transit". This apparently excludes data momentarily at rest during transmission, and data amounting to "stored communication" in Australia.

Exclusions from the interception offence

3.63 The exclusions in section 216B(2) to (5) mainly relate to law enforcement and necessary interception by a provider of an internet or other communication service.

3.64 Guidance on the exclusion under section 216B(2)(a), ie where the interceptor of a private communication is a party to it, can be found in section 216A(3):

"A reference in this Part to a party to a private communication is a reference to—

(a) any originator of the communication and any person intended by the originator to receive it; and

(b) a person who, with the express or implied consent of any originator of the communication or any person intended by the originator to receive it, intercepts the communication."

Joint study by the Law Commission and the Ministry of Justice

3.65 The Law Commission and the Ministry of Justice of New Zealand, in their joint Issues Paper published on 8 November 2016,[36] referred to a number of issues with the definitions of "intercept" and "private communication" in the Search and Surveillance Act 2012 which are almost identical to those in section 216A(1) of the New Zealand Act.

---

[36] The Law Commission and the Ministry of Justice, *Review of the Search and Surveillance Act 2012 (IP40)*, available at https://www.lawcom.govt.nz/our-projects/search-surveillance-act-2012 (accessed on 3 May 2022). See Chapter 4.

3.66 While the language of section 216B in the New Zealand Act suggests that it is meant to apply to (among other scenarios) interception targeted at a computer, the Issues Paper makes the following points:

> *"4.11 … The test for what is 'private' depends on whether any party to the communication 'ought reasonably to expect that the communication may be intercepted' ... if interception of communications by the State becomes commonplace, it will almost always be reasonable for a person to expect that their communication may be intercepted.*
>
> *…*
>
> *4.19 Another example of a type of communication unlikely to be covered by the definition of 'private communication' is metadata or machine-to-machine communications. In broad terms, metadata is information about electronic activity that does not relate to its content. It includes the data created when forms of electronic communication are made, such as the time and date of a phone call or email, the email addresses or phone numbers of the parties, and the cell towers or IP addresses the communication was sent to and received from. It can also include websites visited by an Internet user.*
>
> *4.20 Metadata can reveal information about relationships, location, identity and activity, which may be a valuable investigative tool. For example, metadata may allow Police to establish that a suspect is in communication with members of a criminal organisation, or has been visiting websites displaying objectionable material.*
>
> *4.21 However, it does not appear to fit within the definition of 'private communication'. This is because the definition refers to the parties to the communication and their intentions, which implies that the communication must be between two or more people."* (emphasis in original)

3.67 The Law Commission and the Ministry of Justice made the following recommendations (among others) in their Report published on 30 January 2018.[37] The Act referenced below is the Search and Surveillance Act 2012 but it appears that the recommendations largely apply as well in the context of section 216B of the New Zealand Act:

[37] Available on the New Zealand Law Commission's website at https://www.lawcom.govt.nz/our-projects/search-surveillance-act-2012 (accessed on 3 May 2022).

(a) The Act should be amended to refer to interception "technology" as opposed to "devices". The definition should be redrafted in a way that includes the use of computer programs, devices and other technological aids.[38]

(b) The definition of "private communication" should be repealed. Wherever the term "private communication" is currently used, it should be replaced with "communication". This will require amendments to the definitions of "intercept" and "interception device".[39]

(c) A provision should be inserted into the Act defining "communication" as including signs, signals, impulses, writing, images, sounds, information, or data that a person or machine produces, sends, receives, processes, or holds in any medium.[40]

(d) The New Zealand Government should consider whether the country should accede to the Budapest Convention.[41]

3.68 The Report by the Law Commission and the Ministry of Justice is awaiting the New Zealand Government's response.

Singapore

Section 6 of the CMA-SG

3.69 Section 6 of the CMA-SG ("*Unauthorised use or interception of computer service*") provides as follows:

> *"(1) Subject to subsection (2), any person who knowingly —*
>
> *(a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service;*
>
> *(b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electromagnetic, acoustic, mechanical or other device; or*

38 Recommendation 14.
39 Recommendation 24. Readers would recall that the Budapest Convention's requirement is to prohibit interception of non-public transmissions of computer data.
40 Recommendation 25.
41 Recommendation 44.

(c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b),

shall be guilty of an offence and shall be liable on conviction —

(d) to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; and

(e) in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the unauthorised access or interception is not directed at —

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer."

3.70 Section 6 of the CMA-SG is modelled on section 301.2(1) of the Criminal Law Amendment Act 1985 in Canada, which has become section 342.1(1) of the Criminal Code 1985 cited above.

3.71 Among the three limbs in section 6(1) of the CMA-SG, limb (b) corresponds to the subject matter of this Chapter. The parallel between its formulation of the *actus reus* (in particular, interception of "any function of a computer by means of an electro-magnetic, acoustic, mechanical or other device") and that under section 342.1(1)(b) in the Criminal Code 1985[42] is obvious. Section 2(1) of the CMA-SG adopts verbatim the broad definition of "function" in section 342.1(2) of the Canadian legislation.

[42] "*Everyone is guilty of an … offence … who, fraudulently and without colour of right … by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system*".

3.72 Despite these similarities, the statutes in Singapore and Canada also have material differences:

(a) In relation to the *mens rea*, knowledge suffices under the Singaporean provision. The Canadian provision requires the perpetrator to have acted "fraudulently and without colour of right".

(b) The interception in question must be "without authority" under the Singaporean provision. That is not an element of the offence as such on the face of the provision in Canada although, arguably, use of the words "without colour of right" implies that only interception without authority is outlawed.

Section 61(b) of the Telecommunications Act 1999

3.73 Separately, under section 61 of the Telecommunications Act 1999 ("*Intentional damage to installation or plant used for telecommunications*") in Singapore:

> *"Any person who intending —*
>
> *(a) to prevent or obstruct the transmission or delivery of any message;*
>
> *(b) to intercept or to acquaint himself or herself with the contents of any message; or*
>
> *(c) to commit mischief,*
>
> *damages, removes, tampers with or touches any installation or plant (or any part of it) used for telecommunications belonging to a public telecommunication licensee or interferes with the radio-communication service or system of a public telecommunication licensee*[43] *shall be guilty of an offence."*

3.74 Limb (b) of this provision can be compared with section 27(b) of the Telecommunications Ordinance (Cap 106) in Hong Kong, which refers to a person's intent to "intercept or discover the contents of a message" and apparently does not cover interception of metadata associated with a message. The latter point seems true with respect to section 61(b) of the Singaporean legislation as well.

---

[43] Under s 6 of the Act:
"*The [Info-communications Media Development] Authority may, with the approval of the Minister, designate any person who has been granted a licence under section 5 as a public telecommunication licensee to perform all or any of the functions relating to the operation and provision of telecommunication systems and services in Singapore within the exclusive privilege of the Authority under this Act.*"

Comparison between Canadian law and Singaporean law

3.75 As noted above,[44] it appears that the offences created by both sections 342.1(1)(b) and 184(1) of the Criminal Code 1985 in Canada apply to cyberspace, but only the latter covers an interception not targeted at a computer system. The different coverage of the two offences may give rise to unfairness given that they have different *mens rea* ("fraudulently and without colour of right" versus "knowingly") and different maximum sentences (imprisonment for ten years versus five years).

3.76 In contrast, neither of the offences created by section 6(1)(b) of the CMA-SG and section 61(b) of the Telecommunications Act 1999 requires a standard of *mens rea* as high as "fraudulently" (only "knowingly" and "intending" respectively). Conviction under either provision can result in a fine not exceeding SGD10,000, or imprisonment for a term not exceeding three years, or both.[45] The two provisions outlaw similar conduct and carry the same maximum sentence which is commensurate with the corresponding *mens rea* prescribed.

3.77 So far as the statutes cited in the two preceding paragraphs are concerned, inconsistency seems to be less of a problem under Singaporean law than Canadian law.

USA

Overview

3.78 The following academic view casts the USA's legislation in a rather unfavourable light:

> "*Surveillance law in the United States has been described by a leading commentator as 'famously complex, if not entirely impenetrable', and by the courts as 'convoluted', 'confusing and uncertain' and an 'evidentiary nightmare'. Major reform of interception laws occurred with the Electronic Communications Privacy Act of 1986 (ECPA), and many of the difficulties arise because the ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication and is 'widely perceived as outdated'.*"[46]

---

44 Paras 3.45 to 3.46.

45 CMA-SG, s 6(1) and the Telecommunications Act 1999, s 85.

46 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015), at 155 (internal citations omitted).

3.79 The same writer also comments that much of the complexity, debate and reform concerning interception law relates to the ability of law enforcement to conduct surveillance, and that case law and commentary in the USA is dominated by the Fourth Amendment protection against unreasonable search and seizure.[47]

3.80 The relevant legislation in the USA now comprises three parts known as the Wiretap Act[48] governing interception of communication content, the Stored Communications Act[49] governing access to stored communications, and the Pen Register Act[50] governing access to traffic data (a category of metadata).

18 USC 2511(1) within the Wiretap Act

3.81 For the purposes of this Chapter, one can focus on 18 USC 2511(1):

> *"Except as otherwise specifically provided in this chapter*[51] *any person who-*
>
> *(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;*
>
> *(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication …*
>
> *(c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;*
>
> *(d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or*

---

47 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015), at 150.
48 Title I of the Electronic Communications Privacy Act, codified at 18 USC 2510 to 2523.
49 Title II of the Electronic Communications Privacy Act, codified at 18 USC 2701 to 2713.
50 Title III of the Electronic Communications Privacy Act, codified at 18 USC 3121 to 3127.
51 Chapter 119 (Wire and Electronic Communications Interception and Interception of Oral Communications) in Part I (Crimes) of Title 18 (Crimes and Criminal Procedure), United States Code.

(e) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted … ,

(ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation,

(iii) having obtained or received the information in connection with a criminal investigation, and

(iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).”

Meaning of wire, oral and electronic communications

3.82 Section 2511(1) distinguishes among wire, oral and electronic communications. Section 2510 defines them as follows:

“(1) ‘wire communication’ means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception … ;

(2) ‘oral communication’ means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

(12) ‘electronic communication’ means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device … ; or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds".

Subject of an interception

3.83 Section 2511(1)(a) proscribes interception of "any wire, oral, or electronic communication", whereas section 2511(1)(c), (d) and (e) applies to the disclosure and use of "the contents of" intercepted communication in prescribed circumstances. Notwithstanding this difference, it appears that the subject of an interception outlawed by section 2511(1)(a) is restricted to a communication's contents because of the following definitions in section 2510:

"(4) 'intercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device;

(8) 'contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication".

Data momentarily at rest during transmission

3.84 Specifically with regard to an "electronic communication", words such as "transfer" and "transmitted" in the term's statutory definition suggest that it refers to a communication in motion. However, the Court of Appeals for the First Circuit held in *United States v Councilman* that the term "*includes transient electronic storage that is intrinsic to the communication process*".[52]

Exclusions from the offences

3.85 The offences created under section 2511(1) do not apply to those who are excluded by way of section 2511(2). Those excluded are mainly:

(a) a provider of wire or electronic communication service;

(b) an officer, employee or agent of the Federal Communications Commission in discharge of law enforcement (monitoring) responsibilities;

---

52 *United States v Councilman*, 418 F 3d 67 (1st Cir 2005), at 85.

(c) an officer, employee or agent of the USA conducting authorised electronic surveillance;

(d) a party to the communication in question; and

(e) an interceptor with prior consent by a party to the communication in question.

The Stored Communications Act (18 USC 2701 to 2713)

3.86 In gist, the Stored Communications Act:

> *"… protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers, such as subscriber name, billing records, or IP addresses."*[53]

3.87 The main provision in the Stored Communications Act is 18 USC 2701(a):

> *"Except as provided in subsection (c) of this section whoever—*
>
> *(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or*
>
> *(2) intentionally exceeds an authorization to access that facility;*
>
> *and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section."*

3.88 The exceptions set forth in 18 USC 2701(c) include conduct authorised:

> *"(1) by the person or entity providing a wire or electronic communications service;*
>
> *(2) by a user of that service with respect to a communication of or intended for that user; or*

---

[53] Bureau of Justice Assistance, "Electronic Communications Privacy Act of 1986 (ECPA)", available at https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285 (accessed on 3 May 2022).

(3) in section 2703,[54] *2704*[55] *or 2518*[56] *of this title."*

The Pen Register Act (18 USC 3121 to 3127)

3.89 The legislation defines two key terms in the Pen Register Act, namely "*pen register*" and "*trap and trace device*", as follows:

> *"(3) the term 'pen register' means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication … ;*
>
> *(4) the term 'trap and trace device' means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication".*[57]

3.90 The Pen Register Act starts with a general prohibition on the use of pen registers and trap and trace devices:

> *"Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523."*[58]

3.91 The next section then provides that an attorney for the USA Government may apply to court for authorisation or approval of the installation and use of a pen register or a trap and trace device.[59]

---

54 "*Required disclosure of customer communications or records*".
55 "*Backup preservation*".
56 "*Procedure for interception of wire, oral, or electronic communications*".
57 18 USC 3127.
58 18 USC 3121(a).
59 18 USC 3122(a)(1).

The Sub-committee's views

Outlawing unauthorised interception of computer data

3.92 We started this Chapter by pointing out that, just as data at rest deserves protection against illegal access, so should data in motion be protected against illegal interception. Both would give rise not only to privacy concerns,[60] but also other potential issues such as use of intercepted data which may cause financial loss.[61]

3.93 To our understanding, an external party can intercept any unencrypted computer data being transmitted in a network that is open for connection,[62] and it is quite possible for transmission of computer data to continue notwithstanding any interception. Any human sender and human recipient of a communication constituted by such data may be unaware of the interception, which may come to light only through a third party.

3.94 To safeguard the integrity of communications, we take the view that unauthorised interception of computer data should be an offence. Unauthorised disclosure or use of the intercepted data should be prohibited as well. Since modern use of different devices constantly involves data in motion (ie data potentially susceptible to unauthorised interception), we hope our proposed offences can, among other things, facilitate and enhance reliable connectivity between devices. We further anticipate that our proposed offence will become even more important when the era of quantum computing (which may allow the retention of all data) arrives.

3.95 Our study of the prevailing legislation in Hong Kong and various other jurisdictions reveals the co-existence of multiple statutes that are relevant to illegal interception of computer data. Apparently, a reason behind this is the need for the law to cover interception of all forms of communication, including communication within and outside cyberspace.

3.96 Given the Sub-committee's mandate, we recommend the enactment of an interception offence applicable to computer data, while leaving the possibility to legislate against the equivalent crime in the physical world for the Government to deliberate. We believe the proposed offence will complement the ICSO, which only applies to public officers.

---

60 The Personal Data (Privacy) Ordinance (Cap 486) only applies to data by which a living individual can be identified, and the penalty stipulated in that Ordinance is comparatively low.

61 For example, wrongful use of credit card details intercepted during transmission to the vendor.

62 Much online communication adopts the protocol known as HTTPS (hypertext transfer protocol secure), under which data is encrypted before transmission. Although one may be able to intercept part of a communication, it would not be plain text and must be decrypted.

Interception for a dishonest or criminal purpose

3.97 The operation of modern networking devices has an element of interception. We acknowledge that, given the prevailing technology, the scope of our proposed offence will be unjustifiably broad if mere unauthorised interception of computer data will result in criminal liability. For instance, we believe not many people would regard the following phenomena as objectionable even if they may involve unauthorised interception:

(a) Analysis of network has become a standard feature of network systems. Statistical information generated by such analysis can show whether a network is abused, how frequently its users accessed a particular website, etc. Such information can be useful for management purposes, eg in prompting a network administrator to block a website at the domain name system ("**DNS**") level.

(b) In the daily operation of an internet service provider, somehow it would possess some data in transit through its equipment. The capture of metadata is a technical necessity in such operation. Moreover, some types of data (eg communication relating to a DNS lookup) would be transient, whereas other types of data (eg DNS log, login data, and email transactions) would not be.

3.98 Having canvassed various possibilities in terms of the *mens rea* under our proposed offence, we have concluded against insisting on proof of an intent to commit *a specific offence* as this may cause excessive difficulty in law enforcement.

3.99 We recommend that under our proposed offence, an interception in question must have been carried out "for a dishonest or criminal purpose".

Offence not to be restricted to private communication

3.100 We mentioned that the offence under Article 3 of the Budapest Convention applies to "non-public" transmissions of computer data.[63] As stated in the Explanatory Report, the term "non-public" qualifies the nature of the transmission (communication) process and not the nature of the data transmitted.[64] In other words, Article 3 of the Budapest Convention does not require the computer data in question to be private.

3.101 We also noted that in New Zealand, the Law Commission and the Ministry of Justice:

---

63 Para 3.17.

64 Explanatory Report, at para 54 (quoted above at para 3.18).

(a) found it unsatisfactory to determine whether a communication is private by reference to whether any party to it "ought reasonably to expect that the communication may be intercepted";[65] and

(b) suggested that references to "private communication" in the Search and Surveillance Act 2012 be replaced with "communication".[66]

3.102 In our view, while the suggestion of the Law Commission and the Ministry of Justice is premised on the statutory definition of "private communication" in New Zealand, their reasoning (which highlights the undesirability to focus on what the parties to a communication expect)[67] is wise counsel for other jurisdictions as well.

3.103 In light of the above considerations, we favour an interception offence that will protect communication in general, rather than just private communication.

Offence to cover all data including metadata

3.104 Broadly speaking, one can contrast metadata in respect of a communication with the content of a communication. Metadata in cyberspace usually relates to things at a protocol level or a system level.

3.105 However, the reality is more complicated from a technological perspective. In particular, the internet adopts a layered approach. Metadata in one layer may be data in another layer. For example, relay information would be data at the network level but metadata in relation to an email. Metadata is not a well-defined concept.

3.106 Separately, although the interception offences in some jurisdictions seem to be inapplicable to metadata, a possible reason is that those offences were introduced many years ago, before the emergence of the modern concept of metadata in the context of electronic or computer communication.

3.107 Taking the above factors into account, we recommend that our proposed offence should apply to data generally, whether it be metadata or not.

---

65 The Law Commission and the Ministry of Justice, *Review of the Search and Surveillance Act 2012 (IP40)*, at para 4.11 (quoted above at para 3.67).

66 Para 3.67(b).

67 As stated in para 3.82, the statutory definition of "oral communication" in the USA also refers to the expectation of a party to the communication.

Offence to apply to data throughout its transmission

3.108 We discussed above[68] the issues relating to data momentarily at rest during transmission.

3.109 For simplicity, we propose that so long as the data in question is *en route* from the sender to the intended recipient, intercepting it should be an offence. One way to achieve this is to introduce a deeming provision along the lines of section 5F of the TIAA as set out in paragraph 3.22 above.

3.110 In relation to data stored in a communication system, we noted above that such data is apparently not subject to the ICSO.[69] Therefore, we suggest that the proposed offence of illegal interception should not apply to such data (which, in our view, should instead be subject to the offence of illegal access proposed in Chapter 2).

Model for Hong Kong legislation

3.111 The relevant statutes in all of the jurisdictions examined are different. In terms of a reference for Hong Kong, section 8 of the Model Law ("*Illegal interception of data etc.*") is closest to what we have in mind:

> *"A person who, intentionally without lawful excuse or justification, intercepts by technical means:*
>
> *(a) any non-public transmission to, from or within a computer system; or*
>
> *(b) electromagnetic emissions from a computer system that are carrying computer data;*[70]
>
> *commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both."*

3.112 The above formulation will have to be adapted so as to reflect our other recommendations. For instance, the provision in Hong Kong:

---

68 Paras 3.21 to 3.24.

69 Para 3.25.

70 The following definition of "computer data" in the Model Law appears consistent with our recommendation that the proposed offence should apply to data generally, including metadata and not restricted to data that constitutes a private communication:
" *'computer data' means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*".

(a) should stipulate that it applies to interceptions carried out without "authority" rather than "justification" (the latter appears to be a broader concept);

(b) should not limit its application to "non-public" transmissions; and

(c) should incorporate the *mens rea* that an interception in question must have been carried out "for a dishonest or criminal purpose".

Recommendation 4

The Sub-committee recommends that:

(a) Unauthorised interception, disclosure or use of computer data carried out for a dishonest or criminal purpose should be an offence under the new legislation.

(b) The proposed offence should:

(i) protect communication in general, rather than just private communication;

(ii) apply to data generally, whether it be metadata or not; and

(iii) apply to interception of data *en route* from the sender to the intended recipient, ie both data in transit and data momentarily at rest during transmission.

(c) The proposed provision should, subject to the above, be modelled on section 8 of the Model Law on Computer and Computer Related Crime, including the *mens rea* (ie to intercept "intentionally").

Conduct which society may regard as proper investigations

3.113 In Chapter 2, we mentioned the potential impact on cybersecurity practitioners that our proposed offence of illegal access may cause. Our Recommendation 2 asks whether there should be a specific defence or

exemption for unauthorised access for cybersecurity purposes.[71]

3.114 When we considered the proposed offence of illegal interception, we likewise discussed whether it may have the unintended consequence of affecting the conduct of what society may regard as proper investigations.

3.115 We welcome comments on this issue from all quarters of society.

Interception by genuine businesses

Prevalence of interception by genuine businesses

3.116 While it is likely that most people would agree that it is wrong to intercept other persons' data maliciously by, for example, setting up a bogus Wi-Fi hotspot (perhaps with a misleading service set identifier), it is worth discussing whether a genuine business – a coffee shop, a hotel, a shopping mall, an employer, etc – which provides its customers or employees with a Wi-Fi hotspot or a computer for use should, in addition to providing network connectivity, be allowed to intercept data being transmitted:

(a) With the advent of data analytics, even a genuine business may be motivated to intercept and potentially derive value from data belonging to or regarding its customers, who may not be aware of the depth of the data analysis that can be (and, in our understanding, often is) carried out.

(b) In an employment relationship, the employer may want to intercept and analyse data transmitted to and from an employee's computer due to suspicion that the employee has, for example, committed a crime, or breached a restrictive covenant in the employment contract by disclosing confidential trade information to a competitor or prospective employer.

Uses of the intercepted data

3.117 The data intercepted in the above-mentioned examples and similar contexts have many possible uses. We outline some of them below:

(a) Vendors of network systems have been marketing a new business to owners of shopping malls. In particular, a network system inside a shopping mall can track the locations of devices (smartphones, tablet computers, etc of patrons visiting the shopping mall) connected to it. The movements of the patrons holding those devices can be tracked. Such location data can:

[71] Paras 2.110 to 2.114.

(i) indicate which shops are patronised more frequently by the users of those devices (who would be target customers of those shops);[72] and

(ii) facilitate location-based service (eg the "pushing" of relevant advertisements, which has become commonplace).

(b) Networking devices have a standard feature of showing which websites are the most popular among users of the network service provided by those devices. An internet service provider can supply the users' data it intercepted to a content ranking company for analysis.

Terms and conditions

3.118 The businesses described above may provide a Wi-Fi hotspot or a computer for use on terms and conditions that reserve the right to intercept and utilise data of their customers or employees, eg to conduct traffic analysis and other types of data analytics. The authority to intercept and utilise the data is contractual in nature.

3.119 In some cases, it is doubtful how many of the customers or employees would peruse or understand those terms and conditions. A related consideration is that although, in principle, the same conduct (data interception) should lead to the same legal consequences irrespective of the size of the business involved, it is typically the larger businesses that can afford to draw up meticulous terms and conditions, which tend to be non-negotiable and slanted towards the business in question.

3.120 One possible way to better protect the customers and the employees is to require the businesses to have statutory authority in order to intercept data lawfully, ie an interception must satisfy certain requirements imposed by legislation. Yet, we foresee that many data analytics will have to stop doing so if one can carry out data analytics only under a statutory authority but not a contractual authority. Some may regard this as too draconian.

Public feedback requested

3.121 In the preceding paragraphs,[73] we have outlined a range of possible examples and circumstances in which professions and genuine businesses may intercept and use the data intercepted or transmitted. We are keen to ensure that our recommendations are fair to all stakeholders and their interests are fairly balanced. We would therefore like to receive the public's

---

[72] The shopping mall's owner may find this information useful in optimising the tenant mix, deciding the appropriate level of rental, etc.

[73] Paras 3.113 to 3.120.

views as to whether the types of data interception and usage identified in the paragraphs above should be allowed. If the response in this regard is affirmative, we would welcome further suggestions on the types of professions and businesses that should be permitted to intercept and use the data intercepted or transmitted, and whether such permission should carry any conditions or restrictions. If the relevant examples and circumstances can be comprehensively identified, we will be in a better position to consider how the proposed defence or exemption should be framed (eg whether these examples and circumstances may be described generically in the new cybercrime legislation with reference to well-recognised legal concepts, such as the existence of legitimate purposes or lawful authority, and the absence of malice) and how such defence or exemption should operate (eg how the burden of proof is discharged).

3.122 We look forward to public feedback on the following consultation questions in Recommendation 5.

Recommendation 5

The Sub-committee invites submissions on:

(a) Should there be a defence or exemption for professions who have to intercept and use the data intercepted in the course of their ordinary and legitimate business? If the answer is yes, what types of professions should be covered by the defence or exemption, and in what terms (eg should there be any restrictions on the use of the intercepted data)?

(b) Should a genuine business (a coffee shop, a hotel, a shopping mall, an employer, etc) which provides its customers or employees with a Wi-Fi hotspot or a computer for use be allowed to intercept and use the data being transmitted without incurring any criminal liability? If the answer is yes, what types of businesses should be covered, and in what terms (eg should there be any restrictions on the use of the intercepted data)?

Chapter 4

Illegal interference of computer data

Introduction

4.1 In this Chapter, we will proceed to examine the third cyber-dependent offence, ie illegal interference of computer data whereas illegal interference of computer system will be the focus of the next chapter. Broadly speaking, an offence in respect of this subject matter would seek to:

(a) combat intentional damage, deletion, alteration, etc of computer data; and

(b) thereby protect the integrity and proper functioning or use of computer data.

4.2 The offence of illegal access, proposed in Chapter 2, focuses on the initial stage of an intrusion into a computer system. As the intrusion progresses, interference of data may constitute the offence to be discussed in this Chapter. The two offences are closely related to each other especially because:

> *"… one argument used in favour of criminalizing mere unauthorized access to a system is that such access can result in non-intentional damage."*[1]

4.3 The offence of data interference may be committed in the following ways:

(a) Modifying a file saved in a computer after accessing it without authority.

(b) Interfering with data by means of a computer virus that can, say, delete specified data stored in an infected computer.

---

1 Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press, 2007), at para 3.268.

Current Hong Kong law

Crimes Ordinance (Cap 200)

Section 60

4.4 At present, Hong Kong law addresses illegal interference of computer data mainly by treating it as a form of criminal damage. Under section 60(1) and (2) of the Crimes Ordinance (Cap 200) ("*Destroying or damaging property*"):

> *"(1) A person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage any such property or being reckless as to whether any such property would be destroyed or damaged shall be guilty of an offence.*
>
> *(2) A person who without lawful excuse destroys or damages any property, whether belonging to himself or another—*
>
> *(a) intending to destroy or damage any property or being reckless as to whether any property would be destroyed or damaged; and*
>
> *(b) intending by the destruction or damage to endanger the life of another or being reckless as to whether the life of another would be thereby endangered,*
>
> *shall be guilty of an offence."*

4.5 It is clear that the offence under section 60(2) is an aggravated form of the offence compared with section 60(1). Their maximum sentences, prescribed in section 63 ("*Punishment of offences*"), differ significantly:

> *"(1) A person guilty … of an offence under section 60(2) … shall be liable on conviction upon indictment to imprisonment for life.*
>
> *(2) A person guilty of any other offence under this Part [ie including section 60(1)] shall be liable on conviction upon indictment to imprisonment for 10 years."*

Legislative amendments in 1993

4.6 The Computer Crimes Ordinance 1993 (No 23 of 1993) extended the meaning of "property" as used in the Crimes Ordinance (Cap 200) to include "*any program, or data, held in a computer or in a computer storage medium,*

whether or not the program or data is property of a tangible nature."[2]

4.7 The Computer Crimes Ordinance 1993 further added section 59(1A) to the Crimes Ordinance (Cap 200), which provides that to destroy or damage any property in relation to a computer includes "misuse of a computer". This phrase is defined in section 59(1A) to mean the following acts:

> *"(a) to cause a computer to function other than as it has been established to function by or on behalf of its owner, notwithstanding that the misuse may not impair the operation of the computer or a program held in the computer or the reliability of data held in the computer;*
>
> *(b) to alter or erase any program or data held in a computer or in a computer storage medium;*
>
> *(c) to add any program or data to the contents of a computer or of a computer storage medium,*
>
> *and any act which contributes towards causing the misuse of a kind referred to in paragraph (a), (b) or (c) shall be regarded as causing it."*

Among the three limbs of section 59(1A), limbs (b) and (c) are the most relevant to this Chapter.

4.8 In addition, the Computer Crimes Ordinance 1993:

(a) applied the offence of making false entry in bank book, etc to entries made on a computer;[3]

(b) extended the offence of burglary to a person entering a building as a trespasser with intent to misuse computer/computer program or data in the building;[4] and

(c) applied the offence of false accounting to records kept by means of a computer.[5]

---

2 Crimes Ordinance (Cap 200), s 59(1)(b).
3 By adding a new s 85(2) to the Crimes Ordinance (Cap 200).
4 By adding a new s 11(3A) to the Theft Ordinance (Cap 210).
5 By adding a new s 19(3) to the Theft Ordinance (Cap 210).

Authorities illustrating successful enforcement

4.9 *HKSAR v Chan Chi Kong*[6] was the first case prosecuted for misuse of computer pursuant to the Crimes Ordinance (Cap 200) as amended in 1993.[7] The defendant pleaded guilty to destroying, without lawful excuse, his employer's computer files installed in the clients' offices. In the appeal against his sentence, the Court of Appeal held that a custodial sentence was justified [8] notwithstanding that the affected computer systems were subsequently restored and what was lost could be retrieved.

4.10 In *HKSAR v Ko Kam Fai*,[9] the male defendant hacked into two female victims' email accounts, altering data in their computers and rendering their email accounts inoperative. His emails to the victims contained obscene materials and a threat of rape. He pleaded guilty to charges of criminal intimidation and criminal damage contrary to sections 24 and 60(1) of the Crimes Ordinance (Cap 200) respectively.

4.11 The damage to the computers was short-term in nature and the defendant was sentenced to four months' imprisonment on each of the eight criminal damage charges. The two criminal intimidation charges were more serious and a longer term of imprisonment (twelve months on each running concurrently with each other and to the sentence relating to the criminal damage charges) was imposed. The defendant's appeal against the sentence for criminal intimidation only was dismissed with a remark by the Court of Appeal that, in relation to the lower sentences for the criminal damage charges, "*whilst they may seem on the face of it to have been short, in the particular circumstances of this case, the gravamen of the offences lay in the criminal intimidation charges*".[10]

Comparison with S161

4.12 While the maximum penalty under section 60 of the Crimes Ordinance (Cap 200) (ordinarily, imprisonment for ten years) is heavier than that under S161 (imprisonment for five years), both provisions apply to cyberspace. In our understanding, people charged under S161 are occasionally also charged under section 60 as an alternative. Depending on the facts of a case, the prosecution may consider section 60 a good fallback for S161:

(a) Evidence of a person intentionally accessing or operating a computer without authorisation can warrant a charge under S161 if the computer is not damaged because it is robust enough.

---

6 [1997] 3 HKC 702, CACC 245/1997 (date of judgment: 25 Sept 1997).

7 According to the submission of counsel for the defendant, mentioned in the judgment at 706H.

8 The sentence of two years and eight months' imprisonment as passed by the District Court was, however, reduced to one of one year and nine months.

9 [2001] 3 HKC 181, CACC 83/2001 (date of judgment: 20 Jun 2001).

10 Same as above, at 185.

(b) However, where the evidence only shows that an alteration of computer data originated from certain internet protocol addresses (from which one can trace to the offender), a charge under section 60 may be more appropriate.

(c) Either intent or recklessness suffices as the *mens rea* under section 60. This is probably more straightforward to prove than the intent as particularised in S161(1)(a) to (d).[11]

Telecommunications Ordinance (Cap 106)

Section 25(a)

4.13 Section 25(a) of the Telecommunications Ordinance (Cap 106) ("*Secretion, etc., of messages by persons other than telecommunications officers*") creates the following summary offence:

> *"Any person, not being a telecommunications officer, or a person who, though not a telecommunications officer, has official duties in connection with a telecommunications service, who—*
>
> *(a) wilfully secretes, detains or delays a message intended for delivery to some other person; or*
>
> *(b) […]*
>
> *shall be guilty of an offence and shall be liable on summary conviction to a fine at level 4*[12] *and to imprisonment for 12 months."*

Not bespoke provision against cybercrime

4.14 The language of section 25(a) appears sufficiently broad to prohibit people from suppressing transmission (by telecommunications) of computer data that constitutes a "message". However, when section 25(a) is applied to computer data, it has limitations similar to those concerning section 27(b) as discussed in Chapter 3:[13]

---

11 Under S161(1), a person must not obtain access to a computer "*(a) with intent to commit an offence;*
(b) with a dishonest intent to deceive;
(c) with a view to dishonest gain for himself or another; or
(d) with a dishonest intent to cause loss to another".

12 Currently $25,000 under Schedule 8 to the Criminal Procedure Ordinance (Cap 221).

13 Paras 3.14 to 3.16.

(a) The formulation of section 25(a) – including the references to "telecommunications officer", "message",[14] etc – does not apply well to cyberspace because it presupposes a telecommunications context.

(b) The *actus reus* under section 25(a) only covers secretion, detention or delay of a message. It does not cover other ways to interfere with computer data, such as deletion or encryption.

Standard of criminalisation under the Budapest Convention

4.15 For this Chapter, the pertinent Article in the Budapest Convention[15] is Article 4 in Title 1 under section 1:

> *"1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.*
>
> *2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm."*

4.16 The Explanatory Report with regard to Article 4 reads as follows:

> *"60. The aim of this provision is to provide computer data and computer programs with protection similar to that enjoyed by corporeal objects against intentional infliction of damage. The protected legal interest here is the integrity and the proper functioning or use of stored computer data or computer programs.*
>
> *61. In paragraph 1, 'damaging' and 'deteriorating' as overlapping acts relate in particular to a negative alteration of the integrity or of information content of data and programmes. 'Deletion' of data is the equivalent of the destruction of a corporeal thing. It destroys them and makes them unrecognisable. Suppressing of computer data means any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored. The term 'alteration' means the modification of existing data. The input of malicious codes, such as viruses and Trojan horses is, therefore, covered under this paragraph, as is the resulting modification of the data.*

---

14 The statutory definition of "message" is set out in para 3.14.

15 See para 11 of the Preface and paras 1.6 to 1.10 of Chapter 1 for background information regarding the Budapest Convention.

62. The above acts are only punishable if committed 'without right'. Common activities inherent in the design of networks or common operating or commercial practices, such as, for example, for the testing or protection of the security of a computer system authorised by the owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system acquires new software (eg, software permitting access to the Internet that disables similar, previously installed programs), are with right and therefore are not criminalised by this article. The modification of traffic data for the purpose of facilitating anonymous communications (eg, the activities of anonymous remailer systems), or the modification of data for the purpose of secure communications (eg encryption), should in principle be considered a legitimate protection of privacy and, therefore, be considered as being undertaken with right. However, Parties may wish to criminalise certain abuses related to anonymous communications, such as where the packet header information is altered in order to conceal the identity of the perpetrator in committing a crime.

63. In addition, the offender must have acted 'intentionally'.

64. Paragraph 2 allows Parties to enter a reservation concerning the offence in that they may require that the conduct result in serious harm. The interpretation of what constitutes such serious harm is left to domestic legislation ..."[16]

Statutory regimes in other jurisdictions

Australia

Statutory definitions of key concepts

4.17 Readers would recall from Chapter 3 that the main types of conduct outlawed under Part 10.7 of the Criminal Code (Cth) are unauthorised access to computer data, unauthorised modification of computer data, and unauthorised impairment of electronic communication.[17]

4.18 Before we examine the relevant offences, it is convenient to first look at how section 476.1(1) defines the second and third types of unlawful conduct (the definition of "impairment of electronic communication to or from a computer" was stated in Chapter 3 but is worth reiterating here):

---

16 Explanatory Report, at paras 60 to 64.

17 Para 3.32.

*"**electronic communication** means a communication of information in any form by means of guided or unguided electromagnetic energy."*

*"**modification**, in respect of data held in a computer, means:*

(a) the alteration or removal of the data; or

(b) an addition to the data."

*"**impairment of electronic communication to or from a computer** includes:*

(a) the prevention of any such communication; or

(b) the impairment of any such communication on an electronic link or network used by the computer;

but does not include a mere interception of any such communication."

4.19 So defined, the boldfaced terms correspond to illegal interference of computer data, albeit its different aspects.

Section 477.1 of the Criminal Code (Cth)

4.20 Section 477.1 ("*Unauthorised access, modification or impairment with intent to commit a serious offence*") was discussed in Chapter 2 with an emphasis on section 477.1(1)(a)(i) regarding unauthorised access to computer data.[18]

4.21 Section 477.1(1)(a)(ii) and (iii) are relevant to this Chapter. They provide that it is an offence for a person to cause either "unauthorised modification of data held in a computer" or "unauthorised impairment of electronic communication to or from a computer" with knowledge that the conduct is unauthorised, and with intent to commit (or facilitate the commission of) a serious offence against Commonwealth, State or Territory law by the conduct.

4.22 A "serious offence" is an offence punishable by imprisonment for life or a period of five or more years.[19] An offender of section 477.1(1) is punishable by a penalty not exceeding the penalty applicable to the serious offence.

---

18 Para 2.21.

19 Criminal Code (Cth), s 477.1(9).

Section 477.2 of the Criminal Code (Cth)

4.23 Where the evidence does not establish an intent to commit (or facilitate the commission of) a serious offence, section 477.2 ("*Unauthorised modification of data to cause impairment*") may nonetheless apply:

> *"(1) A person commits an offence if:*
>
> *(a) the person causes any unauthorised modification of data held in a computer; and*
>
> *(b) the person knows the modification is unauthorised; and*
>
> *(c) the person is reckless as to whether the modification impairs or will impair:*
>
> *(i) access to that or any other data held in any computer; or*
>
> *(ii) the reliability, security or operation, of any such data.*
>
> *Penalty: 10 years imprisonment.*
>
> *(3) A person may be guilty of an offence against this section even if there is or will be no actual impairment to:*
>
> *(a) access to data held in a computer; or*
>
> *(b) the reliability, security or operation, of any such data.*
>
> *(4) A conviction for an offence against this section is an alternative verdict to a charge for an offence against section 477.3 (unauthorised impairment of electronic communication)."*

4.24 It appears that section 477.2(3) seeks to put it beyond doubt that a person will be guilty of an offence under section 477.2(1) if the person is reckless as to whether or not his unauthorised modification will result in the actual impairment described in section 477.2(3). Nevertheless, since the subject of impairment in section 477.2(1)(c)(ii) is couched in wide terms, a person may commit the offence in section 477.2(1) by, for example, introducing software akin to a time bomb (ie software designed to impair data at a future time without further intervention or upon the occurrence of certain event) into a computer system. We make a similar observation in respect of the legislation in the USA in paragraph 4.73 below.

Section 477.3 of the Criminal Code (Cth)

4.25 In contrast, actual impairment is essential for a charge under section 477.3 ("*Unauthorised impairment of electronic communication*"):

> *"(1) A person commits an offence if:*
>
> *(a) the person causes any unauthorised impairment of electronic communication to or from a computer; and*
>
> *(b) the person knows that the impairment is unauthorised.*
>
> *Penalty: 10 years imprisonment.*
>
> *(3) A conviction for an offence against this section is an alternative verdict to a charge for an offence against section 477.2 (unauthorised modification of data to cause impairment)."*

4.26 Pursuant to sections 477.2(4) and 477.3(3), the offences under sections 477.2(1) and 477.3(1) (which apply to modification of data and impairment of communication respectively) are statutory alternatives to each other. With both offences punishable by up to ten years' imprisonment, it is unlikely that a defendant can allege any unfairness arising from the possibility of an alternative verdict. It is, however, unclear as to why the same statutory maximum penalty is set for illegal interference even without actual impairment contrary to section 477.2(1) (where culpability under that section is attributable to recklessness as to whether the unauthorised modification of data may cause actual impairment) as well as for illegal interference contrary to section 477.3(1) where impairment of electronic communication is required but it is not expressly mentioned that the perpetrator "intends to cause the impairment".[20]

Section 478.1 of the Criminal Code (Cth)

4.27 Sections 478.1 ("*Unauthorised access to, or modification of, restricted data*") and 478.2 ("*Unauthorised impairment of data held on a computer disk etc.*") can be seen as another pair of provisions dealing with modification and impairment respectively. While the offences created by them

---

[20] The Explanatory Memorandum of the Cybercrime Bill 2001 (which introduced ss 477.2 and 477.3 into the Criminal Code) explained the background of the maximum penalties of 10 years' imprisonment under these two provisions. For s 477.2, the penalty is equivalent to the penalty for the then computer offences under the Crimes Act and that for fraud and forgery offences in the Criminal Code. For s 477.3, the penalty *"recognises the importance of reliable computer-facilitated communication and the considerable damage that can result if that communication is impaired*". There is, however, no other secondary information explaining why ss 477.2 and 477.3 entail the same maximum penalty despite the difference in their *actus reus*.

are not statutory alternatives, they have the same maximum penalty of imprisonment for up to two years.

4.28 Section 478.1 provides as follows:

> *"(1) A person commits an offence if:*
>
> *(a) the person causes any unauthorised access to, or modification of, restricted data; and*
>
> *(b) the person intends to cause the access or modification; and*
>
> *(c) the person knows that the access or modification is unauthorised.*
>
> *Penalty: 2 years imprisonment.*
>
> *(3) In this section:*
>
> ***restricted data** means data:*
>
> *(a) held in a computer; and*
>
> *(b) to which access is restricted by an access control system associated with a function of the computer."*

4.29 The offences under sections 477.2 and 478.1 apply to unauthorised modification of data. A commonality between them is that, in terms of the *mens rea*, the perpetrator must know that the modification is unauthorised. However:

(a) The perpetrator's recklessness would suffice for section 477.2(1)(c), whereas his or her intent to cause the modification is necessary to satisfy section 478.1(1)(b).

(b) Besides, section 477.2(1)(a) does not require the data in question to be "restricted data" as section 478.1(1)(a) does.

These features appear at odds with the heavier maximum sentence for the offence under section 477.2, which shows that section 477.2 is meant to be the more serious offence compared to section 478.1.

Section 478.2 of the Criminal Code (Cth)

4.30 As stated above, the offences created by sections 478.1 and 478.2 have the same maximum penalty of imprisonment for up to two years. The latter provision is in these terms:

> *"A person commits an offence if:*
>
> *(a) the person causes any unauthorised impairment of the reliability, security or operation of data held on:*
>
> *(i) a computer disk; or*
>
> *(ii) a credit card; or*
>
> *(iii) another device used to store data by electronic means; and*
>
> *(b) the person intends to cause the impairment; and*
>
> *(c) the person knows that the impairment is unauthorised.*
>
> *Penalty: 2 years imprisonment."*

4.31 The offences under sections 477.3 and 478.2 apply to unauthorised impairment of electronic communication, and the reliability, security or operation of data respectively. A common element of both offences is the perpetrator's knowledge that the impairment is unauthorised.

4.32 Having said that, section 477.3 does not refer to the perpetrator's intent to cause the impairment as section 478.2(b) does. This appears counter intuitive given that the former provision stipulates a heavier maximum sentence and is presumably intended to create the more serious offence.

Canada

Section 430(1.1) of the Criminal Code 1985

4.33 Compared with the legislation in Australia, the Canadian legislation is succinct. The relevant provision is section 430(1.1) of its Criminal Code 1985 ("*Mischief in relation to computer data*"):

> *"Everyone commits mischief who wilfully*
>
> *(a) destroys or alters computer data;*

(b) renders computer data meaningless, useless or ineffective;

(c) obstructs, interrupts or interferes with the lawful use of computer data; or

(d) obstructs, interrupts or interferes with a person in the lawful use of computer data or denies access to computer data to a person who is entitled to access to it."

Similarity to the Model Law

4.34 Section 430(1.1) of the Criminal Code 1985 provides for the *actus reus* in almost the same terms as those in section 6 of the Model Law ("*Interfering with data*") set out below:

"(1) A person who, intentionally or recklessly, without lawful excuse or justification, does any of the following acts:

(a) destroys or alters data;

(b) renders data meaningless, useless or ineffective;

(c) obstructs, interrupts or interferes with the lawful use of data; or

(d) obstructs, interrupts or interferes with any person in the lawful use of data; or

(e) denies access to data to any person entitled to it;

commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.

(2) Subsection (1) applies whether the person's act is of temporary or permanent effect."

Mischief under section 430(1.1)

4.35 Some features of the "mischief" provided for in section 430(1.1) of the Criminal Code 1985 are notable:

(a) In relation to the *actus reus*, section 430(1.1) focuses on the prohibited results without outlawing any specific conduct. It refers to neither the concept of authorisation nor its absence. It appears that the provision applies to a defendant who wilfully

caused a prohibited result by omission, ie by not doing certain thing.[21] The statutory language also seems broad enough to cover damage of computer data by physical means, such as placing a strong magnet near an old floppy disk.

(b) In relation to the *mens rea*, a defendant must have wilfully committed the mischief. Under section 429(1):

> *"Every one who causes the occurrence of an event by doing an act or by omitting to do an act that it is his duty to do, knowing that the act or omission will probably cause the occurrence of the event and being reckless whether the event occurs or not, shall be deemed, for the purposes of this Part, wilfully to have caused the occurrence of the event."*

Criminal consequences of committing mischief

4.36 Section 430 of the Criminal Code 1985 prescribes the criminal consequences of committing a "mischief" in various circumstances. Under section 430(5):

> *"Everyone who commits mischief in relation to computer data*
>
> *(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or*
>
> *(b) is guilty of an offence punishable on summary conviction."*

4.37 Besides, some other subsections may also apply to mischief in relation to computer data. For instance, section 430(2) provides as follows:

> *"Every one who commits mischief that causes actual danger to life is guilty of an indictable offence and liable to imprisonment for life".*

England and Wales

Section 3 of the CMA-EW

4.38 Sections 3 ("*Unauthorised acts with intent to impair, or with*

[21] Support for this interpretation can be found in s 430(5.1) of the Criminal Code 1985, under which:
"*Everyone who wilfully does an act or wilfully omits to do an act that it is their duty to do, if that act or omission is likely to constitute mischief causing actual danger to life, or to constitute mischief in relation to property or computer data …*"
is guilty of an offence.

recklessness as to impairing, operation of computer, etc") and 3ZA ("*Unauthorised acts causing, or creating risk of, serious damage*") of the CMA-EW show a two-tier approach. Looking first at section 3:

> *"(1) A person is guilty of an offence if—*
>
> *(a) he does any unauthorised act in relation to a computer;*
>
> *(b) at the time when he does the act he knows that it is unauthorised; and*
>
> *(c) either subsection (2) or subsection (3) below applies.*
>
> *(2) This subsection applies if the person intends by doing the act—*
>
> *(a) to impair the operation of any computer;*
>
> *(b) to prevent or hinder access to any program or data held in any computer; or*
>
> *(c) to impair the operation of any such program or the reliability of any such data; or*
>
> *(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.*
>
> *(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above.*
>
> *(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to—*
>
> *(a) any particular computer;*
>
> *(b) any particular program or data; or*
>
> *(c) a program or data of any particular kind.*
>
> *(5) In this section—*
>
> *(a) a reference to doing an act includes a reference to causing an act to be done;*
>
> *(b) 'act' includes a series of acts;*
>
> *(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.*

(6) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) […]

(c) on conviction on indictment, to imprisonment for a term not exceeding ten years or to a fine or to both."

Authority illustrating successful enforcement

4.39 *R v Victor Lindesay*[22] illustrates successful enforcement under section 3 of the CMA-EW. The facts there resembled those in *HKSAR v Chan Chi Kong*.[23] Mr Lindesay pleaded guilty to three charges of causing unauthorised modification to the contents of a computer. Although the damage was not permanent, he was sentenced to imprisonment for nine months.

4.40 The English Court of Appeal upheld the sentence, noting that:

> *"… however real the grievance, however impulsive the act of revenge and however inevitable the discovery of the appellant's responsibility for these acts, the fact remains that the appellant used his skill and his knowledge of his former employer's business to cause a great deal of work, inconvenience and worry to organisations that were entirely innocent. That was properly met, in this Court's judgment, by an immediate sentence of imprisonment to mark the breach of trust."*[24]

Section 3ZA of the CMA-EW

4.41 An offender under section 3 is liable to imprisonment for a term not exceeding ten years, or to a fine, or both. The maximum penalty under section 3ZA, set out below, is much heavier:

"(1) A person is guilty of an offence if—

(a) the person does any unauthorised act in relation to a computer;

(b) at the time of doing the act the person knows that it is unauthorised;

---

22 [2001] EWCA Crim 1720; [2002] 1 Cr App R (S) 86.
23 Para 4.9.
24 See fn 22 above, at 373 (para 15).

(c) the act causes, or creates a significant risk of, serious damage of a material kind; and

(d) the person intends by doing the act to cause serious damage of a material kind or is reckless as to whether such damage is caused.

(2) Damage is of a 'material kind' for the purposes of this section if it is—

(a) damage to human welfare in any place;

(b) damage to the environment of any place;

(c) damage to the economy of any country; or

(d) damage to the national security of any country.

(3) For the purposes of subsection (2)(a) an act causes damage to human welfare only if it causes—

(a) loss to human life;

(b) human illness or injury;

(c) disruption of a supply of money, food, water, energy or fuel;

(d) disruption of a system of communication;

(e) disruption of facilities for transport; or

(f) disruption of services relating to health.

(4) It is immaterial for the purposes of subsection (2) whether or not an act causing damage—

(a) does so directly;

(b) is the only or main cause of the damage.

(5) In this section—

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) 'act' includes a series of acts;

(c) a reference to a country includes a reference to a territory, and to any place in, or part or region of, a country or territory.

(6) A person guilty of an offence under this section is (unless subsection (7) applies) liable, on conviction on indictment, to imprisonment for a term not exceeding 14 years, or to a fine, or to both.

(7) Where an offence under this section is committed as a result of an act causing or creating a significant risk of—

(a) serious damage to human welfare of the kind mentioned in subsection (3)(a) or (3)(b), or

(b) serious damage to national security,

a person guilty of the offence is liable, on conviction on indictment, to imprisonment for life, or to a fine, or to both."

The actus reus under sections 3 and 3ZA

4.42 The *actus reus* under both provisions includes "*any unauthorised act in relation to a computer*". For the purposes of section 3ZA, such an act must additionally cause, or create a significant risk of, "*serious damage of a material kind*".

4.43 The word "act" indicates that a person would not commit an offence under either section by omission. Besides, it appears from the drafting of the two provisions that conviction does not require actual damage.

4.44 Moreover, it seems that a physical act can constitute the *actus reus* under the two provisions. In this respect, the example of placing a strong magnet near an old floppy disk was given above when discussing Canadian law.[25] *R v Nicholas Alan Whiteley*[26] suggested that, before the CMA-EW came into force, doing so might constitute an offence under section 1(1) ("*Destroying or damaging property*") of the Criminal Damage Act 1971.[27] Section 10(5) of the same Act must now be taken into account:

"For the purposes of this Act a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition."

4.45 In light of section 10(5), modification of the content of a computer without impairment of its physical condition should be charged under the CMA-EW instead of the Criminal Damage Act 1971.

---

25 Para 4.35(a).

26 (1991) 93 Cr App R 25.

27 "*A person who without lawful excuse destroys or damages any property belonging to another intending to destroy or damage any such property or being reckless as to whether any such property would be destroyed or damaged shall be guilty of an offence.*"

The mens rea under sections 3 and 3ZA

4.46 As regards the *mens rea*, both provisions require a defendant's knowledge that his or her act is unauthorised. They further require that the defendant:

(a) intends to cause (in the case of section 3) specified types of damage[28] or (in the case of section 3ZA) "serious damage of a material kind";[29] or

(b) is reckless as to whether such damage will ensue.

Mainland China

Article 286(2) of the PRC Criminal Law

4.47 According to Article 286(2) of the PRC Criminal Law:

> *"Whoever, in violation of State regulations, cancels, alters or increases the data stored in or handled or transmitted by the computer information system or its application program, if the consequences are serious, shall be punished in accordance with the provisions of the preceding paragraph."*[30]
>
> (emphasis added)

Authority illustrating successful enforcement

4.48 In case number 34 of the 9th batch of SPP's Guiding Cases,[31] the defendant impersonated other internet users and logged in their online shopping accounts to remove or revise the negative ratings posted on an online shopping platform by such internet users against some online sellers. The defendant was convicted under Article 286(2) for altering the data in the computer information system, ie the negative ratings on the online shopping platform, which the court regarded as the "core component" of the computer information system of the shopping platform.

---

28 Impairing any computer's operation, preventing or hindering access to any program or data, impairing such program's operation, or impairing such data's reliability (s 3(2)).

29 S 3ZA(2) and (3).

30 The English translation of Article 286(2) is the official version published by the Legislative Affairs Commission of the NPCSC in 1997. Article 286(2) states that: "*違反國家規定，對計算機信息系統中存儲、處理或者傳輸的數據和應用程序進行刪除、修改、增加的操作，後果嚴重的，依照前款的規定處罰。*"

31 李駿傑等破壞計算機信息系統案。

New Zealand

Section 250(2) of the New Zealand Act

4.49 The statutory scheme in New Zealand is similar to that in England and Wales, in that the legislation provides for a basic offence and an aggravated form premised on more serious consequences caused by a defendant's act.

4.50 Section 250(2) ("*Damaging or interfering with computer system*") of the New Zealand Act creates the basic offence. So far as this Chapter is concerned, section 250(2) provides as follows:

> *"Every one is liable to imprisonment for a term not exceeding 7 years who intentionally or recklessly, and without authorisation, knowing that he or she is not authorised, or being reckless as to whether or not he or she is authorised—*
>
> *(a) damages, deletes, modifies, or otherwise interferes with or impairs any data or software in any computer system; or*
>
> *(b) causes any data or software in any computer system to be damaged, deleted, modified, or otherwise interfered with or impaired; …"*

4.51 Section 250(2)(c) will be addressed in Chapter 5.

Deletion of computer data or software

4.52 Section 250(2)(a) and (b) refers to, among other things, deletion of computer data or software. A pertinent question is whether this means rendering the data or software irrecoverable ("wiping"), or would criminal liability arise even if one can easily recover the data or software? Some examples of the latter situation are as follows:

(a) If someone is using a word processor to edit a document, and another person deleted certain content without authorisation, the "undo" function may help recover the deleted content.

(b) After someone deletes a file in a computer, locating the file in the "Recycle Bin", "Trash" or equivalent and recovering it may be possible.

(c) A deleted file can be restored if a backup copy or an image of the relevant storage medium exists.[32]

---

[32] As in *HKSAR v Chan Chi Kong* (cited in para 4.9).

4.53 A commentator noted that the case of *Police v Robb*[33] highlighted the difference between wiping and recoverable deletion. As the District Court (Christchurch) observed, it appeared that the computer files in question:

> *"… were simply deleted rather than wiped. Wiping involves overwriting a file's data prior to being deleted. It is generally considered that no traces can be found of a wiped file and recovery is impossible."*[34]

4.54 The commentator summarised the court's rulings in these terms:

> *"Deletion in and of itself did not, according to the Judge, amount to damaging or interfering with a computer system contrary to s 250 [of the Crimes Act 1961]. Further, to establish a criminal offence of damaging or interfering with a computer system, it is necessary to exclude innocent or accidental data deletion. The Judge observed that wiping a file required an additional conscious decision over and above simple deletion whereas it was not possible to use forensic methods to determine whether a file was deliberately deleted or not."*[35]

4.55 Critical of the ruling that it was necessary to prove "*deliberate steps ensuring that the data was not recoverable, ie wiping*",[36] the commentator argued as follows:

> *"Parliament's intention, when it used the term 'delete' [in section 250(2) of the Crimes Act 1961], could not have been to mean that the file was completely irrecoverable in whole or in part … Parliament's intention … could not have been that the normal operation of a computer could include intervening remedial steps to make the machine or system operational after intentional activities designed to preclude its proper operation."*[37]

4.56 Construing section 250(2) as held in *Police v Robb*[38] would, unless mitigated by the commentator's argument, likely render it inapplicable to the facts in *HKSAR v Chan Chi Kong*[39] (where the deleted files were eventually restored but only after immediate emergency procedures had been brought into play) if the case took place in New Zealand.

---

33 [2006] DCR 388 (the written decision appears unavailable online).

34 Same as above, at para 27, quoted in:
David Harvey, *internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015), at para 7.92.

35 David Harvey, *internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015), at para 7.93.

36 *Police v Robb* at para 40, quoted in David Harvey, *internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015), at para 7.93.

37 See fn 35 above, at para 7.94.

38 [2006] DCR 388.

39 Para 4.9.

The mens rea under section 250(2)

4.57 Section 250(2) describes the *mens rea* for carrying out the *actus reus* as "intentionally or recklessly", whereas the *mens rea* regarding the lack of authorisation is knowledge or recklessness. Two points can be made:

(a) While the legislation could have referred to a defendant carrying out the *actus reus* "knowingly or recklessly", it has opted for "intentionally or recklessly". There is an academic view that, in the context of New Zealand criminal law, "*it is apparent that 'knowingly' may be used as a synonym for 'intention'* ".[40] For comparison, under the Model Penal Code of the American Law Institute:[41]

> "*Except as provided in Section 2.05, a person is not guilty of an offense unless he acted purposely,*[42] *knowingly,*[43] *recklessly*[44] *or negligently,*[45] *as the law may require, with respect to each material element of the offense.*"[46]

Therefore, "purposely" (which is defined to be similar in nature to "intentionally") and "knowingly" are different concepts under that Code.

(b) In comparison, the meaning of recklessness is clearer. The New Zealand Supreme Court held as follows in *Cameron v R*:[47]

---

40 Kris Gledhill, "The Meaning of Knowledge as a Criminal Fault Element: Is to Know to Believe?" (2019) 45(2) University of Western Australia Law Review 216, at 228.

41 The Model Penal Code is not law but, as the American Law Institute states, it "*played an important part in the widespread revision and codification of the substantive criminal law of the United States*". See American Law Institute, "Model Penal Code", available at https://www.ali.org/publications/show/model-penal-code/ (accessed on 3 May 2022).

42 "*A person acts purposely with respect to a material element of an offense when:*
(i) if the element involves the nature of his conduct or a result thereof, it is his conscious object to engage in conduct of that nature or to cause such a result; and
(ii) if the element involves the attendant circumstances, he is aware of the existence of such circumstances or he believes or hopes that they exist." (S 2.02(2)(a))

43 "*A person acts knowingly with respect to a material element of an offense when:*
(i) if the element involves the nature of his conduct or the attendant circumstances, he is aware that his conduct is of that nature or that such circumstances exist; and
(ii) if the element involves a result of his conduct, he is aware that it is practically certain that his conduct will cause such a result." (S 2.02(2)(b))

44 "*A person acts recklessly with respect to a material element of an offense when he consciously disregards a substantial and unjustifiable risk that the material element exists or will result from his conduct. The risk must be of such a nature and degree that, considering the nature and purpose of the actor's conduct and the circumstances known to him, its disregard involves a gross deviation from the standard of conduct that a law-abiding person would observe in the actor's situation.*" (S 2.02(2)(c))

45 "*A person acts negligently with respect to a material element of an offense when he should be aware of a substantial and unjustifiable risk that the material element exists or will result from his conduct. The risk must be of such a nature and degree that the actor's failure to perceive it, considering the nature and purpose of his conduct and the circumstances known to him, involves a gross deviation from the standard of care that a reasonable person would observe in the actor's situation.*" (S 2.02(2)(d))

46 S 2.02(1).

47 [2017] NZSC 89.

> "*In cases … in which the offence is not defined in terms which require actual knowledge or intention and nothing less, we consider that recklessness as explained in [R v G*[48]*] will (at least usually and perhaps always) be sufficient to satisfy mens rea requirements as to circumstance and result. For these purposes, recklessness is established if:*
>
> *(a) The defendant recognised that there was a real possibility that:*
>
> *i. his or her actions would bring about the proscribed result; and/or*
>
> *ii. That the proscribed circumstances existed; and*
>
> *(b) Having regard to that risk those actions were unreasonable.*"[49]

Section 250(1) of the New Zealand Act

4.58 Turning to the aggravated offence, under section 250(1) of the New Zealand Act:

> *"Every one is liable to imprisonment for a term not exceeding 10 years who intentionally or recklessly destroys, damages, or alters any computer system if he or she knows or ought to know that danger to life is likely to result."*

4.59 On its face, the provision only covers the destruction, damage or alteration of computer system, but not computer data. However in some cases where "danger to life is likely to result" from a defendant's act, he or she would conceivably have destroyed, damaged or altered computer data in addition to the computer system as a whole. In reality, one can say that the provision is relevant to both Chapters 4 and 5.

4.60 Separately, unlike section 250(2), authorisation is apparently an irrelevant concept under section 250(1). This is understandable given the danger to life involved.

Section 258(1) of the New Zealand Act

4.61 The maximum sentence for the offence created by section 250(1) (ten years' imprisonment) is the same as that provided in section 258(1)

---

48 [2003] UKHL 50; [2004] 1 AC 1034.

49 *Cameron v R*, at para 73, cited in Nick Chisnall, "Case Note: *Cameron v R* [2017] NZSC 89 – Controlled Drug Analogues, Indeterminacy and *Mens Rea* under the Misuse of Drugs Act 1975" [2017] NZCLR 256, at 262.

("*Altering, concealing, destroying, or reproducing documents with intent to deceive*") set out below:

> *"Every one is liable to imprisonment for a term not exceeding 10 years who, with intent to obtain by deception any property, privilege, service, pecuniary advantage, benefit, or valuable consideration, or to cause loss to any other person,—*
>
> *(a) alters, conceals, or destroys any document, or causes any document to be altered, concealed, or destroyed; or*
>
> *(b) makes a document or causes a document to be made that is, in whole or in part, a reproduction of any other document."*[50]

4.62 In *R v Johannes Hendrik Middeldorp*,[51] the court held that the word "document" in section 258(1)(b), quoted above, includes computer files (representing scanned images) saved on a computer hard-drive, and attachments (representing images) to emails sent or received. Logic supports the same construction of the word "document" in section 258(1)(a). On this basis, the provision would apply where computer data is altered, concealed or destroyed.

4.63 Comparing the offences under section 250(1) (which is computer-specific) and section 258(1) (which is of general application), a potentially material difference is that recklessness would suffice as the *mens rea* under the former provision, but not under the latter.

Singapore

Section 5 of the CMA-SG

4.64 Section 5 of the CMA-SG ("*Unauthorised modification of computer material*") is pertinent to this Chapter:

> *"(1) Subject to subsection (2), any person who does any act which the person knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on conviction —*

---

50 S 258(2) elaborates as follows:
"*An offence against subsection (1) is complete as soon as the alteration or document is made with the intent referred to in that subsection, although the offender may not have intended that any particular person should—*
(a) use or act upon the document altered or made; or
(b) act on the basis of the absence of the document concealed or destroyed; or
(c) be induced to do or refrain from doing anything."

51 [2015] NZHC 951.

(a) to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; and

(b) in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the act in question is not directed at —

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

(4) For the purposes of this section, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary."

Unauthorised modification

4.65 As regards the *actus reus*, section 2(7) and (8) of the same Act explains the key concept of unauthorised modification:

"(7) For the purposes of this Act, a modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer —

(a) any program or data held in the computer concerned is altered or erased;

(b) any program or data is added to its contents; or

(c) any act occurs which impairs the normal operation of any computer,

and any act which contributes towards causing such a modification is taken as causing it.

(8) Any modification mentioned in subsection (7) is unauthorised if the person whose act causes it —

(a) is not himself or herself entitled to determine whether the modification should be made; and

(b) does not have consent to the modification from any person who is so entitled."

Mens rea

4.66 The prescribed *mens rea* is knowledge that the perpetrator's act will cause an unauthorised modification. Hence, mere recklessness does not suffice for criminal liability.

Enhanced punishment if "protected computer" is involved

4.67 The jurisdictions canvassed above provide for a basic offence, as well as an aggravated form premised on more serious consequences (eg danger to life intended or caused by the offender).

4.68 An alternative approach features in the CMA-SG. Apart from section 5(1) (which stipulates a heavier maximum penalty applicable to repeat offenders) and section 5(2) (pursuant to which an even heavier maximum penalty may be imposed on an offender who caused "any damage"), section 11(1) reserves the heaviest maximum penalty for cases involving access to a "protected computer":

> *"(1) Where access to any protected computer is obtained in the course of the commission of an offence under section 3, 5, 6 or 7, a person convicted of the offence shall, in lieu of the punishment prescribed in those sections, be liable to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 20 years or to both.*
>
> *(2) For the purposes of subsection (1), a computer is treated as a 'protected computer' if the person committing the offence knew, or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for —*
>
> *(a) the security, defence or international relations of Singapore;*
>
> *(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;*
>
> *(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or*
>
> *(d) the protection of public safety including systems related to essential emergency services such as*

police, civil defence and medical services.

(3) For the purposes of any prosecution under this section, it is presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in subsection (2) if there is, in respect of the computer, program or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that computer, program or data attracts an enhanced penalty under this section."

4.69 The CMA-SG illustrates that, in formulating an aggravated offence, the involvement of certain class of data or computer system can be an aggravating factor.

USA

18 USC 1030(a)(5) within the Computer Fraud and Abuse Act

4.70 In the USA, as noted in Chapters 1[52] and 2,[53] the key federal legislation on cybercrime is the Computer Fraud and Abuse Act (18 USC 1030). Whoever carried out the acts relating to any of the various scenarios in section 1030(a) is punishable as provided in section 1030(c).

4.71 The offence relevant to this Chapter is created by 18 USC 1030(a)(5) and has three limbs:

"(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss."

Damage to a protected computer

4.72 All three limbs concern "damage" to a "protected computer". 18 USC 1030(e)(8) defines "damage" to mean "*any impairment to the integrity*

52 Para 1.10(b).
53 Para 2.81.

or availability of data, a program, a system, or information".

4.73 With this expansive definition, the offence seems applicable to a person doing something – such as intentionally disseminating a computer virus or planting software akin to a time bomb – which causes no immediate damage but has already amounted to actual interference of computer data introducing a risk of damage occurring at a later time. Although such interference might not have occurred yet, the person's act has already impaired the data's integrity. The definition of "damage" would also cover unauthorised encryption of data which impairs its availability.

4.74 18 USC 1030(e)(2) defines a "protected computer" to mean a computer:

> *"(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government;*
>
> *(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States; or*
>
> *(C) that—*
>
> *(i) is part of a voting system; and*
>
> *(ii) (I) is used for the management, support, or administration of a Federal election; or*
>
> *(II) has moved in or otherwise affects interstate or foreign commerce".*

Without authorisation

4.75 The requirement of "*without authorization*" is present in all three limbs in 18 USC 1030(a)(5), but linked to different elements, namely the causing of damage for limb (A) and the access to a protected computer for limbs (B) and (C). Hence, in the case of limb (A), "*even where the transmission is authorised the defendant may still be liable if the damage caused is not*".[54]

---

[54] Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015), at 117 citing *Lockheed Martin Corp v Speed*, 2006 US Dist LEXIS 53108 (MD Fla 2006), at 21.

4.76 None of the three limbs in 18 USC 1030(a)(5) refers to the scenario of a defendant acting in excess of authorisation, whereas that scenario is expressly contemplated under 18 USC 1030(a)(1), (a)(2) and (a)(4).[55]

4.77 The distinction led the Fifth Circuit Court of Appeals in *US v Phillips*[56] to conclude that 18 USC 1030(a)(5) applies "*exclusively to users [of the relevant computer] who lack access authorization altogether*". Citing Congressional record which stated that 18 USC 1030(a)(5) would "*be aimed at 'outsiders'* ", the court observed as follows:

> *"In conditioning the nature of the intrusion in part on the level of authorization a computer user possesses, Congress distinguished between 'insiders, who are authorized to access a computer,' and 'outside hackers who break into a computer.' "*[57]

Transmission in limb (A)

4.78 The term "transmission" in limb (A) has been subject to judicial interpretation. It appears that:

(a) the term covers infection of a computer "*via telecommunication lines or by direct input*";[58] and

(b) "*even the act of typing and overwriting data could fall within the provision so long as the necessary damage was caused*".[59]

Loss in limb (C)

4.79 Limb (C) requires "damage and loss" to result from a defendant's act. Under 18 USC 1030(e)(11):

> *"the term 'loss' means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service".*

---

55 Paras 2.83 to 2.88 consider the distinction between a person acting without authorisation and in excess of authorisation.

56 477 F 3d 215 (5th Cir 2007).

57 Same as above, at 219.

58 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015), at 121 citing *Lloyd v US*, 2005 US Dist LEXIS 18158 (D NJ 2005).

59 Same as above, at 122, citing *International Airport Centers LLC v Citrin*, 440 F 3d 418 (7th Cir 2006).

Mens rea

4.80 The *mens rea* under the three limbs in 18 USC 1030(a)(5) can be summarised and contrasted as follows:

(a) Under limb (A), the defendant must knowingly cause the transmission of program, etc and intentionally cause damage.

(b) Limb (B) requires an access to a protected computer to be intentional, and further requires the defendant to recklessly cause damage.

(c) Limb (C) also requires an intentional access to a protected computer, but stipulates no mental element with respect to the causing of damage and loss.

The Sub-committee's views

Prohibiting intentional and unauthorised data interference

4.81 From the outset of our discussion, we recognise that alteration of computer data is commonplace. Data is inevitably altered whenever there is any operation of a computer (eg booting up or logging into the computer) or interaction with the internet. The following are common examples of such alteration:

(a) A social media platform would inspect data provided by a user when he or she posts a photograph or a link to a webpage. The platform may modify or remove some of the data, such as a photograph's metadata.

(b) An email server would scan an email's attachment and remove it if the server finds it to be dangerous.

(c) A website may alter data in a visitor's computer, or add data to it, by saving "cookies"[60] in it.

4.82 These scenarios are probably acceptable to many computer users notwithstanding that their data is intentionally altered (in that the alteration is consciously caused by the administrator of the social media platform, the email server or the website).

---

60 "*A packet of data sent by a web server to a browser, which is returned by the browser each time it subsequently accesses the same server, used to identify the user or track their access to the server.*" See: Oxford University Press, "Lexico.com" (2021) at https://www.lexico.com/definition/cookie (accessed on 3 May 2022).

4.83 While the applicable terms and conditions may have authorised the alteration, it is also possible that there is no explicit authorisation for the alteration. For example, we understand that when an internet service provider operates an email service or upgrades its infrastructure, it may not necessarily inform its users of formal changes to their data if the substance remains intact.

4.84 At the same time, cases such as *HKSAR v Chan Chi Kong*[61] illustrate the harm that can result from interference of computer data. In principle, the law should prohibit interference that may cause or has caused harm. Logically, such interference would be unauthorised and may be intentional.

4.85 The question then is what criteria a statutory offence of data interference should adopt so that it only targets cases involving (potential or actual) harm, but not generally accepted circumstances such as the examples of social media platforms, email servers and websites mentioned above. In light of the existing legislation on criminal damage, our view is that the issue ultimately boils down to whether the interference is justified by any reasonable excuse.

4.86 We therefore propose that intentional interference (damaging, deletion,[62] deterioration, alteration or suppression) of computer data without lawful authority or reasonable excuse should be an offence. Having agreed this general direction, we took the current law – specifically, sections 59 to 64 of the Crimes Ordinance (Cap 200) regarding criminal damage – as the blueprint in discussing the various aspects of the proposed offence.

Actus reus

4.87 Regarding the *actus reus*, in our view, the concept of "misuse of a computer" as particularised in section 59(1A) of the Crimes Ordinance (Cap 200) [63] seems largely sufficient to cover the conceivable scenarios relevant to this Chapter.

4.88 While section 59(1A) does not include a general limb found in section 430(1.1)(b) of the Criminal Code 1985 in Canada,[64] there appears to be no scenario covered by this general limb that the provision in Hong Kong does not cover. The general limb may reflect a view in Canada that to damage a computer is, in essence, to damage its data.

---

61 Para 4.9.
62 Even if it may be recoverable by using certain data recovery tools.
63 Para 4.7.
64 Rendering computer data "*meaningless, useless or ineffective*" (see para 4.33).

Mens rea

4.89 At present, "misuse of a computer" is a form of criminal damage. This is sensible because such misuse is analogous to criminal damage of tangible property. From a consistency perspective, both forms of criminal damage should have the same *mens rea*, ie intent or recklessness.

4.90 The legislation creating the offence of criminal damage in Hong Kong is largely modelled on the Criminal Damage Act 1971 in England and Wales, which was enacted based on the proposals of the Law Commission.[65] As explained in its Report,[66] most of the offences under the predecessor legislation (the Malicious Damage Act 1861) required the defendant to have acted "unlawfully and maliciously". The Law Commission recommended against using those words;[67] we see no reason reverting to the old law by requiring malice for the proposed offence.

Lawful excuses

4.91 In the same Report, the Law Commission described its thinking behind the (then proposed) offence of criminal damage as follows:

> *"Although the accused will not have to raise the issue of lawful excuse, it will only be when he does raise it, or when the possibility of lawful excuse appears from the evidence that the question will arise. The definition of the offence is so framed that there is to be a burden upon the prosecution of proving the absence of lawful excuse, if the question arises."*[68]

4.92 In Hong Kong, section 64(2) of the Crimes Ordinance (Cap 200) provides for two lawful excuses while preserving any other lawful excuse or defence recognised by law.

4.93 The first lawful excuse applies where a defendant believed that the person(s) whom the defendant believed to be entitled to consent to the property's destruction or damage either had consented, or would have consented. The latter case means that actual consent is unnecessary. The defendant can invoke this lawful excuse so long as his or her belief is honest, even if it is unjustified,[69] but realistically the belief should not be too far-fetched. This lawful excuse appears to be broad enough to cover the cases of social media platforms, email servers and websites mentioned

---

65 Law Commission, *Criminal Law Report on Offences of Damage to Property* (1970), Law Com No 29, available at https://www.lawcom.gov.uk/project/criminal-law-report-on-offences-or-damage-to-property/ (accessed on 3 May 2022).

66 Same as above, at 16 (para 42).

67 Same as above, at 17 (para 44) and 18 (para 48).

68 Same as above, at 18 (para 48).

69 Crimes Ordinance (Cap 200), s 64(3).

above.[70] A further hypothetical scenario is where a technician applies the latest security patch to a computer without obtaining the consent of the computer's owner beforehand.

4.94 The second lawful excuse is premised on the need to protect property, or a right or interest in property. It seems to apply where, for instance, a person has to remove a virus in a computer in order to protect its data.

4.95 We have concluded that it is appropriate to maintain the above lawful excuses, while preserving any other lawful excuse or defence recognised by law.

Aggravated offence

4.96 We have seen that, in Canada, mischief in relation to computer data is punishable by imprisonment for a term not exceeding ten years, whereas a person who commits mischief causing actual danger to life is liable to life imprisonment.[71] Such maximum sentences are the same as those applicable to the offence of criminal damage, including "misuse of a computer", in Hong Kong.[72]

4.97 In our opinion, the distinction drawn in Canada and Hong Kong (between cases involving and not involving danger to life) is justifiable. A hypothetical scenario involving danger to life is where someone interferes with computer data being processed by the system of an airport's control tower, a railway signal system, etc.

4.98 We favour retention of the aggravated offence under section 60(2) of the Crimes Ordinance (Cap 200).

Transposing the offence to the new legislation

4.99 To summarise, our consensus is that the existing regime is generally satisfactory. Given our recommendation to enact a piece of bespoke legislation on cybercrime,[73] we suggest that the provisions regarding "misuse of a computer" be separated from the offence of criminal damage and adopted in the new legislation, while deleting section 59(1)(b) and (1A) of the Crimes Ordinance (Cap 200).

---

70 Para 4.81.
71 Paras 4.36 to 4.37.
72 Para 4.5.
73 Para 2.90.

Recommendation 6

The Sub-committee recommends that:

(a) Intentional interference (damaging, deletion, deterioration, alteration or suppression) of computer data without lawful authority or reasonable excuse should be an offence under the new legislation.

(b) The new legislation should adopt the following features under the Crimes Ordinance (Cap 200):

(i) the *actus reus* under section 59(1A)(a), (b) and (c);

(ii) the *mens rea* under section 60(1) (which requires intent or recklessness, but not malice);

(iii) the two lawful excuses under section 64(2), while preserving any other lawful excuse or defence recognised by law; and

(iv) the aggravated offence under section 60(2).

(c) The above provisions regarding "misuse of a computer" should be separated from the offence of criminal damage and adopted in the new legislation, while deleting section 59(1)(b) and (1A) of the Crimes Ordinance (Cap 200).

Chapter 5

Illegal interference of computer system

Introduction

5.1 In this Chapter, we examine the fourth cyber-dependent offence, ie illegal interference of computer system. Broadly speaking, an offence in respect of this subject matter would seek to:

(a) prohibit hindrance of lawful use of computer systems by using or interfering with computer data; and

(b) thereby protect the proper functioning of computer systems.

5.2 This Chapter builds on the discussion in Chapter 4, given the close relationship between illegal interference of computer data and that of computer system. The academic commentary below is apposite:

> "*Although hindering the functioning of a computer system will commonly occur due to modification of data, it may also occur where there is no modification of data but access to the computer is prevented or its functioning restricted; for example, a DoS [denial of service] attack.*"[1]

5.3 A denial of service attack, which involves "*[a]n interruption in an authorized user's access to a computer network, typically one caused with malicious intent*",[2] is a prime example of the types of misconduct to be examined in this Chapter. An intensified form of such attack is carried out in a distributed manner and known as DDOS attack, defined as "*[t]he intentional paralysing of a computer network by flooding it with data sent simultaneously from many individual computers*".[3]

5.4 A DDOS attack is often, though not necessarily, perpetrated by means of a "botnet". A criminal can disseminate online – for example, through a virus, a hyperlink on a webpage which an unwary internet user may click – a piece of malware that would allow the surreptitious control of a compromised computer. Each compromised computer is known as a "bot" (ie robot), hence the term "botnet" for a group of compromised computers. A botnet with more

---

1 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015), at 113.

2 Oxford University Press, "Lexico.com" (2021) at https://www.lexico.com/definition/denial_of_service (accessed on 3 May 2022).

3 Same as above.

bots is more powerful. A criminal can, for example, remotely instruct all computers in a botnet to request the same webpage simultaneously and repeatedly. If the server hosting the webpage has insufficient capacity to respond to the same request from a large number of computers at the same time, the server may freeze, crash or otherwise fail. This can happen with those computers' owners, who may well be innocent, kept in the dark.

5.5 Where a computer system has been subject to what appears to be a DDOS attack, whether the parties who collectively caused the result intended to attack the system may be a crucial factual issue. For instance, an emergency hotline service that operates through a computer system may be jammed by a large number of incoming calls. One must differentiate between many people coincidentally dialling the hotline at the same moment, and someone commanding hundreds or thousands of computers to dial the hotline in a concerted manner. The latter scenario is more comparable to a DDOS attack.

5.6 Apart from DDOS attack, a new way to interfere with a computer system – called slow attack – has emerged. A DDOS attack is analogous to the situation where many customers place orders in a restaurant at the same time, whereas one can liken a slow attack to a customer using many small-denomination coins to pay a bill in the restaurant, thus disrupting normal services. While a DDOS attack causes the target computer system to generate a large amount of log record, a slow attack may only keep the target computer system engaged for a prolonged period.

Current Hong Kong law

Crimes Ordinance (Cap 200)

Section 60

5.7 As stated in Chapter 4, one form of criminal damage under section 60 of the Crimes Ordinance (Cap 200) is "misuse of a computer". Section 59(1A) defines that phrase to mean the following acts:

> *"(a) to cause a computer to function other than as it has been established to function by or on behalf of its owner, notwithstanding that the misuse may not impair the operation of the computer or a program held in the computer or the reliability of data held in the computer;*
>
> *(b) to alter or erase any program or data held in a computer or in a computer storage medium;*

(c) to add any program or data to the contents of a computer or of a computer storage medium,

and any act which contributes towards causing the misuse of a kind referred to in paragraph (a), (b) or (c) shall be regarded as causing it."

The reference to "*paragraph (a), (b) or (c)*" suggests that the three paragraphs are disjunctives. Among them, paragraphs (b) and (c) were considered in Chapter 4. Paragraph (a) is most relevant to this Chapter.

Authorities illustrating DDOS attacks

5.8 Case law has established that a DDOS attack can constitute "misuse of a computer" as defined in section 59(1A). In the magistracy appeal of *香港特別行政區 訴 朱婷婷*,[4] Albert Wong J held that there was "***absolutely no problem***"[5] with the trial Magistrate's finding that the server for the website <www.police.gov.hk> was criminally damaged within the meaning of section 59(1A)(a) as a result of a DDOS attack constituted by 7,000 odd attempts in 49 minutes by one internet protocol address to browse that website.

5.9 The defendant's appeal was allowed mainly because the evidence did not establish that the defendant was responsible for the attack. It was therefore unnecessary to consider the issue of *mens rea*. Even so, after noting that "*the basis for conviction was the appellant being reckless*"[6] and referring to the general standard of recklessness[7] laid down by the Court of Final Appeal in *Sin Kam Wah v HKSAR*,[8] the learned judge set out the following views on how the issue of *mens rea* should be approached:

"In the present case, if the appellant [ie, the defendant] was found to be the person who had pressed the button [shown on an international hacker group's webpage accessed by the defendant] causing damage to the police website, even her knowledge of the risk had been established, considering what she did was only pressing a button which was the only button shown on the webpage and the fact that there was no particular evidence showing what kind of button it was, the [Magistrates'] Court should also scrutinise what did the appellant see on the webpage and consider carefully whether she was acting unreasonably before

---

4 [2017] 4 HKLRD 651 (English translation of the judgment reported as *HKSAR v Chu Ting Ting* [2017] 4 HKLRD 666), HCMA 33/2016 (date of judgment: 11 Oct 2016).

5 Same as above, at 673 (para 22) ("*這裁定絕無問題*").

6 Same as above, at 685 (para 79).

7 Same as above, at 685 (paras 81 and 82).

8 A person acts recklessly with respect to:
(1) (a)…a circumstance when he is aware of a risk that it exists or will exist;
(b)…a result when he is aware of a risk that it will occur; and
(2) …it is, in the circumstances known to him, unreasonable to take the risk
(*Sin Kam Wah v HKSAR* (2005) 8 HKCFAR 192, FACC 14/2004 (date of judgment: 26 May 2005)).

coming to a conclusion."[9]

5.10 While a DDOS attack can hinder normal access to a computer or restrict its intended functioning, section 59(1A)(a) is couched in broader terms. In *HKSAR v Chu Tsun Wai*（*朱峻瑋*）[10] ("***Chu Tsun Wai***"), the defendant participated in a DDOS attack on a bank's website, but the attack failed because the server had enough surplus capacity to prevent the attack from having any effect upon its other operations. The Court of Final Appeal construed and applied section 59(1A)(a) as follows:

> *"In my opinion, the functions for which the computer is established to do are not so much concerned with the way it works (or fails to work) but what it was intended to* ***do****. The way it works depends upon how it was constructed by its manufacturer. But the statute is concerned with what the owner has set it up to do. The website and its server were established to provide banking services, not to deal with a multitude of requests made for no purpose except to inconvenience the bank and its customers and generate publicity for the attackers."*[11] (emphasis in original)

5.11 The Court further noted a degree of analogy between carrying out a DDOS attack and sending a torrent of emails to a recipient.[12] The latter scenario featured in *Director of Public Prosecutions v Lennon*,[13] where the English Divisional Court remarked that a computer owner's general consent to receiving emails:

> *"… plainly does not cover emails which are not sent for the purpose of communication with the owner, but are sent for the purpose of interrupting the proper operation and use of his system."*[14]

5.12 The Court of Final Appeal concluded that the DDOS attack in *Chu Tsun Wai* was "*very appropriately described as a misuse of the bank's computer*",[15] and that the defendant's conviction under section 59(1A)(a) should be upheld. The Court's reasoning suggests that if the facts in *Director of Public Prosecutions v Lennon* occurred in Hong Kong, it is likely for section 59(1A)(a) to similarly apply.

---

9 See fn 4 above, at 686 (para 91).
10 (2019) 22 HKCFAR 30, [2019] HKCFA 3.
11 Same as above, at 36 (para 13). The judgment of the Court of Final Appeal was given by Lord Hoffmann NPJ with whom all the other judges agreed.
12 Same as above, at 37 (para 14).
13 [2006] EWHC 1201 (Admin).
14 Same as above, at para 9.
15 See fn 10 above, at 37 (para 15).

5.13 Although section 59(1A)(c) was not cited in *香港特別行政區 訴朱婷婷*,[16] a DDOS attack may, in principle, also engage that provision on account of the log record that the target computer system generates in response to the attack. The potential relevance of section 59(1A)(c) to a DDOS attack was alluded to in *Chu Tsun Wai*.[17]

Standard of criminalisation under the Budapest Convention

5.14 Pursuant to Article 5 in Title 1 under section 1 of the Budapest Convention:[18]

> *"Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."*

5.15 The Explanatory Report comments on Article 5 as follows:

> *"65. This is referred to in Recommendation No (89) 9 [of the Council of Europe on computer-related crime] as computer sabotage. The provision aims at criminalising the intentional hindering of the lawful use of computer systems including telecommunications facilities by using or influencing computer data. The protected legal interest is the interest of operators and users of computer or telecommunication systems being able to have them function properly. The text is formulated in a neutral way so that all kinds of functions can be protected by it.*
>
> *66. The term 'hindering' refers to actions that interfere with the proper functioning of the computer system. Such hindering must take place by inputting, transmitting, damaging, deleting, altering or suppressing computer data.*
>
> *67. The hindering must furthermore be 'serious' in order to give rise to criminal sanction. Each Party shall determine for itself what criteria must be fulfilled in order for the hindering to be considered 'serious'. For example, a Party may require a minimum amount of damage to be caused in order for the hindering to be considered serious. The drafters considered as 'serious' the sending of data to a particular system in such a form,*

---

16 [2017] 4 HKLRD 651 (The English translation of the judgment was reported as *HKSAR v Chu Ting Ting* [2017] 4 HKLRD 666), HCMA 33/2016 (date of judgment: 11 Oct 2016).

17 See fn 10 above, at 37 (para 18).

18 See para 11 of the Preface and paras 1.6 to 1.10 of Chapter 1 for background information regarding the Budapest Convention.

size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (eg, by means of programs that generate 'denial of service' attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system).

68. The hindering must be 'without right'. Common activities inherent in the design of networks, or common operational or commercial practices are with right. These include, for example, the testing of the security of a computer system, or its protection, authorised by its owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system installs new software that disables similar, previously installed programs. Therefore, such conduct is not criminalised by this article, even if it causes serious hindering.

69. The sending of unsolicited e-mail, for commercial or other purposes, may cause nuisance to its recipient, in particular when such messages are sent in large quantities or with a high frequency ('spamming'). In the opinion of the drafters, such conduct should only be criminalised where the communication is intentionally and seriously hindered. Nevertheless, Parties may have a different approach to hindrance under their law, eg by making particular acts of interference administrative offences or otherwise subject to sanction. The text leaves it to the Parties to determine the extent to which the functioning of the system should be hindered – partially or totally, temporarily or permanently – to reach the threshold of harm that justifies sanction, administrative or criminal, under their law.

70. The offence must be committed intentionally, that is the perpetrator must have the intent to seriously hinder."[19]

Statutory regimes in other jurisdictions

Australia

Section 477.3 of the Criminal Code (Cth)

5.16 It was pointed out in Chapter 1[20] that the origin of the cybercrime

[19] Explanatory Report, at paras 65 to 70.
[20] Para 1.10(g).

provisions in the Criminal Code (Cth) was the MCCOC Report issued in 2001. The offence under section 4.2.6 of the Model Criminal Code, proposed in that Report, "*is aimed at denial of service attacks*"[21] and "*such tactics as flooding email with input beyond its capacity, resulting in system breakdown*".[22] The Report elaborated as follows:

> *"Not every impairment with communications results in an impairment of data … Attacks may take a variety of forms. Communications links to the target computer may be blocked by flooding the system with unwanted messages. The target computer may be induced to generate sufficient volume of messages to prevent communication. Addresses may be altered and messages rerouted. Impairment of communications by the use of these and similar means are collectively described as 'denial of service attacks'. Though some involve impairment of data, others do not."*[23]

5.17 The relevant offence recommended in the MCCOC Report was subsequently enacted as section 477.3 of the Criminal Code (Cth) ("*Unauthorised impairment of electronic communication*"), which was introduced in Chapter 4.[24] Under section 477.3, causing "*any unauthorised impairment of electronic communication to or from a computer*", with knowledge that the impairment is unauthorised, is an offence.

5.18 As noted in Chapter 4,[25] section 476.1 of the Criminal Code (Cth) defines "*impairment of electronic communication to or from a computer*" to include "*the prevention of any such communication*", or "*the impairment of any such communication on an electronic link or network used by the computer*", while excluding "a mere interception of any such communication":

(a) Such non-exhaustive definition allows section 477.3 to apply not only to cases of system interference, but to other circumstances as well. This view is supported by the MCCOC Report's indication that the proposed offence now enacted as section 477.3 was intended to have:

> "*… an extremely broad band of application, from harms which are transient and trifling to conduct which results in serious economic loss or serious disruption of business, government or community activities. The prohibition would be breached by conduct which impaired communication of a single message of no importance … Once it is accepted that criminal liability should be imposed*

---

21 MCCOC Report, at 91.
22 Same as above, at 137.
23 Same as above, at 171.
24 Paras 4.25 to 4.26.
25 Para 4.18.

for intentional impairment of electronic information, conduct which impairs the capacity to receive or transmit that information must similarly fall within the scope of prohibition."[26]

(b) Yet, the reference in section 476.1 to "*prevention*" or "*impairment*" [27] of communication may mean that an unsuccessful attack on a computer system (as in *Chu Tsun Wai*) does not constitute an offence under section 477.3.

5.19 Both the offence recommended in the MCCOC Report and the offence enacted as section 477.3 require knowledge that an impairment is unauthorised. However, the former additionally requires a defendant's intent to impair electronic communication to or from the relevant computer, or recklessness as to any such impairment, whereas this is not required under section 477.3.

Section 477.1 of the Criminal Code (Cth)

5.20 Section 477.1 ("*Unauthorised access, modification or impairment with intent to commit a serious offence*") was discussed in Chapter 2[28] and Chapter 4;[29] the provision is relevant to this Chapter as well.

5.21 Under section 477.1(1)(a)(iii), it is an offence to cause "*any unauthorised impairment of electronic communication to or from a computer*" with knowledge that the impairment is unauthorised, and with intent to commit (or facilitate the commission of) a "*serious offence*" against Commonwealth, State or Territory law by the impairment.

5.22 One can take section 477.1(1)(a)(iii) as section 477.3 with the additional requirement of an intent to commit, or facilitate the commission of, a "*serious offence*". It follows that misconduct such as DDOS attack potentially constitutes an offence under section 477.1(1)(a)(iii) apart from section 477.3.

5.23 A "*serious offence*" is an offence punishable by imprisonment for life or a period of five or more years.[30] A person convicted under section 477.1(1)(a)(iii) is punishable by a penalty not exceeding the penalty applicable to the serious offence.[31]

---

26 MCCOC Report, at 171.
27 Para 3.32.
28 Para 2.21.
29 Para 4.21.
30 Criminal Code (Cth), s 477.1(9).
31 Same as above, s 477.1(6).

Canada

Precedent case of DDOS attack

5.24 The similarity between section 430(1.1) of the Criminal Code 1985 in Canada ("*Mischief in relation to computer data*") and section 6 of the Model Law ("*Interfering with data*") was noted in Chapter 4.[32] However, the Code appears to have no provision corresponding to section 7 of the Model Law ("*Interfering with computer system*") set out below:

> *"(1) A person who intentionally or recklessly, without lawful excuse or justification:*
>
> *(a) hinders or interferes with the functioning of a computer system; or*
>
> *(b) hinders or interferes with a person who is lawfully using or operating a computer system;*
>
> *commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.*
>
> *In subsection (1) 'hinder', in relation to a computer system, includes but is not limited to:*
>
> *(a) cutting the electricity supply to a computer system;*
>
> *(b) causing electromagnetic interference to a computer system;*
>
> *(c) corrupting a computer system by any means; and*
>
> *(d) inputting, deleting or altering computer data."*

5.25 The following incident handled by the Royal Canadian Mounted Police illustrates how a person responsible for a DDOS attack may be prosecuted in Canada:

> *"In 2012, the RCMP [ie, the Royal Canadian Mounted Police] investigated a DDoS attack originating from offices belonging to the House of Commons against the government of Québec's portal website 'www.gouv.qc.ca,' which caused the website to be inaccessible for over two days. During the criminal investigation,*

[32] Para 4.34.

the RCMP used login names, building access records, surveillance images and digital evidence (seized computer equipment) to identify the suspect, a government network administrator who gained administrative privileges to 'www.gouv.qc.ca' to upload malware. In 2013, the suspect was convicted of two counts of unauthorized use of computers and one count of mischief, and sentenced to house arrest."[33]

Section 342.1(1) of the Criminal Code 1985

5.26 While the court documents relating to the above DDOS attack appear unavailable to the public, the charges for "unauthorized use of computers" were probably laid under section 342.1(1) of the Criminal Code 1985 ("*Unauthorized use of computer*"), which was mentioned in Chapter 2:[34]

> *"Everyone is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years, or is guilty of an offence punishable on summary conviction who, fraudulently and without colour of right,*
>
> *(a) obtains, directly or indirectly, any computer service;*
>
> *(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system;*
>
> *(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or under section 430 in relation to computer data or a computer system; or*
>
> *(d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c)."*

Section 430(1) of the Criminal Code 1985

5.27 A possible basis of the charge for mischief in the above DDOS attack was section 430(1) of the Criminal Code 1985 ("*Mischief*"):

---

33 Royal Canadian Mounted Police, *Cybercrime: an overview of incidents and issues in Canada* (2014), at 8, available at http://www.rcmp-grc.gc.ca/en/cybercrime-an-overview-incidents-and-issues-canada (accessed on 3 May 2022).

34 Para 2.28.

"Every one commits mischief who wilfully

(a) destroys or damages property;

(b) renders property dangerous, useless, inoperative or ineffective;

(c) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property; or

(d) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property."

5.28 Section 430(1) applies to mischief in relation to property generally, and its language is similar to that of section 430(1.1) ("*Mischief in relation to computer data*") introduced in Chapter 4.[35] The presence of section 430(1) may explain the absence in the Criminal Code 1985 of a specific provision against the illegal interference of a computer system.

England and Wales

Section 3 of the CMA-EW as enacted

5.29 When the CMA-EW came into force on 29 August 1990, section 3 ("*Unauthorised modification of computer material*") created the following offence:

"(1) A person is guilty of an offence if—

(a) he does any act which causes an unauthorised modification of the contents of any computer; and

(b) at the time when he does the act he has the requisite intent and the requisite knowledge.

(2) For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer and by so doing—

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data.

[35] Para 4.34.

(3) The intent need not be directed at—

(a) any particular computer;

(b) any particular program or data or a program or data of any particular kind; or

(c) any particular modification or a modification of any particular kind.

(4) For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorised.

(5) It is immaterial for the purposes of this section whether an unauthorised modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.

(6) For the purposes of the [1971 c. 48.] Criminal Damage Act 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.

(7) A person guilty of an offence under this section shall be liable—

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and

(b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both."

5.30 A commentator pointed out that there had been "*considerable debate*"[36] at that time over whether the above provision applied to DDOS attack and similar misconduct. In addition, while it was held in *Director of Public Prosecutions v Lennon*[37] (on appeal by case stated) that the then section 3 could apply to an email bombardment, the contrary ruling at first instance "*drew much criticism from the media*".[38]

Reform brought by the Police and Justice Act 2006

5.31 Against such background, section 36 of the Police and Justice Act 2006 substituted a new section (with the heading "*Unauthorised acts with*

---

36 Neil MacEwan, "The Computer Misuse Act 1990: lessons from its past and predictions for its future" [2008] Crim LR 955, at 959.

37 Cited in *Chu Tsun Wai* at 36 (para 14). See para 5.11 above.

38 See fn 36 above, at 960.

intent to impair, or with recklessness as to impairing, operation of computer, etc") for the original section 3 of the CMA-EW. The Explanatory Notes for the Bill enacted as the Police and Justice Act 2006 stated as follows:

> *"301. This amendment is designed to ensure that adequate provision is made to criminalise all forms of denial of service attacks in which the attacker denies the victim(s) access to a particular resource, typically by preventing legitimate users of a service accessing that service, for example by overloading an Internet Service Provider of a website with actions, such as emails… ."*

Section 3 of the CMA-EW in its current form

5.32 The new section 3 came into force in England and Wales on 1 October 2008. The Serious Crime Act 2007 and the Serious Crime Act 2015 have since effected further amendments. The current version of section 3 was set out in Chapter 4[39] but is quoted again here for easy comparison with the original version:

> *"(1) A person is guilty of an offence if—*
>
> *(a) he does any unauthorised act in relation to a computer;*
>
> *(b) at the time when he does the act he knows that it is unauthorised; and*
>
> *(c) either subsection (2) or subsection (3) below applies.*
>
> *(2) This subsection applies if the person intends by doing the act—*
>
> *(a) to impair the operation of any computer;*
>
> *(b) to prevent or hinder access to any program or data held in any computer; or*
>
> *(c) to impair the operation of any such program or the reliability of any such data.*
>
> *(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.*
>
> *(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (c) of subsection (2) above.*

[39] Para 4.38.

(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to—

(a) any particular computer;

(b) any particular program or data; or

(c) a program or data of any particular kind.

(5) In this section—

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) 'act' includes a series of acts;

(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

(6) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) […]

(c) on conviction on indictment, to imprisonment for a term not exceeding ten years or to a fine or to both."

5.33 Section 3 in its current form potentially applies to an unsuccessful DDOS attack, as in *Chu Tsun Wai*, because the target computer's operation need not be actually impaired. According to section 3(2) and (3), it suffices if the attacker intends to cause such impairment, or is reckless as to whether such impairment will result.

Section 3ZA of the CMA-EW

5.34 In cases where an illegal interference of computer system causes or creates a significant risk of "*serious damage of a material kind*" within the meaning of section 3ZA of the CMA-EW, the interference may constitute an offence under section 3ZA. As the provision was examined in Chapter 4,[40] further discussing it here seems unnecessary.

[40] Paras 4.41 to 4.46.

Mainland China

Article 285 and 286 of the PRC Criminal Law

5.35 Article 285(2) of the PRC Criminal Law prescribes that "*any person who, in violation of the State regulations, … conducts illegal control of [the computer information systems not in the fields of State affairs, national defence construction or sophisticated science and technology]*" is subject to punishment.

(emphasis added)

5.36 Article 286(1) is another provision relating to the interference of computer system. It targets acts that makes it impossible for the system to operate normally:

> *"Whoever, in violation of State regulations, cancels, alters, increases or jams the functions of the computer information system, thereby making it impossible for the system to operate normally, if the consequences are serious, shall be sentenced to fixed-term imprisonment of not more than five years or criminal detention; if the consequences are especially serious, he shall be sentenced to fixed-term imprisonment of not less than five years."*[41]

(emphasis added)

Actus reus

5.37 A difference between the Articles 285(2) and 286(1) lies in the acts done to the computer information systems, namely "*conducts illegal control*" versus "*cancels, alters, increases or jams the functions … making it impossible for the system to operate normally*". In practice, it appears that the two Articles may serve as alternative grounds for prosecuting a case.

5.38 In case number 145 in the 26th batch of guiding cases issued by the Supreme People's Court of the PRC,[42] the perpetrators altered or increased the data in a computer information system by planting a Trojan horse program into internet servers to increase the odds of gambling advertisements being shown via search engines. The court held that such acts only resulted in illegal control of the system by the perpetrators, but not any functional damage of, or failure to operate normally by, the system. It therefore decided

---

41 The English translation of Article 286(1) is the official version published by the Legislative Affairs Commission of the NPCSC in 1997. Article 286(1) provides that "*違反國家規定，對計算機信息系統功能進行刪除、修改、增加、干擾，造成計算機信息系統不能正常運行，後果嚴重的，處五年以下有期徒刑或者拘役，後果特別嚴重的，處五年以上有期徒刑。*"

42 Article 7 of the Provisions of the Supreme People's Court on Case Guidance Work (《最高人民法院關於案例指導工作的規定》) requires that the people's courts at all levels shall take the guiding cases published by the Supreme People's Court of the PRC as reference when trying similar cases.

that such acts did not satisfy the requirements imposed by Article 286(1). The perpetrators were, however, convicted of the offence under Article 285(2).[43]

5.39 Furthermore, case number 35 in the 9th batch of SPP's Guiding Cases[44] directs that the act of changing the login credentials of a computer information system (ie a smartphone in the case), with the effect of locking the device and preventing access or proper use by legitimate users, also constitutes an offence under Article 286(1).

New Zealand

Section 250(2)(c) of the New Zealand Act

5.40 When section 250(2) of the New Zealand Act ("*Damaging or interfering with computer system*") was introduced in Chapter 4, we remarked that section 250(2)(c) would be addressed in this Chapter. [45] Under section 250(2)(c):

> *"Every one is liable to imprisonment for a term not exceeding 7 years who intentionally or recklessly, and without authorisation, knowing that he or she is not authorised, or being reckless as to whether or not he or she is authorised …*
>
> *(c) causes any computer system to—*
>
> *(i) fail; or*
>
> *(ii) deny service to any authorised users."*

5.41 Section 250(2) describes the *mens rea* for carrying out the *actus reus* as "*intentionally or recklessly*", whereas the *mens rea* regarding the lack of authorisation is knowledge or recklessness. Concerning the issue of the *mens rea*, our points made in Chapter 4[46] apply to all paragraphs under section 250(2) – including paragraph (c) – and need not be repeated here.

5.42 In relation to the scenarios where section 250(2)(c) applies, a commentator observed as follows:

> *"7.96 Section 250(2)(c) has a broad scope. For example, where software has been badly or recklessly coded with bugs, software manufacturers could be liable under the provision. In addition, those who recklessly send viruses via email would be*

43 張竣傑等非法控制計算機信息系統案。
44 曾興亮、王玉生破壞計算機信息系統案。
45 Paras 4.50 to 4.51.
46 Para 4.57.

liable although it is argued that users should have the latest anti-virus software installed and should be more careful about what they forward.

…

7.98 It is also possible that the subsection could apply to spammers. The element of recklessness is probably applicable to spammers who are unmindful of the impact a large amount of bulk email may have upon a mail server. The flood of unsolicited mail would have to be substantial to bring an ISP mail server to its knees, resulting in a failure, or denial, of service. Thus s 250(2)(c) would not be of universal application to spammers."[47]

Section 250(1) of the New Zealand Act

5.43 Section 250(1), which was also referred to in Chapter 4,[48] is another provision against illegal interference of computer system:

"Every one is liable to imprisonment for a term not exceeding 10 years who intentionally or recklessly destroys, damages, or alters any computer system if he or she knows or ought to know that danger to life is likely to result."

5.44 The commentator cited above compared section 250(1) and (2) in these terms:

"… s 250(1) could apply to a person who has authorisation to access the computer system, but s 250(2) requires a lack of authorisation either:

(1) where the person accessing knows she or he is not authorised; or

(2) is reckless as to whether or not he or she is so authorised.

Putting it another way, an offence under s 250(1) may be committed by a person who is authorised to do certain things to a system like shift or delete files; for example, a system administrator. Section 250(2) requires an absence of authority as an ingredient or the element of recklessness as to authorisation."[49]

---

47 David Harvey, *internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015), at paras 7.96 and 7.98.

48 Para 4.58.

49 See fn 47 above, at para 7.90.

5.45 The commentator's focus on the issue of authorisation underscores its importance in the context of section 250(2) and similar statutes in other jurisdictions. For instance, a mobile data service provider may, by reason of a fair usage policy, secure a contractual right to limit a customer's data transfer speed (when the data usage has exceeded a specified threshold) or to suspend certain data service. While these arrangements restrict the customer's normal use of the data service through his or her device, the customer will, by accepting the fair usage policy, have effectively authorised the restrictions. The service provider need not worry about potential criminal liability when activating the arrangements in situations contemplated in the fair usage policy.

Singapore

Section 7 of the CMA-SG

5.46 Section 7 of the CMA-SG ("*Unauthorised obstruction of use of computer*") prescribes the relevant offence as follows:

> *"(1) Any person who, knowingly and without authority or lawful excuse —*
>
> *(a) interferes with, or interrupts or obstructs the lawful use of, a computer; or*
>
> *(b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer,*
>
> *shall be guilty of an offence and shall be liable on conviction —*
>
> *(c) to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; and*
>
> *(d) in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.*
>
> *(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both."*

5.47 Although the offence provisions of the CMA-SG were based primarily on their counterparts in Canada and England and Wales, the CMA-SG has not added any note informing that section 7 was modelled on any legislative provision in another jurisdiction (which the CMA-SG has done with regard to some other provisions).

Without authority or lawful excuse

5.48 On a plain reading of section 7, no offence is committed if there is either authority or lawful excuse for the conduct set out in paragraphs (a) and (b). The phrase "*without authority*" also appears in section 3 ("*Unauthorised access to computer material*") and section 6 ("*Unauthorised use or interception of computer service*"). Section 2(5) explains the phrase as follows in the context of access to computer program or data:

> *"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 the person—*
>
> *(a) is not himself or herself entitled to control access of the kind in question to the program or data; and*
>
> *(b) does not have consent to access by him or her of the kind in question to the program or data from any person who is so entitled."*

It seems reasonable for "*without authority*" in section 7 to be understood analogously.

5.49 In the CMA-SG, the term "*lawful excuse*" only appears once in section 7 and is undefined. This contrasts with section 64(2) of the Crimes Ordinance (Cap 200) in Hong Kong, which provides for two lawful excuses with regard to a charge for criminal damage (including "*misuse of a computer*").[50]

Scope of application of section 7

5.50 Section 7 of the CMA-SG is widely drafted. Conceptually, its application is not limited to DDOS attack and similar misconduct. A commentator described a case on point as follows:

> *"A systems engineer formerly employed by SMC Marine Services has been accused of secretly setting passwords within a program that he developed before leaving the company, allegedly leaving his former employer unable to check, modify or upgrade the*

[50] Paras 4.92 to 4.94.

> *system. This could constitute an offence under section 5 (Unauthorised Modification) or section 7 (Unauthorised Obstruction) of the [Computer Misuse] Act. Civil litigation seeking injunctions to prevent disclosure of the company's confidential information was also commenced in the High Court."*[51]

5.51 The former employer succeeded in applying for interim injunctions to prevent disclosure and infringement of its alleged copyright.[52] Reportedly, the civil lawsuit then settled. The systems engineer was charged with illegally modifying a computer system, but ultimately acquitted because the court held that the prosecution had "*not satisfied the burden of proof beyond reasonable doubt*".[53]

Maximum penalties in different circumstances

5.52 The CMA-SG stipulates consistent maximum penalties for its offences. The same tariff of maximum penalties, summarised below, applies to a person convicted under either section 5 ("*Unauthorised modification of computer material*")[54] or section 7:

(a) A first offender is liable to a fine not exceeding SGD10,000, or up to three years' imprisonment, or both.

(b) A heavier maximum penalty (a fine not exceeding SGD20,000, or up to five years' imprisonment, or both) is prescribed for a repeat offender.

(c) The maximum penalty for an offender causing actual damage includes a fine not exceeding SGD50,000, or up to seven years' imprisonment, or both.

(d) If an offender accessed any "*protected computer*",[55] section 11(1) of the CMA-SG prescribes an even heavier maximum penalty (a fine not exceeding SGD100,000, or up to twenty years' imprisonment, or both).

---

51 Gregor Urbas, "An Overview of Cybercrime Legislation and Cases in Singapore" (ASLI Working Paper No 001, Dec 2008), at 14.

52 *SMC Marine Services (Pte) Ltd v Thangavelu Boopathiraja and Others* [2008] SGHC 29.

53 The Straits Times, "Man cleared of sabotage" (3 Jun 2009), available at https://www.asiaone.com/News/AsiaOne%2BNews/Crime/Story/A1Story20090603-145841.html (accessed on 3 May 2022).

54 Para 4.64.

55 The statutory definition is set out at para 4.68.

USA

18 USC 1030(a)(5) within the Computer Fraud and Abuse Act

5.53 Despite a view that launching a DDOS attack is analogous to a sit-in[56] (ie a form of protest in which demonstrators occupy a place, refusing to leave until their demands are met)[57] and should be legal,[58] it appears well established in the USA that doing so may violate 18 USC 1030(a)(5), which is set out below. As mentioned in Chapter 4,[59] whoever carried out the following acts is punishable as provided in section 1030(c):

> *"(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;*
>
> *(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or*
>
> *(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss."*

DDOS attacks in the USA

5.54 By way of illustration, an online journal had the following entry dated 19 January 2001:

> *"The US District Court (Alaska) sentenced Scott Dennis, its former computer systems administrator, to six months incarceration and 240 hours of community service for launching three denial of service attacks against the servers of the US District Court (EDNY) … Dennis plead guilty to one misdemeanor count of violation of 18 USC §1030(a)(5)(C). 'It is not the first time a US District Court system has come under attack,' added*

---

56 See, for instance, Chris Peterson, "In Praise of [Some] DDoSs?" (21 Jul 2009) available at http://www.cpeterson.org/2009/07/21/in-praise-of-some-ddoss/ (accessed on 3 May 2022):
"*In some ways a DDoS is like a sit-in. Both, at their conceptual core, consist of overutilizing scarce resources (in the former, server cycles; in the latter, space at a counter) to exclude others for political effect. Both are nonviolent but economically painful. And both can have a political character that might contextualize the offense.*"

57 Oxford University Press, "Lexico.com" (2021) at https://www.lexico.com/definition/sit-in (accessed on 3 May 2022).

58 See, for instance, Mike Masnick, "Anonymous Launches White House Petition Saying DDoS Should Be Recognized As A Valid Form Of Protest" (11 Jan 2013), available at https://www.techdirt.com/articles/20130111/08053821642/anonymous-launches-white-house-petition-saying-ddos-should-be-recognized-as-valid-form-protest.shtml (accessed on 3 May 2022).

59 Paras 4.70 to 4.71.

Cooper; there was an attack against the Western District of Washington. Dennis no longer works for the US District Court. See also, FBI release."[60]

5.55 There continue to be cases of DDOS attacks in the USA. In a high-profile case, the offender pleaded guilty to:

> *"… one count of knowingly causing the transmission of a program, information, code, and command, and as a result of such conduct, intentionally causing damage to a protected computer."*[61]

This was apparently a charge under 18 USC 1030(a)(5)(A). The offender was sentenced to imprisonment for six years.[62]

Overloading voicemail and email systems

5.56 The court documents in the above cases seem to be unavailable online. To understand how 18 USC 1030(a)(5) outlaws the illegal interference of computer system, reference to *Pulte Homes, Inc v Laborers' International Union of North America*[63] is instructive notwithstanding that it was a civil case (which stemmed from an employment dispute).[64]

5.57 The employer in this case (Pulte) alleged that a trade union (LIUNA) "*bombarded Pulte's sales offices and three of its executives with thousands of phone calls and e-mails*"[65] with the following consequences:

> *"The calls clogged access to Pulte's voicemail system, prevented its customers from reaching its sales offices and representatives, and even forced one Pulte employee to turn off her business cell phone. The e-mails wreaked more havoc: they overloaded Pulte's system, which limits the number of e-mails in an inbox; and this, in turn, stalled normal business operations because Pulte's employees could not access business-related e-mails or send e-mails to customers and vendors."*[66]

---

60 Tech Law Journal, "News Briefs from January 11-20, 2001", available at http://www.techlawjournal.com/home/newsbriefs/2001/01b.asp (accessed on 3 May 2022).

61 Federal Bureau of Investigation Cleveland, "Akron Man Arrested and Charged for DDoS Attacks" (10 May 2018), available at https://www.fbi.gov/contact-us/field-offices/cleveland/news/press-releases/akron-man-arrested-and-charged-for-ddos-attacks (accessed on 3 May 2022).

62 USA Department of Justice, "Akron man sentenced to six years in prison for launching denial of service attacks that shut down web sites for the city of Akron and the Akron Police Department" (3 Oct 2019), available at https://www.justice.gov/usao-ndoh/pr/akron-man-sentenced-six-years-prison-launching-denial-service-attacks-shut-down-web (accessed on 3 May 2022).

63 648 F 3d 295 (6th Cir 2011). The Opinion (ie the judgment) of the Court of Appeals for the Sixth Circuit, dated 2 Aug 2011, is available on its website at http://www.ca6.uscourts.gov/opinions.pdf/11a0200p-06.pdf (accessed on 3 May 2022).

64 18 USC 1030 both creates certain cybercrime offences and provides for a civil cause of action.

65 See fn 63 above, at 2.

66 See fn 63 above, at 3.

5.58 The Court of Appeals for the Sixth Circuit addressed all three limbs of 18 USC 1030(a)(5), holding as follows with regard to Pulte's "*transmission claim*" under 18 USC 1030(a)(5)(A):

(a) In applying the statutory definition of "damage", ie "*any impairment to the integrity or availability of data, a program, a system, or information*":[67]

> "*… a transmission that weakens a sound computer system – or, similarly, one that diminishes a plaintiff's ability to use data or a system – causes damage*. *LIUNA's barrage of calls and e-mails allegedly did just that.*"[68]

(b) The district court at first instance was wrong to have required Pulte "*to allege that LIUNA **knew** its calls and e-mails would harm Pulte's computer systems*"[69] or that "*LIUNA fully grasped the **actual** consequences of its e-mail campaign*"[70] (emphases in original). It sufficed for Pulte to:

> "*… allege that LIUNA acted with the conscious purpose of causing damage (in a statutory sense) to Pulte's computer system – a standard that does not require perfect knowledge.*"[71]

Accordingly, the Court of Appeals reinstated Pulte's "*transmission claim*" which was dismissed at first instance.

5.59 However, the Court of Appeals affirmed the district court's ruling that Pulte failed to state an "*access claim*" under 18 USC 1030(a)(5)(B) and (C), and held as follows:

> *"To state an access claim, a plaintiff must allege, among other things, that the defendant 'intentionally accesse[d] a protected computer without authorization.' 18 U.S.C. § 1030(a)(5)(B), (C). … We need not decide whether LIUNA's calls and e-mails accessed Pulte's computers because, even if they did, Pulte does not allege access 'without authorization.' "*[72]

> *"LIUNA used unprotected public communications systems, which defeats Pulte's allegation that LIUNA accessed its computers 'without authorization.' Pulte allows all members of the public to contact its offices and executives: it does not allege, for example,*

---

67 18 USC 1030(e)(8).
68 See fn 63 above, at 7.
69 See fn 63 above, at 8.
70 See fn 63 above, at 9.
71 See fn 63 above, at 9.
72 See fn 63 above, at 10.

that LIUNA, or anyone else, needs a password or code to call or e-mail its business. Rather, like an unprotected website, Pulte's phone and e-mail systems '[were] open to the public, so [LIUNA] was authorized to use [them].' See [Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418,] at 420. And though Pulte complains of the number, frequency, and content of the communications, it does not even allege that one or several calls or e-mails would have been unauthorized. Its complaint thus amounts – at most – to an allegation that LIUNA exceeded its authorized access."[73]

5.60 As the Court of Appeals in the *Pulte* case pointed out,[74] the Supreme Court held in *Leocal v Ashcroft*[75] that a statute must be interpreted consistently whether it is applied in a criminal or noncriminal context. One can therefore anticipate that the court will similarly construe 18 USC 1030(a)(5) in a prosecution for an illegal interference of computer system, for instance, by launching a DDOS attack against a website.

The Sub-committee's views

Tackling data and system interference consistently

5.61 As discussed in Chapter 4 and above, Hong Kong law currently addresses illegal interference of computer data and that of computer system mainly by treating both as "*misuse of a computer*", which is a form of criminal damage. The partial overlap of the two types of misconduct justifies such legal position.

5.62 Case law suggests that, overall, the existing statute has functioned satisfactorily. For instance, *Chu Tsun Wai* illustrates that interfering with a computer system may attract criminal liability irrespective of whether the interference succeeded or not. This is in line with our approach that mere access to the whole or any part of a computer without right should be an offence, and access with intent to carry out further criminal activity should constitute an aggravated offence.

5.63 In our view, the consistency of the present regime against data interference and system interference is a virtue and should be preserved. Accordingly, we recommend that the proposed provisions regarding illegal interference of computer data and that of computer system should be phrased in the same way.

---

73 See fn 63 above, at 11 to 12.
74 See fn 63 above, at 8.
75 543 US 1 (9 Nov 2004).

New legislation should adopt the existing provisions

5.64 We have suggested in Recommendation 6(c) that those parts of sections 59(1A) and 60 of the Crimes Ordinance (Cap 200) which relate to "misuse of a computer" should be transposed to the new legislation.

5.65 In devising such recommendation, we considered whether one can still rely on judicial authorities based on the current law regarding "misuse of a computer" (eg *Chu Tsun Wai*) if this concept is no longer covered by the offence of criminal damage, but rather a new and discrete offence not found in the Crimes Ordinance (Cap 200).

5.66 Provided sufficient care is given to the drafting of the new legislation with proper reference to the current statutory language, we may take comfort from a faithful reflection of the purpose of the new legislation that after the recommended change, the policy and legislative intent underpinning "misuse of a computer" will remain clear, especially if the opportunity will be taken to codify the underlying legal principles from relevant case law.

Possible clarification of "misuse of a computer"

5.67 Assuming Recommendation 6(c) will be implemented, the move of the relevant provisions from the Crimes Ordinance (Cap 200) to the new legislation can be an opportunity to refine the statutory concept of "*misuse of a computer*". For instance, it seems beneficial to:

(a) clarify whether the new legislation's equivalent of section 59(1A)(a) – "*to cause a computer to function other than as it has been established to function by or on behalf of its owner*" – is engaged if an attack is so destructive that it causes the target computer not to function at all; and

(b) incorporate notions such as "*impair the operation of any computer*"[76] into the definition of "*misuse of a computer*".

Scope of application of the proposed offence

5.68 The bottom line is that the new legislation should retain the breadth of the existing law and should not be too restrictive. By way of illustration, apart from the scenarios already covered by the existing law, we consider that the proposed offence should apply to the following parties

[76] Under s 3 of the CMA-EW, it is an offence for a person to do "*any unauthorised act in relation to a computer*" with knowledge that it is unauthorised if the person intends to, among other things, "*impair the operation of any computer*" or is reckless as to whether such consequence would ensue. See para 5.32.

noted in the comparative study above:

(a) an unsuccessful attacker of a computer system;[77]

(b) a manufacturer of software which was intentionally or recklessly coded with a bug;[78] and

(c) a person who, without authorisation, knowingly made any change to a computer system which may have the effect of preventing access or proper use by legitimate users.[79]

Recommendation 7

The Sub-committee recommends that:

(a) The proposed provisions regarding the illegal interference of computer data and computer system should be phrased in the same way.

(b) Sections 59(1A) and 60 of the Crimes Ordinance (Cap 200) suffice to prohibit the illegal interference of computer system and should also be adopted in the new legislation.

(c) The new legislation should retain the breadth of the existing law and should not be too restrictive, while clarifying the phrase "misuse of a computer" as appropriate (eg incorporating the notion "impair the operation of any computer").

(d) The proposed offence of illegal interference of computer system should, for example, apply to a person who intentionally or recklessly:

(i) attacked a computer system whether successful or not (criminal liability should not depend on the success of an interference);

(ii) coded a software with a bug during its manufacture; and

77 See para 5.33 regarding s 3 of the CMA-EW.
78 See para 5.42 regarding s 250(2)(c) of the New Zealand Act.
79 See para 5.50 regarding s 7 of the CMA-SG.

> **(iii) changed a computer system without authorisation, knowing that the change may have the effect of preventing access to, or proper use, of the system by legitimate users.**

Lawful excuse

5.69 Readers would recall from Chapter 2 that, at a global level, there are always some people in cyberspace (including but not limited to cybersecurity practitioners) who are testing others' computers often without the knowledge, let alone authorisation, of the target computer's owner.[80]

5.70 The tools for conducting those tests are readily available. One can find them easily by searching the internet; they do not just appear in the dark web. Many types of testing tools exist and they can cause different degrees of intrusion. Some only scan a computer system once and leave it undamaged, whereas others can carry out scanning persistently for, say, several hours. Some tools can cause significant damage to a computer system. The critical issue is how the tool is used.

5.71 Against such background, we discussed in detail whether scanning (or any similar form of testing) of others' computers for whatever reason should qualify as a lawful excuse under the new legislation with regard to the proposed offence of illegal interference of computer system. So far as cybersecurity practitioners who use testing tools are concerned, in terms of how the law should balance their interests and the interests of the general public, our tentative thinking is that any loss which a more regulated regime may cause to cybersecurity practitioners appears less extensive than the damage or loss which unauthorised use of testing tools may cause to the administrator and owner of the target computer system.

5.72 Public feedback on the consultation questions set out in Recommendation 8 will be useful to us as we finalise our stance. Specifically, paragraph (a) focuses on cybersecurity professionals. Paragraph (b) relates to non-security professionals, such as search engine operators and end users of computers.

---

[80] Para 2.112(a).

Recommendation 8

The Sub-committee invites submissions on:

(a) Should scanning (or any similar form of testing) of a computer system on the internet by cybersecurity professionals, for example, to evaluate potential security vulnerabilities without the knowledge or authorisation of the owner of the target computer, be a lawful excuse for the proposed offence of illegal interference of computer system?

(b) Should there be lawful excuse to the proposed offence of illegal interference of computer system for non-security professionals, such as:

(i) web scraping by robots or web crawlers initiated by internet information collection tools, such as search engines, to collect data from servers without authorisation by connecting to designated protocol ports (eg ports as defined in RFC6335);[81] and/or

(ii) scanning a service provider's system (which has the possibility of abuse or bringing down the system) for the purpose of:

(1) identifying any vulnerability for their own security protection, for example, whether the encryption for a credit card transaction is secure before they, as private individuals, provide their credit card details for the transaction; or

(2) ensuring the security and integrity of an Application Programming Interface offered by the service provider's system?

[81] Information about RFC6335 is available on the website of the Internet Engineering Task Force, at https://datatracker.ietf.org/doc/rfc6335/ (accessed on 3 May 2022).

Chapter 6

Making available or possessing a device or data for committing a crime

Introduction

6.1 In this Chapter, we examine the fifth (last) cyber-dependent offence mentioned in the Preface, ie making available or possessing a device or data for committing a crime. Broadly speaking, an offence in respect of this subject matter would seek to:

(a) curb the production and supply and possession of devices or data that can be used in cyberspace for illegitimate purposes; and

(b) thereby prevent the use of such devices or data for the commission of cybercrime.

6.2 If a person actually uses a device or data to, for instance, hack a computer, that would already constitute the *actus reus* of the offence of illegal access. The focus of this Chapter is whether there should be a distinct offence of simply making available or possessing the device or data (eg possessing a thumb drive storing ransomware) and, if yes, how the offence should be formulated.

6.3 Examples of such devices and data include:

(a) software for testing a network, eg by carrying out a penetration test in order to assess the extent to which a computer system can withstand a DDOS attack;

(b) a password cracker, which may be a piece of software or a physical device; and

(c) a degausser, which is a device that can destroy data in a magnetic storage media (eg a hard disk) by removing its magnetism.

6.4 A person may be able to commit cybercrime by using only software, without the need for any special hardware.

Current Hong Kong law

Crimes Ordinance (Cap 200)

Section 62

6.5 The legislative provisions in Hong Kong that address the cyber-dependent offences discussed in Chapters 2 to 5 are mainly found in the Crimes Ordinance (Cap 200) and the Telecommunications Ordinance (Cap 106). Any provision that is relevant to this Chapter, and intended to apply to the cyber-dependent offences canvassed in previous chapters, should logically be found in those two Ordinances.

6.6 It is convenient to start with the Crimes Ordinance (Cap 200). Section 59(1A) provides that in Part VIII of the Ordinance, "*to destroy or damage any property in relation to a computer includes the misuse of a computer*". Accordingly, the following offence under section 62 ("*Possessing anything with intent to destroy or damage property*") in Part VIII, which is punishable by imprisonment for ten years,[1] applies to "*misuse of a computer*" as well:

> *"A person who has anything in his custody or under his control intending without lawful excuse to use it or cause or permit another to use it—*
>
> *(a) to destroy or damage any property belonging to some other person; or*
>
> *(b) to destroy or damage his own or the user's property in a way which he knows is likely to endanger the life of some other person,*
>
> *shall be guilty of an offence."*

Potential issues in practice

6.7 Section 62 applies to a person who intends to destroy or damage property. It also applies to someone who intends to cause or permit another person to destroy or damage property. The provision does not differentiate between things which can be used for both legitimate and illegitimate purposes on the one hand, and things with only illegitimate uses on the other.

6.8 Whether a person with custody or control of a thing in question is liable depends largely on the person's intent. The subjective nature of a person's mental state may give rise to evidentiary issues in enforcement.

---

1 Crimes Ordinance (Cap 200), s 63(2).

Construction of the proscribed object

6.9 The English text of section 62 describes the proscribed object as "*anything*". The corresponding term in the Chinese text is "*任何物品*".

6.10 In common parlance, "*anything*" is not restricted to tangibles and appears to be a broader term than "*任何物品*" if considered in this light: While a physical object clearly falls within the Chinese rendition, whether its natural meaning clearly extends to certain intangibles which may facilitate the commission of a section 62 offence is a different question. In the context of committing "*misuse of a computer*", the question may be asked in respect of, say, these examples:

(a) computer software or data such as malware and login credentials;

(b) provision of hacking or similar service; and

(c) know-how regarding an exploit.

6.11 To the extent that "*anything*" and "*任何物品*" may have different coverage, section 10B of the Interpretation and General Clauses Ordinance (Cap 1) ("*Construction of Ordinances in both official languages*") comes into play:

> *"(1) The English language text and the Chinese language text of an Ordinance shall be equally authentic, and the Ordinance shall be construed accordingly.*
>
> *(2) The provisions of an Ordinance are presumed to have the same meaning in each authentic text.*
>
> *(3) Where a comparison of the authentic texts of an Ordinance discloses a difference of meaning which the rules of statutory interpretation ordinarily applicable do not resolve, the meaning which best reconciles the texts, having regard to the object and purposes of the Ordinance, shall be adopted."*

6.12 In *T v Commissioner of Police*,[2] a key issue before the Court of Final Appeal was how the word "*admitted*" in the definition of "*public entertainment*"[3] under the Places of Public Entertainment Ordinance (Cap 172) should be construed. Although the appeal was argued largely by reference to

---

2 (2014) 17 HKCFAR 593.

3 Ie "*any entertainment … to which the general public is admitted with or without payment*" (s 2).

the English text of the legislation,[4] the Court had regard to the Chinese expression corresponding to "*admitted*" ("*讓…入場*") when deciding the issue.[5] For instance, Ribeiro PJ accepted that:

> *"… the Chinese text of the definition of 'public entertainment', especially use of the expression '入場', carries a connotation of 'locality' which … does not exist in the English text … a difference exists between the two authentic texts which requires resolution …"*[6]

6.13 The Court also affirmed the cardinal principle that:

> *"… a court cannot attribute to a statutory provision a meaning which the language, understood in the light of its context and statutory purpose, cannot bear".*[7]

6.14 The majority of the Court held that "*admitted*" should be construed in "*an active sense of giving permission to enter or have access or letting a person in*".[8] The ruling was supported (if not influenced) by the Chinese text of the legislation, which appears more specific than the English text.

6.15 When construing section 62 of the Crimes Ordinance (Cap 200), one may say its context and purpose require "*anything*" and "*任何物品*" to cover both tangibles and intangibles, but some may argue that so construing the section seems to strain the natural meaning of "*任何物品*". Another possibility is to take "*anything*" and "*任何物品*" collectively to mean only those concepts shared by both terms. Adopting this approach may, so the argument runs, exclude intangibles from section 62, which would not facilitate application of section 62 to cyberspace.

Section 62 is linked to the offence of criminal damage

6.16 Moreover, section 62 prohibits the custody or control of anything intended for use in destroying or damaging property, ie in committing an offence under section 60 of the Crimes Ordinance (Cap 200). Section 62 does not apply with regard to an offence under another provision, eg section 161 of the same Ordinance ("*Access to computer with criminal or dishonest intent*").

---

4 See fn 2 above, at 679 (para 284) (Lord Neuberger of Abbotsbury NPJ).

5 See fn 2 above, at 607 (para 11(5)) (Ma CJ), at 625 (para 82) (Ribeiro PJ), at 648 (para 166) (Tang PJ), at 666 (para 232) and 671 (para 253) (Fok PJ), and at 679 (para 284) (Lord Neuberger of Abbotsbury NPJ).

6 See fn 2 above, at 625 (para 82) (Ribeiro PJ).

7 See fn 2 above, at 655 (para 195) (Fok PJ), similarly at 607 (para 12) (Ma CJ).

8 See fn 2 above, at 670 (para 250) (Fok PJ).

Telecommunications Ordinance (Cap 106)

6.17 While the Telecommunications Ordinance (Cap 106) has no provision corresponding to section 62 of the Crimes Ordinance (Cap 200), it has created a regime for licensing of radiocommunications apparatus.[9] For the purposes of this Consultation Paper, describing the regime in detail seems unnecessary. It suffices to note that, in circumstances where the regime applies, non-compliance is an offence.[10]

6.18 The regime potentially applies to a computer or a smartphone that can be used to commit an offence under sections 27A, 27(b) and 25(a) of the Telecommunications Ordinance (Cap 106), which we have mentioned in Chapters 2, 3 and 4 respectively when discussing the proposed offences of illegal access, data interception and data interference.[11]

6.19 We consider the existing licensing regime insufficient to combat cybercrime. For example, one of the regime's limitations is its narrow coverage, in that it only applies to telecommunication technologies such as radio waves. The shortcomings of the current law form part of the reason why new, bespoke offences should be enacted.

Standard of criminalisation under the Budapest Convention

6.20 Pursuant to Article 6 in Title 1 under section 1 of the Budapest Convention:[12]

> *"1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:*
>
> *a the production, sale, procurement for use, import, distribution or otherwise making available of:*
>
> *i a device,[13] including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;*

---

9 Telecommunications Ordinance (Cap 106), ss 8(1) and 9; Telecommunications (Telecommunications Apparatus) (Exemption from Licensing) Order (Cap 106Z), ss 5 and 7.

10 See para 6.20, 1-a-i below.

11 Paras 2.11, 3.12 and 4.13.

12 See para 11 of the Preface and paras 1.6 to 1.10 of Chapter 1 for background information regarding the Budapest Convention.

13 A device covered by the offence discussed in this Chapter may also constitute radiocommunications apparatus and hence subject to the licensing regime under the Telecommunications Ordinance (Cap 106).

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,

with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b the possession of an item referred to in paragraphs a i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a ii of this article."

6.21 The Explanatory Report comments on Article 6 as follows:

"71. This provision establishes as a separate and independent criminal offence the intentional commission of specific illegal acts regarding certain devices or access data to be misused for the purpose of committing the … offences [under Articles 2 to 5 of the Budapest Convention] … As the commission of these offences often requires the possession of means of access ('hacker tools') or other tools, there is a strong incentive to acquire them for criminal purposes which may then lead to the creation of a kind of black market in their production and distribution…

72. Paragraph 1(a)1 criminalises the production, sale, procurement for use, import, distribution or otherwise making available of a device … 'Distribution' refers to the active act of forwarding data to others, while 'making available' refers to the placing online devices for the use of others … The inclusion of a 'computer program' refers to programs that are for example

designed to alter or even destroy data or interfere with the operation of systems … or programs designed or adapted to gain access to computer systems.

73. The drafters debated at length whether the devices should be restricted to those which are designed exclusively or specifically for committing offences … This was considered to be too narrow … The alternative to include all devices even if they are legally produced and distributed, was also rejected. Only the subjective element of the intent of committing a computer offence would then be decisive for imposing a punishment … the Convention restricts its scope to cases where the devices are objectively designed, or adapted, primarily for the purpose of committing an offence…

74. Paragraph 1(a)2 criminalises the production, sale, procurement for use, import, distribution or otherwise making available of … data by which the whole or any part of a computer system is capable of being accessed.

75. Paragraph 1(b) creates the offence of possessing the items set out in paragraph 1(a)1 or 1(a)2. Parties are permitted … to require by law that a number of such items be possessed. The number of items possessed goes directly to proving criminal intent…

76. The offence requires that it be committed intentionally and without right … there must be the specific (ie direct) intent that the device is used for the purpose of committing any of the offences established in Articles 2-5 of the Convention.

77. Paragraph 2 sets out clearly that those tools created for the authorised testing or the protection of a computer system are not covered by the provision…

78. … paragraph 3 allows, on the basis of a reservation … to restrict the offence in domestic law. Each Party is, however, obliged to criminalise at least the sale, distribution or making available of … data as described in paragraph 1 (a) 2."[14]

[14] Explanatory Report, at paras 71 to 78.

Statutory regimes in other jurisdictions

Australia

Section 478.3 of the Criminal Code (Cth)

6.22 Section 478.3 ("*Possession or control of data with intent to commit a computer offence*") of the Criminal Code (Cth) in Australia prescribes an offence that is relevant to this Chapter:

> *"(1) A person commits an offence if:*
>
> *(a) the person has possession or control of data; and*
>
> *(b) the person has that possession or control with the intention that the data be used, by the person or another person, in:*
>
> *(i) committing an offence against Division 477; or*
>
> *(ii) facilitating the commission of such an offence.*
>
> *Penalty: 3 years imprisonment.*
>
> *(2) A person may be found guilty of an offence against this section even if committing the offence against Division 477 is impossible.*
>
> *No offence of attempt*
>
> *(3) It is not an offence to attempt to commit an offence against this section.*
>
> *Meaning of possession or control of data*
>
> *(4) In this section, a reference to a person having possession or control of data includes a reference to the person:*
>
> *(a) having possession of a computer or data storage device that holds or contains the data; or*
>
> *(b) having possession of a document in which the data is recorded; or*

(c) having control of data held in a computer that is in the possession of another person (whether inside or outside Australia).”

6.23 Division 477 (“*Serious computer offences*”) of the Criminal Code (Cth), referred to in section 478.3(1)(b)(i), includes:

(a) section 477.1 (“*Unauthorised access, modification or impairment with intent to commit a serious offence*”);

(b) section 477.2 (“*Unauthorised modification of data to cause impairment*”); and

(c) section 477.3 (“*Unauthorised impairment of electronic communication*”).

In essence, they together correspond to the proposed offences discussed in Chapters 2 to 5.

Section 478.4 of the Criminal Code (Cth)

6.24 Apart from section 478.3, section 478.4 (“*Producing, supplying or obtaining data with intent to commit a computer offence*”) of the Criminal Code (Cth) is also on point. The structures of the two provisions are similar:

“(1) A person commits an offence if:

(a) the person produces, supplies or obtains data; and

(b) the person does so with the intention that the data be used, by the person or another person, in:

(i) committing an offence against Division 477; or

(ii) facilitating the commission of such an offence.

Penalty: 3 years imprisonment.

(2) A person may be found guilty of an offence against this section even if committing the offence against Division 477 is impossible.

No offence of attempt

(3) It is not an offence to attempt to commit an offence against this section.

Meaning of producing, supplying or obtaining data

(4) In this section, a reference to a person producing, supplying or obtaining data includes a reference to the person:

(a) producing, supplying or obtaining data held or contained in a computer or data storage device; or

(b) producing, supplying or obtaining a document in which the data is recorded."

6.25 Sections 478.3 and 478.4 originated from sections 4.2.7 and 4.2.8 of the Model Criminal Code proposed in the MCCOC Report, which were "*intended to match the requirements of Article 6*" of the Budapest Convention.[15] The offences created by the two provisions form a pair with the following common features:

(a) Both offences require intent that data be used (by the defendant or another person) in committing an offence against Division 477 of the Criminal Code (Cth), or facilitating the commission of such offence. Recklessness or mere knowledge that data can be used for such purpose would not suffice.

(b) Both offences focus on data only, but not any physical object. However, they define possession or control of data (in the case of section 478.3) or production, supply or obtaining of data (in the case of section 478.4) to include certain scenarios involving tangibles.

Canada

Section 342.1(1) of the Criminal Code 1985

6.26 Section 342.1(1) ("*Unauthorized use of computer*") of the Criminal Code 1985 in Canada was mentioned in Chapters 2 and 3.[16] Section 342.1(1)(d) provides that a person:

15 MCCOC Report, at 92.
16 Paras 2.28 and 3.40.

> *"who, fraudulently and without colour of right … uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c)"*

is guilty of an offence.

6.27 Section 342.1(1)(a), (b) and (c) addresses respectively:

(a) the obtaining of any computer service;

(b) the interception of any function of a computer system; and

(c) the use of a computer system with intent to commit an offence under paragraph (a) or (b) or under section 430 in relation to computer data or a computer system.

6.28 Pursuant to section 342.1(2), to "*traffic*" in respect of a computer password means "*to sell, export from or import into Canada, distribute or deal with in any other way*". The same provision defines "computer password" as "*any computer data by which a computer service or computer system is capable of being obtained or used*". Despite the breadth of such definition, however, apparently it does not include, say, know-how regarding an exploit.

Section 342.2(1) of the Criminal Code 1985

6.29 More generally for regulation of a "*device*" for committing cybercrime, one turns to section 342.2(1) ("*Possession of device to obtain unauthorized use of computer system or to commit mischief*") under which a person:

> *"who, without lawful excuse, makes, possesses, sells, offers for sale, imports, obtains for use, distributes or makes available a device that is designed or adapted primarily to commit an offence under section 342.1 or 430, knowing that the device has been used or is intended to be used to commit such an offence"*

is guilty of an offence.

6.30 Section 342.2(4) defines "*device*" non-exhaustively to include "*(a) a component of a device; and (b) a computer program within the meaning of subsection 342.1(2)*". With regard to the term "*device*", a commentator cited two authorities[17] and observed as follows:

[17] *R v Singh* 2006 ABPC 156 and *R v Coman* 2004 ABPC 18.

> *"Ordinarily, this section would not apply to items such as computers that are not **primarily** designed for the purpose of committing a relevant offence. However, it has been held to apply to digital cameras installed to record personal identification numbers associated with credit card accounts."*[18] (emphasis in original)

6.31 The language of section 342.2(1) is the same as that of section 327(1) ("*Possession of device to obtain use of telecommunication facility or service*"), except that the latter provision applies to:

> *"a device that is designed or adapted primarily to use a telecommunication facility or obtain a telecommunication service without payment of a lawful charge".*

Section 191(1) of the Criminal Code 1985

6.32 Reference should also be made to section 191(1) ("*Possession, etc.*") which is among the provisions on the topic of interception of communications, rather than cybercrime. Under section 191(1), a person:

> *"who possesses, sells or purchases any electro-magnetic, acoustic, mechanical or other device or any component of it knowing that its design renders it primarily useful for surreptitious interception of private communications"*

is guilty of an offence.

6.33 Both sections 191(1) and 342.2(1) incorporate the concept of a device's *primary* use, whereas this concept is absent in section 342.1(1)(d) regarding computer password.

England and Wales

Section 3A of the CMA-EW

6.34 In England and Wales, section 37 of the Police and Justice Act 2006 inserted a new section 3A into the CMA-EW. The Explanatory Notes for the Bill enacted as the Police and Justice Act 2006 summarised the new section and explained its background in these terms:

> *"302. … The new section creates three new offences, each punishable on conviction on indictment with two years' imprisonment or a fine or both. The offences are:*

---

[18] Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015), at 140.

- *making, adapting, supplying or offering to supply an article intending it to be used to commit, or to assist in the commission of, an offence under section 1*[19] *or section 3*[20] *(subsection (1) of the new section);*

- *supplying or offering to supply an article believing that it is likely to be used in this way (subsection (2));*

- *obtaining an article with a view to its being supplied for use in this way (subsection (3)).*

If a person were charged with a subsection (2) offence in relation to a quantity of articles, the prosecution would need to prove its case in relation to any particular one or more of those articles; it would not be enough to prove that the person believed that a certain proportion of the articles was likely to be used in connection with an offence under section 1 or 3.

303. The background to these new offences is the existence of a ready and growing market in electronic tools such as 'hacker tools' which can be used for hacking into computer systems, and the increase in the use of such tools in connection with organised crime. Also, Article 6(1)(a) of the 2001 Council of Europe Cybercrime Convention requires the criminalisation of the distribution or making available of a computer password or similar data by which a computer system is capable of being accessed with the intent to commit an offence. The new offences are designed to implement this … ."

6.35 After insertion of section 3A into the CMA-EW, section 41(2) of the Serious Crime Act 2015 inserted into the CMA-EW section 3ZA ("*Unauthorised acts causing, or creating risk of, serious damage*") discussed in Chapters 4 and 5.[21] Consequently, section 3A refers to "*an offence under section 1, 3 or 3ZA*" as the intended offence to be committed using an "article". Moreover, section 42 of the Serious Crime Act 2015 expanded the scope of section 3A(3) of the CMA-EW.

6.36 After the above amendments, section 3A of the CMA-EW ("*Making, supplying or obtaining articles for use in offence under section 1, 3 or 3ZA*") now reads as follows:

"(1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA.

---

19 Unauthorised access to computer material.

20 Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

21 Paras 4.41 and 5.34.

(2) A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA.

(3) A person is guilty of an offence if he obtains any article—

(a) intending to use it to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA, or

(b) with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA.

(4) In this section 'article' includes any program or data held in electronic form.

(5) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) […]

(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both."

Scope of the offence

6.37 Upon the CMA-EW having come into effect for 30 years, some quarters of society started advocating its reform.[22] For instance, a cross-industry group opines in its report that section 3A has "*clear risks of over-criminalisation*"[23] and elaborates as follows:

> *"3.54 … First, section 3A CMA does not restrict 'articles' to those designed or created to commit an offence, let alone to those 'primarily' designed or created for such a purpose. This means that even Virtual Private Network software (VPNs) and Tor, the onion router allowing for secure communications, are within the scope of the offence, so long as they are used for the commission of the offences …*

[22] By way of illustration, see the Cyber Up Campaign at https://www.cyberupcampaign.com/cma-30th-birthday (accessed on 3 May 2022).

[23] Criminal Law Reform Now Network, *Reforming the Computer Misuse Act 1990* (2020), Chapter 2, at para 4.23, available at http://www.clrnn.co.uk/publications-reports/ (accessed on 3 May 2022).

3.55 Secondly, section 3A only requires 'belief that it is likely' that the tools will be used illegally, when the conduct is that of supplying or offering to supply the tool … The main problem with this broader mental element is that all security and threat researchers ***know****, rather than just believe, 'that it is likely' that criminals will use the hacking tools or anonymity tools like VPNs in order to facilitate crime, so security and threat researchers will be caught within the offence.*

3.56 Thirdly, section 3A makes no mention of a legitimate reason …

3.57 Fourthly, section 3A does not criminalise possession alone. Possession is only indirectly recognised as part of other conducts: making, supplying, offering to supply, and obtaining …

3.58 The combined effect of these requirements is that those who supply or offer to supply dual-use hacking tools as well as VPNs and Tor, and/or who obtain them for personal use or with a view to supply to others, are caught within section 3A. This brings into the scope of the offence: security and threat intelligence researchers; whistleblowers who may obtain a VPN or Tor to secure their communications in order to leak data accessed without authorisation (section 1 CMA); and journalists who supply the same tools (for example SecureDrop) in the belief that it will be used to receive data, notably from whistleblowers (section 3A(2))."[24] (emphasis in original)

Authority illustrating successful enforcement

6.38 The negative comments above do not apply to situations where it is clear that the perpetrator is blameworthy. A case on point is *R v Lewys Martin*[25] where the defendant pleaded guilty to, among others, two charges under section 3A in connection with two programs on his computer called Jaindos (which could instigate a denial of service attack) and CyberGhost (which could provide misleading information regarding the location of an internet protocol address, and thereby offer anonymity to its user).

Sections 6 and 7 of the Fraud Act 2006

6.39 Section 8(1) of the Fraud Act 2006 defines "*article*" in section 6 ("*Possession etc. of articles for use in frauds*") and section 7 ("*Making or supplying articles for use in frauds*") in the same way as section 3A(4) of the CMA-EW does, ie including "*any program or data held in electronic form*". Therefore, sections 6 and 7 of the Fraud Act 2006 apparently overlap to an

---

24 Same as above, Chapter 2, at paras 3.54 to 3.58.
25 [2014] 1 Cr App R (S) 63.

extent with section 3A of the CMA-EW.

6.40 The cross-industry group which complains about the risk of over-criminalisation compared these provisions as follows:

> *"From a prosecutor's point of view, pursuing a charge under section 3A of the [CMA-EW] appears to require proof that the articles could be used for an offence under sections 1 or 3 [or 3ZA]. By using sections 6 or 7 of the Fraud Act 2006 the proof has to be that the tools could be used to commit a fraud …"*[26]

Section 126 of the Communications Act 2003

6.41 For completeness, it should be mentioned that:

(a) section 126(1) of the Communications Act 2003 outlaws the possession or control of anything that may be used for obtaining an electronic communications service, or in connection with obtaining such a service, with intent to misuse that thing in a way as particularised in section 126(3); and

(b) section 126(2) creates an offence of supplying or offering to supply the same kind of thing, with knowledge or belief that its recipient intends to misuse it in a way as particularised in section 126(3).

6.42 Section 126(3) of the Communications Act 2003 refers to a person's intention:

(a) to use the thing to obtain an electronic communications service dishonestly;

(b) to use the thing for a purpose connected with the dishonest obtaining of such a service;

(c) dishonestly to allow the thing to be used to obtain such a service; or

(d) to allow the thing to be used for a purpose connected with the dishonest obtaining of such a service.

---

[26] See fn 23 above, Chapter 1, at para 4.6.

Mainland China

6.43 Article 285(3) of the PRC Criminal Law contains the following offence:

> *"Any person who provides programs or instruments used specially for invading or illegally controlling computer information systems, or knowingly provides programs or instruments to another person for committing illegal or criminal acts of invading or illegally controlling computer information systems shall, if the circumstances are serious, be punished in accordance with the provisions of the preceding paragraph."*[27]
>
> (emphasis added)

6.44 There are two limbs under Article 285(3) concerning provision of a program or instrument, ie (i) "used specially" for invading or illegally controlling computer information systems, and (ii) knowing that another person will use it for such purposes.

6.45 As regards the first limb, pursuant to Article 2 of Interpretation No 19/2011, a program or tool shall be deemed to be a "program or instrument used specially for invading or illegally controlling computer information system" as mentioned in Article 285(3) under the following circumstances:

> *"(1) Having the function of avoiding or breaking through the safeguards for a computer information system and obtaining data in a computer information system without or beyond authorization;*
>
> *(2) Having the function of avoiding or breaking through the safeguards for a computer information system and controlling a computer information system without or beyond authorization; or*
>
> *(3) Otherwise specially designed to invade upon or illegally control a computer information system or illegally obtain the data in a computer information system."*[28]

---

27 The English translation of Article 285(3) is the official version published by the Legislative Affairs Commission of the NPCSC in 1997. Article 285(3) states that: "*提供專門用於侵入、非法控制計算機信息系統的程序、工具，或者明知他人實施侵入、非法控制計算機信息系統的違法犯罪行為而為其提供程序、工具，情節嚴重的，依照前款的規定處罰。*"

28 Article 2 of Interpretation No 19/2011 provides that "*具有下列情形之一的程序、工具，應當認定為刑法第二百八十五條第三款規定的'專門用於侵入、非法控制計算機信息系統的程序、工具'：*

（一）具有避開或者突破計算機信息系統安全保護措施，未經授權或者超越授權獲取計算機信息系統數據的功能的；

（二）具有避開或者突破計算機信息系統安全保護措施，未經授權或者超越授權對計算機信息系統實施控制的功能的；

（三）其他專門設計用於侵入、非法控制計算機信息系統、非法獲取計算機信息系統數據的程序、工具。"

6.46 In relation to the second limb, the offence can be committed by providing a program or instrument which is neutral in nature if the defendant knows that others will use the program or instrument to invade or illegally control a computer information system. Therefore, this limb requires proof of the additional mental element of knowledge besides the intent required under Article 14 of the PRC Criminal Law.

6.47 Another relevant offence provision is Article 286(3) of the PRC Criminal Law:

> *"Whoever intentionally creates or spreads destructive programs such as the computer viruses, thus affecting the normal operation of the computer system, if the consequences are serious, shall be punished in accordance with the provisions of the first paragraph."*[29]
>
> (emphasis added)

6.48 Programs are regarded as "destructive programs such as computer viruses" according to Article 5 of Interpretation No 19/2011 under the following circumstances:

> *"(1) The programs that can copy and spread their part, all or variants through media such as the Internet, storage media and files to destroy the functions, data or application programs of computer systems;*
>
> *(2) The programs that can be triggered automatically under preset conditions to destroy the functions, data or application programs of computer systems; or*
>
> *(3) Other programs specially designed for destroying the functions, data or application programs of computer systems."*[30]

---

29 The English translation of Article 286(3) is the official version published by the Legislative Affairs Commission of the NPCSC in 1997. Article 286(3) reads: "*故意製作、傳播計算機病毒等破壞性程序，影響計算機系統正常運行，後果嚴重的，依照第一款的規定處罰。*"

30 The English translation of Interpretation No 19/2011 is based on the version published by Westlaw China. Article 5 of Interpretation No 19/2011 provides that "*具有下列情形之一的程序，應當認定為刑法第二百八十六條第三款規定的計算機病毒等破壞性程序：*

（一）能夠通過網絡、存儲介質、文件等媒介，將自身的部分、全部或者變種進行複製、傳播，並破壞計算機系統功能、數據或者應用程序的；

（二）能夠在預先設定條件下自動觸發，並破壞計算機系統功能、數據或者應用程序的；

（三）其他專門設計用於破壞計算機系統功能、數據或者應用程序的程序。"

New Zealand

Section 251 of the New Zealand Act

6.49 Section 251 ("*Making, selling, or distributing or possessing software for committing crime*") of the New Zealand Act creates two offences relating to software or other information that would enable access to a computer system without authorisation.

6.50 Section 251(1) creates the first offence. Focusing on the supply side of such software or information, the provision outlaws the following acts by a person ("**Person A**"):

(a) inviting another person to acquire such software or information; or

(b) offering or exposing it for sale or supply; or

(c) agreeing to sell or supply it; or

(d) selling or supplying it; or

(e) possessing it for the purpose of sale or supply,

provided that Person A:

(i) knows that its sole or principal use is the commission of an offence, or

(ii) promotes it as being useful for the commission of an offence (whether or not Person A also promotes it as being useful for any other purpose), knowing or being reckless as to whether it will be used for the commission of an offence.

6.51 Section 251(2), which provides for the second offence, targets the demand side by criminalising possession of such software or information with intent to use it to commit an offence.

6.52 Section 251(1) and (2) both refers to the potential commission of "*an offence*". It seems that this can be an offence of any nature and need not be cybercrime.

Section 216D of the New Zealand Act

6.53 Section 216D(1) ("*Prohibition on dealing, etc, with interception devices*") is also relevant to this Chapter. It prohibits the same acts as those

specified in section 251(1), which are set out above, but with regard to any "*interception device*":

(a) the sole or principal purpose of which a person knows to be the surreptitious interception of private communications; or

(b) that the person holds out as being useful for the surreptitious interception of private communications (whether or not the person also holds it out as being useful for any other purpose).

6.54 Under section 216A(1), "*interception device*" means:

> *"any electronic, mechanical, electromagnetic, optical, or electro-optical instrument, apparatus, equipment, or other device that is used or is capable of being used to intercept a private communication"*

but does not include a hearing aid or similar device, or a device exempted by the Governor-General.

6.55 Sections 216D(1)(ii) and 251(1)(b) of the New Zealand Act outlaw the conduct of promoting or holding out software, information or an interception device as being useful for an illegitimate purpose. While the following academic view was stated in the context of section 251(1)(b), it applies to section 216D(1)(ii) analogously:

> *"In practical terms, the section will be futile in its objective. All that a person need do is promote a potentially illicit program as being for a legitimate purpose and leave the rest up to the imagination."*[31]

6.56 The criticism appears to be well founded. Assuming there has not been such promotion or holding out, the prosecution will have to rely on the alternative basis of liability (under section 216D(1)(i) or section 251(1)(a)) that the defendant knows the sole or principal use or purpose of the software, information or interception device is the commission of an offence, or the surreptitious interception of private communications (as the case may be).

Singapore

Section 8 of the CMA-SG

6.57 Section 7 of the Computer Misuse (Amendment) Act 1998 (No 21 of 1998) inserted a new section 6B into the CMA-SG, which is now renumbered

[31] David Harvey, *internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015), at para 7.112.

as section 8 ("*Unauthorised disclosure of access code*"), in the following terms:

> *"(1) Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any computer shall be guilty of an offence if the person did so —*
>
> *(a) for any wrongful gain;*
>
> *(b) for any unlawful purpose; or*
>
> *(c) knowing that it is likely to cause wrongful loss to any person.*
>
> *(2) Any person guilty of an offence under subsection (1) shall be liable on conviction —*
>
> *(a) to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; and*
>
> *(b) in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both."*

Section 10 of the CMA-SG

6.58 Section 3 of the Computer Misuse and Cybersecurity (Amendment) Act 2017 further inserted a new section 10 ("*Obtaining, etc., items for use in certain offences*") into the CMA-SG, which provides as follows:

> *"(1) A person shall be guilty of an offence if the person —*
>
> *(a) obtains or retains any item to which this section applies —*
>
> *(i) intending to use it to commit, or facilitate the commission of, an offence under section 3, 4, 5, 6 or 7; or*
>
> *(ii) with a view to it being supplied or made available, by any means for use in committing, or in facilitating the commission of, any of those offences; or*
>
> *(b) makes, supplies, offers to supply or makes available, by any means any item to which this*

section applies, intending it to be used to commit, or facilitate the commission of, an offence under section 3, 4, 5, 6 or 7.

(2) This section applies to the following items:

(a) any device, including a computer program, that is designed or adapted primarily, or is capable of being used, for the purpose of committing an offence under section 3, 4, 5, 6 or 7;

(b) a password, an access code, or similar data by which the whole or any part of a computer is capable of being accessed.

(3) A person guilty of an offence under subsection (1) shall be liable on conviction —

(a) to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; and

(b) in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both."

6.59 Sections 8(1) and 10(1)(b) of the CMA-SG appear to overlap partially with each other. The prosecution may need to decide under which section a case should proceed. Realistically, this would probably not give rise to unfairness to a defendant because the two sections prescribe the same maximum penalty. As we will recommend below that the new legislation should be modelled on sections 8 and 10 of the CMA-SG,[32] there may be room for reorganising or consolidating these provisions so as to form a neater legal regime. We shall defer this to the law draftsman.

Comparison with the Model Law

6.60 Another notable feature of section 10 of the CMA-SG is that it specifies the items to which it applies using language that is similar to, but more expansive than that in section 9 ("*Illegal devices*") of the Model Law. Section 9(1) of the Model Law is set out below for comparison:

"A person commits an offence if the person:

(a) intentionally or recklessly, without lawful excuse or justification, produces, sells, procures for use, imports,

[32] Para 6.88(b).

exports, distributes or otherwise makes available:

(i) a device, including a computer program, that is designed or adapted for the purpose of committing an offence against section 5, 6, 7 or 8; or

(ii) a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed;

with the intent that it be used by any person for the purpose of committing an offence against section 5, 6, 7 or 8; or

(b) has an item mentioned in subparagraph (a)(i) or (a)(ii) in his or her possession with the intent that it be used by any person for the purpose of committing an offence against section 5, 6, 7 or 8."

USA

18 USC 1030(a)(6) within the Computer Fraud and Abuse Act

6.61 Under 18 USC 1030(a)(6) in the USA, whoever:

"knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States"

shall be punished as provided in 18 USC 1030(c).

6.62 As defined in 18 USC 1029(e)(5), "*traffic*" means "*transfer, or otherwise dispose of, to another, or obtain control of with intent to transfer or dispose of*".

6.63 The legislation does not define "*password or similar information through which a computer may be accessed without authorization*". The natural meaning of this phrase would include things such as login credentials and, depending on how "similar" should be construed, probably know-how regarding an exploit as well. However, whether the phrase covers software for accessing a computer without authorisation seems open to debate.

18 USC 1029

6.64 In any event, the proposition that 18 USC 1030(a)(6) does not apply to a physical object should be uncontroversial. Instead, 18 USC 1029(a) creates ten separate offences relating to (among other things) the possession, production, use and trafficking of an "*access device*".

6.65 The following definition of "*access device*" in 18 USC 1029(e)(1) includes both tangibles and intangibles:

> *"any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)".*

6.66 The Computer Crime and Intellectual Property Section of the USA Department of Justice explained some typical applications of 18 USC 1029 as follows:

> *"Prosecutors commonly bring charges under section 1029 in many types of 'phishing' cases, where a defendant uses fraudulent emails to obtain bank account numbers and passwords, and 'carding' cases, where a defendant purchases, sells, or transfers stolen bank account, credit card, or debit card information."*[33]

18 USC 2512

6.67 Besides 18 USC 1029, the word "*device*" appears in 18 USC 2512(1) which prohibits (in essence) the intentional manufacture, distribution, possession and advertisement of:

> *"any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications".*

---

[33] H Marshall Jarrett, Michael W Bailie, Ed Hagen and Scott Eltringham, *Prosecuting Computer Crimes* (Office of Legal Education, Executive Office for United States Attorneys, 2nd edition, 2010), at 102 to 103, available at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (accessed on 3 May 2022).

6.68 The reference in 18 USC 2512(1) to a device's primary use – as opposed to, say, its only or possible use – is also seen in Article 6 of the Budapest Convention,[34] sections 191(1) and 342.2(1) of the Criminal Code 1985 in Canada,[35] and section 10(2)(a) of the CMA-SG[36] (all discussed above).

The Sub-committee's views

New offence with a basic form and an aggravated form should be enacted

6.69 At present, sections 60 and 62 of the Crimes Ordinance (Cap 200) work together to outlaw criminal damage. If, as suggested in Recommendation 6(c), the provisions in the Ordinance which relate to "*misuse of a computer*" will be transposed to the new legislation, it is only right for the new legislation to include a provision corresponding to section 62.[37] We further take the view that such provision should apply with regard to all four cyber-dependent offences discussed in Chapters 2 to 5.

6.70 Throughout our discussions, we grappled with the challenge presented by devices and data with both legitimate and illegitimate uses. An example is a degausser mentioned at paragraph 6.3(c), which financial institutions would use to clear the content of their old hard disks as a security measure. We believe it is uncontroversial that possessing a degausser in that context raises no issue. In contrast, possessing a degausser with intent to use it for illegitimate purposes (eg sabotage) justifies criminal liability.

6.71 In the physical world, the concept of "*offensive weapon*" gives rise to similar considerations. Under the Public Order Ordinance (Cap 245), the definition of "*offensive weapon*"[38] differentiates between articles "*made*", "*adapted*", "*suitable*"[39] or "*intended*" for causing injury. In applying such definition:

(a) Criminal intent need not be proved and mere possession in a public place suffices for criminal liability in cases involving, for example:

---

34 Para 6.20.

35 Paras 6.29 and 6.32.

36 Para 6.58.

37 "*A person who has anything in his custody or under his control intending without lawful excuse to use it or cause or permit another to use it—*
(a) to destroy or damage any property belonging to some other person; or
(b) to destroy or damage his own or the user's property in a way which he knows is likely to endanger the life of some other person,
shall be guilty of an offence."

38 S 2(1) defines "offensive weapon" as:
"*any article made, or adapted for use, or suitable, for causing injury to the person, or intended by the person having it in his possession or under his control for such use by him or by some other person*".

39 In *R v Chong Ah Choi & Ors* [1994] 3 HKC 68, HCMA 281/1994 (date of judgment: 4 Oct 1994), the Court of Appeal essentially decided (at 7G) that the limb of "suitable" in the definition of "offensive weapon" should no longer apply.

(i) A gun, a machete or a butterfly knife (because it is, by its nature, "*made … for causing injury to [a] person*"); or

(ii) An umbrella with a bayonet attached, or a rod that has been sharpened and has spikes attached (because the umbrella or the rod has been "adapted" for causing injury).

(b) However, given the neutral nature of, say, a fruit knife or a "Swiss Army knife", it would become an offensive weapon only if it is "*intended by the person having it in his possession or under his control for such use*".

6.72 Borrowing from the taxonomy above, we recommend splitting the proposed offence into a basic form and an aggravated form. Apart from categorisation of the device or data based on whether it was made or adapted for illegitimate use in a given case, another differentiating factor should be whether criminal intent exists. Such categorisation alone is not a satisfactory determinant of criminal liability because the uses of a device or data may change as computer and internet technology develops. For instance, people have started using graphics cards to mine cryptocurrencies.

Devices and data to which the proposed offence should apply

For both the basic and aggravated forms of the proposed offence

6.73 Cybercrime can be committed with or without a physical device. By way of illustration, knowingly distributing ransomware on the internet can already wreak havoc. Describing ransomware, viruses, their source code and similar things as cyberweapon is not far-fetched. For the proposed offence to be effective in cyberspace, we consider that it should apply to both tangibles and intangibles.

6.74 Separately, in light of the precedent legislation in New Zealand,[40] we prefer that the illegitimate use of the devices and data to be prohibited by the new legislation should not be limited to committing cybercrime, but should relate to any offence generally.

6.75 We further considered whether the proposed offence should apply to a device or data so long as its primary use is to commit an offence, whether or not the device or data can be used for any legitimate purpose. In our opinion, the proposed offence will be too restrictive if it only applies to a device or data without any possible legitimate use. By the same token, the primary use of a device or data should be determined objectively, regardless of a defendant's subjective intent. In sum, we have come to the view that the proposed offence should apply to a device or data so long as its primary use

[40] See paras 6.50 and 6.51 referring to s 251(1) and (2) of the New Zealand Act.

(to be determined objectively) is to commit an offence, whether or not the device or data can be used for any legitimate purpose.

6.76 We also discussed whether the proposed offence should apply to a device or data that is believed or claimed to be, but not actually, capable of being used to commit a crime, such as:

(a) an incorrect password; or

(b) a password cracker that is supposedly capable of cracking a password in ten minutes, but fails to do so after a much longer period, due to its faulty design or defects.

6.77 Noting that section 62 of the Crimes Ordinance (Cap 200) does not expressly require a thing in question to be actually capable of destroying or damaging property, we have concluded that it should suffice if a device or data is believed or claimed to be capable of being used to commit an offence, irrespective of whether that is true or not. This position will be in line with our consensus, based on *Chu Tsun Wai*, that criminal liability should not depend on the success of a cyberattack.

For the basic offence

6.78 We further recommend that:

(a) the basic offence should cover a device or data made or adapted to commit an offence; and

(b) one should assess whether the criterion in (a) is satisfied by reference to the primary use (to be determined objectively, regardless of a defendant's subjective intent) of the device or data.

6.79 At the same time, our recommended formulation excludes a device or data that is neutral by nature (eg a degausser as discussed above)[41] but intended to be used to cause harm. The reason is that if there is no such intent, criminalisation appears not justified. Conversely, if such intent exists, the aggravated offence will apply.

For the aggravated offence

6.80 Building on our views explained above, we recommend that the aggravated offence should apply to a device or data that is, or is believed or claimed by the perpetrator to be, capable of being used to commit an offence.

---

41 Para 6.70.

Actus reus

6.81 Both the Explanatory Report for the Budapest Convention[42] and the Explanatory Notes for the Bill enacted as the Police and Justice Act 2006[43] referred to the existence of a market for "hacker tools" and similar tools. We believe that, to be comprehensive, a statutory response to the thriving of such market must target all categories of its participants, regardless of whether they represent the supply or the demand in the market.

6.82 We therefore recommend that the *actus reus* of the proposed offence should cover both the supply side (such as production, offering, sale and export of a device or data in question) and the demand side (such as obtaining, possession, purchase and import of a device or data in question).

Mens rea

For both the basic and aggravated forms of the proposed offence

6.83 We consider that a person should be guilty of making available or possessing a device or data described above only if the person does so knowingly. A lower threshold – requiring, say, recklessness or no particular mental state at all – seems inappropriate given that many people possess software or computer data, or even make it available to others, without being aware of it. For example:

(a) A criminal can remotely plant malicious software or data in an innocent person's computer.

(b) A person may possess a computer file that is (unbeknown to that person) infected with malware. The person may upload the file to an online storage space, thinking that only he or she can retrieve it. In reality, the administrator of the storage space can likely access the file. If the storage space is not or inadequately protected, the file may even be available to the whole internet community.

If the offence does not require knowledge but can be committed with mere recklessness, or regardless of a defendant's mental state, the offence potentially applies to the innocent person in scenario (a) and the person in scenario (b) above. The coverage of the offence would appear to be unnecessarily broad.

---

42 Para 71 of the Explanatory Report quoted in para 6.21.

43 Para 303 of the Explanatory Notes quoted in para 6.34.

For the basic offence

6.84 If a person is charged with the basic offence on account of the person's belief[44] that the relevant device or data can be used to commit an offence, such belief will form part of the *mens rea* to be established by the prosecution.

For the aggravated offence

6.85 If a person is charged with the aggravated offence, by definition, the person's intent to use the relevant device or data to commit an offence must be proved in addition to all other aspects of the *mens rea* discussed in paragraphs 6.83 and 6.84 above.

Proposed statutory defence of reasonable excuse

6.86 Possessing an offensive weapon in a public place constitutes no offence if there is "*lawful authority or reasonable excuse*",[45] eg where the possessor uses a pole weapon in performing art.

6.87 We recommend that the proposed offence should likewise incorporate a statutory defence of reasonable excuse, because there can be various legitimate reasons for a person or entity to require devices or data that can be used to commit a crime. In our opinion, the proposed defence can help avoid over-criminalisation as discussed by, say, the cross-industry group critical of the CMA-EW.[46]

Model for the proposed provisions

6.88 The drafting of the other jurisdictions' offences surveyed above differs significantly and demonstrates various possibilities. In formulating the new legislation in Hong Kong, we suggest drawing on, and improving on:

(a) section 3A of the CMA-EW; and

(b) sections 8 and 10 of the CMA-SG.

6.89 We have deliberated whether the concept "possession" sits well with our intention to apply the proposed offence to intangibles such as data. There is a well-established body of case law on the nature of "possession" as a legal concept. The following passage from *Archbold Hong Kong 2021*

---

44 Paras 6.76 to 6.77.
45 Public Order Ordinance (Cap 245), s 33(1).
46 Para 6.37.

describes the essence of this concept:

> "*A person may be held to be in possession of a thing if sufficient evidence is forthcoming to demonstrate both physical control over it, in the sense of ability to use as may be desired, within the parameters of practicality and the law, and to exclude others, and of an intention to exercise such control.*"[47]
>
> (emphasis added)

6.90 In other words, "possession" denotes control over a thing and does not necessarily require the thing to be tangible. In fact, "possession" has been specifically applied to offences involving computer program or data in other statutory contexts, such as possession of infringing articles under the Copyright Ordinance (Cap 528)[48] and possession of child pornography under the Prevention of Child Pornography Ordinance (Cap 579).[49] We further observe that some jurisdictions in our comparative study have applied "possession" to data, information, computer program and software, all of which are intangibles.[50] In these circumstances, we consider "possession" to be an appropriate element of the proposed offence.

Recommendation 9

The Sub-committee recommends that:

(a) Knowingly making available or possessing a device or data (irrespective of whether it is tangible or intangible, eg ransomware, a virus or their source code) made or adapted to commit an offence – ie not necessarily cybercrime – should be a basic offence under the new legislation, subject to a statutory defence of reasonable excuse.

---

47 *Archbold Hong Kong 2021*, at para 29-39.

48 Under s 118(2A) of the Copyright Ordinance (Cap 528), a person commits an offence if he, "*without the licence of the copyright owner of a copyright work to which this subsection applies, possesses an infringing copy of the work for the purpose of or in the course of any trade or business with a view to its being used by any person for the purpose of or in the course of that trade or business.*" By virtue of s 118(2B), s 118(2A) also protects copyright work which is a "computer program".

49 Under s 3(3) of the Prevention of Child Pornography Ordinance (Cap 579), a person who has child pornography in his possession commits an offence. S 2(1) defines "child pornography" to include "*data stored in a form that is capable of conversion into*" a photograph, film, computer-generated image or other visual depiction that is a pornographic depiction of a child.

50 For instance, s 478.3 of the Australian Criminal Code (Cth) criminalises the "possession" or control of data with intent to commit a computer offence (see para 6.22). S 342.2(1) of the Canadian Criminal Code 1985 criminalises, among other things, the "possession" of devices designed or adapted primarily to commit an offence under s 342.1 or s 430, and "device" includes computer program (see paras 6.29 to 6.30). S 251(1) of the New Zealand Act criminalises, among other things, the "possession" of software or information for committing crimes (see para 6.50). In the USA, s 1029(a) of the Computer Fraud and Abuse Act criminalises, among other things, the "possession" of "access devices", which include intangibles and data by virtue of s 1029(e)(1) (see paras 6.64 to 6.65).

(b) **The *actus reus* of the proposed offence should cover both the supply side (such as production, offering, sale and export of a device or data in question) and the demand side (such as obtaining, possession, purchase and import of a device or data in question).**

(c) **The proposed offence should apply to:**

(i) **a device or data so long as its primary use (to be determined objectively, regardless of a defendant's subjective intent) is to commit an offence, regardless of whether or not it can be used for any legitimate purposes; and**

(ii) **a person who believes or claims that the device or data in question could be used to commit an offence, irrespective of whether that is true or not.**

(d) **Knowingly making available or possessing a device or data (irrespective of whether it is tangible or intangible, eg ransomware, a virus or their source code):**

(i) **which is, or is believed or claimed by the perpetrator to be, capable of being used to commit an offence; and**

(ii) **which the perpetrator intends to be used by any person to commit an offence**

should constitute an aggravated offence under the new legislation, subject to a statutory defence of reasonable excuse.

(e) **The proposed provisions should be modelled on section 3A of the CMA-EW as well as sections 8 and 10 of the CMA-SG.**

Possession of data with only harmful use

6.91 Having recommended a general defence of reasonable excuse above, we would like to conclude this Chapter by asking whether the new legislation should also recognise a more specific defence or exemption to the offence of knowingly possessing computer data (the software or the source code) the use of which can only be to perform a cyber-attack. Examples of such computer data include:

(a) ransomware;

(b) virus;

(c) software for creating and managing botnets; and

(d) harvesting software, which can scan a computer for specific items such as banking and credit cards credentials and other data which can be later exploited in frauds.[51]

6.92 Harmful these types of computer data may be, we can see an argument that the law need not (or should not) criminalise their possession in, say, the following circumstances:

(a) keeping of malware by universities for educational or research purposes;

(b) development of antivirus software;

(c) training of spam filters in internet service providers' email servers using malware;[52] and

(d) research of malicious codes by other information technology practitioners through reverse engineering.

6.93 In terms of where the line should be drawn, all would depend on the circumstances. To use an analogy in the physical world, a person's interest in research would unlikely justify the person keeping explosives at home. With these remarks, we look forward to receiving submissions from the public on the questions set forth below.

---

51 The third and fourth examples were given in the report of the cross-industry group mentioned above. See Criminal Law Reform Now Network, *Reforming the Computer Misuse Act 1990* (2020), at para 3.24 of Chapter 1.

52 Spam filters that employ artificial intelligence technology can be trained so that their performance can improve over time.

Recommendation 10

The Sub-committee invites submissions on:

(a) Whether there should be a defence or exemption for the offence of knowingly making available or possessing computer data (the software or the source code), such as ransomware or a virus, the use of which can only be to perform a cyber-attack?

(b) If the answer to paragraph (a) is "yes",

(i) in what circumstances should the defence or exemption be available, and in what terms?

(ii) should such exempted possession be regulated, and if so, what are the regulatory requirements?

Chapter 7

Criteria for the Hong Kong court to assume jurisdiction

Introduction

7.1 This Chapter discusses the jurisdictional issues associated with cybercrime and focuses on the criteria for the Hong Kong court to assume jurisdiction. It is convenient to start with the general principles, before turning to the international experience in addressing jurisdictional issues in cybercrime legislation.

7.2 Commentators[1] have identified the following three separate but interrelated aspects of jurisdiction:

(a) The jurisdiction to prescribe, which is about a legislature's competence to regulate certain conduct;

(b) The jurisdiction to adjudicate, which is about whether certain conduct is justiciable before a court; and

(c) The jurisdiction to enforce, which is about a legal regime's authority to require compliance or punish non-compliance.

General principles on jurisdiction

Common law approach

7.3 As the Court of Final Appeal stated in *HKSAR v Wong Tak Keung* ("***Wong Tak Keung***"):

> *"The general rule is that the courts' criminal jurisdiction is territorial … This applies both to common law and statutory offences. Offence-creating statutes are construed applying a strong presumption against extra-territorial effect."*[2]

---

1 Susan W Brenner and Bert-Jaap Koops, "Approaches to Cybercrime Jurisdiction" (2004) Vol 4, No 1, Journal of High Technology Law, at 5; Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015), at 475; David Harvey, *internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015), at para 6.206; and Alisdair A Gillespie, *Cybercrime: Key Issues and Debates* (Routledge, 2016), at 21.

2 (2015) 18 HKCFAR 62, at 74 and 75 (paras 27 and 28), FACC 8/2014 (date of judgment: 9 Jan 2015).

7.4 In general, therefore, "*the exercise of criminal jurisdiction does not extend to cover acts committed on land abroad*".[3] The Supreme Court of Canada observed as follows in *Libman v The Queen*:

> *"… the territorial principle in criminal law was developed by the courts to respond to two practical considerations, first, that a country has generally little direct concern for the actions of malefactors abroad; and secondly, that other states may legitimately take umbrage if a country attempts to regulate matters taking place wholly or substantially within their territories. For these reasons the courts adopted a presumption against the application of laws beyond the realm …"*[4]

7.5 Despite the general adherence to the territorial principle, many states claim jurisdiction over offences committed upon ships flying the flag of a state in question and aircraft registered there, because those ships and aircraft "*are frequently considered to be an extension of the territory of the State*".[5] In Hong Kong, this concept of extended territoriality has statutory recognition:

(a) Under section 3(1) of the Aviation Security Ordinance (Cap 494):

> "*Any act or omission taking place on board a Hong Kong-controlled aircraft while in flight elsewhere than in or over Hong Kong which, if taking place in Hong Kong, would constitute an offence under the law of Hong Kong shall constitute that offence.*"

(b) Under section 23B(1) of the Crimes Ordinance (Cap 200):

> "*Any act of any person which—*
>
> *(a) takes place on board a Hong Kong ship on the high seas; and*
>
> *(b) apart from this section is not an offence; and*
>
> *(c) would, were it to take place in Hong Kong, constitute an offence under the law of Hong Kong,*
>
> *shall, subject to subsections (5) and (7), whatever the citizenship or nationality of the person, constitute that offence.*"

---

3 *Treacy v DPP* [1971] AC 537, at 552.
4 *Libman v The Queen* [1985] 2 SCR 178, at 208f.
5 Explanatory Report, at para 235.

7.6 Unfortunately, crime "*has ceased to be largely local in origin and effect*" and "*is now established on an international scale*".[6] It is quite possible for only some elements of an offence to occur within one jurisdiction and other elements to occur elsewhere. In cases of:

> *" 'result crimes' where a defendant does a prohibited act producing a prohibited result … and the act and the result occur in two different jurisdictions … The traditional view was that offences in this category were deemed to have been committed only in the place where the offence was completed — where the final essential element occurred — often called the 'terminatory approach'."*[7]

7.7 However, the Supreme Court of Canada adopted a more flexible approach in *Libman*, which La Forest J described as follows on behalf of that court:

> *"I might summarize my approach to the limits of territoriality in this way. As I see it, all that is necessary to make an offence subject to the jurisdiction of our courts is that a significant portion of the activities constituting that offence took place in Canada. As it is put by modern academics, it is sufficient that there be a 'real and substantial link' between an offence and this country, a test well-known in public and private international law …"*[8]

7.8 Other common law jurisdictions have since followed suit and embraced some form of approach that is more flexible than strict adherence to the territorial principle. For instance:

(a) In *Lipohar v R*,[9] where the material facts involved multiple Australian states (and hence multiple jurisdictions), the majority of the High Court upheld the convictions of the appellants (defendants) in South Australia and commented as follows on the issue of jurisdiction:

> "*In the present case, the question becomes whether the connection between the subject matter of the charge and South Australia was sufficient. That is a search for the sufficiency of connecting factors. No question of fiction or deeming intrudes … The requirement of nexus should be liberally applied. A real connection with the jurisdiction will suffice.*"[10]

---

6 *Liangsiriprasert v United States* [1991] 1 AC 225, at 251C.
7 See fn 2 above, at 77 (para 33).
8 [1985] 2 SCR 178, at 212j to 213a.
9 [1999] HCA 65.
10 [1999] HCA 65, at paras 122 and 123.

(b) In England and Wales, the Court of Appeal (Criminal Division) held in *R v Smith (Wallace Duncan) (No 4)* that English courts could assume jurisdiction:

> "*… if either the last act took place in England or a substantial part of the crime was committed [in England] and there was no reason of comity why it should not be tried [in England].*"[11]

(c) In Hong Kong, the Court of Final Appeal in *Wong Tak Keung* endorsed the approach in England and Wales:

> "*… the wider approach derived from R v Smith (No 4), was, in our view correctly, preferred by Deputy Judge Stuart-Moore in HKSAR v Chan Shing Kong, and approved* obiter *by the Court of Appeal in HKSAR v Krieger.*"[12]

Hong Kong legislation prescribing jurisdictional rules

7.9 As the Court of Final Appeal in *Wong Tak Keung* also pointed out, the general rule that the courts' criminal jurisdiction is territorial "*is subject to statutory modification*".[13] For example, under the Criminal Jurisdiction Ordinance (Cap 461) ("**CJO**"):

(a) section 2(2) defines certain substantive offences of fraud and dishonesty under the Theft Ordinance (Cap 210) and the Crimes Ordinance (Cap 200) as Group A offences;[14] and

(b) section 3 provides that a person may be guilty of a Group A offence so long as any "*relevant event*", or in other words:

> "*any act or omission or other event (including any result of one or more acts or omissions) proof of which is required for conviction of the offence*"

occurred in Hong Kong even if other essential elements of the offence occurred elsewhere.

7.10 Conceptually, section 3 of the CJO covers at least the two scenarios described below:

---

11 [2004] QB 1418, at 1434H.
12 See fn 2 above, at 81 (para 45).
13 Same as above, at 75 (para 29).
14 In contradistinction to the inchoate offences of conspiracy, attempt and incitement, ie the Group B offences in s 2(3).

(a) A person in Hong Kong carrying out part of the *actus reus* of a Group A offence against a victim (an individual) or a target (an object, such as a computer) outside Hong Kong; and

(b) A person outside Hong Kong carrying out part of the *actus reus* against a victim or a target in Hong Kong.

7.11 The first scenario in the preceding paragraph broadly corresponds to the more flexible approach at common law as discussed above. The second scenario can be seen as reflecting the "objective territorial principle", under which courts could claim jurisdiction for "*acts committed abroad which have an effect in the jurisdiction*".[15]

7.12 In 2002, the Government submitted the draft Criminal Jurisdiction Ordinance (Amendment of Section 2(2)) Order 2002 to the Legislative Council for approval. The purpose of the draft Order was to add the following three computer offences to the list of Group A offences:

(a) "Unauthorized access to computer by telecommunications" under section 27A of the Telecommunications Ordinance (Cap 106);[16]

(b) "Destroying or damaging property" relating to misuse of a computer under sections 59 and 60 of the Crimes Ordinance (Cap 200);[17] and

(c) "Access to computer with criminal or dishonest intent" under section 161 of the Crimes Ordinance (Cap 200).[18]

However, the above proposal was ultimately not implemented because the relevant Subcommittee of the Legislative Council did not support the draft Order.[19]

7.13 Apart from the CJO, some other Ordinances contain provisions on jurisdictional issues with regard to specific offences. For instance:

(a) Schedule 2 to the Crimes Ordinance (Cap 200) contains a list of sexual offence provisions with extra-territorial effect when

---

15 Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press, 2007), at para 5.27; similarly Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015), at 477.

16 Discussed in Chapter 2 (para 2.11).

17 Discussed in Chapter 4 (para 4.7) and Chapter 5 (para 5.7).

18 Discussed in Chapter 2 (para 2.6).

19 According to the Subcommittee's Report dated 25 Jun 2004, one member did not support the draft Order because she took the view that extended jurisdiction for computer offences should be provided for in a new, consolidated piece of legislation, rather than the CJO. Her view was shared by some other members. Another member considered that the mechanism to amend the list of offences under the CJO (ie by an order made by the Chief Executive in Council with prior approval of the Legislative Council by way of an affirmative resolution) was not as desirable as a three-reading procedure.

committed by or in relation to certain classes of persons.

(b) Under section 4 of the Prevention of Bribery Ordinance (Cap 201), it is an offence for any person "*whether in Hong Kong or elsewhere*" to offer any advantage, or any public servant "*whether in Hong Kong or elsewhere*" to solicit or accept any advantage as, say, an inducement or a reward, without lawful authority or reasonable excuse.

Generally accepted bases of extra-territorial jurisdiction

7.14 There are four generally accepted bases of extra-territorial jurisdiction:

(a) The active personality principle (based on a perpetrator's nationality);

(b) The passive personality principle (based on a victim's nationality);

(c) The universality principle (ie any state should have jurisdiction over the most serious offences, such as crimes against humanity); and

(d) The protective principle (ie a state should have jurisdiction over an act which threatens its national security or interest, even if the act occurred outside the state).[20]

Jurisdictional issues associated with cybercrime

Challenges presented by cybercrime

7.15 The financial and technological thresholds to launch a cross-jurisdictional attack in cyberspace are low. Partly due to this, cybercrime often involves multiple jurisdictions. An apparently domestic cybercrime case may nonetheless involve, say:

(a) an internet server in another jurisdiction; or

(b) a service provider (such as an operator of social media or communication software) headquartered in another jurisdiction.

---

[20] Alisdair A Gillespie, *Cybercrime: Key Issues and Debates* (Routledge, 2016), at 23; similarly Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press, 2007), at para 5.27.

7.16 With cybercrime, determining where a fact occurred is potentially difficult. For example, cloud computing works in a way that "*the data requested may not be in one location but instead is spread out across multiple locations*".[21] In a case of illegal access to a victim's data stored in cloud, the following observations in the UNODC Comprehensive Study on Cybercrime are apt:

> *"Cloud data processing involves multiple data locales or data centres, distributed across different national jurisdictions, and with different private data controllers and processors. Under present conditions, although data location may be technically knowable, cloud computing users are not always informed exactly 'where' their data is held. In turn, jurisdictional approaches both to the data protection regime governing data held by cloud service providers, and criminal procedure law governing national law enforcement investigations are complex."*[22]

Judicial recognition of challenges in cybercrime

7.17 The courts have long recognised the jurisdictional issues often found in cybercrime. For instance, the English Court of Appeal remarked as follows in *R v Governor of Brixton Prison and Another, Ex parte Levin*:

> *"In the case of a virtually instantaneous instruction intended to take effect where the computer is situated it seems to us artificial to regard the insertion of an instruction onto the disk as having been done only at the remote place where the keyboard is situated."*[23]

7.18 Gillard J of the Supreme Court of Victoria (Australia) expressed a similar view in *DPP v Sutcliffe*:

> *"Technology has reached the point where communications can be made around the world in less than a second. The Internet provides a speedy, relatively inexpensive means of communication between persons who have access to a computer and a telephone line. Access is not confined to ownership of a computer and businesses have sprung up offering access to the Internet for a small charge. The law must move with these changes."*[24]

---

21 Alisdair A Gillespie, *Cybercrime: Key Issues and Debates* (Routledge, 2016), at 25.

22 UNODC, Comprehensive Study on Cybercrime (Feb 2013), at 140.

23 *R v Governor of Brixton Prison and Another, Ex parte Levin* [1997] QB 65, at 82E. The House of Lords subsequently upheld the Court of Appeal's decision, see [1997] AC 741.

24 [2001] VSC 43, at paras 62 and 63.

7.19 The appellants (defendants) in *R v Sheppard and Whittle* were convicted of publishing racially inflammatory material, contrary to section 19 of the Public Order Act 1986 in England and Wales. The material was published on the internet. The following submission of counsel, noted in the judgment, illustrates the various possibilities in terms of where the publication should be regarded as published:

> *"Mr Davies submitted that there were essentially three jurisprudential theories as to publications on the internet. The first is that a publication is only cognisable in the jurisdiction where the web server upon which it is hosted is situated — the country of origin theory. The second is that publication on the internet is cognisable in any jurisdiction in which it can be downloaded — the country of destination theory. The third is that while a publication is always cognisable in the jurisdiction where the web server upon which it is hosted is situated, it is also cognisable in a jurisdiction at which the publication is targeted — the directing and targeting theory."*[25]

7.20 It is instructive to also mention *Dow Jones and Co Inc v Gutnick,*[26] notwithstanding that it was a civil case. The facts were that allegedly defamatory material was published in the USA on the web servers of Dow Jones in New Jersey, but downloaded in Australia. The High Court of Australia held that the defamation claim was justiciable in Australia because:

> *"In the case of material on the World Wide Web, it is not available in comprehensible form until downloaded on to the computer of a person who has used a web browser to pull the material from the web server. It is where that person downloads the material that the damage to reputation may be done. Ordinarily then, that will be the place where the tort of defamation is committed."*[27]

7.21 Online material can potentially be downloaded anywhere in the world. If an allegedly defamatory online publication relates to a person having a reputation in many jurisdictions, the courts in each of those jurisdictions which adopt the reasoning of the High Court of Australia may assert jurisdiction in respect of the publication. The *Gutnick* decision "*has inspired much controversy*"[28] with, for instance, one commentator warning of its potential "*chilling effect on Internet speech*",[29] and another noting that the decision

---

25 [2010] 1 Cr App R 26, at 402. The English Court of Appeal was satisfied that it had jurisdiction on the facts, and therefore refrained from exploring further the theories put forward by counsel.

26 (2002) 210 CLR 575.

27 Same as above, at 607 (para 44).

28 Richard Garnett, "*Dow Jones & Company Inc v Gutnick*: An Adequate Response to Transnational Internet Defamation?" (2003) 4(1) Melbourne Journal of International Law 196. Academic discussions on the *Gutnick* case have not died down years after it was decided. See, for example, the article: David Rolph, "Publication, Innocent Dissemination and the Internet after *Dow Jones & Co Inc v Gutnick*" (2010) 33(2) UNSW Law Journal 562.

29 Nathan W Garnett, "*Dow Jones & Co v Gutnick*: Will Australia's Long Jurisdictional Reach Chill Internet Speech World-Wide?" (2004) 13 Pac Rim L & Pol'y J 61, at 62.

"*highlights the divergence between Australian and United States law on Internet jurisdiction*".[30]

7.22 Whatever jurisdictional principles are adopted, the exercise of extra-territorial jurisdiction must be reasonable lest it involves "*an unjustifiable interference in the sovereignty of other states*".[31] In the international effort against cross-border crime, the aim ought to be the avoidance and resolution of both negative jurisdiction conflicts (ie a situation where no country claims jurisdiction over a crime) and positive jurisdiction conflicts (ie when multiple countries claim jurisdiction over a crime).[32] In practice, resolution of the latter conflicts may also prevent double jeopardy issues from arising in the jurisdictions concerned.[33]

Jurisdictional rules under the Budapest Convention

7.23 Article 22 of the Budapest Convention[34] prescribes how member states should address the jurisdictional issues with regard to the offences established under Articles 2 to 11:

> "*1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:*
>
> *a in its territory; or*
>
> *b on board a ship flying the flag of that Party; or*
>
> *c on board an aircraft registered under the laws of that Party; or*
>
> *d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial*

---

30 Brian Fitzgerald, "*Dow Jones & Co Inc v Gutnick*: Negotiating 'American Legal Hegemony' in the Transnational World of Cyberspace" (2003) 27(2) Melbourne University Law Review 590.

31 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015), at 483 and 485.

32 Susan W Brenner and Bert-Jaap Koops, "Approaches to Cybercrime Jurisdiction" (2004) Vol 4, No 1, Journal of High Technology Law, at 40 and 41.

33 The rule against double jeopardy applies to barring the prosecution of a person if he has been previously acquitted or convicted of an offence and is later charged with the same offence. The rule also applies to previous conviction or acquittal in another jurisdiction. As the Court of Final Appeal has confirmed in *Yeung Chun Pong & Others v Secretary for Justice* (2009) 12 HKCFAR 867, there is a discretionary power to stay a prosecution as an abuse of process where "*a person faces a second trial arising from the same or substantially the same set of facts as gave rise to an earlier trial (whether in the same jurisdiction or in a competent court in another jurisdiction)*" (para 21).

34 See para 11 of the Preface and paras 1.6 to 1.10 of Chapter 1 for background information regarding the Budapest Convention.

jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution."

7.24 Paragraphs 1a to 1c of Article 22 manifest the territorial principle, as well as its extension to ships and aircraft, discussed above when considering the general principles on jurisdiction. Paragraph 1d is premised on the active personality principle.

7.25 The first proviso in paragraph 1d ("*if the offence is punishable under criminal law where it was committed*") hints at the double criminality requirement under the extradition law of many countries. As applied to Hong Kong, the requirement means that an act must be criminal both under the law of the place where the act was done, and under Hong Kong law, for Hong Kong courts to assume jurisdiction.[35] In the context of extradition, the House of Lords in *Norris v Government of the United States of America*[36] stated the underlying rationale of the double criminality rule to be that "*a person's liberty is not to be restricted as a consequence of offences not recognised as criminal by the requested state*".[37]

7.26 The Explanatory Report comments on the other parts of Article 22 as follows:

"237. Paragraph 2 allows Parties to enter a reservation to the jurisdiction grounds laid down in paragraph 1, litterae b, c, and d. However, no reservation is permitted with respect to the establishment of territorial jurisdiction under littera a, or with

35 The CJO does not require double criminality in respect of the Group A offences, which are typical and traditional offences of fraud and dishonesty.

36 [2008] 1 AC 920.

37 Same as above, at 954H.

respect to the obligation to establish jurisdiction in cases falling under the principle of 'aut dedere aut judicare' (extradite or prosecute) under paragraph 3, i.e. where that Party has refused to extradite the alleged offender on the basis of his nationality and the offender is present on its territory. Jurisdiction established on the basis of paragraph 3 is necessary to ensure that those Parties that refuse to extradite a national have the legal ability to undertake investigations and proceedings domestically instead, if sought by the Party that requested extradition pursuant to the requirements of 'Extradition', Article 24, paragraph 6 of this Convention.

…

239. In the case of crimes committed by use of computer systems, there will be occasions in which more than one Party has jurisdiction over some or all of the participants in the crime. For example, many virus attacks, frauds and copyright violations committed through use of the Internet target victims located in many States. In order to avoid duplication of effort, unnecessary inconvenience for witnesses, or competition among law enforcement officials of the States concerned, or to otherwise facilitate the efficiency or fairness of the proceedings, the affected Parties are to consult in order to determine the proper venue for prosecution. In some cases, it will be most effective for the States concerned to choose a single venue for prosecution; in others, it may be best for one State to prosecute some participants, while one or more other States pursue others. Either result is permitted under this paragraph. Finally, the obligation to consult is not absolute, but is to take place 'where appropriate.' Thus, for example, if one of the Parties knows that consultation is not necessary (e.g., it has received confirmation that the other Party is not planning to take action), or if a Party is of the view that consultation may impair its investigation or proceeding, it may delay or decline consultation."[38]

7.27 The commentaries in the Explanatory Report quoted above reflect the international practice at large. According to the UNODC's Comprehensive Study on Cybercrime, countries reported "*resolving jurisdictional disputes by relying on formal and informal consultations with other countries in order to avoid double-investigations and jurisdictional conflicts*".[39] Some regional instruments provide guidance on the factors that may be taken account of during legal cooperation among states.[40] This is even though the countries,

[38] Explanatory Report, at paras 237 and 239.

[39] UNODC, Comprehensive Study on Cybercrime (Feb 2013), at 195.

[40] For example, Article 10(4) of the Council Framework Decision 2005/222/JHA on attacks against information systems in the European Union and Article 30(3) of the Arab Convention on Combating Information Technology Offences (21 Dec 2010) set out the following factors:
(i) the state whose security or interests were disrupted by the offence;

in general, do not enact specific legislation for resolving jurisdictional conflicts in cybercrime cases.[41]

7.28 Under the Basic Law,[42] the Central People's Government is responsible for the foreign affairs relating to Hong Kong and Hong Kong is authorised to conduct relevant external affairs on its own in accordance with the Basic Law.[43] Therefore, the negotiation and conclusion of any bilateral agreements between Hong Kong and foreign governments falling outside the scope of relevant external affairs requires the authorisation of the Central People's Government and the assistance of the Office of the Commissioner of the Ministry of Foreign Affairs of the People's Republic of China in Hong Kong ("**OCMFA**").[44] Pending the conclusion of any such agreements, we envisage that if our recommendations are implemented by the Government, the relevant law enforcement agency and the prosecutorial authority will invoke the jurisdictional rules that the new cybercrime legislation prescribes for each of the five cyber-dependent offences,[45] bearing in mind that the rule against double jeopardy applies to a previous conviction or acquittal in another jurisdiction as it does to one in Hong Kong.[46]

Statutory regimes in other jurisdictions

Australia

Section 15.1 of the Criminal Code (Cth)

7.29 In Australia, section 476.3 of the Criminal Code (Cth) prescribes that "*extended geographical jurisdiction—Category A*" as particularised in section 15.1 applies to the offences under Part 10.7, ie the computer offences. Section 15.1 is long and need not be set out here in full. Looking first at section 15.1(1):

> *"If a law of the Commonwealth provides that this section applies to a particular offence, a person does not commit the offence unless:*

(ii) the state in whose territory the offences have been committed;
(iii) the state of which the perpetrator is a national;
(iv) the state in which the perpetrator has been found; and
(v) (in case of similar circumstances) the first state that requests the extradition.

41 See fn 39 above.

42 See Article 13 and Chapter VII.

43 Relevant external affairs include conclusion of agreements with foreign states and region and relevant international organizations in the appropriate fields, including the economic, trade, financial and monetary, shipping, communications, tourism, cultural and sports fields as stipulated in Article 151.

44 The main functions of the OCMFA are stated on its website, available at http://www.fmcoprc.gov.hk/eng/zjgs/zygy/201206/t20120625_7462695.htm (accessed on 3 May 2022).

45 The jurisdictional rules proposed for the five cyber-dependent offences are summarised in Recommendations 11, 12, 13, 14 and 15 respectively. For details of the considerations of the rules, see paras 7.71 to 7.100.

46 See fn 33 above.

(a) the conduct constituting the alleged offence occurs:

(i) wholly or partly in Australia; or

(ii) wholly or partly on board an Australian aircraft or an Australian ship; or

(b) the conduct constituting the alleged offence occurs wholly outside Australia and a result of the conduct occurs:

(i) wholly or partly in Australia; or

(ii) wholly or partly on board an Australian aircraft or an Australian ship; or

(c) the conduct constituting the alleged offence occurs wholly outside Australia and:

(i) at the time of the alleged offence, the person is an Australian citizen; or

(ii) at the time of the alleged offence, the person is a body corporate incorporated by or under a law of the Commonwealth or of a State or Territory; or

(d) all of the following conditions are satisfied:

(i) the alleged offence is an ancillary offence;

(ii) the conduct constituting the alleged offence occurs wholly outside Australia;

(iii) the conduct constituting the primary offence to which the ancillary offence relates, or a result of that conduct, occurs, or is intended by the person to occur, wholly or partly in Australia or wholly or partly on board an Australian aircraft or an Australian ship."

7.30 To summarise section 15.1(1), Australian courts could claim jurisdiction over a primary offence under:

(a) The territorial principle, including its extension to Australian ships and aircraft;

(b) The objective territorial principle, where the conduct constituting an offence occurs outside Australia but a result occurs in Australia;

and

(c) The active personality principle, as applied to both citizens and bodies corporate of Australia.

7.31 Section 15.1(2) then stipulates a defence applicable to primary offences:

> *"If a law of the Commonwealth provides that this section applies to a particular offence, a person does not commit the offence if:*
>
> *(aa) the alleged offence is a primary offence; and*
>
> *(a) the conduct constituting the alleged offence occurs wholly in a foreign country, but not on board an Australian aircraft or an Australian ship; and*
>
> *(b) the person is neither:*
>
> *(i) an Australian citizen; nor*
>
> *(ii) a body corporate incorporated by or under a law of the Commonwealth or of a State or Territory; and*
>
> *(c) there is not in force in:*
>
> *(i) the foreign country where the conduct constituting the alleged offence occurs; or*
>
> *(ii) the part of the foreign country where the conduct constituting the alleged offence occurs;*
>
> *a law of that foreign country, or a law of that part of that foreign country, that creates an offence that corresponds to the first-mentioned offence."*

7.32 Section 15.1(4) is in similar terms to section 15.1(2) but applies to ancillary offences.[47] In brief, section 15.1(2) and (4) together create a defence in respect of conduct occurring outside Australia if the conduct is not criminalised by any law of the jurisdiction where it occurred. The two

---

[47] The Dictionary at the end of the Criminal Code (Cth) defines an ancillary offence as "*(a) an offence against section 11.1, 11.4 or 11.5; or (b) an offence against a law of the Commonwealth, to the extent to which the offence arises out of the operation of section 11.2, 11.2A or 11.3*".
The Judicial College of Victoria stated in its Victorian Criminal Proceedings Manual that the term ancillary offence essentially "*relates to attempts, incitement, conspiracy, or offences committed pursuant to complicity or common purpose or using an innocent agent*" (para 56, s 1.3).

subsections broadly correspond to the double criminality requirement under the Budapest Convention.[48]

Section 16.2 of the Criminal Code (Cth)

7.33 Section 16.2 of the Criminal Code (Cth) ("*When conduct taken to occur partly in Australia*") further provides as follows:

> *"* *Sending things*
>
> *(1)* *[…]*
>
> *Sending electronic communications*
>
> *(2)* *For the purposes of this Part, if a person sends, or causes to be sent, an electronic communication:*
>
> *(a)* *from a point outside Australia to a point in Australia; or*
>
> *(b)* *from a point in Australia to a point outside Australia;*
>
> *that conduct is taken to have occurred partly in Australia.*
>
> *Point*
>
> *(3)* *For the purposes of this section,* ***point*** *includes a mobile or potentially mobile point, whether on land, underground, in the atmosphere, underwater, at sea or anywhere else."*

7.34 If a person located in Australia sends an electronic communication or causes one to be sent, the conduct occurred in Australia. A deeming provision along the lines of section 16.2 would be unnecessary. This suggests that section 16.2 is meant to apply to cases where a person is located outside Australia at the time of his or her conduct in question.

7.35 If one construes section 16.2(2) expansively, its practical effect seems to be as follows:

(a) So long as an electronic communication sent or caused to be sent by a person has "*a point in Australia*" as its origin or destination, the jurisdictional criterion that the person's conduct "*occurred partly in Australia*" is taken as satisfied.

---

[48] See para 7.25 regarding the first proviso in para 1d of Art 22 of the Budapest Convention.

(b) For an inbound electronic communication (ie the scenario in section 16.2(2)(a)), proof of its having entered Australia is unnecessary.

(c) For an outbound electronic communication (ie the scenario in section 16.2(2)(b)), whether it has left Australia or not is irrelevant.

7.36 Another possible construction is that there must be proof of the electronic communication's presence in Australia during some part of the material times, before a person's conduct of sending the electronic communication or causing it to be sent can be regarded as complete. This construction potentially impacts cases of inbound electronic communications more.

Canada

Section 477.1 of the Criminal Code 1985

7.37 In Canada, under section 477.1 of the Criminal Code 1985 ("*Offences outside of Canada*"):

> *"Every person who commits an act or omission that, if it occurred in Canada, would be an offence under a federal law … is deemed to have committed that act or omission in Canada if it is an act or omission*
>
> *(a) in the exclusive economic zone of Canada that*
>
> *(i) is committed by a person who is in the exclusive economic zone of Canada in connection with exploring or exploiting, conserving or managing the natural resources … of the exclusive economic zone of Canada, and*
>
> *(ii) is committed by or in relation to a person who is a Canadian citizen or a permanent resident … ;*
>
> *(b) that is committed in a place in or above the continental shelf of Canada and that is an offence in that place by virtue of section 20 of the Oceans Act;*
>
> *(c) that is committed outside Canada on board or by means of a ship registered or licensed, or for which an identification number has been issued, pursuant to any Act of Parliament;*

(d) that is committed outside Canada in the course of hot pursuit; or

(e) that is committed outside the territory of any state by a Canadian citizen."

7.38 Among the scenarios provided for in paragraphs (a) to (e) above, paragraph (e) – which manifests the active personality principle – appears to be the most relevant to cybercrime cases.

Section 476(d) of the Criminal Code 1985

7.39 For an offence committed in an aircraft in the course of a flight, section 476(d) of the Criminal Code 1985 ("*Special jurisdictions*") deems the offence to have been committed:

"(i) in the territorial division[49] *in which the flight commenced,*

(ii) in any territorial division over which the aircraft passed in the course of the flight, or

(iii) in the territorial division in which the flight ended".

Canadian courts' jurisdiction to adjudicate

7.40 Section 481.2 of the Criminal Code 1985 ("*Offence outside Canada*") prescribes the Canadian courts' jurisdiction to adjudicate an offence which is subject to the extra-territorial jurisdiction of Canadian law:

"Subject to this or any other Act of Parliament, where an act or omission is committed outside Canada and the act or omission is an offence when committed outside Canada under this or any other Act of Parliament, proceedings in respect of the offence may, whether or not the accused is in Canada, be commenced, and an accused may be charged, tried and punished within any territorial division in Canada in the same manner as if the offence had been committed in that territorial division."

7.41 Supplementing the above provisions is the common law principle established in *Libman*, cited above,[50] under which Canadian courts would assume jurisdiction over an offence having a "*real and substantial link*" with Canada.

---

49 S 2 of the Criminal Code 1985 defines "territorial division" as including "*any province, county, union of counties, township, city, town, parish or other judicial division or place to which the context applies*".

50 Para 7.7.

England and Wales

Overview

7.42 The CMA-EW:

(a) creates five offences in sections 1, 2, 3, 3ZA and 3A; and

(b) addresses jurisdictional issues in sections 4 to 9.

7.43 Since each of the five offences under the CMA-EW has different jurisdictional rules, summarising those rules is not straightforward. In broad terms, under section 4 ("*Territorial scope of offences under this Act*"):

(a) There must be a "*significant link with domestic jurisdiction*" for an offence under the following sections to be committed:

(i) section 1 ("Unauthorised access to computer material");

(ii) section 3 ("Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc"); or

(iii) section 3ZA ("Unauthorised acts causing, or creating risk of, serious damage").

For these offences, it is immaterial whether any act or other event the proof of which is required for conviction occurred in the "*home country concerned*",[51] or whether the accused was there.[52]

(b) For an offence under section 2 ("*Unauthorised access with intent to commit or facilitate commission of further offences*"), a "*significant link with domestic jurisdiction*" need not exist in respect of the unauthorised access.[53] Nonetheless, section 2(2)[54] suggests that the intended further offence must be triable under English law.

---

51 S 4(6) of the CMA-EW defines this term as England and Wales in the application of the Act to England and Wales (the Act also applies to Scotland and Northern Ireland).

52 CMA-EW, s 4(1).

53 CMA-EW, s 4(3).

54 "*This section applies to offences—*
(a) for which the sentence is fixed by law; or
(b) *for which a person who has attained the age of twenty-one years (eighteen in relation to England and Wales) and has no previous convictions may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the Magistrates' Courts Act 1980).*"

(c) If a "*significant link with domestic jurisdiction*" exists in relation to an offence under section 3A ("*Making, supplying or obtaining articles for use in offence under section 1, 3 or 3ZA*"), it is immaterial whether the accused was in the "*home country concerned*" at the time of any act or other event the proof of which is required for conviction of the offence.[55]

Meaning of a "significant link with domestic jurisdiction"

7.44 Section 5 of the CMA-EW explains what a "*significant link with domestic jurisdiction*" is. Apparently, this term is intended to be a unifying concept which applies to the offences under sections 1, 3, 3ZA and 3A. However, the exact meaning of a "*significant link with domestic jurisdiction*" and its implications differ depending on the offence in question. Such link can take one of the following forms specified in section 5:

(a) where the accused was a UK national who was in a country outside the UK, and the accused's act constituted an offence under the law of the country in which it occurred[56] – this form is premised on the active personality principle and applies to an offence under section 1, 3, 3ZA or 3A;

(b) where the accused was in the "*home country concerned*" at the time when the accused did the act in question[57] – this form reflects the territorial principle and applies to an offence under section 1, 3 or 3ZA;

(c) where the target computer was in the "*home country concerned*"[58] – this form incorporates the objective territorial principle and applies to an offence under section 1,3 or 3ZA; or

(d) where the unauthorised act caused, or created a significant risk of, "*serious damage of a material kind*" in the "*home country concerned*" [59] – this form embodies the protective principle and only applies to an offence under section 3ZA.

7.45 Given the complexity of the scheme above, it is perhaps unavoidable for sections 4 and 5 to be rather complicated.

Double criminality

7.46 A common feature of the five offences under the CMA-EW is that double criminality is required only in one of the various possible fact patterns

55 CMA-EW, s 4(4A).
56 CMA-EW, s 5(1A).
57 CMA-EW, s 5(2)(a), (3)(a) and (3A)(a).
58 CMA-EW, s 5(2)(b), (3)(b) and (3A)(b).
59 CMA-EW, s 5(3A)(c).

where the courts in England and Wales can assume jurisdiction. In terms of how the double criminality requirement applies, the five offences can be categorised into the following two groups:

(a) For an offence under section 1, 3, 3ZA or 3A, the first possible form of a "*significant link with domestic jurisdiction*" introduced above[60] – which is based on the active personality principle – has double criminality as an element, in that it requires the accused's act to constitute an offence under the law of the country in which the act occurred.

(b) For an offence under section 2, as stated above,[61] a "*significant link with domestic jurisdiction*" need not exist in respect of the unauthorised access. However, section 8 applies if:

(i) commission of an offence under section 1 is alleged; and

(ii) a "*significant link with domestic jurisdiction*" exists.[62]

Section 8(1) includes a double criminality requirement:

> "*A person is guilty of an offence triable by virtue of section 4(4) above only if what he intended to do or facilitate would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place.*"[63]

Mainland China

PRC Criminal Law

7.47 The jurisdictional rules that apply to cybercrimes are set out in Articles 6 to 8 of the PRC Criminal Law:

> *"Article 6 This Law shall be applicable to anyone who commits a crime within the territory and territorial waters and space of the People's Republic of China, except as otherwise specifically provided by law.*

60 Para 7.44(a).
61 Para 7.43(b).
62 CMA-EW, s 4(4).
63 S 8(3) is in similar terms, but applies to an attempted offence as particularised in it:
"*A person is guilty of an offence triable by virtue of section 1(1A) of the Criminal Attempts Act 1981 only if what he had in view would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place.*"

This Law shall also be applicable to anyone who commits a crime on board a ship or aircraft of the People's Republic of China.

If a criminal act or its consequence takes place within the territory or territorial waters or space of the People's Republic of China, the crime shall be deemed to have been committed within the territory and territorial waters and space of the People's Republic of China.

Article 7 *This Law shall be applicable to any citizen of the People's Republic of China who commits a crime prescribed in this Law outside the territory and territorial waters and space of the People's Republic of China; however, if the maximum punishment to be imposed is fixed-term imprisonment of not more than three years as stipulated in this Law, he may be exempted from the investigation for his criminal responsibility.*

This Law shall be applicable to any State functionary or serviceman who commits a crime prescribed in this Law outside the territory and territorial waters and space of the People's Republic of China.

Article 8 *This Law may be applicable to any foreigner who commits a crime outside the territory and territorial waters and space of the People's Republic of China against the State of the People's Republic of China or against any of its citizens, if for that crime this Law prescribes a minimum punishment of fixed-term imprisonment of not less than three years; however, this does not apply to a crime that is not punishable according to the laws of the place where it is committed."*[64]

---

64 The English translation of Articles 6 to 8 is the official version published by the Legislative Affairs Commission of the NPCSC in 1997. Articles 6 to 8 read:

"*第六條 凡在中華人民共和國領域內犯罪的，除法律有特別規定的以外，都適用本法。*

凡在中華人民共和國船舶或者航空器內犯罪的，也適用本法。

犯罪的行為或者結果有一項發生在中華人民共和國領域內的，就認為是在中華人民共和國領域內犯罪。

第七條 中華人民共和國公民在中華人民共和國領域外犯本法規定之罪的，適用本法，但是按本法規定的最高刑為三年以下有期徒刑的，可以不予追究。

中華人民共和國國家工作人員和軍人在中華人民共和國領域外犯本法規定之罪的，適用本法。

第八條 外國人在中華人民共和國領域外對中華人民共和國國家或者公民犯罪，而按本法規定的最低刑為三年以上有期徒刑的，可以適用本法，但是按照犯罪地的法律不受處罰的除外。"

7.48 In summary, the PRC Criminal Law allows courts to exercise jurisdiction over a criminal offence under:

(a) The territorial principle, including the scenario where either the criminal act or its consequence takes place in the PRC, as well as the extension to ships and aircraft of the PRC (pursuant to Article 6);

(b) The active personality principle, as applied to any citizens of the PRC (pursuant to Article 7); and

(c) The passive personality principle and the protective principle, as applied to crimes against citizens of the PRC and the State of the PRC, provided that the offence carries a fixed-term imprisonment of not less than three years and the double criminality requirement is satisfied (pursuant to Article 8).

New Zealand

Section 7 of the New Zealand Act

7.49 Section 7 of the New Zealand Act ("*Place of commission of offence*"), set out below, is comparable to section 3 of the CJO in Hong Kong:

> "*For the purpose of jurisdiction, where any act or omission forming part of any offence, or any event necessary to the completion of any offence, occurs in New Zealand, the offence shall be deemed to be committed in New Zealand, whether the person charged with the offence was in New Zealand or not at the time of the act, omission, or event.*"

7.50 The New Zealand Law Commission commented on section 7 as follows in its Report on Computer Misuse:

> *"… in our view the existing jurisdiction provisions in the Crimes Act 1961 are inadequate to deal with computer misuse activities. First, there are situations where the effects of computer misuse may be felt in New Zealand even though neither the hacker nor the computer were situated in this country. In these situations, it may not always be possible to successfully argue, in terms of s 7 Crimes Act 1961, that 'any act or omission forming part of [the] offence, or any event necessary to the completion of [the] offence' had occurred within New Zealand. Secondly, in many cases it will be impossible to determine where the hacker was at the time the computer misuse activities took place … we recommend that a provision be enacted giving New Zealand courts jurisdiction in*

computer misuse offences wherever they are committed."[65]

7.51 A commentator does not favour the Law Commission's recommendation, [66] which apparently has not been implemented. While a new section 7A ("*Extraterritorial jurisdiction in respect of certain offences with transnational aspects*")[67] was inserted into the New Zealand Act in 2002, it only applies to a number of offences prescribed by the Act which do not include the offences involving computers under sections 249 to 252.

Double criminality

7.52 Section 7 of the New Zealand Act does not incorporate the principle of double criminality. However, section 8 of the Act ("*Jurisdiction in respect of crimes on ships or aircraft beyond New Zealand*") provides for a defence based on that principle. It suffices to quote section 8(1) and (2A) here:

> *"(1) This section applies to any act done or omitted beyond New Zealand by any person—*
>
> *(a) on board any Commonwealth ship; or*
>
> *(b) on board any New Zealand aircraft; or*
>
> *(c) on board any ship or aircraft, if that person arrives in New Zealand on that ship or aircraft in the course or at the end of a journey during which the act was done or omitted; or*
>
> *(d) being a British subject, on board any foreign ship (not being a ship to which he or she belongs) on the high seas, or on board any such ship within the territorial waters of any Commonwealth country; or*
>
> *(e) being a New Zealand citizen or a person ordinarily resident in New Zealand, on board any aircraft:*
>
> *provided that paragraph (c) shall not apply where the act was done or omitted by a person, not being a British subject, on any ship or aircraft for the time being used as a ship or aircraft of any of the armed forces of a country that is not a Commonwealth country.*

---

65 New Zealand Law Commission, *Computer Misuse: Report 54* (May 1999), at 26 and 27.

66 David Harvey, *internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015), at fn 239 under para 6.221 *("... the author considers this [recommendation] overkill … the establishment of universal jurisdiction would set a dangerous precedent in a grey area of law*").

67 S 7A reflects the territorial principle as extended to ships and aircraft, the active personality principle and the passive personality principle.

(2A) If any proceedings are taken by virtue of the jurisdiction conferred by this section, it is a defence to prove that the act or omission would not have been an offence under the law of the country of which the person charged was a national or citizen at the time of the act or omission, if it had occurred in that country."

Singapore

Section 13 of the CMA-SG

7.53 In Singapore, the jurisdictional rules that apply to the CMA-SG are set out in section 13 ("*Territorial scope of offences under this Act*"):

"(1) Subject to subsection (3), the provisions of this Act have effect, in relation to any person, whatever the person's nationality or citizenship, outside as well as within Singapore.

(2) Where an offence under this Act is committed by any person in any place outside Singapore, the person may be dealt with as if the offence had been committed within Singapore.

(3) For the purposes of this section, this Act applies if —

(a) for the offence in question, the accused was in Singapore at the material time;

(b) for the offence in question (being one under section 3, 4, 5, 6, 7 or 8), the computer, program or data was in Singapore at the material time; or

(c) the offence causes, or creates a significant risk of, serious harm in Singapore.

(4) In subsection (3)(c), 'serious harm in Singapore' means —

(a) illness, injury or death of individuals in Singapore;

(b) a disruption of, or a serious diminution of public confidence in, the provision of any essential service in Singapore;

(c) a disruption of, or a serious diminution of public

confidence in, the performance of any duty or function of, or the exercise of any power by, the Government, an Organ of State, a statutory board, or a part of the Government, an Organ of State or a statutory board; or

(d) damage to the national security, defence or foreign relations of Singapore.

…

(5) For the purposes of subsection (3)(c), it is immaterial whether the offence that causes the serious harm in Singapore —

(a) causes such harm directly; or

(b) is the only or main cause of the harm.

(6) In subsection (4)(b), 'essential service' means any of the following services:

(a) services directly related to communications infrastructure, banking and finance, public utilities, public transportation, land transport infrastructure, aviation, shipping, or public key infrastructure;

(b) emergency services such as police, civil defence or health services.

(7) In subsection (4)(c), 'statutory board' means a body corporate or unincorporate established by or under any public Act to perform or discharge a public function."

7.54 The following academic view has been expressed with regard to section 13:

"[Subsections] 1 and 2 give the Act unlimited extraterritorial effect; [subsection] 3, however, may be read as to limit the scope of [subsections] 1 and 2. Only if the perpetrator, the computer, program or data related to the crime was in Singapore at the time of the offence will the act apply. That is, however, still a very broad application. The requirement of the data being in Singapore at the material time is comparable to West Virginia's data passing through the state in transit."[68]

---

[68] Susan W Brenner and Bert-Jaap Koops, "Approaches to Cybercrime Jurisdiction" (2004) Vol 4, No 1, Journal of High Technology Law, at 21.

Serious harm in Singapore

7.55 As shown above, section 13(4) of the CMA-SG prescribes four scenarios where a "*serious harm in Singapore*" exists. The legislation gives the following examples[69] of the scenarios in section 13(4)(b) and (c):

> *"Example 1.— The following are examples of acts that seriously diminish or create a significant risk of seriously diminishing public confidence in the provision of an essential service:*
>
> *(a) publication to the public of the medical records of patients of a hospital in Singapore;*
>
> *(b) providing to the public access to the account numbers of customers of a bank in Singapore.*
>
> *Example 2.— The following are examples of acts that seriously diminish or create a significant risk of seriously diminishing public confidence in the performance of any duty or function of, or the exercise of any power by, the Government, an Organ of State, a statutory board, or a part of the Government, an Organ of State or a statutory board:*
>
> *(a) providing to the public access to confidential documents belonging to a ministry of the Government;*
>
> *(b) publication to the public of the access codes for a computer belonging to a statutory board."*

7.56 The assertion of jurisdiction on the basis that "*the offence causes, or creates a significant risk of, serious harm in Singapore*"[70] reflects the protective principle.

USA

Computer Fraud and Abuse Act (18 USC 1030)

7.57 As mentioned in previous chapters, the key federal legislation on cybercrime in the USA is the Computer Fraud and Abuse Act codified at 18 USC 1030.

---

69 Under s 7A of the Interpretation Act ("*Examples and illustrations*"):
"*Where an Act includes an example or illustration of the operation of a provision —*
(a) the example or illustration shall not be taken to be exhaustive; and
(b) if the example or illustration is inconsistent with the provision, the provision prevails."

70 CMA-SG, s 13(3)(c).

7.58 Many offences created in the Computer Fraud and Abuse Act mean, or include, the perpetration of specified criminal acts against a "*protected computer*". Section 1030(e)(2) defines a "*protected computer*" to mean, among other things, a computer:

> *"(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government;*
>
> *(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States; or*
>
> *(C) that—*
>
> *(i) is part of a voting system; and*
>
> *(ii) (I) is used for the management, support, or administration of a Federal election; or*
>
> *(II) has moved in or otherwise affects interstate or foreign commerce".*

7.59 The word "*foreign*" in section 1030(e)(2)(B), quoted above, was construed as meaning international in *United States v Ivanov*. [71] A commentator makes the following point:

> *"This has the potential to greatly expand federal extraterritorial laws, as any computer which is connected to the internet can be said to be used in or affect an interstate or foreign communication. Further, the computer need not even be located in the United States; so long as it is connected to the internet it could be described as being used in a manner which affects interstate or foreign communication or communication of the United States."*[72]

7.60 While case law has clarified the Computer Fraud and Abuse Act's extra-territorial reach, the statutory definition of a "*protected computer*" does not seem to be the best place to include a reference to extra-territoriality. The other jurisdictions examined in this Chapter have enacted specific

---

71 175 F Supp 2d 367 (D Conn 2001).

72 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015), at 479; similarly Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press, 2007), at para 5.18 ("*This effectively extends the territorial scope to the global arena, since any computer connected to the Internet would potentially be encompassed*").

legislative provisions to address jurisdictional issues.

Objective territorial principle in case law

7.61 Separately, the court in *Ivanov* also affirmed the objective territorial principle:

> *"Here, all of the intended and actual detrimental effects of the substantive offenses Ivanov is charged with in the indictment occurred within the United States … The fact that the [target] computers were accessed by means of a complex process initiated and controlled from a remote location [outside the USA] does not alter the fact that the accessing of the computers, i.e. part of the detrimental effect prohibited by the statute, occurred at the place where the computers were physically located … in Vernon, Connecticut."*

The Sub-committee's views

Preliminary considerations

New legislation should prescribe the jurisdictional rules

7.62 In cases of cybercrime, a perpetrator's act carried out in one physical location can, through the internet, affect numerous victims in multiple physical locations within a short period. A large amount of traffic in cyberspace may be involved. We consider that cybercrime's nature justified extra-territorial application of Hong Kong law.

7.63 To prevent disputes in future legal proceedings, the new legislation should expressly prescribe the jurisdictional rules which apply to the offences created by it. This approach has an educational and deterrence effect because anyone minded to commit those offences in a multi-jurisdictional setting would be able to know the legal position in Hong Kong.

7.64 If, for example, the new legislation should provide that a person outside Hong Kong who intruded a computer in Hong Kong commits an offence under Hong Kong law, the person can be arrested in case he or she travels to Hong Kong. Should the person remain out of the jurisdiction, law enforcement agencies in Hong Kong may request assistance from their counterparts in other jurisdictions as appropriate.

7.65 In the above example, we appreciate the possibility that the person's act constituted no offence at the place where it was done. Leaving aside the potential relevance of the double criminality principle, we take the view that criminalising the act under Hong Kong law is justified if it affects

Hong Kong.[73] In the spirit of our guiding principle,[74] a person's right to carry out an act must be balanced against the need to protect the general public as potential victims of the act, having regard to whether the act's harm is more material and damaging than an intended law's restriction of the person's right to carry out the act.

Case for less restrictive jurisdictional rules

7.66 When law enforcement agencies decide whether to request assistance from other jurisdictions, a practical consideration is how their counterparts in those jurisdictions will respond. We are aware that such request for assistance is often infeasible because large-scale cases of cybercrime are rare in Hong Kong. Even if the aggregate loss in a case is significant, the monetary value at stake for each victim may be low.

7.67 Against such background, we understand that law enforcement agencies and the prosecution will find it useful for the new legislation to incorporate a broad range of jurisdictional rules. The thinking is that, if the offences in Hong Kong do not apply to certain reprehensible conducts because the jurisdictional rules are too restrictive, no charge can be brought at all. This situation is less desirable than if the offences do apply, but the prosecution retains a discretion as to whether a charge should be brought. This would also offer protection to the public which aligns with our guiding principle.

Jurisdictional rules should be tailored to suit each offence

7.68 At the same time, our comparative study shows that (in line with the common law's general adherence to the territorial principle) the international norm is for a jurisdiction to provide for any extra-territorial application of its law within reasonable bounds. For example:

(a) The New Zealand Law Commission's recommendation that the New Zealand courts should have jurisdiction in computer misuse offences wherever committed apparently has not been implemented.[75]

(b) Although section 13(1) and (2) of the CMA-SG seemingly gives the Act unlimited extra-territorial effect, section 13(3) limits the scope of those provisions.[76]

There seems to be no justification for Hong Kong law to regulate a cyber-attack launched in another jurisdiction against a target in a third jurisdiction, in the absence of any factual and causal connection between the cyber-attack and Hong Kong.

---

73 For instance, because the target computer is in Hong Kong.
74 Para 12 of the Preface.
75 Paras 7.50 to 7.51.
76 Paras 7.53 to 7.54.

7.69 In our opinion, it is also apposite for Hong Kong to follow the above international norm. The doctrine of comity suggests that Hong Kong should be able to rationally explain its legal position to other jurisdictions. We are also mindful of the need to take into account different stakeholders' interests, which may vary depending on the offence in question. We therefore discussed the offences proposed in this Consultation Paper in turn, with reference to the following fact patterns:[77]

(a) any "essential element"[78] of the offence occurred in Hong Kong even if other "essential element(s)" occurred elsewhere;[79]

(b) the perpetrator is a "Hong Kong person";[80]

(c) the victim is a "Hong Kong person";

(d) the target computer, program or data is in Hong Kong; and

(e) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong.

7.70 In our deliberation, we bore in mind that deciding whether to suggest the adoption of a fact pattern largely involves a judgement call; there are no absolute answers. Our recommended jurisdictional rules for each proposed offence are set out below.

Illegal access to program or data

Fact patterns (a), (d) and (e)

7.71 It appears uncontroversial to us that fact patterns (a), (d) and (e) should apply to this proposed offence. We discuss fact patterns (b) and (c) below.

---

77 For discussion purpose, the facts mentioned in each fact pattern are assumed to be its only connections with Hong Kong. An actual case may come under more than one fact pattern.

78 In technical terms, any "*act or omission or other event (including any result of one or more acts or omissions) proof of which is required for conviction of the offence*" as stated in s 3(1) of the CJO.

79 This scenario would include cases where the perpetrator, his or her act, and the victim are all in Hong Kong.

80 Legislation in other jurisdictions may refer to nationals or citizens of the jurisdiction in question. In the context of Hong Kong, drawing on existing offences in other areas of law, we recommend that the concept of a "Hong Kong person" should include a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or a company carrying on business in Hong Kong.

Fact pattern (b)

7.72 One argument in favour of applying fact pattern (b)[81] to the proposed offence of illegal access to program or data is that Hong Kong law should deter Hong Kong people from illegally accessing data stored in, say, a cloud server, regardless of its physical location (which is often immaterial in cyberspace). For instance, web-based email systems are popular and typically use cloud technology. Cloud servers have become a main target of criminals, and the importance of cloud storage has the potential to overtake that of ordinary storage in the next few years.

7.73 However, we are conscious that fact pattern (b) covers cases where the perpetrator (albeit a "Hong Kong person"), his or her act, the device used, the data in question and the victim are all outside Hong Kong. The harm is not suffered by any "Hong Kong person". Law enforcement agencies in Hong Kong may have difficulty obtaining evidence and proving the perpetrator's act. On a positive note, law enforcement agencies in the affected jurisdiction will probably take action if a case is serious, with their Hong Kong counterparts assisting where appropriate.

7.74 Balancing all factors, we recommend against applying fact pattern (b) to the proposed offence of illegal access to program or data.

Fact pattern (c)

7.75 Fact pattern (c)[82] gives rise to the issue of who the victim is in the context of this proposed offence. By way of illustration, if a person in Africa hacked a cloud server in Europe which holds data owned by (among others) a "Hong Kong person", should the victim be the cloud server's owner or the data owner, especially given that the hacking may or may not be targeted at any specific user(s) of the cloud server?

7.76 We have come to the view that the concept of victim should be broadly defined. In the scenario described above, both the cloud server's owner and the data owner should be regarded as potential victims. Moreover, consistent with the focus of the proposed offence (illegal access to *program or data*), the emphasis should be on the data to be protected, irrespective of who should be taken as the victim(s) ultimately.

7.77 We have further concluded that applying fact pattern (c) to the proposed offence of illegal access to program or data would be useful. Adopting the considerations in the preceding paragraph, the proposed offence will apply on the basis of fact pattern (c) if either the cloud server's owner or the owner of the data in question is a "Hong Kong person". Such legal position will maximise the scope of protection offered by the proposed offence.

---

81 The perpetrator is a "Hong Kong person".

82 The victim is a "Hong Kong person".

Double criminality

7.78 In the context of this proposed offence, one may argue that requiring double criminality is sensible because from a technological perspective, access to program or data can occur easily. It may be inappropriate for a person to be liable in Hong Kong for this proposed offence on the basis of the person's act done outside Hong Kong, at a place where the act constitutes no crime.

7.79 Yet, a counterargument is that requiring double criminality may defeat the purpose of strengthening protection of the general public. Apart from the need for the prosecution to prove that a defendant's act is criminal under the law of the place where it was done, a relevant factor is that the legal standards in some jurisdictions may not necessarily be on a par with those of Hong Kong. If double criminality is required, one may seek to evade liability by deliberately launching a cyber-attack at a place where it constitutes no crime. Hong Kong may end up being more vulnerable to such cyber-attacks.

7.80 Our comparative study does not indicate any mainstream or uniform practice in other jurisdictions as to whether their cybercrime legislation requires double criminality. In our opinion, the key to resolving the above conundrum is to note that the case for *not* requiring double criminality is stronger *for serious offences*. We have settled on the middle ground that the double criminality requirement should apply to the *summary* offence of illegal access to program or data, but not the *aggravated* offence. Since the latter involves a defendant's intent to carry out further criminal activity after accessing the program or data in question, the defendant can hardly complain that not requiring double criminality is unfair.

7.81 In reaching our views on requiring double criminality for the proposed summary offence of illegal access to program or data, we have generally adopted the spirit of section 7 of the CJO,[83] which embodies the concept of double criminality in Hong Kong law. Furthermore, our view is that where a perpetrator is charged with the proposed summary offence on the basis of his or her act done outside Hong Kong, such act, either alone or together with other such act(s), omission(s) or event(s) the proof of which is required for conviction of the proposed offence, must constitute a crime in the jurisdiction where it was done.

---

[83] S 7 of the CJO imposes a double criminality requirement on convictions for a Group B offence, namely conspiracy to commit a Group A offence or conspiracy to defraud referred to in s 6(1), and attempting to commit or incitement to commit a Group A offence referred to in s 6(2). S 7 reads:

"*(1) A person is guilty of an offence triable by virtue of section 6(1) only if the pursuit of the agreed course of conduct would at some stage involve —*

(a) an act or omission by one or more of the parties; or

(b) the happening of some other event, constituting an offence under the law in force where the act, omission or other event was intended to take place.

(2) A person is guilty of an offence triable by virtue of section 6(2) only if what he had in view would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place."

Recommendation 11

The Sub-committee recommends that, in respect of the proposed offence of illegal access to program or data, Hong Kong courts should have jurisdiction where:

(a) any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence occurred in Hong Kong, even if other such act(s), omission(s) or event(s) occurred elsewhere;

(b) the victim (the target computer's owner, the data's owner, or both) is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or a company carrying on business in Hong Kong;

(c) the target computer, program or data is in Hong Kong; or

(d) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong,

subject to a requirement that, in respect of a perpetrator charged with the summary offence on the basis of his or her act done outside Hong Kong, such act, either alone or together with other such act(s), omission(s) or event(s) the proof of which is required for conviction of the Hong Kong offence, must constitute a crime in the jurisdiction where it was done.

Illegal interception of computer data

Fact patterns (a), (c), (d) and (e)

7.82 For similar reasons as those canvassed above in relation to the first proposed offence (illegal access to program or data), we recommend that fact patterns (a), (c), (d) and (e) should apply to the proposed offence of illegal interception of computer data.

Fact pattern (b)

7.83 Fact pattern (b) is where the perpetrator is a "Hong Kong person". With regard to the proposed offence of illegal interception of computer data, its features tend to justify an emphasis of the new legislation on deterrence, and lend support to the adoption of fact pattern (b):

(a) This proposed offence can be committed without any geographical restriction.

(b) Assuming Recommendation 4(a) [84] will be adopted, a defendant's dishonest or criminal purpose must be established for this proposed offence.

7.84 However, the points against adopting fact pattern (b) which we raised above in connection with the first proposed offence[85] are equally valid here. To recapitulate:

(a) In a case which satisfies fact pattern (b) only, the harm is likely done not to any "Hong Kong person", but rather to people in other jurisdictions. It would be better for law enforcement agencies in those other jurisdictions to prosecute the perpetrator.

(b) Prosecution in Hong Kong may be impractical, especially if the factual circumstances are complicated, because evidence will have to be obtained from other jurisdictions.

7.85 Moreover, while one may argue that Hong Kong courts should have jurisdiction over a case of fact pattern (b) because any intercepted data may be misused in Hong Kong subsequently, a counterargument is that Hong Kong courts should assume jurisdiction only upon actual misuse of such data.

7.86 Taking the above considerations into account, we recommend against applying fact pattern (b) to the proposed offence of illegal interception of computer data.

Double criminality

7.87 Although interception of data happens naturally in cyberspace due to the technology involved, the proposed offence of illegal interception of computer data only targets those who act with a dishonest or criminal purpose. Therefore, this proposed offence is more analogous with the aggravated offence of illegal access to program or data[86] than the summary offence.[87]

---

84 Chapter 3.
85 Para 7.73.
86 In respect of which we recommended not to require double criminality (para 7.80).
87 In respect of which we recommended that double criminality should be required (para 7.80).

7.88 From the perspective of consistency, we opine that double criminality should not be required of this proposed offence. By our recommendation, we seek to avoid criminals exploiting such requirement by deliberately carrying out their act at a place outside Hong Kong where the act constitutes no crime because, for example, the legal regime there is not sufficiently comprehensive.

Recommendation 12

The Sub-committee recommends that, in respect of the proposed offence of illegal interception of computer data, Hong Kong courts should have jurisdiction where:

(a) any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence occurred in Hong Kong, even if other such act(s), omission(s) or event(s) occurred elsewhere;

(b) the victim is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or a company carrying on business in Hong Kong;

(c) the target computer, program or data is in Hong Kong; or

(d) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong.

Illegal interference of computer data

Fact patterns (a), (c), (d) and (e)

7.89 Again, we believe that applying fact patterns (a), (c), (d) and (e) to the proposed offence of illegal interference of computer data should be uncontroversial. We recommend accordingly and suggest that fact pattern (d),[88] when applied to this proposed offence, should focus on the location of the target program or data (as opposed to the computer storing it).

[88] The target computer, program or data is in Hong Kong.

Fact pattern (b)

7.90 Only fact pattern (b)[89] remains to be addressed. Readers will recall that we have recommended against applying it to the first two proposed offences. After consideration, we suggest that fact pattern (b) should likewise not apply to the proposed offence of illegal interference of computer data.

Double criminality

7.91 We observe that not applying the double criminality requirement to this proposed offence will be consistent with our recommendations regarding the first two proposed offences. The result is that a person can be liable under Hong Kong law for interfering with data in another jurisdiction, irrespective of whether or not the interference constitutes a crime there.

Recommendation 13

The Sub-committee recommends that, in respect of the proposed offence (including its basic and aggravated forms) of illegal interference of computer data, Hong Kong courts should have jurisdiction where:

(a) any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence occurred in Hong Kong, even if other such act(s), omission(s) or event(s) occurred elsewhere;

(b) the victim is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or a company carrying on business in Hong Kong;

(c) the target program or data is in Hong Kong; or

(d) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong.

[89] The perpetrator is a "Hong Kong person".

Illegal interference of computer system

The fact patterns

7.92 We can be relatively brief here given our recommendation to treat this proposed offence and the preceding one in the same way.[90] The close relationship between the two proposed offences suggests that they should have the same jurisdictional reach except that fact pattern (d),[91] when applied to the proposed offence of illegal interference of *computer system*, should focus on the location of the target computer (as opposed to any program or data).

Double criminality

7.93 We also recommend that double criminality should not be required of this proposed offence.

Recommendation 14

The Sub-committee recommends that, in respect of the proposed offence (including its basic and aggravated forms) of illegal interference of computer system, Hong Kong courts should have jurisdiction where:

(a) any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence occurred in Hong Kong, even if other such act(s), omission(s) or event(s) occurred elsewhere;

(b) the victim is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or a company carrying on business in Hong Kong;

(c) the target computer is in Hong Kong; or

(d) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong.

90 Recommendation 7(a) and (b) in Chapter 5.
91 The target computer, program or data is in Hong Kong.

Making available or possessing a device or data for committing a crime

Same jurisdictional rules for both the basic and aggravated forms of the proposed offence

7.94 We have recommended that this proposed offence should include a basic form and an aggravated form, based on whether a defendant intends the device or data in question to be used by any person to commit an offence.[92]

7.95 Nonetheless, in our opinion, even the basic offence should be regarded as serious because it applies to a device or data made or adapted to commit an offence. While the severity of the two forms of the proposed offence varies, the gap is not so wide as to justify the two forms having different jurisdictional rules. We suggest that the same jurisdictional rules should apply to both forms.

Fact patterns (c) and (d)

7.96 A case of this proposed offence may not involve any victim or any target computer, program or data, which fact patterns (c)[93] and (d)[94] presuppose respectively. We thus take these fact patterns as inapposite for this proposed offence.

Fact patterns (a), (b) and (e)

7.97 When considering the other fact patterns, we remind ourselves of the two limbs under this proposed offence:

(a) As regards the limb of *possessing* a device or data, one may say the concept of possession would follow an individual, who has a physical location. Yet, to state that the device or data is possessed at such location may not reflect reality if the device or data is stored in, say, a cloud server.

(b) As regards the limb of *making available* a device or data, when someone physically located outside Hong Kong uploads a piece of malware onto the internet, theoretically it can be available to anyone anywhere in the world with internet access. Many devices and data subject to this proposed offence would most likely be available on the dark web. The physical locations of the vendors and purchasers cannot be traced.

---

92 Recommendation 9(a) and (d) in Chapter 6.
93 The victim is a "Hong Kong person".
94 The target computer, program or data is in Hong Kong.

7.98 In the premises, and recognising the unique nature of this proposed offence compared with that of the other four,[95] we recommend that fact patterns (a),[96] (b)[97] and (e)[98] should apply to this proposed offence.

Double criminality

7.99 Save for the summary offence of illegal access to program or data, we have recommended that double criminality should not be required of the first four proposed offences.

7.100 We consider that the same reasoning and hence recommendation apply to the proposed offence of making available or possessing a device or data for committing a crime, despite its uniqueness. We note that our recommendation promotes consistency among the proposed offences.

Recommendation 15

The Sub-committee recommends that, in respect of the proposed offence of making available or possessing a device or data for committing a crime, Hong Kong courts should have jurisdiction where:

(a) any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence occurred in Hong Kong, even if other such act(s), omission(s) or event(s) occurred elsewhere, eg a person physically in Hong Kong making available on the dark web, a device or data for committing an offence;

(b) the perpetrator is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or a company carrying on business in Hong Kong; or

(c) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong.

---

95 While most offences created by the CMA-EW require a "*significant link with domestic jurisdiction*", this seems to be optional for the offence under s 3A ("*Making, supplying or obtaining articles for use in offence under section 1, 3 or 3ZA*"). See para 7.43.

96 Any "essential element" of the offence occurred in Hong Kong even if other "essential element(s)" occurred elsewhere.

97 The perpetrator is a "Hong Kong person".

98 The perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority.

Chapter 8

Sentencing

Introduction

8.1 In earlier chapters, we have proposed five cyber-dependent offences, and recommended the jurisdictional rules that should apply to each of them. This Chapter:

(a) sets out pertinent statements of principle, sentiment and other dicta from Hong Kong authorities which indicate the courts' views towards cybercrime;

(b) introduces readers to the Appendix to this Consultation Paper, which summarises the maximum sentences for the relevant offences under the current laws in Hong Kong and other jurisdictions; and

(c) states our recommendations on the appropriate maximum sentences for the proposed offences.

Views of Hong Kong court towards cybercrime

8.2 *HKSAR v Chan Chi Kong*[1] involved the first prosecution for "*misuse of a computer*" under sections 59(1A) and 60(1) of the Crimes Ordinance (Cap 200).[2] The Court of Appeal stated as follows:

> *"The HKSAR is an internationally recognised commercial and financial centre, where modern computer technology is relied upon in all spheres of commerce and banking. It is the duty of the courts to ensure that they impose such sentences in cases which are likely to damage or have the potential to damage the trust and confidence which others place in this city, as will deter others similarly inclined from committing such offences … we stress that these offences are serious and call for sentences befitting the circumstances of the case."*[3]

---

1 [1997] 3 HKC 702, CACC 245/1997 (date of judgment: 25 Sept 1997).

2 According to the submission of counsel for the defendant, noted in the judgment at 706H.

3 See fn 1 above, at 709C-E.

8.3 The defendant in *HKSAR v Tsun Shui Lun*[4] was convicted under S161. In dismissing his appeal against conviction (though allowing his appeal against sentence), Chan CJHC said the following:

> *"Computer has become a fact of life in modern society. Daily activities are now so dependent on the computer that it is difficult to imagine what would happen without it. Business transactions are conducted through computers. Confidential and even secret information is stored in computers. Many lives are saved in hospital through computerised operations. If computers are misused or abused, or if access to computers with a criminal or dishonest intent or purpose is tolerated, it may lead to serious consequences. These must be avoided …*
>
> *There is a very wide range of criminal and dishonest activities which fall within the ambit of s.161. In this day and age, very serious crimes or frauds can be committed by gaining access to other people's computers and uplifting information contained therein. Examples include meddling bank records, transferring large sums of money from one account to another, and stealing secret programmes and data such as customers lists and business records. Such activities can be very serious and obtaining access into computers with such intention or for such purposes is no less grave.*
>
> *The maximum penalty under s.161 is 5-year imprisonment … In my view, if access is gained into a computer in order to commit a crime or fraud or where the access is intended to cause huge gain or serious loss, whether financial, proprietary or otherwise, to another person, an immediate custodial sentence should be imposed. Where access is gained not for any personal benefit but for the purpose of vandalizing another person's system or causing great embarrassment and distress to him, the possibility of imprisonment cannot be ruled out. It is however not appropriate for me in this special case to set any sentencing guideline for a s.161 offence."*[5]

8.4 The Court of Appeal in *HKSAR v Tam Hei Lun & Ors*[6] likewise declined to give sentencing guidelines in respect of S161 because at that time (a) there had been less than ten prosecutions under S161, and (b) it was most unlikely that the full range of crimes which would fall within it would be known or appreciated.[7] Nonetheless, the court observed that:

> *"There are undoubtedly many considerations which a court would have to take into account in arriving at an appropriate sentence in*

---

4 [1999] 3 HKLRD 215, HCMA 723/1998 (date of judgment: 15 Jan 1999).
5 Same as above, at 228H-229F.
6 [2000] 3 HKC 745, HCMA 385/2000 (date of judgment: 9 Oct 2000).
7 Same as above, at 749C.

respect of offences under ss 60 and 161 of the Crimes Ordinance. First and foremost would be the loss and damage which was caused to the victims. The gravity of the offence to the victim would be another matter. The purpose of the access would also be relevant as would be any gain financial or otherwise to the person perpetrating the access.

In the present circumstances we consider it sufficient to say that where access has been obtained to someone else's computer whether for gain or for some other reason, the act can in many respects be likened to burglary. What has happened is that there has been access to the computer of another, much in the same way as a person who enters a house or an office and goes through a drawer or filing cabinet. Some of the aspects of the offence of burglary are undoubtedly not present in relation to unauthorised computer access. The analogy is by no means perfect. Whilst indicating that we feel it inappropriate to lay down guidelines now we would indicate that unless there are most unusual circumstances a non-custodial sentence would be inappropriate for offences against s 161."[8]

8.5 The defendant in *HKSAR v Ko Kam Fai*[9] pleaded guilty to charges of criminal intimidation (involving two victims) and those of criminal damage (of their computers and email accounts) contrary to sections 24 and 60(1) of the Crimes Ordinance (Cap 200) respectively. The trial judge equated these offences with offences brought under S161, and passed a deterrent sentence – an immediate custodial sentence – in light of the dicta in *Tam Hei Lun* quoted in the preceding paragraph. The Court of Appeal commended such approach.[10]

8.6 The dicta in *Tam Hei Lun* also led V Bokhary J to rule as follows in *HKSAR v Choy Yau Pun*:[11]

"… even where the circumstances of the offender make him a viable candidate for a community service order, there must be most unusual circumstances before such an order or any other form of non-custodial sentence can be regarded as an appropriate alternative to a custodial sentence for an offence against s.161 …

… the fact is that he offended against s. 161 and, what is more, did so in circumstances which betrayed the trust of a customer who had delivered her computer to him for servicing. Where, as in the present case, the function of the proper sentence includes

---

8 Same as above, at 749F-750A.
9 [2001] 3 HKC 181, CACC 83/2001 (date of judgment: 20 Jun 2001).
10 Same as above, at 183H and 185B.
11 [2002] 3 HKLRD 156, HCMA 450/2002 (date of judgment: 24 Jun 2002).

deterring not only conduct contrary to s.161 in the ordinary way, but also deterring betrayal of trust, it is even more difficult than usual to regard a community service order as appropriate."[12]

8.7 In the same vein, the Court of Final Appeal remarked in *Li Man Wai v Secretary for Justice*[13] that an offence under S161 could be serious in nature:

> *"The type of offence punishable under s.161 of the Crimes Ordinance is no doubt very serious — it could be viewed as a kind of theft, very often with serious consequences but without the victim ever knowing what has happened and why. With the widespread use of computers and the advancement of technology, this valuable equipment has become part of our daily life. It is therefore all the more important to protect the integrity of computers, particularly the integrity of the IRD [the Inland Revenue Department's] computer system. But the law as it now stands does not punish all kinds of unauthorized access to computers, it only prohibits the unauthorized and dishonest extraction and use of information. And it is essentially a question of fact for the jury to decide whether there is dishonesty in each case."*[14]

8.8 In *Liu Wai Shun v HKSAR*,[15] the defendant (a software developer) was dismissed by his employer. In retaliation, the defendant deleted some computer files to prevent the employer, who owned the relevant software, from using it. The defendant was convicted and fined under sections 60(1) and 161(1)(a) of the Crimes Ordinance (Cap 200). His appeal to the Court of First Instance was dismissed. The Appeal Committee of the Court of Final Appeal refused his application for leave to appeal, noting as follows:

> *"We would make one comment regarding sentence. Deliberate damage to computer software and data may of course result in very substantial economic and other harm to organisations using that software and data. The applicant may count himself lucky that the damage inflicted here was remediable largely because of the preventive measures taken by his former employer. The seriousness of the damage inflicted in such a case should properly be reflected in the sentences handed down. If more serious damage had ensued, a fine would not have been a sufficient sentence. We were told that the Court of Appeal has, quite properly in our view, indicated that*

---

12 Same as above, at 159H-I and 160D-E.
13 (2003) 6 HKCFAR 466, FACC 6/2003 (date of judgment: 6 Nov 2003).
14 Same as above, at 474H-J.
15 FAMC 30/2004 (date of judgment: 27 Sept 2004).

such cases should ordinarily attract a custodial sentence."[16]

8.9 The following comments of the sentencing judge in *HKSAR v Luk Wa*[17] are consistent with the above authorities:

> *"The use of computer and Internet are an important part of modern daily life. Virtually all walks of life require the use of computers and Internet for their functioning and smooth running. It is vital that the integrity in the use of computers and Internet should not be allowed to be compromised. That is the reason why the courts have always taken the offences relating to the dishonest use of computer very seriously."*[18]

8.10 At the same time, as another sentencing judge pointed out in *HKSAR v Leung Lai Chung*,[19] no two cases are the same with regard to sentencing. In particular, "*[o]ffences proceeded by way of indictment differ from offences proceeded by way of summary trial*".[20]

Current laws in Hong Kong and other jurisdictions

8.11 The Appendix to this Consultation Paper seeks to offer a bird's-eye view of the maximum sentences for the cybercrime offences in Hong Kong and other jurisdictions, with section numbers (in boldface) and headings (in italics). Details of the offences have been discussed in the previous chapters. The Appendix does not refer to the Model Law because it does not recommend any maximum sentences for the offences proposed in it.

The Sub-committee's views

The relatively serious proposed offences

Uniform maximum sentences preferable

8.12 We recommended in Chapter 7 that, with the exception of the proposed summary offence of illegal access to program or data, double criminality should not be required of the offences proposed in this Consultation Paper. Such recommendation reflects our view that the proposed non-summary offences can cause significant harm. After discussion, we favour setting uniform maximum sentences for:

---

16 Same as above, at para 7 (Ribeiro PJ).
17 DCCC 17/2011 (date of judgment: 18 Feb 2011).
18 Same as above, at para 29 (HH Judge Joseph Yau).
19 DCCC 416/2009 (date of judgment: 1 Feb 2010).
20 Same as above, at para 17 (HH Judge Mary Yuen).

(a) the proposed aggravated offence of illegal access to program or data (Chapter 2);

(b) the proposed offence of illegal interception of computer data (Chapter 3);

(c) the proposed basic offences of illegal interference of computer data and illegal interference of computer system (Chapters 4 and 5); and

(d) the proposed aggravated offence of making available or possessing a device or data for committing a crime (Chapter 6).

Summary conviction and conviction on indictment

8.13 We also recognise that the severity of the harm caused by cybercrime has a wide range. It may be so minor that no material harm is caused, or as serious as the total breakdown of an important system (eg a power supply system or a railway system). Since the consequences can be so diverse, we recommend that each of the proposed offences in (a), (b), (c) and (d) of the preceding paragraph should have two maximum sentences, one applicable to summary convictions and the other to convictions on indictment.

Maximum sentence on conviction on indictment

8.14 We deliberated having regard to the following considerations:

(a) The maximum sentences that the Magistrates' Courts and the District Court can impose are imprisonment for three and seven years respectively.[21] The High Court can impose heavier sentences.

(b) The proposed aggravated offence of illegal access to program or data is similar in nature to the existing offence under S161,[22] which has a maximum sentence of imprisonment for five years. This does not seem to be commensurate with the degree of criminality if the further act intended by a perpetrator of the proposed aggravated offence is as heinous as, say, causing the

---

21 See the Judiciary, Guide to Court Services – Magistrates' Courts:
"*The normal maximum sentence is 2 years' imprisonment and a fine of $100,000. However the court may impose sentences of up to 3 years' imprisonment where there are two or more indictable offences being dealt with at the same time. Indeed under some Ordinances a single offence may carry 3 years' imprisonment and a fine of $5 million.*"
Also see the Judiciary, Guide to Court Services – District Court:
"*The District Court may try all serious criminal cases except murder, manslaughter and rape. The maximum term of imprisonment it can impose is 7 years.*"

22 "*Access to computer with criminal or dishonest intent*" (see para 2.6).

breakdown of Hong Kong's public transport system.[23]

(c) Section 27(b) of the Telecommunications Ordinance (Cap 106)[24] only creates a *summary* offence with regard to the damage or removal of, or interference with, a telecommunications installation with intent to intercept or discover the contents of a message. In addition, it is not a bespoke provision against interception of *computer data*.[25] Therefore, its maximum sentence (a fine at level 4[26] and imprisonment for two years) has limited value as a reference.

(d) The proposed offences of illegal interference of computer data and illegal interference of computer system deal with conducts now addressed by section 60 of the Crimes Ordinance (Cap 200),[27] under which an offender is liable to imprisonment for 10 years ordinarily, or for life imprisonment if a case involves danger to life.[28]

(e) The proposed aggravated offence of making available or possessing a device or data for committing a crime is analogous to the offence under section 62 of the Crimes Ordinance (Cap 200),[29] which is punishable by imprisonment for 10 years.[30]

(f) In terms of where the proposed offences stated at paragraph 8.12(a), (b), (c) and (d) are located in the spectrum of criminality of comparable offences, the maximum terms of imprisonment for the following representative types of crimes in the Theft Ordinance (Cap 210) can be taken as references:

(i) 10 years for theft;[31]

(ii) 14 years for fraud;[32]

(iii) 14 years for blackmail;[33]

---

23 We acknowledge that the facts in most cases are probably less serious and do not require the court passing the maximum sentence. Between 2015 and Sept 2020, convicted offenders of S161 had been sentenced to probation order, community service order, fine, or imprisonment ranging from 10 days to 1 year and 8 months.

24 "*Damaging telecommunications installation with intent*" (see para 3.12).

25 Paras 3.14 to 3.16.

26 Currently $25,000 under Schedule 8 to the Criminal Procedure Ordinance (Cap 221).

27 "*Destroying or damaging property*" (see paras 4.4 and 5.7).

28 Crimes Ordinance (Cap 200), s 63.

29 "*Possessing anything with intent to destroy or damage property*" (see para 6.6).

30 Crimes Ordinance (Cap 200), s 63(2).

31 Theft Ordinance (Cap 210), s 9.

32 Same as above, s 16A(1).

33 Same as above, s 23(3).

(iv) 14 years for burglary;[34]

(v) life imprisonment for aggravated burglary (ie burglary committed by a person with any firearm or imitation firearm, any weapon of offence, or any explosive);[35] and

(vi) life imprisonment for robbery.[36]

(g) Our comparative study suggests that the maximum sentences in other jurisdictions differ because they reflect different definitions of the relevant offences. The sentencing principles in other jurisdictions may also be different from those in Hong Kong.

8.15 Inevitably, whatever the number of years of imprisonment we propose, there would be a degree of arbitrariness. We recommend a maximum sentence of imprisonment for 14 years for the proposed offences stated at paragraph 8.12(a), (b), (c) and (d).[37] We consider that our recommendation will have the necessary deterrent effect to combat cybercrime, and is not too out of line with the maximum sentences for (a) the crimes in the Theft Ordinance (Cap 210) mentioned above[38] as well as (b) relevant offences in other jurisdictions.[39]

Maximum sentence on summary conviction

8.16 In our opinion, a maximum sentence of imprisonment for two years on summary conviction would be proportionate to the above recommendation with regard to cases of conviction on indictment. We recommend accordingly.

The proposed summary offence of illegal access to program or data

8.17 This proposed offence is, to an extent, comparable to the offence under S27A[40] in terms of their nature. However, S27A has rarely been invoked and its maximum sentence (a fine at level 4)[41] appears rather light to

---

34 Same as above, s 11(4).
35 Same as above, s 12(3).
36 Same as above, s 10(2).
37 Apart from the statute creating an offence in question, one may have to refer to other legislative provisions in order to understand the full range of sentencing options available. For instance, even if the offence-creating statute does not refer to any fine or compensation, a magistrate or a court has the jurisdiction to:
(a) impose a fine under s 92 of the Magistrates Ordinance (Cap 227) or s 113A of the Criminal Procedure Ordinance (Cap 221); and
(b) order the payment of compensation under s 98 of the Magistrates Ordinance (Cap 227) or s 73 of the Criminal Procedure Ordinance (Cap 221).
38 Para 8.14(f).
39 The Appendix to this Consultation Paper.
40 "*Unauthorized access to computer by telecommunications*" (see para 2.11).
41 Currently $25,000 under Schedule 8 to the Criminal Procedure Ordinance (Cap 221).

us for adoption by our proposed offence. Although the latter applies to unauthorised access *per se*, with the perpetrator only "taking a look" at the target computer's program or data without causing any interference, we have come to the view that there should be the possibility of imprisonment even in summary cases.

8.18 We recommend a maximum sentence of imprisonment for two years for the proposed summary offence of illegal access to program or data, which will therefore be triable in the Magistrates' Courts.

The proposed aggravated offences of illegal interference of computer data and computer system

8.19 As discussed in Chapters 4 and 5,[42] we:

(a) favour retention of the aggravated offence under section 60(2) of the Crimes Ordinance (Cap 200); and

(b) recommend that the proposed provisions regarding illegal interference of computer data and that of computer system should be phrased in the same way.

8.20 To maintain consistency with the offence of criminal damage, we suggest adopting the maximum sentence now prescribed by section 63(1) of the Crimes Ordinance (Cap 200), ie imprisonment for life, for the proposed aggravated offences of illegal interference of computer data and that of computer system.

The proposed basic offence of making available or possessing a device or data for committing a crime

8.21 As recommended in Chapter 6, a crucial distinction between this proposed offence and the related aggravated offence is whether a defendant intends the device or data in question to be used to commit an offence.[43] The two forms would inform people of the different sentences applicable to the offences of knowingly making available or possessing a device or data for committing a crime with and without intent for the same to be so used respectively.

8.22 When we considered what maximum sentence should apply to the proposed basic offence, two options were raised:

---

42 Paras 4.96 to 4.98 and 5.61 to 5.63.

43 Recommendation 9(d)(ii).

(a) The first was imprisonment for five years, by reference to the existing offence under S161.

(b) The second was imprisonment for seven years, which would lay halfway when compared with the recommended maximum sentence for the related aggravated offence.[44]

8.23 We ultimately preferred the second option, given our view that even the basic offence should be regarded as a serious one because it applies to a device or data made or adapted to commit an offence.[45]

Recommendation 16

The Sub-committee recommends that:

(a) In respect of the proposed offence of illegal access to program or data, an offender should be liable to the following maximum sentences:

(i) for the summary offence, imprisonment for two years; or

(ii) for the aggravated offence, imprisonment for 14 years on conviction on indictment.

(b) In respect of the proposed offence of illegal interception of computer data, an offender should be liable to imprisonment for two years on summary conviction and 14 years on conviction on indictment.

(c) In respect of each of the proposed offences of illegal interference of computer data and illegal interference of computer system, an offender should be liable to the following maximum sentences:

(i) for the basic offence, imprisonment for two years on summary conviction and 14 years on conviction on indictment; or

(ii) for the aggravated offence, imprisonment for life.

44 Para 8.15.
45 Para 7.95.

(d) In respect of the proposed offence of making available or possessing a device or data for committing a crime, an offender should be liable to the following maximum sentences:

(i) for the basic offence, imprisonment for two years on summary conviction and seven years on conviction on indictment; or

(ii) for the aggravated offence, imprisonment for 14 years on conviction on indictment.

Chapter 9

Consolidated recommendations and consultation questions

Introduction

9.1 This Chapter summarises our recommendations and consultation questions, which are grouped under the five offences proposed in this Consultation Paper. We hope that this format better assists readers in considering the recommendations and consultation questions holistically than if they were laid out in their order of appearance in the previous chapters.

9.2 To facilitate references to the pertinent discussions in this Consultation Paper, the relevant Recommendations are identified under each proposed offence.

Illegal access to program or data

– Recommendations 1, 2, 11 and 16(a)

Recommendations

9.3 Subject to a statutory defence of reasonable excuse, unauthorised access to program or data should be a summary offence under a new piece of bespoke legislation on cybercrime. *[Recommendation 1(a)]*[1]

9.4 Unauthorised access to program or data with intent to carry out further criminal activity should constitute an aggravated form of the offence attracting a higher sentence under the new legislation. *[Recommendation 1(b)]*[2]

9.5 Hong Kong courts should have jurisdiction where:

(a) any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence occurred in Hong Kong, even if other such act(s), omission(s) or event(s) occurred elsewhere;

---

1 Paras 2.89 to 2.106.

2 Paras 2.107 to 2.108.

(b) the victim (the target computer's owner, the data's owner, or both) is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or a company carrying on business in Hong Kong;

(c) the target computer, program or data is in Hong Kong; or

(d) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong,

subject to a requirement that, in respect of a perpetrator charged with the summary offence on the basis of his or her act done outside Hong Kong, such act, either alone or together with other such act(s), omission(s) or event(s) the proof of which is required for conviction of the Hong Kong offence, must constitute a crime in the jurisdiction where it was done. *[Recommendation 11]*[3]

9.6 An offender should be liable to the following maximum sentences:

(a) for the summary offence, imprisonment for two years; or

(b) for the aggravated offence, imprisonment for 14 years on conviction on indictment. *[Recommendation 16(a)]*[4]

9.7 The proposed provisions of the new legislation should be modelled on sections 1, 2 and 17 of the Computer Misuse Act 1990 in England and Wales. *[Recommendation 1(c)]*[5]

Consultation questions

9.8 Should there be any specific defence or exemption for unauthorised access?

9.9 If the answer is yes for cybersecurity purposes, in what terms? For example:

(a) should the defence or exemption apply only to a person who is accredited by a recognised professional or accreditation body?

[3] Paras 7.71 to 7.81.
[4] Paras 8.12 to 8.18.
[5] Para 2.109.

(b) If the answer to sub-paragraph (a) is yes, how should the accreditation regime work, eg what are the criteria for such accreditation? Should accredited persons be subject to any continuing education requirements? Should Hong Kong establish an accreditation body (say under the new cybercrime legislation or otherwise created administratively) that maintains a list of cybersecurity professionals so that, for instance, accredited persons who fail to satisfy the continuing education requirements may be removed from the list or not be allowed to renew their accreditation? Who outside the accreditation body (if any) should also have access to the list?

(c) Alternatively, if an accreditation regime is not preferred, should the new bespoke cybercrime legislation prescribe the requirements for putative cybersecurity professionals to invoke the proposed defence or exemption for cybersecurity purposes? If so, what should these requirements be?

9.10 Should the defence or exemption apply to non-security professionals (please see the examples in Recommendation 8(b)) [6] ? *[Recommendation 2]*[7]

Illegal interception of computer data

– Recommendations 4, 5, 12 and 16(b)

Recommendations

9.11 Unauthorised interception, disclosure or use of computer data carried out for a dishonest or criminal purpose should be an offence under the new legislation. *[Recommendation 4(a)]*[8]

9.12 The proposed offence should:

(a) protect communication in general, rather than just private communication;

(b) apply to data generally, whether it be metadata or not; and

(c) apply to interception of data *en route* from the sender to the intended recipient, ie both data in transit and data momentarily at rest during transmission. *[Recommendation 4(b)]*[9]

---

6 Para 9.30.
7 Paras 2.110 to 2.120.
8 Paras 3.92 to 3.99.
9 Paras 3.100 to 3.110.

9.13 Hong Kong courts should have jurisdiction where:

(a) any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence occurred in Hong Kong, even if other such act(s), omission(s) or event(s) occurred elsewhere;

(b) the victim is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or a company carrying on business in Hong Kong;

(c) the target computer, program or data is in Hong Kong; or

(d) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong. *[Recommendation 12]*[10]

9.14 An offender should be liable to imprisonment for two years on summary conviction and 14 years on conviction on indictment. *[Recommendation 16(b)]*[11]

9.15 The proposed provision should, subject to paragraphs 9.11 and 9.12 above, be modelled on section 8 of the Model Law on Computer and Computer Related Crime, including the *mens rea* (ie to intercept "intentionally"). *[Recommendation 4(c)]*[12]

Consultation questions

9.16 Should there be a defence or exemption for professions who have to intercept and use the data intercepted in the course of their ordinary and legitimate business? If the answer is yes, what types of professions should be covered by the defence or exemption, and in what terms (eg should there be any restrictions on the use of the intercepted data)?

9.17 Should a genuine business (a coffee shop, a hotel, a shopping mall, an employer, etc) which provides its customers or employees with a Wi-Fi hotspot or a computer for use be allowed to intercept and use the data being transmitted without incurring any criminal liability? If the answer is yes, what types of businesses should be covered, and in what terms (eg should there be any restrictions on the use of the intercepted data)? [*Recommendation 5]*[13]

10 Paras 7.82 to 7.88.
11 Paras 8.12 to 8.16.
12 Paras 3.111 to 3.112.
13 Paras 3.113 to 3.122.

Illegal interference of computer data

– Recommendations 6, 13 and 16(c)

Recommendations

9.18 Intentional interference (damaging, deletion, deterioration, alteration or suppression) of computer data without lawful authority or reasonable excuse should be an offence under the new legislation.

9.19 The new legislation should adopt the following features under the Crimes Ordinance (Cap 200):

(a) the *actus reus* under section 59(1A)(a), (b) and (c);[14]

(b) the *mens rea* under section 60(1) (which requires intent or recklessness, but not malice);

(c) the two lawful excuses under section 64(2), while preserving any other lawful excuse or defence recognised by law; and

(d) the aggravated offence under section 60(2).

9.20 The above provisions regarding "misuse of a computer" should be separated from the offence of criminal damage and adopted in the new legislation, while deleting section 59(1)(b) and (1A) of the Crimes Ordinance (Cap 200). *[Recommendation 6]*[15]

9.21 Hong Kong courts should have jurisdiction where:

(a) any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence occurred in Hong Kong, even if other such act(s), omission(s) or event(s) occurred elsewhere;

(b) the victim is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or a company carrying on business in Hong Kong;

---

[14] S 59(1A) defines "misuse of a computer" to mean the following acts:
"*(a) to cause a computer to function other than as it has been established to function by or on behalf of its owner, notwithstanding that the misuse may not impair the operation of the computer or a program held in the computer or the reliability of data held in the computer;*
(b) to alter or erase any program or data held in a computer or in a computer storage medium;
(c) to add any program or data to the contents of a computer or of a computer storage medium,
and any act which contributes towards causing the misuse of a kind referred to in paragraph (a), (b) or (c) shall be regarded as causing it."

[15] Paras 4.81 to 4.99.

(c) the target program or data is in Hong Kong; or

(d) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong. *[Recommendation 13]*[16]

9.22 An offender should be liable to the following maximum sentences:

(a) for the basic offence, imprisonment for two years on summary conviction and 14 years on conviction on indictment; or

(b) for the aggravated offence, imprisonment for life. *[Recommendation 16(c)]*[17]

Illegal interference of computer system

– Recommendations 7, 8, 14 and 16(c)

Recommendations

9.23 The proposed provisions regarding the illegal interference of computer data and computer system should be phrased in the same way.

9.24 Sections 59(1A) and 60 of the Crimes Ordinance (Cap 200) suffice to prohibit the illegal interference of computer system and should also be adopted in the new legislation.

9.25 The new legislation should retain the breadth of the existing law and should not be too restrictive, while clarifying the phrase "misuse of a computer" as appropriate (eg incorporating the notion "impair the operation of any computer").

9.26 The proposed offence of illegal interference of computer system should, for example, apply to a person who intentionally or recklessly:

(a) attacked a computer system whether successful or not (criminal liability should not depend on the success of an interference);

(b) coded a software with a bug during its manufacture; and

(c) changed a computer system without authorisation, knowing that

---

16 Paras 7.89 to 7.91.

17 Paras 8.12 to 8.16, 8.19 to 8.20.

the change may have the effect of preventing access to, or proper use, of the system by legitimate users. *[Recommendation 7]*[18]

9.27 Hong Kong courts should have jurisdiction where:

(a) any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence occurred in Hong Kong, even if other such act(s), omission(s) or event(s) occurred elsewhere;

(b) the victim is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or a company carrying on business in Hong Kong;

(c) the target computer is in Hong Kong; or

(d) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong. *[Recommendation 14]*[19]

9.28 An offender should be liable to the following maximum sentences:

(a) for the basic offence, imprisonment for two years on summary conviction and 14 years on conviction on indictment; or

(b) for the aggravated offence, imprisonment for life. *[Recommendation 16(c)]*[20]

Consultation questions

9.29 Should scanning (or any similar form of testing) of a computer system on the internet by cybersecurity professionals, for example, to evaluate potential security vulnerabilities without the knowledge or authorisation of the owner of the target computer, be a lawful excuse for the proposed offence of illegal interference of computer system?

18 Paras 5.61 to 5.68.
19 Paras 7.92 to 7.93.
20 Paras 8.12 to 8.16, 8.19 to 8.20.

9.30 Should there be lawful excuse to the proposed offence for non-security professionals, such as:

(a) web scraping by robots or web crawlers initiated by internet information collection tools, such as search engines, to collect data from servers without authorisation by connecting to designated protocol ports (eg ports as defined in RFC6335); and/or

(b) scanning a service provider's system (which has the possibility of abuse or bringing down the system) for the purpose of:

(i) identifying any vulnerability for their own security protection, for example, whether the encryption for a credit card transaction is secure before they, as private individuals, provide their credit card details for the transaction; or

(ii) ensuring the security and integrity of an Application Programming Interface offered by the service provider's system? *[Recommendation 8]*[21]

Making available or possessing a device or data for committing a crime

– Recommendations 9, 10, 15 and 16(d)

Recommendations

9.31 Knowingly making available or possessing a device or data (irrespective of whether it is tangible or intangible, eg ransomware, a virus or their source code) made or adapted to commit an offence – ie not necessarily cybercrime – should be a basic offence under the new legislation, subject to a statutory defence of reasonable excuse. *[Recommendation 9(a)]*[22]

9.32 The *actus reus* of the proposed offence should cover both the supply side (such as production, offering, sale and export of a device or data in question) and the demand side (such as obtaining, possession, purchase and import of a device or data in question). *[Recommendation 9(b)]*[23]

21 Paras 5.69 to 5.72.
22 Paras 6.73 to 6.79, 6.83 to 6.84, 6.86 to 6.87.
23 Paras 6.81 to 6.82.

9.33 The proposed offence should apply to:

(a) a device or data so long as its primary use (to be determined objectively, regardless of a defendant's subjective intent) is to commit an offence, regardless of whether or not it can be used for any legitimate purposes; and

(b) a person who believes or claims that the device or data in question could be used to commit an offence, irrespective of whether that is true or not. *[Recommendation 9(c)]*[24]

9.34 Knowingly making available or possessing a device or data (irrespective of whether it is tangible or intangible, eg ransomware, a virus or their source code):

(a) which is, or is believed or claimed by the perpetrator to be, capable of being used to commit an offence; and

(b) which the perpetrator intends to be used by any person to commit an offence

should constitute an aggravated offence under the new legislation, subject to a statutory defence of reasonable excuse. *[Recommendation 9(d)]*[25]

9.35 Hong Kong courts should have jurisdiction where:

(a) any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence occurred in Hong Kong, even if other such act(s), omission(s) or event(s) occurred elsewhere, eg a person physically in Hong Kong making available on the dark web, a device or data for committing an offence;

(b) the perpetrator is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or a company carrying on business in Hong Kong; or

(c) the perpetrator's act has caused or may cause serious damage to Hong Kong, for example, to its infrastructure or public authority, or has threatened or may threaten the security of Hong Kong. *[Recommendation 15]*[26]

---

24 Paras 6.76 to 6.77, 6.84.
25 Paras 6.73 to 6.80, 6.83, 6.85 to 6.87.
26 Paras 7.94 to 7.100.

9.36 An offender should be liable to the following maximum sentences:

(a) for the basic offence, imprisonment for two years on summary conviction and seven years on conviction on indictment; or

(b) for the aggravated offence, imprisonment for 14 years on conviction on indictment. *[Recommendation 16(d)]*[27]

9.37 The proposed provisions should be modelled on section 3A of the Computer Misuse Act 1990 in England and Wales as well as sections 8 and 10 of the Computer Misuse Act 1993 in Singapore. *[Recommendation 9(e)]*[28]

Consultation questions

9.38 Should there be a defence or exemption for the offence of knowingly making available or possessing computer data (the software or the source code), such as ransomware or a virus, the use of which can only be to perform a cyber-attack?

9.39 If the answer to the question above is "yes",

(a) in what circumstances should the defence or exemption be available, and in what terms?

(b) should such exempted possession be regulated, and if so, what are the regulatory requirements? *[Recommendation 10]*[29]

Limitation period for summary proceedings

Recommendation

9.40 The limitation period applicable to a charge for any of the proposed offences by way of summary proceedings should be two years after discovery of any act or omission or other event (including any result of one or more acts or omissions) the proof of which is required for conviction of the offence, notwithstanding section 26 of the Magistrates Ordinance (Cap 227). *[Recommendation 3]*[30]

---

27 Paras 8.12 to 8.16, 8.21 to 8.23.
28 Para 6.88.
29 Paras 6.91 to 6.93.
30 Paras 2.121 to 2.123.

Appendix

Proposed offence	Hong Kong	Australia	Canada	England and Wales	Mainland China	New Zealand	Singapore	USA
(a) Illegal access to program or data	**Section 27A, Telecommunications Ordinance (Cap 106)** – "*Unauthorized access to computer by telecommunications*" • fine at level 4, ie HKD25,000 (Schedule 8, Criminal Procedure Ordinance (Cap 221))	**Section 477.1(1)(a)(i), Criminal Code (Cth)** – "*Unauthorised access, modification or impairment with intent to commit a serious offence*"[1] • a penalty not exceeding the penalty applicable to the serious offence in question	**Section 326(1)(b), Criminal Code 1985** – "*Theft of telecommunication service*" • (summary conviction) CAD5,000 fine, or imprisonment for 2 years less a day, or both[2] • (if loss less than CAD5,000, conviction on indictment) 2-year imprisonment • (if loss exceeds CAD5,000, conviction on indictment) 10-year imprisonment	**Section 1, Computer Misuse Act 1990** – "*Unauthorised access to computer material*" • (summary conviction) a fine not exceeding the statutory maximum,[3] or 12-month imprisonment, or both • (conviction on indictment) a fine,[4] or 2-year imprisonment, or both	**Article 285(1) of the PRC Criminal Law** • 3-year imprisonment or criminal detention	**Section 249, Crimes Act 1961** – "*Accessing computer system for dishonest purpose*" • (access with intent to obtain property, etc or cause loss) 5-year imprisonment • (access and thereby obtains property, etc or causes loss) 7-year imprisonment	**Section 3, Computer Misuse Act 1993** – "*Unauthorised access to computer material*" • SGD5,000 fine, or 2-year imprisonment, or both • (second or subsequent conviction) SGD10,000 fine, or 3-year imprisonment, or both	**18 USC 1030(a)(1) to (4)** – "*Fraud and related activity in connection with computers*" • offence under subsection (a)(1) - (ordinarily) a fine,[5] or 10-year imprisonment, or both - (if previously convicted of another offence under 18 USC 1030) a fine, or 20-year imprisonment, or both

1 S 477.1(9) of the Criminal Code (Cth) defines a "serious offence" as "an offence that is punishable by imprisonment for life or a period of 5 or more years".

2 S 787(1) of the Criminal Code 1985.

3 It appears from s 85 of the Legal Aid, Sentencing and Punishment of Offenders Act 2012 that "*a fine not exceeding the statutory maximum*" now means a fine of any (ie unlimited) amount.

4 It appears from s 85 of the Legal Aid, Sentencing and Punishment of Offenders Act 2012 that a fine with no maximum amount stated means a fine of any (ie unlimited) amount.

5 The maximum amount of fine is prescribed at 18 USC 3571 (up to USD250,000 for an individual and up to USD500,000 for an organisation, or alternatively, the greater of twice the gross pecuniary gain from the offence or twice the gross loss caused to a person other than the defendant).

Proposed offence	Hong Kong	Australia	Canada	England and Wales	Mainland China	New Zealand	Singapore	USA
	Section 161, Crimes Ordinance (Cap 200) – "*Access to computer with criminal or dishonest intent*" • (conviction on indictment) 5-year imprisonment	**Section 478.1, Criminal Code (Cth)** – "*Unauthorised access to, or modification of, restricted data*" • 2-year imprisonment	**Section 342.1(1), Criminal Code 1985** – "*Unauthorized use of computer*" • (summary conviction) CAD5,000 fine, or imprisonment for not more than 2 years less a day, or both • (conviction on indictment) 10-year imprisonment	**Section 2, Computer Misuse Act 1990** – "*Unauthorised access with intent to commit or facilitate commission of further offences*" • (summary conviction) a fine not exceeding the statutory maximum, or 12-month imprisonment, or both • (conviction on indictment) a fine, or 5-year imprisonment, or both	**Article 285(2) of the PRC Criminal Law** – • (if circumstances are serious) 3-year imprisonment or criminal detention and concurrently a fine, or a fine alone • (if circumstances are especially serious) imprisonment of not less than 3 years but not more than 7 years and concurrently a fine	**Section 252, Crimes Act 1961** – "*Accessing computer system without authorisation*" • 2-year imprisonment	• (if damage caused) SGD50,000 fine, or 7-year imprisonment, or both • (if protected computer[6] accessed) SGD100,000 fine, or 20-year imprisonment, or both **Section 4, Computer Misuse Act 1993** – "*Access with intent to commit or facilitate commission of offence*" • SGD50,000 fine, or 10-year imprisonment, or both	• offence under subsection (a)(2) - (ordinarily) a fine, or 1-year imprisonment, or both - (if offence committed for commercial advantage or private financial gain, etc) a fine, or 5-year imprisonment, or both - (if previously convicted of another offence under 18 USC 1030) a fine, or 10-year imprisonment, or both

[6] Under s 11(2) of the CMA-SG:
"*… a computer shall be treated as a 'protected computer' if the person committing the offence knew, or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for —*
(a) the security, defence or international relations of Singapore;
(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;
(c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or
(d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services."

Proposed offence	Hong Kong	Australia	Canada	England and Wales	Mainland China	New Zealand	Singapore	USA
				Section 125, Communications Act 2003 – "*Dishonestly obtaining electronic communications services*" • (summary conviction) a fine not exceeding the statutory maximum, or 6-month imprisonment, or both • (conviction on indictment) a fine, or 5-year imprisonment, or both				• offence under subsection (a)(3) - (ordinarily) a fine, or 1-year imprisonment, or both - (if previously convicted of another offence under 18 USC 1030) fine, or 10-year imprisonment, or both • offence under subsection (a)(4) - (ordinarily) a fine, or 5-year imprisonment, or both - (if previously convicted of another offence under 18 USC 1030) a fine, or 10-year imprisonment, or both

Proposed offence	Hong Kong	Australia	Canada	England and Wales	Mainland China	New Zealand	Singapore	USA
								18 USC 2701 – "*Unlawful access to stored communications*" • if offence committed for purposes of commercial advantage, malicious destruction or damage, etc: - (first offence) a fine, or 5-year imprisonment, or both - (subsequent offence) a fine, or 10-year imprisonment, or both • in any other case: - (first offence) a fine, or 1-year imprisonment, or both - (if previously convicted of another offence under 18 USC 2701) a fine, or 5-year imprisonment, or both

Proposed offence	Hong Kong	Australia	Canada	England and Wales	Mainland China	New Zealand	Singapore	USA
(b) Illegal interception of computer data	**Section 27, Telecommunications Ordinance (Cap 106)** – "*Damaging telecommunications installation with intent*" • (summary conviction) fine at level 4 (ie HKD25,000) and 2-year imprisonment	**Section 7(1), Telecommunications (Interception and Access) Act 1979 (Cth)** – "*Telecommunications not to be intercepted*"[7] • (summary conviction) 6-month imprisonment • (conviction on indictment) 2-year imprisonment	**Section 184(1), Criminal Code 1985** – "*Interception*" *[of private communication]* • (summary conviction) CAD5,000 fine, or imprisonment for not more than 2 years less a day, or both • (conviction on indictment) 5-year imprisonment	**Section 3, Investigatory Powers Act 2016** – "*Offence of unlawful interception*" • (summary conviction) a fine • (conviction on indictment) a fine, or 2-year imprisonment, or both	**Article 285(2) of the PRC Criminal Law** See above.	**Section 216B, Crimes Act 1961** – "*Prohibition on use of interception devices*" • 2-year imprisonment	**Section 6, Computer Misuse Act 1993** – "*Unauthorised use or interception of computer service*" • SGD10,000 fine, or 3-year imprisonment, or both • (second or subsequent conviction) SGD20,000 fine, or 5-year imprisonment, or both • (if damage caused) SGD50,000 fine, or 7-year imprisonment, or both • (if protected computer accessed) SGD100,000 fine, or 20-year imprisonment, or both	**18 USC 2511(1)** – "*Interception and disclosure of wire, oral, or electronic communications prohibited*" • A fine, or 5-year imprisonment, or both

[7] S 105 of the Telecommunications (Interception and Access) Act 1979 (Cth) prescribes the maximum sentences for contravening s 7(1).

Proposed offence	Hong Kong	Australia	Canada	England and Wales	Mainland China	New Zealand	Singapore	USA
(c) Illegal interference of computer data	**Section 60, Crimes Ordinance (Cap 200)** – "*Destroying or damaging property*" • (the offence under section 60(1), conviction on indictment) 10-year imprisonment • (the aggravated offence under section 60(2), conviction on indictment) life imprisonment **Section 25, Telecommunications Ordinance (Cap 106)** – "*Secretion, etc., of messages by persons other than telecommunications officers*" • (summary conviction) fine at level 4 (ie HKD25,000) and 12-month imprisonment	**Section 477.2, Criminal Code (Cth)** – "*Unauthorised modification of data to cause impairment*" • 10-year imprisonment **Section 477.3, Criminal Code (Cth)** – "*Unauthorised impairment of electronic communication*" • 10-year imprisonment **Section 478.2, Criminal Code (Cth)** – "*Unauthorised impairment of data held on a computer disk etc.*" • 2-year imprisonment	**Section 430(1.1), Criminal Code 1985** – "*Mischief in relation to computer data*" • (summary conviction) CAD5,000 fine, or imprisonment for 2 years less a day, or both • (conviction on indictment) imprisonment for: - (ordinarily) 2 years - (if loss exceeds CAD5,000) 10 years - (if actual danger to life caused) life imprisonment	**Section 3, Computer Misuse Act 1990** – "*Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc*" • (summary conviction) a fine not exceeding the statutory maximum, or 12-month imprisonment, or both • (conviction on indictment) a fine, or 10-year imprisonment, or both **Section 3ZA, Computer Misuse Act 1990** – "*Unauthorised acts causing, or creating risk of, serious damage*" • (ordinarily) a fine, or 14-year imprisonment, or both	**Article 286(2) of the PRC Criminal Law** (if consequences are serious) 5-year imprisonment or criminal detention	**Section 250, Crimes Act 1961** – "*Damaging or interfering with computer system*" • (ordinarily) 7-year imprisonment • (if the offender knows or ought to know that danger to life is likely to result) 10-year imprisonment **Section 258(1), Crimes Act 1961** – "*Altering, concealing, destroying, or reproducing documents with intent to deceive*" • 10-year imprisonment	**Section 5, Computer Misuse Act 1993** – "*Unauthorised modification of computer material*" • SGD10,000 fine, or 3-year imprisonment, or both • (second or subsequent conviction) SGD20,000 fine, or 5-year imprisonment, or both • (if damage caused) SGD50,000 fine, or 7-year imprisonment, or both • (if protected computer accessed) SGD100,000 fine, or 20-year imprisonment, or both	**18 USC 1030(a)(5)** – "*Fraud and related activity in connection with computers*" • offence under subsection (a)(5)(A) - (ordinarily) a fine, or 1-year imprisonment, or both - (if harm specified in 18 USC 1030(c)(4)(A)(i) was caused) a fine, or 10-year imprisonment, or both - (if previously convicted of another offence under 18 USC 1030) a fine, or 20-year imprisonment, or both - (if the offender attempts to cause or knowingly or recklessly causes serious bodily injury) a fine, or 20-year imprisonment, or both

Proposed offence	Hong Kong	Australia	Canada	England and Wales	Mainland China	New Zealand	Singapore	USA
		Section 477.1(1)(a)(ii) and (iii), section 478.1, Criminal Code (Cth) See above.		• (where offence committed as a result of an act causing or creating a significant risk of: - serious damage to human welfare of the kind mentioned in subsection (3)(a) (loss to human life) or (3)(b) (human illness or injury), or - serious damage to national security) a fine, or life imprisonment, or both				- (if the offender attempts to cause or knowingly or recklessly causes death) a fine, or imprisonment for any term of years or for life, or both • offence under subsection (a)(5)(B) - (ordinarily) a fine, or 1-year imprisonment, or both - (if harm specified in 18 USC 1030(c)(4)(A)(i) was caused) a fine, or 5-year imprisonment, or both - (if previously convicted of another offence under 18 USC 1030) a fine, or 20-year imprisonment, or both

Proposed offence	Hong Kong	Australia	Canada	England and Wales	Mainland China	New Zealand	Singapore	USA
								• offence under subsection (a)(5)(C) - (ordinarily) a fine, or 1-year imprisonment, or both - (if previously convicted of another offence under 18 USC 1030) a fine, or 10-year imprisonment, or both

Proposed offence	Hong Kong	Australia	Canada	England and Wales	Mainland China	New Zealand	Singapore	USA
(d) Illegal interference of computer system	**Section 60, Crimes Ordinance (Cap 200)** See above.	**Sections 477.2, 477.3, 477.1(1)(a)(ii) and (iii), 478.1 and 478.2, Criminal Code (Cth)** See above.	**Section 430(1.1) and section 430(4), Criminal Code 1985** See above.	**Sections 3 and 3ZA, Computer Misuse Act 1990** See above.	**Article 285(2) of the PRC Criminal Law** See above. **Article 286(1) of the PRC Criminal Law** • (if consequences are serious) 5-year imprisonment or criminal detention • (if consequences are especially serious) imprisonment of not less than 5 years	**Sections 250 and 258(1), Crimes Act 1961** See above.	**Section 7, Computer Misuse Act 1993** – "*Unauthorised obstruction of use of computer*" • SGD10,000 fine, or 3-year imprisonment, or both • (second or subsequent conviction) SGD20,000 fine, or 5-year imprisonment, or both • (if damage caused) SGD50,000 fine, or 7-year imprisonment, or both • (if protected computer accessed) SGD100,000 fine, or 20-year imprisonment, or both	**18 USC 1030(a)(5)** See above.

Proposed offence	Hong Kong	Australia	Canada	England and Wales	Mainland China	New Zealand	Singapore	USA
(e) Making available or possessing a device or data for committing a crime	**Section 62, Crimes Ordinance (Cap 200)** – "*Possessing anything with intent to destroy or damage property*" • (conviction upon indictment) 10-year imprisonment	**Section 478.3, Criminal Code (Cth)** – "*Possession or control of data with intent to commit a computer offence*" • 3-year imprisonment **Section 478.4, Criminal Code (Cth)** – "*Producing, supplying or obtaining data with intent to commit a computer offence*" • 3-year imprisonment	**Section 191(1), Criminal Code 1985** – "*Possession, etc.*" *[of device for intercepting private communications]* • (summary conviction) CAD5,000 fine, or imprisonment for not more than 2 years less a day, or both • (conviction on indictment) 2-year imprisonment **Section 327(1), Criminal Code 1985** – "*Possession of device to obtain use of telecommunication facility or service*" • (summary conviction) CAD5,000 fine, or imprisonment for not more than 2 years less a day, or both • (conviction on indictment) 2-year imprisonment	**Section 3A, Computer Misuse Act 1990** – "*Making, supplying or obtaining articles for use in offence under section 1, 3 or 3ZA*" • (summary conviction) a fine not exceeding the statutory maximum, or 12-month imprisonment, or both • (conviction on indictment) a fine, or 2-year imprisonment, or both **Section 126, Communications Act 2003** – "*Possession or supply of apparatus etc. for contravening s.125" [ie dishonestly obtaining electronic communications services]*	**Article 285(3) of the PRC Criminal Law** • (if circumstances are serious) 3-year imprisonment or criminal detention and concurrently a fine, or a fine alone **Article 286(3) of the PRC Criminal Law** • (if consequences are serious) 5-year imprisonment or criminal detention	**Section 216D, Crimes Act 1961** – "*Prohibition on dealing, etc, with interception devices*" • 2-year imprisonment **Section 251, Crimes Act 1961** – "*Making, selling, or distributing or possessing software for committing crime*" • 2-year imprisonment	**Section 8, Computer Misuse Act 1993** – "*Unauthorised disclosure of access code*" • SGD10,000 fine, or 3-year imprisonment, or both • (second or subsequent conviction) SGD20,000 fine, or 5-year imprisonment, or both **Section 10 of the Computer Misuse Act 1993** – "*Obtaining, etc., items for use in certain offences*" • SGD10,000 fine, or 3-year imprisonment, or both • (second or subsequent conviction) SGD20,000 fine, or 5-year imprisonment, or both	**18 USC 1030(a)(6)** – "*Fraud and related activity in connection with computers*" • (ordinarily) a fine, or 1-year imprisonment, or both • (if previously convicted of another offence under 18 USC 1030) a fine, or 10-year imprisonment, or both **18 USC 2512(1)** – "*Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices prohibited*" • A fine, or 5-year imprisonment, or both

Proposed offence	Hong Kong	Australia	Canada	England and Wales	Mainland China	New Zealand	Singapore	USA
			Section 342.2(1), Criminal Code 1985 – "*Possession of device to obtain unauthorized use of computer system or to commit mischief*" • (summary conviction) CAD5,000 fine, or imprisonment for not more than 2 years less a day, or both • (conviction on indictment) 2-year imprisonment	• (summary conviction) a fine not exceeding the statutory maximum, or 6-month imprisonment, or both • (conviction on indictment) a fine, or 5-year imprisonment, or both				