香港法律改革委員會

報告書

依賴電腦網絡的罪行及司法管轄權事宜

本報告書已上載互聯網，網址為：**http://www.hkreform.gov.hk**。

2026 年 **1** 月

香港法律改革委員會（“法改會”）於 1980 年 1 月由當時的行政局任命成立，負責研究由律政司司長或終審法院首席法官轉交該會的有關香港法律的課題，以進行改革。

法改會現時的成員如下：

主席：　林定國資深大律師　GBS，JP
律政司司長

成員：	**張舉能首席法官**	**大紫荊勳賢，終審法院首席法官**
	林文翰法官	**終審法院常任法官**
	林少忠先生	**法律草擬專員**
	陳淑薇女士	**GBS，JP**
	熊運信先生	**MH**
	蔡關穎琴女士	**BBS，MH，JP**
	陳澤銘先生	**JP**
	梁高美懿議員	**SBS，JP**
	陸飛鴻教授	
	莊邁豪教授	
	駱敏賢資深大律師	
	習超教授	

法改會的秘書長是**律政專員黃惠沖資深大律師，JP**，法改會的辦事處地址為：

香港中環花園道三號
冠君大廈 9 樓
電話：3703 6518
傳真：3702 0136
電郵：hklrc@hkreform.gov.hk
網址：http://www.hkreform.gov.hk

陳澤銘先生，JP 在 2025 年 12 月 31 日後卸任法律改革委員會（法改會）成員。法改會主席及秘書處感謝陳先生多年來對法改會工作的寶貴貢獻及意見。

香港法律改革委員會

報告書

依賴電腦網絡的罪行及司法管轄權事宜

目錄

頁

頁

界定用語

用語／簡稱	定義
取覽罪	非法取覽程式或數據
《基本法》第二十三條立法	《維護國家安全條例》
《布達佩斯公約》	歐洲委員會（Council of Europe）的《電腦網絡罪行公約》（Convention on Cybercrime）
《英格蘭誤用電腦法令》	《1990 年誤用電腦法令》（Computer Misuse Act 1990）（英格蘭及威爾斯）
《新加坡誤用電腦法令》	《1993 年誤用電腦法令》（Computer Misuse Act 1993）（新加坡）
《刑事罪行條例》	《刑事罪行條例》（第 200 章）
私隱專員	個人資料私隱專員
同意免責辯護	《刑事罪行條例》（第 200 章）第 64(2)(a)條所示的免責辯護[1]
分布式拒絕服務	分布式拒絕服務（Distributed denial of service，“DDOS”）
域名系統	域名系統（Domain name system，“DNS”）
《數位服務法案》	《數位服務法案》（Digital Services Act）
歐盟	歐洲聯盟
大律師公會	香港大律師公會
女律師協會	香港女律師協會有限公司
香港特區	中華人民共和國香港特別行政區

[1] 見第 2.96 及 4.11 段。

女工商專聯	香港女工商及專業人員聯會
《截取通訊及監察條例》	《截取通訊及監察條例》(第 589 章)
干擾罪	非法干擾電腦數據及非法干擾電腦系統
互聯網規程	互聯網規程(Internet protocol，“IP”)
互聯網服務提供者	互聯網服務提供者(Internet service provider，“ISP”)
英格蘭法律委員會	英格蘭及威爾斯法律委員會(Law Commission of England and Wales)
律師會	香港律師會
《精神健康條例》	《精神健康條例》(第 136 章)
《相互法律協助條例》	《刑事事宜相互法律協助條例》(第 525 章)
《裁判官條例》	《裁判官條例》(第 227 章)
《示範法》	《電腦罪行及電腦相關罪行示範法》(Model Law on Computer and Computer Related Crime)
《國安法》	《中華人民共和國香港特別行政區維護國家安全法》
國安公署	中央人民政府駐香港特別行政區維護國家安全公署
私隱專員公署	個人資料私隱專員公署
《私隱條例》	《個人資料(私隱)條例》(第 486 章)
《公安條例》	《公安條例》(第 245 章)

保護財產免責辯護	《刑事罪行條例》（第 200 章）第 64(2)(b)條所示的免責辯護[2]
《俄羅斯公約》	俄羅斯聯邦於 2017 年 10 月 11 日向聯合國提交的《聯合國合作打擊網絡犯罪公約》草案（*Draft United Nations Convention on Cooperation in Combating Cybercrime*）
第 161 條	《刑事罪行條例》（第 200 章）第 161 條
第 64(2)條	《刑事罪行條例》（第 200 章）第 64(2)條
第 27A 條	《電訊條例》（第 106 章）第 27A 條
《儲存通訊法案》	《儲存通訊法案》（Stored Communications Act）
《盜竊罪條例》	《盜竊罪條例》（第 210 章）
《電訊條例》	《電訊條例》（第 106 章）
《聯合國公約》	《聯合國打擊網絡犯罪公約》（United Nations Convention against Cybercrime）
《兒童權利公約》	《聯合國兒童權利公約》（United Nations Convention on the Rights of the Child）
美國	美利堅合眾國

[2] 見第 2.96 及 4.11 段。

導言

引言

1. 法律改革委員會轄下的電腦網絡罪行小組委員會（“**小組委員會**”）在2022年7月發表《依賴電腦網絡的罪行及司法管轄權事宜》諮詢文件（“**諮詢文件**”）。本報告書論述就該諮詢文件收到的回應，並載列我們對這個課題的分析及最終建議。

背景

2. 對世上很多人而言，資訊科技、電腦和互聯網已滲透日常生活各方面。正當我們享受科技進步帶來的便利，不法之徒亦藉此從事非法勾當。關於刑事法應如何應對這些不當手段，全球各地似乎普遍認為特別針對電腦網絡空間的法例可補足一般適用的法例。

3. 中華人民共和國香港特別行政區（“**香港特區**”）最近期的電腦網絡罪行官方研究追溯至2000年，當時香港特區政府召開了電腦相關罪行跨部門工作小組。隨着過去20年科技和社會發展一日千里，現正是再次檢視這個課題的成熟時機。因此，於2019年初，終審法院首席法官聯同律政司司長將電腦網絡罪行這課題轉介予香港法律改革委員會研究。法律改革委員會委任小組委員會探討法律現況和提出建議。

4. 小組委員會就這課題展開討論後，《中華人民共和國香港特別行政區維護國家安全法》（**《國安法》**）於2020年6月30日制定為全國性法律，並在香港特區公布實施。香港特區維護國家安全的責任，再次確認有需要改革香港特區的電腦網絡罪行法律，[1] 我們研究電腦網絡罪行這課題時已將此考慮在內。

研究範圍

5. 2019年，小組委員會就電腦網絡罪行課題展開研究，研究範圍如下：

---

[1] 除了《中華人民共和國香港特別行政區維護國家安全法》第三條所載的總則外，第九條亦特別規定，對網絡等涉及國家安全的事宜，香港特別行政區政府應當採取必要措施，加強管理。

"鑑於資訊科技、電腦和互聯網方面發展迅速，加上其有被利用來從事犯罪活動的潛在可能，

(a) 從刑事法角度找出這些迅速發展對保障個人權利和執法帶來哪些挑戰；

(b) 檢討處理上文(a)段所指挑戰的現有法例和其他相關措施；

(c) 探討其他司法管轄區的相關發展；及

(d) 建議可作出哪些法律改革以應對上述事宜。"

小組委員會的成員

6. 小組委員會由陳政龍資深大律師出任主席，成員如下：

陳政龍資深大律師 ***（由 2023 年 1 月 19 日起出任主席）***	資深大律師
梁鎮宇先生 ***（由 2018 年 12 月 13 日至 2023 年 1 月 18 日出任主席）***	德同國際有限法律責任合夥 資深顧問律師
陳淑儀女士 （任期由 2018 年 12 月 13 日至 2023 年 9 月 12 日）	律政司助理刑事檢控專員
陳穎詩女士 （任期由 2025 年 3 月 25 日起）	保安局首席助理秘書長
鄭松岩博士 （任期由 2022 年 1 月 12 日至 2024 年 2 月 25 日）	中國銀行（香港）有限公司 前首席信息官

鄭麗琪女士 （任期由2022年5月3日至2024年2月25日）	香港警務處財富情報及調查科總警司 香港警務處網絡安全及科技罪案調查科前總警司
張佩珊女士 （任期由2023年4月21日至2025年3月24日）	保安局前首席助理秘書長
鄒錦沛博士	物流及供應鏈多元技術研發中心有限公司研究顧問 香港大學計算機科學系前副教授
徐詩妍女士 （任期由2019年8月12日至2023年4月16日）	保安局前首席助理秘書長
方永佳先生 （任期由2018年12月13日至2020年9月13日）	香港海關版權及商標調查(行動）課前監督
何沈潔玲女士 （任期由2018年12月13日至2020年12月20日）	香港上海滙豐銀行有限公司亞太區復元風險管理前主管
何應富先生 （任期由2023年1月13日起）	消費者委員會副總幹事
關煜群博士	亞太互聯網中心首席執行官
林焯豪先生 （任期由2024年2月26日起）	香港警務處網絡安全及科技罪案調查科總警司

羅紹佳先生 （任期由 2018 年 12 月 13 日至 2020 年 7 月 13 日）	羅本信律師行前合夥人
羅越榮博士 （任期由 2018 年 12 月 13 日至 2022 年 4 月 12 日）	香港警務處東九龍總區指揮官 香港警務處網絡安全及科技罪案調查科前高級警司
梁育珩先生 （任期由 2023 年 9 月 13 日起）	律政司署理高級助理刑事檢控專員
譚佩英女士 （任期由 2024 年 5 月 21 日至 2025 年 7 月 31 日）	香港海關版權及商標調查科高級監督 香港海關版權及商標調查（行動）課前監督
鄧均林先生 （任期由 2021 年 1 月 11 日至 2022 年 1 月 11 日）	香港上海滙豐銀行有限公司香港及澳門區營運韌性風險前總監
鄧子揚先生 （任期由 2023 年 1 月 9 日起）	鄧子揚顧嘉恩律師行合夥人
湯熾忠先生 （任期由 2018 年 12 月 13 日至 2023 年 1 月 12 日）	消費者委員會前副總幹事
曾裕彤先生 （任期由 2018 年 12 月 13 日至 2019 年 8 月 9 日）	保安局前首席助理秘書長
王家俊先生 （任期由 2025 年 8 月 1 日起）	香港海關版權及商標調查（行動）課監督

黃佩琪資深大律師	資深大律師
黃蕙荃女士 （任期由 2020 年 9 月 14 日至 2024 年 5 月 8 日）	香港海關助理關長 香港海關版權及商標調查（行動）課前監督
黃詠恒女士 （任期由 2024 年 2 月 26 日至 2025 年 12 月 19 日）	香港上海滙豐銀行有限公司前常務總監兼首席資訊科技總監
葉旭暉先生	香港互聯網供應商協會主席

7. 小組委員會自成立以來，一直定期召開會議。法律改革委員會秘書處高級政府律師卓芷穎女士是小組委員會的秘書。[2]

項目的三個階段

8. 由於小組委員會的研究範圍廣泛，加上國際間電腦網絡罪行的規管情況瞬息萬變，我們決定分階段處理這課題所引起的事宜：

(a) 項目第一部分處理依賴電腦網絡的罪行及司法管轄權事宜；

(b) 第二部分會涵蓋借助電腦網絡的罪行，該部範圍適時再作討論；及

(c) 第三部分會處理證據事宜及執法（程序）事宜。

第一部分研究的五類依賴電腦網絡的罪行

9. 本報告書關乎項目的第一部分。我們借鑑歐洲委員會（Council of Europe）《電腦網絡罪行公約》（Convention on Cybercrime，**《布達佩斯公約》**）及《聯合國打擊網絡犯罪公約》（United Nations Convention against Cybercrime，**《聯合國公約》**），[3] 集中研究以下五類依賴電腦網絡的罪行。這些罪行是全球公認應對付的主要電腦網絡罪行種類：

---

[2] 時任高級政府律師馬文舜先生擔任小組委員會的秘書至 2021 年 5 月，而高級政府律師李灝棋先生由 2024 年 9 月 2 日至 2025 年 9 月 17 日擔任小組委員會的秘書。

[3] 歐洲委員會《電腦網絡罪行公約》及《聯合國打擊網絡犯罪公約》的詳情載於第 1 章。

(a) 非法取覽程式或數據；

(b) 非法截取電腦數據；

(c) 非法干擾電腦數據；

(d) 非法干擾電腦系統；及

(e) 提供被製造或改裝以用作干犯電腦網絡相關罪行的器材、程式或數據（包括為向他人提供該等器材、程式或數據而管有它們）。

建議背後的指導原則

10. 我們明白制訂建議時需顧及各方持份者不同的權益及看法，亦理解當中的重要性。我們的指導原則，是同時平衡兼顧：

(a) 網民的權利和資訊科技業內人士的權益；及

(b) 保障公眾在使用和操作電腦系統時免受騷擾或攻擊的權益和權利。

諮詢過程

11. 為期三個月的諮詢期於 2022 年 10 月 19 日結束。總計收到的意見書共 65 份（部分於要求延期後收到），由簡單的確認收到諮詢文件，以至對諮詢文件內小組委員會的建議及問題發表詳細意見不等。

12. 提交意見書的回應者包括學者、政府決策局／部門、半官方機構、資訊科技相關團體、法律專業團體、商業團體、政黨，以及公眾人士（“**回應者**”）。回應者的名單載於本報告書附件。我們十分感謝所有曾對諮詢文件提出意見的回應者，後述各章會概述他們所提交的意見書。

13. 小組委員會的代表除了出席電視及電台訪問，解釋諮詢文件內的建議之外，亦參加了由香港大學計算機科學系於 2022 年 9 月 14 日舉辦的網上科技論壇（HKU-CS Online Tech Forum），以及由立法會科技創新界功能界別邱達根議員於 2022 年 10 月 27 日主持的答問環節。兩個場合席上大多為資訊科技及電訊界別的持份者，為小組委員會提供適當機會接觸網絡安全從業員，並釐清諮詢文件內某些建議。

14. 2022年11月7日（此為徵詢立法會後為小組委員會所能安排的最早會議時段），小組委員會成員出席立法會司法及法律事務委員會的會議，簡介諮詢文件內容，並聽取團體代表意見。

本報告書的結構

15. 本報告書由九個章節組成，處理16項最終建議：

(a) 第1章交代背景，描述國際機構和舉措如何將電腦網絡罪行歸類。

(b) 第2章先探討五類依賴電腦網絡罪行的第一類，即非法取覽程式或數據。

(c) 第3章集中討論第二類依賴電腦網絡的罪行，即非法截取電腦數據。

(d) 第4章涵蓋第三類依賴電腦網絡的罪行，即非法干擾電腦數據。

(e) 第5章繼而檢視第四類依賴電腦網絡的罪行，即非法干擾電腦系統。

(f) 第6章處理第五類依賴電腦網絡的罪行，即提供用作干犯電腦網絡相關罪行的器材、程式或數據，或管有用作干犯電腦網絡相關罪行的器材、程式或數據。

(g) 第7章轉談香港法庭行使司法管轄權的準則。

(h) 第8章處理有關上述依賴電腦網絡罪行的判刑事宜。

(i) 第9章總結我們的最終建議。

16. 回應者的名單（附件）載於本報告書末。

第 1 章　電腦網絡罪行的歸類

引言

1.1　正如小組委員會在諮詢文件指出，[1] 電腦網絡罪行既沒有確切的清單，也無法巨細無遺地逐一臚列。文獻列述了多種電腦網絡罪行的歸類方法，以及多組用於有關歸類的術語。在聯合國的層面，聯合國毒品和犯罪問題辦公室（United Nations Office on Drugs and Crime）在 2013 年展開的網絡犯罪問題全球方案（Global Programme on Cybercrime），區分*"依賴電腦網絡的罪行"*及*"借助電腦網絡的罪行"*。[2] 聯合王國政府的以下闡釋有助理解：

(a) 依賴電腦網絡的罪行指*"只能通過使用資訊及通訊科技器材進行的罪行，當中有關器材既是犯罪工具，亦是犯罪目標"*。[3] 依賴電腦網絡的罪行的例子包括：黑客入侵、散播電腦病毒及分布式拒絕服務攻擊。

(b) 借助電腦網絡的罪行指*"通過使用電腦、電腦網絡或其他形式的資訊及通訊科技，使犯罪規模或範圍得以擴大的傳統罪行"*。[4] 借助電腦網絡的罪行的例子包括：在網上散布兒童色情物品、設立仿冒詐騙網站及網上"起底"（即在互聯網未經授權而披露他人的私人資料或識別身分資料）。

在《布達佩斯公約》下的歸類

《布達佩斯公約》訂明的罪行

1.2　歐洲委員會（Council of Europe）的《電腦網絡罪行公約》（Convention on Cybercrime，**《布達佩斯公約》**）於 2001 年 11 月 23 日開放予各國

1　第 1.2 段。

2　聯合國毒品和犯罪問題辦公室（"**聯合國毒罪辦**"），*"網絡犯罪問題全球方案"*，登載於 https://www.unodc.org/unodc/en/cybercrime/our-approach（於 2025 年 11 月 1 日瀏覽）。

3　內閣辦公室國家安全及情報部（Cabinet Office, National security and intelligence）、英國財政部（HM Treasury）和國會議員夏文達（The Rt Hon Philip Hammond MP）：《2016–2021 年國家網絡安全戰略》（*National Cyber Security Strategy 2016-2021*）（聯合王國政府，2016 年），第 3.2 段，登載於 https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021（於 2025 年 11 月 1 日瀏覽）。

4　同上。

簽署，並於 2004 年 7 月 1 日生效。[5] 此後，《布達佩斯公約》由兩項《附加議定書》（Additional Protocol）作為補充，內容分別關於宣告將利用電腦系統犯下的種族主義或仇外行為訂為犯罪行為，[6] 以及關於加強合作和披露電子證據。[7]《布達佩斯公約》似乎是首份規管電腦網絡空間的跨國協議。[8] 截至 2025 年 11 月 1 日，已有 81 個國家批准或加入《布達佩斯公約》。[9]

1.3 《布達佩斯公約》第一節（第二至十三條）旨在制定有關罪行的共同最低標準，藉以改善防止和制止電腦罪行或電腦相關罪行的方法。[10]《布達佩斯公約》規定各締約國均須 *"採取必要的立法和其他措施"*，在其本土法律中就以下主題訂定刑事罪行（就遵從規定而言，顯然是"重實質多於形式"）：

(a) 損害電腦數據及系統的機密性、完整性和可用性的罪行（包括非法取用電腦系統、非法截取非公開傳送的電腦數據、非法干擾電腦數據、非法干擾電腦系統，以及為犯電腦網絡罪行而誤用器材或數據）；

(b) 電腦相關罪行（包括電腦相關偽造及電腦相關欺詐）；

(c) 內容相關罪行（包括兒童色情物品相關罪行，以及通過電腦系統散布種族主義和仇外材料的相關罪行）；及

(d) 關於侵犯版權和相關權利的罪行。

---

5 全文登載於歐洲委員會（Council of Europe）網站，網址為 https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185（於 2025 年 11 月 1 日瀏覽）。

6 第一項《附加議定書》於 2006 年 3 月 1 日生效，全文登載於歐洲委員會網站，網址為 https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189（於 2025 年 11 月 1 日瀏覽）。

7 第二項《附加議定書》於 2022 年 5 月開放予各國簽署，全文登載於歐洲委員會網站，網址為 https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224（於 2025 年 11 月 1 日瀏覽）。

8 除《布達佩斯公約》外，亦有其他區域舉措。例子見：聯合國毒罪辦，*"International and regional instruments"*，登載於 https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/international-and-regional-instruments.html（於 2025 年 11 月 1 日瀏覽）。

9 歐洲委員會，簽署及批准《電腦網絡罪行公約》列表（ETS 第 185 號），登載於 https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185（於 2025 年 11 月 1 日瀏覽）。

10 歐洲委員會，《電腦網絡罪行公約說明報告》（*Explanatory Report to the Convention on Cybercrime*）（ETS 第 185 號，2001 年 11 月 23 日），第 33 段，登載於 https://rm.coe.int/16800cce5b（於 2025 年 11 月 1 日瀏覽）。

《電腦罪行及電腦相關罪行示範法》

1.4 英聯邦（Commonwealth of Nations）秘書處是歐洲委員會電腦網絡罪行公約委員會（Cybercrime Convention Committee of the Council of Europe）的觀察員。英聯邦經參照《布達佩斯公約》，制定了《電腦罪行及電腦相關罪行示範法》（Model Law on Computer and Computer Related Crime）[11]（**《示範法》**）。《示範法》於 2002 年獲採納，而截至 2017 年 7 月，當局正考慮檢討該法。[12]

1.5 英聯邦秘書處於 2016 年 4 月 22 日的新聞稿指出，已有 22 個英聯邦國家採用《示範法》，作為其全國性電腦網絡罪行法律的基礎。[13]

聯合國的最新動向

1.6 國際間對電腦網絡罪行的規管情況正在急速變化。聯合國以下動向可能具影響力，值得密切關注：

(a) 俄羅斯聯邦（Russian Federation）於 2017 年 10 月 11 日向聯合國提交《聯合國合作打擊網絡犯罪公約》草案（Draft United Nations Convention on Cooperation in Combating Cybercrime，**《俄羅斯公約》**）。聯合國大會的有關決議沒有記錄任何協定的後續行動。[14]

(b) 大會於 2019 年 12 月 27 日採納的第 74/247 號決議[15] 中決定：

> "……設立一個代表所有區域的不限成員名額特設政府間專家委員會，以擬訂一項關於打擊為犯罪目的使用信息和通信技術行為的全面國際公約，同時充分考慮到關於打擊為犯罪目的使用信息和通信技術行為的現有國際文書和國家、區域和國際各級的現有努力，特別是

---

11 全文登載於英聯邦網站，網址為 http://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf（於 2025 年 11 月 1 日瀏覽）。

12 2018 年，在倫敦舉行的英聯邦政府首腦會議上簽署了《英聯邦網絡宣言》（Commonwealth Cyber Declaration）。此後展開了一項計劃，以便在英聯邦各國落實《網絡宣言》的承諾。

13 英聯邦秘書處，*"Commonwealth model law promises co-ordinated cybercrime response"*（2016 年 4 月 22 日），登載於 https://thecommonwealth.org/media/news/commonwealth-model-law-promises-co-ordinated-cybercrime-response（於 2025 年 11 月 1 日瀏覽）。

14 聯合國大會，第 72/196 號決議（A/RES/72/196，2017 年 12 月 19 日）。

15 聯合國大會，第 74/247 號決議（A/RES/74/247，2019 年 12 月 27 日）。

全面研究網絡犯罪問題不限成員名額政府間專家組的工作和成果”。[16]

(c) 經過上述特設委員會多年努力，《聯合國打擊網絡犯罪公約》（**《聯合國公約》**）於 2024 年 12 月 24 日由大會透過第 79/243 號決議採納。[17] 《聯合國公約》於 2025 年 10 月 25 日在越南開放供各國簽署，並會在紐約聯合國總部繼續開放供簽署，直至 2026 年 12 月 31 日。在 40 個國家成為締約方後，《聯合國公約》便會生效，而締約國會議將定期召開，審議該公約的實施情況，以期增強締約國的能力和促進締約國之間的合作，從而實現該公約的各項目標。[18]

1.7 《聯合國公約》是首條全面針對電腦網絡罪行的全球性條約，為各國提供一系列可採取的措施，以預防和打擊電腦網絡罪行，同時亦旨在加強國際合作，共享嚴重罪案的電子證據。[19]

1.8 讀者會記得，在 2022 年發表的諮詢文件中，有關建議借鑑了《布達佩斯公約》及《俄羅斯公約》的概念。[20] 就研究第一部分所載的依賴電腦網絡罪行而言，該等罪行在《布達佩斯公約》及《聯合國公約》下的歸類基本上相同，只是後述公約採用不同術語，例如“信息通信技術”（一如在諮詢文件中曾研究的《俄羅斯公約》）[21] 及“電子數據”，而非《布達佩斯公約》所分別採用的“電腦”及“電腦數據”。[22] 由此，繼續沿用諮詢文件所採納的術語，以及在本報

---

16 第 3 段。2022 年至 2023 年間，特設委員會召開六次會議，其閉幕會議於 2024 年 1 月 29 日至 2 月 9 日在紐約舉行，並於 2024 年 7 月 29 日至 8 月 9 日重新召開閉幕會議，由該委員會批准《聯合國打擊網絡犯罪公約》的決議草案。見：聯合國毒罪辦，*“Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes”*，登載於 https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home（於 2025 年 11 月 1 日瀏覽）。

17 聯合國毒罪辦，*“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”*，登載於 https://www.unodc.org/unodc/en/cybercrime/convention/home.html（於 2025 年 11 月 1 日瀏覽）。

18 同上。2025 年 10 月的簽署儀式結束時有 72 個簽署國，包括中國。各國在簽署後會完成本土的內部程序，以履行該公約，並會於完成後向秘書長交存批准書、接受書或核准書，以正式成為該公約的締約國。沒有簽署該公約的國家也可透過交存加入書而成為締約方。作為進一步資訊提供，特設委員會將於 2026 年 1 月 26 至 30 日在維也納召開會議，以擬備該公約締約國會議議事規則草案。見 https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_session_on_RoP/main.html（於 2025 年 11 月 1 日瀏覽）。

19 見上文註腳 17。

20 諮詢文件導言第 10 段。

21 諮詢文件第 2.93 至 2.95 段。

22 第 2.42 至 2.46 段會解釋，我們認為在新訂針對電腦網絡罪行的特定法例中保留“電腦”一詞屬恰當。

告書下文提述《布達佩斯公約》，並不影響項目第一部分所提出的最終建議的理據。政府如落實本報告書的建議，當然可自由決定如何以最理想的方式在新訂針對電腦網絡罪行的特定法例表述相關概念。

第 2 章　非法取覽程式或數據

引言

2.1　本章討論關於諮詢文件建議 1 至 3 的回應。建議 1 關乎第一類依賴電腦網絡的罪行，即非法取覽電腦中的程式或數據（“**取覽罪**”）：

> “小組委員會建議：
>
> (a) 在未獲授權下取覽程式或數據，應在新法例下定為簡易程序罪行，而合理辯解可作為法定免責辯護。
>
> (b) 在未獲授權下取覽程式或數據，並意圖進行其他犯罪活動，應構成新法例所訂的加重罪行，並招致更高刑罰。
>
> (c) 新法例的建議條文應以〔英格蘭及威爾斯《1990 年誤用電腦法令》（Computer Misuse Act 1990，《**英格蘭誤用電腦法令**》）〕第 1、2 及 17 條為藍本。”

2.2　正如小組委員會在諮詢文件解釋，[1] 概括而言，取覽罪一般旨在：

(a) 應對損害電腦系統安全的危險威脅及攻擊；

(b) 從而保護人們以不受干擾及不受限制的方式管理、操作和控制其電腦系統的權利。

2.3　由於部分回應提述《刑事罪行條例》（第 200 章）第 161 條（*“有犯罪或不誠實意圖而取用電腦”*）（“**第 161 條**”），這項條文又常被用來檢控現行法律下的電腦罪行，因此宜在本章複述該條的內容：

> “(1) 任何人有下述意圖或目的而取用電腦——
>
> (a) 意圖犯罪（不論是在取用電腦的同時或在日後任何時間）；

[1] 第 2.1 段。

(b) 不誠實地意圖欺騙(不論是在取用電腦的同時或在日後任何時間);

(c) 目的在於使其本人或他人不誠實地獲益(不論是在取用電腦的同時或在日後任何時間);或

(d) 不誠實地意圖導致他人蒙受損失(不論是在取用電腦的同時或在日後任何時間),

即屬犯罪,一經循公訴程序定罪,可處監禁5年。

(2) 就第(1)款而言,獲益(gain)及損失(loss)的適用範圍須解釋作不單擴及金錢或其他財產上的獲益或損失,亦擴及屬暫時性或永久性的任何該等獲益或損失;而且——

(a) 獲益(gain)包括保有已有之物的獲益,以及取得未有之物的獲益;及

(b) 損失(loss)包括沒有取得可得之物的損失,以及失去已有之物的損失。"

2.4 在*律政司司長 訴 鄭嘉儀*[2](*Secretary for Justice v Cheng Ka Yee*),終審法院裁定,*"根據恰當的詮釋,當任何人使用自己的電腦,而其中不涉及取用另一人的電腦,該行為便不干犯第161(1)(c)條"*。[3] 按邏輯推斷,亦可就第161(1)條的其他部分得出同一結論。因此,舉例來說,第161條不適用於任何人使用自己的電腦設立仿冒詐騙網站的情況。

2.5 與考慮取覽罪相關的另一條文是《電訊條例》(第106章)第27A條(*"藉電訊而在未獲授權下取用電腦資料"*)("**第27A條**"):

"(1) 任何人藉着電訊,明知而致使電腦執行任何功能,從而在未獲授權下取用該電腦所保有的任何程式或數據,即屬犯罪,一經定罪,可處第4級罰款。

---

2 (2019) 22 HKCFAR 97, FACC 22/2018(判決日期:2019年4月4日)。

3 同上,第48段。

(2) 就第(1)款而言——

(a) 該人的意圖不一定要針對——

(i) 任何個別程式或數據；

(ii) 任何個別種類的程式或數據；或

(iii) 任何個別電腦所保有的程式或數據；

(b) 任何人如無權控制對電腦所保有的程式或數據的有關種類的取用，且有下述情況，則他對電腦所保有的任何程式或數據的該類取用，即屬未獲授權——

(i) 他未獲有此權利的人授權，使他獲得對該電腦所保有的程式或數據的該類取用；

(ii) 他不相信自己已獲如此授權；及

(iii) 他不相信若他曾申請適當的授權，則他本已獲如此授權。

(3) 第(1)款的效力，並不損害關於檢查、搜查或檢取權力的任何法律。

(4) 儘管有《裁判官條例》（第227章）第26條的規定，關於本條所訂罪行的法律程序，可在發生該罪行的3年內或檢控人發現該罪行的6個月內（以最先屆滿的期間為準）任何時間提出。"

2.6 正如原訟法庭在*香港特別行政區 訴 秦瑞麟*（*HKSAR v Tsun Shui Lun*）[4] 裁定，第27A條適用的前提是犯罪者已"藉着電訊"獲得有關取用。由此可見，除了目標電腦外，當中亦涉及使用電訊器材（例如另一部電腦）以獲得有關取用。與此一致的是，第27A條在*鄭嘉儀*被定性為*"'黑客入侵'罪行"，"明顯是針對不屬於犯罪者自己的電腦"*。[5]

---

4 [1999] 3 HKLRD 215, HCMA 723/1998（判決日期：1999年1月15日），原訟法庭審理的裁判法院上訴案件，於*香港特別行政區 訴 歐陽家敏*（*HKSAR v Au Yeung Ka Man Yuniko*）[2018] HKCFA 23獲引用和認同。

5 見上文註腳2，第41段。

對小組委員會建議 1 的回應

2.7 就建議 1 提出意見的回應者普遍同意，在未獲授權下取覽程式或數據應定為罪行。香港與內地法律專業聯合會有限公司認為，第 161 條及第 27A 條有其 *"明顯"* 局限，因為該等條文均不適用於任何人使用自己的電腦或其他非電訊器材干犯電腦網絡罪行的情況。某政治團體及某商業機構也持同一看法，指出 *"終審法院"* 在 *鄭嘉儀*[6] *"大幅收窄了"* 第 161 條的適用範圍。

2.8 同樣地，消費者委員會也總體上同意需要立法禁止純粹在未獲授權下取覽程式或數據，前提是合理辯解可作為免責辯護，而且有特定的免責辯護或豁免涵蓋在未獲授權下為網絡安全目的而取覽。

2.9 然而，部分回應者關注取覽罪的範圍，並質疑"沒有犯罪意圖"而在未獲授權下取覽程式或數據（即純粹在未獲授權下取覽）應否屬犯罪。就建議 1 提出意見的其他回應者，則提議釐清"合理辯解"免責辯護的涵蓋範圍。下文會更詳細地載列回應者就建議 1 提出的各項意見。

建議 1(a)所述的純粹在未獲授權下取覽這項簡易程序罪行的犯罪意念

2.10 部分回應者將建議 1 與第 161 條比較，認為建議 1 完全沒有把 *"惡意意圖"* 納入考慮之列。多個資訊科技相關團體及個別人士均強調，把"犯罪／惡意意圖"、"惡意"、"罔顧後果"及／或發生損壞列為取覽罪的構成元素，實屬重要。從有關意見書中的闡述來看，回應者所構想的"惡意"或"惡意意圖"，似乎包括被告人參與 *"犯罪活動或非法活動"*，或被告人如第 161 條所述般 *"不誠實地意圖獲益、導致損失或欺騙"*。這些回應者有以下看法：

(a) 若不規定須懷有惡意，則合法行為也有可能被定罪。這些行為包括技術及保安方面的做法，例如雲端計算、滲透測試，以及保安專業人員、白帽黑客及漏洞賞金計劃參與者所採取的其他正常做法。

(b) 資訊科技專業人員及一般用戶均可輕易接觸大量數據（例如電話紀錄、電腦日誌紀錄），當中許多更是無須提交

---

[6] 見上文註腳 2。

密碼即可取覽。建議的（沒有惡意或犯罪意圖而）純粹在未獲授權下取覽罪，*"忽視了取覽作為的目的或意圖"*。

合理辯解作為法定免責辯護

2.11 部分回應者（包括某商業團體）認為，建議 1 所述的"合理辯解"法定免責辯護的範圍含糊不清、流於主觀，亦有欠明確。多間資訊科技相關機構、商業團體及某政治團體共作出三項提議：

(a) 在"合理辯解"的定義內明文加入各種獲豁免活動，例如*"網絡安全操作"*、*"互聯網服務提供者基於運作原因而進行的網絡掃描"*及*"沒有犯罪意圖的合法業務運作"*；

(b) 在法例中提供一份非盡列的例子清單，列舉會構成"合理辯解"的合法活動；及

(c) 就建議罪行訂定特定的免責辯護，以涵蓋合法的商業服務或行為，並應以概括方式擬定有關法定免責辯護或豁免，讓合法的業務經營者有足夠空間為自己辯白。

證明加重罪行

2.12 正如小組委員會在諮詢文件解釋，[7] 犯非法取覽罪的人或會在取覽有關程式或數據後進一步帶來可能嚴重的傷害。舉例來說，犯罪者可能會嘗試在目標電腦安裝間諜軟件，或意圖勒索受害人。單靠就建議的簡易程序罪行立法，將不足以應對社會所面臨的有關威脅。故此建議 1(b)提出，參照《英格蘭誤用電腦法令》第 2 條的擬定方式，[8] 訂明在未獲授權下取覽，並意圖進行其他犯罪活動，應構成新法例所訂罪行的加重形式。

2.13 就加重罪行而言，香港女律師協會有限公司認為，要就*"未犯的潛在罪行"*證明意圖*"頗為困難"*，故在嚴重罪行無法被確立為

---

7 第 2.107 段。

8 《英格蘭誤用電腦法令》第 2 條規定：

"(1) 任何人如犯上述第 1 條所訂罪行（'在未獲授權下取覽罪'），並——

(a) 意圖干犯本條所適用的罪行；或

(b) 意圖利便干犯該等罪行（不論是由其本人干犯或由他人干犯），

即屬犯本條所訂罪行；而該人意圖干犯或意圖利便的罪行，在本條下文提述為其他罪行。

……

(3) 就本條而言，不論其他罪行是與在未獲授權下取覽罪同時干犯或在日後任何時間干犯，屬無關重要。

(4) 即使有關事實顯示干犯其他罪行並不可能，任何人仍可被裁定犯本條所訂罪行。"

加重罪行時，當局或會極其依賴建議 1(a)所述的簡易程序罪行來處理該等罪行。該會進一步請小組委員會在判刑方面考慮這點，即就簡易程序罪行處以兩年監禁是否具足夠阻嚇性。

罪行互相重疊

2.14 對於小組委員會建議保留第 161 條，直至新訂的電腦網絡罪行法例顯然足以取而代之，兩名回應者在第 161 條所訂罪行與取覽罪互相重疊的問題上意見分歧。

2.15 一方的看法是，罪行互相重疊 *"相當可能會對公眾造成混淆，亦令法律變得不必要地複雜模糊"*，並指出若對各項罪行的檢控繼續根據第 161 條而非根據新法例提出，則未必能達到小組委員會所期望的目的。

2.16 相反的看法是，罪行互相重疊大概只是看似令人擔憂，但實際上不足為慮。有關論據引述如下：

> "……控方的檢控常規，是'充分反映指稱罪行的刑責，方式為既能兼顧檢控效率亦能令法庭於社會與被告兩者之間秉公行義'，且'在合理可行的情況下，控罪的數目應盡量減少'（《檢控守則》第 8.1 段）……即使某人被控並被裁定犯了多項在刑責上可能互相重疊的罪行，法庭也必然須按照確立已久的整體量刑原則對被告人判刑。"

界定若干詞語

2.17 部分商業團體、關注組及個別人士認為，應清晰界定或向公眾解釋若干概念（包括"在未獲授權下"／"在獲授權下"取用或取覽、"取用或取覽"、"電腦網絡"及"數據"）的涵義。

我們的分析及回應

釐清犯罪意念

2.18 某些回應者認為 *"沒有犯罪意圖"* 而純粹在未獲授權下取覽程式或數據不應屬犯罪，他們似乎把建議的罪行視為嚴格法律責任罪行，或認為必須有從事犯罪活動的意圖，方可構成在未獲授權下取覽罪。

2.19 在諮詢文件的建議 1(c)，小組委員會建議取覽罪應以《英格蘭誤用電腦法令》第 1、2 及 17 條為藍本。應當強調的是，有關的英格蘭罪行並非嚴格法律責任罪行，而是規定須證明犯罪意念。為清晰起見，宜在本報告書再次引述英格蘭取覽罪的相關條文。

2.20 《英格蘭誤用電腦法令》第 1 條（*"在未獲授權下取覽電腦資料"*）是英格蘭取覽罪的基本形式，該條規定如下：

"(1) 任何人在以下情況，即屬犯罪——

(a) 該人致使某電腦執行任何功能，意圖獲得對存於任何電腦內的任何程式或數據的取覽，或意圖使他人能夠獲得該項取覽；

(b) 該人意圖獲得該項取覽，或意圖使他人能夠獲得該項取覽，但該項取覽未獲授權；及

(c) 該人在致使該電腦執行該功能時，知悉情況如此。

(2) 任何人犯本條所訂罪行須具備的意圖，不一定要針對——

(a) 任何特定程式或數據；

(b) 任何特定種類的程式或數據；或

(c) 存於任何特定電腦內的程式或數據。

....."

（底線後加）

2.21 《英格蘭誤用電腦法令》第 17(5)及(8)條解釋取覽的未獲授權性質：

"(5) 在以下情況下，任何人取覽存於某電腦內的任何程式或數據，不論取覽屬任何種類，即屬未獲授權取覽——

(a) 該人本身無權控制對該程式或數據作出有關種類的取覽；及

(b) 該人未獲有此權利的人同意他對該程式或數據作出該類取覽……

……

(8) 在以下情況下，如某人就某電腦作出某作為，或導致就某電腦作出某作為，該作為即屬未獲授權——

(a) 該人本身不是對該電腦負有責任並有權決定可否作出該作為的人；及

(b) 該人未獲任何上述的人同意該作為。

在本款中，'作為'包括一連串作為。"

2.22 故此，《英格蘭誤用電腦法令》第 1(1)條所訂的簡易程序罪行的犯罪意念包括以下兩項：(i)被告人意圖獲得對任何程式或數據的取覽（或意圖使他人能夠獲得該項取覽）；及(ii)被告人在犯罪行為發生時，知悉該項意圖作出的取覽未獲授權。換言之，關於取覽性質的犯罪意念是控方必須證明的所需元素，而且只有當犯罪行為（即取覽的行為元素）及犯罪意念（即知悉取覽的未獲授權性質這項意念元素）同時存在，才能夠產生取覽罪。控方或法庭必須信納，被告人在未獲授權的取覽作出時，知悉該項取覽未獲授權。

2.23 我們維持原先看法，即我們認為把某人知悉其取覽未獲授權定為取覽罪的先決條件，是公允的做法。我們預料，法庭很可能會根據案件的環境證據，作出關於某人是否知悉未獲授權的推論。[9] 就此而言，部分回應者的意見書所引述的一宗真實案例正可闡明這點：某乘客發現，航空公司發出的電子登機證存在保安漏洞，令他能透過修改有關劃一資源定位址（URL）的最後兩位字元，查閱其他乘客的資料。事件經調查後，發現被告人的互聯網規約（"**IP**"）地址在未獲授權下連接至另一乘客的網上預訂頁面。被告人根據第 27A 條被起訴。[10] 我們認為，雖然該航空公司沒有採取足夠的保安措施，以保護其他乘客的登機資料，但被告人乘客作為該公司有關電子系統的普通用戶，並不應預期該公司已授權自己透過修改有關 URL，取覽同機乘客的登機證。故此，有充分理由根據第 27A 條對他提出起訴。

---

9 諮詢文件第 2.101 段。

10 案件編號是 WKS6208/2019。最終，被告人同意簽保守行為一年，獲控方不提證供起訴。見 https://www.hk01.com/article/347780（於 2025 年 11 月 1 日瀏覽）。

2.24　我們在此補充一點，凡任何人指稱自己不知悉某項取覽的未獲授權性質，便應在引致該項取覽的整個事件過程中驗證該項指稱是否屬實。舉例來說，假設某法定機構的數據檔案外洩，令數千名與該機構有事務往來的人的資料被洩露，某君自稱積極分子，維持某網站或社交媒體專頁（並宣稱以在香港推動透明問責為宗旨），將這宗資料外洩事故公諸於世。若某人因此發現了這宗資料外洩事故，繼而取覽在公眾領域的外洩數據，法庭便會對引致被告人瀏覽實際載有外洩資料的網站的各項事實進行查訊。最終法庭會在考慮案件的整體情況後，裁定是否可從證據作出以下必然推論：被告人在作出有關取覽時，知悉該項取覽未獲授權。

純粹在未獲授權下取覽應屬犯罪

2.25　各回應者就取覽罪的意念元素所提出的意見，也關乎純粹在未獲授權下取覽程式或數據應否屬犯罪這問題，諮詢文件第 2 章已對此作透徹的討論。[11] 小組委員會從一開始就理解到，電腦網絡空間因為其本質，與具有形和明確界線的現實世界分屬截然不同的領域：

> "……鑑於虛擬空間的設計和運作的固有特點，以及在虛擬空間的慣常做法，在某些獲廣泛接受的情況下，網上用戶均已默示給予取覽程式或數據的授權。事實上，任何人若把器材連接至互聯網或使用互聯網服務，他某程度上已默許與其他網上用戶作某（合理）程度的互動。舉例來說，我們一般並不預期網上用戶在向傳送對象（即另一網上用戶）發送電郵或展示網頁廣告前，須事先尋求後者的明示授權，尤其是當有關發送或展示並非惡意作出。另一例子是，搜尋器會在多個互聯網規約地址掃描互聯網，[12] 從而確定這些地址是否有網頁伺服器，並為找到的網頁建立索引。因此，在電腦網絡空間

11　第 2.4、2.5、2.96 至 2.101 段。

12　具體而言，搜尋器會經常測試連接埠 80 及 443，這兩個連接埠一般都與取覽網站相關。在電腦網絡空間，連接埠是網絡連接開始與結束的電腦虛擬點，均以軟件為基礎，並由電腦系統管理。連接埠 80 被指定用於"HTTP"（超文本傳輸規約），用作傳送網頁。連接埠 443 被指定用於"HTTPS"（保密超文本傳輸規約），用作安全地經由傳輸層保安（TLS）或保密插口層（SSL）傳送網頁。見 https://isc.sans.edu/forums/diary/Cyber+Security+Awareness+Month+Day+25+Port+80+and+443/7450（於 2025 年 11 月 1 日瀏覽）。鑑於對連接埠 80 及 443 的明確指定，法律不應禁止連接至這些連接埠，以作其指明所用的指定用途。另外，搜尋器一般會使用網絡爬蟲軟件，有系統地瀏覽網頁，以搜集網頁的相關資料。這過程可為有關資料建立索引，並讓用戶在進行搜尋查詢時得以檢索這些資料。見 Alexander S Gillis, "What is a web crawler?"，登載於 https://www.techtarget.com/whatis/definition/crawler（於 2025 年 11 月 1 日瀏覽）。

這一領域，應在上述背景之下理解‘在未獲授權下’取用或取覽這個概念。”[13]

2.26 換言之，基於我們在上文解釋“在未獲授權下”取用或取覽這概念時所述的理由，將繼續容許在日常生活中已普遍接受在進入電腦網絡空間時的慣常做法或行業常規，亦即無須就小組委員會已舉例說明（而我們亦同意）的取用或取覽程度，事先尋求明示授權。[14] 建議 1 正是在這基礎上提出純粹在未獲授權下取覽程式或數據應構成罪行。個別案件中的取覽是否獲得默示授權，會視乎證據所顯示的事實和情況而定。[15] 另一些涉及默示授權的情況例子，包括但不限於以下情況：因設計緣故[16] 和實際需要[17] 而進行自動連接，並由此而產生取覽程式或數據。

2.27 在此亦宜複述歐洲委員會（Council of Europe）的《電腦網絡罪行公約說明報告》（Explanatory Report to the Convention on Cybercrime）中的評註，當中論述純粹在未獲授權下取用電腦／取覽程式或數據所造成的後果：

> “44. 原則上，純粹在未獲授權下入侵……本身應屬非法。有關行為可能會對系統和數據的合法使用者造成阻礙，亦可能導致涉及高昂重建費用的更改或摧毀。這類入侵行為或會使人得以取覽機密數據（包括密碼、關於目標系統的資料）及秘密，以及免費使用有關系統，甚或鼓勵黑客干犯更具危害性的電腦相關罪行，例如電腦相關欺詐或電腦相關偽造。

---

13 諮詢文件第 2.5 段。

14 同上。

15 諮詢文件第 2.100 段。

16 例如，當智能電話的用戶在購物商場開機並啟動其 Wi-Fi 功能時，即使該用戶沒有選擇把自己的電話連接至商場的 Wi-Fi 熱點，該器材也會自動偵測商場所提供的可用 Wi-Fi 熱點，而商場的網絡亦同樣會偵測到該用戶的電話。另一個例子是，當用戶把自己的個人電腦連接至某公共 Wi-Fi 接駁點並將電腦設定為可搜尋時，連接至同一 Wi-Fi 接駁點的任何其他電腦或電子器材均能夠偵測到該用戶的個人電腦。在上述每個例子，有關用戶的器材（前者）均是通過以下方式而被另一器材（後者）接達：後者向前者發出通訊請求，前者繼而發出回應。

17 以下例子可用作說明：(i)點對點檔案分享；及(ii)分散區塊鏈技術。點對點檔案分享讓用戶無需借助中央伺服器，便能互相分享數據及電子檔案。某用戶在個人電腦運行點對點軟件時，該軟件會向其他可供接達的節點（即其他連接至互聯網的電腦）發出數據，而這些節點可能會發出回覆，然後在兩個節點之間建立連線。同樣地，分散區塊鏈經常會使用點對點網絡來搜尋節點。在這種情況下，各節點（例如能夠連接互聯網的電腦或智能電話）會向有關網絡作出廣播以示其存在，並聽候來自其他節點的信息。某節點在收到來自新節點的信息時，便可建立連線並交換信息。見 Radovan Stevanovic, *“Blockchain from Scratch: Understanding Network Communication in Blockchains”*（2023 年 1 月 3 日）。

> 45. 最有效防止在未獲授權下取用的方法，當然是推行和制訂有效的保安措施。不過，全面的應對方案亦須包括威脅施加和採用刑事法律措施。以刑事法例禁止在未獲授權下取用，能夠及早為有關系統和數據本身提供額外保護，免受上述各種危險。"
>
> （底線後加）

2.28 我們曾進一步研究《英格蘭誤用電腦法令》的外在立法材料，當中闡明訂立取覽罪的基本形式（即純粹在未獲授權下取覽）的目的。由於黑客的企圖入侵所造成的不確定性及成本，英格蘭及威爾斯法律委員會（Law Commission of England and Wales，"**英格蘭法律委員會**"）把通過在未獲授權下進入而進行的黑客入侵，視為*"系統用戶有正當理由高度關注的事情"*。[18] 據英格蘭法律委員會解釋：

> "……由於任何企圖進入者或許均已透過密碼獲得重要級別的權限，其級別之高，有時更讓他們可從有關系統中刪除自己的活動紀錄，因此須極為嚴肅看待一切在未獲授權下成功取覽的情況。故此，在以下兩方面產生龐大費用：(i)採取保安措施抵禦未獲授權進入系統，並採取同等重要的預防措施，監察企圖進入系統的情況；以及(ii)調查事實上確有發生未獲授權進入系統的一切事件，不論案情如何輕微……我們信納……相關成本龐大。"[19]
>
> （底線後加）

2.29 因此，純粹在未獲授權下取覽罪當時所回應的一點，是*"人們需要保護電腦系統的完整及安全，使其免受尋求進入這些系統的未獲授權人士攻擊，不論這些人有何意圖或動機"*，[20] 而英格蘭法律委員會建議分別訂立《英格蘭誤用電腦法令》第1及2條的簡易程序罪行及加重罪行，*"藉此阻嚇黑客入侵"*。[21] 這兩項罪行旨在共同發揮作用，以有效阻嚇各種形式的未獲授權取覽。[22]

---

18 英格蘭法律委員會，*"Criminal Law – Computer Misuse"*（英格蘭法律委員會第 186 號，1989 年），第 1.29 段。

19 同上，第 1.37 段。

20 同上，第 1.37 段。

21 同上，第 1.37 段。

22 同上，第 3.2 段。

2.30　由於《英格蘭誤用電腦法令》在數碼時代來臨前已經制定，當時互聯網的使用較不普及，故我們曾考慮英格蘭法律委員會的理據在現今狀況下依然適用的程度。我們認為，由於互聯網如今滲透大部分公共和私人生活，因此更有需要確保電腦系統及網絡的完整性，使其免受未獲授權的取用或取覽。最近數碼港及消費者委員會先後遭黑客入侵的新聞，正好顯示在電腦網絡空間這範疇上絕不能掉以輕心。[23]

2.31　鑑於上述理由，我們維持原先看法，認為純粹在未獲授權下取覽程式或數據應構成罪行。

合理辯解作為法定免責辯護——應否在“合理辯解”的定義內明文加入某些活動，以及應否在法例中提供一份非盡列的例子清單

2.32　正如終審法院在*香港特別行政區　訴　何來*（*HKSAR v Ho Loy*）[24]所解釋，“無合理辯解”（不論作為免責辯護，還是控方須證明的元素）是法規中常見的用語，而某辯解是否合理須視乎個別案件的具體事實和情況而定。[25] 我們認為，嘗試在電腦網絡罪行法例中詮釋“合理辯解”，或嘗試闡明有關立法原意（例如擬定一份“合理辯解”的例子清單），均可能會收窄合理辯解免責辯護的範圍。倘若被告人在案中的作為或行為偏離法例中的例子所述，便會面臨法庭對其作出不利裁決的風險。因此，為了讓“合理辯解”的範圍盡可能廣闊，我們建議不應界定該詞。

2.33　另外，我們留意到就概念而言，“合理辯解”是被告人無須承擔法律責任的辯白理由，而非支持其行為的理由。故此，“合理辯解”這概念，本來就與不應視為違法的合法目的並不契合。正因如此，我們認為不宜把各種合法活動歸入合理辯解免責辯護的範圍，反而較適宜把這些活動訂明為法定免責辯護，即表明有關活動並不構成罪行。

2.34　故此，我們建議應在合理辯解免責辯護之外提供特定的免責辯護，以豁除我們認為顯然不屬非法的行為。這樣會消除公眾對某些

23　2023 年 8 月，據報某勒索軟件組織先對數碼港的電腦系統進行黑客入侵，再向它勒索。大量個人資料外洩，其後在暗網被公開，當中包括銀行帳戶資料、身分證號碼及職員證資料。兩星期後，消費者委員會亦遭黑客入侵，被盜取的內容包括員工及空缺申請人的資料。見《南華早報》社評，*"Hong Kong's Cyberport hack sends reminder to be alert"*（2023 年 9 月 16 日），以及《星島日報》*"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"*（2023 年 9 月 22 日）。

24　(2016) 19 HKCFAR 110, FACC 7/2015（判決日期：2016 年 3 月 23 日）。

25　同上，第 127 頁（第 37 段）。

活動是否屬合理辯解免責辯護範圍的疑惑，而在我們建議的特定免責辯護並不適用時，合理辯解免責辯護或可作為後備選擇。這種處理方法亦清晰明確，可釋除對法例有含糊之處的疑慮。在本章的後半部分，我們會詳細闡釋建議的各項特定免責辯護。[26]

執法機關取覽程式或數據

2.35 部分回應者（包括政府相關機構及商業團體）尋求澄清以下一點：執法機關在有手令或無手令的情況下為刑事調查目的而取覽電腦程式或數據（例如疑犯的流動電話所儲存的電腦程式或數據），以及業務經營者為執法目的而取覽上述程式或數據（例如資料當事人的個人資料），會否獲豁免刑事法律責任。

2.36 我們留意到，*岑永根 訴 警務處處長*（*Sham Wing Kan v Commissioner of Police*）[27] 就執法機關搜查被捕人身上流動電話的數碼內容，訂下清晰指引。正如上訴法庭裁定，裁判官可根據《警隊條例》（第 232 章）第 50(7)條發出手令，[28] 授權搜查流動電話或其他電子器材的數碼內容。[29] 對於沒有手令的搜查，該搜查的範圍和目的須因有關逮捕而附帶引起。警務人員須有合理依據支持即時進行沒有手令的搜查對以下目的而言屬必要：(i)調查相關人士懷疑涉及的罪行，包括獲取及保存與罪行有關的資料或證據；或(ii)保護個人安全。[30] 此外，有關人員應按上述準則，將對數碼內容的仔細審查範圍限於相關項目，並對該項沒有手令的搜查的目的和範圍，作出充分書面記錄。[31]

2.37 由於取覽罪並非旨在影響執法機關進行的任何合法活動，我們建議將*"無合法權限"*納入為取覽罪的元素。個別案件中是否有*"合法權限"*這問題關乎客觀事實。警務人員如已為搜查流動電話或其他電子器材而取得裁判官所發出的搜查令，或有合理依據支持在無手令的情況下搜查這些器材，因而符合*岑永根*案中訂立的規定，便屬有*"合法權限"*而取覽程式或數據。若沒有搜查令或合理依據，則有關情況會類似於執法機關以脅迫或欺騙等手段非法取證。在該等

---

26 下文第 2.63 至 2.102 段。

27 [2020] 2 HKLRD 529, CACV 270/2017（判決日期：2020 年 4 月 2 日）。

28 《警隊條例》（第 232 章）第 50(7)條訂明，裁判官如覺得有合理因由懷疑在任何地方內，有任何物品或實產是相當可能對調查任何人所犯或合理地懷疑任何人已經或即將或意圖犯的罪行有價值的（不論就其本身或連同任何其他東西），則該裁判官可向任何警務人員發出手令，賦權給他搜查及接管該等物品或實產。

29 見上文註腳 27，第 34、163、166 及 218(a)段。

30 見上文註腳 27，第 187 及 218(b)段。

31 見上文註腳 27，第 188、199、218(c)及(d)段。

情況下，有關證據的可接納性可能受到質疑，執法機關的負責人員亦可能面對刑事調查，若有充分證據並符合公眾利益，更可能須面對刑事檢控。不論是否有合法權限，在迫切情況下取覽程式或數據，本身便可能屬於合理辯解免責辯護的範圍。因此我們認為，如未能提供充分理由而在無手令的情況下取覽程式或數據，即使是為了執法目的，也應構成取覽罪，實屬適當。

適宜訂立加重罪行

2.38 對於有回應者指出加重罪行*"太難證明"*，[32] 我們相信本港法庭會從個別案件的情況作出推論，並能據此就被告人的思想狀態作出裁定，因為這正是它們日常必須作出的判斷。此外，根據《檢控守則》，*"控方必須在法律上有充分證據支持檢控"*，[33] 而驗證標準是*"根據這些證據，是否有合理機會達致定罪"*。[34] 故此，控方相當可能只會在下述情況下就加重罪行提出檢控：有人實際上干犯有關較嚴重的罪行；或案件中有充分或具說服力的環境證據，可據此推論被告人意圖干犯其他罪行或（如未有人干犯加重罪行）意圖利便干犯其他罪行。控方亦可能就初步罪行（即企圖干犯加重罪行）提出檢控。基於這些原因，加重罪行雖然在觀感上看似難以證明，但事實上或許並非如此。

2.39 然而，倘若控方如上述回應者所指，在確立加重罪行時遇到實際困難，我們並不排除控方可能會改控建議 1(a)所建議訂立的簡易程序罪行。這亦說明了為何需要保留純粹在未獲授權下取覽這項簡易程序罪行。

2.40 須注意的另一重點是，無論如何，控方時刻有責任就眾多可循簡易程序審訊的可公訴罪行（不論它們是由成文法規訂立還是根據普通法訂立）選定審訊法庭。控方須考慮的主要因素包括：指稱罪行的嚴重程度、整體案情，以及定罪後可能判處的刑罰。[35] 因此，儘管有關加重罪行是可公訴罪行，但如根據案情有此需要，控方仍可選擇在裁判法院循簡易程序審訊該罪行。

---

32 上文第 2.13 段。

33 香港特別行政區律政司，《檢控守則》（2013 年），第 5.4 段。

34 同上，第 5.5 段。

35 同上，第 8.4 段。其他因素包括：可能有爭議的事宜、須予裁定的爭議事宜是否涉及社會的標準及／或價值觀、法律程序對公眾的重要性，以及任何加重或減輕刑罰的因素。

罪行互相重疊

2.41 毫無疑問，每項作為均可能被多於一項法定條文或法定罪行所涵蓋。由於非法作為可在不同情況下發生，我們認為法律中有重疊之處屬可接受。在建議的依賴電腦網絡的罪行仍未訂立時，就先揣測控方日後會如何處理電腦網絡罪行案件，似乎並無實質意義。如議論針對電腦網絡罪行的特定法例與第 161 條相比的優劣利弊，而沒有參考任何刑事案件的事實背景，上述揣測就顯得更無意義。

應否界定“取用或取覽”、“在獲授權下／在未獲授權下”取用或取覽、“電腦網絡”及“數據”

2.42 正如諮詢文件所解釋，[36] 小組委員會曾考慮應否參考俄羅斯聯邦（Russian Federation）擬備的《聯合國合作打擊網絡犯罪公約》草案（Draft United Nations Convention on Cooperation in Combating Cybercrime，**《俄羅斯公約》**），為“電腦”賦予法定定義。該公約把“資訊及通訊科技器材”界定為*“任何用於或設計用於自動處理和儲存電子資料的硬件組件的集合體（組合體）”*。[37] 小組委員會留意到原訟法庭對*律政司司長 訴 王嘉業*[38] 的判決的以下摘錄，並認為法庭有關觀點也適用於建議的依賴電腦網絡的罪行：

> “69. ……立法會對《刑事罪行條例》第 161 條之‘電腦’一詞不作出定義，是因為科技發展迅速，‘電腦’的定義廣闊和演變，不能盡錄。
>
> ……
>
> 73. ……詮釋涉及科學及技術的條文時，應視之為‘一直發言’，按照法例的語言，給與廣義的詮釋，應用於立法後演變的情況，除非超越了法例語言的自然釋義，或後果是荒謬或明顯不公義的。”[39]

2.43 我們贊同小組委員會的看法。隨着物聯網興起，未來可能會有越來越多器材成為罪犯的攻擊目標，即使是“資訊及通訊科技器材”這一概括定義，也可能落後於資訊科技勢如破竹的發展與演進。我們理解到若然欠缺定義，可能會令人無法立即清楚分辨某種採用較

---

36 第 2.93 至 2.95 段。

37 第四條第(o)款。

38 [2013] 4 HKLRD 588, HCMA 77/2013（判決日期：2013 年 4 月 29 日）。

39 同上，第 601 頁（高等法院原訟法庭法官馮驊）。

新穎技術的器材是否構成“電腦”。不過我們亦緊記，不管法定定義的表達是如何清晰（例如《俄羅斯公約》對“資訊及通訊科技器材”或《聯合國公約》對“信息通信技術系統”所下的定義），[40] 法定定義在實際應用上也不無困難，這是因為被告人或會極力提出各種技術性論點，辯稱有關“器材”在法律上並不構成立法機關原意中的“電腦”，隨着加入有關法定定義後時間日久，尤其會出現這種情況。我們固然可以信任法庭會在法例文本容許的情況下，因應科技進步而靈活地解釋在針對電腦網絡罪行的特定法例所加入的任何定義，以盡量體現真正的立法原意，但這樣也無法排除上述困難。

2.44 正如某商業團體在提交的意見書中正確地指出，“取用或取覽”及“截取”等電腦相關作為均可隨着科技發展而不斷演變。取覽電腦程式或數據的嶄新方法可能不時湧現。故此，較為適當的做法是不硬性界定何謂“取用或取覽”，而是賦予“取用或取覽”其通常涵義，以使建議的罪行達到應對損害電腦系統安全的威脅及攻擊這目的。

2.45 我們亦傾向認為，是否獲得授權的問題與事實密切相關，應由法庭按照個別案件的情況裁定，而且對“在未獲授權下”作出具體定義，可能會使某些獲普遍接受或慣常的互聯網做法變成違法行為，而由於有關網上用戶已默示給予取覽程式或數據的授權，這些做法是我們的建議所擬容許的（見上文第 2.25 及 2.26 段）。

2.46 基於上述理由，我們仍然認為較可取的做法是不界定“取用或取覽”、“在獲授權下／在未獲授權下取用或取覽”、“電腦”及“電腦系統”等詞語。無論如何，若我們的建議得到政府落實，法律草擬專員可在立法階段進一步探討這議題。

有關建議 1 的結論

2.47 基於上述各項理由，我們的結論是建議 1 可予保留，並可進一步釐清如下：

---

[40] 《聯合國公約》則力求界定甚麼會視為“信息通信技術系統”。根據該公約第二條第（一）項，“信息通信技術系統”指*“任何設備或任何一組相互連接或相關的設備，其中一個或多個設備按照某一程序收集、存儲並自動處理電子數據”*。有關《聯合國公約》的詳情，見第 1.6 至 1.8 段。

最終建議 1

我們建議：

(a) 無合法權限而在未獲授權下取覽程式或數據，應在新法例下定為簡易程序罪行，而合理辯解可作為法定免責辯護。

(b) 這項建議罪行的犯罪意念是：

(i) 被告人意圖獲得對有關程式或數據的取覽，或意圖使他人能夠獲得該項取覽；及

(ii) 被告人在取覽有關程式或數據時，知悉該項意圖作出的取覽未獲授權。

(c) 在未獲授權下取覽程式或數據，並意圖進行其他犯罪活動，應構成新法例所訂的加重罪行，並招致更高刑罰。

(d) 新法例的建議條文應以英格蘭及威爾斯《誤用電腦法令》第 1、2 及 17 條為藍本。

對小組委員會建議 2 的回應

2.48 我們接着探討諮詢文件建議 2 之中的諮詢問題，這項建議由以下幾部分組成：

> "小組委員會邀請公眾就以下問題提交意見書：在未獲授權下取覽，應否有任何特定的免責辯護或豁免：
>
> (a) 對於為網絡安全目的而取覽而言，如答案是應該的話，應有甚麼條款？舉例來說：
>
> (i) 該免責辯護或豁免應否只適用於經認可專業團體或評審團體審定的人士？

(ii) 如(i)段的答案是應該的話，評審制度應如何運作，例如有關評審的準則是甚麼？經審定人士應否有持續進修的規定？香港應否設立（譬如根據新訂的電腦網絡罪行法例設立或以行政方式設立）一個評審團體，並由該團體備存一份網絡安全專業人員名單，而比方說如經審定人士未能符合持續進修規定，便可將該人從該名單內除名或不准該人將其審定資格續期？評審團體以外的哪些人（如有的話）也應獲准查閱該名單？

(iii) 反之，如不屬意設立評審制度，則新訂針對電腦網絡罪行的特定法例應否訂明指認的網絡安全專業人員須符合某些規定，方可援引建議為網絡安全目的提供的免責辯護或豁免？如應該的話，這些規定應是甚麼？

(b) 該免責辯護或豁免應否適用於非保安專業人員（請參閱建議 8(b)所述的例子）？"

支持為網絡安全業界提供特定免責辯護的回應者的意見

2.49 絕大多數回應者均支持建議 2，當中包括法律專業團體、大專院校、資訊科技相關團體、商業團體及政府機構。他們提出的主要理由如下：

(a) 許多回應者均表示，白帽黑客及其他網絡安全專業人員在偵測網絡安全威脅及保安漏洞方面所進行的工作，的確有其價值。他們認為，廣泛類別的人士均可受惠於白帽黑客的工作。舉例來說，網絡安全專家的工作可揭示電子服務或產品的潛在保安漏洞或安全缺陷，促進網上消費體驗的安全和公平性。

(b) 白帽黑客入侵若進行得當並受到妥善監管，會令香港受惠，不但可加強本港的網絡安全，亦推動本港網絡安全業界的強勁和穩健發展，從而建立香港作為網絡安全專業服務樞紐的信譽。

(c) 為在未獲授權下取覽訂定免責辯護或豁免，對推動善意的安全研究和促進把新科技引入香港，均至關重要。

反對為網絡安全業界提供特定免責辯護的回應者的意見

2.50 少數回應者（包括三個資訊科技相關團體及一名個別人士）則反對為網絡安全業內人士提供特定免責辯護。某資訊科技相關機構指出，若專為這些經認可人士訂定免責辯護，實際上便會帶來一個*"享有特權的界別"*，當中的行事者不論有何意圖，均可獲豁免刑事法律責任，因此特定的免責辯護或豁免應適用於所有人，而非只適用於經由認可專業團體或認可團體認可的人士。

2.51 另一方面，另一資訊科技界機構則表示，各機構在委託他人提供網絡安全服務（例如網絡掃描）時，通常會訂立書面合約，當中界定網絡安全服務提供者的取覽範圍。故此，可能無須為在未獲授權下取覽訂定特定的免責辯護或豁免。

應否推行認可制度？

2.52 明顯大多數回應者均同意應設立認可制度，當中包括政府部門、資訊科技相關團體及商業機構。這結果與回應者普遍認為適宜為在未獲授權下取覽訂定特定免責辯護或豁免的意見相符。

支持設立認可制度的回應者的意見

2.53 贊成設立認可制度的回應者（包括消費者委員會）指出，認可制度的好處在於能為網絡安全專業人員提供認證機制，若屆時需確定法定免責辯護或豁免是否適用，便能以此輕易識別出這些專業人員。消費者委員會在其回應中有以下提議：

> "……應考慮設立一套設有發牌或認可準則（例如'適當人選'規定及持續進修規定）的法定制度。鑑於認可情況如小組委員會所言不斷演變，認可團體或發牌機構可因應這些變化，發布各種指引、通告及實務守則。就認可制度的行政和運作事宜，應全面徵詢網絡安全業界的意見。"

2.54 與此同時，多個資訊科技相關團體也同意，設立一個認可團體讓網絡安全專業獲得適當認可，會為香港帶來長遠裨益。

2.55 回應者提出了多種認可網絡安全從業員的方式。除上述消費者委員會提議的法定制度外，香港女律師協會有限公司（"**女律師協會**"）認為，可用行政方式在認可團體的規章中列載認可準則，並認為這樣會較易修訂認可準則，以緊貼任何技術要求的變化。另外，

少數資訊科技相關團體則認為可設立網絡安全從業員註冊制度，讓他們在進行滲透測試前自行註冊。

2.56 香港律師會的以下意見也值得一提：香港應否設有認可制度，應屬政府的政策事項。該專業團體指出，需要敲定認可制度的某些運作細節：

> "政府應全面徵詢各持份者和業界的意見……宜考慮例如以下的各種（並非盡列無遺的）問題：若設立一個認可團體，該團體發出的證書可否作為這項控罪的免責辯護？如可以的話，其免責程度有多大？該免責辯護又如何施行？這種基於認證的免責辯護，是否與被告人有權提出的其他免責辯護分開看待？另一方面，即使有認可團體發出的證書，執法機關是否仍可不受其限，調查指稱在未獲授權下作出的取覽？"

2.57 在認可制度的細節方面，我們收到回應者的有用意見。某資訊科技相關團體認為，將予設立的負責監督認可或註冊事宜的機構，應有權在任何個人違反或未能達至有關專業的道德及專業標準的情況下，撤銷該人的註冊，但必須實行正當程序。

2.58 此外，一名有多年網絡安全從業經驗的個別人士表示，可備存一份網絡安全專業人員資料名單，以記錄有關人員的資歷，而該名單應區分不同的網絡安全專業工種。然而，這名回應者有以下告誡：

> "其中部分特殊資訊敏感工種，例如：電子取證調查人員（Forensics and Investigation），密碼（解碼／密碼分析）學家（Cryptanalysis Expert），漏洞研究人員（Zero Day Vulnerability Researcher）等等……的名冊查閱應當受到限制以保護這些人員的人身安全"。

2.59 最後，某商業團體表示，在香港推行的任何認可制度都不應過於複雜，以免窒礙資訊科技行業的發展。

反對設立認可制度的回應者的意見

2.60 儘管大多數對建議 2 作出回應的資訊科技相關團體均同意推行認可制度，其中兩個團體反對這項建議，理由如下：

(a) 無論是科技或是網絡安全專業，兩者都瞬息萬變。服務提供者、軟件公司及網絡安全團體均不時提供經認可的網絡

安全課程。認可制度無法迅速適應變化，以法規為基礎的尤其如此。

(b) 若設立認可制度，很可能會對招聘合資格人才投身香港的資訊科技行業構成挑戰。網絡安全專業人員匱乏，或會無意中限制本港網民所得到的保障。

(c) 開放源碼軟件日漸增多，非保安專業人員用戶都能加以修改或改良，造福社群。若訂有認可方面的規定，可能會限制電腦愛好者在識別潛在網絡安全威脅方面的參與度。

我們的分析及回應

2.61 由於建議 2 的諮詢問題關乎在未獲授權下為網絡安全目的而取覽這項免責辯護或豁免，因此我們會先討論取覽罪的網絡安全免責辯護，然後再探討其他特定免責辯護。

2.62 在諮詢文件中，[41] 小組委員會已參考以下的學術文章說明何謂“網絡安全”，在此複述有其用處：

> “網絡安全又稱為資訊科技安全，指為了保護電腦、網絡及程式免受網絡攻擊或電腦網絡罪行行為（例如病毒、惡意軟件或勒索軟件）損害而採取的各種步驟。”[42]

為經認可的網絡安全從業員提供特定的免責辯護

2.63 在就建議 2 提交意見書的資訊科技團體之中，大多數均樂於接受設立認可制度的建議，理由是此舉能提升資訊科技專業。我們相信，為資訊科技行業內某界定類別的人士訂定特定免責辯護，會是合理而務實的做法。雖然部分回應者可能認為，特定免責辯護會將網絡安全專業人員提升為享有特權的界別，但我們希望指出，該免責辯護實際上使網絡安全專業人員和所有其他人均受制於一套新的規管制度，在該制度下，任何人必須先經認可，才能以可能涉及未獲授權取覽的方式從事網絡安全服務。從這角度來看，該免責辯護事實上是對任何有意在未獲授權下（包括在無法證明有默示授權的情況下）作出取覽的人（包括資訊科技專業人員）施加責任。

---

41 第 2.111 段。

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

2.64 我們建議，經認可的網絡安全從業員如為真正的網絡安全目的而行事，應有特定的免責辯護或豁免。在顧及整體情況後，被告人的目的和行為必須是合理的，亦即施加客觀標準。在下述各段，我們會闡釋所作建議的各項元素背後的理念。

(i) 經認可或持牌網絡安全從業員

2.65 鑑於為網絡安全目的而取覽程式或數據的入侵程度，以及網絡安全目的這寬廣概念，我們認為應只有持牌或經認可的從業員才可為網絡安全目的而作出取覽。這意味着援引上述免責辯護的人士，應同時具備一定水平的專業技能和正直品格。換言之，不是每名自稱網絡安全專業人員或從業員的人士，都可提出為網絡安全目的而取覽這項特定免責辯護。

2.66 由於大多數回應者均支持推行認可制度，因此對參與網絡安全工作的資訊科技業內人士實行制度措施，既可更好地保障所有持份者（即網絡安全專業、有意僱用網絡安全專業服務的人，以至社會大眾），亦能使法律更為明確。故此，我們認為應設有一套獨立的制度，以對網絡安全從業員進行認可，並監督他們的紀律事宜。透過設立認可制度，加上訂定為網絡安全目的而取覽這項特定免責辯護，不但能提升資訊科技行業的專業性，亦會使網絡安全專業人員免於承擔取覽罪的法律責任。

由政府決定認可制度的細節

2.67 儘管如此，我們也意識到本港的網絡安全人才供應短缺，若推行認可制度，可能會造成招聘資訊科技界人才方面的困難，加劇業界競爭，由此推高網絡安全服務的費用。

2.68 我們同意回應者所言，認可制度可透過不同方式落實。舉例來說，可指定由某法定主管當局對網絡安全專業人員進行認可。就此而言，較嚴格的認可制度很可能會影響網絡安全專業人員的供應和收費。相反，或許也可採用較寬鬆的模式，任何人如是聲譽良好的資訊科技專業團體或國際資訊科技協會的成員，即可獲得認可。視乎所採用的模式，認可制度對網絡安全業界和電腦網絡空間用戶的影響會有所不同。

2.69 如何落實認可制度的細節問題，本質上屬政府的政策事宜，故這些細節問題（包括對網絡安全專業人員的認可要求、從業員須遵行的備存紀錄責任、認可團體是由資訊科技行業還是其他主管當局

管理，以及應如何為認可制度提供資金）適宜留待政府決定。為方便政府考慮認可制度，我們已在本報告書對認可建議及它可能造成的影響提出看法。

2.70 我們預計，政府如傾向設立一個網絡安全認可團體，但又無意就此成立一個專責機構的話，或可考慮訂定一個架構，當中指定由一間或多間現有機構（屬自我規管的專業團體及專業協會）履行與香港律師會、香港大律師公會及香港國際公證人協會相類似的職能。香港律師會、香港大律師公會及香港國際公證人協會受託履行法定責任，分別負責監督律師（及外地律師）、大律師及公證人的行為操守，以維持他們的水平。法律執業者若表現未達水平或有違反道德操守的行為，會面臨紀律處分；同樣地，網絡安全專業人員若違反認可團體所公布的任何行為守則，也會面臨紀律處分。

(ii) 真正的網絡安全目的

2.71 我們認為被告人的認可資格或身分，不應是裁定為網絡安全目的而取覽這項特定免責辯護是否適用的決定性因素。經認可人士是為真正的網絡安全目的而取覽程式或數據，才是重點所在。女律師協會及另一商業團體所提出的意見，亦強調這點：

> "儘管我們同意，認可專業團體或認可團體給予的認可，為取覽程式／數據的人有充分理由作出有關取覽提供表面證據，但仍需要審視實際的作為，認可本身並不是充分的免責辯護。為成功確立有關豁免或免責辯護而需要證明的關鍵事項，是未獲授權的取覽是為網絡安全目的而作出，而不是作出該項取覽的人是經認可人士。"

2.72 "真正的網絡安全目的"這規定，意味着經認可的網絡安全從業員如為真正的網絡安全目的而取覽電腦程式或數據，便能以為網絡安全目的而取覽這項特定免責辯護作訴；但從業員如取覽自己女兒電話內的數據，則不能提出相同的免責辯護，反而只能援引"為保障兒童利益而取覽"作為免責辯護，這會在下文第 2.75 至 2.89 段討論。

(iii) 在顧及整體情況後，被告人的行為必須是合理的

2.73 為進一步收緊為網絡安全目的而取覽這項免責辯護的範圍，我們建議在該免責辯護加入"合理性"要求。我們相信，若以合理性作為指導原則，為網絡安全目的而取覽這項特定免責辯護所附帶

的條件便能提供穩妥和一致的規範，以界定一名明理的人所能接受的行為。“合理性”問題與事實極為密切相關。舉例來說，如電腦擁有人或數據擁有人不授權經認可的網絡安全從業員（可能是該擁有人的前僱員或已知的競爭對手）取覽該擁有人的程式或數據，但該從業員仍然作出取覽，則必須就該從業員所作的取覽提出令人信服的解釋或理由，才能令法庭信納該項取覽符合“合理性”要求，從而確立建議的網絡安全免責辯護。若認可團體公布任何道德守則，法庭當然可參考該守則，以評定被告人的行為是否合理。

2.74 這項“合理性”要求也旨在使為網絡安全目的而取覽這項特定免責辯護，與非法干擾電腦數據及非法干擾電腦系統這兩項建議罪行的免責辯護看齊（本報告書第 4 及 5 章會討論後述兩項罪行）。

取覽罪的其他特定的免責辯護

為保障兒童利益而取覽

2.75 在諮詢文件發表後，小組委員會成員出席多次傳媒訪問，期間有人問及家長如查看子女電話內的內容，會否干犯建議的罪行。若沒有訂立關於家長監護的特定免責辯護，被控以建議罪行的家長便只能援引合理辯解這項一般免責辯護。

2.76 在收到的意見書中，本地慈善組織“母親的抉擇”強調兒童在上網時特別容易遇到的危害。這名回應者提到香港大學進行的一項研究，引述年青人遭受多種網絡虐待的情況：香港有四成青少年在非情願的情況下收到網上性裸露內容，每 10 名青少年就有 1 人曾受到網絡性騷擾，每 5 名青少年就有 1 人遭受網絡欺凌。

2.77 這名回應者因此認為，小組委員會應考慮提出立法建議，以*“防止兒童從互聯網、數碼及串流媒體取覽含有不當、侮辱性或有害內容的資訊”*。該回應者再作出以下簡短的評析，認同家長要監督兒童使用互聯網的情況：

> “我們了解到，對於網絡安全及保安這課題，為兒童提供支援的網絡（包括家長、個別人士及專業人員）只具備有限的知識和技能。我們建議，與處於風險的易受傷害兒童有接觸的所有持份者，均應作好裝備並獲賦權力，以預防、應對和舉報網上風險。預防、應對和舉報網上的保護兒童問題，對保障社會上易受傷害人士的安全和福祉至關重要”。

2.78 同樣地，法律援助署也提議應訂有一些豁免，讓家長能為了保障子女利益（例如在發生網絡欺凌的情況下）而取用他們的電腦。

2.79 根據在 1997 年後繼續適用於香港的《聯合國兒童權利公約》（**《兒童權利公約》**）第十六條，兒童享有一般私隱權，[43] 但我們相信，由於兒童容易因為電腦網絡空間上的各種危險而受到傷害，家長確實有充分理由採取行動來保護子女的福祉。在人們頻繁進行網上活動和接通互聯網的現今世界，對育有子女的家長而言，切實可行的行動可能包括取用子女的流動電話或電腦，以找出（比如說）哪些人透過社交平台或通訊應用程式與他們接觸。

2.80 在這方面值得注意的是，以推廣保障及尊重個人資料私隱為使命的個人資料私隱專員公署（“**私隱專員公署**”），也發布了為家長及教師而設的多項建議，讓他們能教導其照顧的兒童在網上保護自己，[44] 其中一項建議就是善用家長監護功能。私隱專員公署指出，有些網上平台或系統提供家長監護功能，讓家長監察或配置適當設定，以免兒童（尤其是年幼兒童）接觸不良內容或人士。此外，私隱專員公署亦認為，家長及教師 *“應警戒兒童，網上通訊有可能會為人身安全帶來危機及造成財物損失”*。[45]

我們的分析

2.81 總結而言，有一點似乎很清楚：家長監護是香港社會所接受的慣常做法，家長在互聯網使用方面的指導角色亦得到大眾認同。我們認為，為了達到保護兒童的目的，新訂的電腦網絡罪行法例把“為保障某年齡以下兒童的利益而取覽”明文豁除於取覽罪之外，會是明智之舉。我們理解到，這項特定免責辯護可能會削弱兒童的私隱權，但鑑於年幼兒童的互聯網滲透率甚高，我們認為訂有此免責辯護會符合保障兒童利益的原則。

---

43 見香港特別行政區政府政制及內地事務局於 2009 年 3 月發布的小冊子，第 3 頁。《兒童權利公約》第十六條第一款有以下規定：*“兒童的隱私……或通信不受任意或非法干涉……”*。

44 個人資料私隱專員公署，《兒童網上私隱——給家長及老師的建議》（2015 年），登載於 https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/leaflet_childrenonlineprivacy_c.pdf（於 2025 年 11 月 1 日瀏覽）。

45 同上。

兒童的年齡

2.82 根據本港法例，16 歲以下的人，在香港法律上一般不能對性接觸給予同意。[46] 由於《兒童權利公約》第一條把“兒童”界定為 18 歲以下的任何人，因此我們曾考慮就電腦網絡罪行而言，是否需要把這項特定免責辯護的兒童年齡上限定為 18 歲。我們認為，相較於對個人身體的自主權，私隱權屬較次要的權利。由於本港法例確定了 16 歲以下的人對自己的身體並沒有自主權(即 16 歲以下的人不能對性接觸給予有效的同意)，因此就電腦網絡罪行而言，似乎沒有充分理由為取覽罪的這項特定免責辯護訂定不同的年齡上限。總結而言，我們認為把年齡上限定為 16 歲既能夠提供足夠保障，亦與香港的其他現有法例大體上相符。

對程式或數據的取覽應屬合理

2.83 我們認為，如果把對程式或數據的取覽，限於在顧及案件的整體情況後為保障兒童利益而合理所需者，便可避免這項特定的免責辯護被濫用，這項合理性要求無異於為網絡安全目的而取覽的免責辯護。在取覽的目的和程度均受限制的情況下，法庭會有更大空間審視證據，以裁定某項取覽是否超乎適度。法庭最終會在考慮個別案件的所有相關因素後評估被告人的行為，以確保被告人沒有逾越對兒童行使管教方面所應有的行為界限。

有關免責辯護的範圍

2.84 我們已詳細考慮這項建議的免責辯護的兩個制定方案。方案一的涵蓋範圍較廣，適用於為保障兒童利益而取覽程式或數據；方案二的涵蓋範圍則較窄，只限於為防止兒童受到身體、情緒或心理傷害而取覽程式或數據。

(i) 為保障兒童利益而取覽程式或數據

2.85 支持訂定這種較廣闊免責辯護的主要論據，是家長可能在多種情況下有意取覽兒童的程式或數據(例如為了確定兒童是否曾取覽網上的色情或暴力資訊)，較廣闊的免責辯護能夠將這些情況涵蓋

---

[46] 例如，根據《刑事罪行條例》第 122(2)條，年齡在 16 歲以下的人，在法律上是不能給予同意，使某項作為不構成猥褻侵犯的。就性交而言，根據《刑事罪行條例》第 124(1)條，與年齡在 16 歲以下的女童非法性交，即屬犯罪。此外，《刑事罪行條例》第 146(1)條亦訂明，與或向年齡在 16 歲以下的兒童作出嚴重猥褻作為，或煽惑年齡在 16 歲以下的兒童與另一人或向另一人作出此種作為，即屬犯罪。根據第 146(2)條，即使被控人證明該兒童同意作出該項嚴重猥褻作為，亦不得以此作為免責辯護。

在內。若訂定具限制性的免責辯護，則可能令家長感到被剝奪父母權利，因為電腦網絡罪行法例會禁止他們做某些在教養子女的過程中原本可做的事情。由於訂有取覽須屬合理的要求，贊成訂定這種較廣闊免責辯護的人相信，法庭不但會考慮到家長主觀相信有必要為保障兒童利益而作出取覽，也會客觀評估家長的行為，以裁定有關取覽是否有理可據。這樣能限制對兒童的程式或數據的取覽範圍，從而防止家長過度侵犯兒童的私隱權。

(ii) 為防止兒童受到身體、情緒或心理傷害而取覽程式或數據

2.86 另一方面，我們也理解到，鑑於其他實際考慮因素，範圍較窄的免責辯護可能較為合宜。廣闊的免責辯護或會對親子關係造成不良影響，有損家庭和睦。就父母已經離婚的情況而言，相對狹隘的免責辯護也許能防止其中一方操控子女，使他們投訴尋求對自己行使父母責任或管教的另一方。此外，私隱權亦正獲得前所未有的重視。為了對兒童的私隱給予更多尊重，作為折衷做法，便不得不削弱或約束其他對立權利（例如透過取覽子女的電腦程式或數據來行使父母管教的權利）。

2.87 最終，小組委員會稍微佔多的成員屬意採用涵蓋範圍較廣的方案一，即為保障兒童利益而取覽程式或數據。由於政府若決定落實小組委員會這項建議，可進一步徵詢公眾意見，加上新訂的電腦網絡罪行法例的內容會由立法機關作最終決定，因此我們認為，這議題最好由政府在考慮社會意見後再作定奪。

有關免責辯護不應取決於取覽者與取覽對象的關係

2.88 為了體現這項免責辯護背後保障兒童利益的理念，我們進一步建議這項免責辯護是否成立，應視乎尋求取覽兒童的程式或數據的人的主觀目的而定。事與願違的是，實際上兒童並不一定能在安全穩妥的環境中得到適切保護。家長或監護人忽略履行或沒有履行自己保護或照顧兒童福祉的責任，並不鮮見。我們亦想像到，即使某兒童得到家長或監護人的適切照顧，現實中仍可能出現多種情況，需要陌生人介入來保障該兒童的利益。舉例來說，若有人發現某兒童境況堪憂（例如兒童迷路），容許該人取覽有關兒童的電話或電子器材內的程式或數據而無須負上刑事法律責任，似乎是合理的做法。

2.89　上述的考慮因素正好證明，支持在未獲授權下取覽兒童的程式或數據的充分理據，在於某人為達至保障兒童利益此真實目的而在未獲授權下取覽有關程式或數據，而非該人與該兒童的關係。如這項免責辯護並不取決於兒童與取覽者的關係，便可為兒童利益提供最大保障。我們認為，“為保障而合理所需”這項凌駕性規定能夠避免濫用。

把有關免責辯護延伸至保護易受傷害人士

2.90　由於精神上無能力的成年人可能容易遭受剝削，因此我們認為，上述在未獲授權下取覽程式或數據的特定免責辯護應延伸至保護易受傷害人士。至於應如何界定易受傷害人士，我們認為宜參考《精神健康條例》（第 136 章）（**《精神健康條例》**）對 *“精神紊亂的人”*[47] 及 *“弱智人士”*[48] 所作的清晰定義。根據《精神健康條例》第 2 條：

(a) *“精神紊亂”*界定為 *“精神病”*，*“屬智力及社交能力的顯著減損的心智發育停頓或不完全的狀態，而該狀態是與有關的人的異常侵略性或極不負責任的行為有關連的”*，*“精神病理障礙”*，[49] 或 *“不屬弱智的任何其他精神失常或精神上無能力”*，而 *“精神紊亂”*當用作形容詞時亦須據此解釋；及

(b) *“弱智”*指 *“低於平均的一般智能並帶有適應行為上的缺陷”*，而 *“弱智”*當用作形容詞時亦須據此解釋。第 2 條進一步把 *“低於平均的一般智能”*界定為 *“按照魏克斯勒兒童智力測量表或按照任何標準化智力測驗中的同等智力測量表是 70 或低於 70 的智商”*。

2.91　如有需要，法庭在個別案件中裁定是否已在所需的舉證標準下證明前段所引定義的構成元素時，會借助從註冊醫生或精神科醫生等所獲得的專家證據。故此我們建議，上述在未獲授權下取覽程式或數據的特定免責辯護應延伸至保障易受傷害人士（即《精神健康條例》所界定的精神紊亂的人或弱智人士）的利益。[50] 這項建議也進一步

47　根據《精神健康條例》第 2 條，*“精神紊亂的人”*指 *“任何患有精神紊亂的人”*。

48　根據《精神健康條例》第 2 條，*“弱智人士”*指 *“弱智的人或看來屬弱智的人”*。

49　*“精神病理障礙”*界定為 *“長期的性格失常或性格上無能力（不論是否兼有顯著的智力減損），導致有關的人有異常侵略性或極不負責任的行為”*。

50　這與法改會在 2019 年 12 月發表的《檢討實質的性罪行》報告書的最終建議 35 相符。該項建議提出，新訂的涉及精神缺損人士的罪行，應適用於精神紊亂的人或弱智人士（如《精神健康條例》所界定者），而其精神紊亂或弱智（視屬何情況而定）的性質或程度令他或她沒有能力保護自己免受性剝削。

鞏固我們上文得出的結論，即有關免責辯護不應取決於取覽者與取覽對象的關係。一如保護兒童的情況，“為保障而合理所需”這項規定亦同樣適用。

為真正的研究目的而取覽

2.92 對諮詢文件作出回應的多個資訊科技相關團體均提議，取覽程式或數據如是為了在受控環境中進行研究、分析或測試自己擁有的器材或目標，應獲得豁免。

2.93 我們同意，除了為網絡安全目的而取覽這項免責辯護外，“為研究目的而取覽程式或數據”（例如研究人員或網絡安全從業員為了確定在香港未受保護的電腦數目而作出取覽）也應訂為免責辯護或豁免。由於這些研究或許能得出有用的分析或資訊，因此提供“為研究目的而取覽程式或數據”這項特定免責辯護，屬合理之舉。我們認為，《防止兒童色情物品條例》（第 579 章）第 4(2)(a)及(3)(a)條就各項關於兒童色情物品的罪行所訂的免責辯護可用作藍本，把上述建議的免責辯護制定為“為真正的教育、科學或研究目的而取覽程式或數據”。

2.94 為免這項研究免責辯護被濫用，我們建議，該免責辯護應訂有以下要求：取覽須屬合理，而該取覽不得超過為達到有關教育、科學或研究目的而所需者。這項“合理性”要求會作為客觀準則，用以裁定被告人的取覽是否適度或合理。

《刑事罪行條例》第 64(2)條所訂、關於非法干擾電腦數據罪及非法干擾電腦系統罪的免責辯護

2.95 現行《刑事罪行條例》第 64(2)條所訂的兩項免責辯護，均適用於諮詢文件建議 6 及 7 所述的非法干擾電腦數據罪及非法干擾電腦系統罪（“**干擾罪**”），這會在本報告書第 4 及 5 章討論。由於第 64(2)條目前適用於刑事損壞罪，而上述兩項干擾罪又建議以該罪行為藍本，因此宜先簡述第 64(2)條所訂的兩項免責辯護。

2.96 第 64(2)條由兩部分組成。任何被告人被控以刑事損壞罪，在下述情況下均須被視為有合法辯解：

(a) 如指稱構成該罪行的作為作出時，被告人相信，他相信有權同意有關財產的摧毀或損壞的人已予同意，或相信該人如知道有關財產的摧毀或損壞及有關情形亦會予以同意（“**同意免責辯護**”）；或

(b) 如被告人摧毀或損壞有關財產或威脅會如此做，或（在被控以第 62 條所訂罪行時）意圖使用或導致或准許使用某些物品以摧毀或損壞有關財產，而他如此做是為了保護財產（不論屬於其本人或另一人），且於指稱構成該罪行的作為作出時，被告人相信——

(i) 該財產需即時保護；及

(ii) 在顧及一切有關情況後，所採用或打算採用的保護方法是或會是合理的（“**保護財產免責辯護**”）。

2.97 由於干擾電腦數據及／或干擾電腦系統通常只會在取覽程式或數據後發生，因此我們認為，《刑事罪行條例》所訂的同意免責辯護及保護財產免責辯護，應同樣適用於取覽罪。

第 64(2)(a)條所訂的同意免責辯護

2.98 為了闡釋這項免責辯護，我們現假設以下情境：被告人在登入另一人的電腦後更改了當中的數據（例如病毒），並相信該另一人會對有關更改予以同意。若這名被告人因可提出同意免責辯護而無須負上非法干擾電腦數據的法律責任，但卻被裁定犯取覽罪的話，這樣的推論顯然有悖邏輯。故此我們認為，取覽罪及干擾罪的免責辯護應採用統一的處理方式。有關免責辯護條文的詳細草擬工作可在立法階段處理。

第 64(2)(b)條所訂的保護財產免責辯護

2.99 同樣地，由於可就干擾罪提出保護財產免責辯護，故我們認為被告人也應可就取覽罪以相同的免責辯護理由作訴。

加入合理性要求，訂明被告人須合理地相信有關事情

2.100 根據現行第 64(2)(a)條，被告人相信存有同意是完全主觀的。《刑事罪行條例》第 64(3)條訂明，*“只要是誠實地相信有關事情，則是否有充分理由支持，不具關鍵性”*。故此，只要法庭接納被告人是真確相信有關事情，有關免責辯護便會適用，被告人所相信的事情無須有合理依據支持。

2.101 將第 64(2)條所訂的免責辯護改列於新法例時，我們建議提高有關免責辯護的門檻，在同意免責辯護及保護財產免責辯護加入客觀驗證標準：

(a) 就同意免責辯護而言，被告人必須合理地相信自己已獲同意或會獲同意取覽有關程式或數據；及

(b) 就保護財產免責辯護而言，被告人必須合理地相信有關財產需即時保護。

2.102 換言之，我們建議在針對電腦網絡罪行的特定法例加入取覽罪，而《刑事罪行條例》第 64(3)條不適用於該罪行。上述調整會使同意免責辯護及保護財產免責辯護，與我們在上文就取覽罪所建議的其他特定免責辯護看齊，即所有免責辯護均採用“合理性”要求，以確保一致。我們相信這種處理方法可避免各項免責辯護被濫用，並體現我們的指導原則：一方面平衡兼顧網民的權利和資訊科技業內人士的權益，另一方面亦保障公眾在使用電腦系統時免受騷擾或攻擊的權益和權利。

非保安專業人員取覽程式或數據

2.103 諮詢文件的建議 2(b)及 8(b)分別邀請公眾對以下問題提出意見：非保安專業人員取覽程式或數據及干擾電腦系統，應否有任何免責辯護或合法辯解。有關非保安專業人員的例子包括：由機械人進行網頁抓取（web scraping）或由互聯網資訊收集工具（例如搜尋器）啟動網絡爬蟲（web crawlers），從而在未獲授權下從伺服器收集數據；以及為找出保安漏洞或確保應用程式界面（Application Programming Interface）安全和完整而掃描服務供應商的系統。[51]

2.104 正如我們將在本報告書第 5 章解釋，[52] 我們認為無須就電腦網絡空間日常運作中所遇到的非保安代理提供特定的免責辯護，原因是人們在使用電腦網絡空間時普遍接受的做法，如它們是以電腦用戶通常接受的規模進行的，均會根據默示授權的原則而獲准。同樣道理，我們認為無須就取覽罪為非保安專業人員建議訂定特定的免責辯護。

有關建議 2 的結論

2.105 總結上述討論，我們建議就取覽罪訂定各免責辯護如下：

---

51 見諮詢文件建議 8(b)。

52 第 5.29 至 5.33 段。

最終建議 2

就建議的非法取覽程式或數據罪而言，我們建議除合理辯解可作為法定免責辯護外：

(a) 在未獲授權下為網絡安全目的而取覽，應有特定的免責辯護，但須符合以下條件：

(i) 被告人必須是經認可的網絡安全從業員（認可制度的細節本質上屬政策事項，最好留待政府考慮）；

(ii) 被告人必須為真正的網絡安全目的而行事；及

(iii) 在顧及整體情況後，被告人的行為必須是合理的。

(b) 在未獲授權下為保障 **16** 歲以下兒童及易受傷害人士（即《精神健康條例》（第 **136** 章）所界定的精神紊亂的人或弱智人士）的利益而取覽，應有特定的免責辯護：

(i) 這項免責辯護建基於取覽兒童或易受傷害人士的程式或數據的人的主觀目的（即為了保障有關兒童或易受傷害人士的利益），而非該人與有關兒童或易受傷害人士的關係。

(ii) 在顧及整體情況後，被告人對程式或數據的取覽必須是合理的。

(c) 在未獲授權下為教育、科學或研究目的而取覽，應有特定的免責辯護。在顧及整體情況後，被告人對程式或數據的取覽必須是合理的。

(d) 《刑事罪行條例》（第 200 章）第 64(2)條所訂的關於非法干擾電腦數據罪及非法干擾電腦系統罪的免責辯護，也應可就非法取覽程式或數據罪而提出。

(i) 第 64(2)條所訂的兩項免責辯護涵蓋以下情況：

(1) 被告人在取覽程式或數據時，相信其作為已獲同意或會獲同意；或

(2) 被告人在取覽程式或數據時，相信有關財產需即時保護，並相信在顧及整體情況後，所採用的保護方法是合理的。

(ii) 被告人不論是提出同意免責辯護或保護財產免責辯護，均必須合理地相信該免責辯護所訂的有關事宜。

對小組委員會建議 3 的回應

簡易程序案件的時效期

2.106 建議 3 處理適用於循簡易程序就諮詢文件所建議的五類依賴電腦網絡罪行提出檢控的時效期：

> "小組委員會建議，儘管有《裁判官條例》（第 227 章）第 26 條的規定，適用於循簡易程序就任何建議罪行提出檢控的時效期，應為發現就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）後的兩年。"

2.107 根據《裁判官條例》（第 227 章）（**《裁判官條例》**）第 26 條，簡易程序罪行的時效期一般為所涉事項發生後起計的六個月，但如有關法例另有規定則除外。

2.108　大多數回應者均支持建議 3。某商會表示，電腦網絡罪行案件往往相當複雜，控方需耗用較多資源和時間來決定應否繼續檢控某宗案件。不過該商會也告誡，兩年的時效期應視為用作應付較複雜案件的安全網，而不應視為通常所需的時間。然而，數名回應者不贊成把時效期從六個月“延遲”至兩年，理由是六個月的期限可鼓勵執法機關加快處理電腦網絡罪行案件，因而能更好地保障公眾利益。

2.109　正如小組委員會在諮詢文件解釋，[53]《裁判官條例》所訂的預設時效期或不足以調查電腦網絡罪行案件。受害人可能在案件發生後兩至三個月才向警方報案，而更甚者，六個月的時效期在事件被揭發時已屆滿。警方從互聯網服務提供者取得日誌紀錄，可能再需要兩至三個月。分析這些日誌紀錄可能又另需兩至三個月，還須顧及達至檢控決定所需的額外時間。

2.110　我們希望澄清一點，建議 3 僅旨在把時效期延長至兩年，以確保即使由於本身涉及的難題，以致有關指稱罪行的調查按理不能在預設的六個月期限內完成，隨後提出檢控的時限也不會屆滿，而非因為我們不相信執法機關能在公平情況下盡速處理電腦網絡罪行案件。因此，我們建議保留建議 3。

最終建議 3

我們建議，儘管有《裁判官條例》（第 227 章）第 26 條的規定，適用於循簡易程序就任何建議罪行提出檢控的時效期，應為發現就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）後的兩年。

[53]　第 2.122 段。

第 3 章　非法截取電腦數據

引言

3.1　本章討論關於諮詢文件建議 4 及 5 的回應。建議 4 建議訂立第二類依賴電腦網絡的罪行，即非法截取電腦數據：

> "小組委員會建議：
>
> (a) 為不誠實或犯罪目的而在未獲授權下截取、披露或使用電腦數據，應在新法例下定為罪行。
>
> (b) 建議的罪行應：
>
> (i) 保障一般通訊，而並非只保障私人通訊；
>
> (ii) 一般適用於數據（不論有關數據是否元數據）；及
>
> (iii) 適用於截取在傳送人一端前往傳送對象一端途中的數據，即傳送中的數據及在傳送期間暫時靜止的數據。
>
> (c) 除上述另有規定外，建議的條文應以《電腦罪行及電腦相關罪行示範法》（Model Law on Computer and Computer Related Crime）〔（**《示範法》**）〕第 8 條為藍本，包括犯罪意念（即"蓄意"截取）。"

3.2　正如諮詢文件所解釋，[1] 在所有經研究司法管轄區的相關法規當中，就作為香港的參考對象而言，按下文所述修改的《示範法》第 8 條（*"非法截取數據等"*）與小組委員會的構思最為相近：

> "任何人如為不誠實或犯罪目的而在無合法辯解或權限的情況下，蓄意以技術截取：
>
> (a) 任何往來某電腦系統或在某電腦系統內的傳送；或

[1] 第 3.111 及 3.112 段。

(b) 來自某電腦系統並載有電腦數據的電磁發射；[2]

即屬犯罪，一經定罪，可處為期不超過〔刑期〕的監禁或不超過〔金額〕的罰款，或兩者兼處。”

3.3 概括而言，非法截取電腦數據罪旨在：[3]

(a) 把類似傳統竊聽和記錄電話對話，而並非依照法律權限（例如在執法時）進行的電腦數據截取定為不合法；及

(b) 從而保障人們的數據通訊私隱權。

3.4 在現今世界，即使無需特別設備或先進資訊科技知識，截取電腦數據也可以隨處發生。[4] 例如，某人惡意設置虛假 Wi-Fi 熱點，以獲取受害人已連接的器材所傳送的數據，可謂易如反掌。更精密的截取數據方式，則可能涉及設置“後門程式”[5] 或安裝間諜軟件。

香港的現行法律

3.5 由於部分回應者的意見書就現有法律的不足之處提出意見，因此我們宜先扼要重述現行法定機制的主要特點，然後再處理這些回應。

《截取通訊及監察條例》（第 589 章）

3.6 正如小組委員會在諮詢文件解釋，[6]《截取通訊及監察條例》着眼於規管執法機構（即公職人員）何時和如何可合法侵犯某人的私人通訊權利，例如藉着就擬進行的截取通訊或擬進行的秘密監察取得“訂明授權”而侵犯該權利。[7] 另外，《截取通訊及監察條例》只規管截取在傳送過程中的通訊。[8]

---

2 《示範法》中“電腦數據”的定義似乎與我們的建議一致，即建議的罪行應一般適用於數據（包括元數據），而非只限於構成私人通訊的數據：
“‘電腦數據’指任何對事實、資料或概念的表述，而該表述的形式適合電腦系統處理，電腦數據包括適合用於致使電腦系統執行功能的程式”。

3 諮詢文件第 3.1 段。

4 數據經不同器材傳送期間會留下足跡，這些器材甚至會保留數據的複本。控制任何這些器材的人或許能夠分析傳送的數據。

5 後門程式是*“獲授權用戶及未獲授權用戶能藉以繞過正常保安措施，從而按高用戶級別取用或取覽某電腦系統、網絡或應用軟件的任何方法。”*見 https://www.malwarebytes.com/backdoor（於 2025 年 11 月 1 日瀏覽）。

6 第 3.7 及 3.9 段。

7 《截取通訊及監察條例》（第 589 章）第 2 條。

8 見《截取通訊及監察條例》第 2(1)條對“截取作為”的定義。

《電訊條例》（第 106 章）第 27(b)條

3.7 在執法情況以外，則有《電訊條例》第 27 條下述規定：

> "任何人損壞、移走或以任何方式干擾電訊裝置，而意圖是——
>
> (a) 阻止或妨礙任何訊息的傳送或傳遞；或
>
> (b) 截取或找出任何訊息的內容，
>
> 即屬犯罪，一經循簡易程序定罪，可處第 4 級罰款及監禁 2 年。"

3.8 正如小組委員會在諮詢文件指出，[9] 第 27(b)條並非針對截取電腦數據的特定條文。該條文預設電訊背景，並不完全適用於電腦網絡空間。此外，根據第 27(b)條，擬截取的目標只限於 *"任何訊息的內容"*，這句顯然並不涵蓋元數據（即提供其他數據相關資料的數據）。

對小組委員會建議 4 的概括回應

支持建議 4 的回應者的意見

3.9 在明確表達立場的回應者當中，明顯大多數均支持建議 4。表示贊同的回應者包括法律專業團體、資訊科技相關團體、大專院校、商業團體及政府部門。

3.10 小組委員會收到的正面回應當中，個人資料私隱專員公署（"**私隱專員公署**"）表示，訂立為不誠實或犯罪目的而在未獲授權下截取電腦數據這項罪行，會 *"有助遏止愈趨常見的資料外洩事故"*。基於這項截取罪的政策原意是 *"保障人們的數據通訊私隱權"*，私隱專員公署支持引入這項罪行。

3.11 香港與內地法律專業聯合會有限公司亦支持建議的罪行，並且同意上文第 3.8 段小組委員會對《電訊條例》第 27 條的局限所作出的分析。該會更提到，違反《電訊條例》第 27 條的最高刑罰頗輕，只是第 4 級罰款（25,000 元）[10] 及監禁 2 年。

---

9 第 3.14 段。

10 《刑事訴訟程序條例》（第 221 章）附表 8。

3.12 其他回應者——資訊科技相關團體及個別人士——亦贊成引入在未獲授權下截取電腦數據罪，但強調加入“犯罪目的”或“犯罪意圖”作為罪行構成元素這點至為重要。

反對建議 4 的回應者的意見

3.13 只有一個資訊科技相關團體反對擴大電腦罪行的範圍。該回應者憂慮建議的截取罪會對網絡安全從業員進行的合法作為（例如，網絡入侵偵測及滲透測試可能涉及截取電腦數據）帶來潛在不確定性，並認為即使被告人享有免責辯護，控方仍須負證明被告人意圖的舉證責任。

對小組委員會建議 4 的詳細回應

截取罪的範圍

3.14 關於諮詢文件建議 4(a)，私隱專員公署表示，“披露”和“使用”電腦數據顯然構成不同的刑事作為，與“截取”有所區別。私隱專員公署繼而作出以下提議：

> “如政策原意是立法禁止披露或使用由先前截取作為而獲得的電腦數據，我們提議應在法例內清楚述明，否則新訂罪行的管轄範圍可能涵蓋披露或使用並非由截取而獲得的電腦數據。”

截取罪與《個人資料（私隱）條例》（第 486 章）（《私隱條例》）現有的“起底”罪行是否互相重疊

3.15 私隱專員公署亦提述《私隱條例》第 64(1)[11]、(3A)[12] 及(3C)[13]條，該等條文訂立有關“起底”的刑事罪行。私隱專員公署指出，

---

11 《私隱條例》第 64(1)條規定，*“任何人披露未經資料使用者同意而取自該資料使用者的某資料當事人的任何個人資料，而該項披露是出於以下意圖的，該人即屬犯罪——*
(a) 獲取金錢得益或其他財產得益，不論是為了令該人或另一人受惠而獲取；或
(b) 導致該當事人蒙受金錢損失或其他財產損失。”（底線後加）

12 《私隱條例》第 64(3A)條規定，*“如任何人（披露者）在未獲資料當事人的相關同意下，披露該當事人的個人資料，而——*
(a) 披露者的意圖，是導致該當事人或其任何家人蒙受任何指明傷害；或
(b) 披露者罔顧是否會（或相當可能會）導致該當事人或其任何家人蒙受任何指明傷害，披露者即屬犯罪。”（底線後加）
指明傷害指對某人的滋擾、騷擾、纏擾、威脅或恐嚇、身體傷害或心理傷害；導致某人合理地擔心其安全或福祉的傷害；或某人的財產受損（見第 64(6)條）。

13 《私隱條例》第 64(3C)條規定，*“如——*
(a) 任何人（披露者）在未獲資料當事人的相關同意下，披露該當事人的個人資料，而——

建議的非法截取電腦數據罪與現有的“起底”罪行對犯罪意念的規定明顯有別。不過，私隱專員公署認為，視乎個別案件的案情及證據，相關的個人資料披露可能同時構成建議的截取罪及《私隱條例》所訂罪行。

“為不誠實或犯罪目的”這項元素是否充分或適當

3.16 香港女律師協會有限公司（“**女律師協會**”）贊成建議 4，並表達以下意見：

> “應考慮是否亦應把任何不當目的包括在內，例如是否有披露個人或保密資料，而有關披露可能既不構成罪行，亦不涉及‘財務上不誠實’此涵義中的不誠實”。

3.17 不過，該回應者並無提出任何實質例子，以說明有何構成罪責的電腦數據截取可能不符合建議 4 所訂的 *“不誠實或犯罪目的”* 這個門檻。

3.18 此外，某資訊科技相關團體關注到，防毒解決方案提供者及其他互聯網保安公司等科技保安公司或會監察網絡，以找出攻擊訊號或分析網絡通訊。該回應者解釋，這些活動的性質或會顯示出截取電腦數據的特徵，但這些活動不一定針對任何特定組織，並認為只有截取電腦數據的作為關乎向一個或多個特定目標發動攻擊，才應屬犯罪。

3.19 另一方面，另一個資訊科技相關團體認為，*“不誠實或犯罪目的”* 這項規定足以保障網上服務提供者的正常運作，並同意所需犯罪意念應如建議 4(a)所述，即為 *“不誠實或犯罪目的”* 而截取。

行使執法權力的公職人員的刑事法律責任

3.20 對於公職人員（例如執法機關成員）在超逾其權限範圍的情況下截取或取覽電腦數據須負上的法律責任，某政府部門要求釐清小組委員會在這方面的立場。該回應者提出：

(i) 披露者的意圖，是導致該當事人或其任何家人蒙受任何指明傷害；或

(ii) 披露者罔顧是否會（或相當可能會）導致該當事人或其任何家人蒙受任何指明傷害；及

(b) 該項披露導致該當事人或其任何家人蒙受任何指明傷害，

披露者即屬犯罪。”（底線後加）

"在某些情況下，或會有公職人員真誠行事，卻不慎超逾其獲授執法權力的權限……在這些情況下，公職人員無須負刑事法律責任，才是符合重大公眾利益的做法，否則公職人員或會傾向採取過分規避風險的執法態度……"

"超逾權限"的截取

3.21 兩個專業團體(即女律師協會及香港女工商及專業人員聯會〔"**女工商專聯**"〕)提議，在未獲授權下截取，應包括超逾權限的截取作為。就此，女律師協會特別建議採納美利堅合眾國("**美國**")《儲存通訊法案》(Stored Communications Act)所載有關"超逾"授權範圍的概念。

3.22 正如諮詢文件所提及，[14]《儲存通訊法案》的主要條文是《美國法典》第 18 篇第 2701(a)條：

"除本條(c)款另有規定外，任何人如——

(1) 在未獲授權下蓄意取用藉以提供電子通訊服務的設施；或

(2) 蓄意超逾授權範圍而取用該設施；

從而在有線或電子通訊以電子方式儲存於有關系統內期間，取得或更改該等通訊，或阻止對該等通訊的獲授權取覽，則須按照本條(b)款的規定懲處。"

(底線後加)

截取罪應否只保障私人通訊

3.23 關於建議 4(b)(i)，某資訊科技相關團體表示，建議的截取罪應只保障私人通訊。該團體認為，*"以電腦網絡世界而言，一般通訊屬過於廣泛"*，建議的罪行擬為公眾提供的保障*"或會不必要地擾亂正當通訊"*。

---

14 第 3.87 段。

應否界定何謂“截取”

3.24 正如第 2 章提到，[15] 部分商業團體認為應清晰界定或向公眾解釋若干概念（包括“截取”及“取用或取覽”）的涵義。他們憂慮隨着科技發展，這些概念或會有所重疊和不斷演變。

我們的分析及回應

重訂截取罪的焦點

3.25 在諮詢文件中，[16] 小組委員會解釋擬禁止在未獲授權下披露或使用“截取的數據”，原因在於其後披露或使用截取的數據，可能會引起私隱方面的關注及其他潛在問題（例如在電子商貿交易中，倘若信用卡資料在傳送至賣方期間被截取作不當用途，持有人可能會蒙受財務損失）。

3.26 正如上文第 3.14 段所述，私隱專員公署就建議的非法截取電腦數據罪的涵蓋範圍提出疑問。就此，我們審慎檢視該項罪行的應用情況。我們認為，若罪行是基於為不誠實或犯罪目的而在未獲授權下披露或使用“任何數據”（不限於截取的數據），則未免過於廣泛，因為這項罪行實質上會適用於我們日常數碼生活中接觸到的各類數據。

3.27 此外，在未獲授權下披露或使用電腦數據的罪行，只要涉及個人資料，就更當屬私隱專員公署檢視的範疇。我們注意到，最近一次在 2021 年的立法修訂工作中，[17] 私隱專員公署特別聚焦於“起底”罪行，務求遏止在未獲同意下披露個人資料。[18] 《私隱條例》第 64(3A)[19] 及(3C)[20] 條的罪行，均規定須有意圖導致指明傷害，或

---

15 上文第 2.17 段。

16 第 3.92 及 3.94 段。

17 透過制定《2021 年個人資料（私隱）（修訂）條例》（2021 年第 32 號條例），在《個人資料（私隱）條例》（第 486 章）加入有關“起底”的條文。

18 見《2021 年個人資料（私隱）（修訂）條例》的詳題。

19 《私隱條例》第 64(3A)條規定，*“如任何人（披露者）在未獲資料當事人的相關同意下，披露該當事人的個人資料，而——*
(a) 披露者的意圖，是導致該當事人或其任何家人蒙受任何指明傷害；或
(b) 披露者罔顧是否會（或相當可能會）導致該當事人或其任何家人蒙受任何指明傷害，
披露者即屬犯罪。”（底線後加）
指明傷害指對某人的滋擾、騷擾、纏擾、威脅或恐嚇、身體傷害或心理傷害；導致某人合理地擔心其安全或福祉的傷害；或某人的財產受損（見第 64(6)條）。
根據第 64(3B)條，最高刑罰為第 6 級罰款（即 100,000 元）及監禁兩年。

20 《私隱條例》第 64(3C)條規定，*“如——*
(a) 任何人（披露者）在未獲資料當事人的相關同意下，披露該當事人的個人資料，而——

罔顧是否會導致指明傷害。正如私隱專員公署在意見書內適切指出，“起底”罪行的犯罪意念非常局限於特定範圍。

3.28 鑑於在未獲授權下披露或使用電腦數據這項一般罪行影響甚廣，為審慎起見，我們應先在研究的第二部分[21] 深入探討這議題，然後才就應否建議訂立這方面的新罪行（以及如應該的話，如何訂立）發表任何確定意見。例如，可進一步斟酌該項罪行應否局限於“截取的數據”，因為有人或會認為，某人如 *“為不誠實或犯罪目的”* 而披露或使用電腦數據，該項行為本身便應構成罪責，不論有關數據是在獲授權下截取而獲得，或是在未獲授權下截取（或以任何其他方式）而獲得。另外，該項罪行與《私隱條例》“起底”罪行之間的相互影響，或許亦值得再加考慮。

3.29 對於私隱專員公署認為在未獲授權下披露或使用電腦數據罪與“起底”罪行或有重疊，考慮到我們建議的方案，這是我們現階段的回應。不過，我們順帶補充，建議的截取罪針對在未獲授權下“截取”一般電腦數據，雖然須證明有不誠實或犯罪目的，但該截取罪並非基於導致傷害。就此而言，截取罪與《私隱條例》的“起底”罪行可清楚區分開來。

“為不誠實或犯罪目的”這項規定適當

3.30 我們認為，某目的是否“不當”，可以是個視乎詮釋而定的主觀問題。相反，要判斷某目的是否 *“不誠實或犯罪”*，則存在客觀標準。例如，*R v Ghosh* 釐定了不誠實驗證標準，[22] 而該案仍然是香港遵循的主導案例。[23] 至於“犯罪目的”，在大多數案件中，某作為是

(i) 披露者的意圖，是導致該當事人或其任何家人蒙受任何指明傷害；或

(ii) 披露者罔顧是否會（或相當可能會）導致該當事人或其任何家人蒙受任何指明傷害；及

(b) 該項披露導致該當事人或其任何家人蒙受任何指明傷害，

披露者即屬犯罪。”（底線後加）

根據第 64(3D)條，最高刑罰為罰款 1,000,000 元及監禁五年。

21 第二部分的範圍適時再作討論，該部分會涵蓋借助電腦網絡的罪行，即通過使用電腦、電腦網絡或其他形式的資訊及通訊科技，使犯罪規模或範圍得以擴大的傳統罪行。見導言第 8 段。

22 [1982] QB 1053。根據 *Ghosh* 案的驗證標準，陪審團必須首先根據明理且誠實的人的一般標準，決定有關行為是否不誠實。假如有關行為屬於不誠實，則陪審團必須進而考慮，被告人本人是否必定已認知其行為按該等標準衡量屬於不誠實。

23 就不誠實驗證標準而言，*Ghosh* 案的驗證標準現時仍然是香港的有效法律，但因應英國最高法院就一宗民事申索案件（即 *Ivey v Genting Casinos (UK) Ltd (trading as Crockfords Club)* [2018] AC 391, [2017] 3 WLR 1212）作出決定之後，英格蘭及威爾斯上訴法院在 *R v Barton* [2021] QB 685, [2020] 3 WLR 1333 內確認的法理發展，香港法庭或須待有機會時對 *Ghosh* 案的驗證標準加以考慮。見 *Archbold Hong Kong 2025*，第 22–20 段。

否屬犯罪，相對上清楚分明。此外，“犯罪目的”亦是訂立已久的法定概念。

3.31 我們應強調，在諮詢文件內，[24] 小組委員會已完全知悉現代網絡器材的運作方式難免牽涉截取，而網絡安全公司在正常業務中亦可能會以各種方式截取數據。正如小組委員會所概述，以下現象即使可能牽涉在未獲授權下進行截取，亦不大可能被視為不妥：[25]

(a) 網絡分析已成為網絡系統一項標準特點。分析所得的統計資料可顯示是否有人濫用網絡、用戶登入某網站的次數等等。這些資料可具管理用途，例如提醒網絡管理員在域名系統層面封鎖某網站。

(b) 在日常運作中，互聯網服務提供者會因為各種原因透過其設備管有某些傳送中的數據，而這些運作在技術上需獲取元數據。

3.32 這正正解釋小組委員會為何建議把*“為不誠實或犯罪目的”*而截取列為建議的截取罪的要求之一，以免日常使用電腦網絡科技時正常進行的數據截取會被定罪。*“為不誠實或犯罪目的”*這項元素旨在訂立較高的犯罪意念門檻，避免把在未獲授權下進行截取過度刑事化，或避免所訂罪行的範圍不合理地廣泛。憑藉*“為不誠實或犯罪目的”*這項規定，網絡安全公司防範網絡攻擊的活動便會排除在建議的罪行的涵蓋範圍以外。

3.33 我們應補充，隨着科技日新月異，如要新訂的電腦網絡罪行法例精準描述數據截取會被視為合法的各種確切情況，既不切實際，亦毫不恰當。我們認為，新訂的電腦網絡罪行法例只要能夠清楚述明，建議的罪行只禁止為不誠實或犯罪目的而在未獲授權下截取電腦數據，便已充分足夠。

3.34 我們亦承認，如要把*“為不誠實或犯罪目的”*這項意念元素應用於若干臨界情況的行為（例如私家偵探及狗仔隊可能作出的數據截取作為），或會出現一些不確定性。在該等情況下，某人是否犯截取罪會視乎案件的特定情況而定。除了截取的目的之外，例如倘若被告人知道所截取的數據涉及私人通訊，法庭則可能會在考慮一般明理的人的標準後，裁定該項截取作為屬不誠實。

---

24 第 3.97 段。

25 同上。

3.35 不過，採用*“為不誠實目的”*這標準的好處在於法庭可以考慮眾多因素，以決定被告人的截取行為是否屬於可接受的界限內。例如，倘若一名電腦科學學生在購物商場截取數據，指稱僅為某類研究目的進行數據截取（例如確定使用某個電話型號的人數），但截取的數據卻包含信用卡資料或電話號碼，而他未能提出一些屬實或可能屬實的清白解釋說明為何收集過多數據，則法庭很可能會裁定他是*“為不誠實或犯罪目的”*而進行截取。

3.36 權衡之下，我們的結論是，*“為不誠實或犯罪目的”*這個犯罪意念門檻屬適當，能夠避免令無惡意進行截取的人無意間誤墮法網。

行使執法權力的公職人員的刑事法律責任

3.37 正如我們剛才已在上文數段解釋，建議的截取罪附帶相對較高的意念門檻，即為不誠實或犯罪目的而在未獲授權下截取電腦數據。倘若一名公職人員真誠行事，只是不慎超逾其權限，我們相信，除非香港法庭因應英格蘭及威爾斯的法理發展[26]而對 *Ghosh* 案的不誠實驗證標準再作考慮，否則該名公職人員不大可能會被裁定犯建議的罪行。在任何情況下，只要公職人員沒有*“為不誠實或犯罪目的”*而截取數據，便不會構成截取罪。

3.38 另一方面，公職人員如*“為不誠實或犯罪目的”*而截取數據，便應該如其他人一樣，被判犯了非法截取電腦數據罪。因此，我們認為無須在針對電腦網絡罪行的特定法例內，就公職人員履行執法職務訂定特定豁免。

在未獲授權下截取，包括“超逾權限”的截取

3.39 “未獲授權”這個概念體現於我們建議的首四項依賴電腦網絡的罪行，即第 2 章討論的非法取覽程式或數據罪（“**取覽罪**”）、

---

[26] 如上文註腳 22 解釋，根據 *Ghosh* 案的驗證標準，陪審團必須：(i)根據明理且誠實的人的一般標準，決定有關行為是否不誠實；及假如有關行為屬於不誠實，(ii)則考慮被告人本人是否必定已認知其行為按該等標準衡量屬於不誠實。有人憂慮，*Ghosh* 案的驗證標準的第二部分取決於被告人對社會標準的理解，因此道德準則薄弱的人只要堅稱自己不知悉社會上對誠實的標準，便可逃避法律責任。在 *R v Barton and Booth* [2021] QB 685 第 729 頁，英格蘭上訴法院確認，在 *Ivey v Genting Casinos (UK) Ltd* [2018] AC 391, [2017] 3 WLR 1212 確立的驗證標準將會是用於所有刑事案件的不誠實驗證標準，即一旦確定被告人就事實所知或所信的實際思想狀態，則其行為是否不誠實這個問題，會應用一般合乎體統的人的客觀標準而裁定，而不是按被告人對該等標準的理解。香港法庭會否偏離 *R v Ghosh* 的不誠實驗證標準，仍有待觀察。

建議的非法截取電腦數據罪，以及我們會於第 4 及 5 章討論的非法干擾電腦數據罪及非法干擾電腦系統罪（“**干擾罪**”）。

3.40 在最終建議 1，我們建議取覽罪應以英格蘭及威爾斯《誤用電腦法令》（Computer Misuse Act，**《英格蘭誤用電腦法令》**）第 1 及 2 條為藍本。《英格蘭誤用電腦法令》第 1(1)及 17(5)條已載於本報告書第 2 章，[27] 現再次引述以便讀者參閱。第 1(1)條規定：

> “任何人在以下情況，即屬犯罪——
>
> (a) 該人致使某電腦執行任何功能，意圖獲得對存於任何電腦內的任何程式或數據的取覽，或意圖使他人能夠獲得該項取覽；
>
> (b) 該人意圖獲得該項取覽，或意圖使他人能夠獲得該項取覽，但該項取覽未獲授權；及
>
> (c) 該人在致使該電腦執行該功能時，知悉情況如此。”
>
> （底線後加）

3.41 《英格蘭誤用電腦法令》第 17(5)條規定如下：

> “在以下情況下，任何人取覽存於某電腦內的任何程式或數據，不論取覽屬任何種類，即屬未獲授權取覽——
>
> (a) 該人本身無權控制對該程式或數據作出有關種類的取覽；及
>
> (b) 該人未獲有此權利的人同意他對該程式或數據作出該類取覽……”
>
> （底線後加）

[27] 上文第 2.20 及 2.21 段。

3.42 正如小組委員會在諮詢文件解釋，[28] 上議院在 *R v Bow Street Metropolitan Stipendiary Magistrate, Ex parte United States* [29] 裁定，第 17(5) 條並無引入按不同級別取用有關電腦的概念，而任何獲有限度授權取覽電腦內數據的僱員，如在超逾該授權範圍下行事，便可能犯《英格蘭誤用電腦法令》第 1 條所訂罪行。換言之，"未獲授權"一詞涵蓋某人在超逾權限範圍下行事的情況，意味着以《英格蘭誤用電腦法令》為藍本的取覽罪擬適用於以下情況：(i) 被告人在沒有權限的情況下行事；或 (ii) 被告人在超逾權限範圍下行事。

3.43 為保持一致，就"未獲授權"這個概念而言，建議的截取罪及干擾罪應採用同一範圍。倘若政府決定落實最終建議 4，法律草擬專員可考慮有關罪行條文應否明文述明"未獲授權"包括 *"在超逾權限範圍下行事"*（如諮詢文件討論的美國《電腦欺詐及濫用法案》〔Computer Fraud and Abuse Act〕第 1030(a) 條所述明），[30] 以確保建議的截取罪涵蓋範圍清楚明白。

截取罪不只適用於"私人通訊"，而是適用於一般"通訊"及"數據"，並包括元數據等

3.44 此處宜回顧《布達佩斯公約》第三條關於訂定非法截取電腦數據罪的標準。正如諮詢文件引述公約的《說明報告》所述：[31]

> "有關罪行適用於'非公開'傳送電腦數據。'非公開'一詞規限傳送（通訊）過程的性質，而非所傳送數據的性質。所傳達的數據可能屬公開資料，但有關各方希望將通訊保密。或者在服務獲繳款前，數據可能因

---

28 第 2.45 及 2.46 段。

29 [2000] 2 AC 216.

30 第 2.81 段。《電腦欺詐及濫用法案》第 1030(a)條列出與取用有關而可根據第 1030(c)條規定予以懲處的作為，包括某人：

"(1) 知悉在未獲授權下取用某電腦或知悉超逾獲授權的取用範圍，並已藉該行為而取得已裁斷為……須獲得保護以免被未獲授權披露的資料……或任何受限數據……而且有理由相信該等資料……可用作損害美國〔等〕，而故意把該等資料傳達〔等〕給任何無權收取該等資料的人〔等〕；

(2) 在未獲授權下蓄意取用某電腦或超逾獲授權的取用範圍，並藉此——

(A) 取得載於某財務機構的財務紀錄的資料〔等〕；

(B) 從美國任何部門或機關取得資料；或

(C) 從任何受保護電腦取得資料；

……

(4) 意圖蓄意欺詐並知悉在未獲授權下取用某受保護電腦或超逾獲授權的取用範圍，並藉該行為而促成故意欺詐並取得任何有價值的物品……"。（底線後加）

31 第 3.18 段。

商業目的而保密（例如是收費電視的情況）。因此，‘非公開’一詞本身並不排除公共網絡上的通訊……”

（底線後加）

3.45 換言之，《布達佩斯公約》第三條並無規定有關電腦數據須為私人數據。[32] 有關數據可以是公開數據或私人數據。

3.46 我們亦緊記，新西蘭對《2012 年搜查及監察法令》（Search and Surveillance Act 2012）的檢討，曾識別出其法定機制僅限於涵蓋截取“私人通訊”而引起的問題。新西蘭的法律委員會（Law Commission）與司法部（Ministry of Justice）於 2016 年聯合發表議事文件，強調不宜聚焦於通訊各方的期望，因為這存在循環論證成分，*“一直引來大量批評”*。[33] 鑑於上文所述，新西蘭於 2017 年發布的報告書建議，“私人通訊”的定義應以“通訊”取代。[34]

3.47 此外，必須留意根據諮詢文件建議 4(b)，建議的截取罪適用於所有“數據”，不論是元數據、傳送中的數據，還是在傳送期間暫時靜止的數據，以免審訊中需要傳喚極為技術性的證據。[35]

3.48 總括而言，我們認為建議的截取罪不應只保障“私人通訊”，而是應同時保障一般“通訊”及“數據”，並應包括元數據等。

不界定“截取”

3.49 正如某商業團體指出，“取用或取覽”及“截取”等電腦相關作為會隨着科技發展而不斷演變。截取電腦數據的嶄新方法可能不時湧現，並超乎我們的想像。若界定何謂“截取”，可能會損害有關法律應對新環境的彈性。

---

32 諮詢文件第 3.100 段。

33 新西蘭法律委員會及司法部，*Review of the Search and Surveillance Act 2012*（第 40 號議事文件，2016 年），第 4.11 段。

34 新西蘭法律委員會及司法部，*Review of the Search and Surveillance Act 2012*（第 141 號報告書，2017 年），建議 24。另見諮詢文件第 3.101(b)段。

35 正如諮詢文件所討論（見第 3.19 至 3.24、3.108 及 3.109 段），只要有關數據是在傳送人一端前往傳送對象一端的途中，截取數據便應屬犯罪。因此，截取罪適用於整個傳送過程中的通訊，不論數據是暫時靜止還是正在傳遞中。訂立這項罪行的方法之一，是加入類似於澳大利亞《1979 年電訊（截取及取覽）法令》（Telecommunications (Interception and Access) Act 1979）第 5F 條的推定條文。該條規定，通訊：(a)在傳送人 *“發送或傳送該通訊的那刻起，視為開始經過電訊系統”*；及(b) *“視為繼續經過該系統，直至……傳送對象可取覽該通訊為止”*（見諮詢文件第 3.22 段）。這會使控方無須援引極為技術性的證據，以證明有關罪行元素。

3.50 因此，儘管現有的《截取通訊及監察條例》（第 589 章）[36] 及某些其他司法管轄區[37] 已界定“截取作為”，但我們認為，較為適當的做法是不在新訂的電腦網絡罪行法例中界定何謂“截取”，而是賦予“截取”其通常涵義，以使建議的罪行達到保障人們數據通訊私隱權這目的。

有關建議 4 的結論

3.51 我們的結論是建議 4 可予保留，但基於上文第 3.25 至 3.28 段所闡述的理由，有關 *“披露或使用電腦數據”* 的部分應予刪除，以待作進一步研究。

最終建議 4

我們建議：

(a) 為不誠實或犯罪目的而在未獲授權下截取電腦數據，應在新法例下定為罪行。

(b) 建議的罪行應：

(i) 保障一般通訊，而並非只保障私人通訊；

(ii) 一般適用於數據（不論有關數據是否元數據）；及

(iii) 適用於截取在傳送人一端前往傳送對象一端途中的數據，即傳送中的數據及在傳送期間暫時靜止的數據。

(c) 除上述另有規定外，建議的條文應以《電腦罪行及電腦相關罪行示範法》（Model Law on Computer and Computer Related Crime）第 8 條為藍本，包括犯罪意念（即“蓄意”截取）。

---

36 根據《截取通訊及監察條例》（第 589 章）第 2(1)條，“截取作為”的定義如下：*“截取作為(intercepting act)就任何通訊而言，指在該通訊藉郵政服務或藉電訊系統傳送的過程中，由並非該通訊的傳送人或傳送對象的人查察該通訊的某些或所有內容”*。

37 即英格蘭及威爾斯（《2016 年調查權力法令》〔Investigatory Powers Act 2016〕第 4 條）、新西蘭（《1961 年刑事罪行法令》〔Crimes Act 1961〕第 216A(1)條）及美利堅合眾國（《搭線竊聽法案》〔Wiretap Act〕第 2510(4)條）。

(d) 關於在未獲授權下披露或使用電腦數據（不論該數據是以截取或其他方式取得），我們應先在研究的第二部分更詳盡探討它所帶來的影響，然後才就應否建議訂立任何這方面的新罪行（以及如應該的話，如何訂立）發表任何確定意見。

非法截取電腦數據罪的免責辯護：建議 5

3.52 諮詢文件建議 5 邀請公眾就以下問題提交意見書：

"(a) 任何專業如需在合法業務的通常運作過程中截取數據和使用截取的數據，應否有免責辯護或豁免？如答案是應該的話，該免責辯護或豁免應涵蓋哪類專業，並應有甚麼條款（例如應否對使用截取的數據有任何限制）？

(b) 提供 Wi-Fi 熱點或電腦供顧客或僱員使用的真正業務（咖啡店、酒店、購物商場、僱主等）應否獲准截取和使用傳送中的數據，而無須負上任何刑事法律責任？如答案是應該的話，哪類業務應受涵蓋，並應有甚麼條款（例如應否對使用截取的數據有任何限制）？"

對小組委員會建議 5 的回應

3.53 由於對建議 5(a)及(b)諮詢問題的回應在某程度上密切相關及互相重疊，因此我們會一併分析。

建議 5(a)

支持豁免專業的回應者的意見

3.54 絕大多數回應者認為，任何專業如需在合法業務的通常運作過程中截取數據和使用截取的數據，均應享有免責辯護或豁免。該等回應者提議，有關免責辯護或豁免應涵蓋以下類別的專業或活動：

(a) 互聯網服務提供者；

(b) 日常工作經常需要使用和處理截取的數據的機構(建議這項豁免的資訊科技相關團體並無提出這類機構的具體例子);

(c) 純粹為偵測安全威脅而截取其本身網絡的公司,不論是由該等公司自行截取,還是由其授權的安全顧問截取;

(d) 執法機關就犯罪活動及國家安全事宜進行的調查;

(e) 為公眾利益或為日後法律程序搜證而真誠地進行的舉報活動;及

(f) 合理相信有損害其利益的活動正在進行的業務或機構(女工商專聯註明,這項免責辯護或豁免應以嚴謹及狹義的方式表達)。

反對豁免專業的回應者的意見

3.55 不過,部分來自資訊科技界別的回應者不贊成對任何專業在合法業務的通常運作過程中截取和使用數據的情況,一律提供免責辯護或豁免。他們指出:

(a) 第一,截取的數據不一定與進行截取的業務有關,這方面有不少灰色地帶,很可能會引起爭議;及

(b) 第二,免責辯護或豁免應適用於任何人,而非只適用於任何享有特權的特定界別。

建議 5(b)

支持豁免真正業務的回應者的意見

3.56 與建議 5(a)的情況類似,明顯大多數的回應者均贊成真正業務應獲准截取和使用傳送中的數據,而無須負上刑事法律責任。該等回應者當中,私隱專員公署與小組委員會看法一致,認為倘若業務根據若干條款及條件提供 Wi-Fi 熱點或電腦供人使用,而有關條款及條件保留權利截取和使用顧客或僱員的數據,則這類截取和使用數據的權限屬於合約性質。[38] 私隱專員公署又指,如收集的數據涉及個人資料,則收集和使用這些個人資料會受到《私隱條例》的保障資料原則規管。

---

[38] 諮詢文件第 3.118 段。

3.57 支持豁免真正業務的回應者就豁免條件作出建議。不同界別的回應者均認為，業務不得為不誠實或犯罪目的而截取和使用數據。女律師協會進一步提議，為了提供充分理據支持業務可截取和使用傳送中的數據而無須負上刑事法律責任，這類截取的目的必須予以限制，而有關免責辯護或豁免亦可規定，進行截取的人與截取對象之間須存在特定關係（例如僱傭關係）。

3.58 關於建議 5 諮詢問題內重點提出的購物商場例子，女律師協會指出：

> "似乎並無任何明顯理由能解釋為何顧客傳送的數據應被截取。購物商場營運者／業主〔與〕整體顧客之間並無真正關係，因此這類法定許可會顯得過於廣泛。"

反對豁免真正業務的回應者的意見

3.59 另一方面，部分回應者對容許真正業務截取和使用傳送中的數據有所保留。例如，消費者委員會提出以下觀點：

> "當商場或商店提供免費 Wi-Fi 熱點服務，消費者或會合理期望，有關服務性質上純粹是為了招徠生意的增值服務。消費者未必會合理期望其數據會被截取和用於其他目的……
>
> ……儘管商場或商店或會列出使用條款，規定消費者須表示同意數據被截取，作為取用服務的條件，但消費者是否會花時間或精力妥為審閱該等條款，這卻是個疑問……即使消費者給予同意，亦未必是在知情下同意。
>
> 不加區別地收集透過 Wi-Fi 熱點傳送的數據，在任何情況下也是過於廣泛之舉。有關收集可能會包括個人資料，甚或銀行帳戶資料及密碼等敏感數據。不論數據是否經過編碼處理，或該業務是否有意使用該等數據，消費者亦不大可能認為這樣收集數據是公平的。"

3.60 最後，某資訊科技相關團體指出，業務為客戶提供的 Wi-Fi 熱點或電腦如被不當使用，可能會導致資料外洩，因此該回應者並不贊成為這類業務提供特定免責辯護或豁免。

我們的分析及回應

3.61 我們審慎衡量回應者的意見書及建議的非法截取電腦數據罪的元素後，認為無須為需在合法業務的通常運作過程中截取和使用電腦數據的人士，訂定任何特定免責辯護或豁免。理論上，就已特意明確規定須證明*"不誠實或犯罪目的"*的罪行提供任何免責辯護，似乎不合邏輯。在這前提下，某專業或真正業務如為不誠實或犯罪目的而截取電腦數據，則不應只是因為它經營某專業或業務，便獲豁免刑事法律責任。

3.62 關於部分回應者認為特定類別的專業或業務應獲提供免責辯護或豁免，我們有以下看法：

(a) 由於在正常業務過程中行事的互聯網服務提供者已受保障，不會因並無犯罪意圖的數據截取而負上法律責任，因此無須就建議的截取罪為他們提供任何免責辯護。

(b) 要為日常工作經常需要使用和處理截取的數據的機構提供免責辯護，但實際上又不向日常營運涉及數據截取的某些專業或業務（例如私家偵探社或傳媒機構）給予截取數據的無限制授權，根本並不可行。

(c) 真正業務的確或會收集或截取電腦數據，主要作多種營銷用途。然而，如證明在未獲授權下截取確曾發生，並且是為不誠實目的（相對於以不誠實方式）而進行，即使該業務只是出於牟利動機，亦更有理由不應提供免責辯護。

(d) 非法取覽程式或數據的作為[39] 或非法干擾電腦數據及／或電腦系統的作為，[40] 即使是為公眾利益或為日後法律程序搜證而真誠地進行，亦沒有獲提供免責辯護。因此，我們難以理解為何應就建議的截取罪為舉報者提供此等免責辯護。此外，不同人對甚麼構成"真誠"或各有標準，諮詢文件討論的*香港特別行政區 訴 秦瑞麟*（*HKSAR v Tsun Shui Lun*）[41] 是一個好例子。案中任職醫院僱員的被告人向傳媒洩露一名主要官員的醫療報告，被控觸犯《刑事罪行

---

39 有關非法取覽程式或數據罪的免責辯護，在第 2 章第 2.63 至 2.102 段討論。

40 有關非法干擾電腦數據罪及非法干擾電腦系統罪的免責辯護，分別在第 4 章第 4.32 至 4.44 段及第 5 章第 5.23 至 5.28 段討論。

41 [1999] 3 HKLRD 215, HCMA 723/1998（判決日期：1999 年 1 月 15 日）。見諮詢文件第 2.9 及 2.10 段。

條例》（第 200 章）第 161(1)(c)條，[42] 他爭辯指自己以為公眾有權知道真相。然而，原訟法庭裁定他針對定罪的上訴缺乏理據。[43]

(e) 最後但同樣重要的是，在針對電腦網絡罪行的特定法例內為特定類別的專業或人士提供免責辯護，或會暗示法例內未有指明的其他專業或人士截取數據必然是不合法，繼而令有關法律更為含糊，而非更為清晰。

3.63 基於所有這些原因，我們傾向建議的截取罪無須提供免責辯護或豁免。任何業務如有意截取客戶或消費者的數據，均可向後者索取截取數據的授權。倘若截取的數據用於獲授權目的以外的其他目的，則會由法庭根據個別案件的證據，決定有關截取是否為不誠實或犯罪目的而進行。

3.64 總括而言，有別於取覽罪及干擾罪，建議的截取罪就截取電腦數據採用*"為不誠實或犯罪目的"*這個較高標準的犯罪意念，而這項犯罪意念本身已免除為有關罪行提供任何特定豁免或免責辯護的需要。

最終建議 5

我們不建議為在通常運作過程中截取或使用電腦數據的專業或真正業務（例如咖啡店、酒店、購物商場、僱主）提供任何免責辯護或豁免。為不誠實或犯罪目的而截取電腦數據這項犯罪意念規定，已免除訂定任何特定免責辯護或豁免的需要。

---

42 根據《刑事罪行條例》（第 200 章）第 161(1)(c)條，任何人取用電腦，*"目的在於使其本人或他人不誠實地獲益"*（不論是在取用電腦的同時或在日後任何時間），即屬犯罪，一經循公訴程序定罪，可處監禁 5 年。

43 見上文註腳 41，第 228 頁。原訟法庭裁定，上訴人在超逾權限範圍下取用醫院的電腦系統，意圖取得電腦內的保密資料，目的在於列印有關掃描報告的複本，並洩露予傳媒，這屬於《刑事罪行條例》第 161 條定義的獲益。有關行為是不誠實行為，而被告人亦知悉事實如此。

第 4 章　非法干擾電腦數據

引言

4.1　本章討論關於諮詢文件建議 6 的回應。建議 6 建議訂立第三類依賴電腦網絡的罪行，即非法干擾電腦數據：

> "小組委員會建議：
>
> (a) 無合法權限或合理辯解而蓄意干擾（損壞、刪除、弄壞、更改或抑制）電腦數據，應在新法例下定為罪行。
>
> (b) 新法例應採用《刑事罪行條例》（第 200 章）所訂的以下特點：
>
> (i) 第 59(1A)(a)、(b)及(c)條所訂犯罪行為；
>
> (ii) 第 60(1)條所訂犯罪意念（規定須懷有意圖或罔顧後果，但無須懷有惡意）；
>
> (iii) 第 64(2)條所訂兩項合法辯解，並同時保留任何獲法律承認的其他合法辯解或免責辯護；及
>
> (iv) 第 60(2)條所訂加重罪行。
>
> (c) 上述有關'誤用電腦'的條文應與刑事損壞罪拆開，並納入新法例內，同時刪除《刑事罪行條例》（第 200 章）第 59(1)(b)及(1A)條。"

4.2　正如小組委員會在諮詢文件解釋，[1] 概括而言，干擾電腦數據罪旨在：

(a) 打擊蓄意損壞、刪除、更改電腦數據等行為；

(b) 從而保護電腦數據的完整性，確保有關數據能正常運作或使用。

---

[1] 第 4.1 段。

4.3 干擾數據罪可藉以下方式進行：

(a) 在沒有權限的情況下取覽儲存於電腦的檔案後，修改該檔案。

(b) 藉電腦病毒（譬如是能夠刪除受感染電腦所儲存的特定數據的電腦病毒）干擾數據。

4.4 由於干擾數據通常只會在某人初步入侵電腦系統時發生，因此非法干擾電腦數據罪與第 2 章所討論的非法取覽程式或數據罪（“**取覽罪**”）息息相關。

對建議 6 的概括回應

4.5 絕大多數就建議 6 發表具體意見的回應者均支持該建議，這些回應者包括法律專業團體、資訊科技相關團體、大專院校、商業機構及政府部門。

4.6 個人資料私隱專員公署支持訂立建議的非法干擾電腦數據罪，理由是此舉有助遏止愈趨常見的資料外洩事故。

4.7 多個機構（包括香港與內地法律專業聯合會有限公司、香港女律師協會有限公司、另一個專業協會及兩個商業團體）同意，《刑事罪行條例》（第 200 章）下應對非法干擾電腦數據及電腦系統的現行制度（包括第 59(1A)條 *“誤用電腦”* 這概念）令人滿意。這些回應者因此同意小組委員會的建議，將《刑事罪行條例》第 59、60 及 64 條的現有條文改列於新訂的電腦網絡罪行法例，以求貫徹一致。

香港的現行法律

4.8 正如小組委員會在諮詢文件解釋，[2] 現行的香港法律處理非法干擾電腦數據的主要方式，是把它視為刑事損壞的其中一種形式。根據《刑事罪行條例》第 60(1)及(2)條（ *“摧毀或損壞財產”* ）：

> “(1) 任何人無合法辯解而摧毀或損壞屬於他人的財產，意圖摧毀或損壞該財產或罔顧該財產是否會被摧毀或損壞，即屬犯罪。

[2] 第 4.4 及 4.5 段。

(2) 任何人無合法辯解而摧毀或損壞任何財產(不論是屬於其本人或他人的)——

(a) 意圖摧毀或損壞任何財產或罔顧任何財產是否會被摧毀或損壞;及

(b) 意圖藉摧毀或損壞財產以危害他人生命或罔顧他人生命是否會因而受到危害,

即屬犯罪。"

4.9 與第 60(1)條相比,第 60(2)條所訂罪行是有關罪行的加重形式。第 63 條(*"罪行的懲處"*)就這些罪行所訂明的最高刑罰差別很大:

"(1) 任何人犯……第 60(2)條所訂的罪行……,一經循公訴程序定罪,可處終身監禁。

(2) 任何人犯本部所訂的其他罪行〔即包括第 60(1)條〕,一經循公訴程序定罪,可處監禁 10 年。"

《刑事罪行條例》在干擾電腦數據及電腦系統方面的應用

4.10 刑事損壞罪可處理非法干擾電腦數據(以及將於下一章討論的非法干擾電腦系統),是因為《1993 年電腦罪行條例》(1993 年第 23 號)在《刑事罪行條例》加入以下條文:

(a) 第 59(1)(b)條將"財產"一詞界定為包括 *"電腦內或電腦儲存媒體內的任何程式或資料,不論該程式或資料是否屬實體性質的財產。"*

(b) 第 59(1A)條訂明摧毀或損壞財產,就電腦而言,包括 *"誤用電腦"*。該詞在第 59(1A)條界定為以下作為:

"(a) 導致電腦並非如其擁有人或其擁有人代表對其所設定的運作方式運作,即使如此誤用不會令該電腦的操作、該電腦內的程式或該電腦內的資料的可靠性減損亦然;

(b) 更改或刪抹電腦內或電腦儲存媒體內的程式或資料;

(c) 在電腦或電腦儲存媒體所收納的內容上增加程式或資料，

而造成導致(a)、(b)或(c)段所提述的任何類別誤用情形的任何作為，須視為導致該項誤用情形的作為。”

第 59(1A)條的三個部分當中，(b)及(c)部分與非法干擾電腦數據罪最為相關。

4.11 根據《刑事罪行條例》第 64(2)條，任何人被控以刑事損壞罪，在下述情況下均須被視為有 *“合法辯解”*：

“(a) 如指稱構成該罪行的作為作出時，被控人相信，他相信有權同意有關財產的摧毀或損壞的人已予同意，或相信該人如知道有關財產的摧毀或損壞及有關情形亦會予以同意；或

(b) 如被控人摧毀或損壞有關財產或威脅會如此做，或（在被控以第 62 條所訂罪行時）意圖使用或導致或准許使用某些物品以摧毀或損壞有關財產，而他如此做是為了保護屬於其本人或另一人的財產，或保護歸屬於或他相信歸屬於其本人或另一人的財產權利或財產權益，且於指稱構成該罪行的作為作出時，他相信——

(i) 該財產、權利或權益即需保護；及

(ii) 在顧及一切有關情況後，所採用或打算採用的保護方法是或會是合理的。”

4.12 憑藉第 64(3)條，只要被告人是誠實地相信有關事情，則是否有充分理由支持，不具關鍵性。

對小組委員會建議 6 的詳細回應

4.13 雖然極大多數回應者均支持訂立建議的非法干擾電腦數據罪，但部分回應者亦就建議 6 所建議罪行的構成元素發表具體意見：

(a) 數個資訊科技相關團體留意到，建議的非法干擾電腦數據罪一經循公訴程序定罪，最高刑罰為監禁 14 年（見建議 16(c)）。鑑於刑罰甚重，這些團體認為“惡意”應是建議的干擾罪的所需元素。

(b) 香港律師會指出，不清楚為何“罔顧後果”的規定屬恰當或相關。該回應者認為，如某人想到要干擾儲存於某電腦的數據，必然有“意圖”這樣做。舉例來說，該人會預先計劃，獲取所需工具（軟件），把握機會取用該電腦，把數據拿到手，再加以更改或刪除。香港律師會認為這些行動需要透過 *“一連串故意行為”* 來進行。

(c) 某政府部門建議，除《刑事罪行條例》第 60(2)條所述元素外，*“任何意圖危害國家安全的行為或活動，或罔顧國家安全是否會因而受到危害”*，亦應視為加重罪行。該回應者引用以下其他司法管轄區的例子，指出它們的法律條文明確提及損害國家安全：

(i) 英格蘭及威爾斯《誤用電腦法令》（Computer Misuse Act，**《英格蘭誤用電腦法令》**）訂明，被告人的作為如導致國家安全嚴重損害，或產生導致該損害的重大風險，最高刑罰為終身監禁。[3] 被告人如就某電腦作出未獲授權的作為，而該作為導致 *“對任何國家的國家安全的損害”*，或產生導致該損害的重大風險，[4] 一經循公訴程序定罪，最高刑罰為監禁 14 年或罰款，或兩者兼處。[5]

---

3 諮詢文件第 4.41 段。第 3ZA(7)條的內容如下：
“如任何人——
……
(b) 因導致國家安全嚴重損害的作為而干犯〔第 3ZA 條〕所訂罪行，或因產生導致該損害的重大風險的作為而干犯該罪行，
則該人一經循公訴程序定罪，可處終身監禁或罰款，或兩者兼處。”（底線後加）

4 諮詢文件第 4.41 段。第 3ZA 條相關條款的內容如下：
“(1) 任何人在以下情況，即屬犯罪——
(a) 該人就某電腦作出任何未獲授權的作為；
(b) 該人在作出該作為時，知悉該作為未獲授權；
(c) 該作為導致關鍵性嚴重損害，或產生導致關鍵性嚴重損害的重大風險；及
(d) 該人意圖藉作出該作為而導致關鍵性嚴重損害，或罔顧會否導致上述損害。
(2) 就本條而言，損害如屬——
……
(d) 對任何國家的國家安全的損害，
即屬‘關鍵性’損害。”（底線後加）

5 《英格蘭誤用電腦法令》第 3ZA(6)條。

(ii) 新加坡《誤用電腦法令》（Computer Misuse Act，**《新加坡誤用電腦法令》**）第 11 條把最重的最高刑罰預留給涉及取用“受保護電腦”的案件。某電腦須視為“受保護電腦”，前提是干犯該罪行的人知悉或理應知悉有關電腦、程式或數據是在與*“新加坡的安全、防務或國際關係”*有直接關連的情況下使用的，或對*“新加坡的安全、防務或國際關係”*屬必要的。[6]

我們的分析及回應

非法干擾電腦數據的罪行元素

惡意

4.14 我們希望指出，“惡意”是表達犯罪意念的陳舊用語，常見於較早期的法例。正如時任的上訴法院常任法官迪普洛克（Diplock LJ）在 *R v Mowatt* 所指出，[7] *“‘非法及惡意’是 1861 年英國國會法律草擬人員的流行用詞”*，[8] 舊法例《1861 年惡意損壞法令》（Malicious Damage Act 1861）正是於當年制定。

4.15 在刑事法中，“惡意”的涵義是有實際意圖造成某種特定傷害，並事實上造成了該種傷害，或罔顧該種傷害是否應當發生（即被控人已預見可能會造成該種傷害，但仍然冒這風險行事），[9] “惡意”並不要求對受傷害的人懷有敵意。這項詮釋解釋了為何英格蘭及威爾斯法律委員會（Law Commission of England and Wales）在檢討關於損壞財產的罪行時，發現難以處理“惡意”一詞，導致後來制定了《1971 年刑事損壞法令》（Criminal Damage Act 1971，香港的刑事損壞罪亦以該法令為藍本）：

> “因此，我們認為目前所需的相同元素應予保留，但同時應將該等元素表達得更加簡潔清晰。我們尤其傾向避免使用‘惡意地’一詞，無非是由於其字眼會令人以為，這項意念元素有異於其他規定須懷有傳統犯罪意念

---

6 《新加坡誤用電腦法令》第 11(2)(a)條。第 11 條載於諮詢文件第 4.68 段。

7 [1968] 1 QB 421.

8 同上，第 425 頁。

9 *Archbold Hong Kong 2025*，第 16−35 段，引用 *R v Cunningham* [1957] 2 QB 396；41 Cr App R 155 及其後發展（見下文進一步討論）。亦見*香港特別行政區 訴 鍾志輝*[2014] 3 HKLRD 538，第 26 段。

的罪行所施加的意念元素。從 *R v Cunningham* 及 *R v Mowatt* 等案例可見，該詞可能會造成詮釋上的困難……”[10]

（底線後加）

4.16 考慮到上述問題，保留建議 6(b)(ii)的犯罪意念元素是恰當的，即 *“須懷有意圖或罔顧後果，但無須懷有惡意”*。

罔顧後果

4.17 正如在本章較前部分所見，[11] “意圖”及“罔顧後果”是現有《刑事罪行條例》第 60(1)條就刑事損壞罪所訂的替代犯罪意念元素，而憑藉第 59(1)(b)及(1A)條，刑事損壞罪的現行法定框架適用於 *“誤用電腦”*。因此，建議 6 在建議採納第 60 條的現行制度時，亦同樣採納“意圖”及“罔顧後果”作為建議的非法干擾電腦數據罪的意念元素。

4.18 我們留意到，某些其他司法管轄區的電腦網絡罪行法例亦一併採納“罔顧後果”與“意圖”作為意念元素。這些法例包括：

(a) 澳大利亞《刑事法典》（聯邦）（Criminal Code (Cth)）第 477.2 條（ *“在未獲授權下修改數據，以導致損害”*）；[12]

(b) 《英格蘭誤用電腦法令》第 3 條（ *“作出未獲授權的作為，並意圖損害或罔顧是否會損害電腦的操作等”*）[13] 及

---

10 英格蘭法律委員會，*Criminal Law Report on Offences of Damage to Property*（1970 年），英格蘭法律委員會第 29 號，第 44 段。

11 第 4.8 及 4.10 段。

12 諮詢文件第 4.23 段。《刑事法典》（聯邦）第 477.2(1)條規定，*“任何人在以下情況，即屬犯罪：*

(a) 該人導致在未獲授權下修改存於某電腦內的數據；及

(b) 該人知悉該項修改未獲授權；及

(c) 該人罔顧該項修改是否損害或會否損害：

(i) 對存於任何電腦內的該等數據的取覽，或對存於任何電腦內的任何其他數據的取覽；或

(ii) 上述數據的可靠性、保安或操作。”（底線後加）

13 諮詢文件第 4.38 段。《英格蘭誤用電腦法令》第 3(1)條規定，*“任何人在以下情況，即屬犯罪——*

(a) 該人就某電腦作出任何未獲授權的作為；

(b) 該人在作出該作為時，知悉該作為未獲授權；及

(c) 下文第(2)款或第(3)款適用。”

第 3(2)條述明，*“如上述人士意圖藉作出有關作為而……則本款適用。”*

第 3(3)條述明，*“如上述人士罔顧有關作為是否會造成上文第(2)款(a)至(d)段所述的任何事宜，則本款適用。”*（底線後加）

第 3ZA 條（*"作出未獲授權的作為而導致嚴重損害或產生導致嚴重損害的風險"*）；[14] 及

(c) 新西蘭《1961 年刑事罪行法令》（Crimes Act 1961）第 250(2) 條。[15]

4.19 在刑事法中，"罔顧後果"這概念要求證明被告人察覺有關風險，而在被告人所知的情況下，承擔該風險並不合理。[16] 這項對罔顧後果的詮釋適用於整體刑事法，而非僅適用於電腦網絡罪行。正因如此，被告人的作為在甚麼情況下發生，本身並非充分理據，支持排除以罔顧後果為理由而引用建議的非法干擾電腦數據罪。

4.20 事實上，不少刑事罪行一併採納"罔顧後果"與"意圖"或"知悉"作為過失元素。以下是數個例子：

(a) 根據《刑事罪行條例》（第 200 章）第 118(3)條，任何人與女子非法性交，而該女子對此並不同意，他亦 *"知道"* 該女子並不同意性交，或 *"罔顧"* 該女子是否對此同意，即屬強姦。在現實中，強姦罪的檢控理由，通常是被告人罔顧受害人是否同意性交（例如受害人喝醉，無能力給予同意）；

(b) 如任何人藉作出任何 *"欺騙"*（不論是*蓄意或罔顧後果地作出*）並意圖詐騙而誘使另一人作出任何作為或有任何不作為，而導致該另一人以外的任何人獲得利益，或該進行誘使的人以外的任何人蒙受不利或有相當程度的可能性會蒙受不利，即屬犯欺詐罪；[17]

---

14 諮詢文件第 4.41 段。《英格蘭誤用電腦法令》第 3ZA(1)條規定，*"任何人在以下情況，即屬犯罪——*

(a) 該人就某電腦作出任何未獲授權的作為；

(b) 該人在作出該作為時，知悉該作為未獲授權；

(c) 該作為導致關鍵性嚴重損害，或產生導致關鍵性嚴重損害的重大風險；及

(d) 該人意圖藉作出該作為而導致關鍵性嚴重損害，或罔顧會否導致上述損害。"（底線後加）

15 諮詢文件第 4.50 段。《1961 年刑事罪行法令》第 250(2)條規定，*"任何人知悉自己未獲授權或罔顧自己是否已獲授權，而蓄意或罔顧後果地在未獲授權下——*

(a) 損壞、刪除、修改或以其他方式干擾或損害任何電腦系統內的任何數據或軟件；或

(b) 導致任何電腦系統內的任何數據或軟件被損壞、刪除、修改或以其他方式受到干擾或損害；……

可處為期不超過 7 年的監禁。"（底線後加）

16 *Archbold Hong Kong 2025*，第 16−40 段，討論就刑事損壞罪作出判決的 *R v G* [2004] AC 341 及其後的法理發展。

17 《盜竊罪條例》（第 210 章）第 16A 條。

(c) 以欺騙手段取得財產罪亦有類似的過失元素，該罪行是指任何人以欺騙手段（不論是*蓄意或是罔顧後果*）而不誠實地取得屬於另一人的財產，意圖永久地剝奪該另一人的財產；[18] 及

(d) 根據《證券及期貨條例》（第 571 章）第 295(1)條，任何人如 *"意圖"* 使某事情具有或相當可能具有造成在認可市場交易的證券或期貨合約交投活躍的虛假或具誤導性表象的效果，或 *"罔顧"* 某事情是否具有或相當可能具有造成該表象的效果，即屬犯虛假交易的罪行。

4.21 此外，"罔顧後果"這概念強調人們應小心謹慎及負責任地使用電腦科技的重要性，即當事人必須保持警惕，注意其網上行為可能帶來的後果（包括這些行為可能對他人造成的影響）。

4.22 基於上文所解釋的理由，我們建議保留"罔顧後果"這項元素，與"意圖"一同作為非法干擾電腦數據罪的過失元素。

加重形式的干擾罪應否明確涵蓋危害國家安全行為？

4.23 首先，值得我們仔細考慮的是，於 2020 年 6 月 30 日制定為全國性法律，並在香港公布實施的《中華人民共和國香港特別行政區維護國家安全法》（**《國安法》**），在多大程度上已涵蓋建議的非法干擾電腦數據罪及／或非法干擾電腦系統罪。

4.24 《國安法》的罪行條文主要着重具體說明威脅國家安全的受禁活動、從事這些活動的人所懷目的及這些活動的影響。受禁活動的進行方式（例如在現實世界還是電腦網絡空間進行），就《國安法》而言相對無關重要。

4.25 然而，《國安法》第二十四（四）條清楚涵蓋干擾及損壞互聯網電子控制系統的作為。第二十四條述明：

> "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：
>
> ……

---

18 同上，第 17 條。

（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。”

（底線後加）

4.26 我們已仔細考慮干擾電腦數據（以及干擾電腦系統）的加重罪行應否明確涵蓋危害國家安全行為，與《國安法》有關的法律及實際考慮因素如下：

(a) 《國安法》地位超然，理應必然凌駕所有其他本地法例，包括我們所建議制定的針對電腦網絡罪行的特定法例。倘若電腦網絡罪行同時符合《國安法》所訂罪行的元素，我們預料援引《國安法》應屬執法機關、檢控機關及法庭的首要考慮。

(b) 如《國安法》已涵蓋非法干擾電腦數據罪及／或非法干擾電腦系統罪，加重形式的干擾罪又再特別提述危害國家安全行為，就可能會顯得多餘。儘管如此，我們留意到第二十四條所訂罪行有非常特定的意圖——被告人必須造成或意圖造成嚴重社會危害，並懷有特定意圖，為脅迫中央人民政府、香港特別行政區（“**香港特區**”）政府或者國際組織或者威嚇公眾以圖實現政治主張。

(c) 《國安法》以概括的措辭表達。《國安法》的其他條文（即明確提述互聯網電子控制系統的第二十四（四）條[19] 以外的條文）強調受禁活動的目的及影響，範圍似乎相當廣闊，足以涵蓋非法干擾電腦數據（以及非法干擾電腦系統）的作為。例如：

(i) 第二十四（三）條沒有提及被告人可藉甚麼方式“破壞”該條所述的各項公用設施。由於第二十四（三）條着眼於受禁行為（即“破壞”），該條似乎適用於任何會導致破壞指明公用設施的作為，包括非法干擾

19 上文第 4.25 段。

與相關公用設施有關的電腦數據及／或電腦系統而造成破壞。

(ii) 《國安法》第二十四（五）條是一項包含一切的條文，涵蓋所有嚴重危害公眾安全的危險活動，其重點規定在於有關方法的性質，即必須是危險方法。由於電腦網絡罪行與現實世界的罪行均可符合這項規定，第二十四（五）條看來相當廣闊，足以涵蓋非法干擾電腦數據罪及非法干擾電腦系統罪（"**干擾罪**"）。

(d) 第二十四條所訂罪行設有兩層罰則。如被告人致人重傷、死亡或者使財產遭受重大損失，刑罰為無期徒刑或者十年以上有期徒刑。這項《國安法》所訂的最高刑罰較重，與非法干擾電腦系統的加重罪行的最高刑罰相稱，後者建議判處終身監禁。[20] 在其他情形下，較輕的刑罰（即三年以上十年以下有期徒刑）適用於第二十四條所訂罪行。

4.27 尤其是因為《國安法》構成我們法律制度不可或缺的部分，所以重要的一點，是針對電腦網絡罪行的特定法例不得與《國安法》有任何抵觸或衝突，即使並非有意亦然。國家安全至關重要，我們預料在《國安法》下訂立國家安全相關罪行時，已充分考慮該等罪行須以電腦網絡中立的措辭來擬訂，並據此解釋，但如《國安法》的文本、文意和目的顯示相反情況，則屬例外。我們意識到，若然沒有政府對國家安全實體法律整體立場的全面觀點，則分析建議干擾罪的加重罪行會有欠完整。

4.28 2024 年 3 月，立法會制定《維護國家安全條例》（"**《基本法》第二十三條立法**"），以全面落實《基本法》第二十三條、《全國人民代表大會關於建立健全香港特別行政區維護國家安全的法律制度和執行機制的決定》，以及《國安法》所規定的憲制責任及義務，並有效應對現今及日後可能出現的國家安全風險和威脅。[21]

4.29 《基本法》第二十三條立法所訂罪行包括以下罪行：意圖危害國家安全（或罔顧是否會危害國家安全）而進行破壞活動，損壞或削弱公共基礎設施（包括組成該設施的軟件）；[22] 更具體的是，意圖危害國家安全，而在沒有合法權限下，就某電腦或電子系統作出某項

---

20 最終建議 16(c)(ii)。至於非法干擾電腦數據及電腦系統的基本罪行，建議刑罰為一經循簡易程序定罪，可處兩年監禁，一經循公訴程序定罪，可處 14 年監禁。

21 《立法會參考資料摘要——維護國家安全條例草案》（2024 年 3 月）。

22 《維護國家安全條例》第 49 條（危害國家安全的破壞活動）。

作為。[23] 就後一項罪行而言，政府於 2024 年 1 月發表的諮詢文件解釋背後理據如下：

> "本文件中所討論的建議罪行，基本上並不取決於犯罪者實際上採用了哪種特定的方法或技術實施犯罪行為，因此應涵蓋大部分透過電腦進行的危害國家安全的行為和活動。另一方面，由於電腦或電子系統科技非常普及且發展迅速，例如人工智能技術正廣泛應用於社會上不同的領域，其蘊含的潛在國家安全風險不容忽視，特別是電腦或電子系統遭受入侵或干擾而引起的風險。為應對現時電腦或電子世界及未來可能出現的新技術所帶來的國安風險，建議引入罪行，打擊對電腦或電子系統作出危害國家安全的行為。"[24]

4.30 終審法院裁定，《國安法》第四十二（二）條[25] 提述的 *"危害國家安全行為"*，是指任何根據其性質可構成違反《國安法》或香港特區法例中維護國家安全的罪行的行為。[26] 因此，《國安法》的特定程序規則（包括在保釋、[27] 陪審團審訊、[28] 海外律師參與案件[29] 及判刑[30] 方面的規則），應用範圍並不局限於《國安法》所訂罪行。

---

23 同上，第 50 條（就電腦或電子系統作出危害國家安全的作為）。

24 香港特別行政區政府保安局，《維護國家安全：〈基本法〉第二十三條立法公眾諮詢文件》（2024 年 1 月），第 6.5 段。

25 《國安法》第四十二條規定：
"對犯罪嫌疑人、被告人，除非法官有充足理由相信其不會繼續實施危害國家安全行為的，不得准予保釋。"

26 *香港特別行政區 訴 黎智英*（*HKSAR v Lai Chee Ying*）[2021] HKCFA 3，(2021) 24 HKCFAR 33（判決日期：2021 年 2 月 1 日及 9 日），第 53(c)(ii)及 70(d)(ii)段。

27 同上，第 53(a)及(b)段。終審法院指出，《國安法》第四十二（二）條 *"訂下的門檻要求嚴格得多"*，原因是有利於保釋的假定已即時被排除——根據《國安法》，此條文開宗明義說不得准予保釋，除非法官有充足理由相信被控人不會繼續實施危害國家安全行為。終審法院亦注意到，國安法第四十二（二）條的主題內容，與《刑事訴訟程序條例》（第 221 章）第 9G(1)(b)條的主題內容重疊：兩者均以被控人可能在保釋期間犯罪的風險為拒絕保釋的基礎。

28 《國安法》第四十六條規定：
"對高等法院原訟法庭進行的就危害國家安全犯罪案件提起的刑事檢控程序，律政司長可基於保護國家秘密、案件具有涉外因素或者保障陪審員及其家人的人身安全等理由，發出證書指示相關訴訟毋須在有陪審團的情況下進行審理……。"

29 在*香港特別行政區 訴 黎智英*（*HKSAR v Lai Chee Ying*）[2023] HKCFI 1440（判決日期：2023 年 2 月 2 日及 29 日），原訟法庭裁定在《基本法》第三十五條下並無"選擇律師"的絕對權利。"選擇律師"的權利只不過是指訴訟人可從可供選擇的律師當中自由選擇代表律師。任何人均無權堅持由在香港不具一般執業資格的律師作為代表（見第 75 及 87 段）。

30 在*香港特別行政區 訴 呂世瑜*（*HKSAR v Lui Sai Yu*）[2023] HKCFA 26（判決日期：2023 年 8 月 22 日），終審法院裁定，《國安法》第二十一條就情節嚴重的案件訂明 *"五年以上……有期徒刑"* 的罰則，屬強制性規定。因此，下級法院不以上訴人認罪為由，全數扣減三分一刑期，做法是恰當的，因為扣減三分一刑期會導致最終刑期低於《國安法》第二十一條訂明的較高幅度下限（見第 66 及 76 段）。

如某人干犯干擾罪的方式亦構成《國安法》或《基本法》第二十三條立法所訂罪行，《國安法》所規定的程序規則即告適用。

4.31 考慮到《基本法》第二十三條現已藉本地立法的方式落實(包括引入特定罪行，涵蓋電腦網絡空間當中的國家安全風險)，我們認為，政府更具條件全面評估所有現存國家安全相關罪行是否足夠，從而考慮我們的建議，以研究應否建議任何可完善之處(假如政府日後決定接納我們的建議，在針對電腦網絡罪行的特定法例中引入新的干擾罪)。

特定的免責辯護

考慮適用於取覽罪的免責辯護

4.32 正如本章開首所解釋，[31] 取覽程式或數據通常於干擾電腦數據前發生，因此非法干擾電腦數據罪與取覽罪息息相關。有見及此，我們已並行探討取覽罪與非法干擾電腦數據罪(以及非法干擾電腦系統罪)的免責辯護，以確保我們所建議的法律是一致的。當然，隨着科技進步，將來或可能無須取覽任何程式或數據，已可干擾電腦數據(或電腦系統)，但我們認為這點不應影響我們分析這兩項罪行的接近程度，因為在一般情況下，取覽程式或數據都會在干擾數據前發生。

4.33 在本報告書第2章，我們回應受諮詢者對取覽罪的“合理辯解”一般免責辯護所提出的意見時，[32] 已解釋在電腦網絡罪行法例加入特定的免責辯護有何好處。概括而言，這些特定的免責辯護可預防日後出現關於某項作為是否構成“合理辯解”的爭議。畢竟，“合理辯解”這概念不易為外行人所理解，而且可作不同詮釋。訂立特定的免責辯護，能使公眾有所依從，了解哪些行為屬可接受，從而令法律更加清晰。

為網絡安全目的而干擾電腦數據

4.34 在第2章，我們建議，就在未獲授權下為網絡安全目的而取覽訂定特定的免責辯護，其條件如下：[33]

---

31 第4.4段。
32 第2.32至2.34段。
33 第2.63至2.74段。

(a) 該項免責辯護應只適用於經認可的網絡安全從業員(認可制度的細節本質上屬政策事項，最好留待政府考慮）。

(b) 被告人必須為真正的網絡安全目的而行事。

(c) 在顧及整體情況後，被告人的行為必須是合理的。

4.35 由於干擾電腦數據（或電腦系統）通常只會在取覽程式或數據後發生，為非法干擾電腦數據罪（以及非法干擾電腦系統罪）提供類似的免責辯護，是合乎邏輯且連貫一致的做法。因此，我們建議，就建議的非法干擾電腦數據罪而言，為網絡安全目的而干擾電腦數據應可作為免責辯護。

為保障兒童或易受傷害人士的利益而干擾電腦數據

4.36 雖然家長、監護人或其他人士或會要求取覽兒童或易受傷害人士的程式或數據，以保護該兒童或易受傷害人士免受網上危害，但據我們理解，這種取覽並不涉及更改或干擾電腦數據(或電腦系統)。況且，按照常理，准許某人取覽任何程式或數據，絕不表示該人獲授權更改或以其他方式干預有關數據。

4.37 因此，我們認為，與取覽罪不同，無須為保障兒童或易受傷害人士的利益而就非法干擾電腦數據罪提供特定的免責辯護。

為真正的研究目的而干擾電腦數據

4.38 同樣地，若從事真正研究需要干擾電腦數據(或電腦系統)，我們認為是匪夷所思的。因此，與取覽罪不同，我們認為無須提供特定的免責辯護，以豁免為真正的研究目的而進行的非法干擾電腦數據（或電腦系統）行為。

改列《刑事罪行條例》第 64(2)條的免責辯護

4.39 正如本章開首所概述，[34] 諮詢文件建議 6 建議採納現時《刑事罪行條例》第 64(2)條所訂的兩項“合法辯解”（於上文第 4.11 段引述）。

---

[34] 第 4.1 段。

4.40 在本報告書第 2 章，[35] 我們已解釋這兩項“合法辯解”（分別稱為同意免責辯護及保護財產免責辯護）也應適用於取覽罪。

4.41 就非法干擾電腦數據罪（以及非法干擾電腦系統罪）而言，由於回應者普遍歡迎採納《刑事罪行條例》所設的現行制度，我們認為適宜維持建議 6，但須在同意免責辯護及保護財產免責辯護加入客觀驗證標準（和上文第 2.101 段所討論的取覽罪一樣）：

(a) 就同意免責辯護而言，被告人必須*合理地*相信自己已獲同意或會獲同意干擾有關電腦數據（或電腦系統）；及

(b) 就保護財產免責辯護而言，被告人必須*合理地*相信有關財產需即時保護。

4.42 換言之，我們建議在針對電腦網絡罪行的特定法例加入非法干擾電腦數據罪（以及非法干擾電腦系統罪），而《刑事罪行條例》第 64(3)條不適用於該等罪行。上述調整會使同意免責辯護及保護財產免責辯護與我們就非法干擾電腦數據罪（以及非法干擾電腦系統罪）所建議的其他特定免責辯護看齊，即所有免責辯護均採用“合理性”要求，以確保一致。與取覽罪的免責辯護一樣，我們相信這種處理方法可避免各項免責辯護被濫用，並體現我們的指導原則：一方面平衡兼顧網民的權利和資訊科技業內人士的權益，另一方面亦保障公眾在使用電腦系統時免受騷擾或攻擊的權益和權利。

4.43 經檢視第 64(2)條，我們留意到現時《刑事罪行條例》第 64(2)(b)條之下的“合法辯解”僅限於保護財產，但不包括保護人命。因此，我們曾考慮，就非法干擾電腦數據罪（以及非法干擾電腦系統罪）而言，應否為保護生命及／或防止對他人造成身體傷害訂定特定的免責辯護。

4.44 我們傾向認為，如有人為保護生命及／或防止身體傷害而干擾電腦數據（或電腦系統），建議 6 的“合理辯解”一般免責辯護能夠應對這種情況，因此未必需要為此特定目的建議另一項免責辯護。我們相信，在保護生命這方面不設明文訂定的特定免責辯護，或可留給法庭更大的迴旋餘地，處理人命攸關的情況。因此，我們贊成在這方面維持第 64(2)(b)條的現狀。相同的原則及理據亦適用於第 2 章所討論的取覽罪。

---

[35] 第 2.95 至 2.99 段。

有關建議 6 的結論

4.45 概括而言，我們的結論是建議 6 可予保留，但建議就非法干擾電腦數據罪而對第 64(2)條作出改進，並將為網絡安全目的而干擾數據加入為免責辯護。

最終建議 6

我們建議：

(a) 無合法權限而蓄意干擾（損壞、刪除、弄壞、更改或抑制）電腦數據，應在新法例下定為罪行，而合理辯解可作為法定免責辯護。

(b) 新法例應採用《刑事罪行條例》（第 200 章）所訂以下特點：

(i) 第 59(1A)(a)、(b)及(c)條所訂犯罪行為；

(ii) 第 60(1)條所訂犯罪意念（該條規定須懷有意圖或罔顧後果，而非懷有惡意）；

(iii) 第 64(2)條所示的兩項免責辯護，但須因應上文(a)段所重新擬訂的罪行，為恰當表達該兩項免責辯護而作出所需改進，並同時保留任何獲法律承認的其他合法辯解或免責辯護；及

(iv) 第 60(2)條所訂加重罪行。

(c) 第 64(2)條所涵蓋的兩項免責辯護適用於以下情況：

(i) 被告人在干擾電腦數據時，相信其作為已獲同意或會獲同意；或

(ii) 被告人在干擾電腦數據時，相信有關財產需即時保護，並相信在顧及整體情況後，所採用的保護方法是合理的。

被告人不論是提出同意免責辯護或保護財產免責辯護，均必須合理地相信該免責辯護所訂的有關事宜。

(d) 上述有關“誤用電腦”的條文應與刑事損壞罪拆開，並納入新法例內，同時刪除《刑事罪行條例》（第 **200** 章）第 **59(1)(b)** 及 **(1A)** 條。

(e) 為網絡安全目的而非法干擾電腦數據，應有特定的免責辯護，但須符合以下條件：

(i) 被告人必須是經認可的網絡安全從業員（認可制度的細節本質上屬政策事項，最好留待政府考慮）；

(ii) 被告人必須為真正的網絡安全目的而行事；及

(iii) 在顧及整體情況後，被告人的行為必須是合理的。

第 5 章　非法干擾電腦系統

引言

5.1　本章討論關於諮詢文件建議 7 及 8 的回應。建議 7 建議訂立第四類依賴電腦網絡的罪行，即非法干擾電腦系統：

> "小組委員會建議：
>
> (a) 關於非法干擾電腦數據及非法干擾電腦系統的建議條文，應採用一致的措辭。
>
> (b) 《刑事罪行條例》（第 200 章）第 59(1A)及 60 條足以禁止非法干擾電腦系統，也應納入新法例內。
>
> (c) 新法例在適當釐清'誤用電腦'一詞（例如將'損害任何電腦的操作'的概念納入該詞）的同時，應保留現有法律的廣度，不宜過於局限。
>
> (d) 舉例來說，建議的非法干擾電腦系統罪應適用於蓄意或罔顧後果地作出以下行為的人：
>
> (i) 攻擊電腦系統（不論成功與否——刑事法律責任不應取決於干擾成功與否）；
>
> (ii) 在軟件生產時，在軟件編入缺損程式；及
>
> (iii) 在未獲授權下更改電腦系統，並知悉該項更改可能導致合法使用者不能取用或正常使用系統。"

5.2　正如諮詢文件所解釋，[1] 概括而言，非法干擾電腦系統罪旨在：

(a) 禁止藉使用或干擾電腦數據，阻礙合法使用電腦系統；

(b) 從而確保電腦系統能正常運作。

---

[1] 第 5.1 段。

香港的現行法律

5.3 鑑於非法干擾電腦數據罪與非法干擾電腦系統罪（“**干擾罪**”）息息相關，本章會在第 4 章討論的基礎上再作探討。正如第 4 章所述，[2] 根據《刑事罪行條例》（第 200 章）第 60 條，刑事損壞的其中一種形式是“誤用電腦”。第 59(1A)條把該詞界定為：

> “(a) 導致電腦並非如其擁有人或其擁有人代表對其所設定的運作方式運作，即使如此誤用不會令該電腦的操作、該電腦內的程式或該電腦內的資料的可靠性減損亦然；
>
> (b) 更改或刪抹電腦內或電腦儲存媒體內的程式或資料；
>
> (c) 在電腦或電腦儲存媒體所收納的內容上增加程式或資料，
>
> 而造成導致(a)、(b)或(c)段所提述的任何類別誤用情形的任何作為，須視為導致該項誤用情形的作為。”

這三個部分中，第 59(1A)(a)條與建議的非法干擾電腦系統罪最為相關。

5.4 正如小組委員會在諮詢文件解釋，[3] 非法干擾電腦系統可能以分布式拒絕服務攻擊這形式進行，其定義是：*“蓄意從多台獨立電腦同時向某電腦網絡發送大量數據，藉此癱瘓該電腦網絡”*。[4] 分布式拒絕服務攻擊通常藉一組被入侵的電腦發動，這組電腦稱為“殭屍網絡（botnet）”。如寄存有關網頁的伺服器的容量不足，未能回應大量電腦同時發出的相同請求，該伺服器就可能沒有反應、崩潰或發生其他故障。

對小組委員會建議 7 的回應

5.5 由於建議的非法干擾電腦系統罪與非法干擾電腦數據罪息息相關，對建議 7 的回應與對建議 6 的大致相似，我們已在第 4 章討論對建議 6 的回應。

---

2 第 4.10 段。

3 第 5.3 及 5.4 段。

4 https://www.cpaaustralia.com.au/tools-and-resources/cyber-security/cyber-threats-introduction（於 2025 年 11 月 1 日瀏覽）。

5.6 絕大多數回應者表示支持建議 7，當中香港與內地法律專業聯合會有限公司及香港女律師協會有限公司（“**女律師協會**”）同意《刑事罪行條例》的現行制度行之有效，而“誤用電腦”這概念足以涵蓋干擾電腦系統的作為。因此，女律師協會同意建議 7，認為關於非法干擾電腦系統及非法干擾電腦數據的條文，應採用一致的措辭。

罔顧後果作為建議罪行的犯罪意念元素之一

5.7 正如建議 6，多名就建議 7 提供意見的回應者，要求澄清是否會將“罔顧後果”納入為建議的非法干擾電腦系統罪的意念元素之一。數個資訊科技相關機構提出，建議的罪行應只在有“犯罪意圖”的情況下才產生，而且應摒棄建議 7 的“罔顧後果地”這項元素。

5.8 讀者會記得諮詢文件的建議 7(d)列出數個例子，說明建議的非法干擾電腦系統罪如何應用。這些例子包括在生產軟件時，某人“蓄意”或“罔顧後果地”在軟件編入缺損程式。[5] 兩個資訊科技相關團體指出，缺損程式在電腦軟件、電腦應用程式及器材十分常見。其中一個團體認為，程式開發人員推出尚未成熟的新發明，便可能導致缺損程式出現。由於測試受時間及資源所限，即使識別出保安問題，當中有些問題在程式推出前未獲軟件開發人員糾正，也不足為奇。該回應者詢問，在這種情況下，軟件開發人員會否須就建議的罪行負上法律責任。

5.9 與此同時，香港律師會認為，對罔顧後果地向電腦系統發送大量數據的行為施加刑事法律責任，需要更全面分析相關的法律依據。該專業團體引用的例子，是歌迷在網上爭相搶購演唱會門票。

我們的分析及回應

一致處理干擾數據及干擾系統

5.10 我們已在第 4 章分析以“罔顧後果”作為建議的非法干擾電腦數據罪的替代犯罪意念元素，由於干擾罪相當近似，有關分析亦同樣適用於回應者就建議 7 所提出的意見。[6]

---

[5] 建議 7(d)(ii)。

[6] 我們的分析載列於第 4.17 至 4.22 段。

5.11 概括而言，“意圖”及“罔顧後果”是現有《刑事罪行條例》第 60(1)條刑事損壞罪的替代犯罪意念元素，而憑藉第 59(1)(b)及(1A)條，刑事損壞罪的現行法定框架適用於*“誤用電腦”*。因此，建議 7 建議採納第 60 條的現行制度，以一致處理非法干擾電腦系統及非法干擾電腦數據，亦同樣採納“意圖”及“罔顧後果”作為建議的非法干擾電腦系統罪的意念元素。

5.12 我們重申在第 4 章提出的觀點：“罔顧後果”是常見且確立已久的刑事罪行過失元素。“罔顧後果”這概念要求證明被告人察覺某特定風險，而在被告人所知的情況下，承擔該風險並不合理。[7] 這項對罔顧後果的詮釋適用於整體刑事法，而非僅適用於電腦網絡罪行。至於被告人在某特定情境下干擾有關電腦系統是否罔顧後果（例如在網上購買演唱會門票，或是開發機械人顯微手術所用的軟件，這兩種情況可以大為不同），最終須由法庭根據個別案件的證據，並針對整體情況來進行評估及評定。因此，被告人的作為在甚麼情況下發生，本身並非充分理據，支持排除以罔顧後果為理由而引用建議的罪行。

5.13 恰當理解上文所解釋的“罔顧後果”概念後便會明白，程式開發人員大致知悉軟件存在缺損程式或缺陷，這一點本身並不足以確立干擾罪所需的犯罪意念元素。“罔顧後果”的門檻及所代表的罪責，比純粹不小心或一般疏忽為高。在開發軟件的情境中，多項因素與法庭評定甚麼行為會構成罔顧後果固然相關，例如軟件開發人員在質素保證方面是否遵照業界標準。眾所周知，在軟件開發期間，難免會出現一些合理地預期的缺損程式或缺陷。因此，某人購買或以其他方式取得某程式或軟件，可視為同意有關產品內一般會存有可能造成不便的瑕疵，甚至是可合理容忍的保安漏洞。正因如此，《刑事罪行條例》第 64(2)條的同意免責辯護可能有機會適用，從而免除程式開發人員負上非法干擾電腦系統罪的法律責任，而我們亦建議在新訂的電腦網絡罪行法例中為干擾罪納入這項免責辯護。[8]

5.14 基於以上理由，我們建議保留“罔顧後果”這項元素，與“意圖”一同作為非法干擾電腦系統罪的過失元素。總括而言，關於非法干擾電腦數據及非法干擾電腦系統的建議條文，應採用一致的措辭，我們亦保留這項建議。

---

7 *Archbold Hong Kong 2025*，第 16－40 段。

8 上文第 4.39 段。我們亦建議，《刑事罪行條例》第 64(2)條所示的免責辯護應適用於第 2 章所討論的非法取覽程式或數據罪（見上文第 2.95 至 2.97 段）。

有關建議 7 的結論

5.15 基於上述所有理由，加上考慮到絕大多數回應者均支持訂立非法干擾電腦系統罪（以及非法干擾電腦數據罪），我們的結論是建議 7 可予保留。

最終建議 7

我們建議：

(a) **關於非法干擾電腦數據及非法干擾電腦系統的建議條文，應採用一致的措辭。**

(b) **《刑事罪行條例》（第 200 章）第 59(1A)及 60 條足以禁止非法干擾電腦系統，也應納入新法例內。**

(c) **新法例在適當釐清 *"誤用電腦"* 一詞（例如將"損害任何電腦的操作"的概念納入該詞）的同時，應保留現有法律的廣度，不宜過於局限。**

(d) **舉例來說，建議的非法干擾電腦系統罪應適用於蓄意或罔顧後果地作出以下行為的人：**

(i) **攻擊電腦系統（不論成功與否——刑事法律責任不應取決於干擾成功與否）；**

(ii) **在生產軟件時，在軟件編入缺損程式；及**

(iii) **在未獲授權下更改電腦系統，並知悉該項更改可能導致合法使用者不能取用或正常使用有關系統。**

對小組委員會建議 8 的回應

5.16 諮詢文件建議 8(a)及(b)就以下議題徵詢意見：

"(a) 就建議的非法干擾電腦系統罪而言，如網絡安全專業人員在目標電腦的擁有人並不知情或沒有給予授權的情況下，在互聯網掃描（或以類似的形式測試）某電腦系統，例如評估潛在的保安漏洞，應否屬合法辯解？

(b) 就建議的非法干擾電腦系統罪而言，非保安專業人員應否有合法辯解，例如：

(i) 由機械人進行網頁抓取（web scraping）或由互聯網資訊收集工具（例如搜尋器）啟動網絡爬蟲（web crawlers），從而藉着連接指定的協定埠（例如 RFC6335 所界定的連接埠），在未獲授權下從伺服器收集數據；及／或

(ii) 為以下目的，掃描服務供應商的系統（從而有可能令該系統被濫用或被拖垮）：

(1) 為保障他們自身安全，找出任何保安漏洞（例如他們在以私人身分提供信用卡資料進行交易前，找出信用卡交易的加密是否安全）；或

(2) 確保該服務供應商系統所提供的應用程式界面（Application Programming Interface）安全和完整？"

建議 8(a)

5.17 明顯大多數的回應者均明確同意為網絡安全專業人員掃描（或以類似的形式測試）電腦系統提供免責辯護。部分回應者則認為無須提供這項免責辯護，並指出網絡安全專業人員如沒有清晰草擬的合約，不大可能會提供安全掃描、評估或其他服務。

5.18 香港大律師公會表示：

> "由於網絡安全專業人員及非保安專業人員可對電腦系統進行各種合法行為，以使用該系統內的選定資料或觀察所得（如識別系統漏洞），要是試圖詳盡無遺地界定在建議的罪行下可構成'合法辯解'的行為種類，並不可取……這種處理方法使法律具備必要的彈性，以便按每宗個案的情況來考慮被告專業人員的行為，使法庭得以在更多樣的情境中考慮這項免責辯護。"

建議 8(b)

5.19 相類於建議 8(a)，明顯大多數的回應者均支持為非保安專業人員提供免責辯護。

5.20 消費者委員會認為：

> "網頁抓取和網絡爬蟲（web crawling）可在互聯網上收集公開數據，在香港及世界各地甚為普遍。舉例來說，谷歌（Google）使用網絡爬蟲為其搜尋器建立網頁索引。全面禁止使用網頁抓取和網絡爬蟲在互聯網上收集公開資料，或會阻礙用作改善市場透明度、幫助消費者作出知情的消費選擇，以及加強消費者保障的調查與研究（不論該調查與研究以商業、存檔、新聞報道、學術或諮詢為目的）。"

5.21 此外，消費者委員會在回應中述明，有關數據可能受版權、網站使用條款規限，或載有個人資料，在相應範圍內收集及／或使用該等數據會受版權法、合約法及私隱法規管。如收集該等數據的方式或方法並不合法，有關行為可能會干犯建議的依賴電腦網絡罪行。

5.22 再者，由於"網頁抓取"可包括"數據抓取（data scraping）"（即某電腦程式從另一程式所產生的輸出中提取數據），個人資料私隱專員公署指出，只有"經同意"或"合法"干擾電腦系統才應構成建議罪行的免責辯護，這是因為根據該署的執法經驗：

> "數據抓取所收集的個人資料，有時會在資料當事人並不知情且沒有給予同意的情況下在暗網出售，而抓取本身已構成資料外洩事故。為加強網絡安全，我們認為未獲授權的網頁抓取（包括數據抓取）及對服務供應商

系統的未獲授權掃描，均應受建議的罪行所涵蓋，只有經同意或合法干擾電腦系統，方可構成免責辯護……”

我們的分析及回應

建議 8(a)：特定的免責辯護

為網絡安全目的而干擾電腦系統

5.23 在第 4 章，[9] 我們建議，就建議的非法干擾電腦數據罪而言，為網絡安全目的而干擾電腦數據應可作為免責辯護，其條件如下：

(a) 該項免責辯護應只適用於經認可的網絡安全從業員（認可制度的細節本質上屬政策事項，最好留待政府考慮）。

(b) 被告人必須為真正的網絡安全目的而行事。

(c) 在顧及整體情況後，被告人的行為必須是合理的。

5.24 由於兩項干擾罪息息相關，我們同樣建議，就建議的非法干擾電腦系統罪而言，為網絡安全目的而干擾電腦系統應可作為免責辯護。因此，如符合上一段所述的條件，在互聯網掃描（或以類似的形式測試）電腦系統並不屬犯法。

為保障兒童或易受傷害人士的利益而干擾電腦系統

5.25 正如第 4 章所解釋，[10] 我們認為無須為保障兒童或易受傷害人士的利益而就非法干擾電腦數據罪提供特定的免責辯護，理由如下：首先，取覽程式或數據本身並不會導致電腦數據受到干擾；其次，容許某人取覽程式或數據，並不表示該人獲授權干預有關數據。

5.26 由於上述邏輯亦適用於干擾電腦系統的情況，我們認為無須為保障兒童或易受傷害人士的利益而就非法干擾電腦系統罪設置特定的免責辯護。

---

9 我們的分析載列於第 4.34 及 4.35 段。

10 第 4.36 及 4.37 段。

為真正的研究目的而干擾電腦系統

5.27 與干擾電腦數據一樣，若從事真正研究需要干擾電腦系統，我們認為是匪夷所思的。因此，我們認為無須提供特定的免責辯護，以豁免為真正的研究目的而進行的非法干擾電腦系統行為。

改列《刑事罪行條例》第 64(2)條的免責辯護

5.28 我們重申上文第 4.39 至 4.44 段的分析。概括而言，將《刑事罪行條例》第 64(2)條的免責辯護改列於新訂的電腦網絡罪行法例時，我們建議就非法干擾電腦系統罪而對同意免責辯護及保護財產免責辯護作出以下改進：

(a) 就同意免責辯護而言，被告人必須*合理地*相信自己已獲同意或會獲同意干擾有關電腦系統；及

(b) 就保護財產免責辯護而言，被告人必須*合理地*相信有關財產需即時保護。

建議 8(b)：無須為非保安專業人員建議免責辯護

5.29 除網絡安全專業人員外，我們留意到有些活動不一定會達致網絡安全目的，但本身卻存在於電腦網絡空間的運作之中，或是電腦器材或系統之間的互動之中。正如諮詢文件建議 8(b)所提及，這些活動的例子包括網頁抓取（即利用電腦自動程式〔bots〕從網站提取內容及數據的過程）及網絡爬蟲（即為建立索引而有系統地瀏覽網頁的電腦自動程式）。

5.30 受惠於專家意見，小組委員會進一步了解到，正常使用電腦系統必然會產生流量。舉例來說，支援通訊平台（如 WhatsApp 及 Telegram）的應用程式界面會充當中介層，處理電腦系統之間的數據傳輸，從而使公司可向第三方開放其應用數據及功能。

5.31 電腦網絡空間內有不少我們認為是數碼生活中不可或缺，因而可以接受的合法活動，但是要把這些活動詳盡無遺地全數列出，是不可能的，尤其是當我們考慮到科技發展步伐之快，情況更是如此。因此，我們同意小組委員會在諮詢文件表達的觀點，即當某人選擇連接互聯網，便應視為默示同意任何在使用電腦網絡空間時可合理預期會發生的互動。舉例來說，我們一般並不預期網上用戶在向傳送對象（即另一網上用戶）發送電郵或展示網頁廣告前，須事先尋求後者的明示授權，尤其是當有關發送或展示並非惡意作出。另一例子是，

搜尋器會使用稱為網絡爬蟲的軟件，定期探測互聯網，以尋找網頁並將它們添加至索引。[11]

5.32 關於建議為非保安專業人員提供非法干擾電腦系統罪及取覽罪的免責辯護，我們有以下看法：

(1) 互聯網通訊及使用電腦均需要電腦系統之間進行一定程度的互動。我們應避免無意中使一些廣為接受的互聯網做法變成違法行為，而由於互聯網或電腦系統的正常運作所需，這些做法應予准許。

(2) 其他國家雖然制定了非法干擾電腦系統罪及非法取覽程式或數據罪，但這些國家的電腦網絡罪行法例並沒有為非保安專業人員(如操作搜尋器)提供任何特定的免責辯護。

5.33 鑑於上文所述，我們認為無須就電腦網絡空間日常運作中所遇到的非保安代理提供特定的免責辯護，因為有關情況可作為事實和程度的問題來裁斷，並應能夠與電腦網絡攻擊（例如在一分鐘內向某特定郵箱發送 10,000 封電郵，使郵箱及相應伺服器不勝負荷）區分開來。然而，若負責落實建議的決策局或法律草擬專員在立法階段認為需要就此明文訂定免責辯護，可在該階段進一步探討這議題。

最終建議 8

我們建議：

(a) 為網絡安全目的而非法干擾電腦系統，應有特定的免責辯護，但須符合以下條件：

(i) 被告人必須是經認可的網絡安全從業員（認可制度的細節本質上屬政策事項，最好留待政府考慮）；

(ii) 被告人必須為真正的網絡安全目的而行事；及

11 諮詢文件第 2.5 段。

(iii) 在顧及整體情況後，被告人的行為必須是合理的。

(b) 就建議的非法干擾電腦系統罪而言，無須為非保安專業人員提供任何特定的免責辯護（例如由機械人進行網頁抓取或由互聯網資訊收集工具啟動網絡爬蟲，從而藉着連接指定的協定埠，在未獲授權下從伺服器收集數據），理由是根據默示授權的原則，構成互聯網或電腦系統正常運作一部分的活動應繼續獲准。

第 6 章　提供或管有用作干犯電腦網絡相關罪行的器材、程式或數據

引言

6.1　本章討論關於諮詢文件建議 9 的回應。建議 9 涉及第五類（最後一類）依賴電腦網絡的罪行，即提供或管有用作犯罪的器材或數據。

"小組委員會建議：

(a) 在新法例下，蓄意提供或管有器材或數據（不論是有形物或無形物，例如勒索軟件、病毒或其源碼），如製造或改裝該器材或數據的目的是犯罪（即並非一定是電腦網絡罪行），應定為基本罪行，而合理辯解可作為法定免責辯護。

(b) 建議罪行的犯罪行為，應涵蓋供應（例如生產、提供、出售及輸出有關器材或數據）及需求（例如取得、管有、購買及輸入有關器材或數據）兩方面。

(c) 建議的罪行應適用於：

(i) 主要用作（以客觀方式界定，不論被告人的主觀意圖為何）犯罪的器材或數據，不論該器材或數據能否用作任何合法目的；及

(ii) 相信或聲稱有關器材或數據可用作犯罪的人，不論該人所信或所聲稱的是否屬實。

(d) 在新法例下，蓄意提供或管有符合以下說明的器材或數據（不論是有形物或無形物，例如勒索軟件、病毒或其源碼）：

(i) 如該器材或數據能夠用作犯罪，或犯罪者相信或聲稱該器材或數據能夠用作犯罪；及

(ii) 犯罪者意圖任何人將該器材或數據用作犯罪，

應構成加重罪行，而合理辯解可作為法定免責辯護。

(e) 建議的條文應以《英格蘭誤用電腦法令》第 3A 條，以及《新加坡誤用電腦法令》第 8 及 10 條為藍本。”

6.2 正如小組委員會在諮詢文件解釋，[1] 概括而言，就此主題而訂立的罪行，旨在：

(a) 遏制生產、供應和管有可在電腦網絡空間作非法用途的器材或數據；

(b) 藉以防止這類器材或數據被用作干犯電腦網絡罪行。

6.3 如任何人實際使用器材或數據（例如對電腦進行黑客入侵），即會構成第 2 章所討論的非法取覽程式或數據罪（“**取覽罪**”）的犯罪行為。本章着眼於一項獨立的罪行，即提供被製造或改裝以用作干犯電腦網絡相關罪行的器材、程式或數據（如黑客器材），當中包括為提供該等器材、程式或數據而管有罪。

6.4 除黑客器材外，只可作有害用途的器材、程式及數據舉例如下：[2]

(a) 存有勒索軟件的記憶棒；

(b) 惡意軟件；

(c) 病毒；

(d) 建立及管理殭屍網絡的軟件；及

(e) 收集軟件（harvesting software），這類軟件可掃描電腦來尋找特定物品（例如銀行及信用卡憑證，以及其後可用作欺詐的其他數據）。

香港的現行法律

《刑事罪行條例》（第 200 章）第 62 條

6.5 正如諮詢文件所解釋，[3] 第 59(1A)條已訂明在《刑事罪行條例》的第 VIII 部中，*“摧毀或損壞財產（to destroy or damage any property），*

---

1 第 6.1 段。
2 諮詢文件第 6.2、6.10 及 6.91 段。
3 諮詢文件第 6.6 段。

就電腦而言，包括誤用電腦”。[4] 因此，第 VIII 部第 62 條（*“管有任何物品意圖摧毀或損壞財產”*）所訂的罪行，也適用於*“誤用電腦”*：

> “任何人保管或控制任何物品，意圖在無合法辯解的情況下使用或導致他人使用或准許他人使用該物品——
>
> (a) 以摧毀或損壞屬於另一人的財產；或
>
> (b) 以摧毀或損壞該人本人或使用人的財產，而且知道所用方法相當可能會危害另一人的生命，
>
> 即屬犯罪。”

6.6 然而，第 62 條有兩個潛在主要問題，值得考慮法律改革：

(a) 第 62 條的英文文本用“anything”一詞來描述受禁物。按照一般用語，該詞並不限於有形物，且涵蓋範圍似乎比中文文本的對應詞（“任何物品”）更廣。然而，這個中文詞語的慣常涵義會否明確引伸至某些無形物（例如惡意軟件及有關利用漏洞〔exploit〕的專門知識），則是另一個問題。[5]

(b) 第 62 條與《刑事罪行條例》第 60 條所訂的刑事損壞罪相關。對於其他條文所訂罪行（例如《刑事罪行條例》第 161 條所訂的*“有犯罪或不誠實意圖而取用電腦”*罪），第 62 條並不適用。[6]

6.7 在上述背景下，小組委員會經考慮第 62 條及香港與其他司法管轄區的其他法例條文後，提出載於諮詢文件的建議 9。

對小組委員會建議 9 的回應

6.8 與第 2 至第 5 章所介紹的另外四類依賴電腦網絡的罪行相比，建議 9 在市民大眾之間引發不少爭論，支持與反對該建議的

---

[4] 《刑事罪行條例》（第 200 章）第 59(1A)(a)至(c)條中界定*“誤用電腦”*。這概念與第 4 及第 5 章所討論的非法干擾電腦數據罪及非法干擾電腦系統罪相關（見上文第 4.10 及 5.3 段）。

[5] 諮詢文件第 6.9 及 6.10 段。

[6] 諮詢文件第 6.16 段。

回應者幾乎各佔一半。眾多回應者提出意見或觀點，但沒有明確表示支持或反對訂立建議的罪行。

支持建議 9 的回應者的意見

6.9 某商會認為《刑事罪行條例》第 62 條 *"某程度上涵蓋"* 建議的罪行，該條禁止保管或控制任何物品，意圖使用以摧毀或損壞財產，即干犯《刑事罪行條例》第 60 條所訂的刑事損壞罪。該回應者同意小組委員會在諮詢文件中的分析，指出第 62 條可能會豁除無形物（如電腦軟件），無助於將該條應用於電腦網絡空間。[7]

6.10 香港公司治理公會表明支持建議 9，並同意如建議 9(e)所提議，建議的罪行可用新加坡《1993 年誤用電腦法令》（Computer Misuse Act 1993，**《新加坡誤用電腦法令》**）第 8[8] 及 10[9] 條為藍本。

反對建議 9 或對建議 9 另有意見的回應者的意見

6.11 多名回應者（特別是來自資訊科技界的回應者）反對訂立建議 9(a)的基本罪行。他們的疑慮與其他機構（包括香港律師會及消費者委員會）的意見書互相呼應，這些意見書概括就建議的罪行提出觀點。

---

7 同上，第 6.9 至 6.15 段。

8 《新加坡誤用電腦法令》第 8(1)條訂明：

"任何人在沒有權限的情況下，故意披露可取覽存於任何電腦的任何程式或數據的任何密碼、取用碼或任何其他方法，而該人作出上述作為——

(a) 是為了不當地獲益；

(b) 是為了達到任何非法目的；或

(c) 並知悉該作為相當可能會不當地導致任何人蒙受損失，

即屬犯罪。"

9 《新加坡誤用電腦法令》第 10 條訂明：

"(1) 任何人在以下情況，即屬犯罪——

(a) 該人取得或保留本條適用的任何物品——

(i) 並意圖將該物品用作干犯或用作利便干犯第 3、4、5、6 或 7 條所訂罪行；或

(ii) 以藉任何方式使該物品被供應或提供用作干犯或利便干犯任何該等罪行；或

(b) 該人以任何方式製造、供應、要約供應或提供本條適用的任何物品，意圖使該物品用作干犯或用作利便干犯第 3、4、5、6 或 7 條所訂罪行。

(2) 本條適用於以下物品：

(a) 經設計或改裝以主要用作干犯第 3、4、5、6 或 7 條所訂罪行的任何器材（包括電腦程式），或可用作干犯第 3、4、5、6 或 7 條所訂罪行的任何器材（包括電腦程式）；

(b) 可藉以取用整台電腦或其任何部分的密碼、取用碼或類似數據。"

建議罪行的基本形式性質廣泛

6.12 回應者的意見書顯示，主要關注點（不論意見書如何入手分析）均在於建議罪行的基本形式的廣度。

管有有關器材或數據的人所懷意圖

6.13 香港律師會認為，按照建議 9(a)至(e)而擬定的建議罪行：

> "極為廣泛，而檢控門檻甚低……根據有關建議，管有可能被改裝以用作犯罪（並非一定是電腦網絡罪行）的有形或無形數據，即屬犯罪。任何人如相信有關數據可用作犯罪，便會犯法。"

6.14 該專業團體舉出以下假設例子作說明：

> "……假如某方（甲方）交給另一方（乙方）一幅數碼私人照片，顯示某名人與第三方共度親密時刻，乙方理論上可以入罪，原因是：(i)該照片可用來勒索該名人，以及(ii)乙方相信該照片可用作干犯勒索罪……上述情況可能造成廣泛影響，比方說，例子中的乙方是私家偵探，甲方則是其委託人。委託人將數碼照片交給私家偵探尋求意見，私家偵探卻有機會因建議的罪行而被控告。這點令人憂慮——在這例子中，私家偵探只是為了正當做好自己的工作，才會接收數據，卻面臨被檢控的風險。為何他要承受被檢控的風險呢？"

6.15 多名來自資訊科技界的回應者認為，只有存在*"犯罪意圖"*，而*"有關工具的唯一用途是用作犯罪目的，且有關刑事作為已確實作出"*，才應產生建議的罪行。這個建議實際上要求刪除建議罪行的基本形式。

6.16 消費者委員會就建議的基本罪行闡述其關注事項，內容如下：

> "本會理解小組委員會的顧慮，假如被告人須有主觀意圖，便會需要證明被告人的主觀思想狀態，導致舉證困難。然而，如無需證明犯罪意圖，建議的基本罪行的範圍則會過於廣泛，以致消費者可能無意中犯法……建議的罪行將不考慮有關器材或數據能否作任何其他合法目的，亦不考慮管有人對使用該器材或數據的主觀

意圖，這點亦令人擔憂。舉例來說，消費者為合法目的而管有器材，假如該器材的客觀主要用途並不合法，則無論該消費者是否察覺這個主要用途，也可能會干犯建議的基本罪行。”

使用器材或數據以干犯罪行

6.17 消費者委員會及幾個資訊科技團體認為，只有有關器材或工具用作干犯第2至第5章所考慮的另外四類依賴電腦網絡的罪行[10]其中之一（而非用作干犯一般任何罪行）才應產生建議的罪行（不論是基本形式或加重形式）。

“合理辯解”作為免責辯護

6.18 根據諮詢文件的建議9(a)，建議的罪行包括合理辯解這項法定免責辯護，原因是任何人或機構可因各種合法理由處理可用作犯罪的器材或數據。[11]

6.19 消費者委員會及另外數名來自商界及資訊科技界的回應者，均支持這項法定免責辯護的範圍及適用情況應更為明確，理由是“合理辯解”並無定義，可有不同詮釋。他們當中有些回應者提議在法例中制定一份非盡列的例子清單，列舉屬於“合理辯解”免責辯護範圍的合法活動。

我們的分析及回應

背景

6.20 引入建議罪行的基本形式，源於小組委員會曾考慮《公安條例》（第245章）的管有攻擊性武器罪。在諮詢文件中，小組委員會指出：

(a) 就攻擊性武器而言，《公安條例》區分以下物品：被製造以用作造成傷害的物品、被改裝以用作造成傷害的物品，以及擬供用作上述用途的物品。在將*“攻擊性武器”*的定義應用於槍、開山刀、蝴蝶刀、裝有刺刀的雨傘，或削尖

10 即非法取覽程式或數據（第2章）、非法截取電腦數據（第3章）、非法干擾電腦數據及非法干擾電腦系統（第4及第5章）。

11 諮詢文件第6.87段。

並裝有尖釘的手杖等物品時，無須證明犯罪意圖。純粹在公眾地方管有該等物品，便足以招致刑事法律責任；[12] 及

(b) 兼具合法及非法用途的器材及數據相當常見。例如財務機構為安全起見，管有消磁器，並用它來清除舊硬碟的內容，如此這項工具是合法的。不過，如管有這項工具並意圖將它用作非法目的（例如破壞），承擔刑事法律責任則屬合理。[13]

6.21 基於上述考慮，諮詢文件的建議 9 借鏡《公安條例》的分類方法，把建議的罪行分為基本形式及加重形式。正如小組委員會所解釋，[14] 在個別案件中，除了以某器材或數據是否被製造或改裝以用作非法用途來將它們歸類之外，還應以是否有犯罪意圖作為另一區別因素，這是因為器材或數據的用途，可能隨着電腦及互聯網科技發展而改變，故單靠器材或數據是否被製造或改裝用作非法用途來定奪刑事法律責任，並不理想。

全盤處理建議罪行及相關免責辯護

6.22 從公眾諮詢收取的意見，讓我們有機會重新考慮建議 9。我們同意，將現實世界中“攻擊性武器”的現有概念移至電腦網絡世界並非直截了當的問題。與現實世界的攻擊性武器（如鐵蓮花）相比，器材、程式或數據即使被主要用作犯罪目的，也較難為人注意，而任何人亦未必了解某器材、程式或數據屬惡性。

6.23 我們在考慮建議 9 及 10 的建議罪行及相關免責辯護的廣度時，已全盤研究所有相關事項。假如擴闊建議罪行中個別元素的範圍，則可能需要調整該罪行的其他部分，又或提供適當的免責辯護或豁免，以確保該罪行不會過於寬泛。我們會在本章詳細解釋我們的最終建議。

在建議的罪行加入“程式”，即“器材、程式及數據”

6.24 這項修訂源自香港警務處的提議，該處提出將建議的罪行與第 2 章所討論的取覽罪看齊（取覽罪的刑事作為與“程式或數據”而非電腦有關聯）。由於我們建議的罪行旨在同樣禁止使用

12 同上，第 6.71 段。
13 同上，第 6.70 段。
14 同上，第 6.72 段。

實體“器材”以干犯電腦網絡罪行，[15] 我們認為“器材”應保留為建議罪行的標的之一。

6.25 儘管如此，建議罪行的目的在於打擊電腦網絡罪行，我們認為將“程式”加入為建議罪行可涵蓋的標的之一，是適當的做法。這立場亦與歐洲委員會（Council of Europe）的《電腦網絡罪行公約》（Convention on Cybercrime）第六條[16] 訂定罪行的標準相符，該條規定，各締約方應採取措施將以下行為定為刑事罪行：

> “生產、出售、為使用而獲取、輸入、分發或以其他方式提供經設計或改裝以主要用作干犯第二至五條所訂任何〔依賴電腦網絡的〕罪行的器材〔包括電腦程式〕。”
>
> （底線後加）

將建議罪行的適用範圍限於使用器材、程式或數據以干犯電腦網絡相關罪行

6.26 我們在反覆思量後提議，建議的罪行應只適用於以下情況：透過提供器材、程式或數據（或為提供該器材、程式或數據而管有它）而干犯罪行，而該罪行屬於第 2 至第 5 章所討論的另外四類依賴電腦網絡的罪行其中之一，即取覽罪、非法截取電腦數據、非法干擾電腦數據及非法干擾電腦系統（最後兩類罪行統稱“**干擾罪**”）。

背景

6.27 我們理解，小組委員會在諮詢文件提出建議 9，目標是訂立一項全面性的罪行，以防範誤用器材、程式或數據——任何人如取得或供應用作犯罪的器材、程式或數據，理論上應負法律責任。

原有建議 9 的影響

6.28 我們同意，禁止誤用是重要的合理目的，但“器材”一詞可作廣闊的詮釋，也是值得注意的問題。假如器材、程式或數據的非法用途並不局限於干犯電腦網絡罪行，則建議 9 會使建議的罪行超出電腦網絡世界，在現實世界的適用範圍更是無遠弗屆。舉例而言，如任何人撰寫電郵，試圖勒索受害人，但最終決定不送出電郵，只保留

---

15 上文第 6.2 段。

16 諮詢文件第 6.20 段。

草稿，該人也屬於管有可用作干犯“罪行”的數據，因而觸犯小組委員會建議 9 的建議罪行。

其他司法管轄區的法例

6.29 我們還注意到，在諮詢文件所討論的其他司法管轄區，電腦網絡罪行法例均一致將建議罪行的範圍限制於干犯依賴電腦網絡的罪行。[17]

6.30 由於建議 9 是因應新西蘭先有的法例[18]（即當時的《1961 年刑事罪行法令》〔Crimes Act 1961〕第 251(1)條）而制訂，我們宜詳加審視這項條文。第 251(1)條內容如下：

> “任何人（該人）如邀請他人從該人獲取任何令另一人能夠在未獲授權下取用電腦系統的軟件或其他資料，或向他人要約出售或要約供應或為向他人出售或供應而展示該軟件或資料，或同意向他人出售或供應或向他人出售或供應該軟件或資料，或為向他人出售或供應而管有該軟件或資料，而：
>
> (a) 該人知悉該軟件或資料的唯一或主要用途，是用作犯罪；或
>
> (b) 該人知悉該軟件或資料會用作犯罪，或罔顧該軟件或資料會否用作犯罪，並宣傳該軟件或資料對犯罪有用（不論該人是否也宣傳該軟件或資料對任何其他目的有用），
>
> 可處為期不超過 2 年的監禁。”
>
> （底線後加）

6.31 經過更仔細審視後，我們察覺到，該項由第 251 條所訂的新西蘭罪行的範圍實際上受一項規定所限制，即有關軟件或資料必須可令另一人能夠在未獲授權下取用電腦系統。因此，這項新西蘭罪行並非廣泛至足以涵蓋一般純粹可用來干犯 *“任何罪行”* 的軟件或

---

17 諮詢文件第 6.22 段（澳大利亞）、6.29 段（加拿大）、6.36 段（英格蘭及威爾斯）、6.43 段（中國內地）及 6.58 段（新加坡）。

18 諮詢文件第 6.74 段，小組委員會在該段表示：*“鑑於已有新西蘭法例作為先例，我們屬意新法例所禁止的器材及數據之非法用途，不應限於干犯電腦網絡罪行，而應普及地關乎任何罪行”*。

資料。第 251 條現已廢除，並經由第 254 條重新制定，儘管有所修改，上述觀察仍然適用。[19]

6.32 經進一步考慮，我們亦注意到，如任何人使用器材、程式或數據，以干犯並非電腦網絡罪行的其他一般罪行，該項構成罪責的行為可根據香港各項法定罪行及普通法罪行來處理，而無須援引針對電腦網絡罪行的特定法例。

6.33 我們留意到，將建議罪行的適用範圍局限於電腦網絡罪行，還有其他優點。除了避免我們的建議牽涉現行法律其他不只關乎電腦罪行的範疇（如“起底”、侵犯版權的罪行），以這種方式局限建議罪行的適用範圍，亦為將該罪行廣泛適用於器材、程式及數據提供額外理據。

對“電腦網絡相關罪行”的提述

6.34 在現階段，“電腦網絡相關罪行”一詞主要是指第 2 至第 5 章所討論的四類依賴電腦網絡的罪行，[20] 這些罪行連同本章所建議的罪行，組成我們的研究第一部分所考慮的主要罪行。

6.35 然而，由於電腦網絡罪行不斷迅速演變，新訂的針對電腦網絡罪行的特定法例應當具有彈性。為確保電腦網絡罪行法例能夠緊貼科技發展，我們建議該法例在附表加入電腦網絡相關罪行的清單，

---

19 第 251 條由 2025 年 7 月 31 日生效的《2025 年布達佩斯公約及相關事宜法例修訂法令》（Budapest Convention and Related Matters Legislation Amendment Act 2025）第 65 條廢除。該法令在《1961 年刑事罪行法令》新增了第 253 條及第 254 條，以便與歐洲委員會（Council of Europe）的《電腦網絡罪行公約》（稱為《布達佩斯公約》）第六條看齊。概括而言，《布達佩斯公約》第六條建議制訂罪行，針對為干犯該公約第二至第五條所載的電腦網絡相關罪行而生產、出售、提供及管有電腦軟件或資料等作為。第 253 條及第 254 條所處理的作為，均與令人能夠干犯電腦網絡相關罪行的軟件或資料有關。第 253 條針對設計、編寫或改裝更多類型軟件，即是令人能夠干犯“為不誠實目的而取用電腦系統”罪（第 249 條）、“損壞或干擾電腦系統”罪（第 250 條）及“在未獲授權下取用電腦系統”罪（第 252 條）的軟件，而第 254 條只側重於為干犯第 252 條罪行而經營或管有軟件或其他資料。一如《布達佩斯公約及相關事宜法例修訂條例草案》的註釋（Explanatory Note to the Budapest Convention and Related Matters Legislation Amendment Bill）述明：

(a) 在《布達佩斯公約》第六條關於為干犯類似於第 249 條、第 250 條及第 252 條所載的任何罪行而生產電腦程式的範圍內，第 253 條與第六條看齊；及

(b) 第 254 條大致上重塑已廢除的第 251 條的效力，而第 251 條在關於軟件及某些類別資料的範圍內大致與《布達佩斯公約》第六條看齊。為“確保更能夠與《布達佩斯公約》第六條完全看齊”，第 254 條的主要實質改動如下：(i)在舊有第 251(1)條所載罪行涵蓋的各種經營內，加入“取得相關軟件或其他資料”；以及(ii)將有關罪行延伸至涵蓋意圖使軟件或其他資料被任何其他人用作干犯罪行的人。

儘管第 251 條已廢除，並透過新的第 254 條（在有所修改下）重新制訂實質相同的罪行，但這兩項條文的範圍相同，僅限於干犯第 252 條所訂的“在未獲授權下取用電腦系統”罪這一目的。

20 即非法取覽程式或數據（第 2 章）、非法截取電腦數據（第 3 章）、非法干擾電腦數據及非法干擾電腦系統（第 4 及第 5 章）。

附表的內容可因應日新月異的社會狀況，透過立法修訂加以擴充或作其他調整。這種做法在法例普遍採用，包括《裁判官條例》（第 227 章）在附表 2 列明不可由裁判官循簡易程序處理的罪行。

6.36 在研究涵蓋借助電腦網絡的罪行的第二部分，我們會考慮還有哪些罪行（如有的話）亦應納入“電腦網絡相關罪行”的清單內，並載於針對電腦網絡罪行的特定法例的附表。

重寫建議罪行關於管有的部分

6.37 經仔細考慮，我們認為人們在日常生活中使用電腦網絡空間時，會如何與程式或數據互動，實在有太多可能性，而結果是人們可能會在各種無惡意的情況下管有惡意程式或數據。以下僅是數個例子：

(a) 某人在電腦執行防毒掃描時，可能從中得知自己管有惡意程式或數據，但防毒掃描未必能夠為一般電腦使用者提供很多關於該惡意程式或數據的性質或影響的資料。

(b) 電腦系統可能會產生自動信息，通知使用者其器材已受某東西“感染”。使用者由於怠惰，或是對電腦一無所知，可能沒有花工夫去了解或查看該電腦所匯報的問題。

(c) 在上述兩個例子中，該人儘管繼續“管有”有關惡意程式或數據，他未必有意圖使用該程式或數據以干犯電腦網絡罪行或任何其他罪行。

6.38 再者，可用作干犯電腦網絡相關罪行的器材、程式或數據所造成的危害程度各異，外行人對這些器材、程式或數據的觀感亦不同。舉例而言，殭屍裝置（bots）明顯有害，惡意垃圾電郵則可能較難辨識。我們甚至無法確定，如“殭屍裝置”（而非其他類別的惡意軟件）潛入某人的電腦，一般電腦使用者是否能夠辨識。

6.39 我們認為，只要該人並無意圖使用該程式或數據以干犯電腦網絡相關罪行（即建議罪行的加重形式），便不應純粹因管有該程式或數據而招致刑事法律責任。因此，為避免造成過度刑事化的情況，我們建議重寫建議 9(a)關於管有的部分，將有關罪行改為：*“為向他人提供被製造或改裝以用作干犯電腦網絡相關罪行的器材、程式或數據而管有它”*。

6.40　這項管有罪現經修訂後形式較為狹隘，如某人在不構成罪責的情況（包括上文第 6.37 段所討論的情況）下管有被製造或改裝以用作干犯電腦網絡相關罪行的器材、程式或數據，該罪行不會懲處該人。換言之，純粹管有而並無意圖使用或向他人提供有關器材、程式或數據，並不屬犯罪，但某人如管有有關器材、程式或數據供自用，以干犯電腦網絡相關罪行，則會招致刑事法律責任。

在建議的罪行加入額外的犯罪意念規定

6.41　正如上文所提及，[21] 我們明白難以將《公安條例》管有攻擊性武器罪的分類方法應用於電腦網絡世界，原因之一是任何人未必可準確知悉或了解某器材、程式或數據的主要用途。舉例來說，某人可能以為程式無害而下載（即該人並不了解程式屬惡性）。如程式的有害性質並非可輕易識別，又或該有害程式並非廣為人知，情況更是如此。如該人亦並無意圖讓該程式用作干犯電腦網絡相關罪行，對該人施加刑事法律責任的理據似乎令人存疑。

就器材、程式或數據的性質的所知所信等

6.42　因此我們建議，建議的罪行應加入額外的犯罪意念規定——控方必須證明被告人知悉、相信或聲稱某器材、程式或數據主要用作（以客觀方式界定）干犯電腦網絡相關罪行。由於有此規定，如某人誤解該器材、程式或數據的性質，或不知悉該器材、程式或數據主要用作犯罪用途，該人便不會因建議的罪行而須負上法律責任。

6.43　雖然上述額外的犯罪意念規定會將更高的舉證門檻加諸於控方，但我們認為加入此規定是公平合理的。畢竟，與實物（如攻擊性武器）的情況不同，法庭未必可憑目測斷定程式及數據的真實性質。

6.44　我們預期，若然爭論點在於某器材、程式或數據的主要用途，提出爭議的各方會需要援引專家證據以供裁決。舉例來說，假如某工具的設定令人能夠繞過目標電腦的任何網絡防火牆保安措施而取用有關電腦，法庭或可作出更有力的推論，指該工具的主要用途值得懷疑。相反，假如證據顯示該工具獲電腦系統管理員或網絡安全公司廣泛使用，以進行診斷測試或監察網絡保安，則可見該工具普遍用於商業用途，法庭不大可能裁定該工具的主要用途是干犯依賴電腦網絡的罪行。

21　第 6.22 段。

應否保留“提供”這項基本罪行

6.45 就為“提供”而管有而言，我們必須先考慮建議的罪行是否應規定被告人須“知悉”他人或“意圖”由他人將有關器材、程式或數據用作犯罪（即被告人必須知悉該器材、程式或數據實際擬作的用途）。訂立這項規定，實際上等同摒棄小組委員會在諮詢文件所建議的基本罪行。

6.46 引入這項規定的隱憂，是可能會導致某些有害器材、程式或數據（如特洛依木馬、[22] 殭屍程式[23] 或病毒）的供應者處於有關罪行的涵蓋範圍之外，原因是供應者如純粹在暗網提供該等器材、程式或數據，而不顧（並因而不知悉）買家意圖如何使用它們，便不會犯法。

6.47 由於建議的罪行旨在遏制供應和管有可在電腦網絡空間作非法用途的器材或數據，完全取消上述基本罪行與該目標背道而馳，因此我們認為應保留這項基本罪行，但須按上文第 6.39 及 6.42 段的建議作出修改。

替代精神意念元素：有合理理由相信某器材、程式或數據的主要用途構成罪責

6.48 我們亦留意到，就建議的罪行而言，雖然管有如電腦程式的被告人或許實際並不知悉該程式內含勒索軟件或病毒（而可用作干犯電腦網絡相關罪行），但情況可能相當可疑，足以令被告人有合理理由如此相信。被告人會如此相信，起因可能是陌生人將某程式交予被告人，要求被告人於指明日期的特定時間上載該程式至某電腦系統，以換取大額金錢報酬，但不作任何解釋；又或是被告人在並無充分理由的情況下受匿名者所託，為對方保管某程式以換取金錢報酬（即使該匿名者本應可自行保管該程式）。

6.49 我們理解加入*“有合理理由相信”*這部分作為替代過失元素，會擴闊建議的罪行，以致該罪行可能適用於例如是容易受騙而被無良罪犯操控的人。然而，我們認為，基於以下考慮因素，建議加入這項替代精神意念元素是合適的：

---

22 特洛依木馬是經下載並安裝於電腦的程式，看似無害，但實際上是惡意程式。見 https://www.techtarget.com/searchsecurity/definition/Trojan-horse（於 2025 年 11 月 1 日瀏覽）。

23 殭屍程式是在受感染的電腦上秘密啟動的程式，目的是向其他電腦發動攻擊。見 https://www.igi-global.com/dictionary/zombie-programs/69048（於 2025 年 11 月 1 日瀏覽）。

(a) *"有合理理由相信"*這項精神意念元素只適用於建議罪行的某一特定元素，即有關器材、程式或數據主要用作干犯電腦網絡相關罪行。就"提供"或"為提供而管有"的意圖以及對"管有"的知悉這兩項元素，控方仍須證明被告人具有十足的犯罪意念。換言之，儘管某人有合理理由相信其管有的器材、程式或數據被製造或改裝以用作干犯電腦網絡相關罪行，但如無法證明該人有意圖提供該器材、程式或數據，或為向他人提供該器材、程式或數據而管有它，或為自用該器材、程式或數據而管有它，該人也不干犯這項罪行。

(b) 蓄意提供用作干犯電腦網絡罪行的器材、程式或數據，以及蓄意為提供任何上述物品而管有它們，均帶有相當程度的刑責。若把*"有合理理由相信"*這部分加入為替代的定罪基礎，可提高打擊上述犯罪行為的成效。如建議的罪行規定須證明被告人對某器材、程式或數據的主要用途的實際所知所信，這項罪行的犯罪者很容易便可招募另一人作出受禁行為，而只要犯罪者沒有實際告知該另一人有關器材、程式或數據的主要用途構成罪責，主犯則可以肯定，應募者縱然被捕，也不會被裁定干犯任何罪行，即使情況大有可疑亦然（因為應募者實際並不知悉或相信有關主要用途構成罪責）。這一點意味着兩個問題。第一，人們的警覺性會減低，以致犯罪者更容易招募中間人。第二，在可疑情況下行事的人會知道，如沒有*"有合理理由相信"*這部分，他們不可能被裁定有罪，因此他們在被捕後沒有誘因向當局提供協助，以期法庭判刑時據此減刑。

(c) 隨着科技發展，任何人在任何地方干犯提供用作干犯電腦網絡相關罪行的器材、程式或數據（或為提供任何上述物品而管有它們）這項建議罪行，都變得更為容易。透過同時針對中間人以遏止這種行為，與建議罪行的更廣泛目標相符，即防止有害器材、程式或數據被用作干犯電腦網絡罪行。如任何人應當意識到某器材、程式或數據有害，透過將建議的罪行延伸至涵蓋這些人，可加強法律的阻嚇作用及效果。

(d) 一般人對於林林總總可用作干犯電腦網絡相關罪行的不良電腦程式及數據，可能並不熟悉。*"有合理理由相信"*這部分未必如一些人所想般能夠輕易引用。

(e) *"有合理理由相信"*的概念混合了主觀元素與客觀元素，[24]即：

(i) 有甚麼事實或情況（包括被告人的個人情況）是被告人知道，且可能影響他相信有關器材、程式或數據是或不是主要用作干犯電腦網絡相關罪行？

(ii) 任何明理人士若得知被告人所知道的事情，是否必然相信有關器材、程式或數據主要用作干犯電腦網絡相關罪行？

有了這個雙重驗證標準，被告人即使可被視為*"有合理理由相信"*某器材、程式或數據主要用作干犯電腦網絡相關罪行，也不會純粹因為其資訊科技能力水平而被視為有合理理由相信這事情。法庭應用上述的兩階段驗證標準時，首先必須視乎證據決定被告人主觀上知道甚麼事情，可能影響被告人相信有關器材、程式或數據的主要用途構成罪責。其後，法庭必須以客觀方式決定，任何明理人士若得知被告人所知道的事情，是否必然相信該器材、程式或數據的主要用途構成罪責。由於法庭會以被告人所知的主觀事情作為考慮基礎，*"有合理理由相信"*這部分並不會如一些人所擔憂般造成過度刑事化。很多時候，被告人在可疑情況下管有或提供有關器材、程式或數據，才會導致引用*"有合理理由相信"*這部分。

6.50 無論如何，為了在堵塞法律漏洞與避免過度刑事化的危險這兩個目標之間取得平衡，我們建議在合理辯解一般免責辯護以外，另設多項適用於建議罪行的特定免責辯護，這些免責辯護會在本章較後部分討論。

6.51 總括而言，我們建議如被告人*"有合理理由相信"*某器材、程式或數據主要用作干犯電腦網絡相關罪行，建議的罪行應同樣適用。

---

24 由香港司法學院發出的《陪審團指引》第二冊（特選課題 2020 年修訂版），第 119 章：*"處理從可公訴罪行的得益（Dealing with Proceeds of an Indictable Offence）"*，第 119-13 及 119-14 頁。

被告人只提供或管有被製造或改裝以用作干犯電腦網絡相關罪行的惡意器材、程式或數據的部分

6.52 隨着科技進步，現已可將程式或數據分散（例如在星際檔案系統〔InterPlanetary File System，“**IPFS**”〕等分散式檔案系統，或區塊鏈技術）[25] 儲存、取覽及分享。因此，犯罪者有可能只持有整體數據的一部分，而此舉本身並不屬於犯罪。然而，藉着如分散式雜湊表（Distributed Hash Tables）[26] 等索引系統，IPFS的節點能夠聚集儲存於多個地點的數據，並向任何使用 IPFS軟件的人提供合成惡意數據。

6.53 我們已仔細考慮，如某人只管有惡意器材、程式或數據的部分，是否適宜將建議的罪行應用於這種情況。我們認為：

(a) 儘管某人可能只提供或管有惡意軟件或數據當中無害的組成部分，但理論上一群人可以把惡意器材、程式或數據分成若干部分各自儲存，以攻擊關鍵基礎建設。假若分散式儲存或寄存愈趨普及，而建議的罪行卻不適用，情況似乎並不理想。

(b) 雖然在現實世界中，單一成分（如氮氣）透過與其他成分結合，既可用作合法用途（如製造肥料），也可用作非法用途（如製造爆炸品），但惡意軟件的組成部分不大可能同時是另一項無害程式或數據的組成部分。

6.54 為使法例更具彈性，我們建議改進建議 9，訂明對 *“器材、程式或數據”* 的提述包括該器材、程式或數據的部分。必須強調的是，這項修改根本上沒有改變建議罪行的性質，因為要產生刑事法律責任，控方仍須在毫無合理疑點下證明相同的犯罪意念元素，即某人如只持有某惡意器材、程式或數據的部分，該人：

(a) 知悉自己管有某器材、程式或數據（或其任何部分）；及

(b) 知悉、相信、有合理理由相信，或聲稱某器材、程式或數據（或其任何部分）主要用作干犯電腦網絡相關罪行。

---

25 關於區塊鏈的涵義，見下文註腳 48。

26 星際檔案系統的分散網絡由互連的電腦（稱為節點）組成。該些節點使用分散式雜湊表（Distributed Hash Tables，“**DHT**”），亦即是提供查詢及儲存功能的分散儲存系統，把鍵值（keys）與資料（values）配對起來。在 DHT 中，每個節點負責特定的鍵值及與之配對的資料，能夠有效地以任何鍵值檢索相應資料。見 *“What is the Interplanetary File System (IPFS), and how does it work?”*，登載於 https://cointelegraph.com/learn/what-is-the-interplanetary-file-system-ipfs-how-does-it-work（於 2025 年 11 月 1 日瀏覽）。

被告人聲稱（不論該項聲稱是否屬實）或誤信某器材、程式或數據主要用作干犯電腦網絡相關罪行

6.55 根據諮詢文件的建議 9(c)(ii)，小組委員會建議如任何人相信或聲稱某器材或數據能夠用作犯罪，不論該人所信或所聲稱的是否屬實，亦應足以構成罪行。正如諮詢文件所解釋，[27] 此立場與*香港特別行政區 訴 朱峻瑋*（*HKSAR v Chu Tsun Wai*）[28] 一致，即刑事法律責任不應取決於網絡攻擊成功與否。

6.56 我們認為，如任何人錯誤聲稱或誤信某器材、程式或數據主要用作干犯電腦網絡相關罪行，應同屬犯建議的罪行，猶如任何人即使就所販運物質的性質構成罪責的信念原來出錯，亦可被裁定干犯企圖販運危險藥物罪一樣。[29]

"合理辯解"作為法定免責辯護

6.57 我們在第 2 章分析就取覽罪諮詢所得的回應時，決定不應界定"合理辯解"一詞，讓"合理辯解"的範圍盡可能廣闊。[30] 正如我們所指出，是否存在"合理辯解"須視乎個別案件的事實和情況而定。不界定"合理辯解"一詞的好處是，法庭可按每宗個案的情況來斷定被告人的行為是否合理。這些考慮同樣適用於建議的罪行。

6.58 我們亦重申在第 2 章的觀點：嘗試在電腦網絡罪行法例中詮釋"合理辯解"，或嘗試闡明有關立法原意（例如擬定"合理辯解"的例子清單），均可能會收窄合理辯解免責辯護的範圍。[31] 倘若被告人在案中的作為或行為偏離法例中的例子所述，便會面臨法庭對其作出不利裁決的風險。此外，"合理辯解"這概念，本來就與不應視為違法的合法目的並不契合。正因如此，我們認為不宜把各種合法活動

---

27 第 6.77 段。

28 (2019) 22 HKCFAR 30，[2019] HKCFA 3，FACC 20/2018（判決日期：2019 年 2 月 1 日）。在該案中，被告人參與一次以某銀行網站為目標的分布式拒絕服務攻擊，但由於該銀行的伺服器擁有足夠的剩餘容量處理有關請求，該伺服器的其他操作並未遭受影響，因此該次攻擊並不成功。終審法院維持根據《刑事罪行條例》（第 200 章）第 59(1A)(a)條對被告人所作的定罪。見諮詢文件第 5.10 至 5.12 段。

29 《危險藥物條例》（第 134 章）第 4(1)條規定，任何人不得為其本人或代表不論是否在香港的其他人士：

"(a) 販運危險藥物；

(b) 提出販運危險藥物或提出販運他相信為危險藥物的物質；或

(c) 作出或提出作出任何作為，以準備販運或目的是販運危險藥物或他相信為危險藥物的物質。"

《刑事罪行條例》第 159G(1)條規定，*"如任何意圖犯本條所適用的罪行的人作出的某項作為已超乎只屬犯該罪行的預備作為者，則該人即屬企圖犯該罪行"*。

30 上文第 2.32 段。

31 同上。

歸入合理辯解免責辯護的範圍，反而較適宜把這些活動訂明為法定免責辯護，即表明有關活動並不構成罪行。[32]

6.59 故此，我們認為無須提供一份非盡列的例子清單，列舉會屬於建議罪行的“合理辯解”一般免責辯護範圍內的合法活動。

6.60 正如諮詢文件所提及，[33] 其他司法管轄區草擬的罪行差異甚大，顯示多種不同的可能性。除了我們在前文所解釋對建議罪行的修改外，我們建議採納英格蘭及威爾斯《誤用電腦法令》(Computer Misuse Act) 第 3A 條，[34] 以及《新加坡誤用電腦法令》第 8 及 10 條作為基礎，並加以改進該等條文，以制訂針對電腦網絡罪行的特定法例中的罪行。

6.61 須注意的另一重點是，無論如何，控方時刻有責任就眾多可循簡易程序審訊的可公訴罪行(不論它們是由成文法規訂立還是根據普通法訂立)選定審訊法庭。控方須考慮的主要因素包括：指稱罪行的嚴重程度、整體案情，以及定罪後可能判處的刑罰。[35] 因此，儘管有關加重罪行是可公訴罪行，但如根據案情有此需要，控方仍可選擇在裁判法院循簡易程序審訊該罪行。

有關建議 9 的結論

6.62 基於上文所述，我們的結論是建議 9 應修改如下：

最終建議 9

(a) 在新法例下，蓄意提供被製造或改裝以用作干犯電腦網絡相關罪行[36] 的器材、程式或數據(或其

---

32 上文第 2.33 段。

33 第 6.88 段。

34 英格蘭及威爾斯《誤用電腦法令》第 3A 條內容如下：

"(1) 任何人製造、改裝、供應或要約供應任何物品，並意圖使該物品用作干犯(或用作協助干犯)第 1、3 或 3ZA 條所訂罪行，即屬犯罪。

(2) 任何人供應或要約供應任何物品，並相信該物品相當可能會用作干犯(或用作協助干犯)第 1、3 或 3ZA 條所訂罪行，即屬犯罪。

(3) 任何人取得任何物品，並——

(a) 意圖將該物品用作干犯(或用作協助干犯)第 1、3 或 3ZA 條所訂罪行；或

(b) 以使該物品被供應用作干犯(或用作協助干犯)第 1、3 或 3ZA 條所訂罪行，即屬犯罪。

(4) 在本條中，'物品'包括以電子形式所存的任何程式或數據。"

35 香港特別行政區律政司，《檢控守則》(2013 年)，第 8.4 段。其他因素包括：可能有爭議的事宜、須予裁定的爭議事宜是否涉及社會的標準及／或價值觀、法律程序對公眾的重要性，以及任何加重或減輕刑罰的因素。

36 即非法取覽程式或數據、非法截取電腦數據、非法干擾電腦數據及非法干擾電腦系統。

部分），或蓄意為提供該器材、程式或數據而管有它，不論它是有形物或無形物（例如勒索軟件、病毒或其源碼），應定為基本罪行，而合理辯解可作為法定免責辯護。

(b) 建議罪行的犯罪行為，應涵蓋供應（例如生產、提供、出售及輸出有關器材、程式或數據）及需求（例如取得、管有、購買及輸入有關器材、程式或數據）兩方面。

(c) 建議的罪行應適用於主要用作（以客觀方式界定）干犯電腦網絡相關罪行的器材、程式或數據（或其部分），不論該器材、程式或數據是否亦可能用作任何合法目的。

(d) 建議罪行的犯罪意念規定為：

(i) 某人知悉自己提供某器材、程式或數據（或其部分），或知悉自己為提供該器材、程式或數據（或其部分）而管有它；及

(ii) 某人知悉、相信、有合理理由相信，或聲稱某器材、程式或數據（或其部分）主要用作干犯電腦網絡相關罪行。

(e) 某人如聲稱（不論該項聲稱是否屬實）或誤信某器材、程式或數據主要用作干犯電腦網絡相關罪行，亦應屬犯罪，猶如任何人即使就所販運物質的性質構成罪責的信念原來出錯，亦屬干犯企圖販運危險藥物罪一樣。

(f) 在新法例下，蓄意提供被製造或改裝以用作干犯電腦網絡相關罪行的器材、程式或數據（或其部分），或蓄意為提供該器材、程式或數據而管有它，不論它是有形物或無形物（例如勒索軟件、病毒或其源碼），在以下情況下應構成加重罪行，而合理辯解可作為法定免責辯護：

(i) **該器材、程式或數據能夠用作干犯電腦網絡相關罪行，或犯罪者知悉、相信[37] 或聲稱該器材、程式或數據能夠用作干犯電腦網絡相關罪行；及**

(ii) **犯罪者意圖任何人將該器材、程式或數據用作干犯電腦網絡相關罪行。**

(g) **在新法例下，蓄意管有器材、程式或數據（或其部分），在以下情況下應構成加重罪行，而合理辯解可作為法定免責辯護：**

(i) **該器材、程式或數據能夠用作干犯電腦網絡相關罪行，或犯罪者知悉、相信[38] 或聲稱該器材、程式或數據能夠用作干犯電腦網絡相關罪行；及**

(ii) **犯罪者意圖將該器材、程式或數據用作干犯電腦網絡相關罪行。**

(h) **除上述另有規定外，建議的條文應以英格蘭及威爾斯《誤用電腦法令》第 3A 條，以及新加坡《誤用電腦法令》第 8 及 10 條為藍本。**

建議罪行的免責辯護：建議 10

6.63 諮詢文件建議 10 邀請公眾就以下問題提交意見書：

"(a) 就蓄意提供或管有電腦數據（軟件或源碼）這項罪行而言，如該數據只可用作進行網絡攻擊（例如是勒索軟件或病毒），應否有免責辯護或豁免？

(b) 如(a)段的答案是'應該'的話，

(i) 上述免責辯護或豁免應在甚麼情況下可用，並應有甚麼條款？

---

37 包括某人有合理理由相信該器材、程式或數據能夠用作干犯電腦網絡相關罪行的情況。

38 同上。

(ii) 這種獲豁免的管有應否受到規管，以及如應該的話，有甚麼規管規定？”

對小組委員會建議 10 的回應

為網絡安全目的提供免責辯護或豁免

6.64 對於為網絡安全目的而提供或管有有害器材、程式或數據，大部分就建議 10 發表意見的回應者均支持就此提供免責辯護或豁免。支持者包括香港女律師協會有限公司、香港女工商及專業人員聯會（“**女工商專聯**”）、多個資訊科技相關團體，以及來自商界的回應者。

6.65 某資訊科技相關團體在回應中表示：

> “就管有只可用作進行網絡攻擊的電腦數據而言，如管有該等數據的個人或機構直接涉及所管有數據的相應範疇，則可能需要有免責辯護。舉例來說，開發防毒方案的公司必須管有病毒軟件。”

6.66 香港公司治理公會及女工商專聯均提議，如管有犯罪器材或軟件是為了進行獲授權的網絡攻擊，以測試電腦系統是否完整或安全，應獲提供免責辯護。

為教育或研究目的提供免責辯護

6.67 一如網絡安全免責辯護，回應者普遍支持為教育或研究目的而提供特定的免責辯護。大律師公會認為需要另設一項免責辯護，原因是“合理辯解”一般免責辯護取決於一般明理的人所信之事的客觀標準，很可能無法顧及某人對任何數據的具體知識或了解。

6.68 大律師公會繼而提出以下意見：

> “由於援引這項免責辯護的被告人相當可能會聲稱管有有關數據是其工作不可或缺的部分（例如為開發防毒軟件而進行研究）……對使用這項免責辯護的任何限制，應根據被告人在從事有關活動（如研究）的‘通常過程中’所作出的管有來制定。”

我們的分析及回應

6.69 讀者會記得，上述回應者建議為網絡安全及教育或研究目的提供的免責辯護或豁免，與我們在第 2 章為取覽罪，以及在第 4 及第 5 章為干擾罪所考慮訂立的特定免責辯護互相呼應。

6.70 我們同意應制定類似的免責辯護，以顧及為網絡安全、教育、科學、研究及其他合法目的而提供或管有有害器材、程式或數據的情況。此舉可確保建議的罪行只會阻遏非法供應及管有不良器材、程式或數據。

為網絡安全目的提供有害器材、程式或數據（或為了為網絡安全目的提供該器材、程式或數據而管有它）

6.71 正如第 2 及第 4 章所討論，[39] 我們建議經認可的網絡安全從業員如為真正的網絡安全目的而行事，就取覽罪及干擾罪而言，他們應有特定的免責辯護或豁免，而認可制度的細節將由政府考慮。在顧及整體情況後，被告人的目的和行為必須是合理的。

6.72 我們同意，上述的免責辯護條件可同樣轉移到建議罪行的網絡安全免責辯護。

6.73 然而，建議罪行的網絡安全免責辯護有必要增加一個額外部分。就取覽罪及干擾罪而言，取覽和干擾電腦數據及／或取用和干擾電腦系統的作為由經認可的網絡安全從業員作出。反之，器材、程式或數據可由經認可的網絡安全從業員以外的人管有或提供。舉例來說，在開發防毒軟件的公司，其技術人員、銷售員及其他非專業人員的僱員在履行職務期間也可能管有電腦病毒。

6.74 因此，我們建議，就建議的罪行而言，網絡安全免責辯護應延伸至網絡安全從業員以外，以涵蓋獲網絡安全從業員事先批准或授權，為網絡安全目的而管有或提供器材、程式或數據的人。我們的用意是，只有“事先”給予批准或授權，建議的免責辯護才會適用，原因是這安排會對網絡安全從業員施加積極主動的責任，批准或授權適當人選持有具潛在危險的器材、程式或數據，以給予公眾更佳保障。

6.75 我們希望補充，視乎整體網絡安全認可制度如何設立（正如我們在第 2 章所解釋，[40] 這是由政府決定的事宜）：

---

39 第 2.63 至 2.74 段、4.34 段及 4.35 段。

40 第 2.67 至 2.70 段。

(a) 認可制度所訂明的任何行為守則或詳細規則或需制定條文，規管網絡安全從業員適當地批准取用或取覽具潛在危險的器材、程式或數據，向為發展或推動網絡安全而需要取用或取覽該等器材、程式或數據的人給予批准；及

(b) 在網絡安全認可制度下經認可實體不一定是自然人，也可以是法人團體（如網絡安全公司）。因此，如何適當地批准負責執行相關工作的個別人員取用或取覽具潛在危險的器材、程式或數據，會是需要考慮的問題。

為教育、科學或研究目的提供有害器材、程式或數據（或為上述目的提供該器材、程式或數據而管有它）

6.76 我們同意回應者所言，建議的罪行應有為教育或研究目的而設的免責辯護，而且該免責辯護不應只適用於網絡安全業內人士。舉例來說，“教育目的”這部分會保障電腦科學領域的教師及學生，“科學”及“研究”這兩部分則涵蓋為自行研究而取得或製造有害電腦程式（例如特洛依木馬）的業餘愛好者。

6.77 我們理解到，從事電腦科學研究可出於善意或惡意，例如某項研究的目的既可以是展示如何抵禦電腦病毒，也可以是展示如何對另一電腦系統進行黑客入侵。我們認為，法律應留有空間，以促進對有害器材、程式或數據的研究，因此為教育、科學或研究目的提供有害器材、程式或數據（或為上述目的提供該器材、程式或數據而管有它），應獲提供免責辯護，否則便會窒礙對惡意軟件的分析，無法造福社會。此外，網絡安全從業員起初通常是業餘愛好者或電腦奇才。提供特定的免責辯護是合理之舉。

6.78 至於第 2 章的取覽罪，我們建議，為研究目的而取覽程式或數據應屬合理，而該取覽不得超過為達到有關教育、科學或研究目的而所需者。[41] 這項合理性要求會作為客觀準則，用以裁定被告人的取覽是否適度或合理，從而預防濫用。

6.79 同樣地，為教育、科學或研究目的提供有害器材、程式或數據（或為上述目的提供該器材、程式或數據而管有它）這項建議罪行的免責辯護，也應加入合理性要求。基於這點，我們相信這項特定的免責辯護所帶來的好處，定會大於其潛在害處。如被告人並非為真正

41 第 2.94 段。

的教育、科學或研究目的而行事，控方應可援引證據，證明被告人的犯罪意圖。

其他特定的法定免責辯護

不建議為保障兒童或易受傷害人士的利益而提供免責辯護

6.80 我們在第 2 章建議，為保障兒童或易受傷害人士的利益而取覽程式或數據，應有免責辯護。[42] 另一方面，這項關於家長監護的免責辯護並不適用於第 4 及第 5 章所討論的干擾罪，原因是准許某人取覽程式或數據，並不表示該人會獲授權更改有關數據。[43]

6.81 為保障兒童或易受傷害人士的利益會需要提供主要用作干犯電腦網絡相關罪行的器材、程式或數據（或為提供該器材、程式或數據而管有它），我們認為是匪夷所思的。因此，我們認為無須為保障兒童或易受傷害人士的利益而就建議的罪行提供特定的免責辯護。

為互聯網服務提供者提供免責辯護

6.82 互聯網服務提供者為個人及機構提供互聯網連接及相關服務（如網頁寄存）。透過互聯網服務提供者的伺服器傳送的內容通常會被加密，但經第三方通知，互聯網服務提供者能夠得知源自其網絡的內容。一般而言，互聯網服務提供者在日常運作中會收到大量關於其網絡載有指稱違法內容的通知。

6.83 然而，由於互聯網服務提供者所分配的互聯網規約地址可能寄存多個網站及 URL，[44] 要使有害網站、程式或數據不能被接達並非總是可行，因為此舉可能擾亂向其他互聯網使用者提供的服務。

6.84 上文段落所述的互聯網服務提供者之運作方式，意味着互聯網服務提供者可蓄意提供虛假網站（如偽冒銀行網站），此舉明顯是干犯電腦網絡罪行的手段。考慮到互聯網服務提供者的處境，我們建議以《數位服務法案》（Digital Services Act）第 4 條所訂的純導管免責辯護（mere conduit defence）為藍本，為互聯網服務提供者提供免責辯護。該法案在 2022 年由歐洲聯盟（“**歐盟**”）部長理事會通過，是歐盟

---

42 第 2.81 至 2.91 段。

43 第 4.36 及 5.25 段。

44 URL 是指“劃一資源定位址”，是獨一無二的識別碼或網址，用來尋找互聯網資源。見 https://www.techtarget.com/searchnetworking/definition/URL（於 2025 年 11 月 1 日瀏覽）。

數碼規管策略的重要一環，目的是將法律框架現代化，締造更安全的數碼環境。[45]

6.85 為使新訂的電腦網絡罪行法例更具彈性，以應對電腦網絡世界的各種情況，我們認為參考如《版權條例》（第 528 章）第 65A(2)條中“服務提供者”那般廣闊的定義會有幫助。該條訂明“服務提供者”是*“藉電子設備或網絡（或同時藉兩者），提供任何聯線服務或為任何聯線服務操作設施的人”*。根據第 65A(2)(a)至(c)條，“聯線服務”包括：

(a) 傳送使用者所選擇的資料或材料，或為該資料或材料作出路由選擇，或為該資料或材料的數碼聯線通訊提供連接，而該等數碼聯線通訊，是在使用者指明的超過一個點之間或之中進行的；

(b) 寄存使用者能接達的資料或材料；及

(c) 在使用者能接達的系統或網絡儲存資料或材料。

6.86 透過採納第 65A(2)條中“服務提供者”的廣闊定義，我們所建議的免責辯護可涵蓋大大小小的服務提供者，以及設立網上空間（例如論壇或網站）以寄存或儲存程式或數據的個人。

6.87 總括而言，我們建議“服務提供者”如證明以下事項，即為免責辯護：

(a) 它並無啟動傳送有關器材、程式或數據（統稱“**違法內容**”）；

(b) 它並無選定該項傳送的接收人；及

(c) 它並無選定或修改該項傳送所載的違法內容。

---

45 《數位服務法案》的涵蓋範圍廣闊，多方面規管數位服務，包括關於網上內容及服務的法律責任。《數位服務法案》第 4(1)條內容如下：

“凡提供資訊社會服務，而該服務包含在通訊網絡傳送服務對象所提供的資訊，或包含提供途徑接達通訊網絡，有關服務提供者無須為所傳送或接達的資訊承擔法律責任，前提是該提供者：

(a) 並無啟動該項傳送；

(b) 並無選定該項傳送的接收人；及

(c) 並無選定或修改該項傳送所載的資訊。”

為儲存及／或發布器材、程式或數據提供免責辯護

6.88 互聯網服務提供者只是眾多類別的網上服務提供者之一。在數碼時代，寄存服務提供者、雲端服務提供者及數據儲存設施均提供各種各樣的互聯網服務。為使針對電腦網絡罪行的特定法例臻於完善，而又不會令該法例不必要地複雜化，我們認為適宜借鑑《數位服務法案》第 6 條[46] 訂立免責辯護，以針對“服務提供者”的服務包括“儲存”及／或“發布”服務對象所提供的器材、程式或數據的情況。這種處理方式既涵蓋所有上述服務提供者，又無須將它們加以區別。

6.89 正如我們在上文所指出，[47] 服務提供者移除違法內容或使違法內容不能被接達，並非總是技術上可行，因為會造成連鎖效應，影響其他使用者。為解決這項實際困難，我們建議服務提供者如已在合理地切實可行的範圍內盡快就存在違法內容向執法機關備案，應獲免除對提供該違法內容所負的刑事法律責任。

6.90 此外，我們建議 *“提供被製造或改裝以用作干犯電腦網絡相關罪行的器材、程式或數據”* 這項犯罪行為，應包括提供途徑接達（不論以直接或間接方式）有害器材、程式或數據。舉例來說，惡意程式或數據可能嵌入到超連結，或是服務提供者寄存超連結，純粹提供途徑接達另一個載有惡意程式或數據的網上位置。在後者情況，該惡意程式或數據並非由服務提供者儲存。在我們看來，建議的免責辯護也應涵蓋這種情況。

6.91 基於上文所述，我們建議凡任何服務提供者的服務包括儲存及／或發布服務對象所提供的器材、程式或數據，而該服務提供者察覺或有合理理由相信，服務對象已提供違法內容或已提供途徑接達（不論是以直接或間接方式）該違法內容，則該服務提供者如證明以下事項，即為免責辯護：

---

46 《數位服務法案》第 6(1)條內容如下：

“凡提供資訊社會服務，而該服務包含儲存服務對象所提供的資訊，有關服務提供者無須為應服務對象要求而儲存的資訊承擔法律責任，前提是該提供者：

(a) 實際上並不知悉違法活動或違法內容，而就損害賠償申索而言，該提供者並不察覺明顯可見該違法活動或違法內容的事實或情況；或

(b) 知悉或察覺上述事宜後，已迅速行事移除該違法內容或使該違法內容不能被接達。”

47 上文第 6.83 段。

(a) 它知悉或有合理理由相信上述事宜後，已在合理地切實可行的範圍內盡快移除該違法內容或使該違法內容不能被接達；或

(b) （如移除該違法內容或使該違法內容不能被接達，在技術上不可行或並不合理地切實可行）它已在合理地切實可行的範圍內，就存在該違法內容盡快向執法機關備案。

6.92 我們希望補充，建議訂定上述免責辯護，基礎在於服務提供者與服務對象是不同的人。無論如何，如犯罪者本人寄存儲存服務，並在該處存放違法內容，藉以分享惡意器材、程式或數據，該犯罪者即使辯稱自己是“服務提供者”，以求免除任何關於主動提供惡意軟件的刑事法律責任，也不會得逞。這是因為該犯罪者一開始便知悉有關違法內容，因而不符合免責辯護的首項條件（即在合理地切實可行的範圍內盡快移除該違法內容）。

以自動化科技提供器材、程式或數據的免責辯護

6.93 我們亦留意到，現今科技發展使有害器材、程式或數據能夠透過自動化程序來提供或發布。舉例來說，我們預計會出現以下情況：用來分發數據的自動化程序、工具或科技（如區塊鏈[48] 或電腦自動程式〔internet bot〕）本身可能無害，但該程序、工具或科技被犯罪者以惡意器材、程式或數據（如病毒或惡意流動應用程式）玷污，而該區塊鏈或電腦自動程式繼而將惡意材料自動分發出去。

6.94 在上述情境，任何人如察覺到惡意器材、程式或數據，但沒有停止參與自動化程序或科技（例如沒有中斷區塊鏈節點與該人的硬碟之間的連接），*表面上*即屬干犯建議的罪行。我們有以下觀點：

(a) 如怠惰或對電腦一無所知的人沒有中斷區塊鏈節點的連接，便須承擔刑事法律責任，法律未免過於嚴苛。

(b) 區塊鏈或其他相當普及的自動化科技（如比特幣區塊鏈及Spotify）可能廣泛為人使用，終止自動化程序未必切實可行或恰當。

---

48 區塊鏈是由電腦網絡節點共用的分散式數據庫或分類帳，最廣為人知的是它們在加密貨幣系統的關鍵作用，以維持安全而分散的交易紀錄，但其用途不限於加密貨幣。區塊鏈可用於任何行業的數據，使該些數據不可竄改。見 https://www.investopedia.com/terms/b/blockchain.asp（於 2025 年 11 月 1 日瀏覽）。

6.95 在上述情況下，我們認為任何使用自動化程序、工具或科技的人，只要沒有主動或有意採取任何步驟以提供任何有害器材、程式或數據，為該人提供免責辯護是公平的。這項免責辯護的要點是該人並非自願作出有關犯罪行為，即提供用作干犯電腦網絡相關罪行的器材、程式或數據（或為提供該器材、程式或數據而管有它）。隨着科技繼續演變，或會出現區塊鏈及電腦自動程式的替代品。因此，建議的免責辯護應以一般通用的方式擬定，而非具體述明任何科技。

6.96 總括而言，我們建議凡某些違法內容純粹藉某自動化程序、工具或科技而提供，則任何人如證明以下事項，即為免責辯護：

(a) 他並無蓄意參與設計、製作或產生上述違法內容；及

(b) 他並無蓄意參與使上述違法內容成為該自動化程序一部分的過程。

有關建議 10 的結論

6.97 對於建議罪行的各項特定免責辯護，我們的建議概述如下：

最終建議 10

我們建議，除合理辯解可作為法定免責辯護外，提供用作干犯電腦網絡相關罪行的器材、程式或數據罪（或為提供用作干犯電腦網絡相關罪行的器材、程式或數據而管有罪）應有以下特定的免責辯護：

(a) 為網絡安全目的提供有關器材、程式或數據（或為了為網絡安全目的提供該器材、程式或數據而管有它）：

(i) 這項免責辯護應只適用於為真正的網絡安全目的而行事的經認可網絡安全從業員（其資格會根據政府所設立的制度認可）；

(ii) 在顧及整體情況後，該網絡安全從業員的目的和行為必須是合理的；及

(iii) 這項免責辯護應延伸至：

(1) 獲網絡安全從業員事先批准或授權，為網絡安全目的而管有或提供該器材、程式或數據的人；及

(2) 協助網絡安全從業員履行其專業職務的人。

(b) 為真正的教育、科學或研究目的提供有關器材、程式或數據（或為了為真正的教育、科學或研究目的提供該器材、程式或數據而管有它）。在顧及整體情況後，援引這項免責辯護的人的行為必須是合理的。

(c) 以歐洲聯盟《數位服務法案》（**Digital Services Act**）第 **4** 條為藍本，規定凡任何互聯網服務提供者[49]作為提供有關器材、程式或數據（或為提供該器材、程式或數據而管有它）的純導管，則該提供者如證明以下事項，即為免責辯護：

(i) 它並無啟動傳送該器材、程式或數據（“違法內容”）；

(ii) 它並無選定該項傳送的接收人；及

(iii) 它並無選定或修改該項傳送所載的違法內容。

(d) 以《數位服務法案》第 **6** 條為藍本，規定凡任何服務提供者[50] 的服務包括儲存及／或發布服務對象所提供的器材、程式或數據，而該服務提供者察覺或有合理理由相信，服務對象已提供違法內容或已提供途徑接達（不論以直接或間接方式）該違法內容，則該服務提供者如證明以下事項，即為免責辯護：

---

49 我們建議採納如《版權條例》（第 528 章）第 65A(2)條中“服務提供者”那般廣闊的定義，以涵蓋大大小小的服務提供者，以及設立網上空間（例如論壇或網站）以寄存或儲存程式或數據的個人。見上文第 6.85 及 6.86 段。

50 同上。

(i) 它知悉或有合理理由相信上述事宜後，已在合理地切實可行的範圍內盡快移除該違法內容或使該違法內容不能被接達；或

(ii) （如移除該違法內容或使該違法內容不能被接達，在技術上不可行或並不合理地切實可行）它已在合理地切實可行的範圍內，就存在該違法內容盡快向執法機關備案。

(e) 凡違法內容純粹藉某自動化程序、工具或科技而提供，則任何人如證明以下事項，即為免責辯護：

(i) 他並無蓄意參與設計、製作或產生該違法內容；及

(ii) 他並無蓄意參與使該違法內容成為該自動化程序一部分的過程。

第 7 章　香港法庭行使司法管轄權的準則

引言

7.1　本章討論關於建議 11 至 15 的回應，該等建議載列對於第 2 至 6 章所建議的五類依賴電腦網絡的罪行，香港法庭行使司法管轄權的準則。

"建議 11

小組委員會建議，在以下情況下，就建議的非法取覽程式或數據罪，香港的法庭應具有司法管轄權：

(a) 就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）在香港發生，即使其他有關作為、不作為或事情在其他地方發生；

(b) 受害人（目標電腦的擁有人、有關數據的擁有人或兩者皆是）是香港永久性居民、通常居於香港的人或在香港經營業務的公司；

(c) 目標電腦、程式或數據處於香港；或

(d) 犯罪者的作為，已導致或可能導致對香港的嚴重損害（例如導致對香港的基礎建設或公共機構的嚴重損害，或已威脅或可能威脅香港的安全），

惟須符合以下規定：如犯罪者因其在香港境外所作的作為而被控這項簡易程序罪行，該作為本身或連同就這項香港罪行定罪而須予以證明的其他有關作為、不作為或事情，須在該作為作出的司法管轄區構成罪行。

建議 12

小組委員會建議，在以下情況下，就建議的非法截取電腦數據罪，香港的法庭應具有司法管轄權：

(a) 就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生

的任何後果）在香港發生，即使其他有關作為、不作為或事情在其他地方發生；

(b) 受害人是香港永久性居民、通常居於香港的人或在香港經營業務的公司；

(c) 目標電腦、程式或數據處於香港；或

(d) 犯罪者的作為，已導致或可能導致對香港的嚴重損害（例如導致對香港的基礎建設或公共機構的嚴重損害，或已威脅或可能威脅香港的安全）。

建議 13

小組委員會建議，在以下情況下，就建議的非法干擾電腦數據罪（包括基本形式及加重形式），香港的法庭應具有司法管轄權：

(a) 就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）在香港發生，即使其他有關作為、不作為或事情在其他地方發生；

(b) 受害人是香港永久性居民、通常居於香港的人或在香港經營業務的公司；

(c) 目標程式或數據處於香港；或

(d) 犯罪者的作為，已導致或可能導致對香港的嚴重損害（例如導致對香港的基礎建設或公共機構的嚴重損害，或已威脅或可能威脅香港的安全）。

建議 14

小組委員會建議，在以下情況下，就建議的非法干擾電腦系統罪（包括基本形式及加重形式），香港的法庭應具有司法管轄權：

(a) 就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）在香港發生，即使其他有關作為、不作為或事情在其他地方發生；

(b) 受害人是香港永久性居民、通常居於香港的人或在香港經營業務的公司；

(c) 目標電腦處於香港；或

(d) 犯罪者的作為，已導致或可能導致對香港的嚴重損害（例如導致對香港的基礎建設或公共機構的嚴重損害，或已威脅或可能威脅香港的安全）。

建議 15

小組委員會建議，在以下情況下，就建議的提供或管有用作犯罪的器材或數據罪，香港的法庭應具有司法管轄權：

(a) 就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）在香港發生，即使其他有關作為、不作為或事情在其他地方發生，例如實際身處香港的人在暗網上提供用作犯罪的器材或數據；

(b) 犯罪者是香港永久性居民、通常居於香港的人或在香港經營業務的公司；或

(c) 犯罪者的作為，已導致或可能導致對香港的嚴重損害（例如導致對香港的基礎建設或公共機構的嚴重損害，或已威脅或可能威脅香港的安全）。”

與電腦網絡罪行相關的司法管轄權事宜

7.2 正如小組委員會在諮詢文件解釋，[1] 在電腦網絡空間發動跨司法管轄區的襲擊，資金門檻和技術門檻並不高，這也是電腦網絡罪行通常涉及多個司法管轄區的部分原因。表面看來是某國家內的電腦網絡罪行案件，亦可能涉及（例如）：

(a) 在另一司法管轄區的互聯網伺服器；或

(b) 總部設於另一司法管轄區的服務提供者（例如社交媒體或通訊軟件的營運者）。

---

[1] 第 7.15 段。

7.3 有鑑於此，新訂的特定法例需要應付電腦網絡罪行在司法管轄權方面所帶來的獨特挑戰。諮詢文件以*香港特別行政區 訴 黃得強*（*HKSAR v Wong Tak Keung*）展開討論。[2] 終審法院在該案確認，法庭的刑事司法管轄權受地域所限這一般原則，*"可經法律修改"*。[3] 故此，例如《刑事司法管轄權條例》（第 461 章）第 3 條規定，就任何甲類罪行而言，只要任何*"有關事情"*，或即是說：

> "就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）"

在香港發生，即使該罪行的其他主要元素在香港以外的任何地方發生，任何人亦可因犯該甲類罪行而被判有罪。

普遍獲接受的域外管轄權基礎

7.4 小組委員會的比較研究進一步顯示，國際慣例是各司法管轄區在合理範圍內，為其法律的域外應用訂定條文，這與普通法一般奉行屬地管轄原則的做法一致。[4] 就此，域外管轄權有四項普遍獲接受的基礎：

(a) 主動屬人管轄原則（建基於犯罪者的國籍）；

(b) 被動屬人管轄原則（建基於受害人的國籍）；

(c) 普遍管轄原則，即任何國家對最嚴重的罪行（例如違反人道罪）應具有司法管轄權；及

(d) 保護管轄原則，即一個國家對威脅其國家安全或利益的作為（即使該作為在該國以外發生）應具有司法管轄權。[5]

---

2 第 7.9 段。

3 (2015) 18 HKCFAR 62，第 75 頁（第 29 段），FACC 8/2014（判決日期：2015 年 1 月 9 日）。見諮詢文件第 7.9 段。

4 諮詢文件第 7.68 段。

5 Alisdair A Gillespie, *Cybercrime: Key Issues and Debates* (Routledge, 2016)，第 23 頁；類似看法見 Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press, 2007)，第 5.27 段。

電腦網絡罪行司法管轄權規則的五種事實情況

7.5 小組委員會認為香港適宜依循國際慣例，遂參照以下事實情況，就建議的五類依賴電腦網絡的罪行制訂司法管轄權規則：[6]

(a) 罪行的任何“主要元素”[7] 在香港發生，即使其他“主要元素”在其他地方發生；[8]

(b) 犯罪者是“香港人”；

(c) 受害人是“香港人”；

(d) 目標電腦、程式或數據處於香港；及

(e) 犯罪者的作為，已導致或可能導致對香港的嚴重損害（例如導致對香港的基礎建設或公共機構的嚴重損害，或已威脅或可能威脅香港的安全）。

7.6 小組委員會最終結論是，鑑於電腦網絡罪行通常涉及多個司法管轄區，建議的五類依賴電腦網絡的罪行應具有域外法律效力。[9] 為防止日後的法律程序出現爭議，小組委員會建議，針對電腦網絡罪行的特定法例應明確訂明適用於該五類罪行的司法管轄權規則，[10] 因而制定建議 11 至 15。正如諮詢文件所解釋，[11] 這做法兼具教育和阻嚇作用，因為任何存心在多個司法管轄區干犯該等罪行的人會知悉香港的法律立場。

對小組委員會建議 11 至 15 的概括回應

7.7 上文列出建議 11 至 15 的背景後，我們現討論諮詢回應。

支持建議的司法管轄權規則的回應者意見

7.8 政府部門、半官方機構、法律團體、商業團體及學術界當中，絕大多數支持建議的電腦網絡罪行法例適用於域外範圍。

---

6 為方便討論，每種事實情況所述的事實，均假定為該事實情況與香港的僅有聯繫，實際案件可能在多於一種事實情況下發生。

7 如以術語表達，即如《刑事司法管轄權條例》（第 461 章）第 3(1)條所述明：*“就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）”*。

8 這種情況會包括犯罪者、其作為及受害人全部均處於香港的案件。

9 諮詢文件第 7.62 段。

10 同上，第 7.63 段。

11 同上。

7.9 香港大律師公會（“**大律師公會**”）的概括意見是同意建議 11 至 15 *“有合理基礎，並與域外法律效力的一般原則及相互尊重原則相符”*。

7.10 從保障消費者的角度而言，消費者委員會注意到，*“在消費群當中，網上購物及其他形式的電子商貿近年急增，跨境交易因此愈趨普遍”*。消費者委員會認為，為充分保障香港的消費者，電腦網絡罪行法律的域外應用既有需要，亦有理可據。

7.11 回應者普遍同意上文第 7.5 段載述的五種事實情況。具體而言，關於事實情況(b)，即 *“犯罪者是香港人”*，個人資料私隱專員公署（“**私隱專員公署**”）及大律師公會均支持小組委員會的建議，即首四類依賴電腦網絡的罪行不應以這種事實情況作為依據。

7.12 私隱專員公署列出理由如下：

> “我們的執法經驗中，基於互聯網無分疆界，犯罪者犯案時並非香港人或並非居於香港的情況十分常見，因此與香港毫無聯繫。”

7.13 大律師公會亦同意排除事實情況(b)，指小組委員會的做法：

> “審慎避免建議的法例在電腦網絡罪行背景下過於無遠弗屆，因為電腦網絡罪行可能很容易就涉及至少兩個甚或更多司法管轄區”。[12]

反對建議的司法管轄權規則的回應者意見

7.14 某商業團體的部分成員認為，法庭可變更司法管轄權規則，以適應不斷演變的技術環境，並認為僅為電腦網絡罪行另訂不同的司法管轄權規則這做法不恰當。與此同時，某個人回應者表示，香港應遵循刑事司法管轄權的主要形式，即屬地管轄原則。在這項原則下，香港法庭對在香港境內作出的作為具有司法管轄權。

回應者的其他概括評述

7.15 不同回應者指出，基於電腦網絡罪行的跨境性質，要有效執行任何電腦網絡罪行法例，均需國際間通力合作，而執行當局亦應確保作出有效安排，以便向其他司法管轄區的執法機關尋求協助。

---

12 大律師公會引用的例子是：在香港的電腦使用惡意軟件，在未獲授權下取覽儲存於其他司法管轄區電腦系統內的數據，以獲取財務利益。

對小組委員會建議 11 至 15 的詳細回應

有關“香港人”的概念

7.16 對於事實情況(c)中有關“香港人”的概念，小組委員會建議應包括香港永久性居民、通常居於香港的人或在香港經營業務的公司。[13]

7.17 私隱專員公署留意到小組委員會這項建議，於是請小組委員會考慮《個人資料（私隱）條例》（第 486 章）（**《私隱條例》**）第 66M(5)條的擬定方式。第 66M 條屬於《私隱條例》第 9A 部，該部賦予個人資料私隱專員（“**私隱專員**”）法定權力，以送達停止披露通知，要求採取停止或限制披露“起底”內容的行動。如私隱專員有合理理由相信某名“香港人士”有能力就“起底”訊息採取停止披露行動，則私隱專員可送達通知。

7.18 根據第 66M(5)條的定義，[14] 任何人如 *“身處香港”*，即視為“香港人士”。私隱專員公署認為：

> “相比採用較複雜方式擬定永久性居民身分或通常居住地方的條文，〔第 66M(5)條的〕擬定方式較為直接簡單，爭議空間亦較少，因為複雜的事實及法律問題往往是由甚麼構成‘永久性居民身分’或‘通常居於某個地方’而引起”。

事實情況(d)：“目標電腦、程式或數據處於香港”

7.19 私隱專員公署亦認為，根據其執法經驗，目標電腦、程式或數據雖然儲存香港人的個人資料，但往往並非處於香港。為有效打擊電腦網絡罪行，私隱專員公署建議從建議 11(c)、12(c)、13(c)及 14(c)剔除這項規定。

---

13 諮詢文件第 7.69(b)段註腳 79。

14 《個人資料（私隱）條例》（第 486 章）第 66M(5)條把“香港人士”界定為指——

“(a) 身處香港的個人；或

(b) 符合以下說明的團體——

(i) 在香港成立為法團、設立或註冊；或

(ii) 在香港有業務地點。”（底線後加）

《刑事事宜相互法律協助條例》（第 525 章）（《相互法律協助條例》）及其他程序事宜

7.20 考慮到建議的電腦網絡罪行法例適用於域外範圍的可行性，大律師公會在意見書內作出以下評論：

> "電腦網絡世界跨越司法管轄權界限，在這個特定背景下，有效執行任何法例均需國際間通力合作。因此，當我們思考任何新訂法例可如何防範電腦網絡罪犯侵犯市民及商界權利時，都必須緊記這點。"

7.21 鑑於電腦網絡罪行案件可能涉及多個司法管轄區，而有關法律適用於域外範圍，大律師公會請小組委員會考慮應否修訂《相互法律協助條例》下任何相關條文。

7.22 與此同時，資訊科技業部分回應者舉出以下證據事宜：

(a) 如何從其他司法管轄區搜集證據；

(b) 應按照業界最佳作業方法及本地和國際數據法證調查組織採納的標準，保存取自雲端環境的證據（例如電腦數據）；

(c) 從雲端環境搜集的證據是否可接納呈堂；及

(d) 應解決香港與相關數據或伺服器所在的其他司法管轄區之間任何在法律上的衝突。

建議 11(d)、12(d)、13(d)、14(d)及 15(c)應否釐清"香港的安全"包括"國家安全"？

7.23 某政府部門提出，基於保護管轄原則，[15] 就五類依賴電腦網絡的罪行，應訂定針對危害國家安全行為的域外法律效力條文，而非只是針對威脅*"香港的安全"*的作為立法，以免有人以為*"香港的安全"*較國家安全的概念狹隘。該回應者提議將建議 11(d)、12(d)、13(d)、14(d)及 15(c)重寫如下：

> "犯罪者的作為，已導致或可能導致對香港的嚴重損害（例如導致對香港的基礎建設或公共機構的嚴重

[15] 上文第 7.4(d)段。

損害，或已威脅或可能威脅香港的安全），或已危害國家安全。”

（底線後加）

7.24 該回應者亦提出，另一做法是將“香港的安全”界定為包括“國家安全”。

我們的分析及回應

擴大事實情況(c)的範圍：“受害人是香港人”

7.25 正如上文第 7.17 段所述，私隱專員公署意見書內提到的《私隱條例》第 66M 條，所關乎的是截然不同的法律文意，當中條文劃定“香港人士”這個概念，是為了斷定私隱專員可向誰人送達停止披露通知，以要求就“起底”訊息採取行動。縱然如此，私隱專員公署載於上文第 7.17 及 7.18 段的意見，令我們深思香港法庭為電腦網絡罪行受害人提供的保障範圍應有多大。

7.26 我們明白，除了永久性居民及通常居於香港的人以外，不同人或各有原因而暫時在香港工作或逗留，例子包括外籍家庭傭工、遊客及其他在香港短暫逗留的訪客（例如為進行某項商業交易或洽商、參加展銷會或出席法庭或仲裁程序）。我們認為，倘若這些人身處香港時遇上電腦網絡罪行，他們亦應受到香港法律保障。換言之，電腦網絡罪行的保障範圍，應延伸至永久性居民及通常居於香港的人以外。

7.27 我們亦已考慮電腦網絡罪行案件是否有可能只屬於事實情況(c)（將按前段所載方式修改），而不屬於事實情況(a)、[16] (b)、[17] (d)[18] 或(e)。[19] 倘若如此，案件與香港之間的唯一聯繫，就是受害人是香港永久性居民、通常居於香港的人，或有關電腦網絡罪行發生時身處香港的人，而電腦網絡罪行其他必要元素則全部在香港以外發生。我們理解，調查有關案件或將之送交香港法庭審理或有實際困難，因為香港的執法機關須從其他司法管轄區搜集和保存證據，並解決其他

---

16 *“就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）在香港發生，即使其他有關作為、不作為或事情在其他地方發生”。*

17 *“犯罪者是香港人”。*

18 *“目標電腦、程式或數據處於香港”。*

19 *“犯罪者的作為，已導致或可能導致對香港的嚴重損害（例如導致對香港的基礎建設或公共機構的嚴重損害，或已威脅或可能威脅香港的安全）”。*

後勤方面的困難。不過，不論電腦網絡罪行的受害人是否香港居民，這些可行性的問題亦會出現。鑑於電腦網絡罪行無分疆界，與其他司法管轄區有關機關在現有相互法律協助框架下合作或商討完善有關框架是勢在必行。由於我們的研究第三部分會處理證據事宜及執法事宜，我們會在該部分考慮可如何加強現有執法及調查權力，以利便調查和處理跨境電腦網絡罪行。

7.28 總括而言，為了使短暫身處香港的人同樣受到保障，以防建議的依賴電腦網絡的罪行，我們建議將事實情況(c)改進如下：

> "受害人是香港永久性居民、通常居於香港的人，或於相關罪行發生時身處香港，又或是在香港經營業務的公司。"
>
> （底線後加）

事實情況(d)："目標電腦、程式或數據處於香港"

7.29 我們同意，針對電腦網絡罪行的特定法例所旨在保障的目標電腦、程式或數據，在很多情況下均未必處於香港。正如諮詢文件所解釋，[20] 為方便討論，五種事實情況各自所述的事實，均假定為該事實情況與香港的僅有聯繫，實際案件可能只在一種或在多於一種事實情況下發生。換言之，建議 11(c)、12(c)、13(c)及 14(c)所列的事實情況，均並非首四項建議的罪行適用於域外範圍的先決條件，而只代表香港法庭可主張對電腦網絡罪行案件具有司法管轄權的四項可能基礎之一。

7.30 因此，雖然無須如建議所述從建議 11(c)、12(c)、13(c)及 14(c)剔除這項規定，但私隱專員公署的執法經驗的確證實，該等建議的相關事實情況之間應有表示任選其一的"或"字。

證據事宜、程序事宜及《相互法律協助條例》的相關立法修訂

7.31 正如上文所述，[21] 我們的研究第三部分會處理執法及程序事宜。這些事宜本身為一大議題，我們會緊記上文第 7.22 段內回應者幫忙識別的問題。

---

20 第 7.69 段註腳 76。

21 上文第 7.27 段。

7.32 我們相信《相互法律協助條例》的相關修訂，最終會取決於建議的電腦網絡罪行法例的制定形式。我們亦預期香港特別行政區政府或需與其他司法管轄區有關機關商討，以促進不同地方執法機關互相合作。在這情況下，我們若對《相互法律協助條例》的相應修訂作出任何建議，實屬言之尚早。有關修訂最好留待政府適時按需要決定。

建議 11(d)、12(d)、13(d)、14(d)及 15(c)對“香港的安全”的提述

7.33 我們在第 4 章討論建議的非法干擾電腦數據罪時，[22] 提述於 2024 年 3 月制定的《維護國家安全條例》（“**《基本法》第二十三條立法**”）。《基本法》第二十三條立法就多項釋義訂定條文，當中包括“特區的安全”這概念的釋義。凡《基本法》第二十三條立法以外的條例提述“特區的安全”（包括與這項提述涵義相同的詞句），[23] 須理解為包括法例所界定的“國家安全”。[24] 隨着《基本法》第二十三條立法落實，新訂電腦網絡罪行法例內任何對“香港的安全”的提述，其範圍將會充分寬廣。[25]

7.34 我們亦已在第 4 章[26] 強調，《中華人民共和國香港特別行政區維護國家安全法》（**《國安法》**）構成我們法律制度不可或缺的部分，所以重要的一點，是針對電腦網絡罪行的特定法例不得與《國安法》有任何抵觸或衝突，即使並非有意亦然。

7.35 故此，我們必須指出，《國安法》第四章已訂明若干適用於危害國家安全犯罪案件的司法管轄權及程序規則。第四十條起首便訂明：

> “香港特別行政區〔（“**香港特區**”）〕對〔《國安法》〕規定的犯罪案件行使管轄權，但〔《國安法》〕第五十五條規定的情形除外。”

---

22 上文第 4.28 段。

23 《維護國家安全條例》（“**《基本法》第二十三條立法**”）第 8(2)條。

24 同上，第 4 條。

25 無論如何，《基本法》第二十三條立法第 8(1)條規定，凡《基本法》第二十三條立法與另一條例，如無該款的話是會有不一致之處的，則須以最能顧及《基本法》第二十三條立法的目的和作用的方式，理解該另一條例。

26 上文第 4.27 段。

7.36 第五十五條列出下述例外情形：

> “有以下情形之一的，經香港特別行政區政府或者駐香港特別行政區維護國家安全公署〔（“**國安公署**”）〕提出，並報中央人民政府批准，由〔國安公署〕對〔《國安法》〕規定的危害國家安全犯罪案件行使管轄權：
>
> （一）案件涉及外國或者境外勢力介入的複雜情況，香港特別行政區管轄確有困難的；
>
> （二）出現香港特別行政區政府無法有效執行〔《國安法》〕的嚴重情況的；
>
> （三）出現國家安全面臨重大現實威脅的情況的。”

（底線後加）

7.37 因此，當電腦網絡罪行案件涉及《國安法》規定的任何罪行時，顯而易見，一般原則是香港法庭可根據第四十條對案件行使司法管轄權，即使針對電腦網絡罪行的特定法例並無任何司法管轄權規則規定該等案件須在香港審理，情況亦是如此。

7.38 在例外情形下，當根據第五十五條提出的要求獲中央人民政府批准，國安公署將據此對案件行使司法管轄權。《國安法》第五十六條亦隨之適用：

> “根據〔《國安法》〕第五十五條規定管轄有關危害國家安全犯罪案件時，由駐香港特別行政區維護國家安全公署負責立案偵查，最高人民檢察院指定有關檢察機關行使檢察權，最高人民法院指定有關法院行使審判權。”

（底線後加）

7.39 鑑於電腦網絡罪行案件如危害國家安全，有關案件的司法管轄權並不完全歸於香港法庭，為避免預先限制香港特區政府、國安公署、最高人民檢察院及最高人民法院可如何按每宗案件的情況所需，根據《國安法》第四章所列程序處理有關案件，我們認為並不適合在針對電腦網絡罪行的特定法例中訂立司法管轄權規則，訂明香港法庭對有關案件行使司法管轄權。

7.40 因此，我們維持在諮詢文件提出的建議 11(d)、12(d)、13(d)、14(d)及 15(c)。

結論

7.41 鑑於上文所述，我們敲定有關司法管轄權規則的建議如下：

最終建議 11

我們建議，在以下情況下，就建議的非法取覽程式或數據罪，香港的法庭應具有司法管轄權：

(a) **就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）在香港發生，即使其他有關作為、不作為或事情在其他地方發生；**

(b) **受害人（目標電腦的擁有人、有關數據的擁有人或兩者）是香港永久性居民、通常居於香港的人，或於該罪行發生時身處香港，又或是在香港經營業務的公司；**

(c) **目標電腦、程式或數據處於香港；或**

(d) **犯罪者的作為，已導致或可能導致對香港的嚴重損害（例如導致對香港的基礎建設或公共機構的嚴重損害，或已威脅或可能威脅香港的安全），**

惟須符合以下規定：如犯罪者因其在香港境外所作的作為而被控這項簡易程序罪行，該作為本身或連同就這項香港罪行定罪而須予以證明的其他有關作為、不作為或事情，須在該作為作出的司法管轄區構成罪行。

最終建議 12

我們建議，在以下情況下，就建議的非法截取電腦數據罪，香港的法庭應具有司法管轄權：

(a) 就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）在香港發生，即使其他有關作為、不作為或事情在其他地方發生；

(b) 受害人是香港永久性居民、通常居於香港的人，或於該罪行發生時身處香港，又或是在香港經營業務的公司；

(c) 目標電腦、程式或數據處於香港；或

(d) 犯罪者的作為，已導致或可能導致對香港的嚴重損害（例如導致對香港的基礎建設或公共機構的嚴重損害，或已威脅或可能威脅香港的安全）。

最終建議 13

我們建議，在以下情況下，就建議的非法干擾電腦數據罪（包括基本形式及加重形式），香港的法庭應具有司法管轄權：

(a) 就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）在香港發生，即使其他有關作為、不作為或事情在其他地方發生；

(b) 受害人是香港永久性居民、通常居於香港的人，或於該罪行發生時身處香港，又或是在香港經營業務的公司；

(c) 目標程式或數據處於香港；或

(d) 犯罪者的作為，已導致或可能導致對香港的嚴重損害（例如導致對香港的基礎建設或公共機構的嚴重損害，或已威脅或可能威脅香港的安全）。

最終建議 **14**

我們建議，在以下情況下，就建議的非法干擾電腦系統罪（包括基本形式及加重形式），香港的法庭應具有司法管轄權：

(a) 就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）在香港發生，即使其他有關作為、不作為或事情在其他地方發生；

(b) 受害人是香港永久性居民、通常居於香港的人，或於該罪行發生時身處香港，又或是在香港經營業務的公司；

(c) 目標電腦處於香港；或

(d) 犯罪者的作為，已導致或可能導致對香港的嚴重損害（例如導致對香港的基礎建設或公共機構的嚴重損害，或已威脅或可能威脅香港的安全）。

最終建議 15

我們建議，在以下情況下，就建議的提供用作干犯電腦網絡相關罪行的器材、程式或數據罪（或為提供用作干犯電腦網絡相關罪行的器材、程式或數據而管有罪），香港的法庭應具有司法管轄權：

(a) 就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）在香港發生，即使其他有關作為、不作為或事情在其他地方發生（例如身處香港的人在暗網上提供用作干犯電腦網絡相關罪行的器材、程式或數據）；

(b) 犯罪者是香港永久性居民、通常居於香港的人，或在香港經營業務的公司；或

(c) 犯罪者的作為，已導致或可能導致對香港的嚴重損害（例如導致對香港的基礎建設或公共機構的嚴重損害，或已威脅或可能威脅香港的安全）。

第 8 章　判刑

引言

8.1　　本章討論關於建議 16 的回應。建議 16 載列就五類依賴電腦網絡的罪行所建議的最高刑罰：

> "小組委員會建議：
>
> (a) 就建議的非法取覽程式或數據罪而言，犯罪者應可處下述最高刑罰：
>
> (i) 如屬簡易程序罪行，可處兩年監禁；或
>
> (ii) 如屬加重罪行，一經循公訴程序定罪，可處 14 年監禁。
>
> (b) 就建議的非法截取電腦數據罪而言，犯罪者一經循簡易程序定罪，應可處兩年監禁，一經循公訴程序定罪，應可處 14 年監禁。
>
> (c) 就建議的非法干擾電腦數據罪及非法干擾電腦系統罪而言，犯罪者就每項罪行應可處下述最高刑罰：
>
> (i) 如屬基本罪行，一經循簡易程序定罪，可處兩年監禁，一經循公訴程序定罪，可處 14 年監禁；或
>
> (ii) 如屬加重罪行，可處終身監禁。
>
> (d) 就建議的提供或管有用作犯罪的器材或數據罪而言，犯罪者應可處下述最高刑罰：
>
> (i) 如屬基本罪行，一經循簡易程序定罪，可處兩年監禁，一經循公訴程序定罪，可處七年監禁；或
>
> (ii) 如屬加重罪行，一經循公訴程序定罪，可處 14 年監禁。"

小組委員會提出建議 16 背後的考慮因素

8.2 在我們開始討論回應者就建議 16 提出的意見前，宜先重溫小組委員會在擬定其判刑建議時所考慮的各項因素。

8.3 正如小組委員會在諮詢文件論述，[1] 在擬定建議 16 時，小組委員會參考了《盜竊罪條例》（第 210 章）就以下各類具代表性罪行所訂的最高監禁刑期：

(a) 盜竊罪可處 10 年監禁；[2]

(b) 欺詐罪可處 14 年監禁；[3]

(c) 勒索罪可處 14 年監禁；[4]

(d) 入屋犯法罪可處 14 年監禁；[5]

(e) 嚴重入屋犯法罪（即任何人在犯入屋犯法罪時攜帶任何火器或仿製火器、任何攻擊性武器或任何炸藥）可處終身監禁；[6] 及

(f) 搶劫罪可處終身監禁。[7]

8.4 小組委員會提到，不論我們所建議的監禁年期長度如何，某程度上也有武斷成分。[8] 在上述背景之下，建議 16 提出以下各項建議罪行的最高監禁刑期應訂為 14 年：非法取覽程式或數據的加重罪行、非法截取電腦數據罪、非法干擾電腦數據的基本罪行及非法干擾電腦系統的基本罪行，以及提供或管有用作犯罪的器材或數據的加重罪行。小組委員會認為這項建議不但會發揮必要的阻嚇作用，足以打擊電腦網絡罪行，亦不會過分偏離以下罪行的最高刑罰：(a)前段所述《盜竊罪條例》所訂的罪行，以及(b)其他司法管轄區的有關罪行。[9]

---

1 第 8.14(f)段。
2 《盜竊罪條例》（第 210 章）第 9 條。
3 同上，第 16A(1)條。
4 同上，第 23(3)條。
5 同上，第 11(4)條。
6 同上，第 12(3)條。
7 同上，第 10(2)條。
8 諮詢文件第 8.15 段。
9 見諮詢文件的附錄，當中概述香港及其他司法管轄區的現行法律就建議的五類依賴電腦網絡的罪行所訂的最高刑罰。

對小組委員會建議 16 的回應

概覽

8.5 我們就建議 16 的判刑建議收到的回應意見不一。概括而言，來自多個政府部門、法律團體、商業團體及大專院校的回應者，均支持香港引入一套較現有法定電腦相關罪行的罰則更重的罰則，以加大打擊電腦網絡罪行的力度。在這些回應者當中，部分認為加重罰則將有助阻嚇依賴電腦網絡的罪行，而良好穩健的網絡安全制度亦會促進香港的商業地位。

非法取覽程式或數據罪（“取覽罪”）

8.6 正如第 2 章所述，[10] 香港女律師協會有限公司認為，加重形式的取覽罪因涉及 *“未犯的潛在罪行的意圖”* 而可能 *“太難證明”*，並認為這或會使控方在無法證明嚴重罪行構成有關加重罪行時，極其依賴有關簡易程序罪行來處理該嚴重罪行。正因如此，這名回應者提議小組委員會應進一步考慮，就簡易程序形式的取覽罪處以最高兩年監禁是否具足夠阻嚇性。

非法干擾電腦數據及非法干擾電腦系統（“干擾罪”）的加重罪行

8.7 少數來自資訊科技界的回應者認為，把干擾罪的最高刑罰訂為終身監禁 *“過分嚴厲”*，原因是終身監禁是謀殺罪及其他類似的極嚴重刑事罪行的最高刑罰。

8.8 同樣地，香港律師會要求小組委員會闡釋把最高刑罰訂為終身監禁這項建議背後的理念。這名回應者有以下評論：

> “有關理據似乎是參照並基於第 200 章〔《刑事罪行條例》〕第 63 條，[11] 該條涉及縱火罪。這項罪行直接導致身體受嚴重傷害，人命攸關。諮詢文件沒有解釋，《刑事罪行條例》第 63 條與建議的（非法干擾電腦數據及非法干擾電腦系統的）加重罪行，在可導致傷害的

---

10 上文第 2.13 段。

11 《刑事罪行條例》第 63 條的內容如下：

“(1) 任何人犯第 60 條所訂的縱火的罪行或第 60(2)條所訂的罪行（不論是否屬縱火），一經循公訴程序定罪，可處終身監禁。

(2) 任何人犯本部所訂的其他罪行，一經循公訴程序定罪，可處監禁 10 年。”

（底線後加）

嚴重性或其他方面如何相關或對等。另一方面，據我們所知，從未有人因刑事損壞而被判處終身監禁。諮詢文件也沒有列明應就這項罪行引入哪些加重刑罰的因素，作為如此重判的理由。目前，我們無法設想在哪些情況下，控方可能會促請法庭就這項罪行判處終身監禁，例如干擾要有多嚴重才應判處終身監禁。〔小組委員會〕宜對上述各點加以闡釋。”

我們的分析及回應

取覽罪

8.9 正如我們已在第 2 章解釋，[12] 取覽罪的加重形式是針對以下一類案件而訂立的：本港法院在履行其事實審裁者的職責時，能夠根據案中證據，基於承認或透過從個別案件的事實和情況作出推論（視乎屬何情況而定），就所需的被告人思想狀態（即該人是否意圖干犯其他罪行）作出裁定。故此，保留有關簡易程序罪行作為後備選擇不應被視為是避重就輕的做法，令到被裁定犯較輕罪行的被告人，基本上仍可在有犯加重罪行之嫌的基礎上而被判刑，猶如有證明顯示他已犯了該加重罪行一樣。

8.10 儘管有上文所述，但我們也藉此機會反思把簡易程序形式的取覽罪的最高刑罰訂為兩年監禁的建議，這是因為我們注意到，英格蘭及威爾斯《1990 年誤用電腦法令》（Computer Misuse Act 1990）僅採納 12 個月監禁作為類似罪行的最高刑罰。我們同意小組委員會的看法，認為不論我們所建議的監禁年期長度如何，某程度上也有武斷成分。[13] 至於應否採納上述建議，要視乎它與香港現有罪行的比較情況而定。

8.11 舉例來說，我們留意到，任何人犯一些本身不會增加損傷或財產損壞風險的道路交通罪行，可處最高 12 個月監禁。這類罪行包括在道路上使用汽車而沒設有規定的強制保險，[14] 以及司機沒有在被

12 上文第 2.38 段。

13 諮詢文件第 8.15 段。

14 見《汽車保險（第三者風險）條例》（第 272 章）第 4(2)(a)條所訂的刑罰。第 4(1)條禁止*“任何人在道路上使用汽車，或致使或允許任何其他人在道路上使用汽車，除非就該人或該其他人……對車輛的使用已備有一份有效的和符合”*該條例*“規定的第三者風險保險單或保證單”*。

警務人員要求時提供血液或尿液樣本。[15] 若交通意外風險確實發生，而在有關調查過程中偵查到有人犯這類罪行（或在路障處隨機發現有人犯這類罪行，或在有關司機因駕駛時無執照或於取消駕駛資格期間駕駛而被當場拘捕時發現有人犯這類罪行），則法庭會考慮整體量刑原則，[16] 在計及就控方提出而被告人也會被判罪成的其他較嚴重控罪所應判處的適當刑罰後，對被告人判刑。

8.12 考慮到最高刑罰應具有足夠的阻嚇作用，把該刑罰訂為兩年監禁，便能彰顯簡易程序形式的取覽罪的嚴重性：任何人一旦干犯該罪行，即使沒有足夠證據證明該人在未獲授權下取覽程式或數據後意圖進行其他犯罪活動，法律旨在保護的有關目標系統的不可侵犯性或有關資料的機密性，也已經受到侵害。因此，在考慮所有因素後，我們也同意小組委員會的看法，即簡易程序形式的取覽罪的最高刑罰，適宜建議訂為兩年監禁。這樣會讓法院在判刑時有足夠權力，可視乎有關入侵程度和外洩資料的重要性，判處能恰當地反映罪行重點的刑罰。

8.13 最後我們想補充一點，即使某刑事罪行條文沒有就罰款作出明文規定，根據《裁判官條例》（第 227 章），裁判法院也具有一般權力判處不超過某級數的罰款。[17] 政府如在適當時候決定落實我們的建議，可在立法階段進一步考慮電腦網絡罪行法例應否訂明罰款級數，故我們確實認為，無須就簡易程序形式的取覽罪建議最高罰款。

建議的干擾罪的加重罪行

8.14 正如第 4 及 5 章所論述，我們建議：

(a) 就非法干擾電腦數據罪加重形式的罪行，應採用《刑事罪行條例》第 60(2)條所訂的加重罪行；[18] 及

---

15 《道路交通條例》（第 374 章）第 39S(1)(b)(ii)條規定：任何人無合理辯解，沒有在根據第 39P 條被要求提供血液或尿液樣本以作化驗時按要求行事，或沒有給予第 39Q(4)(b)條所指的對分析血液樣本的同意，即屬犯罪；一經循簡易程序定罪，如曾循公訴程序定罪，可處第 4 級罰款及監禁 12 個月。

16 整體量刑原則是指法庭在判處分期執行的刑期時，*"應把各有關罪行視為一個整體，審視合計刑期並考慮須服的總刑期是否適當"*，而*"審慎運用整體量刑原則，有助於判處合理和恰當，卻又不過於嚴苛的整體刑期"*。見 *Archbold Hong Kong 2025*，第 5－91 段。

17 例如，《裁判官條例》（第 227 章）第 97 條有以下規定：
"任何人被裁定犯並非可公訴罪行的罪行時，如裁判官並無因為要行使其他權力（例如根據《罪犯感化條例》（第 298 章）第 3 條發出感化令的權力）而不能判處該人，則除任何成文法則規定該人須受某一特定方式處置外，該裁判官可判處罰款以代替任何他有權力處置該人的其他方式，亦可在以該等其他方式處置該人外，再判處罰款。"

18 最終建議 6(b)(iv)。

(b) 關於非法干擾電腦系統及非法干擾電腦數據的建議條文，應採用一致的措辭。[19]

8.15 正如小組委員會嘗試在諮詢文件解釋，[20] 就干擾罪的加重罪行所建議的最高刑罰，僅旨在與現行《刑事罪行條例》第 63(1)條就加重形式的刑事損壞罪所訂的刑罰保持貫徹一致。若把第 63(1)條與《刑事罪行條例》第 60(2)(b)條[21] 一併閱讀，便可明顯看到，有關條文處理的情況，涉及意圖危害生命的財產損壞或摧毀。

8.16 就現行法例所訂刑事損壞的加重罪行而言，根據《刑事罪行條例》第 63(1)條，一經循公訴程序定罪，最高刑罰為終身監禁。事實上，《刑事罪行條例》第 63(1)條不但涵蓋縱火，亦適用於被告人意圖摧毀或損壞財產以危害他人生命（或罔顧他人生命是否會因財產的摧毀或損壞而受到危害）的任何刑事損壞罪。第 63(1)條有以下明確規定：

> "任何人犯第 60 條所訂的縱火的罪行或第 60(2)條所訂的罪行（不論是否屬縱火），一經循公訴程序定罪，可處終身監禁。"
>
> （底線後加）

8.17 小組委員會建議，就加重形式的干擾罪採納《刑事罪行條例》第 63(1)條現時訂明的最高刑罰，亦即終身監禁。小組委員會在諮詢文件[22] 提供了涉及生命受危害的假設情境：某人干擾機場控制塔系統、鐵路信號系統等所處理的電腦數據。另一些例子包括干擾發電廠及供氣等大型基礎建設的電腦系統。由於這類干擾行為可能會危害數以千計的人的生命，因此我們同意，有充分理由就干擾罪的加重罪行處以相對嚴厲的刑罰。

8.18 我們希望重申，針對電腦網絡罪行的特定法例的用意，並非重新訂定現行《刑事罪行條例》已為各干擾罪所構思的最高刑罰。視乎案情而定，非法干擾電腦數據及／或非法干擾電腦系統的行為可能已構成刑事損壞的加重罪行，該罪行現時的最高刑罰為終身監禁。

---

19 最終建議 7(a)。

20 第 8.20 段。

21 《刑事罪行條例》（第 200 章）第 60(2)條規定：
"任何人無合法辯解而摧毀或損壞任何財產（不論是屬於其本人或他人的）——
(a) 意圖摧毀或損壞任何財產或罔顧任何財產是否會被摧毀或損壞；及
(b) 意圖藉摧毀或損壞財產以危害他人生命或罔顧他人生命是否會因而受到危害，
即屬犯罪。"（底線後加）

22 第 4.97 段。

我們所作建議的用意，只是使這些在《刑事罪行條例》下已包含的干擾罪在納入新訂的電腦網絡罪行法例時，在該法例中得以反映。

建議的提供用作干犯電腦網絡相關罪行的器材、程式或數據（或為向他人提供該等器材、程式或數據而管有它們）的基本罪行

8.19 我們在討論有關回應期間，也全盤檢討了諮詢文件所載的建議16，以確保有關建議不但會發揮必要的阻嚇作用，足以打擊電腦網絡罪行，亦不會過分偏離以下罪行的最高刑罰：(a)前述《盜竊罪條例》所訂的罪行，[23] 以及(b)其他司法管轄區的有關罪行。[24] 舉例來說，就提供或管有用作干犯電腦網絡相關罪行的器材、程式或數據的基本罪行而言，小組委員會建議，該基本罪行一經循公訴程序定罪，最高刑罰為七年監禁。這項刑罰是相關加重罪行的建議最高刑罰的一半，整體上亦與其他司法管轄區的刑罰看齊。

8.20 我們信納，建議16體現上文闡述的原則。

最終建議16

我們建議：

(a) 就建議的非法取覽程式或數據罪而言，犯罪者應可處下述最高刑罰：

(i) 如屬簡易程序罪行，可處兩年監禁；或

(ii) 如屬加重罪行，一經循公訴程序定罪，可處14年監禁。

(b) 就建議的非法截取電腦數據罪而言，犯罪者一經循簡易程序定罪，應可處兩年監禁，一經循公訴程序定罪，應可處14年監禁。

---

23 第8.3段。

24 見諮詢文件的附錄，當中概述香港及其他司法管轄區的現行法律就建議的五類依賴電腦網絡的罪行所訂的最高刑罰。

(c) 就建議的非法干擾電腦數據罪及非法干擾電腦系統罪而言，犯罪者就每項罪行應可處下述最高刑罰：

(i) 如屬基本罪行，一經循簡易程序定罪，可處兩年監禁，一經循公訴程序定罪，可處 **14** 年監禁；或

(ii) 如屬加重罪行，可處終身監禁。

(d) 就建議的提供用作干犯電腦網絡相關罪行的器材、程式或數據罪（或為向他人提供該等器材、程式或數據而管有罪）而言，犯罪者應可處下述最高刑罰：

(i) 如屬基本罪行，一經循簡易程序定罪，可處兩年監禁，一經循公訴程序定罪，可處七年監禁；或

(ii) 如屬加重罪行，一經循公訴程序定罪，可處 **14** 年監禁。

第 9 章　　我們的最終建議摘要

非法取覽程式或數據

——最終建議 1、2、11 及 16(a)

最終建議 1

我們建議：

(a) 無合法權限而在未獲授權下取覽程式或數據，應在新法例下定為簡易程序罪行，而合理辯解可作為法定免責辯護。

(b) 這項建議罪行的犯罪意念是：

(i) 被告人意圖獲得對有關程式或數據的取覽，或意圖使他人能夠獲得該項取覽；及

(ii) 被告人在取覽有關程式或數據時，知悉該項意圖作出的取覽未獲授權。

(c) 在未獲授權下取覽程式或數據，並意圖進行其他犯罪活動，應構成新法例所訂的加重罪行，並招致更高刑罰。

(d) 新法例的建議條文應以英格蘭及威爾斯《誤用電腦法令》第 1、2 及 17 條為藍本。

最終建議 2

就建議的非法取覽程式或數據罪而言，我們建議除合理辯解可作為法定免責辯護外：

(a) 在未獲授權下為網絡安全目的而取覽，應有特定的免責辯護，但須符合以下條件：

(i) 被告人必須是經認可的網絡安全從業員（認可制度的細節本質上屬政策事項，最好留待政府考慮）；

(ii) 被告人必須為真正的網絡安全目的而行事；及

(iii) 在顧及整體情況後，被告人的行為必須是合理的。

(b) 在未獲授權下為保障 16 歲以下兒童及易受傷害人士（即《精神健康條例》（第 136 章）所界定的精神紊亂的人或弱智人士）的利益而取覽，應有特定的免責辯護：

(i) 這項免責辯護建基於取覽兒童或易受傷害人士的程式或數據的人的主觀目的(即為了保障有關兒童或易受傷害人士的利益），而非該人與有關兒童或易受傷害人士的關係。

(ii) 在顧及整體情況後，被告人對程式或數據的取覽必須是合理的。

(c) 在未獲授權下為教育、科學或研究目的而取覽，應有特定的免責辯護。在顧及整體情況後，被告人對程式或數據的取覽必須是合理的。

(d) 《刑事罪行條例》（第 200 章）第 64(2)條所訂的關於非法干擾電腦數據罪及非法干擾電腦系統罪的免責辯護，也應可就非法取覽程式或數據罪而提出。

(i) 第 64(2)條所訂的兩項免責辯護涵蓋以下情況：

(1) 被告人在取覽程式或數據時，相信其作為已獲同意或會獲同意；或

(2) 被告人在取覽程式或數據時，相信有關財產需即時保護，並相信在顧及整體情況後，所採用的保護方法是合理的。

(ii) 被告人不論是提出同意免責辯護或保護財產免責辯護，均必須合理地相信該免責辯護所訂的有關事宜。

最終建議 11

我們建議，在以下情況下，就建議的非法取覽程式或數據罪，香港的法庭應具有司法管轄權：

(a) 就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）在香港發生，即使其他有關作為、不作為或事情在其他地方發生；

(b) 受害人（目標電腦的擁有人、有關數據的擁有人或兩者）是香港永久性居民、通常居於香港的人，或於該罪行發生時身處香港，又或是在香港經營業務的公司；

(c) 目標電腦、程式或數據處於香港；或

(d) 犯罪者的作為，已導致或可能導致對香港的嚴重損害（例如導致對香港的基礎建設或公共機構的嚴重損害，或已威脅或可能威脅香港的安全），

惟須符合以下規定：如犯罪者因其在香港境外所作的作為而被控這項簡易程序罪行，該作為本身或連同就這項香港罪行定罪而須予以證明的其他有關作為、不作為或事情，須在該作為作出的司法管轄區構成罪行。

最終建議 16(a)

就建議的非法取覽程式或數據罪而言，我們建議犯罪者應可處下述最高刑罰：

(i) 如屬簡易程序罪行，可處兩年監禁；或

(ii) 如屬加重罪行，一經循公訴程序定罪，可處 14 年監禁。

非法截取電腦數據

——最終建議 4、5、12 及 16(b)

最終建議 4

我們建議：

(a) 為不誠實或犯罪目的而在未獲授權下截取電腦數據，應在新法例下定為罪行。

(b) 建議的罪行應：

(i) 保障一般通訊，而並非只保障私人通訊；

(ii) 一般適用於數據（不論有關數據是否元數據）；及

(iii) 適用於截取在傳送人一端前往傳送對象一端途中的數據，即傳送中的數據及在傳送期間暫時靜止的數據。

(c) 除上述另有規定外，建議的條文應以《電腦罪行及電腦相關罪行示範法》（Model Law on Computer and Computer Related Crime）第 8 條為藍本，包括犯罪意念（即“蓄意”截取）。

(d) 關於在未獲授權下披露或使用電腦數據（不論該數據是以截取或其他方式取得），我們應先在研究的第二部分更詳盡探討它所帶來的影響，然後才就應否建議訂立任何這方面的新罪行（以及如應該的話，如何訂立）發表任何確定意見。

最終建議 5

我們不建議為在通常運作過程中截取或使用電腦數據的專業或真正業務（例如咖啡店、酒店、購物商場、僱主）提供任何免責辯護或豁免。為不誠實或犯罪目的而截取電腦數據這項犯罪意念規定，已免除訂定任何特定免責辯護或豁免的需要。

最終建議 12

我們建議，在以下情況下，就建議的非法截取電腦數據罪，香港的法庭應具有司法管轄權：

(a) 就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）在香港發生，即使其他有關作為、不作為或事情在其他地方發生；

(b) 受害人是香港永久性居民、通常居於香港的人，或於該罪行發生時身處香港，又或是在香港經營業務的公司；

(c) 目標電腦、程式或數據處於香港；或

(d) 犯罪者的作為，已導致或可能導致對香港的嚴重損害（例如導致對香港的基礎建設或公共機構的嚴重損害，或已威脅或可能威脅香港的安全）。

最終建議 16(b)

就建議的非法截取電腦數據罪而言，我們建議犯罪者一經循簡易程序定罪，應可處兩年監禁，一經循公訴程序定罪，應可處 14 年監禁。

非法干擾電腦數據

——最終建議 6、13 及 16(c)

最終建議 6

我們建議：

(a) 無合法權限而蓄意干擾（損壞、刪除、弄壞、更改或抑制）電腦數據，應在新法例下定為罪行，而合理辯解可作為法定免責辯護。

(b) 新法例應採用《刑事罪行條例》（第 200 章）所訂以下特點：

(i) 第 59(1A)(a)、(b)及(c)條所訂犯罪行為；

(ii) 第 60(1)條所訂犯罪意念（該條規定須懷有意圖或罔顧後果，而非懷有惡意）；

(iii) 第 64(2)條所示的兩項免責辯護，但須因應上文(a)段所重新擬訂的罪行，為恰當表達該兩項免責辯護而作出所需改進，並同時保留任何獲法律承認的其他合法辯解或免責辯護；及

(iv) 第 60(2)條所訂加重罪行。

(c) 第 64(2)條所涵蓋的兩項免責辯護適用於以下情況：

(i) 被告人在干擾電腦數據時，相信其作為已獲同意或會獲同意；或

(ii) 被告人在干擾電腦數據時，相信有關財產需即時保護，並相信在顧及整體情況後，所採用的保護方法是合理的。

被告人不論是提出同意免責辯護或保護財產免責辯護，均必須合理地相信該免責辯護所訂的有關事宜。

(d) 上述有關“誤用電腦”的條文應與刑事損壞罪拆開，並納入新法例內，同時刪除《刑事罪行條例》（第 200 章）第 59(1)(b)及(1A)條。

(e) 為網絡安全目的而非法干擾電腦數據，應有特定的免責辯護，但須符合以下條件：

(i) 被告人必須是經認可的網絡安全從業員（認可制度的細節本質上屬政策事項，最好留待政府考慮）；

(ii) 被告人必須為真正的網絡安全目的而行事；及

(iii) 在顧及整體情況後，被告人的行為必須是合理的。

最終建議 13

我們建議，在以下情況下，就建議的非法干擾電腦數據罪（包括基本形式及加重形式），香港的法庭應具有司法管轄權：

(a) 就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）在香港發生，即使其他有關作為、不作為或事情在其他地方發生；

(b) 受害人是香港永久性居民、通常居於香港的人，或於該罪行發生時身處香港，又或是在香港經營業務的公司；

(c) 目標程式或數據處於香港；或

(d) 犯罪者的作為，已導致或可能導致對香港的嚴重損害（例如導致對香港的基礎建設或公共機構的嚴重損害，或已威脅或可能威脅香港的安全）。

最終建議 16(c)

就建議的非法干擾電腦數據罪而言，我們建議犯罪者應可處下述最高刑罰：

(i) 如屬基本罪行，一經循簡易程序定罪，可處兩年監禁，一經循公訴程序定罪，可處 14 年監禁；或

(ii) 如屬加重罪行，可處終身監禁。

非法干擾電腦系統

——最終建議 7、8、14 及 16(c)

最終建議 7

我們建議：

(a) 關於非法干擾電腦數據及非法干擾電腦系統的建議條文，應採用一致的措辭。

(b) 《刑事罪行條例》（第 200 章）第 59(1A)及 60 條足以禁止非法干擾電腦系統，也應納入新法例內。

(c) 新法例在適當釐清“誤用電腦”一詞（例如將“損害任何電腦的操作”的概念納入該詞）的同時，應保留現有法律的廣度，不宜過於局限。

(d) 舉例來說，建議的非法干擾電腦系統罪應適用於蓄意或罔顧後果地作出以下行為的人：

(i) 攻擊電腦系統（不論成功與否——刑事法律責任不應取決於干擾成功與否）；

(ii) 在生產軟件時，在軟件編入缺損程式；及

(iii) 在未獲授權下更改電腦系統，並知悉該項更改可能導致合法使用者不能取用或正常使用有關系統。

最終建議 8

我們建議：

(a) 為網絡安全目的而非法干擾電腦系統，應有特定的免責辯護，但須符合以下條件：

(i) 被告人必須是經認可的網絡安全從業員（認可制度的細節本質上屬政策事項，最好留待政府考慮）；

(ii) 被告人必須為真正的網絡安全目的而行事；及

(iii) 在顧及整體情況後，被告人的行為必須是合理的。

(b) 就建議的非法干擾電腦系統罪而言，無須為非保安專業人員提供任何特定的免責辯護（例如由機械人進行網頁抓取或由互聯網資訊收集工具啟動網絡爬蟲，從而藉着連接指定的協定埠，在未獲授權下從伺服器收集數據），理由是根據默示授權的原則，構成互聯網或電腦系統正常運作一部分的活動應繼續獲准。

最終建議 14

我們建議，在以下情況下，就建議的非法干擾電腦系統罪（包括基本形式及加重形式），香港的法庭應具有司法管轄權：

(a) 就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）在香港發生，即使其他有關作為、不作為或事情在其他地方發生；

(b) 受害人是香港永久性居民、通常居於香港的人，或於該罪行發生時身處香港，又或是在香港經營業務的公司；

(c) 目標電腦處於香港；或

(d) 犯罪者的作為，已導致或可能導致對香港的嚴重損害（例如導致對香港的基礎建設或公共機構的嚴重損害，或已威脅或可能威脅香港的安全）。

最終建議 16(c)

就建議的非法干擾電腦系統罪而言，我們建議犯罪者應可處下述最高刑罰：

(i) 如屬基本罪行，一經循簡易程序定罪，可處兩年監禁，一經循公訴程序定罪，可處 14 年監禁；或

(ii) 如屬加重罪行，可處終身監禁。

提供或管有用作干犯電腦網絡相關罪行的器材、程式或數據

——最終建議 9、10、15 及 16(d)

最終建議 9

(a) 在新法例下，蓄意提供被製造或改裝以用作干犯電腦網絡相關罪行[1] 的器材、程式或數據（或其部分），或蓄意為提供該器材、程式或數據而管有它，不論它是有形物或無形物（例如勒索軟件、病毒或其源碼），應定為基本罪行，而合理辯解可作為法定免責辯護。

(b) 建議罪行的犯罪行為，應涵蓋供應（例如生產、提供、出售及輸出有關器材、程式或數據）及需求（例如取得、管有、購買及輸入有關器材、程式或數據）兩方面。

(c) 建議的罪行應適用於主要用作（以客觀方式界定）干犯電腦網絡相關罪行的器材、程式或數據（或其部分），不論該器材、程式或數據是否亦可能用作任何合法目的。

(d) 建議罪行的犯罪意念規定為：

(i) 某人知悉自己提供某器材、程式或數據（或其部分），或知悉自己為提供該器材、程式或數據（或其部分）而管有它；及

(ii) 某人知悉、相信、有合理理由相信，或聲稱某器材、程式或數據（或其部分）主要用作干犯電腦網絡相關罪行。

(e) 某人如聲稱（不論該項聲稱是否屬實）或誤信某器材、程式或數據主要用作干犯電腦網絡相關罪行，亦應屬犯罪，猶如任何人即使就所販運物質的性質構成罪責的信念原來出錯，亦屬干犯企圖販運危險藥物罪一樣。

(f) 在新法例下，蓄意提供被製造或改裝以用作干犯電腦網絡相關罪行的器材、程式或數據（或其部分），或蓄意為提供該器材、程式或數據而管有它，不論它是有形物或無形

---

1 即非法取覽程式或數據、非法截取電腦數據、非法干擾電腦數據及非法干擾電腦系統。

物（例如勒索軟件、病毒或其源碼），在以下情況下應構成加重罪行，而合理辯解可作為法定免責辯護：

(i) 該器材、程式或數據能夠用作干犯電腦網絡相關罪行，或犯罪者知悉、相信[2] 或聲稱該器材、程式或數據能夠用作干犯電腦網絡相關罪行；及

(ii) 犯罪者意圖任何人將該器材、程式或數據用作干犯電腦網絡相關罪行。

(g) 在新法例下，蓄意管有器材、程式或數據（或其部分），在以下情況下應構成加重罪行，而合理辯解可作為法定免責辯護：

(i) 該器材、程式或數據能夠用作干犯電腦網絡相關罪行，或犯罪者知悉、相信[3] 或聲稱該器材、程式或數據能夠用作干犯電腦網絡相關罪行；及

(ii) 犯罪者意圖將該器材、程式或數據用作干犯電腦網絡相關罪行。

(h) 除上述另有規定外，建議的條文應以英格蘭及威爾斯《誤用電腦法令》第 3A 條，以及新加坡《誤用電腦法令》第 8 及 10 條為藍本。

最終建議 10

我們建議，除合理辯解可作為法定免責辯護外，提供用作干犯電腦網絡相關罪行的器材、程式或數據罪（或為提供用作干犯電腦網絡相關罪行的器材、程式或數據而管有罪）應有以下特定的免責辯護：

(a) 為網絡安全目的提供有關器材、程式或數據（或為了為網絡安全目的提供該器材、程式或數據而管有它）：

(i) 這項免責辯護應只適用於為真正的網絡安全目的而行事的經認可網絡安全從業員（其資格會根據政府所設立的制度認可）；

---

2 包括某人有合理理由相信該器材、程式或數據能夠用作干犯電腦網絡相關罪行的情況。

3 同上。

(ii) 在顧及整體情況後，該網絡安全從業員的目的和行為必須是合理的；及

(iii) 這項免責辯護應延伸至：

(1) 獲網絡安全從業員事先批准或授權，為網絡安全目的而管有或提供該器材、程式或數據的人；及

(2) 協助網絡安全從業員履行其專業職務的人。

(b) 為真正的教育、科學或研究目的提供有關器材、程式或數據（或為了為真正的教育、科學或研究目的提供該器材、程式或數據而管有它）。在顧及整體情況後，援引這項免責辯護的人的行為必須是合理的。

(c) 以歐洲聯盟《數位服務法案》（Digital Services Act）第 4 條為藍本，規定凡任何互聯網服務提供者[4] 作為提供有關器材、程式或數據（或為提供該器材、程式或數據而管有它）的純導管，則該提供者如證明以下事項，即為免責辯護：

(i) 它並無啟動傳送該器材、程式或數據（“**違法內容**”）；

(ii) 它並無選定該項傳送的接收人；及

(iii) 它並無選定或修改該項傳送所載的違法內容。

(d) 以《數位服務法案》第 6 條為藍本，規定凡任何服務提供者[5] 的服務包括儲存及／或發布服務對象所提供的器材、程式或數據，而該服務提供者察覺或有合理理由相信，服務對象已提供違法內容或已提供途徑接達（不論以直接或間接方式）該違法內容，則該服務提供者如證明以下事項，即為免責辯護：

(i) 它知悉或有合理理由相信上述事宜後，已在合理地切實可行的範圍內盡快移除該違法內容或使該違法內容不能被接達；或

---

4 我們建議採納如《版權條例》（第 528 章）第 65A(2)條中“服務提供者”那般廣闊的定義，以涵蓋大大小小的服務提供者，以及設立網上空間（例如論壇或網站）以寄存或儲存程式或數據的個人。

5 同上。

(ii) （如移除該違法內容或使該違法內容不能被接達，在技術上不可行或並不合理地切實可行）它已在合理地切實可行的範圍內，就存在該違法內容盡快向執法機關備案。

(e) 凡違法內容純粹藉某自動化程序、工具或科技而提供，則任何人如證明以下事項，即為免責辯護：

(i) 他並無蓄意參與設計、製作或產生該違法內容；及

(ii) 他並無蓄意參與使該違法內容成為該自動化程序一部分的過程。

最終建議 15

我們建議，在以下情況下，就建議的提供用作干犯電腦網絡相關罪行的器材、程式或數據罪（或為提供用作干犯電腦網絡相關罪行的器材、程式或數據而管有罪），香港的法庭應具有司法管轄權：

(a) 就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）在香港發生，即使其他有關作為、不作為或事情在其他地方發生（例如身處香港的人在暗網上提供用作干犯電腦網絡相關罪行的器材、程式或數據）；

(b) 犯罪者是香港永久性居民、通常居於香港的人，或在香港經營業務的公司；或

(c) 犯罪者的作為，已導致或可能導致對香港的嚴重損害（例如導致對香港的基礎建設或公共機構的嚴重損害，或已威脅或可能威脅香港的安全）。

最終建議 16(d)

就建議的提供用作干犯電腦網絡相關罪行的器材、程式或數據罪（或為向他人提供該等器材、程式或數據而管有罪）而言，我們建議犯罪者應可處下述最高刑罰：

(i) 如屬基本罪行，一經循簡易程序定罪，可處兩年監禁，一經循公訴程序定罪，可處七年監禁；或

(ii) 如屬加重罪行，一經循公訴程序定罪，可處 14 年監禁。

簡易程序的時效期

最終建議 3

我們建議，儘管有《裁判官條例》（第 227 章）第 26 條的規定，適用於循簡易程序就任何建議罪行提出檢控的時效期，應為發現就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）後的兩年。

附件

諮詢回應者名單

我們收到下列回應者[1]的意見：

1. Asia Cloud Computing Association
2. 亞洲科龍有限公司
3. Cheng Horace
4. 張先生
5. 雲安全聯盟香港澳門分會
6. 消費者委員會
7. Criminal Law Reform Now Network
8. 香港海關
9. 香港警務處網絡安全及科技罪案調查科
10. 民主建港協進聯盟
11. Dyer Allan
12. eWalker Consulting (HK) Limited
13. 香港工業總會
14. Fg Fg
15. 香港金融科技協會
16. Fung Sammy
17. 馮澤謙
18. Gee Sui Wah William
19. 何先生
20. 香港應用科技研究院有限公司
21. 香港大律師公會

---

[1] 按本附件的英文文本所示的次序排列。

22. 香港電腦學會

23. 香港女律師協會有限公司

24. 香港總商會

25. 香港互聯網註冊管理有限公司

26. 香港互聯網供應商協會

27. 香港專業及資深行政人員協會

28. 香港國際公證人協會

29. 香港女工商及專業人員聯會

30. 許佳龍及周佳利（香港科技大學商學院資訊、商業統計及營運學系）

31. Ieong Ricci

32. 資訊保安及法證公會

33. 知識產權署

34. 國際信息系統審計協會（中國香港分會）

35. 法律援助署

36. 物流及供應鏈多元技術研發中心有限公司

37. 母親的抉擇

38. 通訊事務管理局辦公室

39. 政府資訊科技總監辦公室

40. 個人資料私隱專員公署

41. Open Web Application Security Project (Hong Kong Chapter)

42. 民主思路

43. 龐博文

44. 姚兆明教授（香港大學計算機科學系）

45. 西貢區撲滅罪行委員會

46. S-TECH Limited

47. Suen Owen

48. 司徒琬

49. 電視廣播有限公司

50. 當值律師服務

51. 香港與內地法律專業聯合會有限公司

52. 香港公司治理公會

53. 澳洲管理會計師公會（香港分會）

54. 香港律師會

55. 香港地產建設商會

56. 明光社

57. 曾廣熙

58. 灣仔區撲滅罪行委員會

59. 王維

60. 王先生

61. 黃浩華

62. 小市民

63. 碧海

64. 匿名

65. 匿名