# THE LAW REFORM COMMISSION OF HONG KONG

# REPORT

# CYBER-DEPENDENT CRIMES AND JURISDICTIONAL ISSUES

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

**January 2026**

The Law Reform Commission of Hong Kong was established by the Executive Council in January 1980. The Commission considers such reforms of the laws of Hong Kong as may be referred to it by the Secretary for Justice or the Chief Justice.

The members of the Commission at present are:

***Chairman:*** ***The Hon Paul T K LAM, GBS, SC, JP,***
***Secretary for Justice***

***Members:*** ***The Hon Chief Justice Andrew Cheung, GBM***
***The Hon Mr Justice Johnson Lam,***
***Permanent Judge of the Court of Final Appeal***
***Mr Michael Lam, Law Draftsman***
***Ms May Chan, GBS, JP***
***Mr Stephen Hung, MH***
***Mrs Janice Choi, BBS, MH, JP***
***Mr C M Chan, JP***
***The Hon Mrs Margaret Leung, SBS, JP***
***Professor Alexander F H Loke***
***Professor Michael Jackson***
***Ms Frances Lok, SC***
***Professor Chao Xi***

The Secretary of the Commission is **Mr Wesley Wong, SC, JP, Law Officer** and the Commission's offices are at:

***9/F, Champion Tower***
***Three Garden Road***
***Central***
***Hong Kong***

***Telephone:*** ***3703 6518***
***Fax:*** ***3702 0136***
***E-mail:*** ***hklrc@hkreform.gov.hk***
***Website:*** ***http://www.hkreform.gov.hk***

Mr C M Chan, JP ceased to be a member of the Law Reform Commission (LRC) after 31 December 2025. The LRC Chairman and Secretariat express their appreciation to Mr Chan for his valuable contributions and advice to the LRC's work over the years.

# THE LAW REFORM COMMISSION OF HONG KONG

## REPORT

## CYBER-DEPENDENT CRIMES AND JURISDICTIONAL ISSUES

---

***CONTENTS***

## Defined Terms

| Abbreviation | Definition |
|---|---|
| Access Offence | Illegal access to program or data |
| BL 23 legislation | Safeguarding National Security Ordinance |
| Budapest Convention | Council of Europe's Convention on Cybercrime |
| CFA | Court of Final Appeal |
| CMA-EW | Computer Misuse Act 1990 (England and Wales) |
| CMA-SG | Computer Misuse Act 1993 (Singapore) |
| CO | Crimes Ordinance (Cap 200) |
| Commissioner | Privacy Commissioner for Personal Data |
| Consent defence | The defence identified under section 64(2)(a), Crimes Ordinance (Cap 200)[1] |
| DDOS | Distributed denial of service |
| DNS | Domain name system |
| DSA | Digital Services Act |
| EU | European Union |
| HKBA | Hong Kong Bar Association |
| HKFWL Ltd | Hong Kong Federation of Women Lawyers Limited |
| HKSAR | Hong Kong Special Administrative Region of the People's Republic of China |
| HKWPEA | Hong Kong Women Professionals and Entrepreneurs Association |

[1] See paras 2.96 and 4.11.

| | |
|---|---|
| ICSO | Interception of Communications and Surveillance Ordinance (Cap 589) |
| Interference Offences | Illegal interference with computer data and illegal interference with computer system |
| IP | Internet protocol |
| ISP | Internet service provider |
| Law Commission | Law Commission of England and Wales |
| Law Society | Law Society of Hong Kong |
| LEA | Law enforcement agency |
| MHO | Mental Health Ordinance (Cap 136) |
| MLACMO | Mutual Legal Assistance in Criminal Matters Ordinance (Cap 525) |
| MO | Magistrates Ordinance (Cap 227) |
| Model Law | Model Law on Computer and Computer Related Crime |
| NSL | The Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region |
| NS Office | Office for Safeguarding National Security of the Central People's Government in the Hong Kong Special Administrative Region |
| PCPD | Office of the Privacy Commissioner for Personal Data |
| PDPO | Personal Data (Privacy) Ordinance (Cap 486) |
| POO | Public Order Ordinance (Cap 245) |
| Property protection defence | The defence identified under section 64(2)(b), Crimes Ordinance (Cap 200)[2] |

[2] See paras 2.96 and 4.11.

| | |
|---|---|
| Russian Convention | *Draft United Nations Convention on Cooperation in Combating Cybercrime* submitted by the Russian Federation to the United Nations on 11 October 2017 |
| S161 | Section 161, Crimes Ordinance (Cap 200) |
| S64(2) | Section 64(2), Crimes Ordinance (Cap 200) |
| S27A | Section 27A, Telecommunications Ordinance (Cap 106) |
| SCA | Stored Communications Act |
| SPC | Supreme People's Court |
| SPP | Supreme People's Procuratorate |
| Theft Ordinance | Theft Ordinance (Cap 210) |
| TO | Telecommunications Ordinance (Cap 106) |
| UN Convention | United Nations Convention against Cybercrime |
| UNCRC | United Nations Convention on the Rights of the Child |
| USA | United States of America |

# Preface

## Introduction

1. This report ("**Report**") discusses the responses received in respect of the Consultation Paper on Cyber-dependent Crimes and Jurisdictional Issues published by the Law Reform Commission's Cybercrime Sub-committee ("**Sub-committee**") in July 2022 ("**Consultation Paper**"), and sets out our analysis and final recommendations on this topic.

## Background

2. 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.

3. The last official study on cybercrime in the Hong Kong Special Administrative Region of the People's Republic of China ("**HKSAR**") dates back to 2000, when the Government of the HKSAR convened an Inter-departmental Working Group on Computer Related Crime. With the significant technological and societal developments in the last two decades, the time is ripe for another review of the topic. Thus, in early 2019, the Chief Justice and the Secretary for Justice referred the topic of cybercrime to the Law Reform Commission of Hong Kong for consideration. The Sub-committee was appointed to examine the current state of the law and to make recommendations.

4. 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 ("**NSL**") was enacted and applied, as a national law, to the HKSAR by promulgation on 30 June 2020. The duty of the HKSAR to safeguard national security reaffirmed the need for reform of cybercrime laws in the HKSAR[1] and we have taken this into consideration in our pursuit of the cybercrime project.

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

## Terms of Reference

5. The Sub-committee commenced its study on this topic in 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 —*
>
> *(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

6. Composition of the Sub-committee chaired by Mr Derek Chan, SC is as follows:

| | |
|---|---|
| **Mr Derek Chan, SC** ***(Chairman from 19 January 2023)*** | Senior Counsel |
| **Mr Allan Leung** ***(Chairman from 13 December 2018 until 18 January 2023)*** | Senior Consultant, Dentons Hong Kong LLP |
| **Ms Chan Shuk Yi, Christal** (from 13 December 2018 to 12 September 2023) | Assistant Director of Public Prosecutions, Department of Justice |
| **Miss Vinci Chan** (from 25 March 2025) | Principal Assistant Secretary for Security, Security Bureau |

| | |
|---|---|
| **Dr Cheng Chung Ngam, Rocky**<br>(from 12 January 2022 to 25 February 2024) | Former Chief Information Officer, Bank of China (Hong Kong) Limited |
| **Ms Cheng Lai Ki, Kelly**<br>(from 3 May 2022 to 25 February 2024) | Chief Superintendent, Financial Intelligence and Investigation Bureau, Hong Kong Police Force<br><br>Former Chief Superintendent, Cyber Security and Technology Crime Bureau, Hong Kong Police Force |
| **Ms Cheung Pui Shan, Sandy**<br>(from 21 April 2023 to 24 March 2025) | Former Principal Assistant Secretary for Security, Security Bureau |
| **Dr K P Chow** | Research Advisor, Logistics and Supply Chain MultiTech R&D Centre Limited<br><br>Former Associate Professor, Department of Computer Science, The University of Hong Kong |
| **Ms Chui Shih Yen, Joceline**<br>(from 12 August 2019 to 16 April 2023) | Former Principal Assistant Secretary for Security, Security Bureau |
| **Mr Fong Wing Kai, Guy**<br>(from 13 December 2018 to 13 September 2020) | Former Group Head (Intellectual Property Investigation (Operations)), Hong Kong Customs and Excise Department |
| **Ms Clara Ho**<br>(from 13 December 2018 to 20 December 2020) | Former Head of Resilience Risk, Asia Pacific, The Hongkong and Shanghai Banking Corporation Limited |
| **Mr Francis Ho**<br>(from 13 January 2023) | Deputy Chief Executive, Consumer Council |
| **Dr Michael Kwan** | Chief Executive Officer, Asia Pacific Internet Centre |
| **Mr Lam Cheuk Ho, Raymond**<br>(from 26 February 2024) | Chief Superintendent, Cyber Security and Technology Crime Bureau, Hong Kong Police Force |
| **Mr Law Shiu Kai, Andrew**<br>(from 13 December 2018 to 13 July 2020) | Former Partner, Robinsons, Lawyers |

| | |
|---|---|
| **Dr Law Yuet Wing, Frank**<br>(from 13 December 2018 to 12 April 2022) | Regional Commander (Kowloon East), Hong Kong Police Force<br><br>Former Senior Superintendent, Cyber Security and Technology Crime Bureau, Hong Kong Police Force |
| **Mr Leung Yuk Hang, Gary**<br>(from 13 September 2023) | Acting Senior Assistant Director of Public Prosecutions, Department of Justice |
| **Ms Tam Pui Ying, Peggy**<br>(from 21 May 2024 to 31 July 2025) | Head of Intellectual Property Investigation Bureau, Hong Kong Customs and Excise Department<br><br>Former Group Head (Intellectual Property Investigation (Operations)), Hong Kong Customs and Excise Department |
| **Mr Raymond Tang**<br>(from 11 January 2021 to 11 January 2022) | Former Head of Operational and Resilience Risk, Hong Kong and Macau Region, The Hongkong and Shanghai Banking Corporation Limited |
| **Mr Tang Tze Yeung, Eric**<br>(from 9 January 2023) | Partner, Tang & Ku |
| **Mr Tong Chi Chung, Eddy**<br>(from 13 December 2018 to 12 January 2023) | Former Deputy Chief Executive, Consumer Council |
| **Mr Tsang Yue Tung, Andrew**<br>(from 13 December 2018 to 9 August 2019) | Former Principal Assistant Secretary for Security, Security Bureau |
| **Mr Wong Ka Chun, Thomas**<br>(from 1 August 2025) | Group Head (Intellectual Property Investigation (Operations)), Hong Kong Customs and Excise Department |
| **Miss Wong Pui Kei, Maggie, SC** | Senior Counsel |
| **Ms Wong Wai Chuen, Phoebe**<br>(from 14 September 2020 to 8 May 2024) | Assistant Commissioner, Hong Kong Customs and Excise Department<br><br>Former Group Head (Intellectual Property Investigation (Operations)), Hong Kong Customs and Excise Department |

| | |
|---|---|
| **Ms Wong Wing Hang, Charlotte** (from 26 February 2024 to 19 December 2025) | Former Managing Director and Chief Information Officer, The Hongkong and Shanghai Banking Corporation Limited |
| **Mr Yip Yuk Fai, Lento** | Chairman, Hong Kong Internet Service Providers Association |

7. 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.[2]

## Three phases of the project

8. 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:

(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

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

### *Five cyber-dependent offences to study in Part One*

9. This Report relates to Part One of the project. Drawing on the Council of Europe's Convention on Cybercrime ("**Budapest Convention**") and the United Nations Convention against Cybercrime ("**UN Convention**"),[3] 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;

---

2 Mr Edmund Ma, then Senior Government Counsel, was the Secretary to the Sub-committee until May 2021, while Mr Terence Lee, Senior Government Counsel, was the Secretary to the Sub-committee from 2 September 2024 to 17 September 2025.

3 Details of the Council of Europe's Convention on Cybercrime and the United Nations Convention against Cybercrime appear in Chapter 1.

(b) illegal interception of computer data;

(c) illegal interference with computer data;

(d) illegal interference with computer system; and

(e) making available a device, program or data made or adapted to commit a cyber-related crime (which includes possessing such a device, program or data for the purpose of making it available to another).

***Guiding principles behind the recommendations***

10. 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.

## The consultation process

11. The three-month consultation period closed on 19 October 2022. In total, 65 submissions were received (some were received after showing the courtesy of requesting an extension of time), ranging from a simple acknowledgement of the Consultation Paper to detailed submissions on the Sub-committee's recommendations and questions in the Consultation Paper.

12. Those which submitted responses included academics, Government bureaux/departments, quasi-Government bodies, information technology-related bodies, legal professional bodies, business groups, political parties, as well as members of the public (each "**Respondent**" and collectively the "**Respondents**"). A list of the Respondents is set out in the Annex to this Report. We are most grateful to all those who commented on the Consultation Paper. The submissions made are summarised in the following chapters.

13. In addition to attending television and radio interviews to explain the recommendations in the Consultation Paper, the representatives of the Sub-committee participated in the HKU-CS Online Tech Forum organised by the Department of Computer Science of the University of Hong Kong on 14 September 2022 and a Questions-and-Answers session hosted by the Hon

Duncan Chiu, member of the Technology and Innovation Functional Constituency of the Legislative Council, on 27 October 2022. Both occasions were mostly attended by stakeholders from the information technology and telecommunications sector and they provided useful opportunities for the Sub-committee to reach out to cybersecurity practitioners and to clarify some of the recommendations in the Consultation Paper.

14. On 7 November 2022 (which was the earliest meeting slot that could be arranged for the Sub-committee in consultation with the Legislative Council), members of the Sub-committee attended a meeting of the Panel on Administration of Justice and Legal Services of the Legislative Council to provide a briefing on the Consultation Paper and hear views from deputations.

## Structure of this Report

15. This Report consists of nine chapters dealing with 16 Final Recommendations:

(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, 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 with computer data.

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

(f) Chapter 6 deals with the fifth cyber-dependent offence, ie making available or possessing a device, program or data for committing a cyber-related 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 summarises our Final Recommendations.

16. The list of Respondents (Annex) can be found at the end of this Report.

# Chapter 1

# Categorisation of cybercrime

## Introduction

1.1 As the Sub-committee observed in the Consultation Paper,[1] there is no definitive or exhaustive list of cybercrime. Multiple ways to categorise cybercrime and multiple sets of terminologies for such categorisation exist in the literature. At the United Nations' level, the United Nations Office on Drugs and Crime Global Programme on Cybercrime, which commenced in 2013, distinguishes between "*cyber-dependent crimes*" and "*cyber-enabled crimes*".[2] The following elaboration of the United Kingdom Government is instructive:

(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*".[3] Examples of cyber-dependent crimes include hacking, distribution of computer virus, and distributed denial of service attack.

(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*".[4] 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).

1 At para 1.2.

2 United Nations Office on Drugs and Crime ("**UNODC**"), "*Global Programme on Cybercrime*", available at: https://www.unodc.org/unodc/en/cybercrime/our-approach (accessed on 1 Nov 2025).

3 Cabinet Office, National security and intelligence, HM Treasury, and The Rt Hon Philip Hammond MP, *National Cyber Security Strategy 2016-2021* (United Kingdom Government, 2016) at para 3.2, available at https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (accessed on 1 Nov 2025).

4 Same as above.

## Categorisation under the Budapest Convention

### *Offences prescribed by the Budapest Convention*

1.2 The Council of Europe's Convention on Cybercrime ("**Budapest Convention**") was opened for signature on 23 November 2001 and entered into force on 1 July 2004.[5] Since then, it has been supplemented by two Additional Protocols concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems,[6] as well as enhanced co-operation and disclosure of electronic evidence.[7] The Budapest Convention appears to be the first multi-national agreement for regulating cyberspace.[8] As at 1 November 2025, 81 states had ratified or acceded to the Budapest Convention.[9]

1.3 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.[10] 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):

(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

---

5 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 1 Nov 2025).

6 The text of the first Additional Protocol, which entered into force on 1 March 2006, 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 1 Nov 2025).

7 The text of the second Additional Protocol, which was opened for signature in May 2022, is available on the website of the Council of Europe, at https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224 (accessed on 1 Nov 2025).

8 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 1 Nov 2025).

9 Council of Europe, Chart of signatures and ratifications of Convention on Cybercrime (ETS No. 185), available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 (accessed on 1 Nov 2025).

10 Council of Europe, *Explanatory Report to the Convention on Cybercrime* (ETS No 185, 23 Nov 2001), at para 33, available at https://rm.coe.int/16800cce5b (accessed on 1 Nov 2025).

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

***Model Law on Computer and Computer Related Crime***

1.4 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[11] ("**Model Law**") taking into account the Budapest Convention. The Model Law was adopted in 2002 and under consideration for review as of July 2017.[12]

1.5 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.[13]

## Latest developments in the United Nations

1.6 The international landscape of cybercrime regulation is evolving rapidly. The following 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.[14]

(b) In its Resolution 74/247 adopted on 27 December 2019,[15] 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*

---

11 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 1 Nov 2025).

12 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.

13 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 1 Nov 2025).

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

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

*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".*[16]

(c) After years of work by the above ad hoc committee, the United Nations Convention against Cybercrime ("**UN Convention**") was adopted by the General Assembly on 24 December 2024 through its Resolution 79/243.[17] The UN Convention was opened for signature in Vietnam on 25 October 2025 and will remain open for signature at the United Nations Headquarters in New York until 31 December 2026. The UN Convention will enter into force after 40 states become parties, with its implementation reviewed by the Conference of the States Parties to be convened periodically to improve the capacity of, and cooperation among, States Parties to achieve the objectives of the Convention.[18]

1.7 The UN Convention is the first comprehensive global treaty on cybercrime. It provides states with a range of measures to be undertaken to prevent and combat cybercrime. It also aims to strengthen international cooperation in sharing electronic evidence for serious crimes.[19]

1.8 As readers are aware, the recommendations in the Consultation Paper published in 2022 drew on the concepts in the Budapest Convention and the Russian Convention.[20] In respect of the cyber-dependent offences featured in Part One of the study, the categorisation of the offences under the Budapest Convention and the UN Convention is essentially the same, with the latter Convention using different terminologies such as "information and communications technology" (as in the Russian Convention considered in the Consultation Paper)[21] and "electronic data", instead of "computer" and

---

16 At para 3. From 2022 to 2023, the ad hoc committee held six sessions. It held its concluding session from 29 January to 9 February 2024 in New York and reconvened its concluding session from 29 July to 9 August 2024, when the committee approved a draft resolution on the United Nations Convention against Cybercrime. See: UNODC, "*Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*", available at https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home (accessed on 1 Nov 2025).

17 UNODC, "United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes", available at https://www.unodc.org/unodc/en/cybercrime/convention/home.html (accessed on 1 Nov 2025).

18 Same as above. The signing ceremony in October 2025 concluded with 72 signatories, including China. Following signature, states will complete their internal domestic processes to implement the Convention and, once concluded, deposit an instrument of ratification, acceptance, or approval with the Secretary-General to formally become States Parties to the Convention. States that did not sign the Convention may also become Parties by depositing an instrument of accession. For further information, the ad hoc committee will hold a session from 26 to 30 January 2026 in Vienna to prepare the draft rules of procedure of the Conference of the States Parties to the Convention. See https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_session_on_RoP/main.html (accessed on 1 Nov 2025).

19 See fn 17 above.

20 Consultation Paper, Preface, at para 10.

21 Consultation Paper, at paras 2.93 to 2.95.

"computer data" respectively in the Budapest Convention.[22] This being the case, the continued use of the terminologies adopted in the Consultation Paper and the references to the Budapest Convention hereafter in this Report do not affect the merits of the Final Recommendations made for Part One of the project. Should the Government implement the recommendations in this Report, it would of course be at liberty to decide how best the relevant concepts may be articulated in the new bespoke cybercrime legislation.

[22] As we will explain in paras 2.42 to 2.46, we consider it apposite to retain the term "computer" in the new bespoke cybercrime legislation.

# Chapter 2

# Illegal access to program or data

## Introduction

2.1 This Chapter discusses the responses regarding Recommendations 1 to 3 of the Consultation Paper. Recommendation 1 relates to the first cyber-dependent offence, namely illegal access to program or data in a computer ("**Access Offence**"):

> "*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 [Computer Misuse Act 1990 of England and Wales ("**CMA-EW**")].*"

2.2 As the Sub-committee explained in the Consultation Paper,[1] broadly speaking, the Access Offence 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.

2.3 As some of the responses referred to section 161 of the Crimes Ordinance (Cap 200) ("*Access to computer with criminal or dishonest intent*") ("**S161**") and this provision is often used to prosecute computer offences under the current law, it would be helpful to recap the provision in this Chapter:

---

[1] At para 2.1.

*"(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*

*(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."*

2.4 In *Secretary for Justice v Cheng Ka Yee (鄭嘉儀)*,[2] the Court of Final Appeal ("**CFA**") 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*".[3] Logic supports the same conclusion with regard to the other limbs in S161(1). Therefore, S161 does not apply to, for instance, the use of one's own computer to set up a phishing website.

2.5 Another provision relevant to the consideration of the Access Offence 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 (2019) 22 HKCFAR 97, FACC 22/2018 (date of judgment: 4 Apr 2019).
3 Same as above, at para 48.

*(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 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."*

2.6 As the Court of First Instance held in *HKSAR v Tsun Shui Lun*,[4] 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*".[5]

[4] [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.

[5] See fn 2 above, at para 41.

## Responses to the Sub-committee's Recommendation 1

2.7 The Respondents who commented on Recommendation 1 generally agreed that there should be an offence of unauthorised access to program or data. The Hong Kong and Mainland Legal Professional Association Limited opined that the limitations of S161 and S27A are "*obvious*" since these provisions do not apply to a person who uses his own computer or other non-telecommunications devices to commit cybercrimes. This view was echoed by a political group and a business organisation, which noted that the scope of S161 has been "*significantly narrowed by the Court of Final Appeal*" in *Cheng Ka Yee*.[6]

2.8 Likewise, the Consumer Council in general agreed that there is a need to outlaw mere unauthorised access to program or data, provided that the defence of reasonable excuse and the specific defence or exemption for unauthorised access for cybersecurity purposes are available.

2.9 Nevertheless, some Respondents are concerned about the scope of the Access Offence and doubt whether unauthorised access to program or data "without criminal intent" (ie mere unauthorised access) should be an offence. Others who commented on Recommendation 1 suggested clarifying the coverage of the "reasonable excuse" defence. The Respondents' comments on Recommendation 1 are set out in greater detail below.

### *Mens rea of the summary offence of mere unauthorised access under Recommendation 1(a)*

2.10 Some Respondents who compared Recommendation 1 with S161 opined that Recommendation 1 did not factor in any "*malicious intent*". A number of information technology-related bodies and individuals stressed the importance of including "criminal / malicious intent", "malice", "recklessness" and/or the occurrence of damage as the constituent element(s) of the Access Offence. From the elaboration in the submissions, it seems that the "malice" or "malicious intent" contemplated by the Respondents embraces situations where a defendant is involved in a "*criminal activity or unlawful activity*", or has a "*dishonest intent for gain, loss or deception*" as in S161. In their views:

(a) without the requirement of malice, there is a risk that legitimate behaviour may be criminalised. These include technological and security practices, such as cloud computing, penetration testing and other normal practices that security professionals, white-hat hackers and bounty program participants engage in.

(b) information technology professionals, as well as general users, may easily come into contact with voluminous data (eg telephone

[6] See fn 2 above.

records, computer log records) many of which is accessible without submitting any password. The proposed offence of mere unauthorised access (without any malice or intent to commit crime) "*neglects the purpose or intention of the act of access*".

### *Statutory defence of reasonable excuse*

2.11 Some Respondents, including a business group, thought that the scope of the statutory defence of "reasonable excuse" in Recommendation 1 is unclear, vague, subjective and uncertain. Altogether, three suggestions have been put forward by information technology-related organisations, business bodies and a political group:

(a) expressly include the exempted activities in the definition of "reasonable excuse", such as "*cybersecurity operations*", "*network scanning by internet service providers for operational reasons*" and "*legitimate business operations without any criminal intent*";

(b) provide a non-exhaustive list of statutory examples of legitimate activities which would constitute a "reasonable excuse"; and

(c) include specific defences to the proposed offence to cover legitimate business services or behaviour, and the statutory defence or exemptions should be drafted liberally to allow sufficient room for legitimate business operators to exculpate themselves.

### *Proving the aggravated offence*

2.12 As the Sub-committee explained in the Consultation Paper,[7] an offender of illegal access may further cause potentially serious harm 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. Recommendation 1(b) therefore proposed that unauthorised access with intent to carry out further criminal activity should constitute an aggravated form of the offence under the new legislation with reference to the formulation in section 2 of the CMA-EW.[8]

---

7 At para 2.107.

8 Section 2 of the CMA-EW provides that:
"*(1) A person is guilty of an offence under this section if he commits an offence under s 1 above ('the unauthorised access offence') with intent—*

2.13 In relation to the aggravated offence, the Hong Kong Federation of Women Lawyers Limited opined that it is "*fairly difficult*" to prove the intent in relation to "*a potential crime which has not been committed*", so the summary offence under Recommendation 1(a) may be heavily relied on for serious offences which nevertheless cannot be established as aggravated offences. It further invited the Sub-committee to consider this observation in terms of sentencing, ie whether the two years' imprisonment for summary offences would provide sufficient deterrence.

***The overlap of offences***

2.14 Regarding the Sub-committee's proposal to retain S161 before it is clear that the new cybercrime legislation suffices to replace it, two Respondents have divergent views on the overlap of offences under S161 and the Access Offence.

2.15 One view is that the overlap of offences "*is likely to cause confusion to the public and makes the law unnecessarily complex and obscure*". It is also suggested that the Sub-committee's desired purpose may not necessarily be achieved if offences are continued to be prosecuted under S161 instead of under the new legislation.

2.16 A contrary view is that any concern of overlap of offences is likely to be more apparent than real. The relevant argument is quoted below:

> "*… the charging practice of the prosecution is to 'reflect adequately the criminality of the conduct alleged, in a manner that is both efficient and that will enable the court to do justice between the community and the accused', and '[t]he number of charges should be kept as low as reasonably possible' (Prosecution Code, para. 8.1) ... even if a person is charged and convicted of multiple offences that might have overlapped with each other in terms of criminality, the court will inevitably be required to sentence the defendant in accordance with the well-established principle of totality.*"

---

*(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.*

*…*

*(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.*"

***Defining certain terms***

2.17 Some business bodies, interest groups and individuals consider that the meaning of certain concepts, including "unauthorised" / "authorised" access, "access", "computer network" and "data", should be clearly defined or explained to the public.

## Our analysis and response

***Clarifying the mens rea***

2.18 For those Respondents who are of the view that mere unauthorised access to program or data "*without criminal intent*" should not be an offence, it appears that they have either treated the proposed offence as one of strict liability, or have taken the view that there must exist an intention to engage in criminal activities in respect of an offence of unauthorised access.

2.19 Under Recommendation 1(c) of the Consultation Paper, the Sub-committee proposed modelling the Access Offence on sections 1, 2 and 17 of the CMA-EW. It should be emphasised that the English offence is not one of strict liability, but requires proof of *mens rea*. For clarity's sake, it would be helpful to cite the relevant provisions of the English Access Offence in this Report again.

2.20 Section 1 of the CMA-EW ("*Unauthorised access to computer material*"), which is the basic form of the English Access Offence, 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;*
>
> *(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.*

*…"*

(emphasis added)

2.21 Section 17(5) and (8) of the CMA-EW explains the unauthorised nature of an access:

> *"(5) 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 …*
>
> *…*
>
> *(8) 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.*"

2.22 Thus, the *mens rea* of the summary offence under section 1(1) of the CMA-EW includes both the defendant's (i) intention to secure access to any program or data (or to enable such access to be secured), and (ii) knowledge at the time of the *actus reus* that the intended access was unauthorised. In other words, *mens rea* as to the nature of the access is a requisite element that must be proved by the prosecution, and the *actus reus* (ie the conduct element of access) and the *mens rea* (ie the mental element of knowledge about the unauthorised nature of the access) must be present simultaneously before the Access Offence would arise. The prosecution or the court would have to be satisfied that at the time when the unauthorised access was performed, the defendant knew that the access was unauthorised.

2.23 We maintain our view that it is fair for the Access Offence to be premised on a person's knowledge that the access performed by that person is unauthorised. We anticipate that the court will likely draw inferences

regarding such knowledge based on the circumstantial evidence of a case.[9] In this regard, the real life case cited in some of the Respondents' submissions is illustrative of this point: A passenger discovered a security loophole in the electronic boarding pass issued by an airline, which made it possible for him to inspect other passengers' information by revising the last two characters of the URL. Upon investigation of the incident, it was found that the internet protocol ("**IP**") address of the defendant was linked to the booking webpage of another passenger without authorisation. The defendant was charged under S27A.[10] In our view, although the airline did not put in place sufficient security to protect the check-in information of other passengers, the defendant passenger, being an ordinary user of the electronic system of the airline, should not expect that the airline had authorised him to access fellow passengers' boarding pass by revising the URL and the charge laid against him under S27A was justifiable.

2.24 We would add that the veracity of any person's allegation that he did not have knowledge about the unauthorised nature of the access should be tested in the whole course of events leading to the access. For instance, assume that a leak of data files of a statutory body reveals the information of thousands of persons who have dealings with that body, and the data breach was advertised by a self-proclaimed activist who maintains a website or social media page with the professed objective of promoting transparency and accountability in Hong Kong. In respect of a person who thereby discovered the data breach and then accessed the leaked data now in the public domain, the court would inquire into the facts leading to the defendant's browsing the actual website containing the leaked information. It will ultimately be a matter for the court to determine in all the circumstances of the case whether or not the evidence permits the drawing of the necessary inference that at the time when the defendant made the access, he knew that such access was unauthorised.

***Mere unauthorised access should be an offence***

2.25 The Respondents' comments on the mental element of the Access Offence also relate to the question of whether mere unauthorised access to program or data should be an offence, which was discussed thoroughly in Chapter 2 of the Consultation Paper.[11] At the outset, the Sub-committee has acknowledged that the cyberspace, by its very nature, is in a completely different realm from the physical world where boundaries are tangible and well-defined:

> "*… 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*

[9] Consultation Paper, at para 2.101.

[10] The case number is WKS6208/2019. Eventually, the prosecution offered no evidence against the defendant, who agreed to being bound over for one year. See https://www.hk01.com/article/347780 (accessed on 1 Nov 2025)

[11] At paras 2.4, 2.5, 2.96 to 2.101.

*program or data is implicitly granted by 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* [12] *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.*"[13]

2.26 In other words, the customary or industry practices (of not seeking prior express authorisation for access to the level the Sub-committee has given examples of and in respect of which we agree) that are already generally accepted in daily life when entering the cyberspace will continue to be tolerated for the reason we gave above when explaining the concept of "unauthorised" access.[14] It was on this basis that Recommendation 1 proposed 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.[15] Further examples of circumstances involving implied authorisation include, but are not limited to, situations where access to program or data occurs by virtue of automatic connections by design[16] and practical necessity.[17]

---

12 Specifically, search engines regularly test ports 80 and 443, which are ports generally associated with access to websites. In cyberspace, a port is a virtual point of a computer where network connections start and end. Ports are software-based and managed by a computer system. 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 1 Nov 2025). Given their specific designations, connections to the ports for such designated purposes as ports 80 and 443 are designated for should not be prohibited by the law. Further, search engines typically use web crawling software which systematically browse webpages to gather information about them. This process enables the information to be indexed and retrieved when a user makes a search query. See Alexander S Gillis, "What is a web crawler?" See https://www.techtarget.com/whatis/definition/crawler (accessed on 1 Nov 2025).

13 Consultation Paper, at para 2.5.

14 Same as above.

15 Consultation Paper, at para 2.100.

16 Eg When the user of a smart phone switches it on and activates its Wi-Fi function at a shopping mall, the device automatically detects the available Wi-Fi hotspot provided by the mall and the mall's network likewise detects the existence of the user's phone even though the user does not choose to connect his or her phone to the mall's Wi-Fi hotspot. Another example is that when a user connects his or her personal computer to a public Wi-Fi access point and makes it discoverable, any other computers or electronic devices connected to the same Wi-Fi access point are able to detect the existence of the user's personal computer. In each example above, the user's device is accessed by another device through request for communication sent to the user's device by the latter and the response sent from the user's device.

17 This can be illustrated by examples such as (i) peer-to-peer file sharing and (ii) decentralised blockchain technology. Peer-to-peer file sharing enables users to share data and electronic files with each other without a central server. When a user runs a peer-to-peer software on a personal computer, the software

2.27 It would also be useful to recap the comments in the Explanatory Report to the Council of Europe's Convention on Cybercrime, which accounted for the ramifications of mere unauthorised access to a computer / program or data:

> "*44. 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 (including passwords, information about the targeted system) 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.*
>
> *45. The most effective means of preventing unauthorised access is, of course, the introduction and development of effective security measures. However, a comprehensive response has to include also the threat and use of criminal law measures. A criminal prohibition of unauthorised access is able to give additional protection to the system and the data as such and at an early stage against the dangers described above."*
>
> (emphasis added)

2.28 We have further studied the extrinsic legislative materials of the CMA-EW, which shed light on the objectives of creating the basic form of the Access Offence (ie mere unauthorised access). The Law Commission of England and Wales ("**Law Commission**") saw hacking by unauthorised entry as "*a matter of major and legitimate concern to system users*" because of the uncertainty and cost caused by hacking attempts.[18] The Law Commission explained that:

> "*… because of the possibility that any attempted entrant may have had password access to important levels of authority, sometimes to a level which has enabled him to delete records of his activities from the system, any successful unauthorised access must be taken very seriously. Substantial costs are therefore incurred in (i) taking security steps against unauthorised entry and in the equally important precaution of monitoring*

sends out data to other peers which are available for access (ie other computers connected to the internet), and the peers may send back a reply before a connection between two peers is established. Similarly, decentralised blockchains often use a peer-to-peer network for node discovery. In this case, nodes (eg a computer or smart phone capable of connecting to the internet) broadcast their presence to the network and listen for messages from other nodes. When a node receives a message from a new node, it can establish a connection and exchange information. See Radovan Stevanovic, "*Blockchain from Scratch: Understanding Network Communication in Blockchains*" (3 Jan 2023).

[18] Law Commission, "*Criminal Law – Computer Misuse*" (Law Com No 186, 1989), at para 1.29.

*attempts to enter; and (ii) investigating any case, however trivial, where unauthorised entry does in fact occur … we are satisfied … that the costs are substantial.*"[19]

(emphasis added)

2.29 Therefore, the offence of mere unauthorised access was a response to "*the need to protect the integrity and security of computer systems from attacks from unauthorised persons seeking to enter those systems, whatever may be their intention or motive*",[20] and the Law Commission proposed, "*as a deterrent counter to hacking*",[21] the summary and aggravated offences under sections 1 and 2 of the CMA-EW respectively, which were intended to operate together to provide an effective deterrent against all forms of unauthorised access.[22]

2.30 As the CMA-EW was enacted in the pre-digital era when the use of the internet was less prevalent, we have considered to what extent the justifications of the Law Commission are still applicable in the present day context. We take the view that since the internet permeates most aspects of public and private life nowadays, there is all the more a need to ensure the integrity of computer systems and networks against unauthorised access. The recent news that the Cyberport and the Consumer Council have fallen victim to hackers show that there is no room for complacency in cyberspace.[23]

2.31 For the reasons set out above, we maintain our view that mere unauthorised access to program or data should constitute an offence.

***Statutory defence of reasonable excuse — Whether any activities should be explicitly included in the definition of "reasonable excuse", and whether a non-exhaustive list of statutory examples should be given***

2.32 As the CFA explained in *HKSAR v Ho Loy*,[24] the expression "without reasonable excuse" (whether as a defence or an element to be proved by the prosecution) frequently occurs in statutes, and the question of whether or not an excuse is reasonable will be determined in the light of the particular facts and circumstances of an individual case.[25] We are of the view that any

---

19 Same as above, at para 1.37.
20 Same as above, at para 1.37.
21 Same as above, at para 1.37.
22 Same as above, at para 3.2.
23 In August 2023, a ransomware group reportedly blackmailed Cyberport after hacking its computer system. A sizeable amount of personal data, including bank account details, identity card numbers and details of staff identity cards are leaked and subsequently exposed on the dark web. Two weeks later, the Consumer Council also fell victim to hackers and the stolen data included information of employees and job applicants. See SCMP Editorial, "*Hong Kong's Cyberport hack sends reminder to be alert*" (16 Sep 2023), and "*消委會:遭黑客入侵7小時 盜取員工、月刊戶等資料 被要求交50萬美元贖金*", Sing Tao Daily (22 Sep 2023).
24 (2016) 19 HKCFAR 110, FACC 7/2015 (date of judgment: 23 Mar 2016).
25 Same as above, at 127 (para 37).

attempt to provide an interpretation of "reasonable excuse" in the cybercrime legislation or to illuminate the legislative intent (eg formulating a list of examples of "reasonable excuse") may run the risk of narrowing the scope of the reasonable excuse defence. In cases where a defendant's act or conduct deviates from what is described in the statutory examples, there is a risk that the court may rule against the defendant. To leave the scope of the term as wide as possible, we therefore recommend that "reasonable excuse" should be left undefined.

2.33 In addition, we observe that conceptually speaking, a "reasonable excuse" exculpates a defendant from liability, but does not justify the defendant's conduct. Hence, the notion of "reasonable excuse" does not sit well with the legitimate purposes that should not be regarded as contravention of the law in the first place. Thus, instead of weaving the legitimate activities into the reasonable excuse defence, we consider that the preferred approach is to express them as statutory defences, ie make it clear that those activities do not constitute a crime.

2.34 Accordingly, we recommend that specific defence(s) should be provided alongside the reasonable excuse defence to exclude those types of behaviour that plainly should not, in our view, be regarded as illegal. This will dispel the public's doubt as to whether certain activities would fall within the ambit of the reasonable excuse defence, which may serve as a fall-back option when the specific defences proposed by us do not apply. This approach also provides clarity and quells concerns over any ambiguities in the law. We shall explain our recommended specific defences in detail in the latter part of this Chapter.[26]

### *Access to program or data by law enforcement agencies*

2.35 Some Respondents, including Government-related bodies and business bodies, sought clarifications as to whether law enforcement agencies ("**LEAs**") which access computer program or data (eg those stored in a suspect's mobile phone) with or without warrant for criminal investigation purposes, and business operators who access such program or data (eg the personal data of a data subject) for law enforcement purposes, would be exempted from criminal liability.

2.36 We observe that *Sham Wing Kan v Commissioner of Police*[27] has laid down clear guidelines for LEAs in respect of searching the digital contents of a mobile phone found on an arrested person. As decided by the Court of Appeal, a magistrate can issue a warrant under section 50(7) of the Police

[26] Paras 2.63 to 2.102 below.
[27] [2020] 2 HKLRD 529, CACV 270/2017 (date of judgment: 2 Apr 2020).

Force Ordinance (Cap 232)[28] to authorise a search of the digital contents of a mobile phone or other electronic devices.[29] In the case of a warrantless search, the scope and purpose of the search must be incidental to the arrest in question. A police officer must have a reasonable basis for having to conduct a warrantless search immediately as being necessary (i) for the investigation of the offence(s) for which the person was suspected to be involved (including the procurement and preservation of information or evidence connected with such offences), or (ii) for the protection of the safety of persons.[30] Moreover, the officer should limit the scope of the detail examination of the digital contents to relevant items by reference to the criteria set out above and make an adequate written record of the purpose and scope of the warrantless search.[31]

2.37 Since the Access Offence does not intend to affect any lawful activities conducted by LEAs, we recommend adding "*without lawful authority*" as an element of the Access Offence. Whether "*lawful authority*" exists in a particular case is a question of objective fact. If a police officer has obtained a search warrant issued by a magistrate for conducting a search on a mobile phone or other electronic devices, or has a reasonable basis for conducting a warrantless search on these devices such that the requirements laid down in *Sham Wing Kan* are satisfied, there is "*lawful authority*" for the access to program or data. In the absence of a search warrant or reasonable basis, the situation would be analogous to situations where evidence was obtained by LEAs illegally (eg by coercion or deception). In such circumstances, the admissibility of the relevant evidence may be subject to challenge and the responsible LEA officers may face criminal investigation and, when there is sufficient evidence and the public interest so warrants, criminal prosecution. With or without lawful authority, access to program or data made in exigent situations may, in its own right, fall within the reasonable excuse defence. Therefore, even for law enforcement purposes, we consider it appropriate that access to program or data without warrant, when it cannot be justified, should constitute the Access Offence.

### *The aggravated offence is appropriate*

2.38 Regarding the suggestion that the aggravated offence is "*overly difficult to prove*",[32] we are confident that our courts can make rulings on the state of mind of a defendant by drawing inferences from the circumstances of individual cases as this is the judgement that they have to make day in and day out. Besides, pursuant to the Prosecution Code, there must be "*legally*

---

28 Section 50(7) of the Police Force Ordinance (Cap 232) provides that whenever it appears to a magistrate that there is reasonable cause to suspect that there is in any place any article or chattel which is likely to be of value (whether by itself or together with anything else) to the investigation of any offence that has been committed, or that is reasonably suspected to have been committed or to be about to be committed or to be intended to be committed, the magistrate may by warrant directed to any police officer empower him to search for and take possession of such article or chattel.

29 See fn 27 above, at paras 34, 163, 166 and 218(a).

30 See fn 27 above, at paras 187 and 218(b).

31 See fn 27 above, at paras 188, 199, 218(c) and (d).

32 Para 2.13 above.

*sufficient evidence to support a prosecution*",[33] and the test is "*whether the evidence demonstrates a reasonable prospect of conviction*".[34] Thus, it is likely that the prosecution would lay a charge for the aggravated offence only when the more serious crime has actually been committed, or when there are sufficient or compelling circumstantial evidence in a given case which enables inferences to be drawn that the defendant intends to commit or facilitate the commission of a further offence (where that aggravated offence has yet to be committed). It is also possible to charge an inchoate offence, ie attempt to commit the aggravated offence. For these reasons, the perceived difficulty of proving the aggravated offence may be more apparent than real.

2.39 That said, we do not rule out the possibility that the prosecution would fall back on the summary offence proposed under Recommendation 1(a) if confronted with real difficulty in establishing the aggravated offence (as suggested by the Respondent). This in turn justifies the need to retain the summary offence of mere unauthorised access.

2.40 It is also important to note that, in any event, there is always a duty on the part of the prosecution to decide on the venue for trial in respect of the many indictable offences (whether created by statute or under the common law) that are triable summarily. The key factors to be taken into account by the prosecution include the gravity of the allegations, the general circumstances of the case and the likely sentence upon conviction.[35] Thus, although the aggravated offence is indictable, the prosecution may elect to have the offence tried summarily in the Magistrates' Court if the circumstances of the case so warrant.

### *The overlap of offences*

2.41 Certainly, every act could be covered by more than one statutory provision or offence. As unlawful acts may occur in different contexts, we think that some overlap in our laws is acceptable. Pending the enactment of the proposed cyber-dependent crimes, it does not seem meaningful to speculate how the prosecution will handle cybercrime cases in future. This is especially so when one is debating the merits of the bespoke cybercrime legislation vis-à-vis S161 without reference to any factual background of a criminal case.

---

33 Department of Justice, Hong Kong Special Administrative Region, *Prosecution Code* (2013), at para 5.4.

34 Same as above, at para 5.5.

35 Same as above, at para 8.4. Other factors include the issues likely to be in dispute, whether or not issues arise for determination that require the application of community standards and/or values, the public importance of the proceedings and any aggravating and mitigating factors.

***Whether "access", "authorised / unauthorised" access, "computer network" and "data" should be defined***

2.42 As explained in the Consultation Paper,[36] the Sub-committee has considered whether "computer" should be given a statutory definition with reference to the *Draft United Nations Convention on Cooperation in Combating Cybercrime* prepared by the Russian Federation ("**Russian Convention**"), which defines "information and communications technology ('ICT') device" to mean "*an assemblage (grouping) of hardware components used / designed for automatic processing and storage of electronic information*".[37] The Sub-committee noted the following extract from the judgment of the Court of First Instance in *律政司司長 訴 王嘉業*[38] and reasoned that the court's view applies to the proposed cyber-dependent offences as well:

> *"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.*
>
> *…*
>
> *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."*[39]

2.43 We agree with the Sub-committee's view. With the advent of the internet of things, criminals can potentially target more and more devices in the coming 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 or "ICT system" in the UN Convention[40]) in practice as defendants may, especially as time passes since the introduction of such statutory definition, attempt to make every technical

---

36 At paras 2.93 to 2.95.

37 Article 4(o).

38 [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).

39 Same as above, at 621-622 (Barnabas Fung J).

40 The UN Convention instead seeks to define what will be regarded as "ICT system". Under article 2(a) of the Convention, "ICT system" means "*any device or group of interconnected or related devices, one or more of which, pursuant to a program, gathers, stores and performs automatic processing of electronic data*". For details about the UN Convention, see paras 1.6 to 1.8.

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.

2.44 As a business group rightly pointed out in its submissions, computer-related acts, such as "access" and "interception", can evolve with technological developments. New means of accessing computer program or data may emerge from time to time. Thus, it would be more appropriate not to define "access" in rigid terms, but to give "access" its ordinary meaning so as to attain the purpose of the proposed offence to address threats to, and attacks against, the security of computer systems.

2.45 Furthermore, we are inclined to think that whether or not there exists authorisation is a fact-sensitive question to be ruled by the court according to the circumstances of an individual case, and that a specific definition of "unauthorised" would run the risk of outlawing some commonly accepted or customary internet practices which our proposal intends to tolerate on the grounds that authorisation to access program or data is impliedly granted by the online user (see paragraphs 2.25 and 2.26 above).

2.46 For the reasons above, we remain in favour of leaving terms such as "access", "authorised / unauthorised access", "computer" and "computer system" undefined. In any case, should our recommendations be implemented by the Government, this issue may be further explored by the Law Draftsman during the legislative stage.

## Conclusion on Recommendation 1

2.47 For the reasons set out above, we conclude that Recommendation 1 can be retained and further clarified as follows:

**Final Recommendation 1**

**We recommend that:**

**(a) Subject to a statutory defence of reasonable excuse, unauthorised access to program or data without lawful authority should be a summary offence under the new legislation.**

**(b) The *mens rea* of the proposed offence are that:**

**(i) the defendant intends to secure access to the program or data, or intends to enable such access to be secured; and**

**(ii) the defendant knows that the intended access to the program or data was unauthorised when he makes the access.**

**(c) 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.**

**(d) The proposed provisions of the new legislation should be modelled on sections 1, 2 and 17 of the Computer Misuse Act of England and Wales.**

## Responses to the Sub-committee's Recommendation 2

2.48 Next, we shall turn to the consultation questions in Recommendation 2 of the Consultation Paper, which has several parts, namely:

> "*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?*

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

***Comments from Respondents who supported a specific defence for the cybersecurity industry***

2.49 An overwhelming majority of the Respondents supported Recommendation 2. Those in favour included legal professional bodies, tertiary institutions, information technology-related bodies, business groups and Government bodies. The major reasons given by them are set out below:

(a) Many Respondents saw the value of the work undertaken by white hat hackers and other cybersecurity professionals in detecting cybersecurity threats and vulnerabilities. In their view, a wide range of persons can benefit from white hat hackers' work. For instance, the work of cybersecurity experts can reveal potential vulnerabilities or security defects in electronic services or products, which facilitates safer and fairer online consumer experiences.

(b) If white hat hacking is performed properly and well-regulated, it would benefit Hong Kong by enhancing cybersecurity and promoting a strong and robust cybersecurity industry in Hong Kong, thereby establishing Hong Kong as a trusted place for sourcing cybersecurity expertise.

(c) A defence or exemption for unauthorised access would be essential for promoting good-faith security research, as well as facilitating the introduction of new technology into Hong Kong.

***Comments from Respondents who opposed a specific defence for the cybersecurity industry***

2.50 A few Respondents, including three information technology-related bodies and an individual, opposed the idea of providing a specific defence for persons working in the cybersecurity industry. One information technology-related organisation suggested that a defence exclusively for such

accredited persons would effectively create a "*privileged class*" who would be exempted from criminal liability regardless of the intention of the actor, so the specific defence or exemption should apply to everyone, but not only to persons accredited by a recognised professional or accreditation body.

2.51 On the other hand, another organisation in the information technology sector observed that when institutions commission cybersecurity services (eg network scanning), they usually enter into written contracts that define the scope of access by the cybersecurity service provider. For this reason, it may not be necessary to enact any specific defence or exemption for unauthorised access.

***Should an accreditation regime be introduced?***

2.52 In line with the general consensus that a specific defence or exemption for unauthorised access is desirable, a clear majority of the Respondents comprising Government departments, information technology-related bodies and business organisations agreed that an accreditation regime should be put in place.

***Comments from Respondents who supported an accreditation regime***

2.53 Proponents of an accreditation regime, including the Consumer Council, pointed out that the advantage of an accreditation regime is that it would provide a mechanism for certifying cybersecurity professionals who may then be identified with ease to determine whether the statutory defence or exemption applies. The Council suggested in its response that:

> *"… consideration be given to a statutory regime with licensing or accreditation criteria, such as 'fit and proper' requirement and continuing education requirement. In view of the constantly changing accreditation landscape as identified by the Sub-committee, the accreditation or licensing body may publish guidelines, circulars and codes of practice in response to those changes. The cybersecurity industry should be fully consulted on the administrative and operational issues of the accreditation regime.*"

2.54 Meanwhile, a number of information technology-related bodies agreed that the establishment of an accreditation body and a properly recognised cybersecurity profession would bring long-term benefits to Hong Kong.

2.55 The Respondents have proposed various ways of recognising practitioners in the cybersecurity industry. Apart from the statutory regime

suggested by the Consumer Council above, the Hong Kong Federation of Women Lawyers Limited ("**HKFWL Ltd**") opined that the accreditation criteria may be set out in the rules of the accreditation body administratively. In its view, this would make it easier to amend the accreditation criteria to keep pace with any change in technical requirements. Alternatively, a few information technology-related bodies thought that a registration system may be established for cybersecurity practitioners to register themselves before conducting penetration tests.

2.56 It is also noteworthy that the Law Society of Hong Kong commented that whether Hong Kong should have an accreditation regime should be a policy matter for the Government. This professional body pointed out that certain operational details of an accreditation regime would have to be ironed out:

> "*There should be a full consultation by the Government with stakeholders and the industry … It is helpful to consider questions such as the following (which are not exhaustive): if an accreditation body is set up, would a certificate issued by the accreditation body serve as a defence to the charge under this offence? If yes, to what extent and how does it operate? Is that defence of certification separated from other defences an accused is entitled to? On the other hand, could law enforcement agencies go beyond the certificate issued by the accreditation body and investigate into the alleged unauthorized access?*"

2.57 In respect of the details of the accreditation system, we have received helpful feedback from the Respondents. An information technology-related body opined that the body to be established to oversee accreditation or registration should have the power to deregister any individuals who violate or otherwise fail to meet the ethical and professional standards of the profession, provided that due process is in place.

2.58 In addition, an individual with years of experience in the cybersecurity field observed that a list of information of cybersecurity professionals can be maintained to keep track of the persons' qualifications, and the list should be organised into various specialties in cybersecurity. Nevertheless, this Respondent cautioned that:

> "*the inspection of the details of certain special streams, including experts in the fields of forensics and investigation, cryptanalysis, as well as zero day vulnerability researchers, should be restricted so as to safeguard the personal safety of the relevant cybersecurity professionals*".

2.59 Last but not least, a business group commented that any accreditation regime introduced in Hong Kong should not be over-complicated lest it would impede the development of the information technology industry.

***Comments from Respondents who opposed an accreditation regime***

2.60 While the majority of the information-technology related bodies which responded to Recommendation 2 agreed with the introduction of an accreditation regime, two of them objected to this proposal for the following reasons:

(a) Both technology and the cybersecurity profession evolve quickly. Accredited cybersecurity programmes are made available by service providers, software companies and cybersecurity bodies from time to time. An accreditation regime, particularly one that is based on statute, cannot adapt to changes quickly.

(b) An accreditation regime would likely cause challenges in recruiting qualified talent for working in the information technology industry in Hong Kong. A dearth of cybersecurity professionals may unintentionally limit the protection of local netizens.

(c) There has been an increase in open-source software, which allows non-security professional users to modify or enhance the software for the benefit of the community. Requiring accreditation may limit computer hobbyists' participation in identifying potential cybersecurity threats.

## Our analysis and response

2.61 Since the consultation questions in Recommendation 2 concern the defence or exemption for unauthorised access for cybersecurity purposes, we shall discuss the cybersecurity defence first before turning to other specific defences for the Access Offence.

2.62 In the Consultation Paper,[41] the Sub-committee has articulated the meaning of "cybersecurity" with reference to the following academic text, which is useful to recapitulate here:

> "*Cybersecurity refers to the procedures that are taken to protect computers, networks and programs from a cyberattack or acts of*

[41] At para 2.111.

*cybercrime (e.g., viruses, malware or ransomware). It is also referred to as information technology security.*"[42]

### *Specific defence for accredited cybersecurity practitioners*

2.63 The majority of the information technology bodies which made submissions on Recommendation 2 were receptive to the proposal of accreditation regime since this could elevate the information technology profession. We trust that it would be reasonable and pragmatic to create a specific defence for a defined category of persons within the information technology industry. While some Respondents may think that a specific defence would elevate cybersecurity professionals into a privileged class, we wish to point out that the defence in effect subjects cybersecurity professionals and, for that matter, anybody else to a new regulatory regime under which only those so accredited may be engaged in cybersecurity services in such a way which may involve unauthorised access. Viewed from this perspective, the defence actually accords obligations on anyone, including those from the information technology profession, who wish to perform unauthorised access including in situations where implied authorisation cannot be shown.

2.64 We propose that there should be a specific defence or exemption for accredited cybersecurity practitioners who act for a genuine cybersecurity purpose. The defendant's purpose and conduct must be reasonable having regard to all the circumstances, which denotes an objective standard. In the ensuing paragraphs, we will explain our thinking behind the individual elements of our recommendation.

#### *(i) Accredited or licensed cybersecurity practitioners*

2.65 Given the level of intrusion of access to program or data made for cybersecurity purposes and the broad notion of cybersecurity purposes, we consider that access for cybersecurity purposes should only be made by licensed or accredited practitioners. This implies that the persons who avail themselves of the defence are expected to possess a certain level of both professional expertise and standard of integrity. In other words, not every person who claims himself to be a cybersecurity professional or practitioner can mount the specific defence for access for cybersecurity purposes.

2.66 As the majority of the Respondents supported the introduction of an accreditation regime, institutionalising those from the information technology industry who are involved in cybersecurity work would accord better protection to all stakeholders (ie the cybersecurity profession, those who wish to engage its services and the general public alike) and make the law more certain. Thus, we take the view that there should be an independent system for accrediting cybersecurity practitioners and overseeing their disciplinary matters. An

---

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

accreditation regime complemented by the specific defence for access for cybersecurity purposes will not only make the information technology industry more professional, but will also guard cybersecurity professionals against liability of the Access Offence.

*Details of the accreditation regime to be determined by the Government*

2.67 Having said that, we are aware that cybersecurity talent is in short supply in Hong Kong and the introduction of an accreditation system may cause difficulties in recruiting talent in the information technology sector, intensify competition in the industry and drive up the cost of cybersecurity services.

2.68 We agree with the Respondents that an accreditation regime may be implemented in different ways. For instance, a statutory authority might be designated for accrediting cybersecurity professionals. In this regard, a stricter accreditation system would likely affect the supply and the cost of cybersecurity professionals. On the other hand, it might be possible to adopt a more relaxed approach by accrediting persons who are members of reputable information technology professional bodies or international information technology associations. Depending on the approach taken, the impact of the accreditation regime on the cybersecurity industry and cyberspace users would vary.

2.69 The detailed implementation issues of an accreditation regime are essentially ones of Government policy. It would be appropriate to leave the details of the implementation issues (including the requirements for accreditation as a cybersecurity professional, record-keeping obligations on the part of the practitioners, questions as to whether the accreditation body is to be managed by the information technology industry or other authorities, and how the accreditation regime should be financed) to the Government. To facilitate the Government's consideration of the accreditation regime, we have set out our observations on the proposal of accreditation and its potential implications in this Report.

2.70 We envisage that, if the Government is inclined to establish a cybersecurity accreditation body, it may consider, if it does not wish to create a bespoke authority for this purpose, designing a framework by which one or more pre-existing organisations, which are self-regulatory professional bodies and professional associations, are designated to carry out that function similar to the Law Society of Hong Kong, the Hong Kong Bar Association and the Hong Kong Society of Notaries in that they are entrusted with the statutory duty to oversee the conduct of solicitors (and foreign lawyers), barristers and notaries public respectively to maintain their standards. Just as legal practitioners would face disciplinary sanctions for sub-standard performance or unethical conduct, cybersecurity professionals would face disciplinary sanctions if they violate any codes of conduct promulgated by the accreditation body.

*(ii) Genuine cybersecurity purpose*

2.71 We consider that the accreditation or identity of the defendant should not be a conclusive determinant for the application of the specific defence for access for cybersecurity purposes. It is important that the accredited person makes the access to program or data for a genuine cybersecurity purpose. This has been highlighted in the observation by the HKFWL Ltd and another business group:

> *"Whilst we agree that the accreditation by a recognized professional or accreditation body provides prima facie evidence that the person accessing program / data has a justifiable reason for doing so, it is the actual act which needs to be examined and accreditation itself is not a complete defence. The critical issue to prove in order for the exemption or defence to be successfully established is that the unauthorized access was made for cybersecurity purpose, rather than that the unauthorized access was made by an accredited person."*

2.72 The requirement of a "genuine cybersecurity purpose" would mean that while an accredited cybersecurity practitioner who accessed computer program or data for genuine cybersecurity purposes could plead the specific defence for access for cybersecurity purposes, a practitioner who accessed the data on the phone of his daughter could not raise the same defence. Instead, he would have to fall back on the defence of access for protecting the interests of a child (discussed in paragraphs 2.75 to 2.89 below).

*(iii) The defendant's conduct must be reasonable having regard to all the circumstances*

2.73 To further tighten the defence for access for cybersecurity purposes, we propose to incorporate the requirement of "reasonableness" into the defence. By adopting reasonableness as the guiding principle, we believe that the conditions of the specific defence for access for cybersecurity purposes would provide safe and consistent parameters that delineate the conduct that would be acceptable to a reasonable person. The question of "reasonableness" is highly facts-sensitive. If, for example, a computer owner or data owner withholds authorisation to an accredited cybersecurity practitioner (who may be a former employee or a known competitor of the owner) for accessing the owner's program or data, but the cybersecurity practitioner still makes the access, then cogent explanations or justifications for the practitioner's access will have to be put forward so as to satisfy the court of the "reasonableness" requirement (and hence making out the proposed cybersecurity defence). If any code of ethics is promulgated by the accreditation body, the court may certainly make reference to the code when assessing the reasonableness of a defendant's conduct.

2.74 This "reasonableness" requirement also seeks to align the specific defence for access for cybersecurity purposes with the defence to the proposed offences of illegal interference with computer data and computer system, which we will discuss in Chapters 4 and 5 of this Report.

### *Other specific defences to the Access Offence*

#### *Access for protecting the interests of a child*

2.75 At the media interviews that Members of the Sub-committee attended after the publication of the Consultation Paper, questions were raised as to whether a parent who viewed the contents in the phone of his or her child would commit the proposed offence. In the absence of a specific defence on parental control, a parent accused of the proposed offence would have to rely on the general defence of reasonable excuse.

2.76 Among the submissions received, a local charity, namely Mother's Choice, highlighted the specific vulnerabilities faced by children who surf online. Referring to a study conducted by the University of Hong Kong, this Respondent cited various types of cyber abuse experienced by young people: 40% of teenagers in Hong Kong are exposed to unwanted sexual online content; one in ten teenagers have encountered online sexual harassment, and one in five teenagers are subject to cyberbullying.

2.77 Therefore, this Respondent opined that the Sub-committee should consider legislative proposals that "*prevent children from accessing materials of inappropriate, abusive or harmful contents from the internet, digital and streaming media*". Its acknowledgment of parental monitoring on children's internet use is further encapsulated in the following observations:

> *"We recognize the limited knowledge and skills among the support system for children including parents, individuals and professionals surrounding the topic of cyber safety and security. We recommend that all stakeholders working with vulnerable children who are at risk, should be equipped and empowered to prevent, respond to and report online risks. Preventing, responding to and reporting online child protection issues are key to ensuring the safety and welfare of the vulnerable in society".*

2.78 Similarly, the Legal Aid Department suggested that some exemptions should be in place to allow parents to access their children's computers for protection of their interests (eg in case cyberbullying takes place).

2.79 While children have a general right to privacy under Article 16 of the United Nations Convention on the Rights of the Child ("**UNCRC**"), which

continues to apply to Hong Kong after 1997,[43] we believe that the vulnerability of children to dangers in cyberspace justifies actions on the part of parents to safeguard the well-being of their children. For parents raising children in a world steeped in online activities and internet connection, the practicable actions might include accessing the mobile phone or computer of a child to find out, for example, the persons who are in contact with the child on social media platforms or messaging apps.

2.80 In this connection, it is noteworthy that the Office of the Privacy Commissioner for Personal Data ("**PCPD**"), whose mission it is to promote the protection and respect for personal data privacy, has published a host of practical tips to parents and teachers for helping children under their care to protect themselves in the online environment.[44] One of the suggestions from the PCPD is to explore parental controls. The PCPD noted that some online platforms or systems offer parental controls that allow parents to monitor or configure the settings to protect children, especially younger ones, from undesirable contents or contacts. Besides, the PCPD has taken the position that parents and teachers "*should alert children of the potential dangers of personal safety and loss of property when communicating online*".[45]

### *Our analysis*

2.81 In sum, it seems clear that parental control is a social norm accepted in Hong Kong and our society recognises the role of guidance played by parents in the use of the internet. To attain the objective of child protection, we find it sensible for the new cybercrime legislation to explicitly carve out access for the purpose of protecting the interests of children under a certain age from the Access Offence. We appreciate that the specific defence may diminish the privacy right of children, but amid the high internet penetration rate among young children, we consider that the existence of the defence would be consistent with the principle of protecting the interests of children.

#### *Age of the child*

2.82 Under local legislation, persons under the age of 16 generally cannot give consent to sexual contact as a matter of Hong Kong law.[46] As a

---

43 See the pamphlet published by the Constitutional and Mainland Affairs Bureau of the Government of the Hong Kong Special Administrative Region in March 2009, at 3. Article 16(1) of the UNCRC provides that "*No child shall be subjected to arbitrary or unlawful interference with his or her privacy … or correspondence …*".

44 Office of the Privacy Commissioner for Personal Data, *Children Online Privacy: Practical Tips for Parents and Teachers* (2015), available at https://www.pcpd.org.hk/english/resources_centre/publications/files/leaflet_childrenonlineprivacy_e.pdf (accessed on 1 Nov 2025).

45 Same as above.

46 Eg pursuant to s 122(2) of the CO, a person under 16 cannot in law give any consent which would prevent an act being an indecent assault. For sexual intercourse, under s 124(1) of the CO, it is an offence to have unlawful sexual intercourse with a girl under 16. Besides, s 146(1) of the CO provides that it is an offence to commit an act of gross indecency with or towards a child under 16, or to incite a child under 16 to commit such an act with or towards another person. Under s 146(2), it shall not be a defence to prove that the child consented to the act of gross indecency.

"child" is defined under Article 1 of the UNCRC as a person below 18, we have considered whether, in the cybercrime context, it is necessary to pitch the age of the child at 18 for the purpose of this specific defence. In our view, compared with the right to autonomy over a person's body, the right to privacy is a lesser right. As our laws have determined that persons below 16 would not have autonomy over their bodies (in the sense of being able to give valid consent for sexual contact), there does not seem to be any sufficient justification for the specific defence to the Access Offence to prescribe a different age threshold in the cybercrime context. Overall, we consider that the age of 16 would offer sufficient protection and this threshold is largely consistent with other existing laws in Hong Kong.

*The access to program or data should be reasonable*

2.83 As with the defence for access for cybersecurity purposes, we are of the view that abuse of the specific defence could be avoided by restricting the access to program or data to what is reasonably necessary for protecting the interests of a child, having regard to all circumstances of the case. By limiting both the purpose and the extent of the access, the court would have more evidential room to determine whether an access is excessive. The court would ultimately assess the actions of a defendant by considering all the relevant factors in a particular case to ensure that he has not overstepped the boundaries of what should be done to exercise control over the child.

*Scope of the defence*

2.84 We have considered in detail two options of formulating the proposed defence. The first option is broader and applies to access to program or data made for the purpose of protecting the interests of the child, while the second option is narrowed to access for the purpose of preventing physical, emotional or psychological harm to a child.

*(i) Access to program or data for protecting the interests of a child*

2.85 The major argument in support of this wider defence is that it could embrace a myriad of circumstances where a parent may wish to access the child's program or data (eg to find out whether a child has accessed pornographic or violent online contents). A restrictive defence may make parents feel that they are deprived of their parental right because the cybercrime legislation prohibits them from doing what they otherwise may do in the course of raising their children. Coupled with the requirement that the access must be reasonable, proponents of this wider defence are confident that the court would not only consider a parent's subjective belief that the access is necessary for protecting the interests of children, but would also objectively assess the conduct of the parent to determine whether the access is justifiable. This would ringfence the scope of the access to children's program or data and prevent parents from making excessive inroads into children's right to privacy.

*(ii) Access to program or data for preventing physical, emotional or psychological harm to a child*

2.86 On the other hand, we appreciate that a narrower defence may be preferable due to other practical considerations. A wide defence may adversely affect parent-child relationship and operate to the detriment of family harmony. In post-divorce cases, a relatively narrow defence might prevent a parent from manipulating a child into making complaints about the other parent who sought to exercise parental responsibility or control over the child. Besides, the right to privacy has been given more weight than ever before. As a trade-off to according greater respect to children's privacy, other competing rights (eg the right to exercise parental control by accessing the child's computer program or data) would have to be diminished or restrained.

2.87 Eventually, a narrow majority in the Sub-committee preferred the first (wider) option, ie access to program or data for protecting the interests of a child. As the Government may further consult the public should it decide to implement the Sub-committee's recommendation, and the content of the new cybercrime legislation would eventually be decided by the legislature, we consider that the issue will be best left for the decision of the Government having regard to the sentiments in society.

*The defence should not be relationship-dependent*

2.88 In line with the rationale behind the defence to protect the interests of a child, we further propose that the defence should be predicated on the subjective purpose of the person who sought access to the child's program or data. In reality, a child is not necessarily well protected in a stable and safe environment as we may hope. It is not uncommon that a parent or guardian neglects or fails to discharge his duty to protect or take care of his child's well-being. We also conceive that even if a child is well taken care of by his parent or guardian, there may still be a myriad of circumstances in real life where the protection of the child's interests warrants the intervention of a person who is a stranger to the child. For instance, where a person finds a child in a precarious situation (eg a child who has lost his way), it seems reasonable to allow the person to make access to the program or data in the child's phone or electronic device without being held criminally liable.

2.89 The above considerations squarely demonstrate that it is the honest purpose of a person who makes unauthorised access to a child's program or data to protect the child's interests, rather than the relationship between the person and the child, that makes the unauthorised access justifiable. Not being dependent on the relationship between the child and the person who makes the access, the defence maximises the protection of the interests of children. We consider that the overriding requirement of "reasonably necessary for protecting" would serve to avoid abuse.

*Extending the defence to the protection of vulnerable persons*

2.90 Since an adult with mental disability may be prone to exploitation, we consider that the aforementioned specific defence for unauthorised access to program or data should be extended to the protection of vulnerable persons. As to how vulnerable persons should be defined, we find it helpful to refer to the clear definitions of "*mentally disordered person*" [47] and "*mentally handicapped person*"[48] in the Mental Health Ordinance (Cap 136) ("**MHO**"). According to section 2 of the MHO:

(a) "*mental disorder*" is defined to mean "*mental illness*", "*a state of arrested or incomplete development of mind which amounts to a significant impairment of intelligence and social functioning which is associated with abnormally aggressive or seriously irresponsible conduct on the part of the person concerned*", "*psychopathic disorder*",[49] or "*any other disorder or disability of mind which does not amount to mental handicap*", and "*mentally disordered*" is construed accordingly; and

(b) "*mental handicap*" means "*sub-average general intellectual functioning with deficiencies in adaptive behaviour*", and "*mentally handicapped*" is construed accordingly. Section 2 further defines "*sub-average general intellectual functioning*" to mean "*an IQ of 70 or below according to the Wechsler Intelligence Scales for Children or an equivalent scale in a standardized intelligence test*".

2.91 The court will be assisted, if need be, by expert evidence (say from registered medical practitioner or psychiatrist) when deciding whether the ingredients of the definitions cited in the preceding paragraph are proved to the requisite standard in a particular case. Hence, we propose that the specific defence for unauthorised access to program or data should be extended to protect the interests of a vulnerable person (ie a mentally disordered person or a mentally handicapped person as defined in the MHO). [50] This recommendation adds weight to our above conclusion that the defence should not be relationship-dependent. Likewise, the "reasonably necessary for protecting" requirement would also apply as in the case for protecting a child.

---

47 Under s 2 of the Mental Health Ordinance ("**MHO**"), a "*mentally disordered person*" means "*a person suffering from mental disorder*".

48 Under s 2 of the MHO, a "*mentally handicapped person*" means "*a person who is or appears to be mentally handicapped*".

49 "*Psychopathic disorder*" is defined to mean "*a persistent disorder or disability of personality (whether or not including significant impairment of intelligence) which results in abnormally aggressive or seriously irresponsible conduct on the part of the person concerned*".

50 This is in line with Final Recommendation 35 of the LRC Report on Review of Substantive Sexual Offences published in December 2019, which recommended that the new offences involving persons with mental impairment should apply to a mentally disordered person or mentally handicapped person (as defined in the MHO) whose mental disorder or mental handicap, as the case may be, is of such a nature or degree that the person is incapable of guarding himself or herself against sexual exploitation.

***Access for genuine research purposes***

2.92 A number of information technology related bodies which responded to the Consultation Paper suggested exempting access to program or data made for the purposes of research, analysis or testing tester-owned devices or targets performed in a controlled environment.

2.93 We agree that access to program or data made for research purposes (eg a researcher or cybersecurity practitioner ascertaining the number of unprotected computers in Hong Kong) should be a defence or exemption in addition to the defence to access for cybersecurity purposes. As such research could yield useful analysis or information, it would be reasonable to provide a specific defence for access to program or data for research purposes. We opine that the proposed defence, modelled on that for the various offences relating to child pornography under section 4(2)(a) and (3)(a) of the Prevention of Child Pornography Ordinance (Cap 579), may be formulated as access to program or data made for a genuine educational, scientific or research purpose.

2.94 To avoid abuse of the research defence, we propose that one of the requirements of this defence is that the access must be reasonable and no more than is necessary for achieving the educational, scientific or research purpose. This "reasonableness" requirement would serve as an objective yardstick for determining whether the access made by a defendant is proportionate or reasonable.

***The defences under section 64(2) of the Crimes Ordinance for the offences of illegal interference with computer data and computer system***

2.95 As will be discussed in Chapters 4 and 5 of this Report, the two defences under the existing section 64(2) of the CO ("**S64(2)**") are applicable to the offences of illegal interference with computer data and illegal interference with computer system ("**Interference Offences**") under Recommendations 6 and 7 of the Consultation Paper. It would be helpful to first set out the gist of the two defences under S64(2), which now applies to the offence of criminal damage (on which the two Interference Offences are proposed to be modelled).

2.96 S64(2) consists of two limbs. A defendant charged with criminal damage is treated as having a lawful excuse:

(a) if, at the time of the act(s) alleged to constitute the offence, the defendant believed that the person(s) whom the defendant believed to be entitled to consent to the destruction of or damage to the property had so consented, or would have so consented to it if the person(s) had known of the destruction or damage and its circumstances ("**consent defence**"); or

(b) if the defendant destroyed or damaged, or threatened to destroy or damage the property, or in the case of a charge under section 62, intended to use or cause or permit the use of something to destroy or damage the property, in order to protect property (whether belonging to himself or another), and at the time of the act(s) alleged to constitute the offence, the defendant believed—

(i) that the property was in immediate need of protection; and

(ii) that the means of protection adopted or proposed to be adopted were or would be reasonable having regard to all the circumstances ("**property protection defence**").

2.97 As interference with computer data and/or computer system would normally only occur upon access to program or data, we take the view that the consent defence and the property protection defence under the CO should likewise apply to the Access Offence.

*The consent defence under S64(2)(a)*

2.98 To explain this defence, we put forward a hypothetical scenario where a defendant logged into another person's computer and altered the data in the computer (eg a virus) in the belief that the latter person would consent to such alteration. The reasoning would be logically bizarre if the defendant were not liable for illegal interference with computer data (because of the availability of the consent defence), but was convicted of the Access Offence. For this reason, we take the view that uniform treatment should apply to the defences to the Access Offence and the Interference Offences. The detailed drafting of the defence provisions may be dealt with during the legislative stage.

*The property protection defence under S64(2)(b)*

2.99 Similarly, given that the property protection defence is available to the Interference Offences, we consider that a defendant should also be able to plead the same grounds of defence in the case of the Access Offence.

*Adding the reasonableness requirement into the defendant's belief*

2.100 Under the current S64(2)(a), the defendant's belief as to the existence of consent is entirely subjective. Section 64(3) of the CO provides that "*it is immaterial whether a belief is justified or not if it is honestly held*". Thus, as long as the court accepts that the defendant genuinely holds such belief, the defence will be applicable and no reasonable basis for the defendant's belief is necessary.

2.101 When transposing the defences under S64(2) to the new legislation, we propose to set a higher bar for the defence by incorporating an objective test into the consent defence and the property protection defence, ie:

(a) in the case of the consent defence, the defendant must reasonably believe that there was, or would be, consent to his access to the program or data; and

(b) in the case of the property protection defence, the defendant must reasonably believe that the property was in immediate need of protection.

2.102 In other words, we propose to disapply section 64(3) of the CO for the purposes of the Access Offence that we recommend for inclusion in the bespoke cybercrime legislation. The above adjustment would align the consent defence and the property protection defence with other specific defences that we recommend for the Access Offence above, ie all defences adopt the requirement of "reasonableness" as a matter of consistency. We believe this approach would avoid abuse of the defences, reflecting our guiding principle of balancing the rights of netizens and interests of persons in the information technology industry on one hand, and protection of the public's interest and right not to be disturbed or attacked when using their computer system on the other hand.

### *Access to program or data by non-security professionals*

2.103 Recommendations 2(b) and 8(b) of the Consultation Paper respectively invited the public's view as to whether there should be any defence or lawful excuse for access to program or data and interference with computer system conducted by non-security professionals. Examples of non-security professionals include 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.[51]

2.104 As we will explain in Chapter 5 of this Report,[52] we consider it unnecessary to provide any specific defence for non-security agents encountered in the day-to-day operation of cyberspace since practices commonly accepted in the use of cyberspace are allowed under the principle of implied authorisation if they are conducted on a scale that is ordinarily accepted by computer users. By the same token, specific defences need not be proposed for non-security professionals in the case of the Access Offence.

---

51 See Recommendation 8(b) of the Consultation Paper.
52 Paras 5.29 to 5.33.

## Conclusion on Recommendation 2

2.105 Summarising the discussion above, we recommend the defences for the Access Offence as follows:

**Final Recommendation 2**

**Apart from the statutory defence of reasonable excuse, we recommend that for the proposed offence of illegal access to program or data:**

**(a) There should be a specific defence for unauthorised access for cybersecurity purposes with the following conditions:**

**(i) The defendant must be an accredited cybersecurity practitioner (the details of the accreditation regime, which are essentially matters of policy, are best left to the Government's consideration);**

**(ii) The defendant must act for a genuine cybersecurity purpose; and**

**(iii) The defendant's conduct must be reasonable having regard to all the circumstances.**

**(b) There should be a specific defence for unauthorised access for the protection of the interests of a child under the age of 16 and a vulnerable person (ie a mentally disordered person or a mentally handicapped person as defined in the Mental Health Ordinance (Cap 136)):**

**(i) The defence is based on the subjective purpose of the person making the access to the program or data of a child or vulnerable person (ie for the protection of the interests of the child or vulnerable person), but not the relationship between the person and the child or vulnerable person.**

**(ii) The access to program or data made by a defendant must be reasonable having regard to all the circumstances.**

**(c) There should be a specific defence for unauthorised access for educational, scientific or research purposes. The access to program or data made by a defendant must be reasonable having regard to all the circumstances.**

**(d) The defences to the offences of illegal interference with computer data and illegal interference with computer system under section 64(2) of the Crimes Ordinance (Cap 200) ("S64(2)") should also be available to the offence of illegal access to program or data.**

**(i) The two defences under S64(2) cover situations where a defendant:**

**(1) accessed program or data in the belief that his act was, or would be, consented to; or**

**(2) accessed program or data in the belief that the property was in immediate need of protection, and the means of protection adopted was reasonable having regard to all the circumstances.**

**(ii) The defendant's belief under both the consent defence and the property protection defence must be reasonably held.**

## Responses to the Sub-committee's Recommendation 3

***Limitation period in summary cases***

2.106 Recommendation 3 deals with the limitation period that applies to a charge by way of summary proceedings for the five cyber-dependent offences proposed in the Consultation Paper:

> "*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).*"

2.107 Under section 26 of the Magistrates Ordinance (Cap 227) ("**MO**"), the limitation period for summary offences is generally six months from the time when the matter arose unless the relevant legislation prescribes otherwise.

2.108 The majority of the Respondents supported Recommendation 3. A business association observed that cybercrime cases are often complex and the prosecution would require more resources and time in deciding whether to proceed with a case. That said, it cautioned that the limitation period of two years should be regarded as a safety net for the more complex cases rather than the norm. A handful of Respondents, however, preferred not to "defer" the limitation period from six months to two years as a six-month period would encourage LEAs to deal with cybercrime cases more expeditiously and therefore better protect the interest of the public.

2.109 As the Sub-committee explained in the Consultation Paper,[53] the default limitation period under the MO 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.

2.110 We wish to clarify that Recommendation 3 only seeks to extend the limitation period to two years to ensure that the ensuing prosecution of an investigation of alleged offence(s) which cannot reasonably be completed within the default six months given the inherent complications is not time-barred, and not because of the lack of confidence that LEAs are capable of dealing with a cybercrime case as swiftly as is fair and possible. We therefore recommend retaining Recommendation 3.

**Final Recommendation 3**

**We recommend 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).**

[53] At para 2.122.

# Chapter 3

# Illegal interception of computer data

## Introduction

3.1 This Chapter discusses the responses regarding Recommendations 4 and 5 of the Consultation Paper. Recommendation 4 proposes the second cyber-dependent offence, namely illegal interception of computer data:

> "*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 [("**Model Law**")], including the mens rea (ie to intercept "intentionally").*"

3.2 As explained in the Consultation Paper,[1] among the relevant statutes in all of the jurisdictions examined, section 8 of the Model Law ("*Illegal interception of data etc.*") as adapted below is closest to what the Sub-committee had in mind in terms of a reference for Hong Kong:

[1] At paras 3.111 and 3.112.

*"A person who, intentionally without lawful excuse or authority, intercepts for a dishonest or criminal purpose by technical means:*

*(a) any transmission to, from or within a computer system; or*

*(b) electromagnetic emissions from a computer system that are carrying computer data;*[2]

*commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.*"

3.3 Broadly speaking, the offence of illegal interception of computer data would seek to:[3]

(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.

3.4 In today's world, interception of computer data can happen anywhere[4] 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"[5] or installing a spyware.

## Current Hong Kong law

3.5 As some of the Respondents' submissions commented on the inadequacies in the existing law, it would be useful to recap the key features of the current statutory regime before we address the responses.

---

2 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*".

3 Consultation Paper, at para 3.1.

4 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.

5 A backdoor is "*any method by which authorised and unauthorised users are able to get around normal security measures and gain high level user access on a computer system, network, or software application.*" See https://www.malwarebytes.com/backdoor (accessed on 1 Nov 2025).

### *Interception of Communications and Surveillance Ordinance (Cap 589) ("ICSO")*

3.6 As the Sub-committee explained in the Consultation Paper,[6] the emphasis of the ICSO is to regulate when and how law enforcement agencies ("**LEAs**"), ie public officers, can lawfully encroach on a person's right to private communication, eg by obtaining a "prescribed authorization"[7] for an intended interception of a communication or an intended covert surveillance. Besides, the ICSO only regulates the interception of a communication in the course of its transmission.[8]

### *Section 27(b) of the Telecommunications Ordinance (Cap 106) ("TO")*

3.7 Outside the context of law enforcement, section 27 of the TO provides as follows:

> *"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."*

3.8 As the Sub-committee pointed out in the Consultation Paper,[9] section 27(b) is not a bespoke provision against interception of computer data. The provision presupposes a telecommunications context and does not apply well to cyberspace. 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, which is data that provides information about other data.

## General responses to the Sub-committee's Recommendation 4

### *Comments from Respondents who supported Recommendation 4*

3.9 A clear majority of the Respondents who expressly indicated their stance supported Recommendation 4. Those in favour included legal

---

6 At paras 3.7 and 3.9.
7 Interception of Communications and Surveillance Ordinance (Cap 589) ("**ICSO**"), s 2.
8 See the definition of "intercepting act" in s 2(1) of the ICSO.
9 At para 3.14.

professional organisations, information technology-related bodies, tertiary institutions, business groups and Government departments.

3.10 Amongst the positive responses received, the Office of the Privacy Commissioner for Personal Data ("**PCPD**") commented that the creation of the offence of unauthorised interception of computer data carried out for a dishonest or criminal purpose will "*help to deter data security breach, which has become increasingly common*". It supported the introduction of the interception offence on the basis that its policy intent is to "*protect people's right to privacy of data communication".*

3.11 The Hong Kong and Mainland Legal Professional Association Limited supported the proposed offence and echoed the Sub-committee's analysis of the limitations of section 27 of the TO in paragraph 3.8 above. It further noted that the maximum penalty for contravening section 27 of the TO is rather light, ie only a fine at level 4 ($25,000)[10] and 2 years' imprisonment.

3.12 Other Respondents — information technology-related bodies and individuals — also agreed with the introduction of an offence of unauthorised interception of computer data, but stressed the importance of including "criminal purpose" or "criminal intent" as a constituent element of the offence.

### *Comments from Respondent who opposed Recommendation 4*

3.13 Only one information technology-related body opposed expanding the scope of computer offences. This Respondent was concerned that the proposed interception offence would bring potential uncertainties to the legitimate acts carried out by cybersecurity practitioners, such as network intrusion detection and penetration test, which may involve interception of computer data. It opined that even if defences are available for a defendant, the burden of proof should remain on the prosecution to prove the defendant's intention.

## Detailed Responses to the Sub-committee's Recommendation 4

### *The scope of the interception offence*

3.14 With regard to Recommendation 4(a) in the Consultation Paper, the PCPD commented that the "disclosure" and "use" of computer data apparently constitute different criminal acts that are separate and distinct from the act of "interception". It then made the following suggestion:

[10] Criminal Procedure Ordinance (Cap 221), Schedule 8.

"*Insofar as the policy intent is to outlaw the disclosure or use of computer data obtained as a result of the prior interception act, we suggest that be spelt out clearly in the legislation. Otherwise, the purview of the new offence may cover the disclosure or use of computer data which are not obtained from the interception.*"

***Whether the interception offence overlaps with the existing doxxing offences under the Personal Data (Privacy) Ordinance (Cap 486) ("PDPO")***

3.15 The PCPD further referred to section 64(1),[11] (3A)[12] and (3C)[13] of the PDPO, which provides for criminal offences in relation to doxxing. It noted the apparent differences between the *mens rea* requirements for the proposed offence of illegal interception of computer data and those for the existing doxxing offences, but opined that depending on the facts and evidence of a particular case, the relevant disclosure of personal data may constitute both the proposed interception offence and an offence under the PDPO at the same time.

***Whether the element "for a dishonest or criminal purpose" is sufficient or appropriate***

3.16 The Hong Kong Federation of Women Lawyers Limited ("**HKFWL Ltd**") agreed with Recommendation 4 and expressed the following view:

"*Consideration should be given [as to] whether any improper purpose should be included as well, such as whether there is a disclosure of personal or confidential data which may not amount*

---

11 Section 64(1) of the PCPO provides that "*A person commits an offence if the person discloses any personal data of a data subject which was obtained from a data user without the data user's consent, with an intent—*
*(a) to obtain gain in money or other property, whether for the benefit of the person or another person; or*
*(b) to cause loss in money or other property to the data subject.*" (emphasis added)

12 Section 64(3A) of the PCPO provides that "*A person commits an offence if the person discloses any personal data of a data subject without the relevant consent of the data subject—*
*(a) with an intent to cause any specified harm to the data subject or any family member of the data subject; or*
*(b) being reckless as to whether any specified harm would be, or would likely be, caused to the data subject or any family member of the data subject.*" (emphasis added)
Specified harm means harassment, molestation, pestering, threat, intimidation, bodily harm or psychological harm to a person, harm causing a person reasonably to be concerned for his safety or well-being, or damage to the property of a person (see s 64(6)).

13 Section 64(3C) of the PCPO provides that "*A person commits an offence if—*
*(a) the person discloses any personal data of a data subject without the relevant consent of the data subject—*
*(i) with an intent to cause any specified harm to the data subject or any family member of the data subject; or*
*(ii) being reckless as to whether any specified harm would be, or would likely be, caused to the data subject or any family member of the data subject; and*
*(b) the disclosure causes any specified harm to the data subject or any family member of the data subject.*" (emphasis added)

*to a crime, and may not involve dishonesty in the 'financial dishonesty' sense*".

3.17 However, this Respondent did not give any concrete example of culpable interception of computer data which may fall short of the threshold of "*a dishonest or criminal purpose*" set by Recommendation 4.

3.18 In addition, an information technology-related body raised the concern that technical security companies, such as providers of anti-virus solutions and other internet security firms, may monitor the network in order to discover signs of attacks or analyse network traffic. This Respondent explained that the nature of these activities may exhibit attributes of interception of computer data, but they do not necessarily target any specific organisation. It opined that interception of computer data should only be an offence if the act relates to an attack that is launched against one or more specific targets.

3.19 On the other hand, another information technology-related body opined that the requirement of "*dishonest or criminal purpose*" is sufficient for protecting the normal operation of online service providers. It agreed that the requisite *mens rea* should be intercepting for a "*dishonest or criminal purpose*" as described in Recommendation 4(a).

***Criminal liability of public officers who exercise law enforcement powers***

3.20 A Government department sought clarification of the Sub-committee's position towards the liability of public officers (eg members of LEAs) who intercept or access computer data in circumstances where the act exceeds the limits of an officer's authority. This Respondent suggested that:

> "*there may be occasions where a public officer acts in good faith but inadvertently exceeds the authority of any law enforcement power granted to him/her… [t]here is a strong public interest that a public officer should not be held criminally liable under such circumstances, for otherwise public officers may be tempted to take an overly risk averse approach to law enforcement …* "

***Interception that "exceeds authority"***

3.21 Two professional organisations, namely the HKFWL Ltd and the Hong Kong Women Professionals and Entrepreneurs Association ("**HKWPEA**"), suggested that unauthorised interception should include acts of interception that exceed authority. In this regard, the HKFWL Ltd specifically recommended adopting the concepts of "exceeding" authorisation as set out in the Stored Communications Act ("**SCA**") of the United States of America ("**USA**").

3.22 As mentioned in the Consultation Paper,[14] the main provision in the SCA 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.*"
>
> (emphasis added)

***Whether the interception offence should only protect private communication***

3.23 Regarding Recommendation 4(b)(i), an information technology-related body commented that the proposed interception offence should only protect private communication. In its opinion, "*communication in general is too broad in the cyberworld"* and the protection that the proposed offence intended to accord to the public "*may unnecessarily disturb proper communication*".

***Whether "interception" should be defined***

3.24 As mentioned in Chapter 2,[15] some business groups consider that the meaning of certain concepts, including "interception" and "access", should be clearly defined or explained to the public. They are concerned that the concepts may overlap and evolve in the light of technological developments.

---

14 At para 3.87.
15 Para 2.17 above.

## Our analysis and response

### *Refocusing the interception offence*

3.25 In the Consultation Paper,[16] the Sub-committee explained that it intended to prohibit unauthorised disclosure or use of "intercepted data", given that the subsequent disclosure or use of intercepted data may give rise to privacy concerns and other potential issues (for example, financial loss may occur to the holder of a credit card if its details intercepted during their transmission to the vendor in an e-commerce transaction are wrongfully used).

3.26 In the light of the PCPD's query on the scope of the proposed offence of illegal interception of computer data stated in paragraph 3.14 above, we have carefully reflected on the application of this offence. In our view, an offence based on unauthorised disclosure or use of "any data" (which is not limited to intercepted data) for a dishonest or criminal purpose may be too broad since the offence will essentially apply to all kinds of data encountered in our digital everyday life.

3.27 Furthermore, an offence on unauthorised disclosure or use of computer data, insofar as it involves personal data, is more a matter within the purview of the PCPD. We observe that in the most recent legislative amendment exercise in 2021,[17] the PCPD specifically focused on the doxxing offences in a bid to combat disclosure of personal data without consent.[18] The offences under section 64(3A)[19] and (3C)[20] of the PDPO require an intention to cause specified harm, or recklessness as to whether such harm would be caused. As the PCPD pertinently pointed out in its submissions, the *mens rea* for the doxxing offences is highly specific and confined in scope.

---

16 At paras 3.92 and 3.94.

17 The provisions on doxxing were added into the Personal Data (Privacy) Ordinance (Cap 486) through the enactment of the Personal Data (Privacy) (Amendment) Ordinance 2021 (Ord No 32 of 2021).

18 See the long title of the Personal Data (Privacy) (Amendment) Ordinance 2021.

19 Section 64(3A) of the PCPO provides that "*A person commits an offence if the person discloses any personal data of a data subject without the relevant consent of the data subject—*

*(a) with an intent to cause any specified harm to the data subject or any family member of the data subject; or*

*(b) being reckless as to whether any specified harm would be, or would likely be, caused to the data subject or any family member of the data subject.*" (emphasis added)

Specified harm means harassment, molestation, pestering, threat, intimidation, bodily harm or psychological harm to a person, harm causing a person reasonably to be concerned for his safety or well-being, or damage to the property of a person (see s 64(6)).

Pursuant to s 64(3B), the maximum penalty is a fine at level 6 (ie $100,000) and two years' imprisonment.

20 Section 64(3C) of the PCP*O* provides that "*A person commits an offence if—*

*(a) the person discloses any personal data of a data subject without the relevant consent of the data subject—*

*(i) with an intent to cause any specified harm to the data subject or any family member of the data subject; or*

*(ii) being reckless as to whether any specified harm would be, or would likely be, caused to the data subject or any family member of the data subject; and*

*(b) the disclosure causes any specified harm to the data subject or any family member of the data subject.*" (emphasis added)

Pursuant to s 64(3D), the maximum penalty is a fine $1,000,000 and five years' imprisonment.

3.28 Given the wide implications of a general offence of unauthorised disclosure or use of computer data, it would be prudent to study this topic in depth in Part Two[21] of our study before we express any settled view as to whether a new offence in this regard should be recommended, and if so, how. For example, further considerations may be given to whether such offence should be confined to "intercepted data" as some may hold the view that if a person discloses or uses computer data "*for a dishonest or criminal purpose*", the conduct should by itself be culpable, no matter whether the data was obtained by authorised or unauthorised interception, or any other means. Also, the interplay between such offence and the doxxing offences under the PDPO may worth further consideration.

3.29 In view of our proposed approach, this is how we would, at this stage, respond to the PCPD's comment that the offence of unauthorised disclosure or use of computer data may overlap with the doxxing offences. We would, however, add in passing that the proposed interception offence targets unauthorised "interception" of computer data in general and, although a dishonest or criminal purpose is required to be proved, it is not harm-based and is, in that regard, clearly distinguishable from the doxxing offences under the PDPO.

***The requirement "for a dishonest or criminal purpose" is appropriate***

3.30 In our view, whether a purpose is "improper" can be a subjective question which is open to interpretation. On the contrary, objective standards exist for determining whether a purpose is "*dishonest or criminal*". For instance, the test of dishonesty has been laid down in *R v Ghosh*,[22] which remains the leading authority followed in Hong Kong.[23] For "criminal purpose", in most cases, it would be relatively clear-cut whether an act is criminal or not. In addition, "criminal purpose" is a well-established statutory concept.

3.31 We should emphasise that in the Consultation Paper,[24] the Sub-committee fully acknowledged that the operation of modern networking devices has an element of interception and data interception may occur in various ways under the normal practice of cybersecurity companies. The Sub-committee

---

21 Part Two, subject to further discussion in due course on its scope, will cover cyber-enabled crimes, which are traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of information and communications technology. See para 8 of the Preface.

22 [1982] QB 1053. Under the *Ghosh* test, the jury must first decide whether according to the ordinary standards of reasonable and honest people, what was done was dishonest. If so, the jury must then consider whether the defendant himself must have realised that what he was doing was by those standards dishonest.

23 As far as the test of dishonesty is concerned, the *Ghosh* test remains good law in Hong Kong for the time being, but it may be a matter to be considered by Hong Kong courts, in the light of jurisprudential developments recognised by the Court of Appeal of England and Wales in *R v Barton* [2021] QB 685, [2020] 3 WLR 1333 after the UK Supreme Court's decision in a case involving a civil claim (namely *Ivey v Genting Casinos (UK) Ltd (trading as Crockfords Club)* [2018] AC 391, [2017] 3 WLR 1212), when opportunity arises. See *Archbold Hong Kong 2025*, at para 22-20.

24 At para 3.97.

outlined the following phenomena which are unlikely to be regarded as objectionable even if they may involve unauthorised interception:[25]

(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 ("**ISPs**"), somehow it would possess some data in transit through its equipment. The capture of metadata is a technical necessity in such operation.

3.32 This was precisely why the Sub-committee recommended interception "*for a dishonest or criminal purpose*" as a requirement for the proposed interception offence in order that the data interception that normally takes place under the ordinary use of computer network technology will not be criminalised. The element "*for a dishonest or criminal purpose*" intends to impose a high *mens rea* threshold to avoid over-criminalising unauthorised interception or creating an offence whose scope is unjustifiably broad. By virtue of the requirement *"for a dishonest or criminal purpose"*, the activities of the cybersecurity companies in guarding against cyber-attacks are excluded from the ambit of the proposed offence.

3.33 We should add that as technology is constantly evolving, it is neither practicable nor appropriate for the new cybercrime legislation to pinpoint the precise circumstances in which data interception is considered legal. In our view, it suffices for the new cybercrime legislation to make it clear that the proposed offence only proscribes unauthorised interception of computer data carried out for a dishonest or criminal purpose.

3.34 We also acknowledge that some uncertainty may arise in the application of the mental element "*for a dishonest or criminal purpose*" to certain borderline behaviours, such as the possible acts of data interception by private investigators and paparazzi. In those cases, whether a person is guilty of the interception offence would depend on the specific circumstances of the case. Apart from the purpose of interception, if, for example, the defendant knew that the data being intercepted involved private communications, it is possible that the court would find that the intercepting conduct was dishonest, having taken into account the standards of ordinary reasonable people.

3.35 Nevertheless, the merit of the criterion "*for a dishonest purpose*" is that the court may consider a multitude of factors in deciding whether the defendant's conduct of interception fell within the acceptable realm. For

[25] Same as above.

instance, if a computer science student who intercepted data at a shopping mall alleged that he carried out data interception for some research purposes only (eg to ascertain the number of persons who used a particular phone model), but the intercepted data consisted of credit card details or phone numbers, the court would, short of some innocent explanation as to the excessive data collected which was or might be true, likely find that his interception was done "*for a dishonest or criminal purpose*".

3.36 On balance, we conclude that the *mens rea* threshold "*for a dishonest or criminal purpose*" is appropriate as it can avoid catching the innocent interceptors inadvertently.

### *Criminal liability of public officers who exercise law enforcement powers*

3.37 As we have just explained in the preceding paragraphs, the proposed interception offence is accompanied by a relatively high mental threshold, ie unauthorised interception of computer data for a dishonest or criminal purpose. If a public officer acts in good faith and only exceeds his authority inadvertently, we believe that subject to Hong Kong courts' further consideration of the *Ghosh* test of dishonesty in the light of the jurisprudential developments in England and Wales,[26] he will unlikely be found guilty of the proposed offence. In any event, as long as a public officer does not intercept data "*for a dishonest or criminal purpose*", the interception offence would not arise.

3.38 On the other hand, if a public officer intercepts data "*for a dishonest or criminal purpose*", he should be guilty of the offence of illegal interception of computer data like other persons. Thus, we consider that it is not necessary to provide any specific exemptions for public officers in the bespoke cybercrime legislation for the performance of law enforcement duties.

### *Unauthorised interception includes interception that "exceeds authority"*

3.39 The concept of "unauthorised" is embodied in the first four cyber-dependent crimes recommended by us, namely the offence of illegal access to program or data ("**Access Offence**") discussed in Chapter 2, the proposed

[26] As explained in fn 22 above, under the *Ghosh* test, the jury must decide (i) whether according to the ordinary standards of reasonable and honest people, what was done was dishonest, and if so (ii) whether the defendant himself must have realised that what he was doing was by those standards dishonest. The concerns about the second limb of the *Ghosh* test was that it rested on a defendant's understanding of society's standards, so a person with a weak moral compass would be able to avoid liability by asserting that he was unaware of social standards of honesty. In *R v Barton and Booth* [2021] QB 685, at 729, the English Court of Appeal confirmed that the test established in *Ivey v Genting Casinos (UK) Ltd* [2018] AC 391, [2017] 3 WLR 1212 would be the test for dishonesty in all criminal cases, ie when a defendant's actual state of mind as to knowledge or belief as to facts is established, the question whether his conduct was dishonest is to be determined by applying the objective standards of ordinary decent people (rather than the defendant's understanding of those standards). It remains to be seen whether Hong Kong courts will shift away from the test of dishonesty in *R v Ghosh*.

offence of illegal interception of computer data, as well as the offences of illegal interference with computer data and illegal interference with computer system ("**Interference Offences**"), which we will turn to in Chapters 4 and 5.

3.40 In Final Recommendation 1, we proposed that the Access Offence should be modelled on sections 1 and 2 of the Computer Misuse Act in England and Wales ("**CMA-EW**"). Sections 1(1) and 17(5) of the CMA-EW were set out in Chapter 2 of this Report,[27] but are quoted here again for readers' ease of reference. Section 1(1) provides that:

> *"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;*
>
> *(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."*
>
> (emphasis added)

3.41 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 … "*
>
> (emphasis added)

3.42 As the Sub-committee explained in the Consultation Paper,[28] in *R v Bow Street Metropolitan Stipendiary Magistrate, Ex parte United States*,[29] the House of Lords held that section 17(5) did not introduce the concept of different levels of access to the relevant computer, and that an employee with limited authorisation to access data on a computer might commit an offence

---

27 Paras 2.20 and 2.21 above.
28 At paras 2.45 and 2.46.
29 [2000] 2 AC 216.

under section 1 of the CMA-EW by acting in excess of the authorisation. In other words, the term "unauthorised" covers situations where a person acts in excess of his authority, which means that the Access Offence, based on the CMA-EW model, intends to apply to cases where a defendant acts (i) without authority; or (ii) in excess of authority.

3.43 For the sake of consistency, the proposed interception offence and the Interference Offences should adopt the same scope insofar as the concept "unauthorised" is concerned. Should the Government decide to implement Final Recommendation 4, the Law Draftsman may wish to consider whether the offence provisions should explicitly state that "unauthorised" includes "*acting in excess of authority*" (as in section 1030(a) of the Computer Fraud and Abuse Act of the USA discussed in the Consultation Paper)[30] to ensure clarity as to the ambit of the proposed interception offence.

***The interception offence applies to "communication" and "data" in general, not just "private communication" and includes metadata, etc***

3.44 It would be useful to recall the standard of criminalisation under Article 3 of the Budapest Convention, which concerns the offence of illegal interception of computer data. As stated in the Explanatory Report to the Convention quoted in the Consultation Paper:[31]

> *"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*

---

30 At para 2.81. Section 1030(a) of the Computer Fraud and Abuse Act lists the acts relating to access that are punishable as provided in s 1030(c), including a person who:

"*(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—*

*(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;*

*…*

*(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 …*". (emphasis added)

31 At para 3.18.

*term 'non-public' does not per se exclude communications via public networks ...* "

(emphasis added)

3.45 In other words, Article 3 of the Budapest Convention does not require the computer data in question to be private.[32] The data may be public or private.

3.46 We also bear in mind the review of the Search and Surveillance Act 2012 in New Zealand, which identified problems of its statutory regime being limited to interception of "private communications". The Issues Paper jointly published by the New Zealand Law Commission and the Ministry of Justice in 2016 highlighted the undesirability to focus on what the parties to a communication expect, which is an element of circularity "*that has been the subject of considerable criticism*".[33] In view of the aforesaid, the Report released in New Zealand in 2017 recommended that the definition of "private communication" be replaced with "communication".[34]

3.47 Furthermore, it is important to note that under Recommendation 4(b) in the Consultation Paper, the proposed interception offence applies to all "data", whether it be metadata, data in transit or data momentarily at rest during transmission to avoid the need to call highly technical evidence at trial.[35]

3.48 In sum, we take the view that the proposed interception offence should protect both "communication" and "data" in general, not just "private communication" and includes metadata, etc.

---

32 Consultation Paper, at para 3.100.

33 New Zealand Law Commission and Ministry of Justice, *Review of the Search and Surveillance Act 2012* (Issues Paper 40, 2016), at para 4.11.

34 New Zealand Law Commission and Ministry of Justice, *Review of the Search and Surveillance Act 2012* (Report 141, 2017), at Recommendation 24. See also the Consultation Paper, at para 3.101(b).

35 As discussed in the Consultation Paper (see paras 3.19 to 3.24, 3.108 and 3.109), as long as the data in question is en route from a sender to an intended recipient, data interception should be an offence. Thus, the interception offence applies to communication throughout its transmission, irrespective of whether the data was momentarily at rest or in motion. One way to achieve this is to introduce a deeming provision along the lines of s 5F of the Telecommunications (Interception and Access) Act 1979 in Australia, which provides that a communication is (a) "*taken to start passing over a telecommunications system when it is sent or transmitted by*" the sender; and (b) "*taken to continue to pass over the system until it becomes accessible to the intended recipient*" (see para 3.22 of the Consultation Paper). This would save the need for the prosecution to adduce highly technical evidence to prove the elements of the offence.

***Not define "interception"***

3.49 As a business group has pointed out, computer-related acts such as "access" and "interception" evolve with technological developments. New ways of intercepting computer data beyond our contemplation may emerge from time to time. Defining "interception" may make the law less flexible in coping with novel circumstances.

3.50 Thus, despite the fact that "intercepting act" is defined in the existing ICSO [36] and some other jurisdictions, [37] we consider it more appropriate not to define "interception" in the new cybercrime legislation, but to give "interception" its ordinary meaning so as to attain the purpose of the proposed offences to protect people's right to privacy of data communication.

## Conclusion on Recommendation 4

3.51 We conclude that Recommendation 4 can be retained, subject to removing the limb regarding "*disclosure or use of computer data*" pending further study for the reasons articulated in paragraphs 3.25 to 3.28 above.

**Final Recommendation 4**

**We recommend that:**

**(a) Unauthorised interception 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**

[36] Under s 2(1) of the Interception of Communications and Surveillance Ordinance (Cap 589), "intercepting act" is defined as follows:
" *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*".

[37] Namely, England and Wales (s 4 of the Investigatory Powers Act 2016), New Zealand (s 216A(1) of the Crimes Act 1961) and the United States of America (s 2510(4) of the Wiretap Act).

**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").**

**(d) The implications of unauthorised disclosure or use of computer data, intercepted or otherwise, should be studied in greater detail in Part Two of our study before we express any settled view as to whether any new offence in this regard should be recommended, and if so, how.**

## Defences to the offence of illegal interception of computer data: Recommendation 5

3.52 Recommendation 5 of the Consultation Paper invited submissions on the following questions:

> "*(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)?*"

## Responses to the Sub-committee's Recommendation 5

3.53 As the responses to the consultation questions in Recommendation 5(a) and (b) are closely related and overlap to a certain extent, we shall analyse them together.

***Recommendation 5(a)***

*Comments from Respondents who support exempting professions*

3.54 A substantial majority of the Respondents considered that there should be a defence or exemption for professions which have to intercept and use the data intercepted in the course of their ordinary and legitimate business. These Respondents suggested that the defence or exemption should cover the following categories of professions or activities:

(a) ISPs;

(b) Institutions whose daily work frequently requires use and handling of intercepted data (no specific examples of such institutions were given by the information technology-related body which proposed this exemption);

(c) Companies which intercept their own network purely for security threat detection, whether the interception is conducted by the companies themselves or their authorised security consultants;

(d) LEAs' investigation of criminal activities and matters of national security;

(e) Whistleblower activities carried out in good faith, for public interest, or for collecting evidence for future legal proceedings; and

(f) Business or organisations which hold a legitimate belief that activities are being carried out against their interest (The HKWPEA remarked that this defence or exemption should be couched strictly and narrowly).

*Comments from Respondents who oppose exempting professions*

3.55 Nevertheless, some Respondents from the information technology sector disagreed with providing a blanket defence or exemption for intercepting and using data in the course of the ordinary and legitimate business of any profession. They pointed out that:

(a) firstly, the intercepted data does not necessarily relate to the business which carries out the interception, and there are many grey areas in this regard which are likely to give rise to disputes; and

(b) secondly, the defence or exemption should be applicable to every person, but not only any specific privileged class.

***Recommendation 5(b)***

*Comments from Respondents who support exempting genuine business*

3.56 Similar to Recommendation 5(a), a clear majority of the Respondents agreed that a genuine business should be allowed to intercept and use the data being transmitted without incurring criminal liability. Among these Respondents, the PCPD shared the Sub-committee's view that if a business provides Wi-Fi hotspots or computers for use on terms and conditions that reserve the right to intercept and utilise data of their customers or employees, the authority to intercept and utilise the data is contractual in nature.[38] It further pointed out that if the data collected involves personal data, the collection and use of the personal data are governed by the Data Protection Principles under the PDPO.

3.57 Those who supported exempting genuine business have made suggestions on the conditions of the exemption. A common ground among Respondents in different sectors is that the interception and use of the data by the business should not serve any dishonest or criminal purpose. The HKFWL Ltd further suggested that in order to justify allowing a business to intercept and use the data being transmitted without incurring criminal liability, the purposes of such interception must be ringfenced, and that the defence or exemption may require a specific relationship (eg an employment relationship) between the interceptor and interceptee.

3.58 Regarding the example of shopping malls highlighted in the consultation question under Recommendation 5, the HKFWL Ltd observed that:

> "*there would not appear to be any obvious reason why the data being transmitted by a customer should be intercepted. There is no genuine relationship between the shopping mall operator / owner [and] the customers at large and therefore such statutory permission would seem to be too broad.*"

[38] Consultation Paper, at para 3.118.

*Comments from Respondents who oppose exempting genuine business*

3.59 On the other hand, some Respondents have reservations towards allowing genuine business to intercept and use the data being transmitted. For instance, the Consumer Council put forward the following views:

> "*When a mall or shop offers its free Wi-Fi hotspot service, the consumers may legitimately expect that it is simply in the nature of a value-added service to attract patrons. The consumer may not legitimately expect that his data would be intercepted and used for other purposes …*
>
> *… whilst the mall or shop may set out its terms of use and require the consumer's indication of consent to the interception of data as a condition for accessing the service, it is questionable whether a consumer may take time or care to properly review such terms … His consent, even if given, may not be informed.*
>
> *The indiscriminate collection of data transmitted through the Wi- Fi hotspot would in any event be too broad. This could potentially include personal data or even sensitive data such as bank account information and passwords. Irrespective of whether the data is encrypted or the business intends to use such data, it is unlikely that consumers would perceive such collection to be fair.*"

3.60 Lastly, an information-technology related body pointed out that any misuse of the Wi-Fi hotspots or computers which a business provides to its patrons may lead to data leakage, and so this Respondent was not in favour of providing specific defences or exemptions for such a business.

## Our analysis and response

3.61 Upon carefully reflecting on the Respondents' submissions and the elements of the proposed offence of illegal interception of computer data, we take the view that it is not necessary to put in place any specific defences or exemptions for those who have to, in the course of their ordinary and legitimate business, intercept and use computer data. In theory, it does not seem logical to provide any defence to an offence which, by design, already expressly requires proof of a "*dishonest or criminal purpose*". In context, if a profession or genuine business intercepts computer data for a dishonest or criminal purpose, it should not be exempted from criminal liability merely because it runs a particular profession or business.

3.62 Regarding the specific categories of professions or businesses that some of the Respondents consider a defence or exemption should be provided for, we have the following observations:

(a) As ISPs acting in the normal course of business are protected from liability for data interception that is not carried out with any criminal intent, it is not necessary to provide them with any defence to the proposed interception offence.

(b) It is not feasible to provide a defence to institutions whose daily work frequently requires use and handling of intercepted data without in effect giving some professions or businesses whose day-to-day operation involves data interception (such as a private investigation agency or a media agency) a carte blanche licence to intercept data.

(c) A genuine business may indeed collect or intercept computer data primarily for multiple marketing purposes. If upon proof, however, an unauthorised interception had indeed taken place and it was carried out for a dishonest purpose (as opposed to by a dishonest means), there is all the more reason that a defence should not be provided even though the business was otherwise simply motivated by profit.

(d) As no defence is provided to acts of illegal access to program or data[39] or illegal interference with computer data and/or computer system[40] that are carried out in good faith, for public interest, or for collecting evidence for future legal proceedings, it is difficult to conceive why such a defence should be provided to whistleblowers in respect of the proposed interception offence. In addition, different persons may hold different standards as to what constitutes "good faith". A case in point is *HKSAR v Tsun Shui Lun* discussed in the Consultation Paper,[41] where the defendant employee working in a hospital leaked a Principal Official's medical report to the press. When charged with section 161(1)(c) of the Crimes Ordinance (Cap 200),[42] the defendant argued that he thought the public had the right to know

---

39 The defences to the offence of illegal access to program or data are discussed in paras 2.63 to 2.102 of Chapter 2.

40 The defences to the offences of illegal interference with computer data and illegal interference with computer system are discussed in paras 4.32 to 4.44 of Chapter 4 and paras 5.23 to 5.28 of Chapter 5 respectively.

41 [1999] 3 HKLRD 215, HCMA 723/1998 (date of judgment: 15 Jan 1999). See the Consultation Paper, at paras 2.9 and 2.10.

42 Under s 161(1)(c) of the Crimes Ordinance (Cap 200) ("**CO**"), any person who obtains access to a computer "*with a view to dishonest gain for himself or 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.

the truth. The Court of First Instance, however, found no merit in the appeal against conviction.[43]

(e) Last but not least, providing defences to specific categories of professions or persons in the bespoke cybercrime legislation may imply that data interception by other professions or persons not specified in the legislation will always be unlawful, thereby bringing more confusion than clarity to the law.

3.63 For all these reasons, we are inclined to think that no defence or exemption to the proposed interception offence is necessary. Any business that wishes to intercept the data of patrons or consumers may obtain the latter's authorisation for intercepting data. If the intercepted data is used for a purpose other than the authorised purpose, it would be up to the court to decide on the evidence of a particular case whether the interception is carried out for a dishonest or criminal purpose.

3.64 In sum, unlike the Access Offence and the Interference Offences, the proposed interception offence adopts a heightened *mens rea* of interception of computer data "*for a dishonest or criminal purpose*", which in itself has mitigated the need for any specific exemptions or defences to the offence.

**Final Recommendation 5**

**We do not recommend any defence or exemption for professions or genuine businesses (eg coffee shops, hotels, shopping malls, employers) which intercept or use computer data in the ordinary course of their operation. The *mens rea* requirement of interception of computer data for a dishonest or criminal purpose has mitigated the need to provide for any specific defence or exemption.**

[43] See fn 41 above, at 228. The CFI held that the appellant accessed the hospital computer system in excess of his authority, and he intended to obtain the confidential information in the computer for the purpose of printing out a copy of the scan report and leaking it to the press. That was a gain within the definition in s 161 of the CO. It was dishonest conduct and the defendant knew that.

# Chapter 4

# Illegal interference with computer data

## Introduction

4.1 This Chapter discusses the responses regarding Recommendation 6 of the Consultation Paper, which proposes the third cyber-dependent offence, namely illegal interference with computer data:

> "*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).*"

4.2 As the Sub-committee explained in the Consultation Paper,[1] broadly speaking, the offence of interference with computer data would seek to:

(a) combat intentional damage, deletion, alteration, etc of computer data; and

[1] At para 4.1.

(b) thereby protect the integrity and proper functioning or use of computer data.

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.

4.4 Thus, the offence of illegal interference with computer data is closely related to the offence of illegal access to program or data ("**Access Offence**") discussed in Chapter 2 because interference with data usually only occurs upon a person's initial intrusion into a computer system.

## General Responses on Recommendation 6

4.5 An overwhelming majority of the Respondents who specifically commented on Recommendation 6 were supportive of the recommendation. Those in favour included legal professional bodies, information-technology related bodies, tertiary institutions, business organisations and Government departments.

4.6 The Office of the Privacy Commissioner for Personal Data supported the proposed offence of illegal interference with computer data on the grounds that it will help to deter data security breach, which has become increasingly common.

4.7 A number of organisations, including the Hong Kong and Mainland Legal Professional Association Limited, the Hong Kong Federation of Women Lawyers Limited, another professional association and two business groups agreed that the existing regime under the Crimes Ordinance (Cap 200) ("**CO**") for addressing illegal interference with computer data and computer system, including the notion of "*misuse of a computer*" in section 59(1A), is satisfactory. These Respondents therefore agreed with the Sub-committee's proposal of transposing the existing provisions in sections 59, 60 and 64 of the CO to the new cybercrime legislation for the sake of consistency.

***Current Hong Kong law***

4.8 As the Sub-committee explained in the Consultation Paper,[2] the current Hong Kong law addresses illegal interference with computer data mainly by treating it as a form of criminal damage. Under section 60(1) and (2) of the CO ("*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."*

4.9 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."*

*Application of the Crimes Ordinance to interference with computer data and computer system*

4.10 The offence of criminal damage is able to address illegal interference with computer data (and also illegal interference with computer system, which will be discussed in the next Chapter) because of the following

---

[2] At paras 4.4 and 4.5.

provisions added into the CO by the Computer Crimes Ordinance 1993 (No 23 of 1993):

(a) Section 59(1)(b) defines "property" 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*".

(b) Section 59(1A) 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 the offence of illegal interference with computer data.

4.11 Under section 64(2) of the CO ("**S64(2)**"), a person charged with the offence of criminal damage shall be treated as having a "*lawful excuse*":

> *"(a) if at the time of the act or acts alleged to constitute the offence he believed that the person or persons whom he believed to be entitled to consent to the destruction of or damage to the property in question had so consented, or would have so consented to it if he or they had known of the destruction or damage and its circumstances; or*
>
> *(b) if he destroyed or damaged or threatened to destroy or damage the property in question or, in the case of a charge of an offence under section 62, intended to use or cause or permit the use of something to destroy or damage it, in order to protect property belonging to himself or another or a right or interest in property which was or which he*

*believed to be vested in himself or another, and at the time of the act or acts alleged to constitute the offence he believed—*

*(i) that the property, right or interest was in immediate need of protection; and*

*(ii) that the means of protection adopted or proposed to be adopted were or would be reasonable having regard to all the circumstances."*

4.12 By virtue of section 64(3), it is immaterial whether a defendant's belief is justified or not if it is honestly held.

## Detailed Responses to the Sub-committee's Recommendation 6

4.13 While the vast majority of the Respondents support the proposed offence of illegal interference with computer data, some Respondents also expressed specific views on the constituent elements of the offence proposed under Recommendation 6:

(a) A few information technology-related bodies observed that the maximum penalty for the proposed offence of illegal interference with computer data on conviction on indictment is 14 years' imprisonment (see Recommendation 16(c)). Given the severity of the penalty, they opined that "malice" should be a requisite element of the proposed interference offence.

(b) The Law Society of Hong Kong suggested that it was not clear why the requirement of "recklessness" is appropriate or relevant. This Respondent opined that a person who is mindful of interfering with data stored in a computer must have the "intention" to do so. For instance, the person would plan ahead, procure the necessary tools (software), avail himself of the opportunities, gain access to the computer, get hold of the data, and alter or delete them. These actions would, in its opinion, require "*a deliberate chain of actions*".

(c) A Government department suggested that on top of the elements stated in section 60(2) of the CO, "*any act or activity intending to endanger national security or being reckless as to whether national security would be thereby endangered"* should also be regarded as an aggravated offence. This Respondent quoted the following examples from other jurisdictions, whose statutory provisions specifically make reference to damage to national security:

(i) The Computer Misuse Act in England and Wales ("**CMA-EW**") prescribes a maximum penalty of life imprisonment for a defendant whose act causes or creates a significant risk of serious damage to national security.[3] If a defendant's unauthorised act in relation to a computer causes or creates a significant risk of "*damage to the national security of any country*",[4] the maximum penalty for conviction on indictment is 14 years' imprisonment, or a fine, or both.[5]

(ii) Section 11 of the Computer Misuse Act in Singapore ("**CMA-SG**") reserves the heaviest maximum penalty for cases involving access to a "protected computer". A computer is treated as a "protected computer" if the person committing the offence knew, or ought reasonably to have known, that the computer, program or data is used directly in connection with or necessary for "*the security, defence or international relations of Singapore*".[6]

## Our analysis and response

### *Elements of the offence of illegal interference with computer data*

*Malice*

4.14 We wish to point out that "malice" is an archaic *mens rea* expression commonly found in earlier legislation. As Diplock LJ (as he then was) remarked in *R v Mowatt*,[7] " *'unlawfully and maliciously' was a fashionable phrase of parliamentary draftsmen in 1861*",[8] when the old Malicious Damage Act 1861 was enacted.

---

3 Consultation Paper, at para 4.41. Section 3ZA(7) reads as follows:
"*Where an offence under [s 3ZA] is committed as a result of an act causing or creating a significant risk of—*
*…*
*(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.*" (emphasis added)

4 Consultation Paper, at para 4.41. The relevant subsections of s 3ZA read as follows:
"*(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;*
*(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—*
*…*
*(d) damage to the national security of any country.*" (emphasis added)

5 CMA-EW, s 3ZA(6).

6 CMA-SG, s 11(2)(a). Section 11 is set out in para 4.68 of the Consultation Paper.

7 [1968] 1 QB 421.

8 Same as above, at 425.

4.15 The meaning of "malice" in criminal law is an actual intention to do a particular kind of harm that was in fact done, or recklessness as to whether such harm should occur (ie the accused has foreseen that the particular kind of harm might be done and yet has gone on to take the risk of it).[9] It does not require any ill will towards the person injured. This interpretation explains why the Law Commission of England and Wales found difficulty with the term "malice" when it reviewed the offences of damage to property, which led to the enactment of the Criminal Damage Act 1971 (on which the criminal damage offence in Hong Kong was modelled):

> *"We consider, therefore, that the same elements as are required at present should be retained, but that they should be expressed with greater simplicity and clarity. In particular, we prefer to avoid the use of such a word as 'maliciously', if only because it gives the impression that the mental element differs from that which is imposed in other offences requiring traditional mens rea. It is evident from such cases as R v Cunningham and R v Mowatt that the word can give rise to difficulties of interpretation … "*[10]
>
> (emphasis added)

4.16 In light of the aforesaid, it is appropriate to maintain the *mens rea* elements in Recommendation 6(b)(ii), ie "*intent or recklessness, but not malice*".

*Recklessness*

4.17 As seen in the earlier part of this Chapter,[11] "intention" and "recklessness" are alternative *mens rea* elements of the offence of criminal damage under the existing section 60(1) of the CO, and the current statutory framework for the criminal damage offence applies to "*misuse of a computer*" by virtue of section 59(1)(b) and (1A). Therefore, Recommendation 6, which proposes to adopt the current regime under section 60, likewise adopts the mental elements of "intention" and "recklessness" for the proposed offence of illegal interference with computer data.

4.18 We observe that "recklessness" has also been adopted alongside "intention" as a mental element in the cybercrime legislation of some other jurisdictions. These include:

---

9 *Archbold Hong Kong 2025*, at para 16-35, citing *R v Cunningham* [1957] 2 QB 396; 41 Cr App R 155 and subsequent developments (see further discussions below). See also *HKSAR v Chung Chi Fai* [2014] 3 HKLRD 549, at para 26.

10 Law Commission, *Criminal Law Report on Offences of Damage to Property* (1970), Law Com No 29, at para 44.

11 Paras 4.8 and 4.10.

(a) section 477.2 of the Australian Criminal Code (Cth) (*"Unauthorised modification of data to cause impairment"*);[12]

(b) section 3 (*"Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc"*)[13] and section 3ZA ("*Unauthorised acts causing, or creating risk of, serious damage*")[14] of the CMA-EW; and

(c) section 250(2) of the New Zealand Crimes Act 1961.[15]

4.19 The concept of "recklessness" in criminal law requires proof that a defendant was aware of the risk and that, in the circumstances known to him, it was unreasonable to take the risk.[16] This interpretation of recklessness applies to criminal law in general, but not only cybercrimes. This being the case, the context in which a defendant's act took place does not by itself justify the exclusion of the application of the proposed offence of illegal interference with computer data on the ground of recklessness.

4.20 As a matter of fact, many criminal offences adopt "recklessness" as a fault element alongside "intention" or "knowledge". To cite just a few examples:

(a) Under section 118(3) of the Crimes Ordinance (Cap 200), a person commits rape if he has unlawful sexual intercourse with

---

12 Consultation Paper, at para 4.23. Section 477.2(1) of the Criminal Code (Cth) provides that "*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.*" (emphasis added)

13 Consultation Paper, at para 4.38. Section 3(1) of the CMA-EW provides that "*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.*"
Section 3(2) states that "*This subsection applies if the person intends by doing the act …*".
Section 3(3) states that "*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.*" (emphasis added)

14 Consultation Paper, at para 4.41. Section 3ZA(1) of the CMA-EW provides that "*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;*
*(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.*" (emphasis added)

15 Consultation Paper, at para 4.50. Section 250(2) of the Crimes Act 1961 provides that "*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; …*" (emphasis added)

16 *Archbold Hong Kong 2025*, at para 16-40, discussing *R v G* [2004] AC 341 decided in the context of the offence of criminal damage and subsequent jurisprudential developments.

a woman who does not consent to it, and he "*knows*" that she does not consent to it, or he is "*reckless*" as to whether she consents to it. In practice, rape offences are often prosecuted on the grounds that the defendant was reckless as to whether the victim consented to the sexual intercourse (eg the victim was drunk and incapable of giving consent);

(b) The offence of fraud is committed if a person by any "*deceit*" (whether *deliberate or reckless*) and with intent to defraud induces another person to commit an act or make an omission, which results in benefit to any person other than the second-mentioned person, or in prejudice or a substantial risk of prejudice to any person other than the first-mentioned person;[17]

(c) The fault elements are similar for the offence of obtaining property by deception, which refers to a person who by any deception (whether *deliberate or reckless*) dishonestly obtains property belonging to another, with the intention of permanently depriving the other of it;[18] and

(d) Under section 295(1) of the Securities and Futures Ordinance (Cap 571), the offence of false trading occurs if a person does anything with the "*intention*" that, or being "*reckless*" as to whether it has, or is likely to have, the effect of creating a false or misleading appearance of active trading in securities or futures contracts traded on a recognised market.

4.21 Moreover, the concept of "recklessness" stresses the importance of exercising care and responsibility in the use of computer technology, ie a person must be vigilant to the possible consequences of his online actions, including the impact that they may have on other persons.

4.22 For the reasons explained above, we recommend retaining "recklessness" as a fault element alongside "intention" for the offence of illegal interference with computer data.

---

17 Theft Ordinance (Cap 210), s 16A.

18 Same as above, s 17.

*Should the aggravated form of the interference offence specifically cover acts endangering national security?*

4.23 It is useful, first, to carefully consider to what extent the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region ("**NSL**"), which was enacted and applied, as a national law, to Hong Kong by promulgation on 30 June 2020, has already covered the proposed offences of illegal interference with computer data and/or computer system.

4.24 The offence provisions in the NSL largely focus on specifying the prohibited activities that threaten national security, as well as the purposes of the persons who engage in these activities and the effects of these activities. The means by which the prohibited activities are carried out (eg whether in the physical world or cyberspace) is relatively immaterial under the NSL.

4.25 Nevertheless, Article 24(4) of the NSL distinctly covers acts of interference with, and damage to, the electronic control systems of the internet. Article 24 states that:

> *"A person who organises, plans, commits, participates in or threatens to commit any of the following terrorist activities causing or intended to cause grave harm to the society with a view to coercing the Central People's Government, the Government of the Hong Kong Special Administrative Region or an international organisation or intimidating the public in order to pursue political agenda shall be guilty of an offence:*
> *…*
>
> *(3) sabotage of means of transport, transport facilities, electric power or gas facilities, or other combustible or explosible facilities;*
>
> *(4) serious interruption or sabotage of electronic control systems for providing and managing public services such as water, electric power, gas, transport, telecommunications and the internet; or*
>
> *(5) other dangerous activities which seriously jeopardise public health, safety or security."* [19]
>
> (emphasis added)

[19] The English text follows the English translation in Instrument A406 (Promulgation of National Law 2020), which was published in G.N. (E.) 72 of 2020 for information. The source text of Article 24 reads:

4.26 We have carefully considered whether the aggravated offences of interference with computer data (and computer system) should specifically include acts endangering national security in the light of the following legal and practical considerations related to the NSL:

(a) Given the overarching status of the NSL, it should always take precedence over all other local legislation, including the bespoke cybercrime legislation recommended by us. If a cybercrime offence also fulfils the elements of an offence under the NSL, we envisage that invoking the NSL should warrant primary consideration by law enforcement agencies, the prosecuting authority and the courts.

(b) If the NSL has already covered the offences of illegal interference with computer data and/or computer system, it might be superfluous for the aggravated form of the Interference Offences to specifically refer to acts endangering national security again. That said, we note that the intent for an offence under Article 24 is highly specific – the defendant must either cause or intend to cause grave harm to society, with the specific intent to coerce the Central People's Government, the Government of the Hong Kong Special Administrative Region ("**HKSAR**") or an international organisation, or to intimidate the public in order to pursue political agenda.

(c) The NSL is expressed in broad terms. By placing the emphasis on the purposes and effects of the prohibited activities, other provisions of the NSL (ie other than Article 24(4),[20] which specifically refers to the electronic control systems of the internet) seem wide enough to embrace acts of illegal interference with computer data (and computer system) already. For instance:

(i) Article 24(3) is silent on the means by which a defendant may "sabotage" the various utilities mentioned in that provision. Given its focus on the prohibited conduct (ie "sabotage"), Article 24(3) seems applicable to any types of act that lead to the sabotage of the specified utilities, including sabotage by illegal interference with the computer data and/or computer system related to the relevant utilities.

---

"*為脅迫中央人民政府、香港特別行政區政府或者國際組織或者威嚇公眾以圖實現政治主張，組織、策劃、實施、參與實施或者威脅實施以下造成或者意圖造成嚴重社會危害的恐怖活動之一的，即屬犯罪：*

*…*

*(三) 破壞交通工具、交通設施、電力設備、燃氣設備或者其他易燃易爆設備；*

*(四) 嚴重干擾、破壞水、電、燃氣、交通、通訊、網絡等公共服務和管理的電子控制系統；*

*(五) 以其他危險方法嚴重危害公眾健康或者安全。*" (emphasis added)

20 Para 4.25 above.

(ii) Article 24(5) of the NSL serves as a catch-all provision that covers all dangerous activities which seriously jeopardise public safety or security. The essential requirement is the nature of the activity, ie one that is dangerous. As both cybercrimes and crimes in the physical world can fulfil this requirement, Article 24(5) appears to be wide enough to cover the offences of illegal interference with computer data and computer system ("**Interference Offences**").

(d) There are two tiers of penalties for the offence under Article 24. If a defendant causes serious bodily injury, death or significant loss of property, the sentence shall be life imprisonment or a fixed-term imprisonment of not less than ten years. This higher maximum penalty under the NSL is commensurate with that of the aggravated offence of illegal interference with computer system, for which the sentence of life imprisonment is proposed.[21] In other circumstances, a lower penalty (ie a fixed term imprisonment of not less than three years but not more than ten years) will apply to an offence under Article 24.

4.27 Especially because the NSL forms an essential part of the fabric of our legal system, it is important that the bespoke cybercrime legislation does not create any inconsistencies or conflict, even if unintended, with the NSL. Given the paramount importance of national security, we would expect that due consideration would have been given in formulating the national security-related offences in cyber-neutral terms when they were created under the NSL which would be construed accordingly unless its text, context and purpose indicate to the contrary. We acknowledge that an analysis of the aggravated aspect of the proposed Interference Offences would not be complete without the benefit of a holistic view of the Government's overall position on the substantive law on national security.

4.28 In March 2024, the Safeguarding National Security Ordinance ("**BL 23 legislation**") was enacted by the Legislative Council. This is in order to fully implement Article 23 of the Basic Law, the Decision of the National People's Congress on Establishing and Improving the Legal System and Enforcement Mechanisms for the Hong Kong Special Administrative Region to Safeguard National Security and the constitutional duties and obligations as stipulated under the NSL, and to effectively respond to national security risks and threats that may arise at present and in future.[22]

4.29 Offences under the BL 23 legislation include, *inter alia*, the offence of sabotage activities carried out with intent to endanger national security (or being reckless as to whether national security would be endangered), damaging or weakening public infrastructure (which includes

---

[21] Final Recommendation 16(c)(ii). For the basic offence of illegal interference with computer data and computer system, the proposed sentence is imprisonment for two years on summary conviction and 14 years on conviction on indictment.

[22] Legislative Council Brief on the Safeguarding National Security Bill (Mar 2024).

software constituting the infrastructure),[23] and more specifically, the offence of doing an act in relation to a computer or electronic system with intent to endanger national security without lawful authority.[24] Regarding the latter offence, the Government's consultation document released in January 2024 explained its rationale as follows:

> "*Generally speaking, the proposed offences discussed in this document do not essentially depend on which particular method or technology is actually used by the offender to carry out the criminal act. Therefore, the proposed offences should cover most of the acts and activities endangering national security carried out through computers. On the other hand, given the common use and rapid development of computer or electronic system technologies, with the current wide application of artificial intelligence in different areas of society being an example, the potential national security risks posed should not be overlooked, especially the risks arising from computers or electronic systems being hacked into or interfered with. In order to address the national security risks posed by new technologies that may develop in the current cyber or digital world in the future, we recommend introducing an offence to combat acts endangering national security that are done in relation to a computer or electronic system.*"[25]

4.30 The Court of Final Appeal held that the reference to "*acts endangering national security*" in Article 42(2) of the NSL[26] means acts of that nature capable of constituting an offence under the NSL or the laws of the HKSAR safeguarding national security.[27] Thus, the application of the bespoke procedural rules of the NSL, including its rules on bail,[28] jury trial,[29]

---

23 Safeguarding National Security Ordinance, s 49 (sabotage endangering national security).

24 Same as above, s 50 (doing acts endangering national security in relation to computers or electronic systems).

25 Security Bureau of the Government of the Hong Kong Special Administrative Region, Safeguarding National Security: Basic Law Article 23 Legislation Public Consultation Document (Jan 2024), at para 6.5.

26 Article 42 of the NSL provides that:
"*No bail shall be granted to a criminal suspect or defendant unless the judge has sufficient grounds for believing that the criminal suspect or defendant will not continue to commit acts endangering national security.*"

27 *HKSAR v Lai Chee Ying* [2021] HKCFA 3, (2021) 24 HKCFAR 33 (date of judgment: 1 and 9 Feb 2021), at paras 53(c)(ii) and 70(d)(ii).

28 Same as above, at paras 53(a) and (b). The Court of Final Appeal ("**CFA**") pointed out that Article 42(2) of the NSL introduces a "*considerably more stringent threshold requirement*" because the presumption in favour of bail is excluded in the first instance – under the NSL, the starting point is that no bail shall be granted unless the judge has sufficient grounds for believing that the accused will not continue to commit acts endangering national security. The CFA also noted that the subject matter of Article 42(2) of the NSL overlaps with the subject matter of s 9G(1)(b) of the Criminal Procedure Ordinance (Cap 221) which makes the risk of committing an offence while on bail a basis for refusing bail.

29 Article 46 of the NSL provides that:
"*In criminal proceedings in the Court of First Instance of the High Court concerning offences endangering national security, the Secretary for Justice may issue a certificate directing that the case shall be tried without a jury on the grounds of, among others, the protection of State secrets, involvement of foreign factors in the case, and the protection of personal safety of jurors and their family members ...*".

participation of overseas lawyers[30] and sentencing,[31] is not confined to offences created under the NSL. If a person commits the Interference Offences in a manner which also constitutes an offence created under the NSL or the BL 23 legislation, the procedural rules stipulated under the NSL are then applicable.

4.31 Given the manner in which Article 23 of the Basic Law is now implemented by way of local legislation (which includes the introduction of a specific offence covering national security risks in cyberspace), we consider that the Government would be better placed to evaluate the adequacy or otherwise of all extant national security-related offences holistically and consider our recommendations accordingly to see if any refinements should be proposed if it decides in due course to accept the introduction of the new Interference Offences in the bespoke cybercrime legislation we recommend.

### *Specific defences*

*Consideration of the defences applicable to the Access Offence*

4.32 As explained at the beginning of this Chapter,[32] the offence of illegal interference with computer data is closely related to the Access Offence, given that access to program or data normally precedes interference with computer data. For this reason, we have explored the defences to both the Access Offence and the offences of illegal interference with computer data (and computer system) in parallel to ensure that the law recommended by us is consistent. Of course, with the advancement of technology, it may be possible in future to interfere with computer data (or computer system) without accessing any program or data. Nevertheless, we think that this should not affect our analysis of the proximity of the two offences because in ordinary circumstances, access to program or data occurs before data interference.

4.33 When we responded to the consultees' comments on the general "reasonable excuse" defence to the Access Offence in Chapter 2 of this Report,[33] we have explained the advantage of including specific defences in the cybercrime legislation. To recap, such specific defences may pre-empt future disputes as to whether an act qualifies as a "reasonable excuse". After all, the concept of "reasonable excuse" may not be readily

---

30 In *HKSAR v Lai Chee Ying* [2023] HKCFI 1440 (date of judgment: 2 and 29 Feb 2023), the Court of First Instance held that there is no absolute right to "choice of lawyers" under Article 35 of the Basic Law. The right to "choice of lawyers" means no more than that a litigant is free to choose his counsel from those available to represent him. A person has no right to insist on being represented by a lawyer who does not have a general right to practise in Hong Kong (see paras 75 and 87).

31 In *HKSAR v Lui Sai Yu* [2023] HKCFA 26 (date of judgment: 22 Aug 2023), the CFA held that the stipulation of "*fixed-term imprisonment of not less than five years*" in Article 21 of the NSL for offences of a serious nature is mandatory, so it was appropriate for the lower court not to give full effect to the one-third sentencing discount for the defendant's guilty plea as that would lead to a sentence below the lower limit of the upper band set by Article 21 of the NSL (see paras 66 and 76).

32 Para 4.4.

33 Paras 2.32 to 2.34.

comprehensible to laymen and it is also open to interpretation. The presence of specific defences provides better guidance to the public as to what types of actions are acceptable, thereby adding clarity to the law.

*Interference with computer data for cybersecurity purposes*

4.34 In Chapter 2, we recommended a specific defence for unauthorised access for cybersecurity purposes under the following conditions:[34]

(a) The defence should only be available to accredited cybersecurity practitioners (the details of the accreditation regime, which are essentially matters of policy, are best left to the Government's consideration).

(b) The defendant must act for a genuine cybersecurity purpose.

(c) The defendant's conduct must be reasonable having regard to all the circumstances.

4.35 As interference with computer data (or computer system) normally only occurs upon access to program or data, it would be logical and consistent to provide a similar defence for the offences of illegal interference with computer data (and computer system). Therefore, we recommend that interference with computer data for cybersecurity purposes should be a defence to the proposed offence of illegal interference with computer data.

*Interference with computer data for protecting the interests of a child or vulnerable person*

4.36 While a parent, guardian or other persons may require access to the program or data of a child or vulnerable person to safeguard him from online harm, we understand that such access does not entail any alteration or interference with computer data (or computer system). Besides, using a common sense approach, granting a person access to any program or data in no way implies that the person is authorised to alter or otherwise tamper with the data.

4.37 Accordingly, we consider that unlike the Access Offence, it is not necessary to provide a specific defence to the offence of illegal interference with computer data for the purpose of protecting the interests of a child or vulnerable person.

---

[34] Paras 2.63 to 2.74.

*Interference with computer data for genuine research purposes*

4.38 Similarly, we find it inconceivable that the conduct of genuine research would necessitate interference with computer data (or computer system). Thus, unlike the Access Offence, we take the view that it is not necessary to provide a specific defence to exempt illegal interference with computer data (or computer system) carried out for genuine research purposes.

### *Transposing the defences under S64(2) of the Crimes Ordinance*

4.39 As recapped at the beginning of this Chapter, [35] Recommendation 6 of the Consultation Paper proposed to adopt the two "lawful excuses" currently provided for under S64(2) of the CO (which is quoted in paragraph 4.11 above).

4.40 In Chapter 2 of this Report,[36] we have explained that these two "lawful excuses", known as the consent defence and the property protection defence respectively, should be available to the Access Offence as well.

4.41 As the Respondents generally welcomed the adoption of the existing regime under the CO for the purposes of the offences of illegal interference with computer data (and computer system), we find it appropriate to maintain Recommendation 6, subject to the addition of an objective test into the consent defence and the property protection defence (as in the case of the Access Offence discussed in paragraph 2.101 above):

(a) in the case of the consent defence, the defendant must *reasonably* believe that there was, or would be, consent to his interference with the computer data (or computer system); and

(b) in the case of the property protection defence, the defendant must *reasonably* believe that the property was in immediate need of protection.

4.42 In other words, we propose to disapply section 64(3) of the CO for the purposes of the offences of illegal interference with computer data (and computer system) that we recommend for inclusion in the bespoke cybercrime legislation. The above adjustment would align the consent defence and the property protection defence with other specific defences that we recommend for the offences of illegal interference with computer data (and computer system), ie all defences adopt the requirement of "reasonableness" as a matter of consistency. As with the defences to the Access Offence, we believe this approach would avoid abuse of the defences, reflecting our guiding principle of balancing the rights of netizens and interests of persons in the information

---

35 Para 4.1.
36 Paras 2.95 to 2.99.

technology industry on one hand, and protection of the public's interest and right not to be disturbed or attacked when using their computer system on the other hand.

4.43 Upon review of S64(2), we noted that the "lawful excuse" under the existing S64(2)(b) of the CO is confined to the protection of property and does not cover the protection of human lives. We have therefore considered whether the specific defence to the offences of illegal interference with computer data (and computer system) should provide for the protection of life and/or prevention of physical harm to a person.

4.44 We tend to think that the general "reasonable excuse" defence under Recommendation 6 could cater to situations where a person interfered with computer data (or computer system) for the protection of life and/or prevention of physical harm, so it might not be necessary to propose another defence for this specific purpose. We believe that the absence of an express specific defence on the protection of lives may leave the court more room to manoeuvre in situations where human lives are at stake. Accordingly, we are content to maintain the status quo of S64(2)(b) in this respect. The same principle and reasoning apply to the Access Offence discussed in Chapter 2.

## Conclusion on Recommendation 6

4.45 To summarise, we conclude that Recommendation 6 can be retained, but recommend refining S64(2) for the purposes of the offence of illegal interference with computer data and including a defence for data interference for cybersecurity purposes.

**Final Recommendation 6**

**We recommend that:**

**(a) Subject to a statutory defence of reasonable excuse, intentional interference (damaging, deletion, deterioration, alteration or suppression) with computer data without lawful authority 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, instead of malice);**

**(iii) the two defences identified under section 64(2) subject to such refinement as may be required for their proper articulation in the light of the reformulation of the offence under paragraph (a) above, while preserving any other lawful excuse or defence recognised by law; and**

**(iv) the aggravated offence under section 60(2).**

**(c) The two defences covered under section 64(2) apply to situations where a defendant:**

**(i) interfered with computer data in the belief that his act was, or would be, consented to; or**

**(ii) interfered with computer data in the belief that the property was in immediate need of protection, and the means of protection adopted was reasonable having regard to all the circumstances.**

**The defendant's belief under both the consent defence and the property protection defence must be reasonably held.**

**(d) 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).**

**(e) There should be a specific defence for illegal interference with computer data for cybersecurity purposes with the following conditions:**

**(i) The defendant must be an accredited cybersecurity practitioner (the details of the accreditation regime, which are essentially matters of policy, are best left to the Government's consideration);**

**(ii) The defendant must act for a genuine cybersecurity purpose; and**

**(iii) The defendant's conduct must be reasonable having regard to all the circumstances.**

# Chapter 5

# Illegal interference with computer system

## Introduction

5.1 This Chapter discusses the responses regarding Recommendations 7 and 8 of the Consultation Paper. Recommendation 7 proposes the fourth cyber-dependent offence, namely illegal interference with computer system:

> "*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*
>
> *(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.*"

5.2 As explained in the Consultation Paper,[1] broadly speaking, the offence of illegal interference with computer system 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.

## Current Hong Kong law

5.3 This Chapter builds on the discussion in Chapter 4, given the close relationship between the offences of illegal interference with computer data and illegal interference with computer system ("**Interference Offences**"). As stated in Chapter 4,[2] one form of criminal damage under section 60 of the Crimes Ordinance (Cap 200) ("**CO**") 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."*

Among the three limbs, section 59(1A)(a) is the most relevant to the proposed offence of illegal interference with computer system.

5.4 As the Sub-committee explained in the Consultation Paper,[3] illegal interference with computer system may take the form of a distributed denial of service ("**DDOS**") attack, which is defined as "*[t]he intentional paralysing of a computer network by flooding it with data sent simultaneously from many individual computers*".[4] A DDOS attack is often perpetrated by

---

1 At para 5.1.
2 Para 4.10.
3 At paras 5.3 and 5.4.
4 https://www.cpaaustralia.com.au/tools-and-resources/cyber-security/cyber-threats-introduction (accessed on 1 Nov 2025).

means of a group of compromised computers known as a "botnet". 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.

## Responses to the Sub-committee's Recommendation 7

5.5 As the proposed offence of illegal interference with computer system is closely related to that of illegal interference with computer data, the responses on Recommendation 7 were largely similar to those on Recommendation 6 that we discussed in Chapter 4.

5.6 An overwhelming majority of the Respondents expressed their support for Recommendation 7. Amongst them, the Hong Kong and Mainland Legal Professional Association Limited and the Hong Kong Federation of Women Lawyers Limited ("**HKFWL Ltd**") agreed that the existing regime under the CO operates satisfactorily and that the concept of "misuse of a computer" sufficiently covers acts of interference with a computer system. Thus, HKFWL Ltd agreed with Recommendation 7 that the provisions regarding illegal interference with computer system and illegal interference with computer data should be phrased in the same way.

### *Recklessness as one of the mens rea elements of the proposed offence*

5.7 As with Recommendation 6, a number of Respondents who provided feedback on Recommendation 7 sought clarification on the inclusion of "recklessness" as one of the mental elements of the proposed offence of illegal interference with computer system. A few information technology-related organisations suggested that the proposed offence should only arise if there is "criminal intent", and that the element "recklessly" in Recommendation 7 should be discarded.

5.8 Readers will recall that Recommendation 7(d) of the Consultation Paper listed a few examples of how the proposed offence of illegal interference with computer system may apply. These include a person who "intentionally" or "recklessly" coded a software with a bug during its manufacture.[5] Two information technology-related bodies suggested that bugs are commonly found in computer software, computer applications and devices. One of them opined that bugs may emerge from premature innovations of program developers. Since testing may be subject to time and resource constraints, it is not unusual that some of the security issues identified have not been rectified by the software developers before launch. This Respondent asked whether,

[5] Recommendation 7(d)(ii).

in such circumstances, the software developers would be liable for the proposed offence.

5.9 Meanwhile, the Law Society of Hong Kong commented that the legal basis of imposing criminal liability on a reckless flooding of a computer system deserved more comprehensive analysis. An example cited by this professional body was fans fighting online to snap up concert tickets.

## Our analysis and response

### *Tackling data and system interference consistently*

5.10 Given the proximity between the Interference Offences, our analysis on "recklessness" as an alternative *mens rea* element of the proposed offence of illegal interference with computer data in Chapter 4 equally applies to the Respondents' comments on Recommendation 7.[6]

5.11 To recap, "intention" and "recklessness" are alternative *mens rea* elements of the offence of criminal damage under the existing section 60(1) of the CO, and the current statutory framework for the criminal damage offence applies to "*misuse of a computer*" by virtue of section 59(1)(b) and (1A). Therefore, Recommendation 7, which proposes to tackle illegal interference with computer system and illegal interference with computer data consistently by adopting the current regime under section 60, likewise adopts the mental elements of "intention" and "recklessness" for the proposed offence of illegal interference with computer system.

5.12 We repeat our observation in Chapter 4 that "recklessness" is a common and well-established fault element in criminal offences. The notion of "recklessness" requires proof that a defendant was aware of a specific risk and that, in the circumstances known to him, it was unreasonable to take the risk.[7] This interpretation of recklessness applies to criminal law in general, and not only cybercrimes. As to whether or not a defendant was reckless in interfering with the computer system concerned in a particular scenario (eg that in procuring concert tickets online and that in developing a software for robotic micro-surgery can be very different), it is ultimately for the court to make the evaluation and assessment based on the evidence of the individual case against the whole of the circumstances. The context in which a defendant's act took place therefore does not by itself justify the exclusion of the application of the proposed offence on the ground of recklessness.

5.13 When the notion of "recklessness" as explained above is properly understood, a program developer's general knowledge of the existence of software bugs or defects is not of itself sufficient for establishing the requisite

---

6 Our analysis is set out in paras 4.17 to 4.22.

7 *Archbold Hong Kong 2025*, at para 16-40.

mental element for the interference offence. The threshold of "recklessness", as well as the culpability that it represents, is higher than that of mere carelessness or negligence in general. In the context of software development, factors such as whether the program developer has followed the industry standards in quality assurance will certainly be relevant towards the court's assessment of what constitutes recklessness. As it is common knowledge that some bugs or defects which are reasonably expected are inevitable in software development, a person who purchases or otherwise acquires any given program or software may be regarded as having consented to the general existence of possible inconvenience or even security vulnerabilities which are reasonably tolerable within the product. This being the case, the consent defence under section 64(2) of the CO ("**S64(2)**"), which we also propose to be included in the new cybercrime legislation for the Interference Offences, [8] may potentially apply to absolve the program developer from liability of the offence of illegal interference with computer system.

5.14 For the above reasons, we recommend retaining "recklessness" as a fault element alongside "intention" for the offence of illegal interference with computer system. In sum, we also retain our recommendation that the proposed provisions regarding illegal interference with computer data and illegal interference with computer system should be phrased in the same way.

## Conclusion on Recommendation 7

5.15 For all these reasons, and considering the overwhelming support for the offences of illegal interference with computer system (and computer data), we conclude that Recommendation 7 can be retained.

**Final Recommendation 7**

**We recommend that:**

**(a) The proposed provisions regarding the illegal interference with 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 with computer system and should also be adopted in the new legislation.**

[8] Para 4.39 above. We also recommend that the defences identified under S64(2) of the CO be applicable to the offence of illegal access to program or data discussed in Chapter 2 (see paras 2.95 to 2.97 above).

**(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 with 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**

**(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.**

## Responses to the Sub-committee's Recommendation 8

5.16 Recommendation 8(a) and (b) of the Consultation Paper sought views 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); 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?*"

***Recommendation 8(a)***

5.17 A clear majority of Respondents expressly agreed with providing a defence to scanning (or similar form of testing) of a computer system by cybersecurity professionals. Some Respondents who considered such a defence unnecessary suggested that cybersecurity professionals are unlikely to undertake security scanning, assessment or other services without a clearly drafted contract.

5.18 The Hong Kong Bar Association commented:

> "*Given the variety of legitimate actions which may be undertaken by both cybersecurity and non-security professionals vis-à-vis a computer system for using selected information or observation therein (eg identifying system vulnerability), it would not be desirable to attempt to define exhaustively the type of actions which would constitute a 'lawful excuse' under the proposed offence ... this approach offers [the] much needed flexibility for the law to consider the actions of the defendant professional on a case-by-case basis. This would, in turn, enable courts to be able to consider the defence in a much wider range of scenarios.*"

***Recommendation 8(b)***

5.19 Similar to Recommendation 8(a), a clear majority of Respondents supported a defence for non-security professionals.

5.20 The Consumer Council commented that:

> "*web scraping and web crawling collects publicly accessible data on the Internet and is commonplace in Hong Kong and worldwide.*

*For instance, Google uses web crawling to index pages for its search engine. A blanket prohibition on web scraping and web crawling of information publicly accessible on the Internet may inhibit research and studies (whether for commercial, archiving, news reporting, academic or advisory purposes) required for improving market transparency, empowering consumers to make informed consumption choices and advancing consumer protection.*"

5.21 Further, the Council stated in its response that to the extent that the data in question may be subject to copyright, the website's terms of use, or contains personal data, the collection and/or use of such data is regulated by copyright law, contract law and privacy law. If the manner or means of collection of these data is illegal, such behaviour may be caught by the proposed cyber-dependent crimes.

5.22 In addition, on the basis that "web scraping" may include "data scraping" (where a computer program extracts data from output generated by another program), the Office of the Privacy Commissioner for Personal Data pointed out that only "consensual" or "lawful" interference with computer system should constitute a defence to the proposed offence. This is because from their enforcement experience:

"*the personal data collected by data scraping would sometimes be sold in the dark web without the knowledge and consent of the data subject, with the scrapping itself constituting a data breach incident. To enhance cybersecurity, in our view unauthorised web scraping (including data scraping) and scanning of a service provider's system should also be caught by the proposed offence, and only consensual, or lawful, interference of computer system should constitute a defence …* "

## Our analysis and response

### *Recommendation 8(a): Specific defences*

*Interference with computer system for cybersecurity purposes*

5.23 In Chapter 4,[9] we recommended that interference with computer data for cybersecurity purposes should be a defence to the proposed offence of illegal interference with computer data in the following terms:

(a) The defence should only be available to accredited cybersecurity practitioners (the details of the accreditation regime, which are

[9] Our analysis is set out in paras 4.34 to 4.35.

essentially matters of policy, are best left to the Government's consideration).

(b) The defendant must act for a genuine cybersecurity purpose.

(c) The defendant's conduct must be reasonable having regard to all the circumstances.

5.24 Given the close relationship between the two Interference Offences, we similarly recommend that interference with computer system for cybersecurity purposes should be a defence to the proposed offence of illegal interference with computer system. Accordingly, scanning (or any similar form of testing) of a computer system on the internet would not contravene the law if the conditions in the preceding paragraph are satisfied.

*Interference with computer system for protecting the interests of a child or vulnerable person*

5.25 As explained in Chapter 4,[10] we consider it unnecessary to provide a specific defence to the offence of illegal interference with computer data for the purpose of protecting the interests of a child or vulnerable person. This is because firstly, access to program or data in itself does not cause any interference with the computer data, and secondly, allowing a person access to program or data does not mean that the person is authorised to tamper with the data.

5.26 As the above logic also applies in the case of interference with computer system, we are of the view that it is not necessary to include a specific defence to the offence of illegal interference with computer system for the purpose of protecting the interests of a child or vulnerable person.

*Interference with computer system for genuine research purposes*

5.27 As with interference with computer data, we find it inconceivable that the conduct of genuine research would necessitate interference with a computer system. Thus, we take the view that it is not necessary to provide a specific defence to exempt illegal interference with computer system carried out for genuine research purposes.

*Transposing the defences under S64(2) of the Crimes Ordinance*

5.28 We repeat our analysis in paragraphs 4.39 to 4.44 above. In gist, when transposing the defences under S64(2) of the CO to the new cybercrime legislation, we recommend refining the consent defence and the property

[10] Paras 4.36 and 4.37.

protection defence for the purposes of the offence of illegal interference with computer system as follows:

(a) in the case of the consent defence, the defendant must *reasonably* believe that there was, or would be, consent to his interference with the computer system; and

(b) in the case of the property protection defence, the defendant must *reasonably* believe that the property was in immediate need of protection.

***Recommendation 8(b): Not necessary to propose defence for non-security professionals***

5.29 Cybersecurity professionals aside, we are aware that some activities, which do not necessarily serve any cybersecurity purposes, are inherent in the operation of cyberspace or interaction between computer devices or systems. As mentioned in Recommendation 8(b) of the Consultation Paper, examples of these activities include web scraping (ie the process of using bots to extract content and data from a website) and web crawling (ie an internet bot that systematically browses webpages for the purpose of indexing).

5.30 With the benefit of expert views, the Sub-committee further understands that the normal use of computer systems would necessarily generate traffic. For instance, Application Program Interface, which supports messaging platforms (such as WhatsApp and Telegram), acts as an intermediary layer that processes data transfers between computer systems, thereby enabling companies to open their application data and functionality to third parties.

5.31 It would be impossible to exhaustively set out all the legitimate activities in cyberspace which we consider to be part and parcel of our digital life and hence acceptable. This is particularly so when we take into account the quick pace of technological development. In this connection, we agree with the Sub-committee's view expressed in the Consultation Paper that when a person opts to connect himself to the internet, he or she is taken to have impliedly consented to any interaction that can reasonably be expected to occur in the use of cyberspace. For example, 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 that search engines use software known as web crawlers that explore the web regularly to find pages to add to their index.[11]

[11] Consultation Paper, at para 2.5.

5.32 In terms of proposing the defences to the offence of illegal interference with computer system and the Access Offence for non-security professionals, we have the following observations:

(1) Communications on the internet and the use of computers necessitate a certain level of interaction between computer systems. We should avoid inadvertently outlawing some widely accepted internet practices that should be permitted by virtue of the normal functioning of the internet or computer systems.

(2) The cybercrime legislation in other countries has not provided any specific defences for non-security professionals (such as the operation of search engines) although they have enacted the offences of illegal interference with computer system and illegal access to program or data.

5.33 In light of the above, we consider it unnecessary to provide a specific defence for non-security agents encountered in the day-to-day operation of cyberspace, which can be determined as a question of fact and degree and should be distinguishable from a cyber-attack (eg when 10,000 emails are sent to a specific mailbox within a minute to overwhelm it and its corresponding server). Nevertheless, if, during the legislative stage, the implementing bureau or the Law Draftsman considers it necessary to expressly provide for a defence in this regard, the issue may be further explored at that stage.

**Final Recommendation 8**

**We recommend that:**

**(a) There should be a specific defence for illegal interference with computer system for cybersecurity purposes with the following conditions:**

**(i) The defendant must be an accredited cybersecurity practitioner (the details of the accreditation regime, which are essentially matters of policy, are best left to the Government's consideration);**

**(ii) The defendant must act for a genuine cybersecurity purpose; and**

**(iii) The defendant's conduct must be reasonable having regard to all the circumstances.**

**(b) It is not necessary to provide any specific defence to the proposed offence of illegal interference with computer system for non-security professionals (such as web scraping by robots or web crawlers initiated by internet information collection tools to collect data from servers without authorisation by connecting to designated protocol ports) since activities which form part of the normal functioning of the internet or computer systems should continue to be allowed under the principle of implied authorisation.**

# Chapter 6

# Making available or possessing a device, program or data for committing a cyber-related crime

## Introduction

6.1 This Chapter discusses the responses regarding Recommendation 9 of the Consultation Paper, which concerns the fifth (last) cyber-dependent offence, ie making available or possessing a device or data for committing a crime.

"*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.*

*(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 a 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.*"

6.2 As the Sub-committee explained in the Consultation Paper,[1] broadly speaking, an offence in respect of this subject matter would seek to:

(a) curb the production, 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.

6.3 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 to program or data ("**Access Offence**") discussed in Chapter 2. This Chapter focuses on a distinct offence, ie making available a device, program or data made or adapted to commit a cyber-related crime (eg a hacking device), which includes the offence of possessing such a device, program or data for the purpose of making it available.

6.4 Apart from a hacking device, examples of devices, programs and data with only harmful use include:[2]

(a) a thumb drive storing ransomware;

(b) malware;

---

1 At para 6.1.

2 Consultation Paper, at paras 6.2, 6.10 and 6.91.

(c) virus;

(d) software for creating and managing botnets; and

(e) 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.

## Current Hong Kong law

### *Section 62 of the Crimes Ordinance (Cap 200) ("CO")*

6.5 As explained in the Consultation Paper,[3] section 59(1A) already provides that in Part VIII of the CO, "*to destroy or damage any property in relation to a computer includes the misuse of a computer*".[4] Accordingly, the offence under section 62 ("*Possessing anything with intent to destroy or damage property*") in Part VIII 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."*

6.6 Nevertheless, there are two major potential issues with section 62 which warranted consideration for law reform:

(a) The English text of section 62 describes the proscribed object as "anything". This term, in common parlance, is not restricted to tangibles and appears to be broader than the corresponding term in the Chinese text ("任何物品"). However, whether the natural meaning of the Chinese term clearly extends to certain

---

3 Consultation Paper, at para 6.6.

4 "*Misuse of a computer*" is defined in s 59(1A)(a) to (c) of the Crimes Ordinance (Cap 200). This concept relates to the offences of illegal interference with computer data and illegal interference with computer system discussed in Chapters 4 and 5 (see paras 4.10 and 5.3 above).

intangibles (such as malware and know-how regarding an exploit) is another question.[5]

(b) Section 62 is linked to the offence of criminal damage under section 60 of the CO. It does not apply with regard to an offence under another provision, eg section 161 of the CO ("*Access to computer with criminal or dishonest intent*").[6]

6.7 Against this background, the Sub-committee, having considered section 62 and other legislative provisions in Hong Kong and other jurisdictions, made Recommendation 9 as set out in the Consultation Paper.

## Responses to the Sub-committee's Recommendation 9

6.8 Compared with the other four cyber-dependent crimes canvassed in Chapters 2 to 5, Recommendation 9 has sparked much debate among the public. Respondents were almost evenly divided between those who supported and opposed the recommendation. A substantial number of Respondents provided comments or observations without expressly supporting or objecting to the proposed offence.

### *Comments from Respondents who supported Recommendation 9*

6.9 A business association recognised that the proposed offence "*is to some extent covered by*" section 62 of the CO, which prohibits the custody or control of anything intended for use in destroying or damaging property, ie in committing the criminal damage offence under section 60 of the CO. This Respondent agreed with the Sub-committee's analysis in the Consultation Paper that section 62 might exclude intangibles (such as computer software), which would not be conducive to the application of this provision to cyberspace.[7]

6.10 The Hong Kong Chartered Governance Institute, which expressed support for Recommendation 9, agreed that the proposed offence

5 Consultation Paper, at paras 6.9 and 6.10.
6 Consultation Paper, at para 6.16.
7 Same as above, at paras 6.9 to 6.15.

may model on sections 8[8] and 10[9] of the Computer Misuse Act 1993 of Singapore ("**CMA-SG**"), as Recommendation 9(e) proposed.

### *Comments from Respondents who opposed or otherwise commented on Recommendation 9*

6.11 A number of Respondents, notably those in the information technology sector, opposed the basic offence in Recommendation 9(a). Their concerns were echoed in the submissions from other organisations, including the Law Society of Hong Kong ("**Law Society**") and the Consumer Council, which provided general observations on the proposed offence.

### *The broad nature of the basic form of the proposed offence*

6.12 The main concern emerging from the Respondents' submissions (regardless of how they approached the analysis) is the breadth of the basic form of the proposed offence.

*The intention of the person who possesses the device or data*

6.13 The Law Society opined that the proposed offences framed under Recommendation 9(a) to (e):

> "*are extremely wide, with a low threshold for prosecution … Under the proposal, possessing data (tangible or intangible) which may be adapted to commit a crime (not necessarily cyber-crime) would be an offence. A person who believes that the*

---

8 Section 8(1) of the CMA-SG provides that:
"*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.*"

9 Section 10 of the CMA-SG provides that:
"*(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 s 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 s 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 s 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.*"

*data in question could be used to commit an offence would be caught*".

6.14 As an illustration, this professional body provided the following hypothetical example:

> " *… if a party (A) passes to another party (B) a digital private photo of a celebrity having intimate moments with a third party, B in theory could be guilty of the offence, as (i) that photo can be used to blackmail the celebrity, and (ii) B believes that that photo could be used to commit the offence of blackmail… The above could have wide implications as, e.g. B, in the example is a private investigator, and A is his client. The client passes to the private investigator the digital photos for advice. The private investigator potentially could be charged for the proposed offence. This is worrying – in this example the private investigator would be put at risks [of] prosecution, when he is receiving data only to do his job legitimately. Why should he be put at risk for prosecution?*"

6.15 A number of Respondents from the information technology sector opined that the proposed offence should only arise if a "*criminal intent*" exists and "*the only use of the tool(s) is for criminal purposes, and the criminal act has actually been performed*". This suggestion in effect called for the removal of the basic form of the proposed offence.

6.16 The Consumer Council elaborated its concerns over the proposed basic offence in these terms:

> "*The Council understands the Sub-committee's concern that if subjective intent of a defendant was required, the need to prove the subjective mental state of the defendant would give rise to evidential difficulty. Nonetheless, in the absence of the need to prove criminal intent, the proposed basic offence would be too wide in scope such that consumers could contravene the law unintentionally… The proposed disregard of any other legitimate purpose of the device or data as well as the subjective intent of the possessor as to the use of the device or data is also concerning. For instance, a consumer having in his possession a device for a legitimate purpose could be committing the proposed basic offence if the objective primary use of such a device is illegitimate irrespective of whether the consumer was aware of such primary use.*"

*Use of the device or data to commit any offence*

6.17 The Consumer Council and a few information technology bodies considered that the proposed offence (whether in basic or aggravated form)

should only arise if the device or tool concerned is used to commit one of the other four cyber-dependent crimes considered in Chapters 2 to 5,[10] but not any offence at large.

### *The "reasonable excuse" defence*

6.18 Under Recommendation 9(a) of the Consultation Paper, the proposed offence includes a statutory defence of reasonable excuse, given that there can be various legitimate reasons for a person or entity to deal with devices or data that can be used to commit a crime.[11]

6.19 The Consumer Council and a few other Respondents from the business and information technology sectors favoured greater certainty over the ambit and application of this statutory defence on the grounds that "reasonable excuse" is not defined and subject to interpretation. Some of them suggested formulating a non-exhaustive list of statutory examples of legitimate activities which would fall within the "reasonable excuse" defence.

## Our analysis and response

### *Background*

6.20 The introduction of the basic form of the proposed offence sprang from the Sub-committee's consideration of the offence of possession of offensive weapons under the Public Order Ordinance (Cap 245) ("**POO**"). In the Consultation Paper, the Sub-committee observed that:

(a) as far as offensive weapons are concerned, the POO differentiates between articles made or adapted for causing injury and those intended for such use. When applying the definition of "*offensive weapon*" to objects such as a gun, a machete, a butterfly knife, an umbrella with a bayonet attached, or a rod that has been sharpened and has spikes attached, criminal intent need not be proved and mere possession in a public place of the same suffices for criminal liability;[12] and

(b) it is common for devices and data to have both legitimate and illegitimate uses. For example, a degausser possessed by a financial institution for clearing the content of old hard disks as a security measure is legitimate, whereas possessing the same

---

[10] Namely, illegal access to program or data (Chapter 2), illegal interception of computer data (Chapter 3), illegal interference with computer data and illegal interference with computer system (Chapters 4 and 5).

[11] Consultation Paper, at para 6.87.

[12] Same as above, at para 6.71.

tool with intent to use it for illegitimate purposes (eg sabotage) justifies assumption of criminal liability.[13]

6.21 Given the above considerations, Recommendation 9 in the Consultation Paper borrowed the taxonomy under the POO and split the proposed offence into a basic form and an aggravated form. As the Sub-committee explained,[14] 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.

### *A holistic approach towards the proposed offence and related defences*

6.22 The feedback from the public consultation provided us with a fresh opportunity to revisit Recommendation 9. We agree that it is not a straightforward question to transpose the existing concept of "offensive weapon" in the physical world to the cyber world. Compared to offensive weapons in the physical world (such as a brass knuckle), the primary use of a device, program or data for criminal purposes is less conspicuous and a person may not appreciate the malicious nature of a device, program or data.

6.23 In considering the breadth of the proposed offence and the related defences under Recommendations 9 and 10, we have worked through all relevant issues holistically. If the scope of certain elements of the proposed offence is widened, it may be necessary to adjust other parts of the offence, or provide appropriate defences or exemptions, to ensure that the offence is not overly broad. We shall explain our Final Recommendations in detail in this Chapter.

### *Including "program" in the proposed offence, ie "device, program and data"*

6.24 This revision stems from the suggestion of the Hong Kong Police Force, which proposed to align the proposed offence with the Access Offence discussed in Chapter 2, where the criminal act is associated with "program or data" rather than a computer. As our proposed offence intends to also prohibit the use of physical "devices" for commission of cybercrime,[15] we maintain our view that "device" should be kept as one of the subject matters of the proposed offence.

---

13 Same as above, at para 6.70.
14 Same as above, at para 6.72.
15 Para 6.2 above.

6.25 That said, we consider it appropriate to include "program" as one of the possible subject matters of the proposed offence, which aims to combat cybercrime. This position also accords with the standard of criminalisation under Article 6 of the Council of Europe's Convention on Cybercrime,[16] which requires each party to adopt measures to criminalise:

> "*the production, sale, procurement for use, import, distribution or otherwise making available of … a device, including a computer program, designed or adapted primarily for the purposes of committing any of the [cyber-dependent] offences established in accordance with Articles 2 through 5.*"
>
> (emphasis added)

***Limiting the application of the proposed offence to cases where a device, program or data is used to commit a cyber-related crime***

6.26 On reflection, we recommend that the proposed offence should only apply if the offence committed by making available a device, program or data (or possessing such device, program or data for the purpose of making it available) is one of the four other cyber-dependent crimes discussed in Chapters 2 to 5, namely the Access Offence, illegal interception of computer data, illegal interference with computer data and illegal interference with computer system ("**Interference Offences**" for the last two offences).

*Background*

6.27 We understand that in making Recommendation 9 in the Consultation Paper, the Sub-committee aimed for a catch-all offence to guard against the misuse of devices, programs or data – if a person acquired or supplied devices, programs or data for committing a crime, that person should, in theory, be liable.

*Implications of the original Recommendation 9*

6.28 We agree that the legitimate purpose of proscribing misuse is important, but the issue that the term "device" permits a wide construction also deserves attention. If the illegitimate use of a device, program or data is not restricted to the commission of cybercrime, Recommendation 9 will take the proposed offence beyond the cyberworld and have an all pervasive application in the physical world. For instance, if a person who composes an email that seeks to blackmail a victim eventually decides not to send the email but to keep the draft, he will be in possession of data that can be used

[16] Consultation Paper, at para 6.20.

to commit "an offence", and hence be guilty of the proposed offence under the Sub-committee's Recommendation 9.

*Legislation in other jurisdictions*

6.29 We further note that the cybercrime legislation in other jurisdictions discussed in the Consultation Paper has consistently confined the scope of the proposed offence to the commission of cyber-dependent crimes.[17]

6.30 As Recommendation 9 was formulated in light of the precedent legislation in New Zealand,[18] namely the then prevailing section 251(1) of the Crimes Act 1961, it is apposite to examine this provision in greater detail. Section 251(1) read:

> *"Every one is liable to imprisonment for a term not exceeding 2 years who invites any other person to acquire from him or her, or offers or exposes for sale or supply to any other person, or agrees to sell or supply or sells or supplies to any other person, or has in his or her possession for the purpose of sale or supply to any other person, any software or other information that would enable another person to access a computer system without authorisation—*
>
> *(a) the sole or principal use of which he or she knows to be the commission of an offence; or*
>
> *(b) that he or she promotes as being useful for the commission of an offence (whether or not he or she 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.*"
>
> (emphasis added)

6.31 On closer examination, it can be discerned that the scope of the New Zealand offence created by section 251 was in fact qualified by the requirement that the software or information must be capable of enabling another person to access a computer system without authorisation. Thus, the New Zealand offence was not so wide as to cover software or information capable of simply being used to commit "*any offence*" in general. The

---

17 Consultation Paper, at paras 6.22 (Australia), 6.29 (Canada), 6.36 (England and Wales), 6.43 (Chinese Mainland) and 6.58 (Singapore).

18 Consultation Paper, at para 6.74, where the Sub-committee remarked that "*in light of the precedent legislation in New Zealand, 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*".

position remains the same when the repealed section 251 has now been re-enacted by way of section 254 albeit with refinements.[19]

6.32 On further thought, it can also be observed that if a person uses a device, program or data for committing other general offences that are not cybercrime, the culpable conduct can be tackled under the myriad of statutory and common law offences in Hong Kong and it is not necessary to invoke the bespoke legislation which targets cybercrime.

6.33 We see other merits of confining the application of the proposed offence to cybercrime only. Apart from preventing our recommendation from venturing into other areas of existing law that do not solely pertain to computer crimes (eg doxxing, copyright offences), limiting the application of the proposed offence in this manner provides an added justification for applying the offence widely to devices, programs and data.

*Reference to "cyber-related crime"*

6.34 At this stage, the term "cyber-related crime" primarily refers to the four types of cyber-dependent offences discussed in Chapters 2 to 5,[20] which, together with the offence proposed in this Chapter, form the core crimes considered under Part One of our study.

6.35 Nevertheless, as cybercrime evolves quickly, the new bespoke cybercrime legislation ought to be flexible. To ensure that the cybercrime legislation can keep abreast of technological developments, we recommend

---

[19] Section 251 was repealed by s 65 of the Budapest Convention and Related Matters Legislation Amendment Act 2025, which came into operation on 31 July 2025. This Act added new ss 253 and 254 to the Crimes Act 1961 to align with Article 6 of the Council of Europe's Convention on Cybercrime (known as the Budapest Convention), which, generally speaking, proposed offences targeting the production, sale, making available and possession, etc of computer software or information for the commission of the cyber-related offences set out in Articles 2 to 5 of the Convention. Both ss 253 and 254 deal with acts relating to software or information that would enable a person to commit a cyber-related offence. Section 253 targets the designing, writing or adapting of a wider range of software, ie software that would enable a person to commit the offences of accessing computer system for a dishonest purpose (s 249), damaging or interfering with computer system (s 250) and accessing computer system without authorisation (s 252) whereas s 254 concentrates on the dealing in or possession of software or other information for committing a s 252 offence only. As stated in the Explanatory Note to the Budapest Convention and Related Matters Legislation Amendment Bill:

(a) section 253 aligns with Article 6 of the Convention, to the extent that Article 6 relates to producing computer programs for the purpose of committing any of the offences along the lines of those set out in ss 249, 250 and 252; and

(b) section 254 generally re-creates the effect of the repealed s 251, which, to the extent that it relates to software and certain kinds of information, generally aligns with Article 6 of the Convention. The main substantive changes in s 254, which "*ensure more complete alignment with Article 6 of the Budapest Convention*" are (i) procuring the relevant software or other information is added to the kinds of dealings covered by the offence set out in the old s 251(1); and (ii) extending the offence to a person who intends software or other information to be used by any other person to commit an offence.

Notwithstanding the repeal of s 251 and re-creation (with refinement) of substantively the same offence in the new s 254, the scope of both sections is the same in that the provision is confined to the purpose of committing the offence of accessing computer system without authorisation under s 252.

[20] Namely, illegal access to program or data (Chapter 2), illegal interception of computer data (Chapter 3), illegal interference with computer data and illegal interference with computer system (Chapters 4 and 5).

that the legislation include a list of cyber-related offences in a Schedule, whose contents may be expanded or otherwise adjusted by legislative amendments in response to the ever-changing social conditions. This approach is commonly adopted in legislation, including the Magistrates Ordinance (Cap 227), Schedule 2 to which lists the offences that cannot be dealt with summarily by a magistrate.

6.36 We would consider what else, if any, should also come under the list of "cyber-related offences" to be scheduled to the bespoke cybercrime legislation in Part Two of our study, which will cover cyber-enabled crimes.

***Recasting the possession limb of the proposed offence***

6.37 After careful consideration, we come to the view that there are far too many possibilities as to how a person may interact with programs or data in the use of cyberspace in everyday life. The result is that a person may possess a malicious program or data in a wide range of innocent scenarios. Below are just a few examples:

(a) A person may learn from an anti-virus scan run on his computer that he is in possession of a malicious program or data, but the anti-virus scan may not provide an average computer user with a lot of information about the nature or impact of the malicious program or data.

(b) A computer system may generate an automatic message informing its user that his device has been "infected" with something. Being slothful or computer-illiterate, the user may not make any effort to understand or look into the problem reported by the computer.

(c) In the two examples above, although the person continues to "possess" the malicious program or data, the person may have no intent to use it to commit cybercrime or any other crime.

6.38 Furthermore, the degree of harm posed by devices, programs or data that may be used to commit a cyber-related crime varies, and so does the perception of a lay person towards such devices, programs or data. For instance, while it may be clear that bots are harmful, malicious spam emails may be less recognisable. We cannot even be sure whether an average computer user is able to recognise a "bot" (as distinguished from other types of malware) if a bot finds its way into a person's computer.

6.39 We consider it reasonable that as long as the person does not intend to use the program or data to commit a cyber-related crime (ie the aggravated form of the proposed offence), the person should not attract

criminal liability by reason of merely in possession of such program or data. Accordingly, to avoid over-criminalisation, we recommend recasting the possession limb in Recommendation 9(a) as an offence of "*possessing a device, program or data made or adapted to commit a cyber-related crime for the purpose of making it available to another*".

6.40 This possession offence, in its narrower form as now revised, will not punish persons who possess a device, program or data made or adapted to commit a cyber-related crime in non-culpable circumstances, including those discussed in paragraph 6.37 above. In other words, mere possession without any intention of using the device, program or data or making the same available to another will not be a crime, but criminal liability will attach to a person who possesses the device, program or data for his own use to commit a cyber-related crime.

### *Incorporating additional mens rea requirements into the proposed offence*

6.41 As mentioned above,[21] we see the difficulty of applying the taxonomy of the offence of possession of offensive weapons under the POO to cyberspace. One reason is that a person may not accurately know or understand the primary use of a device, program or data. For example, a person may download a program on the understanding that the program is harmless (ie the person does not appreciate the malicious nature of the program). This is particularly so in cases where the harmful nature of a program is not readily identifiable, or where the harmful program is not well-known. If the person also does not intend that the program be used for committing a cyber-related crime, the basis of imposing criminal liability on the person seems questionable.

*Knowledge, belief, etc in respect of the nature of a device, program or data*

6.42 Therefore, we recommend that the proposed offence should incorporate an additional *mens rea* requirement – the prosecution must prove that the defendant knows, believes, or claims that the primary use of a device, program or data (determined objectively) is to commit a cyber-related crime. With this requirement, if a person misunderstands the nature of the device, program or data, or does not know that its primary use is criminal, the person will not be liable for the proposed offence.

6.43 Although the additional *mens rea* requirement will impose a higher evidential threshold for the prosecution, we consider it fair and reasonable to include this requirement. After all, programs and data are not something that the court may have their true nature determined by visual

[21] Para 6.22.

inspection as the court otherwise may in the case of physical objects (eg an offensive weapon).

6.44 We anticipate that if the primary use of a device, program or data is at issue, expert evidence will have to be adduced by the contesting parties for adjudication. For instance, if the setting of a tool is such that it will enable access by bypassing any network firewall security in any target computer, the court may be able to draw a stronger inference that the primary use of the tool is questionable. Conversely, if the evidence shows that the tool is widely used by computer system administrators or cybersecurity companies for conducting diagnostic tests or monitoring network security, then such prevailing commercial use of the tool will make it less likely for the court to find that its primary use is to commit a cyber-dependent offence.

*Whether a basic offence of "making available" should be maintained*

6.45 In the context of possession for the purpose of "making available", we have to first consider whether or not the proposed offence should require a defendant to "know" or "intend" that the device, program or data is to be used by another to commit an offence (ie the defendant must have knowledge as to the actual intended use of the device, program or data). Putting this requirement in place would in effect be abandoning the basic offence that the Sub-committee recommended in the Consultation Paper.

6.46 The potential worry in introducing such a requirement is that it may result in some suppliers of harmful devices, programs or data (eg a trojan horse,[22] zombie program[23] or virus) falling outside the ambit of the offence. This is because a supplier who simply makes available such devices, programs or data on the dark web without caring (and hence not knowing) how buyers intend to use them will not be caught.

6.47 As doing away with the basic offence altogether would run counter to the objective of the proposed offence to curb the supply and possession of devices or data that can be used in cyberspace for illegitimate purposes, we are of the view that the basic offence should be maintained, subject to the refinements recommended in paragraphs 6.39 and 6.42 above.

*Alternative mental element: having reasonable grounds to believe in the culpable primary use of a device, program or data*

6.48 We further observe that in the context of the proposed offence, although a defendant who comes into possession of, for example, a computer

---

[22] A trojan horse is a program downloaded and installed on a computer that appears harmless, but is in fact malicious. See https://www.techtarget.com/searchsecurity/definition/Trojan-horse (accessed on 1 Nov 2025).

[23] Zombie programs are programs that secretly activated on an infected machine for launching attacks on other machines. See https://www.igi-global.com/dictionary/zombie-programs/69048 (accessed on 1 Nov 2025).

program may not have actual knowledge that the program comprises a ransomware or virus (which can be used to commit a cyber-related crime), the circumstances may be so dubious as to warrant the defendant to have reasonable grounds to hold such belief. Such belief may arise if, for instance, a stranger passes a program to a defendant who is requested to upload the program to a certain computer system at a particular time on a specified date in return for a large monetary reward without any explanation, or if a defendant is asked by an anonymous person to keep a program for him in return for monetary reward for no good reasons even though that person could have done this himself.

6.49 We recognise that the addition of the "*reasonable grounds to believe*" limb as an alternative fault element would widen the proposed offence, which might apply to, for example, gullible persons who are manipulated by unscrupulous criminals. Nonetheless, we consider it appropriate to recommend this alternative mental element due to the following considerations:

(a) The mental element of "*reasonable grounds to believe*" only applies to one particular element of the proposed offence, namely the primary use of the device, program or data for the commission of a cyber-related crime. Proof of full *mens rea* on the part of the defendant in respect of the intent of "making available" or "possessing for the purpose of making available" and knowledge as to "possession" is still required. In other words, if a person who has reasonable grounds to believe that the device, program or data in his possession is made or adapted to commit a cyber-related crime cannot be proved to have the intent to make it available or possess it for the purpose of making it available to another or for his own use, he is not guilty of this offence.

(b) There is a substantial degree of criminality in knowingly making available devices, programs or data for committing cybercrime and knowingly possessing any of these items for the purpose of making them available. The "*reasonable grounds to believe*" limb, if added as an alternative basis for conviction, can serve to enhance the effectiveness in combating such criminal conduct. If the proposed offence requires proof of actual knowledge or belief on the part of the defendant on the primary use of a device, program or data, a perpetrator of this offence could easily recruit another person to carry out the prohibited acts and, without having actually informed that other person about the culpable primary use of the device, program or data, the primary offender could be confident that the recruit, even if apprehended, could not (for lack of actual knowledge or belief about the culpable primary use) be found guilty of anything despite any highly suspicious circumstances. This means two things. First, people would be less vigilant which makes

recruitment of intermediaries easier. Second, upon apprehension, those who have acted in suspicious circumstances would, knowing that they could not themselves be found guilty if there is no "*reasonable grounds to believe*" limb, have little incentive to assist the authorities in the hope of getting such credit as they deserve upon sentence.

(c) Technological advancement is making it easier for the proposed offence of making available devices, programs or data for committing a cyber-related crime (or possessing any of these items for the purpose of making them available) to be committed by anyone anywhere. Curbing this sort of behaviour, by targeting also any intermediaries, is in line with the broader objective of the proposed offence to prevent the use of harmful devices, programs or data for the commission of cybercrime. By extending the proposed offence to persons who ought to realise that a device, program or data is or are harmful, the deterrent effect and efficacy of the law is enhanced.

(d) Ordinary persons may not be conversant with various kinds of nefarious computer programs and data that can be used to commit a cyber-related crime. The "*having reasonable grounds to believe*" limb may not be triggered as easily as some may think.

(e) The concept of "*having reasonable grounds to believe*" is a hybrid of subjective and objective elements,[24] namely:

(i) What facts or circumstances, including those personal to the defendant, were known to him that may have affected his belief as to whether the primary use of the device, program or data is to commit a cyber-related crime?

(ii) Would any reasonable person who shared the defendant's knowledge be bound to believe that the primary use of the device, program or data is to commit a cyber-related crime?

With this two-pronged test, a defendant who may be regarded as "*having reasonable grounds to believe*" that the primary use of a device, program or data is offensive would not be so regarded solely because of his level of proficiency in information technology. Applying the two-stage test, the court must first decide on evidence the matters that the defendant subjectively knew of, which may have affected the defendant's belief as to the culpable primary use of the device, program or data. Then, the court must objectively decide whether any

[24] *Specimen Directions in Jury Trials*, Vol 2 (2020 Revision of Selected Topics) issued by the Hong Kong Judicial Institute, Chapter 119: "*Dealing with Proceeds of an Indictable Offence*", at 119-6 and 119-7.

reasonable person who shared the defendant's knowledge would be bound to believe that the primary use of the device, program or data was culpable. As it is the subjective matters known to the defendant that would be the basis for consideration, the "*having reasonable grounds to believe*" limb would not over-criminalise as some may worry. Very often, it would be the dubious circumstances in which the defendant came into possession of, or made available, the device, program or data which will trigger the "*having reasonable grounds to believe*" limb.

6.50 In any case, to balance between the dual objectives of plugging legal loopholes and avoiding the danger of over-criminalisation, we have proposed a range of specific defences to the proposed offence alongside the general reasonable excuse defence. Those defences will be discussed in the latter part of this Chapter.

6.51 To conclude, we recommend that if a defendant "*has reasonable grounds to believe*" that the primary use of a device, program or data is to commit a cyber-related crime, the proposed offence should also apply.

***When a defendant only makes available or possesses part of a malicious device, program or data made or adapted to commit a cyber-related crime***

6.52 With the advancement in technology, it is now possible for programs or data to be stored, accessed and shared in a decentralised way (eg in a distributed file system such as the InterPlanetary File System ("**IPFS**"), or the Blockchain technology[25]). As a result, a perpetrator may only hold a portion of the overall data, which is by itself innocent. However, with indexing systems such as Distributed Hash Tables,[26] IPFS nodes can aggregate data stored at multiple locations and make the composite malicious data available to any person who uses the IPFS software.

6.53 We have carefully considered whether it is appropriate to apply the proposed offence to circumstances where a person only possesses part of a malicious device, program or data. In our view:

(a) although a person may only make available or possess an innocuous component of a malicious software or data, in theory, it is possible for a group of persons to divide up storage of a

[25] For the meaning of blockchain, see fn 48 below.

[26] The decentralised web of an InterPlanetary File System consists of interconnected computers called nodes that use Distributed Hash Tables ("**DHT**"), a decentralised storage system that provides lookups and storage for the mapping of keys to values. In a DHT, each node is accountable for specific keys and mapped values and can effectively retrieve the corresponding value for a given key. See "*What is the Interplanetary File System (IPFS), and how does it work?*", available at https://cointelegraph.com/learn/what-is-the-interplanetary-file-system-ipfs-how-does-it-work (accessed on 1 Nov 2025).

malicious device, program or data to attack a critical infrastructure. If distributed storage or hosting continues to become more popular, it does not seem desirable if the proposed offence does not apply.

(b) while a single component in the physical world (eg nitrogen) may be used for both legitimate (eg making fertilisers) or illegitimate (eg making explosives) purposes by combining such component with other components, it is less likely that a component of a malware is simultaneously a constituent part of another innocuous program or data.

6.54 To allow more flexibility in the law, we recommend refining Recommendation 9 by specifying that the reference to a "*device, program or data*" includes a part thereof. It is important to emphasise that this revision has not fundamentally altered the nature of the proposed offence because for criminal liability to arise, it remains for the prosecution to prove the same *mens rea* elements beyond reasonable doubt, ie the person who only holds part of a malicious device, program or data:

(a) knows that he is in possession of a device, program or data (or any part thereof); and

(b) knows, believes, has reasonable grounds to believe, or claims that the primary use of a device, program or data (or any part thereof) is to commit a cyber-related crime.

***The defendant who claims (whether or not the claim is true) or mistakenly believes that the primary use of a device, program or data is to commit a cyber-related crime***

6.55 Under Recommendation 9(c)(ii) of the Consultation Paper, the Sub-committee recommended that it should suffice if a device or data is or are believed or claimed to be capable of being used to commit an offence, irrespective of whether that is true or not. As explained in the Consultation Paper,[27] this position is in line with *HKSAR v Chu Tsun Wai*[28] that criminal liability should not depend on the success of a cyberattack.

6.56 We maintain the view that a person who wrongly claims or mistakenly believes that the primary use of a device, program or data is to commit a cyber-related crime should likewise be guilty of the proposed

---

[27] At para 6.77.

[28] (2019) 22 HKCFAR 30, [2019] HKCFA 3, FACC 20/2018 (date of judgment: 1 Feb 2019). In this case, the defendant participated in a distributed denial of service 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 upheld the defendant's conviction under s 59(1A)(a) of the Crimes Ordinance (Cap 200) ("**CO**"). See the Consultation Paper, at paras 5.10 to 5.12.

offence, just as a person may be found guilty of the offence of attempting to traffic in a dangerous drug even if the person's culpable belief in the nature of the substance being trafficked turns out to be incorrect.[29]

### *The "reasonable excuse" statutory defence*

6.57 When analysing the consultation responses on the Access Offence in Chapter 2, we resolved that "reasonable excuse" should be left undefined to leave the scope of the term as wide as possible.[30] As we pointed out, whether a "reasonable excuse" exists will depend on the facts and circumstances of an individual case. The merit of not defining "reasonable excuse" is that the court may determine whether a defendant's conduct is reasonable on a case-by-case basis. These considerations equally apply to the proposed offence.

6.58 We also repeat our observations in Chapter 2 that any attempt to provide an interpretation of "reasonable excuse" in the cybercrime legislation or to illuminate the legislative intent (eg formulating a list of examples of "reasonable excuse") may run the risk of narrowing the scope of the reasonable excuse defence.[31] In cases where a defendant's act or conduct deviates from what is described in the statutory examples, there is a risk that the court may rule against the defendant. Besides, the notion of "reasonable excuse" does not sit well with the legitimate purposes that should not be regarded as contravention of the law in the first place. Thus, instead of weaving the legitimate activities into the reasonable excuse defence, we consider that the preferred approach is to express them as statutory defences, ie make it clear that those activities do not constitute a crime.[32]

6.59 Accordingly, we consider it unnecessary to provide a non-exhaustive list of examples of legitimate activities that would fall within the general "reasonable excuse" defence to the proposed offence.

6.60 As mentioned in the Consultation Paper,[33] the drafting of the other jurisdictions' offences differs significantly and demonstrates various possibilities. Subject to the adjustments to the proposed offence that we explained in the preceding paragraphs, we suggest adopting sections 3A of

---

29 Section 4(1) of the Dangerous Drugs Ordinance (Cap 134) provides that no person shall, on his own behalf or on behalf of any other person, whether or not such other person is in Hong Kong—
*"(a) traffic in a dangerous drug;*
*(b) offer to traffic in a dangerous drug or in a substance he believes to be a dangerous drug; or*
*(c) do or offer to do an act preparatory to or for the purpose of trafficking in a dangerous drug or in a substance he believes to be a dangerous drug.*"
Section 159G(1) of the CO provides that "*A person who, intending to commit an offence to which this section applies, does an act that is more than merely preparatory to the commission of the offence is guilty of attempting to commit the offence.*"

30 Para 2.32 above.

31 Same as above.

32 Para 2.33 above.

33 At para 6.88.

the Computer Misuse Act in England and Wales,[34] as well as sections 8 and 10 of the CMA-SG as the basis and improving on those provisions for formulating an offence in the bespoke cybercrime legislation.

6.61 It is also important to note that, in any event, there is always a duty on the part of the prosecution to decide on the venue for trial in respect of the many indictable offences (whether created by statute or under the common law) that are triable summarily. The key factors to be taken into account by the prosecution include the gravity of the allegations, the general circumstances of the case and the likely sentence upon conviction.[35] Thus, although the aggravated offence is indictable, the prosecution may elect to have the offence tried summarily in the Magistrates' Court if the circumstances of the case so warrant.

## Conclusion on Recommendation 9

6.62 In view of the foregoing, we conclude that Recommendation 9 should be refined as follows:

**Final Recommendation 9**

**(a) Knowingly making available a device, program or data (or a part thereof) made or adapted to commit a cyber-related crime,[36] or knowingly possessing the device, program or data for the purpose of making it available, irrespective of whether it is tangible or intangible, eg ransomware, a virus or their source code, should be a basic offence under the new legislation, subject to a statutory defence of reasonable excuse.**

**(b) The *actus reus* of the proposed offence should cover both the supply side (such as production, offering,**

---

34 Section 3A of the Computer Misuse Act of England and Wales reads:
"*(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 s 1, 3 or 3ZA.*
*(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 s 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 s 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 s 1, 3 or 3ZA.*
*(4) In this section 'article' includes any program or data held in electronic form.*"

35 Department of Justice, Hong Kong Special Administrative Region, *Prosecution Code* (2013), at para 8.4. Other factors include the issues likely to be in dispute, whether or not issues arise for determination that require the application of community standards and/or values, the public importance of the proceedings and any aggravating and mitigating factors.

36 Namely, illegal access to program or data, illegal interception of computer data, illegal interference with computer data and illegal interference with computer system.

**sale and export of a device, program or data in question) and the demand side (such as obtaining, possession, purchase and import of a device, program or data in question).**

**(c) The proposed offence should apply to a device, program or data (or a part thereof) so long as its primary use (to be determined objectively) is to commit a cyber-related crime, regardless of whether or not it can also possibly be used for any legitimate purposes.**

**(d) The *mens rea* requirements of the proposed offence are that:**

**(i) a person knows that he is making available or that he is in possession of a device, program or data (or a part thereof) for the purpose of making it available; and**

**(ii) a person knows, believes, has reasonable grounds to believe, or claims that the primary use of a device, program or data (or a part thereof) is to commit a cyber-related crime.**

**(e) A person who claims (whether or not the claim is true) or mistakenly believes that the primary use of a device, program or data is to commit a cyber-related crime should also be guilty of an offence in the same way as a person is guilty of attempting to traffic in a dangerous drug even if the person's culpable belief in the nature of the substance being trafficked turns out to be incorrect.**

**(f) Knowingly making available a device, program or data (or a part thereof) made or adapted to commit a cyber-related crime, or knowingly possessing the device, program or data for the purpose of making it available, irrespective of whether it is tangible or intangible, eg ransomware, a virus or their source code, should constitute an aggravated offence under the new legislation, subject to a statutory defence of reasonable excuse, if the device, program or data:**

**(i) is, or is known, believed[37] or claimed by the perpetrator to be, capable of being used to commit a cyber-related crime; and**

**(ii) the perpetrator intends it to be used by any person to commit a cyber-related crime.**

**(g) Knowingly possessing a device, program or data (or a part thereof) should constitute an aggravated offence under the new legislation, subject to a statutory defence of reasonable excuse, if the device, program or data:**

**(i) is, or is known, believed[38] or claimed by the perpetrator to be, capable of being used to commit a cyber-related crime; and**

**(ii) the perpetrator intends to use it to commit a cyber-related crime.**

**(h) Subject to the above, the proposed provisions should be modelled on section 3A of the Computer Misuse Act in England and Wales as well as sections 8 and 10 of the Computer Misuse Act in Singapore.**

## Defences to the proposed offence: Recommendation 10

6.63 Recommendation 10 of the Consultation Paper invited submissions on the following questions:

"*(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?*"

[37] Including cases where a person has reasonable grounds to believe that the device, program or data is capable of being used to commit a cyber-related crime.

[38] Same as above.

## Responses to the Sub-committee's Recommendation 10

### *Defence or exemption for cybersecurity purposes*

6.64 The majority of the Respondents who commented on Recommendation 10 supported providing a defence or exemptions for making available or possessing a harmful device, program or data for cybersecurity purposes. Those in favour include the Hong Kong Federation of Women Lawyers Limited, Hong Kong Women Professionals and Entrepreneurs Association ("**HKWPEA**"), various information technology-related bodies, as well as Respondents from the business field.

6.65 An information technology-related body stated this in its response:

> "*For possession of computer data that can only be used to perform cyber-attacks, there may be a need for defence where the individual or organisation that possesses such data is directly involved in areas corresponding to the data they possess. For example, it would be essential for a company that develops anti-virus solutions to possess virus software.*"

6.66 Both the Hong Kong Chartered Governance Institute and the HKWPEA suggested providing a defence for possession of offending devices or software for conducting authorised cyber-attacks to test the integrity or security of a computer system.

### *Defence for educational or research purposes*

6.67 As with the cybersecurity defence, there was general support for a specific defence for educational or research purpose among the Respondents. The Hong Kong Bar Association ("**HKBA**") opined that it is necessary to maintain a separate defence because the general "reasonable excuse" defence, which rests on the objective standard of what an ordinary and reasonable man believes, may likely fail to cater for the specific knowledge or understanding that a person has in respect of any data.

6.68 The HKBA further commented as follows:

> "*Since any defendant who invokes this defence [is] likely to claim that [his] possession of the data is part and parcel of [his] work (e.g. in researching the development of anti-virus software) … any limit on the use of such a defence should be termed along the lines of possession 'in the ordinary course of' the subject activity undertaken by the defendant, for example, research.*"

## Our analysis and response

6.69 Readers would recall that the defences or exemptions for cybersecurity and educational or research purpose proposed by the Respondents above echoed the specific defences that we considered for the Access Offence in Chapter 2 and the Interference Offences in Chapters 4 and 5.

6.70 We agree that similar defences should be formulated to cater for making available or possessing harmful devices, programs or data for cybersecurity, educational, scientific, research and other legitimate purposes. This would ensure that the proposed offence only thwarts illegitimate supply and possession of nefarious devices, programs or data.

### *Making available a harmful device, program or data for cybersecurity purposes (or possessing such a device, program or data for making it available for cybersecurity purposes)*

6.71 As discussed in Chapters 2 and 4,[39] we recommend that there should be a specific defence or exemption to the Access Offence and the Interference Offences for accredited cybersecurity practitioners who act for genuine cybersecurity purposes, with the details of the accreditation regime to be considered by the Government. The defendant's purpose and conduct must be reasonable having regard to all the circumstances.

6.72 We agree that the above conditions of the defence may similarly be transposed to the cybersecurity defence to the proposed offence.

6.73 Nevertheless, an additional limb is necessary for the cybersecurity defence to the proposed offence. In the case of the Access Offence and the Interference Offences, the acts of access and interference with computer data and/or computer system are carried out by accredited cybersecurity practitioners. On the other hand, devices, programs or data may be possessed or made available by persons other than accredited cybersecurity practitioners. For example, in a company that develops anti-virus software, its technicians, salespersons and other non-professional employees may come into possession of computer viruses in the course of performing their duties.

6.74 Thus, we recommend that for the purposes of the proposed offence, the cybersecurity defence should extend beyond cybersecurity practitioners to cover persons who possess or make available a device, program or data for cybersecurity purposes with the prior permission or authorisation of cybersecurity practitioners. It is intended that the proposed defence would only apply if "prior" permission or authorisation is granted as

[39] Paras 2.63 to 2.74, 4.34 and 4.35.

this arrangement would accord better protection to the public by imposing a positive and proactive duty on cybersecurity practitioners to permit or authorise proper persons to hold devices, programs or data that are potentially dangerous.

6.75 We wish to add that depending on how the whole cybersecurity accreditation regime is set up (which, as we have explained in Chapter 2,[40] is a matter to be determined by the Government):

(a) provisions may have to be made in any codes of conduct or detailed rules to be prescribed under the accreditation regime to regulate the proper granting of access to potentially dangerous devices, programs or data by cybersecurity practitioners to those who need to access them for the development or advancement of cybersecurity; and

(b) the accredited entities under the cybersecurity accreditation regime are not necessarily natural persons and it is possible for a body corporate (eg a cybersecurity company) to be an accredited entity. Consideration will have to be given as to how access to devices, programs or data that are potentially dangerous may be properly granted to responsible individuals carrying out the relevant tasks.

***Making available a harmful device, program or data for educational, scientific or research purposes (or possessing such a device, program or data for making it available for the aforementioned purposes)***

6.76 We agree with the Respondents that there should be a defence to the proposed offence for educational or research purposes, which would apply beyond persons working in the cybersecurity industry. For instance, the "educational purpose" limb protects teachers and students in the field of computer science, while the "scientific" and "research" limbs can cover amateurs who acquire or create a harmful computer program (eg a trojan horse) for their own study.

6.77 We appreciate that computer science research may be carried out for benevolent or malicious purposes. For example, a research may aim to demonstrate how to fend off computer viruses, or hack into another computer system. We consider that the law should allow room for advancement of research on harmful devices, programs or data by providing a defence for making available a harmful device, program or data for educational, scientific or research purposes (or possessing such a device, program or data for making it available for these purposes). Otherwise, analysis of malware for the benefit of society may be inhibited. Besides,

[40] Paras 2.67 to 2.70.

cybersecurity practitioners often start out as amateurs or computer geniuses. It would be reasonable to provide a specific defence.

6.78 For the Access Offence in Chapter 2, we recommended that the access to program or data made for research purposes should be reasonable and no more than is necessary for achieving the educational, scientific or research purpose.[41] This reasonableness requirement provides safeguards against abuse by serving as an objective yardstick for determining whether the access made by a defendant is proportionate or reasonable.

6.79 Similarly, a reasonableness requirement should be incorporated into the defence to the proposed offence for making available a harmful device, program or data for educational, scientific or research purposes (or possessing such a device, program or data for making it available for these purposes). On this basis, we are confident that the benefits of the specific defence would outweigh its potential harm. If a defendant does not act for a genuine educational, scientific or research purpose, the prosecution should be able to adduce evidence to prove the person's criminal intent.

## Other specific statutory defences

### *No defence recommended for protection of the interest of a child or vulnerable person*

6.80 In Chapter 2, we proposed that there should be a defence for access to program or data made for the purpose of protecting the interests of a child or vulnerable person.[42] On the other hand, this parental control defence does not apply to the Interference Offences discussed in Chapters 4 and 5 because granting a person access to program or data does not imply that the person would be authorised to alter the data.[43]

6.81 We find it inconceivable that the purpose of protecting the interest of a child or vulnerable person would necessitate making available a device, program or data whose primary use is to commit a cyber-related crime (or possessing such a device, program or data for the purpose of making it available). Accordingly, we consider that it is not necessary to provide a specific defence to the proposed offence for the purpose of protecting the interests of a child or vulnerable person.

---

41 Para 2.94.
42 Paras 2.81 to 2.91.
43 Paras 4.36 and 5.25.

***Defence for internet service providers ("ISPs")***

6.82 ISPs provide internet connections and related services (such as web hosting) to individuals and organisations. The contents transmitted through an ISP's server are generally encrypted, but upon notification by third parties, an ISP can know the contents that originate from its network. Generally, ISPs receive voluminous notifications about allegedly illegal contents on their networks in their day-to-day operation.

6.83 Nevertheless, since an internet protocol address assigned by an ISP may host multiple websites and URLs,[44] it may not always be feasible to disable access to harmful websites, programs or data as this may disrupt its provision of services to other internet users.

6.84 The operation of ISPs described in the above paragraphs means that an ISP may knowingly make available a bogus website (say, a fake bank website), which is an obvious means of committing a cybercrime. Taking into account the position ISPs are in, we recommend providing a defence for ISPs by modelling on the mere conduit defence under Article 4 of the Digital Services Act ("**DSA**"), which was approved by the Council of the European Union ("**EU**") in 2022 as a key part of the EU's digital regulation strategy to modernise legal frameworks and create a safer digital environment.[45]

6.85 To allow the new cybercrime legislation flexibility to deal with various situations in cyberspace, we find it helpful to refer to a definition of "service provider" as broad as that in section 65A(2) of the Copyright Ordinance (Cap 528), which provides that a "service provider" is "*a person who, by means of electronic equipment or a network, or both, provides, or operates facilities for, any online services*". Under section 65A(2)(a) to (c), an "online service" includes:

(a) the transmission, routing, or provision of connections for digital online communications, between or among points specified by a user, of information or material of the user's choosing;

---

44 URL means "Uniform Resource Locator", which is a unique identifier or web address used to locate a resource on the internet. See https://www.techtarget.com/searchnetworking/definition/URL (accessed on 1 Nov 2025).

45 The Digital Services Act ("**DSA**") has a broad scope and regulates many aspects of digital services, including liability for online content and services. Article 4(1) of the DSA reads:
"*Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, the service provider shall not be liable for the information transmitted or accessed, on condition that the provider:*
*(a) does not initiate the transmission;*
*(b) does not select the receiver of the transmission; and*
*(c) does not select or modify the information contained in the transmission.*"

(b) the hosting of information or material that can be accessed by a user; and

(c) the storing of information or material on a system or network that can be accessed by a user.

6.86 By adopting the broad definition of "service provider" in section 65A(2), our proposed defence can cover service providers of all sizes, as well as individuals who create an online space (such as a forum or website) for hosting or storing program or data.

6.87 In sum, we recommend that it is a defence for a "service provider" to show that the provider:

(a) does not initiate the transmission of the device, program or data concerned (collectively "**illegal content**");

(b) does not select the receiver of the transmission; and

(c) does not select or modify the illegal content contained in the transmission.

### *Defence for storage and/or dissemination of devices, programs or data*

6.88 ISPs are only one of the many categories of online service providers. In the digital age, a vast array of internet services are offered by hosting service providers, cloud service providers and data storage facilities. To make the bespoke cybercrime legislation comprehensive without complicating it unnecessarily, we find it appropriate to draw on Article 6 of the DSA[46] and develop a defence that targets situations where the services of a "service provider" include the "storage" and/or "dissemination" of devices, programs or data provided by a recipient of the service. This approach will cover all the aforementioned service providers and save the need to differentiate between them.

6.89 As we pointed out above,[47] it may not always be technically feasible for a service provider to remove or disable access to an illegal content due to the knock-on effect on other users. To address this practical difficulty,

---

[46] Article 6(1) of the DSA reads:
"*Where an information society service is provided that consists of the storage of information provided by a recipient of the service, the service provider shall not be liable for the information stored at the request of a recipient of the service, on condition that the provider:*
*(a) does not have actual knowledge of illegal activity or illegal content and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or illegal content is apparent; or*
*(b) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the illegal content.*"

[47] Para 6.83 above.

we propose that a service provider should be relieved of criminal liability for making available the illegal content if the provider has reported the existence of the content to a law enforcement agency ("**LEA**") as soon as reasonably practicable.

6.90 In addition, we recommend that the *actus reus* of "*making available a device, program or data made or adapted to commit a cyber-related crime*" should include providing access (whether directly or indirectly) to a harmful device, program or data. For instance, a malicious program or data may be embedded in a hyperlink, or a service provider hosts a hyperlink that merely provides access to another online location containing malicious program or data. In the latter case, the malicious program or data is not stored with the service provider. In our view, this situation should also be covered by the proposed defence.

6.91 In the light of the above, we recommend that where the services of a service provider include the storage and/or dissemination of devices, programs or data provided by a recipient of the service, and the service provider becomes aware of or has reasonable grounds to believe that illegal content, or access to that illegal content (whether directly or indirectly), has been provided by a recipient of the service, it is a defence for the service provider to prove that:

(a) access to the illegal content is removed or disabled as soon as reasonably practicable upon the provider's obtaining such knowledge or having such reasonable grounds to believe; or

(b) (if the removal, or disabling access to, the illegal content is not technically feasible or reasonably practicable), the service provider has reported the existence of the illegal content to an LEA as soon as reasonably practicable.

6.92 We would supplement that the above defence is proposed on the basis that the service provider and the recipient of the service are different persons. In any case, if an offender shares a malicious device, program or data by hosting a storage service himself and putting the illegal content on the storage, the offender cannot succeed in arguing that he is a "service provider" so as to absolve himself of any criminal liability for actively making available the malware. This is because the offender, who possesses knowledge about the illegal content at the outset, cannot satisfy the first condition of the defence, ie removing the illegal content as soon as reasonably practicable.

***Defence for making available a device, program or data by automated technology***

6.93 We further observe that technological advancement now makes it possible for a harmful device, program or data to be made available or disseminated by means of an automated process. For instance, we envisage situations where an automated process, tool or technology (eg a blockchain[48] or an internet bot) used for distributing data may, in itself, be innocuous, but a perpetrator taints the innocent process, tool or technology with a malicious device, program or data (eg a virus or malicious app), and the blockchain or bot then automatically distributes the malicious material further.

6.94 In the above scenario, if a person, upon becoming aware of the malicious device, program or data, does not cease to take part in the automated process or technology (eg by not disconnecting the blockchain node from his hard drive), the person will *prima facie* be guilty of the proposed offence. We have the following observations:

(a) The law may be too draconian if a slothful person or computer illiterate has to bear criminal liability for not disconnecting his blockchain node.

(b) Blockchain or other automated technology that is reasonably popular (eg Bitcoin blockchain and Spotify) may be widely used. It may not be practicable or appropriate to shut down the automated process.

6.95 In the circumstances, we consider it fair to provide a defence to a person who uses an automated process, tool or technology as long as the person does not actively or consciously take any steps to make available any harmful device, program or data. The essence of the defence is that the person does not perform the *actus reus* of making available a device, program or data for committing a cyber-related crime (or possessing such a device, program or data for the purpose of making it available) voluntarily. As technology continues to evolve, alternatives to blockchain and bots may emerge. Therefore, the proposed defence should be framed in a generic way instead of referring to any technology specifically.

6.96 In sum, we recommend that if certain illegal content is made available solely by means of an automated process, tool or technology, it is a defence for a person to show that he:

---

[48] A blockchain is a distributed database or ledger shared among a computer network's nodes. They are best known for their crucial role in cryptocurrency systems for maintaining a secure and decentralised record of transactions, but they are not limited to cryptocurrency uses. Blockchains can be used to make data in any industry immutable. See https://www.investopedia.com/terms/b/blockchain.asp (accessed on 1 Nov 2025).

(a) was not knowingly involved in designing, producing, or generating such illegal content; and

(b) was not knowingly involved in the process by which such illegal content became part of that automated process.

## Conclusion on Recommendation 10

6.97 Our recommendations on the various specific defences to the proposed offence are summarised below:

**Final Recommendation 10**

**Apart from the statutory defence of reasonable excuse, we recommend the following specific defences to the offence of making available a device, program or data for committing a cyber-related crime (or possessing such device, program or data for the purpose of making it available for committing a cyber-related crime):**

**(a) Making available the device, program or data for cybersecurity purposes (or possessing such device, program or data for the purpose of making it available for cybersecurity purposes):**

**(i) This defence should only apply to an accredited cybersecurity practitioner (whose qualifications would be recognised under a regime to be established by the Government) who has acted for a genuine cybersecurity purpose;**

**(ii) The cybersecurity practitioner's purpose and conduct must be reasonable having regard to all the circumstances; and**

**(iii) This defence should extend to:**

**(1) persons who possess or make available the device, program or data for cybersecurity purposes with the prior permission or authorisation of a cybersecurity practitioner; and**

**(2) persons who assist the cybersecurity practitioner in carrying out his professional duties.**

**(b) Making available the device, program or data for genuine educational, scientific or research purposes (or possessing such device, program or data for the purpose of making it available for genuine educational, scientific or research purposes). The conduct of a person who relies on this defence must be reasonable having regard to all the circumstances.**

**(c) Modelling on Article 4 of the Digital Services Act ("DSA") of the European Union, it is a defence for an internet service provider[49] that serves as a mere conduit in making available the device, program or data (or possessing the device, program or data for the purpose of making it available) to show that the provider:**

**(i) does not initiate the transmission of the device, program or data ("illegal content");**

**(ii) does not select the receiver of the transmission; and**

**(iii) does not select or modify the illegal content contained in the transmission.**

**(d) Modelling on Article 6 of the DSA, where the services of a service provider[50] include storage and/or dissemination of a device, program or data provided by a recipient of the service, and the service provider becomes aware of or has reasonable grounds to believe that illegal content, or access to that illegal content (whether directly or indirectly), has been provided by a recipient of the service, it is a defence for the service provider to show that:**

**(i) access to the illegal content is removed or disabled as soon as reasonably practicable upon the service provider's obtaining such**

---

[49] We recommend adopting a definition of "service provider" as broad as that in s 65A(2) of the Copyright Ordinance (Cap 528) so as to cover service providers of all sizes, as well as individuals who create an online space (such as a forum or website) for hosting or storing program or data. See paras 6.85 and 6.86 above.

[50] Same as above.

**knowledge or having such reasonable grounds to believe; or**

**(ii) (if the removal, or disabling access to, the illegal content is not technically feasible or reasonably practicable) the service provider has reported the existence of the illegal content to a law enforcement agency as soon as reasonably practicable.**

**(e) If an illegal content is made available solely by means of an automated process, tool or technology, it is a defence for a person to show that he:**

**(i) was not knowingly involved in designing, producing, or generating the illegal content; and**

**(ii) was not knowingly involved in the process by which the illegal content became part of that automated process.**

# Chapter 7

# Criteria for the Hong Kong court to assume jurisdiction

## Introduction

7.1 This Chapter discusses the responses regarding Recommendations 11 to 15, which set out the criteria for the Hong Kong court to assume jurisdiction over the five cyber-dependent offences proposed in Chapters 2 to 6:

> "*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.*

*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.*

*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.*

*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.*

*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.*"

## Jurisdictional issues associated with cybercrime

7.2 As the Sub-committee explained in the Consultation Paper,[1] 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.

7.3 Thus, it is necessary for the new bespoke legislation to address the unique jurisdictional challenges presented by cybercrime. As a starting point, the Consultation Paper referred to *HKSAR v Wong Tak Keung*,[2] where the Court of Final Appeal confirmed that the general rule that the courts' criminal jurisdiction is territorial "*is subject to statutory modification*".[3] Therefore, for instance, under section 3 of the Criminal Jurisdiction Ordinance (Cap 461), 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.

### *Generally accepted bases of extra-territorial jurisdiction*

7.4 The Sub-committee's comparative study further showed 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.[4] In this connection, there are four generally accepted bases of extra-territorial jurisdiction:

(a) The active personality principle (based on a perpetrator's nationality);

---

1 At para 7.15.
2 At para 7.9.
3 (2015) 18 HKCFAR 62, at 75 (para 29), FACC 8/2014 (date of judgment: 9 Jan 2015). See Consultation Paper, at para 7.9.
4 Consultation Paper, at para 7.68.

(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).[5]

### *Five fact patterns for the jurisdictional rules on cybercrime*

7.5 Considering that it would be apposite for Hong Kong to follow the international norm, the Sub-committee then devised the jurisdictional rules for the five proposed cyber-dependent offences with reference to the following fact patterns:[6]

(a) any "essential element"[7] of the offence occurred in Hong Kong even if other "essential element(s)" occurred elsewhere;[8]

(b) the perpetrator is a "Hong Kong person";

(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.

7.6 Eventually, the Sub-committee concluded that the five proposed cyber-dependent offences should have extra-territorial effect on the grounds that cybercrime often involves multiple jurisdictions.[9] To prevent disputes in future legal proceedings, the Sub-committee proposed that the bespoke cybercrime legislation should expressly prescribe the jurisdictional rules which apply to the five offences,[10] which resulted in Recommendations 11 to 15. As

---

5 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.

6 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.

7 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 Criminal Jurisdiction Ordinance (Cap 461).

8 This scenario would include cases where the perpetrator, his or her act, and the victim are all in Hong Kong.

9 Consultation Paper, at para 7.62.

10 Same as above, at para 7.63.

explained in the Consultation Paper,[11] 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.

## General responses to the Sub-committee's Recommendations 11 to 15

7.7 Having set out the background of Recommendations 11 to 15, we now proceed to discuss the consultation responses.

### *Comments from Respondents who supported the recommended jurisdictional rules*

7.8 There is overwhelming support for the extra-territorial application of the proposed cybercrime legislation among Government departments, quasi-Government bodies, legal organisations, business bodies and academics.

7.9 As a general comment, the Hong Kong Bar Association ("**HKBA**") agreed that Recommendations 11 to 15 are "*rationally based and in conformity with the general principles of extra-territoriality and the doctrine of comity*".

7.10 From the perspective of consumer protection, the Consumer Council observed that "*cross-border transactions are becoming commonplace owing to the proliferation of online shopping and other forms of e-commerce among consumers in recent years*". In its view, in order to provide sufficient protection for Hong Kong consumers, extra-territorial application of cybercrime laws is both necessary and justifiable.

7.11 The Respondents generally agreed with the five fact patterns stated in paragraph 7.5 above. Specifically, regarding fact pattern (b), namely "*the perpetrator is a Hong Kong person*", both the Office of the Privacy Commissioner for Personal Data ("**PCPD**") and the HKBA supported the Sub-committee's recommendation against relying on this fact pattern in the first four cyber-dependent offences.

7.12 The PCPD stated its reason as follows:

> "*In our enforcement experience, given the borderless nature of the internet, it is very common that the perpetrator is not a Hong Kong person or does not reside in Hong Kong at the time the crime is committed, and thus has no connection with Hong Kong at all.*"

[11] Same as above.

7.13 The HKBA also agreed with the exclusion of fact pattern (b), commenting that the Sub-committee's approach:

> "*prudently avoids an over-expansive reach of the proposed legislation in the cybercrime context, in which offences may easily involve at least two or even more jurisdictions*".[12]

***Comments from Respondents who opposed the recommended jurisdictional rules***

7.14 Some members of a business group considered that courts may adapt their jurisdictional rules to suit the evolving technological circumstances and that it would be inappropriate to formulate distinct jurisdictional rules solely for cybercrime. Meanwhile, an individual Respondent opined that Hong Kong should adhere to the dominant form of criminal jurisdiction, ie the territorial principle under which Hong Kong courts have jurisdiction over acts committed within its territory.

***Other general observations from Respondents***

7.15 Various Respondents pointed out that given the cross-border nature of cybercrime, effective enforcement of any cybercrime legislation would require international co-operation and the enforcement authorities should ensure that there are effective arrangements for seeking assistance from law enforcement agencies ("**LEAs**") in other jurisdictions.

## Detailed responses to the Sub-committee's Recommendations 11 to 15

***The concept of "Hong Kong person"***

7.16 For the concept of "Hong Kong person" in fact pattern (c), the Sub-committee recommended that it should include a Hong Kong permanent resident, a person ordinarily residing in Hong Kong and a company carrying on business in Hong Kong.[13]

7.17 Noting the Sub-committee's recommendation, the PCPD invited the Sub-committee to consider the formulation in section 66M(5) of the Personal Data (Privacy) Ordinance (Cap 486) ("**PDPO**"). Section 66M belongs to Part 9A of the PDPO, which confers statutory powers on the Privacy

---

12 An example cited by the HKBA is the use of malware from a computer in Hong Kong to access without authorisation data stored in a computer system in other jurisdictions for financial gain.

13 Consultation Paper, at para 7.69(b), fn 80.

Commissioner for Personal Data ("**Commissioner**") to serve cessation notices to demand actions to cease or restrict disclosure of doxxing contents. The Commissioner may serve a notice if the Commissioner has reasonable grounds to believe that a "Hong Kong person" is able to take a cessation action in relation to a doxxing message.

7.18 Under the definition in section 66M(5),[14] a person who is "*present in Hong Kong*" is treated as a "Hong Kong person". The PCPD opined that:

> "*the formulation [under section 66M(5)] is more straightforward, simpler and has less room for argument than one using the more complicated formulations of permanent residency or ordinary residence, as complicated factual and legal questions often arise as to what constitutes 'permanent residency' or 'ordinarily' residing in a particular place*".

***Fact pattern (d): "the target computer, program or data is in Hong Kong"***

7.19 The PCPD further opined that from its enforcement experience, the target computer, program or data, albeit storing the personal data of Hong Kong persons, is often not located in Hong Kong. To combat cybercrime effectively, it suggested removing this requirement in Recommendations 11(c), 12(c), 13(c) and 14(c).

***The Mutual Legal Assistance in Criminal Matters Ordinance (Cap 525) ("MLACMO") and other procedural matters***

7.20 Considering the practicalities of the extra-territorial application of the proposed cybercrime legislation, the HKBA made the following remarks in its submissions:

> "*In the particular context of the cyberworld which transcends jurisdictional borders, effective enforcement of any legislation would require international co-operation. We must therefore bear this in mind when we consider how any new legislation could bring about the protection of the rights of our citizens and businesses against cybercriminals.*"

7.21 In the light of the potential involvement of multiple jurisdictions in a cybercrime case and the extra-territorial application of laws, the HKBA invited

---

[14] Section 66M(5) of the Personal Data (Privacy) Ordinance (Cap 486) defines a "Hong Kong person" to mean —
"*(a) an individual who is present in Hong Kong; or*
*(b) a body of persons that—*
*(i) is incorporated, established or registered in Hong Kong; or*
*(ii) has a place of business in Hong Kong.*" (emphasis added)

the Sub-committee to consider whether any relevant provisions under the MLACMO should be amended.

7.22 Meanwhile, some Respondents in the information technology sector flagged up the following evidentiary issues:

(a) how evidence may be collected from other jurisdictions;

(b) the preservation of evidence (eg computer data) obtained from the cloud-based environment should be conducted in accordance with industry best practices and the standards adopted by local and international digital forensics investigation organisations;

(c) whether the evidence collected from the cloud-based environment is admissible in court; and

(d) any conflict of laws between Hong Kong and other jurisdictions which host the relevant data or server should be resolved.

***Should Recommendations 11(d), 12(d), 13(d), 14(d) and 15(c) clarify that "security of Hong Kong" includes "national security"?***

7.23 A Government department suggested that in the light of the protective principle,[15] it would be advisable to provide for the extra-territorial effect of the five cyber-dependent offences over acts endangering national security, but not merely acts threatening the "*security of Hong Kong*", lest it be thought that the latter is narrower than the concept of national security. This Respondent suggested recasting Recommendations 11(d), 12(d), 13(d), 14(d) and 15(c) as follows:

> "*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, or has endangered national security.*"
>
> (emphasis added)

7.24 Alternatively, it proposed to define "security of Hong Kong" to include "national security".

[15] Para 7.4(d) above.

## Our analysis and response

### *Expanding the scope of fact pattern (c): "the victim is a Hong Kong person"*

7.25 As mentioned in paragraph 7.17 above, section 66M of the PDPO referred to in the PCPD's submissions concerns an entirely different statutory context where the concept of "Hong Kong person" is delineated for the purpose of determining the person against whom the Commissioner may serve a cessation notice demanding actions in relation to a doxxing message. Notwithstanding this, the PCPD's comments stated in paragraphs 7.17 and 7.18 above have prompted us to reflect on the scope of protection that Hong Kong courts ought to accord to cybercrime victims.

7.26 We recognise that permanent residents and persons ordinarily residing in Hong Kong aside, various persons may work or stay in Hong Kong temporarily for one reason or another. Examples include foreign domestic helpers, tourists and other visitors staying (eg for conducting a particular business transaction or negotiation, joining a trade fair or attending court or arbitral proceedings) in Hong Kong on a transient basis. In our view, if these persons fall victim to a cybercrime while they are physically present in Hong Kong, they should also be protected by Hong Kong laws. In other words, the protection from cybercrime should extend beyond persons who are permanent residents or persons who ordinarily reside in Hong Kong.

7.27 We have also considered the possibility of a cybercrime case that only falls within fact pattern (c) (to be refined in the manner set out in the preceding paragraph), but not fact patterns (a),[16] (b),[17] (d)[18] or (e).[19] Should such a case arise, the only nexus between the case and Hong Kong would be that the victim is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or a person present in Hong Kong at the time of the commission of the cybercrime, and all other essential elements of the cybercrime occur outside Hong Kong. We appreciate that there may well be practical difficulties in investigating the case or bringing it before Hong Kong courts as the LEAs in Hong Kong will have to collect and preserve evidence from other jurisdictions and resolve other logistical difficulties. Nonetheless, these practicality issues will arise no matter whether the victim of a cybercrime is a Hong Kong resident or not. Given the borderless nature of cybercrime, cooperation under existing framework or negotiation to refine such framework with the relevant authorities in other jurisdictions over mutual legal assistance is indispensable. As Part Three of our study will address evidentiary and enforcement issues, we shall consider how the existing enforcement and investigative powers may be

---

16 "*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*".

17 "*the perpetrator is a Hong Kong person*".

18 "*the target computer, program or data is in Hong Kong*".

19 "*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*".

improved to facilitate the investigation and handling of cross-border cybercrime in that Part.

7.28 In sum, to also protect people who are in Hong Kong on a transient basis against the proposed cyber-dependent offences, we recommend refining fact pattern (c) as follows:

> "*the victim is a Hong Kong permanent resident, a person ordinarily residing in Hong Kong, or was physically present in Hong Kong at the time the relevant offence was committed, or a company carrying on business in Hong Kong.*"
>
> (emphasis added)

***Fact pattern (d): "the target computer, program or data is in Hong Kong"***

7.29 We agree that the target computer, program or data which the bespoke cybercrime legislation seeks to protect may, in many cases, not be located in Hong Kong. As explained in the Consultation Paper,[20] the facts mentioned in each of the five fact patterns are, for discussion purpose, assumed to be the only connection between the fact pattern and Hong Kong. An actual case may come under just one or more than one fact pattern. In other words, the fact pattern spelt out in Recommendations 11(c), 12(c), 13(c) and 14(c) is not a precondition of the extra-territorial application of the first four proposed offences, but only represents one of the four possible bases on any one of which the Hong Kong courts may assert jurisdiction over a cybercrime case.

7.30 While it is, therefore, not necessary to remove this requirement from Recommendations 11(c), 12(c), 13(c) and 14(c) as proposed, the PCPD's enforcement experience does confirm that there should be a disjunctive "or" between the relevant fact patterns in these recommendations.

***Evidentiary, procedural issues and related legislative amendments to the MLACMO***

7.31 As mentioned above,[21] Part Three of our study will address enforcement and procedural issues, which is, in itself, a substantial topic. We shall bear in mind the issues helpfully identified by the Respondents in paragraph 7.22 above.

7.32 We believe that the related amendments to the MLACMO will ultimately depend on the form in which the proposed cybercrime legislation is

---

20 At para 7.69, fn 77.
21 Para 7.27 above.

enacted. We also anticipate that negotiation between the Government of the Hong Kong Special Administrative Region and the relevant authorities in other jurisdictions may be required to foster cooperation among the LEAs in different places. In these circumstances, it would be premature for us to make any recommendations with regard to the consequential amendments to the MLACMO, which would best be left to the Government to decide as necessary in due course.

***References to "security of Hong Kong" in Recommendations 11(d), 12(d), 13(d), 14(d) and 15(c)***

7.33 During the discussion of the proposed offence of illegal interference with computer data in Chapter 4,[22] we referred to the Safeguarding National Security Ordinance ("**BL 23 legislation**") enacted in March 2024. The BL 23 legislation provides for the interpretation of, *inter alia*, the concept of "security of the HKSAR". A reference to the "security of the HKSAR" (including a phrase that means the same as this reference)[23] in an ordinance other than the BL 23 legislation is to be read as including "national security" as it is statutorily defined.[24] With the BL 23 legislation in place, any reference to "security of Hong Kong" in the new cybercrime legislation will be sufficiently wide in scope.[25]

7.34 In Chapter 4,[26] we have also emphasised that since the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region ("**NSL**") forms an essential part of the fabric of our legal system, it is important that the bespoke cybercrime legislation does not create any inconsistencies or conflict, even if unintended, with the NSL.

7.35 We must therefore point out that the NSL has prescribed, under its Chapter IV, certain jurisdictional and procedural rules for cases concerning offences that endanger national security. Article 40 provides, at the outset, that:

> "*The Hong Kong Special Administrative Region [("**HKSAR**")] shall have jurisdiction over cases concerning offences under [the NSL], except under the circumstances specified in Article 55 of [the NSL].*"

7.36 Article 55 sets out the exceptional circumstances as follows:

---

22 Para 4.28 above.
23 Safeguarding National Security Ordinance ("**BL 23 legislation**"), s 8(2).
24 Same as above, s 4.
25 In any event, s 8(1) of the BL 23 legislation provides that if the BL 23 legislation and another ordinance would be inconsistent but for that section, that other ordinance is to be read in a way that have the best regard to the object and purposes of the BL 23 legislation.
26 Para 4.27 above.

"*The Office for Safeguarding National Security of the Central People's Government in the Hong Kong Special Administrative Region [("**NS Office**")] shall, upon approval by the Central People's Government of a request made by the Government of the Hong Kong Special Administrative Region or by the Office itself, exercise jurisdiction over a case concerning offence endangering national security under [the NSL], if:*

*(1) the case is complex due to the involvement of a foreign country or external elements, thus making it difficult for the Region to exercise jurisdiction over the case;*

*(2) a serious situation occurs where the Government of the Region is unable to effectively enforce [the NSL]; or*

*(3) a major and imminent threat to national security has occurred.*"

(emphasis added)

7.37 Thus, when a cybercrime case involves any offence under the NSL, it is abundantly clear that, as a general rule, Hong Kong courts may exercise jurisdiction over the case in accordance with Article 40 even in the absence of any jurisdictional rules in the bespoke cybercrime legislation for such cases to be tried in Hong Kong.

7.38 In the exceptional circumstances when a request made under Article 55 is approved by the Central People's Government, the NS Office shall accordingly exercise jurisdiction over the case. Article 56 of the NSL then kicks in:

"*In exercising jurisdiction over a case concerning offence endangering national security pursuant to Article 55 of [the NSL], the Office for Safeguarding National Security of the Central People's Government in the Hong Kong Special Administrative Region shall initiate investigation into the case, while the Supreme People's Procuratorate [("**SPP**")] shall designate a prosecuting body to prosecute the case and the Supreme People's Court [("**SPC**")] shall designate a court to adjudicate it*."

(emphasis added)

7.39 Bearing in mind that jurisdiction over cybercrime cases that endanger national security is not exclusively vested in Hong Kong courts, we take the view that it would be inappropriate for the jurisdictional rules of the bespoke cybercrime legislation to prescribe that Hong Kong courts shall assume jurisdiction in such cases in order not to pre-empt how they may be

handled by the HKSAR Government, the NS Office, the SPP and the SPC, as the circumstances of each case warrant, in accordance with the procedures set out under Chapter IV of the NSL.

7.40 Accordingly, we maintain Recommendations 11(d), 12(d), 13(d), 14(d) and 15(c) proposed in the Consultation Paper.

## Conclusion

7.41 In light of the foregoing, we settle our recommendations on the jurisdictional rules as follows:

**Final Recommendation 11**

**We recommend 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 was physically present in Hong Kong at the time when the offence was committed, 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.**

**Final Recommendation 12**

**We recommend 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 was physically present in Hong Kong at the time when the offence was committed, 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.**

**Final Recommendation 13**

**We recommend that, in respect of the proposed offence (including its basic and aggravated forms) of illegal interference with 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 was physically present in Hong Kong at the time when the offence was committed, 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.**

**Final Recommendation 14**

**We recommend that, in respect of the proposed offence (including its basic and aggravated forms) of illegal interference with 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 was physically present in Hong Kong at the time when the offence was committed, 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.**

**Final Recommendation 15**

**We recommend that, in respect of the proposed offence of making available a device, program or data for committing a cyber-related crime, or possessing a device, program or data for the purpose of making it available for committing a cyber-related 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, program or data for committing a cyber-related crime;**

**(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.**

# Chapter 8

# Sentencing

## Introduction

8.1 This Chapter discusses the responses regarding Recommendation 16, which sets out the maximum sentences for the proposed five cyber-dependent offences:

> "*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.*
>
> *(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.*"

## Considerations behind the Sub-committee's Recommendation 16

8.2 Before we proceed to discuss the Respondents' feedback on Recommendation 16, it would be useful to recall the considerations that the Sub-committee had in mind when it formulated its sentencing proposals.

8.3 As the Sub-committee discussed in the Consultation Paper,[1] in formulating Recommendation 16, it had taken the maximum terms of imprisonment for the following representative types of crimes in the Theft Ordinance (Cap 210) ("**Theft Ordinance**") as references:

(a) 10 years for theft;[2]

(b) 14 years for fraud;[3]

(c) 14 years for blackmail;[4]

(d) 14 years for burglary;[5]

(e) life imprisonment for aggravated burglary (ie burglary committed by a person with any firearm or imitation firearm, any weapon of offence, or any explosive);[6] and

(f) life imprisonment for robbery.[7]

8.4 The Sub-committee observed that whatever the number of years of imprisonment we propose, there would be a degree of arbitrariness.[8] Against the above background, Recommendation 16 proposed a maximum sentence of imprisonment for 14 years for the following proposed offences, namely, the aggravated offence of illegal access to program or data, the offence of illegal interception of computer data, the basic offences of illegal interference

1 At para 8.14(f).
2 Theft Ordinance (Cap 210), s 9.
3 Same as above, s 16A(1).
4 Same as above, s 23(3).
5 Same as above, s 11(4).
6 Same as above, s 12(3).
7 Same as above, s 10(2).
8 Consultation Paper, at para 8.15.

with computer data and illegal interference with computer system, as well as the aggravated offence of making available or possessing a device or data for committing a crime. The Sub-committee considered that the 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 mentioned in the preceding paragraph as well as (b) the relevant offences in other jurisdictions.[9]

## Responses to the Sub-committee's Recommendation 16

### *Overview*

8.5 We have received mixed responses on the sentencing proposals in Recommendation 16. In general, Respondents from various Government departments, legal organisations, business bodies and tertiary institutions supported enhancing Hong Kong's efforts in tackling cybercrime by introducing a set of penalties that is tougher than that in respect of the current statutory computer-related offences. Some of them opined that the increased penalties will help deterring cyber-dependent crimes, and that a sound and robust cybersecurity regime will contribute positively to Hong Kong's business standing.

### *The offence of illegal access to program or data ("Access Offence")*

8.6 As mentioned in Chapter 2,[10] the Hong Kong Federation of Women Lawyers Limited opined that the aggravated form of the Access Offence, which involves "*the intent of a potential crime which has not been committed*", may be "*overly difficult to prove*". In its view, this may result in the summary offence being heavily relied on for serious offences which the prosecution is unable to prove as amounting to the aggravated offence. For this reason, this Respondent suggested that the Sub-committee should give further thoughts as to whether the two years' maximum imprisonment for the summary form of the Access Offence would provide sufficient deterrence.

### *The aggravated offences of illegal interference with computer data and illegal interference with computer system ("Interference Offences")*

8.7 A few Respondents from the information technology sector considered the maximum sentence of life imprisonment for the Interference

---

9 See the Appendix to the Consultation Paper, which summarises the maximum sentences for the five proposed cyber-dependent offences under the current laws in Hong Kong and other jurisdictions.

10 Para 2.13 above.

Offences "*too severe*" on the grounds that life imprisonment is the maximum penalty for murder and other similar criminal offences that are extremely serious.

8.8 Likewise, the Law Society of Hong Kong sought the Sub-committee's elaboration on the rationale behind the proposed maximum sentence of life imprisonment. This Respondent commented that:

> "*The justification seems to be a reference to and reliance upon section 63, [Crimes Ordinance] Cap 200 [("**CO**")].*[11] *Section 63 is on arson. This offence directly causes grave bodily harm. People's life is at stake. The Consultation Paper has not explained the relevancy or equivalence of section 63 Crimes Ordinance to the proposed aggravated offence (of illegal interference of computer data and computer system), in terms of gravity of the harm potentially caused, or otherwise. On the other hand, we are not aware of any life imprisonment sentence being handed down for criminal damage. The Consultation Paper has also not set out what aggravating factors are to be introduced for this offence (to justify this level of sentence). At the moment, we have no idea on the possible circumstances the Prosecution would urge the Court to hand down life sentence for this offence (e.g. how serious the interference has to be, for a life sentence to be imposed). An elaboration on all [of] the above would be helpful.*"

## Our analysis and response

### *The Access Offence*

8.9 As we have already explained in Chapter 2,[12] the aggravated form of the Access Offence is created for those cases in respect of which our courts, in performing their role as tribunals of fact, are able to make a finding, in the light of the evidence, on the requisite state of mind of a defendant (ie whether the person has the intention to commit a further crime) on admission or, as the case may be, by drawing inferences from the facts and circumstances of individual cases. Thus, the retention of the summary offence as a fallback should not be regarded as a soft option by which the defendant convicted of the lesser offence may still be sentenced essentially on the basis of suspicion as if there were proof that the aggravated offence had been committed.

---

11 Section 63 of the CO reads:
"*(1) A person guilty of arson under s 60 or of an offence under s 60(2) (whether arson or not) shall be liable on conviction upon indictment to imprisonment for life.*
*(2) A person guilty of any other offence under this Part shall be liable on conviction upon indictment to imprisonment for 10 years.*" (emphasis added)

12 Para 2.38 above.

8.10 Notwithstanding the above, we have taken the opportunity to reflect on the proposed maximum sentence of two years' imprisonment for the summary form of the Access Offence, noting that the Computer Misuse Act 1990 of England and Wales adopts a maximum sentence of only 12 months for a similar offence. We agree with the Sub-committee's view that whatever the number of years of imprisonment we propose, there would be a degree of arbitrariness.[13] Whether the recommendation should be adopted would depend on how it compares to existing offences in the Hong Kong context.

8.11 It is noted, for example, that some road traffic offences the commission of which does not of itself increase the risk of injury or property damage may carry a maximum term of imprisonment for 12 months. Such offences include using a motor vehicle on a road without the required compulsory insurance[14] and failure of a driver to provide a specimen of blood or urine when required by a police officer.[15] If the risk of traffic accident does materialise and their commission is detected in the course of such investigation (or is discovered randomly at road blocks or upon the driver being caught red handed for driving without a licence or driving while disqualified), sentence would be passed with regard to the totality principle[16] together with the appropriate sentence(s) which should be imposed in respect of the other more serious charge(s) preferred and of which the defendant will also be convicted.

8.12 Bearing in mind that there should be sufficient deterrent effect, pitching the maximum penalty at two years' imprisonment serves to signify the gravity of the summary form of the Access Offence by the commission of which the sanctity of the targeted system or confidentiality of the information the law seeks to protect has already been violated even though there is insufficient evidence that there is any intent to carry out further criminal activity upon unauthorised access to program or data. All things considered, we therefore also agree with the Sub-committee that the proposed maximum sentence of two years' imprisonment for the summary form of the Access Offence is appropriate. This will allow sufficient power on the part of the sentencing court to impose a punishment which can properly reflect the gravamen of the offence depending on the level of intrusion and importance of the compromised material.

8.13 Finally, we wish to supplement that the magistrates' courts have general powers to impose a fine up to a certain level under the Magistrates

---

13 Consultation Paper, at para 8.15.

14 See the penalty under s 4(2)(a) of the Motor Vehicles Insurance (Third Party Risks) Ordinance (Cap 272). Section 4(1) prohibits "*any person to use, or to cause or permit any other person to use, a motor vehicle on a road unless there is in force in relation to the user of the vehicle by that person or that other person … such a policy of insurance or such a security in respect of third party risks as complies with the requirements*" of the Ordinance.

15 Section 39S(1)(b)(ii) of the Road Traffic Ordinance (Cap 374) provides that a person who, without reasonable excuse, fails to provide a specimen of blood or urine for laboratory test when required to do so under s 39P, or fails to give consent to the analysis of a specimen of blood under s 39Q(4)(b), commits an offence and is liable on summary conviction (subsequent to a conviction on indictment) to a fine at level 4 and to imprisonment for 12 months.

16 The totality principle means that a court that passes consecutive sentences "*should review the aggregate of the sentences, and consider whether the total sentence to be served is appropriate, taking the offences as a whole", and the "measured application of the totality principle contributes to an overall sentence which is justifiable and proper, and not crushing*". See Archbold Hong Kong 2025, at para 5-91.

Ordinance (Cap 227) even if a criminal offence provision does not expressly stipulate any fine.[17] Should the Government decide to implement our proposals in due course, it may further consider whether the cybercrime legislation should prescribe any fine level during the legislative stage and we do consider it unnecessary to recommend any maximum fine for the summary form of the Access Offence.

***The proposed aggravated Interference Offences***

8.14 As discussed in Chapters 4 and 5, we recommend that:

(a) the aggravated offence under section 60(2) of the CO be adopted for the aggravated form of the offence of illegal interference with computer data;[18] and

(b) the proposed provisions regarding illegal interference with computer system be phrased in the same way as those for illegal interference with computer data.[19]

8.15 As the Sub-committee tried to explain in the Consultation Paper,[20] the maximum sentence proposed for the aggravated Interference Offences only sought to maintain consistency with the penalty for the aggravated form of the offence of criminal damage under the existing section 63(1) of the CO which, when read together with section 60(2)(b) of the CO,[21] makes it clear that what is being dealt with here are property damage or destruction situations where an intention to endanger life is involved.

8.16 For the aggravated offence of criminal damage under the prevailing law, the maximum sentence for conviction upon indictment under section 63(1) of the CO is imprisonment for life. In fact, section 63(1) of the CO does not only cover arson, but also applies to any criminal damage offence where the defendant intends to destroy or damage property to endanger the life of another, or is reckless as to whether the life of another would be endangered

---

17 Eg under s 97 of the Magistrates Ordinance (Cap 227):
"*Where a person is convicted of an offence other than an indictable offence the magistrate may, if he is not precluded from sentencing the person by the exercise of some other power (such as the power to make a probation order under s 3 of the Probation of Offenders Ordinance (Cap. 298)), impose a fine in lieu of or in addition to dealing with the person in any other way in which the magistrate has power to deal with him, subject however to any enactment requiring the person to be dealt with in a particular way.*"

18 Final Recommendation 6(b)(iv).

19 Final Recommendation 7(a).

20 At para 8.20.

21 Section 60(2) of the Crimes Ordinance (Cap 200) provides that:
"*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.*" (emphasis added)

by the destruction or damage of property. Section 63(1) provides unequivocally that:

> "*A person guilty of arson under section 60 or of an offence under section 60(2) (whether arson or not) shall be liable for conviction upon indictment to imprisonment for life.*"
>
> (emphasis added)

8.17 The Sub-committee recommended adopting the maximum sentence now prescribed by section 63(1) of the CO, ie imprisonment for life, for the aggravated form of the Interference Offences. In the Consultation Paper,[22] the Sub-committee provided a hypothetical scenario involving danger to life of someone interfering with the computer data being processed by the system of an airport's control tower, a railway signal system, etc. Further examples include interferences with the computer systems of major infrastructures such as power plants and gas supply. As such acts of interference may put the lives of thousands of people at risk, we agree that the aggravated Interference Offences justify a relatively severe sentence.

8.18 We wish to reiterate that it is not intended that the bespoke cybercrime legislation should re-set the maximum penalty for the respective Interference Offences already envisaged under the existing CO. Acts of illegal interference with computer data and/or computer system may, depending on the facts of the case, already constitute the aggravated criminal damage offence, which now attracts a maximum penalty of life imprisonment. Our proposal only intends the new cybercrime legislation to mirror these existing Interference Offences in the CO when it incorporates them.

***The proposed basic offence of making available a device, program or data for committing a cyber-related crime (or possessing such a device, program or data for making it available to another)***

8.19 During our deliberations of the responses, we have also reviewed Recommendation 16 as set out in the Consultation Paper in its entirety to ensure that our recommendations will have the necessary deterrent effect to combat cybercrime, and are not too out of line with the maximum sentences for (a) the crimes in the Theft Ordinance mentioned above[23] as well as (b) the relevant offences in other jurisdictions.[24] For instance, for the basic offence of making available or possessing a device, program or data for committing a cyber-related crime, the Sub-committee proposed a term of imprisonment for seven years as the maximum penalty for the basic offence on conviction on indictment. This penalty, which lays halfway when compared with the

---

22 At para 4.97.

23 Para 8.3.

24 See the Appendix to the Consultation Paper, which summarises the maximum sentences for the five proposed cyber-dependent offences under the current laws in Hong Kong and other jurisdictions.

recommended maximum sentence for the related aggravated offence, is on the whole on par with the penalties in other jurisdictions.

8.20 We are satisfied that Recommendation 16 stands by the principle elucidated above.

**Final Recommendation 16**

**We recommend 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 with computer data and illegal interference with 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.**

**(d) In respect of the proposed offence of making available a device, program or data for committing a cyber-related crime (or possessing such a device, program or data for the purpose of making it available to another), 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

# Summary of our Final Recommendations

## Illegal access to program or data
*– Final Recommendations 1, 2, 11 and 16(a)*

***Final Recommendation 1***

We recommend that:

(a) Subject to a statutory defence of reasonable excuse, unauthorised access to program or data without lawful authority should be a summary offence under the new legislation.

(b) The *mens rea* of the proposed offence are that:

(i) the defendant intends to secure access to the program or data, or intends to enable such access to be secured; and

(ii) the defendant knows that the intended access to the program or data was unauthorised when he makes the access.

(c) 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.

(d) The proposed provisions of the new legislation should be modelled on sections 1, 2 and 17 of the Computer Misuse Act of England and Wales.

***Final Recommendation 2***

Apart from the statutory defence of reasonable excuse, we recommend that for the proposed offence of illegal access to program or data:

(a) There should be a specific defence for unauthorised access for cybersecurity purposes with the following conditions:

(i) The defendant must be an accredited cybersecurity practitioner (the details of the accreditation regime, which are essentially matters of policy, are best left to the Government's consideration);

(ii) The defendant must act for a genuine cybersecurity purpose; and

(iii) The defendant's conduct must be reasonable having regard to all the circumstances.

(b) There should be a specific defence for unauthorised access for the protection of the interests of a child under the age of 16 and a vulnerable person (ie a mentally disordered person or a mentally handicapped person as defined in the Mental Health Ordinance (Cap 136)):

(i) The defence is based on the subjective purpose of the person making the access to the program or data of a child or vulnerable person (ie for the protection of the interests of the child or vulnerable person), but not the relationship between the person and the child or vulnerable person.

(ii) The access to program or data made by a defendant must be reasonable having regard to all the circumstances.

(c) There should be a specific defence for unauthorised access for educational, scientific or research purposes. The access to program or data made by a defendant must be reasonable having regard to all the circumstances.

(d) The defences to the offences of illegal interference with computer data and illegal interference with computer system under section 64(2) of the Crimes Ordinance (Cap 200) ("**S64(2)**") should also be available to the offence of illegal access to program or data.

(i) The two defences under S64(2) cover situations where a defendant:

(1) accessed program or data in the belief that his act was, or would be, consented to; or

(2) accessed program or data in the belief that the property was in immediate need of protection, and the means of protection adopted was reasonable having regard to all the circumstances.

(ii) The defendant's belief under both the consent defence and the property protection defence must be reasonably held.

***Final Recommendation 11***

We recommend 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 was physically present in Hong Kong at the time when the offence was committed, 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.

***Final Recommendation 16(a)***

We recommend that, 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.

## Illegal interception of computer data

*– Final Recommendations 4, 5, 12 and 16(b)*

### *Final Recommendation 4*

We recommend that:

(a) Unauthorised interception 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").

(d) The implications of unauthorised disclosure or use of computer data, intercepted or otherwise, should be studied in greater detail in Part Two of our study before we express any settled view as to whether any new offence in this regard should be recommended, and if so, how.

### *Final Recommendation 5*

We do not recommend any defence or exemption for professions or genuine businesses (eg coffee shops, hotels, shopping malls, employers) which intercept or use computer data in the ordinary course of their operation. The *mens rea* requirement of interception of computer data for a dishonest or criminal purpose has mitigated the need to provide for any specific defence or exemption.

***Final Recommendation 12***

We recommend 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 was physically present in Hong Kong at the time when the offence was committed, 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.

***Final Recommendation 16(b)***

We recommend that, 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.

## Illegal interference with computer data

*– Final Recommendations 6, 13 and 16(c)*

***Final Recommendation 6***

We recommend that:

(a) Subject to a statutory defence of reasonable excuse, intentional interference (damaging, deletion, deterioration, alteration or suppression) with computer data without lawful authority 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, instead of malice);

(iii) the two defences identified under section 64(2) subject to such refinement as may be required for their proper articulation in the light of the reformulation of the offence under paragraph (a) above, while preserving any other lawful excuse or defence recognised by law; and

(iv) the aggravated offence under section 60(2).

(c) The two defences covered under section 64(2) apply to situations where a defendant:

(i) interfered with computer data in the belief that his act was, or would be, consented to; or

(ii) interfered with computer data in the belief that the property was in immediate need of protection, and the means of protection adopted was reasonable having regard to all the circumstances.

The defendant's belief under both the consent defence and the property protection defence must be reasonably held.

(d) 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).

(e) There should be a specific defence for illegal interference with computer data for cybersecurity purposes with the following conditions:

(i) The defendant must be an accredited cybersecurity practitioner (the details of the accreditation regime, which are essentially matters of policy, are best left to the Government's consideration);

(ii) The defendant must act for a genuine cybersecurity purpose; and

(iii) The defendant's conduct must be reasonable having regard to all the circumstances.

***Final Recommendation 13***

We recommend that, in respect of the proposed offence (including its basic and aggravated forms) of illegal interference with 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 was physically present in Hong Kong at the time when the offence was committed, 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.

***Final Recommendation 16(c)***

We recommend that, in respect of the proposed offence of illegal interference with computer data, 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.

## Illegal interference with computer system

*– Final Recommendations 7, 8, 14 and 16(c)*

***Final Recommendation 7***

We recommend that:

(a) The proposed provisions regarding the illegal interference with 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 with 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 with 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

(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.

***Final Recommendation 8***

We recommend that:

(a) There should be a specific defence for illegal interference with computer system for cybersecurity purposes with the following conditions:

(i) The defendant must be an accredited cybersecurity practitioner (the details of the accreditation regime, which are essentially matters of policy, are best left to the Government's consideration);

(ii) The defendant must act for a genuine cybersecurity purpose; and

(iii) The defendant's conduct must be reasonable having regard to all the circumstances.

(b) It is not necessary to provide any specific defence to the proposed offence of illegal interference with computer system for non-security professionals (such as web scraping by robots or web crawlers initiated by internet information collection tools to collect data from servers without authorisation by connecting to designated protocol ports) since activities which form part of the

normal functioning of the internet or computer systems should continue to be allowed under the principle of implied authorisation.

***Final Recommendation 14***

We recommend that, in respect of the proposed offence (including its basic and aggravated forms) of illegal interference with 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 was physically present in Hong Kong at the time when the offence was committed, 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.

***Final Recommendation 16(c)***

We recommend that, in respect of each of the proposed offence of illegal interference with 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.

## Making available or possessing a device, program or data for committing a cyber-related crime

*– Final Recommendations 9, 10, 15 and 16(d)*

### *Final Recommendation 9*

(a) Knowingly making available a device, program or data (or a part thereof) made or adapted to commit a cyber-related crime,[1] or knowingly possessing the device, program or data for the purpose of making it available, irrespective of whether it is tangible or intangible, eg ransomware, a virus or their source code, should be a basic offence under the new legislation, subject to a statutory defence of reasonable excuse.

(b) The *actus reus* of the proposed offence should cover both the supply side (such as production, offering, sale and export of a device, program or data in question) and the demand side (such as obtaining, possession, purchase and import of a device, program or data in question).

(c) The proposed offence should apply to a device, program or data (or a part thereof) so long as its primary use (to be determined objectively) is to commit a cyber-related crime, regardless of whether or not it can also possibly be used for any legitimate purposes.

(d) The *mens rea* requirements of the proposed offence are that:

  (i) a person knows that he is making available or that he is in possession of a device, program or data (or a part thereof) for the purpose of making it available; and

  (ii) a person knows, believes, has reasonable grounds to believe, or claims that the primary use of a device, program or data (or a part thereof) is to commit a cyber-related crime.

(e) A person who claims (whether or not the claim is true) or mistakenly believes that the primary use of a device, program or data is to commit a cyber-related crime should also be guilty of an offence in the same way as a person is guilty of attempting to traffic in a dangerous drug even if the person's culpable belief in the nature of the substance being trafficked turns out to be incorrect.

---

[1] Namely, illegal access to program or data, illegal interception of computer data, illegal interference with computer data and illegal interference with computer system.

(f) Knowingly making available a device, program or data (or a part thereof) made or adapted to commit a cyber-related crime, or knowingly possessing the device, program or data for the purpose of making it available, irrespective of whether it is tangible or intangible, eg ransomware, a virus or their source code, should constitute an aggravated offence under the new legislation, subject to a statutory defence of reasonable excuse, if the device, program or data:

(i) is, or is known, believed[2] or claimed by the perpetrator to be, capable of being used to commit a cyber-related crime; and

(ii) the perpetrator intends it to be used by any person to commit a cyber-related crime.

(g) Knowingly possessing a device, program or data (or a part thereof) should constitute an aggravated offence under the new legislation, subject to a statutory defence of reasonable excuse, if the device, program or data:

(i) is, or is known, believed[3] or claimed by the perpetrator to be, capable of being used to commit a cyber-related crime; and

(ii) the perpetrator intends to use it to commit a cyber-related crime.

(h) Subject to the above, the proposed provisions should be modelled on section 3A of the Computer Misuse Act in England and Wales as well as sections 8 and 10 of the Computer Misuse Act in Singapore.

***Final Recommendation 10***

Apart from the statutory defence of reasonable excuse, we recommend the following specific defences to the offence of making available a device, program or data for committing a cyber-related crime (or possessing such device, program or data for the purpose of making it available for committing a cyber-related crime):

(a) Making available the device, program or data for cybersecurity purposes (or possessing such device, program or data for the

[2] Including cases where a person has reasonable grounds to believe that the device, program or data is capable of being used to commit a cyber-related crime.

[3] Same as above.

purpose of making it available for cybersecurity purposes):

(i) This defence should only apply to an accredited cybersecurity practitioner (whose qualifications would be recognised under a regime to be established by the Government) who has acted for a genuine cybersecurity purpose;

(ii) The cybersecurity practitioner's purpose and conduct must be reasonable having regard to all the circumstances; and

(iii) This defence should extend to:

(1) persons who possess or make available the device, program or data for cybersecurity purposes with the prior permission or authorisation of a cybersecurity practitioner; and

(2) persons who assist the cybersecurity practitioner in carrying out his professional duties.

(b) Making available the device, program or data for genuine educational, scientific or research purposes (or possessing such device, program or data for the purpose of making it available for genuine educational, scientific or research purposes). The conduct of a person who relies on this defence must be reasonable having regard to all the circumstances.

(c) Modelling on Article 4 of the Digital Services Act ("**DSA**") of the European Union, it is a defence for an internet service provider[4] that serves as a mere conduit in making available the device, program or data (or possessing the device, program or data for the purpose of making it available) to show that the provider:

(i) does not initiate the transmission of the device, program or data ("**illegal content**");

(ii) does not select the receiver of the transmission; and

(iii) does not select or modify the illegal content contained in the transmission.

(d) Modelling on Article 6 of the DSA, where the services of a service provider[5] include storage and/or dissemination of a device, program or data provided by a recipient of the service, and the service provider becomes aware of or has reasonable grounds to believe that illegal content, or access to that illegal content

[4] We recommend adopting a definition of "service provider" as broad as that in s 65A(2) of the Copyright Ordinance (Cap 528) so as to cover service providers of all sizes, as well as individuals who create an online space (such as a forum or website) for hosting or storing program or data.

[5] Same as above.

(whether directly or indirectly), has been provided by a recipient of the service, it is a defence for the service provider to show that:

(i) access to the illegal content is removed or disabled as soon as reasonably practicable upon the service provider's obtaining such knowledge or having such reasonable grounds to believe; or

(ii) (if the removal, or disabling access to, the illegal content is not technically feasible or reasonably practicable) the service provider has reported the existence of the illegal content to a law enforcement agency as soon as reasonably practicable.

(e) If an illegal content is made available solely by means of an automated process, tool or technology, it is a defence for a person to show that he:

(i) was not knowingly involved in designing, producing, or generating the illegal content; and

(ii) was not knowingly involved in the process by which the illegal content became part of that automated process.

***Final Recommendation 15***

We recommend that, in respect of the proposed offence of making available a device, program or data for committing a cyber-related crime, or possessing a device, program or data for the purpose of making it available for committing a cyber-related 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, program or data for committing a cyber-related crime;

(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.

***Final Recommendation 16(d)***

We recommend that, in respect of the proposed offence of making available a device, program or data for committing a cyber-related crime (or possessing such a device, program or data for the purpose of making it available to another), 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.

## Limitation period for summary proceedings

***Final Recommendation 3***

We recommend 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).

**Annex**

## List of Respondents to the consultation

Responses were received from the following Respondents, arranged in alphabetical order:

1. Asia Cloud Computing Association
2. Asia Solution Corporation Limited
3. Cheng Horace
4. Cheung Peter
5. Cloud Security Alliance Hong Kong and Macau Chapter
6. Consumer Council
7. Criminal Law Reform Now Network
8. Customs and Excise Department
9. Cyber Security and Technology Crime Bureau, Hong Kong Police Force
10. Democratic Alliance for the Betterment and Progress of Hong Kong
11. Dyer Allan
12. eWalker Consulting (HK) Limited
13. Federation of Hong Kong Industries
14. Fg Fg
15. FinTech Association of Hong Kong
16. Fung Sammy
17. Fung Stephen
18. Gee Sui Wah William
19. Ho Sam
20. Hong Kong Applied Science and Technology Research Institute Company Limited
21. Hong Kong Bar Association
22. Hong Kong Computer Society
23. Hong Kong Federation of Women Lawyers Limited
24. Hong Kong General Chamber of Commerce
25. Hong Kong Internet Registration Corporation Limited
26. Hong Kong Internet Service Providers Association
27. Hong Kong Professionals and Senior Executives Association
28. Hong Kong Society of Notaries

29. Hong Kong Women Professionals and Entrepreneurs Association
30. Hui Kai Lung and Zhou Jiali, Department of Information Systems, Business Statistics and Operations Management, Business School, Hong Kong University of Science and Technology
31. Ieong Ricci
32. Information Security and Forensics Society
33. Intellectual Property Department
34. ISACA China Hong Kong Chapter
35. Legal Aid Department
36. Logistics and Supply Chain MultiTech R&D Centre Limited
37. Mother's Choice
38. Office of the Communications Authority
39. Office of the Government Chief Information Officer
40. Office of the Privacy Commissioner for Personal Data
41. Open Web Application Security Project (Hong Kong Chapter)
42. Path of Democracy
43. Pong Ronald
44. Professor SM Yiu, Department of Computer Science, The University of Hong Kong
45. Sai Kung District Fight Crime Committee
46. S-TECH Limited
47. Suen Owen
48. Szeto Cynthia
49. Television Broadcasts Limited
50. The Duty Lawyer Service
51. The Hong Kong and Mainland Legal Professional Association Limited
52. The Hong Kong Chartered Governance Institute
53. The Institute of Certified Management Accountants (Hong Kong Branch)
54. The Law Society of Hong Kong
55. The Real Estate Developers Association of Hong Kong
56. The Society for Truth and Light
57. Tsang Kwong Hei
58. Wan Chai District Fight Crime Committee
59. Wang Wei
60. Wong Chris
61. Wong Ho Wa

62. 小市民
63. 碧海
64. Anonymous
65. Anonymous