香港法律改革委員會

電腦網絡罪行小組委員會

諮詢文件

依賴電腦網絡的罪行及司法管轄權事宜

本諮詢文件已上載互聯網，網址為：<**http://www.hkreform.gov.hk**>。

2022 年 **6** 月

本諮詢文件是由法律改革委員會（法改會）屬下的電腦網絡罪行小組委員會擬備，以供各界人士討論及發表意見。本諮詢文件的內容並不代表法改會或小組委員會的最終意見。

小組委員會歡迎各界人士就本諮詢文件發表意見，並請於 **2022** 年 **10** 月 **19** 日或之前將有關的書面意見送達：

香港中環

下亞厘畢道 **18** 號

律政中心東座 **4** 樓

法律改革委員會

電腦網絡罪行小組委員會秘書

電話：**(852) 3918 4097**

傳真：**(852) 3918 4096**

電郵：**hklrc@hkreform.gov.hk**

法改會和小組委員會日後與其他人士討論或發表報告書時，可能會提述和引用各界人士就本諮詢文件所提交的意見。任何人士如要求將他提出的所有或部分意見保密，法改會當樂於接納，惟請清楚表明，否則法改會將假設有關意見無須保密。

法改會在日後發表的報告書中，通常會載錄就本諮詢文件提交意見的人士的姓名。任何人士如不願意接納這項安排，請於書面意見中表明。

香港法律改革委員會

電腦網絡罪行小組委員會

諮詢文件

依賴電腦網絡的罪行及司法管轄權事宜

目錄

頁

第 3 章　非法截取電腦數據

頁

第 4 章　非法干擾電腦數據

第 5 章　非法干擾電腦系統

頁

第 8 章　判刑

第 9 章　綜合建議及諮詢問題

頁

界定用語

用語／簡稱	定義
《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）
CCP 制度	認證網絡專業人員保證服務（Certified Cyber Professional assured service）
鄭嘉儀案	*律政司司長 訴 鄭嘉儀*（*Secretary for Justice v Cheng Ka Yee*）(2019) 22 HKCFAR 97, [2019] HKCFA 9
朱峻瑋案	*香港特別行政區 訴 朱峻瑋*（*HKSAR v Chu Tsun Wai*）(2019) 22 HKCFAR 30, [2019] HKCFA 3
《刑事司法管轄權條例》	《刑事司法管轄權條例》(第 461 章)
《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）
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”）
Ex parte United States	*R v Bow Street Metropolitan Stipendiary Magistrate, Ex parte United States (No 2)* [2000] 2 AC 216
《說明報告》	《布達佩斯公約說明報告》（Explanatory Report to the Budapest Convention）

香港	香港特別行政區
國際認可論壇	國際認可論壇（International Accreditation Forum）
《截取通訊及監察條例》	《截取通訊及監察條例》（第 589 章）
法釋〔2011〕19 號	《最高人民法院、最高人民檢察院關於辦理危害計算機信息系統安全刑事案件應用法律若干問題的解釋》
《調查權力法令》	《2016 年調查權力法令》（Investigatory Powers Act 2016）（英格蘭及威爾斯）
《示範法典委員會報告書》	示範刑事法典人員委員會（Model Criminal Code Officers Committee），《報告書》，第 4 章：《損壞及電腦罪行及對第 2 章：司法管轄權的修訂》（2001 年）（*Report, Chapter 4, Damage and Computer Offences and Amendments to Chapter 2: Jurisdiction (2001)*）
《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》
《新西蘭法令》	《1961 年刑事罪行法令》（Crimes Act 1961）（新西蘭）
外交部駐港公署	中華人民共和國外交部駐香港特派員公署
中國	中華人民共和國
《中國刑法》	《中華人民共和國刑法》

《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*）
最高人民檢察院指導性案例	中國最高人民檢察院公布的指導性案例
第 161 條	《刑事罪行條例》（第 200 章）第 161 條
第 27A 條	《電訊條例》（第 106 章）第 27A 條
《電訊（截取及取覽）法令》	《1979 年電訊（截取及取覽）法令》（聯邦）（Telecommunications (Interception and Access) Act 1979 (Cth)）（澳大利亞）
英國	聯合王國
聯合國毒罪辦	聯合國毒品和犯罪問題辦公室（United Nations Office on Drugs and Crime，“UNODC”）
美國	美利堅合眾國
黃得強案	*香港特別行政區 訴 黃得強*（*HKSAR v Wong Tak Keung*）(2015) 18 HKCFAR 62, FACC 8/2014
《無線電訊法令》	《2006 年無線電訊法令》（Wireless Telegraphy Act 2006）（英格蘭及威爾斯）

導言

引言

1. 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。

2. 香港特別行政區政府於 2000 年召開電腦相關罪行跨部門工作小組，進行了香港特別行政區（"**香港**"）迄今為止最近期的電腦網絡罪行官方研究。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。在這背景下，終審法院首席法官聯同律政司司長於 2019 年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電腦網絡罪行小組委員會探討法律現況和提出建議。

3. 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，並在香港公布實施。香港維護國家安全的責任，再次確認有需要改革香港的電腦網絡罪行法律，[1] 小組委員會研究電腦網絡罪行這課題時已將此考慮在內。

研究範圍

4. 2019 年 1 月，電腦網絡罪行小組委員會就電腦網絡罪行課題展開研究，研究範圍如下：

> "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；

[1] 除了《國安法》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。

(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

5. 小組委員會由梁鎮宇先生擔任主席，成員如下：

梁鎮宇先生 ***（主席）***	德同國際有限法律責任合夥 資深顧問律師
方永佳先生 （任期由 2018 年 12 月 13 日至 2020 年 9 月 13 日）	前香港海關版權及商標調查（行動）課監督
何沈潔玲女士 （任期由 2018 年 12 月 13 日至 2020 年 12 月 20 日）	前香港上海滙豐銀行有限公司亞太區復元風險管理主管
徐詩妍女士 （任期由 2019 年 8 月 12 日起）	保安局首席助理秘書長
陳政龍先生，SC	資深大律師
陳淑儀女士	律政司助理刑事檢控專員
曾裕彤先生 （任期由 2018 年 12 月 13 日至 2019 年 8 月 9 日）	前保安局首席助理秘書長
湯熾忠先生	消費者委員會副總幹事
黃佩琪女士，SC	資深大律師

黃蕙荃女士 （任期由2020年9月14日起）	香港海關版權及商標調查（行動）課監督
葉旭暉先生	香港互聯網供應商協會主席
鄒錦沛博士	香港大學計算機科學系副教授
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總監
鄭松岩博士 （任期由2022年1月12日起）	中國銀行（香港）有限公司首席信息官
鄭麗琪女士 （任期由2022年5月3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）	前羅本信律師行合夥人
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
關煜群博士	亞太互聯網中心首席執行官

6. 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。政府律師李灝棋先生也為小組委員會提供協助。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。

研究內容

7. 自討論初期，我們便發現電腦網絡罪行並無普遍接納的歸類方式。

8. 本諮詢文件的第 1 章描述電腦網絡罪行以往如何以不同方式歸類。就本諮詢文件而言，我們採用聯合國毒品和犯罪問題辦公室（United Nations Office on Drugs and Crime，“**聯合國毒罪辦**”）所使用的術語，把罪行分為“依賴電腦網絡”（cyber-dependent）和“借助電腦網絡”（cyber-enabled）兩類性質。聯合王國（“**英國**”）政府的以下闡釋有助理解：[2]

(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”*；及

(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”*。

項目的三個劃定部分

9. 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。具體而言：

(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，並嘗試應對數碼時代的宏觀挑戰，包括數據主權（亦稱為電腦網絡、數碼或技術主權），而第二部分的範圍須待適當時候再作討論。數據主權的要旨，在於地方應能夠就其數碼基礎建設及科技應用作出自主行動和決策。數據主權亦與確保數碼基礎建設安全的工作，以及地方在與它領土和公民有關的數碼通訊事宜方面的權限息息相關；[3] 及

(c) 第三部分會處理證據事宜及執法（程序）事宜。

---

2 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*）（英國政府，2016 年），第 3.2 段，登載於 https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 （於 2022 年 5 月 3 日瀏覽）。

3 Julia Pohle & Thorsten Thiel, “Digital Sovereignty”, Internet Policy Review: Journal on internet regulation (2020), Vol 9, Issue 4，第 8 頁。

小組委員會的研究方法

第一部分研究的五類依賴電腦網絡的罪行

10. 本諮詢文件關乎項目的第一部分。我們借鑑歐洲委員會（Council of Europe）的《電腦網絡罪行公約》（Convention on Cybercrime，**《布達佩斯公約》**）及俄羅斯聯邦（Russian Federation）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），[4] 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：

(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) 提供或管有用作犯罪的器材或數據。

比較研究

11. 我們參考(a)《布達佩斯公約》的規定及(b)香港和其他七個司法管轄區（即澳大利亞、加拿大、英格蘭及威爾斯、中國內地、新西蘭、新加坡和美利堅合眾國（“**美國**”））的法例，[5] 檢視上述罪行及相關的司法管轄權事宜。這些司法管轄區當中，有四個（即澳大利亞、加拿大、英格蘭及威爾斯和美國）是《布達佩斯公約》的締約方，另外四個（即香港、中國內地、新西蘭和新加坡）則並非締約方。

建議背後的指導原則

12. 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。

---

4 《布達佩斯公約》及《聯合國合作打擊網絡犯罪公約》草案的詳情載於第 1 章。

5 就澳大利亞、加拿大和美國而言，則指其聯邦法例。

本諮詢文件的格式

13. 本諮詢文件由以下各章組成：

(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 章先探討項目第一部份所涵蓋的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，即提供或管有用作犯罪的器材或數據。

(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 章臚列我們的綜合建議及諮詢問題。

14. 在這次諮詢工作中，小組委員會徵詢公眾對以下問題的意見：經考慮現有法例下適用於電腦網絡罪行的各項訂罪條文及其他相關條文，有關刑事法律是否需要改革；如認為需要的話，則採用何種改革方案為佳。我們旨在盡可能讓最多的公眾人士參與是次諮詢工作，並熱切期待能聽到社會各界不同聲音。我們希望本諮詢文件有助促進和便利公眾討論當中所提出的議題，並歡迎各界就此等議題發表意見、評論和建議，這將大力協助小組委員會達致研究範圍定下的目標。

第 1 章　電腦網絡罪行的歸類

引言

1.1　正如聯合國毒罪辦在其編寫的《網絡犯罪綜合研究》（Comprehensive Study on Cybercrime）所評析：

> "……互聯網和個人計算機設備的普遍存在意味着計算機系統或數據能夠輔助——至少在發達國家——幾乎所有犯罪行為。"[1]

1.2　換言之，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。此外，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。即使是同一筆者，在不同情況或刊物所採用的歸類及名稱亦未必一致。

在聯合國層面的歸類

1.3　在第十屆聯合國預防犯罪和罪犯待遇大會（the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders）期間，舉辦了一次涉及電腦網絡的犯罪問題講習班。當時，電腦網絡罪行劃分為兩類，各自的定義如下：

> "(a) 狹義上的電腦犯罪（'計算機犯罪'）：任何以電子操作為手段進行的針對計算機系統的安全及其所處理數據的非法行為；
>
> (b) 廣義上的電腦犯罪（'涉及計算機的犯罪'）：任何以計算機系統或網絡為手段進行的或與其有關的非法行為，包括利用計算機系統或網絡非法佔有、提供或分發信息等項犯罪。"[2]

1.4　聯合國毒罪辦在 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、借助電*

1　聯合國毒罪辦，《網絡犯罪綜合研究》（2013 年 2 月），第 18 頁，登載於 https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Chinese.pdf。

2　聯合國，"涉及計算機網絡的犯罪——涉及計算機網絡的犯罪問題講習班背景文件"（A/CONF.187/10，2000 年 2 月 3 日），第 14 段，登載於 https://www.un.org/chinese/events/10thCrimeCong/187_10.html。

腦網絡的罪行，以及網上性剝削和性虐待兒童這種特定罪行類型”。[3] 如導言所述，我們會在本諮詢文件使用“依賴電腦網絡的罪行”和“借助電腦網絡的罪行”這兩個詞語。

1.5 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。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

1.6 《布達佩斯公約》於 2001 年 11 月 23 日開放予各國簽署，並於 2004 年 7 月 1 日生效。[4] 《布達佩斯公約》由一份於 2006 年 3 月 1 日生效的《附加議定書》（Additional Protocol）作為補充，[5] 似乎是首份規管電腦網絡空間的跨國協議。[6] 截至 2020 年 3 月 16 日，已有 65 個國家批准或加入《布達佩斯公約》。[7]

1.7 《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。[8] 《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“實質重於形式”）：

---

3 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/global-programme-cybercrime.html（於 2022 年 5 月 3 日瀏覽）。

4 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 2022 年 5 月 3 日瀏覽）。

5 全稱為《電腦網絡罪行公約關於宣告利用電腦系統犯下的種族主義或仇外行為為犯罪行為的附加議定書》（“Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems”）。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 2022 年 5 月 3 日瀏覽）。

6 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 2022 年 5 月 3 日瀏覽）。

7 歐洲委員會，“Colombia joined the Budapest Convention on Cybercrime”（2020 年 3 月 16 日），登載於 https://www.coe.int/en/web/cybercrime/-/colombia-joined-the-budapest-convention-on-cybercrime（於 2022 年 5 月 3 日瀏覽）。

8 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）（**《說明報告》**），第 33 段，登載於 https://rm.coe.int/16800cce5b（於 2022 年 5 月 3 日瀏覽）。

(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。

《電腦罪行及電腦相關罪行示範法》

1.8 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）[9]（**《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。[10]

1.9 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。[11]

其他司法管轄區法律的相符程度

1.10 如導言所述，本諮詢文件對七個司法管轄區的法律進行比較研究，即澳大利亞、加拿大、英格蘭及威爾斯、中國內地、新西蘭、新加坡和美國。對於該等法律與《布達佩斯公約》所訂規定的一致程度，下文闡述相關的歷史背景：

(a) 在加拿大，最高法院於 1980 年對 *R v McLaughlin*[12] 所作的決定，促使當局改革《刑事法典》（Criminal Code）以應對誤

---

9 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 2022 年 5 月 3 日瀏覽）。

10 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。

11 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 2022 年 5 月 3 日瀏覽）。

12 [1980] 2 SCR 331.

用電腦的問題。[13]《1985 年刑事法修訂法令》（Criminal Law Amendment Act 1985）和《1996 年刑事法改善法令》（Criminal Law Improvement Act 1996）先後在《刑事法典》加入第 342.1 條[14] 和第 430(1.1)條[15] 等多項電腦網絡罪行條文。1997 年 4 月，各方就後來的《布達佩斯公約》展開磋商，[16] 加拿大於 2001 年簽署《布達佩斯公約》。

(b) 在美國，《電腦欺詐及濫用法案》（Computer Fraud and Abuse Act）是應對電腦網絡罪行的主要聯邦法例，該法案於 1986 年制定，並編纂於《美國法典》第 18 篇第 1030 條（18 USC 1030）。《美國法典》第 18 篇第 1030 條的修訂歷程（1986 至 2008 年間共修訂九次）顯示，儘管美國於 2001 年成為《布達佩斯公約》的簽署國，該公約並沒有構成任何直接影響。[17]

(c) 英格蘭及威爾斯法律委員會（Law Commission of England and Wales）於 1989 年建議[18] 制定新法例，最終獲通過成為《1990 年誤用電腦法令》（Computer Misuse Act 1990，**《英格蘭誤用電腦法令》**）。《英格蘭誤用電腦法令》曾修訂數次，但該法令的整體框架於 2001 年英國簽署《布達佩斯公約》之後仍大致維持不變。

(d) 新加坡《1993 年誤用電腦法令》（Computer Misuse Act 1993，**《新加坡誤用電腦法令》**）於 1993 年制定，當中的罪行條文主要以《英格蘭誤用電腦法令》為基礎，但亦有若干差異。[19]

---

13 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 52 至 53 頁。

14 最初編為第 301.2(1)條，現已重新編號，該條的標題是 *"在未獲授權下使用電腦"*（*Unauthorized use of computer*）。

15 最初編為第 387(1.1)條，現已重新編號，該條的標題是 *"與電腦數據有關的損害"*（*Mischief in relation to computer data*）。

16 《說明報告》第 12 段。

17 此書有相關闡述：H Marshall Jarrett, Michael W Bailie, Ed Hagen and Scott Eltringham, *Prosecuting Computer Crimes* (Office of Legal Education, Executive Office for United States Attorneys, 2nd edition, 2010)，第 1 至 3 頁，登載於 https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf（於 2022 年 5 月 3 日瀏覽）。

18 法律委員會，*Criminal Law: Computer Misuse*（1989 年），法律委員會第 186 號，登載於 https://www.lawcom.gov.uk/project/criminal-law-computer-misuse/（於 2022 年 5 月 3 日瀏覽）。

19 Gregor Urbas, "An Overview of Cybercrime Legislation and Cases in Singapore" (ASLI Working Paper No 001, December 2008)，第 1 頁，登載於 https://law.nus.edu.sg/asli/pdf/WPS001.pdf（於 2022 年 5 月 3 日瀏覽）。

(e) 在中國內地，《中華人民共和國刑法》（**《中國刑法》**）於 1997 年（亦即在《布達佩斯公約》2004 年生效前）在第二百八十五及二百八十六條引入電腦網絡罪行條文。[20] 2009 年，第二百八十五條加入更多條文，以擴大電腦網絡罪行的適用範圍。[21]

(f) 按照新西蘭法律委員會（Law Commission of New Zealand）於 1999 年的建議，[22] 新西蘭《1961 年刑事罪行法令》（Crimes Act 1961）於 2003 年加入規管電腦網絡罪行的現有條文（第 248 至 252 條）。從法律委員會報告書所述的立法背景看來，《布達佩斯公約》對新西蘭有關法例的草擬工作並沒有重大影響，甚或毫無影響。

(g) 澳大利亞《刑事法典》（聯邦）（Criminal Code (Cth)）中的電腦網絡罪行條文，乃源於示範刑事法典人員委員會（Model Criminal Code Officers Committee）於 2001 年發表的報告書（**《示範法典委員會報告書》**）。[23] 一份就相關的《2001 年電腦網絡罪行法案》（Cybercrime Bill 2001）所發表的國會文件[24] 顯示，《英格蘭誤用電腦法令》對《示範法典委員會報告書》的方針有 *"明顯影響"*，該報告書亦參照了當時的《布達佩斯公約》草案。儘管如此，而澳大利亞於 2012 年亦批准了《布達佩斯公約》，[25] 界定澳大利亞有關罪行的立法措辭自 2001 年制定以來，均與《英格蘭誤用電腦法令》頗為不同，事實上與直接以《布達佩斯公約》

---

20 《中國刑法》修訂自 1997 年 10 月 1 日起實施。

21 《中國刑法》加入了第二百八十五條第二及三款。由於這些修訂自 2009 年 2 月 28 日起施行，因此非法取覽程式或數據罪亦一般適用於計算機信息系統，並訂立了提供或管有用作犯罪的器材或數據罪。

22 新西蘭法律委員會，*Computer Misuse*（1999 年），第 54 號報告書，登載於 https://www.lawcom.govt.nz/our-projects/computer-crime?id=814（於 2022 年 5 月 3 日瀏覽）。

23 示範刑事法典人員委員會，《報告書》，第 4 章：《損壞及電腦罪行及對第 2 章：司法管轄權的修訂》（*Report, Chapter 4, Damage and Computer Offences and Amendments to Chapter 2: Jurisdiction*）（2001 年 1 月）。該報告書的存檔副本曾登載於律政部（Attorney-General's Department）網站，現時可通過 "Wayback Machine" 查閱（有關部分是第 4 章第 4.2 部），網址為 https://web.archive.org/web/20060920231025/http://www.ag.gov.au/agd/WWW/rwpattach.nsf/viewasattachmentPersonal/(0AFA115E182148C186311CED66C0728D)~modelcode_ch4_Computer_offences_report.pdf/$file/modelcode_ch4_Computer_offences_report.pdf（於 2022 年 5 月 3 日瀏覽）。

24 Department of the Parliamentary Library, *Bills Digest No 48 2001-02* (2001)，登載於 https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd0102/02bd048（於 2022 年 5 月 3 日瀏覽）。

25 按《2012 年電腦網絡罪行法例修訂法令》（聯邦）（Cybercrime Legislation Amendment Act 2012 (Cth)）的詳題所述，這是 *"為實施《歐洲委員會布達佩斯電腦網絡罪行公約》和其他目的而訂立的法令"*，見 https://www.legislation.gov.au/Details/C2012A00120（於 2022 年 5 月 3 日瀏覽）。

為基礎的《示範法》亦有相當差異。

聯合國的最新動向

1.11 國際間對電腦網絡罪行的規管情況正在急速變化。聯合國有兩個動向可能會產生影響，值得密切關注：

(a) 俄羅斯聯邦於 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（**《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。[26]

(b) 然而，最近大會於 2019 年 12 月 27 日採納的第 74/247 號決議[27] 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"。[28]

1.12 若日後在聯合國的框架內訂立關於電腦網絡罪行的條約，該條約所採納的歸類及名稱或許會逐漸成為權威。

---

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

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

28 第 3 段。2021 年 5 月，特設委員會在組織會議上選舉主席團成員並討論其進一步活動的綱要和方法。見 https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home（於 2022 年 5 月 3 日瀏覽）。然而，由於 2019 冠狀病毒病大流行持續，該委員會的首次會議推遲至 2022 年 2 月 28 日至 3 月 11 日。見：聯合國毒罪辦，"First session of the Ad Hoc Committee"，登載於 https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html（於 2022 年 5 月 3 日瀏覽）。

第 2 章　非法取覽程式或數據

引言

2.1　我們會在本章探討五大類依賴電腦網絡的罪行中的第一類：非法取覽電腦中的程式或數據。這類罪行須與非法截取電腦數據區分開來，後者會是下一章的討論重點。概括而言，就非法取覽電腦中的程式或數據而訂立的罪行，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。

2.2　黑客入侵大概是該罪行最典型的例子。此外，至少在某些司法管轄區，[1] 任何獲授權取用電腦的人（例如操作僱主電腦的僱員）在授權範圍外行事，便可能犯罪。

2.3　我們在考慮非法取覽程式或數據罪時，緊記電腦網絡空間的性質獨特。作為起點，在未獲授權下取用電腦（或取覽存於電腦內的程式或數據），可比喻為在現實世界中，陌生人在未獲准許下進入某地方（例如某人的居所）的情境。

2.4　定奪現實世界中入侵的刑事法律責任較為簡單直接，是因為實體空間的界線是有形的，這令在未獲授權下進出的概念有相對明確的定義。舉例來說，陌生人若“進出”他人的住所，便至少曾親身踏足該住所，而且其作為顯然有所不妥。此外，在現實世界中，受害人亦較容易阻止入侵者。

2.5　相反，電腦網絡空間則是截然不同的情境。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

---

[1]　舉例來說，香港、澳大利亞和美國（見第 2.9、2.23 至 2.26 及 2.83 至 2.88 段）。

聯網，[2] 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。

香港的現行法律

《刑事罪行條例》（第 200 章）

第 161 條

2.6 《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**”）有以下規定：

> “(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）；
>
> (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

---

[2] 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。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 2022 年 5 月 3 日瀏覽）。

(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。”

第 161 條所訂的犯罪行為

2.7 *律政司司長 訴 鄭嘉儀*[3]（*Secretary for Justice v Cheng Ka Yee*，“***鄭嘉儀案***”）是關於第 161 條的主導案例。終審法院按照第 161 條的文本、文意和目的來解釋該條文，並對有關犯罪行為（“取用”，“obtain access”）有以下評析：

> “‘Obtain（獲得）’一詞……若用來描述某人使用自己的器材，顯然格格不入，‘access（取用）’一詞亦是如此……從語言的角度來看，一個人必然是本來沒有取用某物，其後才‘獲得’對該物的取用。”[4]

2.8 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”*。[5] 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 條不適用於下述情況：

(a) 任何人使用*自己的*電腦設立仿冒詐騙網站；及

(b) 任何人使用*自己的*智能電話拍攝裙底。[6]

取用的未獲授權性質

2.9 雖然從表面上看，第 161 條並無規定有關取用須屬未獲授權，但法院似乎都將該條解釋為包含這項要求。[7] 在這方面，涉及根本沒有授權的案件相對上簡單直接。在多個司法管轄區，爭議點往往在犯罪者（例如僱員）在超逾授權範圍下行事的案件中產生。*香港特*

---

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

4 同上，第 38 段。

5 同上，第 48 段。

6 第 161 條並無界定何謂“電腦”。早於*鄭嘉儀*案之前，在*律政司司長 訴 王嘉業* [2013] 4 HKLRD 588, HCMA 77/2013（判決日期：2013 年 4 月 29 日）這宗高等法院原訟法庭審理的裁判法院上訴案件，高等法院原訟法庭法官馮驊裁定，就根據第 161 條提出的檢控而言，能夠攝錄短片等的智能電話構成“電腦”。馮驊法官並無採用《證據條例》（第 8 章）第 22A(12)條、《稅務條例》（第 112 章）第 26A 條及《商業登記條例》（第 310 章）第 19 條對“電腦”所下的定義，即*“任何用作儲存、處理或檢索資料的器材”*，而是採用《牛津網上字典》對該詞（computer）的定義：
“一個電子裝置，可以接收某一特定形式的資訊，並可以按照預定但可變的程式指令執行一連串的運算，從而產生資訊或訊號形式的結果”。

7 見上文註腳 3，第 38 段。

別行政區 訴 秦瑞麟（*HKSAR v Tsun Shui Lun*）[8]是一宗相關的香港案例，高等法院首席法官陳兆愷對該案作出以下裁定：

> "就第 161 條所訂罪行而言，本席認為在沒有權限的情況下取用與在超逾權限範圍下取用並無分別，亦不應存在分別。該條並沒有區分這兩種情況。"[9]

第 161 條所指"獲益"的涵蓋範圍

2.10 在*香港特別行政區 訴 秦瑞麟*，首席法官陳兆愷進一步把第 161 條的"獲益"一詞解釋為*"不限於在經濟上或所有權上的利益，而是足以包括無形利益"*，並可能屬*"短暫而非永久性質"*。[10] 按照此廣闊的詮釋，有關罪行適用於任何人從某電腦取得自己先前無法取覽的資料的情況。[11] 舉例來說，該案中的"獲益"是某病人的醫療紀錄，儲存於犯罪者任職的醫院的電腦系統。

《電訊條例》（第 106 章）

第 27A 條

2.11 與本章相關的另一條文是《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) 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；

---

8 [1999] 3 HKLRD 215, HCMA 723/1998（判決日期：1999 年 1 月 15 日），高等法院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。

9 [1999] 3 HKLRD 215，第 223 頁 D 行（第 22 段）。

10 同上，第 223 頁 G 行（第 24 段）。

11 同上，第 223 頁 J 行（第 25 段）。

(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。”

比較第 161 條與第 27A 條

2.12 在*香港特別行政區 訴 秦瑞麟*，高等法院首席法官陳兆愷將第 161 條與第 27A 條比較如下：

> “一方面，第 161 條的適用範圍較《電訊條例》第 27A 條廣闊，因為不論有關取用是否藉着電訊獲得，均有可能犯第 161 條所訂罪行。另一方面，第 161 條所訂罪行須證明犯罪或不誠實的特定意圖或目的，是較嚴重的罪行，這亦反映於該條文指明的最高刑罰。由此推論，並非對電腦的每類取用均構成第 161 條所訂罪行。”[12]

2.13 正如首席法官陳兆愷所述，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*鄭嘉儀案*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”*。[13]

---

12 同上，第 222 頁 B – C 行。

13 見上文註腳 3，第 41 段。

2.14 儘管有此定性，案例顯示，控方傾向根據第 161 條而非第 27A 條檢控黑客入侵事件。[14] *香港特別行政區 訴 譚曦倫及其他人*（*HKSAR v Tam Hei Lun & Ors*）[15] 是其中一例，案中的犯罪者使用名為 Back Orifice 的程式來取用其他互聯網用戶的電腦，並取得他們的登入名稱和密碼。涉及犯罪者使用另一部電腦進行黑客入侵的另一案例是*香港特別行政區 訴 謝文禮*（*HKSAR v Tse Man Lai*），[16] 案中的犯罪者兩度用自己的電腦向“披露易”網站的伺服器發動攻擊，並取得三個靜態影像和錄影片段。

顯然難以證明第 27A 條所訂罪行

2.15 根據第 161 條而非第 27A 條檢控黑客入侵案件，可能是因為控方顯然難以證明第 27A 條所訂的犯罪意念。此犯罪意念涉及的兩方面都以否定語句表達，即被告人：

(a) *“不相信自己已獲……授權”*，使他獲得有關種類的取用；及

(b) *“不相信若他曾申請適當的授權，則他本已獲如此授權”*。

2.16 相比之下，視乎案情而定，有時候可能較容易按照第 161 條的規定證明被告人意圖犯罪或不誠實。此外，正如上文指出，若被告人並非“藉着電訊”獲得有關取用，則第 27A 條並不適用。

2.17 在第 161 條及第 27A 條均可援引的情況下，條文的選擇可能事關重大，因為兩者所訂的最高刑罰各異：根據第 27A 條可處第 4 級罰款，[17] 而根據第 161 條循公訴程序定罪則可處監禁五年。

《布達佩斯公約》訂定罪行的標準

2.18 與本章重點相對應的是《布達佩斯公約》[18] 第一節之下的第一篇第二條：

---

14 迄今為止，似乎並沒有針對黑客入侵而援引第 27A 條的經彙報判決。以下文章探討了 1996 年一宗根據第 27A 條成功提出的檢控：Rynson W H Lau, Kwok-Yan Lam and Siu-Leung Cheung, “The Failure of Anti-Hacking Legislation: a Hong Kong Perspective” (Invited Paper in Proceedings of ACM Conference on Computer and Communications Security, March 1996)，第 62 – 67 頁。然而，未能找到任何書面判決。

15 [2000] 3 HKC 745, HCMA 385/2000（判決日期：2000 年 10 月 9 日）。

16 [2013] 3 HKLRD 691（此案例目前應在*鄭嘉儀*案的規限下予以解讀），CACC 455/2012（判決日期：2013 年 6 月 18 日）。

17 根據《刑事訴訟程序條例》（第 221 章）附表 8，現為 25,000 元。

18 有關《布達佩斯公約》的背景資料，見導言第 11 段，以及第 1 章第 1.6 至 1.10 段。

"各締約方均應採取必要的立法及其他措施，在其本土法律中將下列行為定為刑事罪行：在無權的情況下蓄意取用整個電腦系統或其任何部分。任何締約方可規定，任何人有取得電腦數據的意圖或其他不誠實意圖而違反保安措施，或就連接至另一電腦系統的電腦系統違反保安措施，即屬犯該罪行。"

2.19 《說明報告》對第二條的評註如下：

"44. '非法取用'涵蓋損害電腦系統及數據安全……的危險威脅及攻擊的基本罪行。組織及個人均享有以不受干擾及不受限制的方式管理、操作和控制其系統的權益，因此有需要就此獲得保障。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……及秘密，以及免費使用有關系統，甚或鼓勵黑客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。

……

46. '取用'涉及進入整個電腦系統或其任何部分(硬件、零件、已安裝系統所儲存的數據、目錄、流量數據及內容相關數據)，但並不包括純粹向該系統發送電郵訊息或檔案。'取用'包括進入另一電腦系統……或連接至同一網絡上某電腦系統……。通訊方法……屬無關重要。

47. 有關作為亦須在'無權'的情況下作出……如在有關系統或其任何部分的擁有人或其他權利持有人的授權下而取用……，不屬犯罪……取用開放予公眾自由取用的電腦系統，亦不屬犯罪……

48. 運用特定的技術工具可能會引致第二條所指的取用，例如取覽某網頁……運用這類工具本身不屬'無權'。如某公共網站維持存在，即意味着網站擁有人同意讓任何其他網絡用戶取覽該網站……

……

50. 各締約方可採取寬泛的方針，按照第二條首句把純粹的黑客入侵定為罪行；或者附加第二句列述的任何或所有規限元素：違反保安措施、取得電腦數據的特別意圖、有理由施加罪責的其他不誠實意圖，或規定犯該罪行須與遠程連接至另一電腦系統的電腦系統有關。[19] 若採用最後一個元素，各締約方便可豁除任何人實體取用一部獨立運作的電腦（而並無使用另一電腦系統）的情況。他們可以把該罪行限於非法取用已連接網絡的電腦系統……”[20]

其他司法管轄區的法定體制

澳大利亞

《刑事法典》（聯邦）第 477.1 及 478.1 條

2.20 在澳大利亞，《刑事法典》（聯邦）（Criminal Code (Cth)）第 478.1 條（*“在未獲授權下取覽或修改受限數據”*）規定如下：

“(1) 任何人在以下情況，即屬犯罪：

(a) 該人導致在未獲授權下取覽或修改受限數據；及

(b) 該人意圖導致該項取覽或修改；及

(c) 該人知悉該項取覽或修改未獲授權。

---

19 《說明報告》第 23 及 24 段對“電腦系統”一詞有以下論述：
“23. 《公約》所指的電腦系統是任何由硬件和軟件組成，為自動處理數碼數據而開發的器材。這種器材可能包括輸入、輸出和儲存設施，可能獨立運作或與其他相類器材連成網絡。‘自動’指無需直接的人為干預，‘處理數據’指通過執行電腦程式來運算電腦系統內的數據。‘電腦程式’是一組可由電腦執行，以達致預期產生的結果的指令。電腦可運行不同程式。電腦系統通常由不同器材組成，這些器材區分為處理器（亦稱中央處理器）和周邊設備。‘周邊設備’是任何通過與處理器互動而執行若干特定功能的器材，例如打印機、視像屏幕、光碟閱讀器／燒錄器或其他儲存器材。
24. 網絡是兩個或以上電腦系統的相互連接。這些連接可以是地面連接（例如導線或電纜）、無線連接（例如無線電、紅外線或衞星），或兩種形式兼用。就地域而言，網絡可能限於某個細小區域（局部區域網絡）又或涵蓋某個廣大區域（寬廣區域網絡），而這些網絡本身亦可能互連。互聯網是由眾多互連的網絡組成的全球網絡，全都採用相同的規約。其他類型的網絡亦能在電腦系統之間傳達電腦數據，不論這些網絡是否連接至互聯網。電腦系統連接至有關網絡，可能是作為端點，或用作協助該網絡上的通訊。至關重要的是數據能在網絡上交換。”

20 《說明報告》第 44、46 至 48 及 50 段。

刑罰：監禁 2 年。

(3) 在本條中：

受限數據指符合以下說明的數據：

(a) 存於某電腦內；及

(b) 其取覽受與該電腦任何功能相關的存取控制系統所限。”

2.21 此外，《刑事法典》（聯邦）第 477.1 條（*“在未獲授權下作出取覽、修改或損害，並意圖干犯嚴重罪行”*）實際上是在未獲授權下取覽電腦數據的加重罪行。該條文把三類錯誤行為定為不合法，在未獲授權下取覽電腦數據是其中之一：

“意圖干犯聯邦、各州或領地的嚴重罪行

(1) 任何人在以下情況，即屬犯罪：

(a) 該人導致：

(i) 在未獲授權下取覽存於某電腦內的數據；或

(ii) 在未獲授權下修改存於某電腦內的數據；或

(iii) 在未獲授權下損害往來某電腦的電子通訊；及

(c) 該人知悉該項取覽、修改或損害未獲授權；及

(d) 該人意圖藉該項取覽、修改或損害而干犯或利便干犯任何違反聯邦、各州或領地法律的嚴重罪行（不論是由該人干犯或由他人干犯）。

(3) 在就違反第(1)款的罪行而提出的檢控中，無須證明被告人知悉有關罪行是：

(a) 違反聯邦、各州或領地法律的罪行；或

(b) 嚴重罪行。

刑罰

(6) 任何人犯違反本條的罪行，一經定罪，可處不超過適用於嚴重罪行的刑罰。

不可能性

(7) 即使干犯有關嚴重罪行並不可能，任何人仍可被裁定犯違反本條的罪行。

企圖犯罪不屬犯罪

(8) 企圖干犯違反本條的罪行，不屬犯罪。

嚴重罪行的涵義

(9) 在本條中：

嚴重罪行指可處終身監禁或為期 5 年或以上監禁的罪行。"

企圖取覽但不成功

2.22 在本章探討的法定條文中，第 477.1 條有其獨特之處，當中第 477.1(8)條明文免除企圖犯罪的刑事法律責任。第 477.1 條顯然僅適用於企圖並成功取覽的情況。

取覽的未獲授權性質

2.23 《示範法典委員會報告書》構成《刑事法典》（聯邦）所載電腦網絡罪行條文的基礎，該報告書對取覽的未獲授權性質有以下論述：

"任何個人就某目的獲得授權，但為另一隱秘目的行事，應否屬犯本部所訂罪行？如果原有授權是以與犯罪者目的有關的欺騙手段取得，無疑應施加法律責任；但如果授權是在並無欺詐的情況下取得，而被告人誤用該授權，則不能一定得出應施加法律責任的結論。這點顯然具爭議性……" [21]

---

[21] 《示範法典委員會報告書》，第 4 章：《損壞及電腦罪行及對第 2 章：司法管轄權的修訂》（2001 年），第 141 頁。

2.24 其後制定的《刑事法典》（聯邦）第 476.2(1)及(2)條有以下規定：

(a) *"如任何人取覽存於某電腦內的數據……而該人無權導致該項取覽……，則該人的該項取覽……即屬未獲授權"*；但

(b) *"該人導致的任何上述取覽……，不會純粹因為該人導致該項取覽……時有隱秘目的而屬未獲授權"*。

2.25 新南威爾士上訴法院對 *Salter v DPP (NSW)*[22] 所作的決定，揭示應如何理解上述條文。在該案中，法院對《1900 年刑事罪行法令》（新南威爾士）（Crimes Act 1900 (NSW)）第 308B(2)條（《刑事法典》（聯邦）第 476.2(2)條在州法例中的對等條文）有以下詮釋：

> "第 308B(2)條旨在保障任何有合法權利取覽特定數據，但可能是另有隱秘目的而取覽該等數據的人員〔在該案中是一名警務人員〕。因此，即使另有隱秘目的，有關人員只要有合法目的便不會違反該法令……該款的目的是確保任何人在行使其權限而取用〔電腦〕系統時，不會'純粹'因為另有某種隱秘目的而犯罪。"[23]

2.26 法院最終維持對犯罪者的定罪，因為 *"她〔純粹〕為私人目的而取覽〔有關數據〕，這與她代表警方履行的職能毫無關連"*。[24]

加拿大

《1985 年刑事法典》第 326(1)(b)及 342.1(1)條

2.27 加拿大《1985 年刑事法典》（Criminal Code 1985）訂有兩項相關條文。第一項是第 326(1)(b)條（*"盜取電訊服務"*），根據該條：

> "任何人意圖欺詐、惡意或在無表面權利[25] 的情況下……使用任何電訊設施或取得任何電訊服務，即屬犯盜竊罪。"

---

22 [2011] NSWCA 190.

23 同上，第 19 及 25 段（首席法官麥克萊倫（McClellan CJ））。

24 同上，第 24 段（首席法官麥克萊倫）。

25 "表面權利（colour of right）"一詞指 *"真誠地相信某事實狀況，而該狀況若實際存在，便會在法律上構成所作行為的理由或辯解"*（上訴法院法官馬丁（Martin JA）在 *R v DeMarco* (1973) 13 CCC (2d) 369 第 372 頁的判詞，於 *R v Simpson* [2015] 2 SCR 827 獲引用和認同）。

2.28 第二項是第 342.1(1)條（*“在未獲授權下使用電腦”*）：

> “任何人意圖欺詐並在無表面權利的情況下作出以下作為，即屬犯可公訴罪行，可處為期不超過 10 年的監禁，或屬犯可循簡易程序定罪而懲處的罪行：
>
> (a) 直接或間接取得任何電腦服務；
>
> (b) 藉電磁、聲音、機械或其他器材直接或間接截取某電腦系統的任何功能，或導致藉電磁、聲音、機械或其他器材直接或間接截取某電腦系統的任何功能；
>
> (c) 直接或間接使用某電腦系統，或導致直接或間接使用某電腦系統，意圖干犯(a)或(b)段所訂罪行，或就電腦數據或某電腦系統干犯第 430 條所訂罪行；或
>
> (d) 使用、管有、非法傳送或准許他人取覽某電腦密碼，而該密碼會使某人能夠干犯(a)、(b)或(c)段所訂罪行。”

犯罪行為

2.29 這兩項條文界定犯罪行為時，均提述被告人“使用”電訊設施或電腦系統等。某些學者認為“使用”一詞較“取用或取覽”為佳。舉例來說，某評論員曾對兩詞作出以下比較：

> “科技匯流、非對稱數碼用戶線路（asymmetric digital subscriber line，英文簡稱 ADSL）[26] 及寬頻的使用、無線互聯網以及網絡的不精確性均創造出一種環境，令‘使用’電腦的說法比取用電腦更加準確。採用廣闊的定義，有助避免關於何謂取用或取覽而又往往帶有武斷成分的技術性爭論，令人能夠適當聚焦於餘下的元素。這些元素會決定有關行為的刑責，有助避免涵蓋過廣。”[27]

---

26 憑藉這項技術，以往用來連接電話的銅線現在可支援連接互聯網。

27 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 79 頁。這段見於作者對美國法律的論述，但他的評析亦適用於提述“使用”電腦系統的加拿大法律。

2.30　但就現況來看，加拿大《刑事法典》並無界定何謂“使用”。該詞到底是僅指實際上使用電腦系統，還是亦引伸指毫無實效地使用電腦系統（包括企圖但不成功取用），可能有爭議空間。

主要詞語的法定定義

2.31　該法典也並無界定何謂“電腦”。然而，該法典第 342.1(2)條訂有“電腦數據”、“電腦密碼”、“電腦程式”、“電腦服務”、“電腦系統”及“功能”等詞語的定義。

2.32　當中，該法典對“功能”所下的定義既廣闊而又並非巨細無遺，“功能”包括 *“邏輯、控制、算術運算、刪除、儲存及檢索，以及往來某電腦系統或在某電腦系統內的通訊或電訊”*。這使“電腦系統”一詞涵蓋廣泛，其法定定義載於下文：

> “***電腦系統***指任何符合以下說明的器材，或一組互連或相關的器材，而其中一部或多於一部器材：
>
> (a) 包含電腦程式或其他電腦數據，並且
>
> (b) 藉電腦程式而：
>
> (i) 執行邏輯和控制，以及
>
> (ii) 可執行任何其他功能”。

英格蘭及威爾斯

《英格蘭誤用電腦法令》第 1 條

2.33　在英格蘭及威爾斯，《英格蘭誤用電腦法令》第 1 條（*“在未獲授權下取覽電腦資料”*）有以下規定：

> “(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。

(3) 任何人犯本條所訂罪行——

(a) 一經在英格蘭及威爾斯循簡易程序定罪，可處為期不超過 12 個月的監禁或不超過法定最高罰款，或兩者兼處；

(b) 〔……〕

(c) 一經循公訴程序定罪，可處為期不超過 2 年的監禁或罰款，或兩者兼處。”

“電腦”的涵義

2.34 與澳大利亞及加拿大的法例一樣，《英格蘭誤用電腦法令》沒有界定何謂“電腦”。皇家檢控署（Crown Prosecution Service）的網站載有以下論述：

> “〔《英格蘭誤用電腦法令》〕並無界定何謂電腦，因為在科技急速變遷的情況下，任何定義都會迅即過時。
>
> 因此，電腦的定義應交由法院決定，預期法院會採用該詞當時的涵義。在 *DPP v McKeown*, *DPP v Jones*（[1997] 2 Cr App R 155, HL，第 163 頁），賀輔明勳爵（Lord Hoffman）把電腦界定為‘任何用作儲存、處理和檢索資料的器材。’”[28]

[28] 皇家檢控署，“Legal Guidance, Computer Misuse Act”，登載於 https://www.cps.gov.uk/legal-guidance/computer-misuse-act（於 2022 年 5 月 3 日瀏覽）。

犯罪行為

2.35 第 1(1)(a)條所訂的犯罪行為是致使某電腦執行任何功能。法律委員會（Law Commission）在其編寫的報告書內（該報告書促成制定《英格蘭誤用電腦法令》），認為這種擬定方式較提述取用概念的擬定方式為佳，因為前者：

> "……涵蓋任何有適當的犯罪意圖而操控電腦的情況，而且……其所用詞語日後並不會因科技發展而變得過時。這種擬定方式排除了不涉及與電腦操作互動的純實體取用及純數據檢視。"[29]（強調之處乃原文所有）

2.36 上述犯罪行為提述到"電腦"，而第 1(1)(a)條繼而藉提述存於"任何電腦"內的任何程式或數據來界定犯罪意念。此法定措辭顯然涵蓋涉及兩部電腦的情況，即犯罪者把一部電腦用作工具，另一部電腦則存有程式或數據。

2.37 此外，英格蘭上訴法院在 *Attorney-General's Reference (No 1 of 1991)*[30] 裁定，上述條文中的"任何電腦"一詞包括因被告人而執行任何功能的電腦。換言之，該條文亦適用於涉及單一電腦的情境。[31]

企圖取覽但不成功

2.38 事實上，《英格蘭誤用電腦法令》第 1(1)(a)條對犯罪行為所下定義之廣，令純粹啟動電腦或嘗試不同密碼企圖取覽電腦中的程式或數據，表面上都足以構成犯罪行為[32]（不論該企圖最終是否成功）。除了《布達佩斯公約》訂定罪行的標準之外，[33] 純粹在未獲授權下取覽(當中會涉及企圖並成功取覽)應屬犯罪並未廣獲接納。[34] 支持將企圖但不成功取覽定為罪行的理由，可說是更為薄弱。

---

29 法律委員會，*Criminal Law: Computer Misuse*（1989 年），法律委員會第 186 號，第 3.26 段。

30 [1993] QB 94.

31 為作比較，如上文所述，《布達佩斯公約》的各締約方可選擇免除 *"任何人實體取用一部獨立運作的電腦（而並無使用另一電腦系統）的情況"* 所涉的刑事法律責任（《說明報告》第 50 段）。

32 法律委員會，*Criminal Law: Computer Misuse*（1989 年），法律委員會第 186 號，第 3.20 及 3.26 段。

33 *"原則上，純粹在未獲授權下入侵……本身應屬非法"*（《說明報告》第 44 段）。

34 《說明報告》在第 49 段提出這一點。
例如亦見 Neil MacEwan, "The Computer Misuse Act 1990: lessons from its past and predictions for its future" [2008] Crim LR 955，第 956 頁：
"在〔《英格蘭誤用電腦法令》〕剛施行時，有人已質疑為何在未獲授權下取覽存於電腦內的機密資料應屬犯罪，但如同一資料是存於卡片式索引內，在未獲授權下取覽該等資料卻不屬犯罪"。

2.39　英格蘭案例 *R v Brown*[35] 牽涉到現已廢除的《1984 年資料保護法令》（Data Protection Act 1984），雖然背景不同，但亦說明了類似的觀點。[36] 上議院在該案中以三比二的多數裁定，純粹從電腦數據庫提取資料（例如以屏幕顯示或印本等形式），不足以構成該法令第 5(2)(b)條[37] 所指的“使用”；*“純粹取覽資料並不足夠，還必需對資料作出某些事情”*。[38] 少數法官則持相反看法。

取覽程式或數據，而非取用電腦

2.40　上議院在 *R v Bow Street Metropolitan Stipendiary Magistrate, Ex parte United States (No 2)*[39]（***“Ex parte United States”***）中裁定，高等法院分庭（Divisional Court）錯誤地把《英格蘭誤用電腦法令》第 1 條局限於對電腦系統的“黑客入侵”，而非將該條應用於針對使用電腦以獲得對程式或數據的未獲授權取覽。[40]《英格蘭誤用電腦法令》第 17(6)條的以下內容闡明了“程式或數據”與“電腦”之間的關係：

> “凡提述存於某電腦內的任何程式或數據，即包括提述存於當其時在該電腦內的任何抽取式儲存媒體內的任何程式或數據；而電腦須視作包含存於任何上述媒體內的任何程式或數據。”

2.41　按照以上的闡述，舉例來說，某人（“**甲方**”）如取走另一人的記憶棒並連接至自己的電腦，意圖在未獲授權下取覽存於該記憶棒內的數據，似乎便犯了《英格蘭誤用電腦法令》第 1 條所訂罪行。

在澳大利亞，《示範法典委員會報告書》第 135 頁提到：
“純粹在未獲授權下取覽並不會構成《〔示範刑事〕法典》所訂罪行，這有別於多個司法管轄區的現有法律。然而，委員會建議把在未獲授權下取覽受限數據定為簡易程序罪行。”
同樣，美國聯邦法律沒有把純粹在未獲授權下取用定為罪行，見 Ian Walden, Computer Crimes and Digital Investigations (Oxford University Press, 2007)，第 3.240 段。
儘管有上文所述，但應注意在某些司法管轄區，例如香港、英格蘭及威爾斯、新西蘭和新加坡，純粹在未獲授權下取用或取覽均構成罪行。

35　[1996] AC 543.

36　該案的被告人是一名警務人員，有權以所屬警察總長的代理人身分，為警務工作這一登記目的而使用全國警察電腦數據庫，而該名警察總長是《1984 年資料保護法令》所指的登記使用者。控方指稱，被告人為警務工作以外的目的而使用該數據庫內的個人資料。雖然有關案情是在《英格蘭誤用電腦法令》生效前發生，以致無法根據該法令對被告人提出控罪，但被告人代表律師在提出論點時曾提述該法令。若現在發生相同的案情，被告人很可能會根據《英格蘭誤用電腦法令》被檢控。

37　*“載於〔資料使用者〕登記冊的上述記項所涉及的任何人，不得……(b)為該記項所述一個或多於一個目的以外的目的，持有有關資料或使用自己持有的有關資料”*。

38　見上文註腳 35，第 548 頁 D 行（上議院大法官哥夫（Lord Goff of Chieveley））。

39　[2000] 2 AC 216.

40　同上，第 226 頁 E 行（霍豪斯勳爵（Lord Hobhouse of Woodborough））。

2.42 在上述假設情境中，甲方的目標是存於該記憶棒內的數據。針對在未獲授權下取覽數據的法例，適合處理這類案件。在某些其他案件中，犯罪者針對的可能是某電腦或電腦系統。儘管在技術層面上，取用電腦也許必定牽涉到取覽數據，但若有關犯罪者辯稱在未獲授權下取覽數據（而非取用電腦或電腦系統）的控罪並不適當，也可能言之成理。

取覽的未獲授權性質

2.43 在這方面，《英格蘭誤用電腦法令》第 17(5)條有以下規定：

> "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……"

2.44 在 *DPP v Bignell*，[41] 英格蘭高等法院分庭根據其對第 17(5)條的詮釋，接納 *"凡任何人獲授權獲得對任何程式或數據的取覽，則該人如按獲授權的級別而取用有關電腦，並不屬犯〔《英格蘭誤用電腦法令》〕第 1 條所訂罪行"*，[42] 即使是為未獲授權的目的而取用亦然。這項裁定引發了諸多批評。

2.45 其後，上議院在 *Ex parte United States*[43] 否定 *DPP v Bignell* 對第 17(5)條所作的上述詮釋。上議院頒布判詞，其中指出第 17(5)條並無引入按不同級別取用有關電腦的概念。[44] 因此，按 *"獲授權的級別"* 而取用之說是 *"毫不相干的想法"*。[45] 上議院對第 17(5)條的作用有以下概述：

> "該條純粹指明可取得權限的兩種方式：有關人士本身是有權授權的人，或者已獲有權授權的人授權。該條亦闡明此權限不僅須關乎有關數據或程式，亦須關乎所獲取覽的實際類別。" [46]

---

41 [1998] 1 Cr App R 1.
42 同上，第 13 頁（阿斯蒂爾法官（Astill J））。
43 [2000] 2 AC 216.
44 同上，第 225 頁 C – F 行（霍豪斯勳爵）。
45 同上，第 226 頁 E 行（霍豪斯勳爵）。
46 同上，第 224 頁 C – D 行（霍豪斯勳爵）。

2.46 上議院依據 *Ex parte United States* 的案情作出以下裁定：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。第 17(5)條並不能協助有關僱員。

2.47 藉《2006 年警察及司法法令》（Police and Justice Act 2006）加入《英格蘭誤用電腦法令》的第 17(8)條亦與授權問題相關：

> "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。"

犯罪意念

2.48 《英格蘭誤用電腦法令》第 1(1)條所訂的犯罪意念包括：

(a) 犯罪者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；及

(b) 犯罪者在犯罪行為發生時，知悉該項意圖作出的取覽未獲授權。

2.49 該條提述犯罪者的意圖及知悉的事，似乎意味着採用主觀測試。這些思想狀態是否涉及任何客觀元素，以及牽涉何種舉證責任等問題，均與刑事法律所有範疇相關。舉例來說，載於下文的英格蘭及威爾斯《1967 年刑事司法法令》（Criminal Justice Act 1967）第 8 條普遍適用：

> "法庭或陪審團在裁定某人有否犯某罪行時——
>
> (a) 在法律上並非一定需要僅因他的行動的結果是該等行動的自然和頗有可能的後果，而推斷他意圖造成或預見該結果；但

(b) 須藉參考所有的證據，從該等證據作出在有關情況下看來是恰當的推論，從而決定他當時是否意圖造成或預見該結果。”[47]

加重罪行

2.50 任何人如犯《英格蘭誤用電腦法令》第 1 條所訂罪行，並意圖干犯（或意圖利便干犯）第 2(2)條所指明的罪行，即會構成第 2 條所訂的加重罪行（*“在未獲授權下取覽，並意圖干犯或意圖利便干犯其他罪行”*），其最高刑罰較重：

“(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。

(2) 本條適用於以下罪行——

(a) 刑罰為法律所固定的罪行；或

(b) 任何年滿 21 歲（就英格蘭及威爾斯而言，則為年滿 18 歲）且無定罪紀錄的人，可處為期 5 年監禁的罪行（或在英格蘭及威爾斯，假若沒有《1980 年裁判法院法令》〔Magistrates’ Courts Act 1980〕第 33 條所施加的限制，則可被如此判刑的罪行）。

(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。

(5) 任何人犯本條所訂罪行——

---

[47] 香港的對等條文是《刑事訴訟程序條例》（第 221 章）第 65A(1)條。唯一的分別在於該條提述該人的“作為或不作為”，而英格蘭及威爾斯的法例則提述該人的“行動”。

(a) 一經在英格蘭及威爾斯循簡易程序定罪，可處為期不超過 12 個月的監禁或不超過法定最高罰款，或兩者兼處；

(b) 〔……〕

(c) 一經循公訴程序定罪，可處為期不超過 5 年的監禁或罰款，或兩者兼處。”

《2003 年通訊法令》第 125 條

2.51 為完整起見，下文載列一項與加拿大《1985 年刑事法典》第 326(1)(b)條（於上文引用）相若的英格蘭及威爾斯條文，即《2003 年通訊法令》（Communications Act 2003）第 125 條（*“不誠實地取得電子通訊服務”*）：

“(1) 任何人——

(a) 不誠實地取得某電子通訊服務，而

(b) 作出上述作為的意圖，是逃避繳付適用於提供該服務的收費，

即屬犯罪。

(2) 〔……〕

(3) 任何人犯本條所訂罪行——

(a) 一經循簡易程序定罪，可處為期不超過 6 個月的監禁或不超過法定最高罰款，或兩者兼處；

(b) 一經循公訴程序定罪，可處為期不超過 5 年的監禁或罰款，或兩者兼處。”

中國內地

2.52 首先，我們宜說明在中華人民共和國（“**中國**”）內地全部五類依賴電腦網絡的罪行的共通元素。

犯罪意念

2.53 關乎《中國刑法》所訂罪行(包括五類依賴電腦網絡的罪行)的犯罪意念的一般原則,於《中國刑法》第十四至十六條列明。該等條文規定,犯罪者如:(i)故意犯罪,或(ii)在法律有規定的情況下過失犯罪,須負刑事責任:

> "第十四條 明知自己的行為會發生危害社會的結果,並且希望或者放任這種結果發生,因而構成犯罪的,是故意犯罪。
>
> 故意犯罪,應當負刑事責任。
>
> 第十五條 應當預見自己的行為可能發生危害社會的結果,因為疏忽大意而沒有預見,或者已經預見而輕信能夠避免,以致發生這種結果的,是過失犯罪。
>
> 過失犯罪,法律有規定的才負刑事責任。
>
> 第十六條 行為在客觀上雖然造成了損害結果,但是不是出於故意或者過失,而是由於不能抗拒或者不能預見的原因所引起的,不是犯罪。"

(底線後加)

2.54 由於《中國刑法》第二百八十五及二百八十六條沒有對過失犯罪作出明確規定,因此看來在中國內地,五類依賴電腦網絡的罪行的犯罪意念包括第十四條所界定的意圖,以及第二百八十五及二百八十六條所指明的下述其他意念元素(如有的話)。

"違反國家規定"

2.55 《中國刑法》第二百八十五及二百八十六條中的所有相關罪行均規定,犯罪者須作出"違反國家規定"的作為。按照《中國刑法》第九十六條的解釋,"違反國家規定"是指:

> "違反全國人民代表大會及其常務委員會制定的法律和決定,國務院制定的行政法規、規定的行政措施、發布的決定和命令。"

2.56 中國內地的官方資料來源，沒有詳盡無遺地列明全部相關的國家規定。本諮詢文件重點列述看來最為相關的國家規定。

2.57 根據《中國網絡安全法》第二十七條：

> "任何個人和組織不得從事非法侵入他人網絡、干擾他人網絡正常功能、竊取網絡數據等危害網絡安全的活動；不得提供專門用於從事侵入網絡、干擾網絡正常功能及防護措施、竊取網絡數據等危害網絡安全活動的程序、工具；明知他人從事危害網絡安全的活動的，不得為其提供技術支持、廣告推廣、支付結算等幫助。"
>
> （底線後加）

2.58 根據《中國計算機信息系統安全保護條例》第七條：

> "任何組織或者個人，不得利用計算機信息系統從事危害國家利益、集體利益和公民合法利益的活動，不得危害計算機信息系統的安全。"
>
> （底線後加）

2.59 《計算機信息網絡國際聯網安全保護管理辦法》第六條亦有以下規定：

> "任何單位和個人不得從事下列危害計算機信息網絡安全的活動：
>
> （一）未經允許，進入計算機信息網絡或者使用計算機信息網絡資源的；
>
> （二）未經允許，對計算機信息網絡功能進行刪除、修改或者增加的；
>
> （三）未經允許，對計算機信息網絡中存儲、處理或者傳輸的數據和應用程序進行刪除、修改或者增加的；
>
> （四）故意製作、傳播計算機病毒等破壞性程序的；
>
> （五）其他危害計算機信息網絡安全的。"
>
> （底線後加）

《中國刑法》第二百八十五條

2.60 《中國刑法》第二百八十五條第一款有以下規定：

> "違反國家規定，侵入國家事務、國防建設、尖端科學技術領域的計算機信息系統的，處三年以下有期徒刑或者拘役。"

（底線後加）

2.61 《中國刑法》第二百八十五條第二款進一步述明：

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

（底線後加）

"計算機"的涵義

2.62 按 2011 年 8 月公布的《最高人民法院、最高人民檢察院關於辦理危害計算機信息系統安全刑事案件應用法律若干問題的解釋》（"**法釋〔2011〕19 號**"）所指示，"計算機信息系統"一詞是指具備自動處理數據功能的系統，包括計算機、網絡設備、通信設備、自動化控制設備等。

犯罪行為

2.63 根據第二百八十五條第一款，純粹在未獲授權下進入指明類型[48]的計算機信息系統會構成罪行。就其他類型的計算機信息系統而言，第二百八十五條第二款規定，除了純粹在未獲授權下進入外，犯罪者還須獲取該計算機信息系統中存儲或處理的數據，才會招致刑事責任。

---

48 見上文第 2.60 段。

進入的未獲授權性質

2.64 根據中國最高人民檢察院公布的第九批指導性案例[49]的第36號案例，第二百八十五條第一款中的“侵入”一詞，是指違背被害人意願、非法進入計算機信息系統的行為。其表現形式既包括採用技術手段破壞系統防護進入計算機信息系統，也包括未取得授權擅自進入計算機信息系統，還包括超出授權範圍進入計算機信息系統。[50]

新西蘭

新西蘭《1961年刑事罪行法令》第249及252條

2.65 新西蘭《1961年刑事罪行法令》（Crimes Act 1961，**《新西蘭法令》**）訂有三項與本章相關的罪行，其最高刑罰輕重有別。在這些罪行中，第252條（*“在未獲授權下取用電腦系統”*）所訂罪行的最高刑罰最輕：

> “(1) 任何人知悉自己未獲授權取用任何電腦系統，或罔顧自己是否已獲授權取用任何電腦系統，而在未獲授權下蓄意直接或間接取用該電腦系統，可處為期不超過2年的監禁。
>
> (2) 為免生疑問，任何人如獲授權取用某電腦系統，為某目的獲准取用，而為其他目的而取用該電腦系統，則第(1)款並不適用。”

2.66 其他兩項罪行載於《新西蘭法令》第249條（*“為不誠實目的而取用電腦系統”*）：

> “(1) 任何人直接或間接取用任何電腦系統，並藉此不誠實地或以欺騙手段在無聲稱擁有權利的情況下——
>
> (a) 取得任何財產、特權、服務、金錢利益、得益或有值代價；或

---

49 根據《最高人民檢察院關於案例指導工作的規定》第十五條，各級人民檢察院可以引述相關指導性案例進行釋法說理，但不得代替法律或者司法解釋作為直接依據。

50 最高人民檢察院公布的第九批指導性案例第36號（衛夢龍、龔旭、薛東東非法獲取計算機信息系統數據案），該案的指導意義指出：*“非法獲取計算機信息系統數據罪中的‘侵入’，是指違背被害人意願、非法進入計算機信息系統的行為。其表現形式既包括採用技術手段破壞系統防護進入計算機信息系統，也包括未取得被害人授權擅自進入計算機信息系統，還包括超出被害人授權範圍進入計算機信息系統。”*

(b) 導致其他人蒙受損失，

可處為期不超過 7 年的監禁。

(2) 任何人直接或間接取用任何電腦系統，意圖不誠實地或以欺騙手段在無聲稱擁有權利的情況下——

(a) 取得任何財產、特權、服務、金錢利益、得益或有值代價；或

(b) 導致其他人蒙受損失，

可處為期不超過 5 年的監禁。

(3) 在本條中，**欺騙手段**的涵義與第 240(2)條中該詞的涵義相同。”[51]

2.67 應注意的是，第 249(1)及(2)條均採用類似的措辭。兩者的主要分別在於：

(a) 前者規定被告人須已取得財產、特權等或已導致損失；而

(b) 後者只規定被告人須已意圖取得財產、特權等而行事或已意圖導致損失而行事。

正因為有上述分別，第 249(1)及(2)條所訂兩項罪行的最高刑罰各異。

“電腦系統”和“電腦”的涵義

2.68 根據《新西蘭法令》第 248 條，“電腦系統”一詞：

“(a) 指——

(i) 一部電腦；或

(ii) 兩部或以上互連的電腦；或

---

51 第 240(2)條對欺騙手段的定義如下：

“(a) 屬口頭或書面形式或藉行為作出的虛假申述，而作出該申述的人意圖欺騙其他人並——

(i) 知悉該申述在要項上屬虛假；或

(ii) 罔顧該申述是否在要項上屬虛假；或

(b) 在有責任披露某要項的情況下，意圖欺騙任何人而不披露該要項；或

(c) 意圖欺騙任何人而使用的欺詐手段、手法或計謀。”

(iii) 電腦之間的任何通訊鏈路，或通往遠程終端機或另一器材的任何通訊鏈路；或

(iv) 兩部或以上互連的電腦，並與電腦之間的任何通訊鏈路相結合，或與通往遠程終端機或任何其他器材的任何通訊鏈路相結合；並

(b) 包括(a)段所述項目的任何部分，以及所有相關的輸入、輸出、處理、儲存、軟件或通訊設施及已儲存數據。”

2.69 《新西蘭法令》並無界定何謂電腦。這種做法固然使法律不會因科技進步而變得不合時宜，但在某些案件中，被告人有罪與否可能取決於其所用的器材在法律上是否構成電腦。[52] 這個爭議點與被告人的行為在事實和道德上應否受刑事制裁的問題相去甚遠。

2.70 *Pacific Software Technology Ltd v Perry Group Ltd*[53] 是一宗涉及這個爭議點的新西蘭案例，當中關乎電腦程式的版權爭議。新西蘭上訴法院的以下論述，刻劃出數碼電腦及電腦程式的特點：

> “數碼電腦以五項功能元素為基礎：(i)輸入；(ii)由記憶體系統儲存該輸入；(iii)從記憶體接收數據並發出必要算術指令的控制單元；(iv)執行控制命令的算術運算；及(v)輸出容量。
>
> 電腦程式只是一組向電腦發出的指令。大多數程式均接受並處理使用者所提供的數據。程式編製員採用的基本程序稱為算法（即機械式計算程序），是程式的核心所在。只有運用程式編製員的人類創造力，才能開發出這些算法。因此，程式並不可能包含任何從未被人考慮的算法。電腦的優勢僅僅是能夠比人類更快和更準確地執行這些算法。”[54]

取用的未獲授權性質

2.71 第252(1)條明確規定取用須屬未獲授權，而且犯罪者須對此知情或罔顧實情，才會產生刑事法律責任。然而，第252(2)條繼而訂

---

52 在香港，這種情況見於*律政司司長 訴 王嘉業* [2013] 4 HKLRD 588, HCMA 77/2013（判決日期：2013年4月29日），上文討論第161條時已引述該案。

53 [2004] 1 NZLR 164.

54 同上，第168頁，第25及26段。

明，*"任何人如獲授權取用某電腦系統，為某目的獲准取用，而為其他目的而取用該電腦系統"*，則第 252(1)條並不適用。

2.72 新西蘭上訴法院在 *Watchorn v R*[55] 確認，*"第 252(2)條的效力，是把僱員為未獲授權的目的而取用的情況豁除於該條的適用範圍之外。"*[56] 換言之，有關取用並不構成第 252 條所訂罪行。這似乎較澳大利亞的情況寬鬆。如上文所論述，根據澳大利亞的條文，任何人如為隱秘目的而取覽電腦數據，則只有在該人亦有合法目的之情況下，才可免除刑事法律責任。

2.73 新西蘭的情況看來亦較 *Ex parte United States* 所闡述的《英格蘭誤用電腦法令》寬鬆。如上文所述，上議院在該案中拒絕接納源自 *DPP v Bignell* 的下述觀點：任何獲授權取覽程式或數據的人，如按獲授權的級別而取用有關電腦，並不屬違反《英格蘭誤用電腦法令》第 1 條，即使是為未獲授權的目的而取用亦然。

對第 249 條的解釋

2.74 《新西蘭法令》第 249 條並無提述授權這概念。

2.75 在 *Watchorn v R*，[57] 新西蘭上訴法院對《新西蘭法令》第 249(1)條所訂罪行的元素有以下論述：

> "我們認為，把第 249(1)條說成規定須有取得得益的不誠實目的並不正確。雖然第 249 條的標題是'為不誠實目的而取用電腦系統'，但這並不能準確概述第 249(1)條所訂立的罪行。第 249(1)條的構成元素並不包括不誠實目的。控方須證明的是，被告人曾取用電腦系統，並藉此不誠實地或以欺騙手段在無聲稱擁有權利的情況下取得得益。
>
> 〔依據有關案情〕……控方無須證明〔被告人〕是為甚麼目的而〔從其僱主的電腦系統〕下載〔某些數據〕。控方反而須證明被告人已取得得益，並且是不誠實地在無聲稱擁有權利的情況下取得該得益。"[58]

---

55 [2014] NZCA 493.

56 同上，第 79 段。同時，判案書註腳 33 暗示，第 252(2)條把僱員豁除的做法可能並不符合原意。

57 見上文註腳 55。

58 同上，第 26 及 42 段。

2.76　新西蘭上訴法院亦裁定，雖然有關電腦數據按照先前的案例並不屬第 249(1)(a)條所指的“財產”，[59] 但同一條文中的“得益”涵蓋*“任何使有關人士受益的東西”*，並且不限於經濟利益。[60] 因此，可合理爭辯的是，被告人*“管有、控制並因此而有機會使用已下載的檔案，構成第 249(1)(a)條所指的‘得益’。”*[61]

新加坡

《新加坡誤用電腦法令》第 3 及 4 條

2.77　如導言所指出，《新加坡誤用電腦法令》所訂罪行主要以《英格蘭誤用電腦法令》為基礎。正如《英格蘭誤用電腦法令》以第 1 條把在未獲授權下取覽電腦資料定為不合法，再以第 2 條訂定加重罪行一樣，《新加坡誤用電腦法令》也採用兩層式的做法。《新加坡誤用電腦法令》第 3 條（*“在未獲授權下取覽電腦資料”*）的內容如下：

> “(1) 除第(2)款另有規定外，任何人故意致使某電腦執行任何功能，目的是為了在沒有權限的情況下獲得對存於任何電腦內的任何程式或數據的取覽，即屬犯罪，一經定罪——
>
> (a) 可處不超過$5,000 的罰款或為期不超過 2 年的監禁，或兩者兼處；及
>
> (b) 如屬第二次或其後每次定罪，則可處不超過$10,000 的罰款或為期不超過 3 年的監禁，或兩者兼處。
>
> (2) 如因本條所訂罪行而導致任何損壞，被裁定犯該罪行的人可處不超過$50,000 的罰款或為期不超過 7 年的監禁，或兩者兼處。
>
> (3) 就本條而言，如有關作為並非針對——
>
> (a) 任何特定程式或數據；
>
> (b) 任何種類的程式或數據；或

59　同上，第 22 段。
60　同上，第 81 段。
61　同上，第 83 段。

(c) 存於任何特定電腦內的程式或數據，

均屬無關重要。”

2.78 《新加坡誤用電腦法令》第 4 條（*“意圖犯罪或意圖利便犯罪而取覽”*）訂立了以下加重罪行：

“(1) 任何人如意圖干犯本條所適用的罪行而致使某電腦執行任何功能，目的是為了獲得對存於任何電腦內的任何程式或數據的取覽，即屬犯罪。

(2) 本條適用於任何涉及財產、欺詐、不誠實或導致身體受傷害，且一經定罪可處為期不少於 2 年監禁的罪行。

(3) 任何人犯本條所訂罪行，一經定罪，可處不超過 $50,000 的罰款或為期不超過 10 年的監禁，或兩者兼處。

(4) 就本條而言——

(a) 第(1)款所提述的取覽是否已獲授權；

(b) 不論本條所適用的罪行是在獲得上述取覽時干犯或在任何其他時間干犯，

均屬無關重要。”

“電腦”的法定定義

2.79 儘管《新加坡誤用電腦法令》第 3 及 4 條與《英格蘭誤用電腦法令》中的對等條文有相似之處，值得注意的是，《英格蘭誤用電腦法令》並無界定何謂“電腦”，而《新加坡誤用電腦法令》第 2(1)條則將“電腦”定義為：

“執行邏輯、算術運算或儲存功能的任何電子、磁性、光學、電子化學或其他數據處理器材，或一組互連或相關的該等器材，亦包括任何與該器材或該組互連或相關的該等器材直接有關或共同操作的數據儲存設施或通訊設施，但不包括——

(a) 自動打字機或排字機；

(b) 便攜式手提計算機；

(c) 不可編程或不包含任何數據儲存設施的相類器材；或

(d) 部長藉憲報公告訂明的其他器材”。

2.80 上述定義中的許多部分均與《美國法典》第 18 篇第 1030(e)(1)條（18 USC 1030(e)(1)）[62] 的法定措辭相似。某評論員曾作出以下恰當的評析：排除打字機、排字機、計算機等的做法*“立即顯示出該條文的制定年代，亦完全反映採用特定的技術性措辭所帶來的危險”*。[63] 就電腦網絡罪行這類課題而言，有特別充分的理據支持法例採用科技中立的措辭。

美國

《電腦欺詐及濫用法案》（Computer Fraud and Abuse Act）（《美國法典》第 18 篇第 1030 條）

2.81 在美國，任何人如作出與《美國法典》第 18 篇第 1030(a)條所述各種情境有關的作為，可按第 1030(c)條的規定予以懲處。在這些情境中，與本章相關的情境是某人：

“(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

---

62 *“在用於本條時……‘電腦’一詞指執行邏輯、算術運算或儲存功能的任何電子、磁性、光學、電子化學或其他高速數據處理器材，亦包括任何與該器材直接有關或共同操作的數據儲存設施或通訊設施，但該詞不包括自動打字機或排字機、便攜式手提計算機或其他相類的器材”*。

63 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 65 頁。

(C) 從任何受保護電腦取得資料；

(3) 在未獲授權取用美國某部門或機關的任何非公用電腦的情況下，蓄意取用該部門或機關的上述電腦……

(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……

(5) (A) 故意導致向某受保護電腦傳送程式、資料、代碼或指令，並因着該行為而在未獲授權下蓄意導致該電腦損壞；

(B) 在未獲授權下蓄意取用某受保護電腦，並因着該行為而罔顧後果地導致損壞；或

(C) 在未獲授權下蓄意取用某受保護電腦，並因着該行為而導致損壞及損失。”[64]

企圖取用但不成功

2.82 根據第 1030(b)條，*“任何人如串謀犯或企圖犯本條(a)款所訂罪行，須按本條(c)款的規定予以懲處。”*這項條文與澳大利亞《刑事法典》（聯邦）第 477.1(8)條恰恰相反。如上文所述，第 477.1(8) 條免除企圖犯罪的刑事法律責任。

取用的未獲授權性質

2.83 《美國法典》第 18 篇第 1030 條的結構和格式，與香港的法例和上文所探討的司法管轄區的法例有頗大差別。如美國的法理有值得香港借鑑之處，其中一處是當地法院對《美國法典》第 18 篇第 1030(a)條所提述的 *“在未獲授權下”*取用電腦，以及以 *“超逾獲授權的取用範圍”*的方式取用這兩者的區別，進行了詳盡的分析。

2.84 尤其是，雖然《美國法典》第 18 篇第 1030(e)(6)條說明，*“‘超逾獲授權的取用範圍’一詞指在獲授權下取用某電腦，並藉該項取用而取得或更改該電腦中的資料，但取用者無權如此取得或更改*

64 《美國法典》第 18 篇第 1030(a)(1) – (5)條。

該等資料”，不同巡迴區的多宗案例都關乎 *“在未獲授權下”* 及 *“超逾獲授權的取用範圍”* 這兩個用語的涵義。

2.85 舉例來說，聯邦上訴法院第二巡迴法庭（Court of Appeals for the Second Circuit）在 *United States v Valle*[65] 指出，下述的關鍵爭議點 *“引起了姐妹巡迴區之間的嚴重分歧”*：

> “……如任何人為不當目的而取用電腦，以取得或更改該人在其他情況下獲授權取覽的資料，是否屬‘超逾獲授權的取用範圍’而取用電腦；還是只有該人取得或更改自己未獲授權為任何目的而取覽的資料，而該等資料位於該人在其他情況下獲授權取用的電腦時，方屬‘超逾獲授權的取用範圍’。”

該法院斷定這兩種解釋均可接受，因此 *“須按規定運用從寬原則，並採用後一種解釋”*。

2.86 *United States v Valle*[66] 與聯邦上訴法院第九巡迴法庭（Court of Appeals for the Ninth Circuit）全體法官[67] 於 2012 年對 *United States v Nosal*[68] 所作的裁決相符一致，該項裁決掀起了熱烈的學術辯論。審理 *United States v Nosal*[69] 的同一法庭在其後一項以大比數所作的裁決中，就 *“在未獲授權下”* 一詞作出對被告人較為不利的解釋，[70] 這增添了法律的不確定性。在這其後裁決中，大比數的法官實際上裁定只有電腦系統的擁有人方可授權某人取用該系統，而少數法官則認為系統擁有人或合法的帳戶持有人均可授權。

2.87 不久之後，在 *Facebook, Inc v Power Ventures, Inc*，[71] 由與先前不同的法官所組成的聯邦上訴法院第九巡迴法庭採納 *United States v Nosal*[72]

---

65 807 F 3d 508 (2d Cir 2015)，2015 年 12 月 3 日。

66 同上。

67 《聯邦上訴程序規則》（Federal Rules of Appellate Procedure）第 35(a)條訂明：
“多數並未喪失資格的常任現職巡迴法官，可命令任何上訴或其他法律程序由上訴法院的全體法官進行聆訊或重新聆訊。除非有下述情況，否則由全體法官進行聆訊或重新聆訊並不可取，而且通常不會被命令進行：
(1) 有必要由全體法官考慮，以確保或維持法院裁決的統一性；或
(2) 有關法律程序牽涉某個極為重要的問題。”
根據《美國法典》第 28 篇第 46(c)條，*“全體法官組成的法庭須由所有常任現職巡迴法官組成，或由……訂明人數的法官組成……”*。

68 676 F 3d 854 (9th Cir 2012)，意見書於 2012 年 4 月 10 日送交存檔。

69 844 F 3d 1024 (9th Cir 2016)，意見書於 2016 年 7 月 5 日送交存檔，並於 2016 年 12 月 8 日修訂。

70 同上。

71 844 F 3d 1058 (9th Cir 2016)，意見書於 2016 年 7 月 12 日送交存檔，並於 2016 年 12 月 9 日修訂。

中第二項裁決的方針，並述明 *"在分析《電腦欺詐及濫用法案》〔（即《美國法典》第 18 篇第 1030 條）〕所指的授權時應依循的兩項一般規則"*：

> "首先，若被告人不獲准許取用電腦，或該准許已被明確撤銷，被告人即可能觸犯《電腦欺詐及濫用法案》。一旦准許被撤銷，即使施展科技手段或徵募第三方協助取用，也不會免除法律責任。第二，單單違反網站使用條款，並不足以確立《電腦欺詐及濫用法案》之下的法律責任。"

2.88 2017 年 10 月 10 日，最高法院在 *United States v Nosal* 和 *Facebook, Inc v Power Ventures, Inc* 拒絕作出移審令[73]（即拒絕聆訊擬進行的上訴），並無借此機會闡明有關的解釋方式。

小組委員會的看法

宜制定針對電腦網絡罪行的特定法例

2.89 目前，香港法例並無任何適用於電腦網絡罪行的特定條例。不同罪行在各條例中訂立，當中部分條例亦不合時宜。相比之下，上文論述的其他司法管轄區大多數有針對電腦網絡罪行的特定法例，或以其部分成文法專門處理電腦網絡罪行。我們認為這些司法管轄區的做法有其可取之處，因為這種做法有助確保在此領域內（例如在主要概念的定義方面）做到協調統一、周全完備和貫徹一致。

2.90 故此，我們建議制定一項針對電腦網絡罪行的特定法例，當中包括本章和後面各章所建議的罪行，藉以全盤改革現行法律。儘管如此，我們也緊記第 161 條等現有條文在打擊電腦網絡罪行方面發揮着重要作用。雖然法律應盡量避免罪行互相重疊，但我們建議保留現有條文，直至新法例顯然足以取而代之。

主要詞語的定義

2.91 據我們所觀察，現今不少器材都裝有微處理器，並具備作特定用途的處理能力。《牛津英文字典》（Oxford English Dictionary）目前對"電腦"（computer）的定義已反映現今的科技狀況，內容如下：

---

72 見上文註腳 69。

73 美國最高法院，*Journal of the Supreme Court of the United States* (Oct Term 2017)，第 149 頁，登載於 https://www.supremecourt.gov/orders/journal/Jnl17.pdf（於 2022 年 5 月 3 日瀏覽）。

"一項電子裝置（或一項由多個裝置組成的系統），用於儲存、操控和傳達資料，執行複雜的計算，或控制或調節其他裝置或機器，並可接收資料（數據）及按照可變的程式指令（程式或軟件）處理該等資料；尤指一項供人在家中或工作場所使用的小型自給式電子裝置或系統，尤其用作處理文字、圖像、音樂和錄像，接達和使用互聯網，（例如以電郵等方式）與他人通訊，以及玩遊戲。"[74]

（底線後加）

2.92 1984 年，《證據條例》（第 8 章）加入"電腦"的法律定義。就在刑事法律程序中接納文件證據而言，"電腦"被界定為*"任何用作儲存、處理或檢索資料的裝置"*。[75] 前述寬廣的字典定義（或上文所引述條例中法定定義的字面解讀）涵蓋不同器材，其中一些例子包括：具備加密功能的記憶棒、模糊邏輯電飯煲、智能照明系統、網絡攝影機和智能電視。

2.93 我們亦留意到《俄羅斯公約》所採用的其他術語，當中分別對"資訊及通訊科技"和"資訊及通訊科技器材"下定義。"資訊及通訊科技"指*"為產生、轉換、傳送、利用和儲存資料而互連的方法、流程、硬件和軟件的集合"*。[76] 同樣地，"資訊及通訊科技器材"指*"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）"*。[77] 我們認為，儘管數碼科技不斷演進，但與"資訊及通訊科技器材"相比，"電腦"一詞的概念仍然清晰，不僅為大眾所通曉，我們的比較研究所引述各司法管轄區的法例亦廣泛使用"電腦"一詞。

2.94 我們進一步考慮了應否參考《俄羅斯公約》所採用的"資訊及通訊科技器材"的涵義，為"電腦"賦予法定定義。就此而言，我們注意到高等法院原訟法庭對*律政司司長 訴 王嘉業*[78] 的判決：

"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。

---

74 《牛津英文字典》（2022 年 3 月）。
75 《證據條例》第 22A(12)條。
76 第四條第(f)款。
77 第四條第(o)款。
78 [2013] 4 HKLRD 588, HCMA 77/2013（判決日期：2013 年 4 月 29 日）。

……

> 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。”[79]

2.95 我們認為法院上述觀點也適用於我們所建議的罪行。罪犯可能為不合法的目的而入侵任何具備處理能力的器材，例如為發動分布式拒絕服務攻擊而組成殭屍網絡。隨着物聯網興起，未來數年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”所下的定義），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院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。在考慮和權衡所有因素後，我們認為不界定“電腦”和“電腦系統”等詞語較為可取。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個議題。

把純粹在未獲授權下取用或取覽定為不合法

2.96 我們基於下述法律和實際的考慮因素，仔細考慮新法例應否禁止純粹在未獲授權下取用或取覽：

(a) 在香港，純粹在未獲授權下取用已屬第 27A 條所訂罪行，但該罪行僅適用於犯罪者*“藉着電訊”*取用的情況，而被定罪的人亦只須繳付罰款。某些其他司法管轄區（例如英格蘭及威爾斯、新西蘭）亦把純粹在未獲授權下取覽及取用定為不合法，但所處的最高刑罰一般相對較輕。

---

79 同上，第 601 頁（高等法院原訟法庭法官馮驊）。

(b) 《說明報告》表示，*"原則上，純粹在未獲授權下入侵"*電腦系統及數據*"本身應屬非法。"*[80]

(c) 因着各種合法或可能不合法的理由，在未獲授權下取用電腦／取覽程式或數據的情況每分每秒都在互聯網上發生，例如下文所詳述的連接埠掃描。[81] 舉例來說，取覽網站者未必是人，機械人也可能會"爬行"未受保護的網站。此外，一般無專業知識的人或許難以得知自己的電腦是否曾被他人取用，不論該取用是否惡意作出。

(d) 實際上，即使准許任何網上用戶全面授權他人掃描該用戶的程式或數據（由此無需就未獲授權的掃描提供豁免），也未必有助於應對現實世界的情況。除了難以劃定有關掃描的界線外，獲如此授權的人亦可能會濫用上述權限，為了自己的利益（亦即為網絡安全以外的目的）而使用所取覽的程式或數據。在某些情況下，網上用戶與操作人實際上亦可能無法在有關掃描發生前締結合約關係。舉例來說，要搜尋器開始在互聯網"爬行"之前，先逐一與各網站以某種形式締結令人滿意的合約關係，並非切實可行。

2.97 小組委員會曾詳盡討論以下事項：(a)在未獲授權下取用電腦／取覽程式或數據，與現實世界中陌生人在未獲准許下進入某地方（例如某人的居所）的情境到底有多類似，以及(b)純粹在未獲授權下取用或取覽應否招致刑事後果。在現實世界中，如任何人在未獲准許下進入他人的居所，並告知後者其門鎖不夠牢固，則不論入侵者在通過大門後是否立即止步，該進入本身已屬錯誤。我們難以找到任何理由，支持在電腦網絡空間准許某些在現實世界被禁止的行為。故此我們認為，純粹在未獲授權下取用電腦／取覽程式或數據應屬犯罪。

2.98 就上述在未獲授權下取用或取覽而言，有關取用或取覽應在何時定為不合法可能會令人混淆（例如到底在取用或取覽時便應定為不合法，還是在入侵者於取用或取覽後作出其他錯誤作為時方定為不合法）。由於法律的明確性相當重要，故小組委員會大多數成員認為，純粹在未獲授權下取用電腦／取覽程式或數據應定為簡易程序罪行，該罪行並無規定惡意為罪行元素，而合理辯解可作為法定免責辯護。

---

80 《說明報告》第 44 段（於上文第 2.19 段引用）。

81 連接埠是網絡連接起始與結束的虛擬點，均以軟件為基礎，並由電腦系統管理。每項互聯網服務均與某連接埠相關，例如網絡接達是與連接埠 80 及 443 相關。亦見第 2.5 段註腳 2。

取用或取覽的未獲授權性質

2.99　如上文所述，[82] 取用的未獲授權性質是第 27A 條所訂罪行的元素，但就第 161 條而言，取用須屬未獲授權只不過是法院對該條的解釋。

2.100　我們認為，新法例應明文規定取用或取覽須屬未獲授權，從而提供指引以消除不必要的爭議。上述其他司法管轄區的法規展示了多種方式來描述取用或取覽的未獲授權性質，我們在審視這些法規後，認為 *Ex parte United States*[83] 所闡述的《英格蘭誤用電腦法令》第 17(5)及(8)條較為可取。就此而言，我們希望重申，基於我們在較早部分解釋“在未獲授權下”取用或取覽這一概念時所述的理由，應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，亦即無須就我們已舉例說明的取用或取覽程度，事先尋求明示授權。[84] 我們正是在這基礎上建議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。

2.101　我們進一步認為，把某人知悉其取用或取覽未獲授權定為我們所建議罪行的先決條件，是公允的做法。我們預料，法院很可能會根據環境證據，作出關於某人是否知悉未獲授權的推論。按照常理，人們應知道進入某特定地方是否獲得准許。就此而言，兩種截然不同的比喻，分別是在營業時間內進入百貨公司，以及在銀行保險庫大門敞開時走進去。我們確信，按常理判斷的同一方針也適用於電腦網絡空間，故此舉例來說，即使某人的電腦器材或系統並不受密碼或其他保安措施保護，我們認為也不應視該人為一律同意對有關程式或數據的任何取覽，而且若有關取覽超出了人們在一般使用電腦網絡空間時通常可接受的限度，構成入侵（例如對他人的 WhatsApp 進行黑客入侵），便應產生在未獲授權下取覽的法律責任。

取覽程式或數據

2.102　我們的比較研究顯示，不同司法管轄區在這方面的取向各異。第 27A 條提述取用程式或數據，《英格蘭誤用電腦法令》第 1 條及《新加坡誤用電腦法令》第 3 條提述取覽程式或數據，而第 161

82　第 2.9 及 2.11 段。
83　見第 2.43 至 2.47 段。
84　見第 2.5 段。

條以及《新西蘭法令》第 249 及 252 條則分別提述取用電腦及電腦系統。

2.103 “電腦”的涵義正在迅速演變，但“程式”及“數據”兩詞既有相對明確的定義，亦一直無甚改變。“程式”是*“一連串編碼指令和定義，在輸入某電腦時會自動指示其操作，藉以執行某特定工作”*，[85] “數據”則指*“任何電腦對其進行運算並視為一個整體的數量、字符或符號”*。[86] 在非技術層面上，“數據”亦指*“數碼形式的資料”*。[87] 我們傾向於提述取覽程式或數據，因為這樣較為清晰，亦可避免把有關罪行與任何實體器材不必要地聯繫起來。電腦只是一種工具或器材，當中儲存的資料（主要是數據和程式）才屬重要，亦是任何未獲授權取用或取覽的目標所在。我們認為，若提述取用電腦，看來會過於局限。

合理辯解可作為免責辯護

2.104 我們曾討論應建議訂定多項適用於特定情況的免責辯護、一項基於（比如說）取覽有合理辯解的全面性免責辯護，還是應同時訂定這兩類免責辯護。

2.105 就第一種做法而言，要做到周全無缺並就每項度身訂造的免責辯護制定準則，實非易事。舉例來說，我們曾分析應否為特定類型的取覽（如測試電腦系統是否有已知的保安漏洞，例如是具預設密碼的網絡攝影機或所運行作業系統未經修補的電腦）或者特定類別的人士（如經認可專業團體審定的網絡安全從業員）提供免責辯護。要以切合文化及實況並在技術層面上不易引起事實爭議的準則來制定免責辯護，對我們來說實屬挑戰。

2.106 我們的結論是，基於合理辯解的概括性免責辯護能更有效兼顧公眾利益，應付未能預見的情況，並給予法院酌情權和彈性去決定被告人應否獲判無罪。因此，我們建議採用這種做法。由於一切都視乎案件的證據和情況而定，似乎無須擔心這類免責辯護會有被濫用的風險。以下例子正可闡明這一點：儘管被告人的網絡安全從業員審定資格可能屬重要因素，但被告人未必會因此而獲寬免未獲授權取覽的罪責。

---

85 《牛津英文字典》（2022 年 3 月）。

86 同上。

87 同上。

加重罪行

2.107 在決定建議訂立上述的簡易程序罪行時，我們意識到犯罪者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。

2.108 在借鑑上文所探討的某些司法管轄區的法例後，我們建議，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。至於哪些其他犯罪活動會觸發加重罪行，我們認為適宜以《英格蘭誤用電腦法令》第 2(2)條[88] 的擬定方式為起點。

香港法例的藍本

2.109 我們建議，建議的條文應以《英格蘭誤用電腦法令》第 1、2 及 17 條為藍本，並可適當參照其他司法管轄區法例的良好草擬方式。

建議 1

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《英格蘭誤用電腦法令》第 1、2 及 17 條為藍本。

[88] 於上文第 2.50 段引述。

在未獲授權下為網絡安全目的而取覽

2.110　讀者或許注意到，我們在上文探討應就建議罪行訂定何種免責辯護時，曾多次提及網絡安全從業員。這反映我們曾廣泛討論在未獲授權下為網絡安全目的而取覽這一概念。

2.111　我們認為宜開宗明義先說明何謂“網絡安全”。其他司法管轄區的科技公司和網絡安全機構所下的各種定義[89]的共通點，是以保護電腦系統免受數碼攻擊的做法，作為“網絡安全”這個概念的根基。就本諮詢文件而言，以下的學術文章勾劃出“網絡安全”的精髓：

> “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）損害而採取的各種程序。”[90]

2.112　有鑑於下述背景，我們考慮了在未獲授權下為網絡安全目的而取覽所涉及的各個議題：

(a) 在環球層面，總會有人在電腦網絡空間測試他人的電腦，而往往沒有事先取得他人授權。用作測試電腦數據或系統的工具既容易獲取，又得到廣泛使用。

(b) 舉例來說，這類測試的一種常見形式稱為連接埠掃描。[91]雖然連接埠掃描只會令被掃描的電腦產生日誌紀錄而不會造成不良影響，但若網絡活動異常增加，有關電腦的系統管理員或擁有人可能會有所警覺，耗費時間和金錢來調查該電腦是否已被入侵。

(c) 從科技角度來看，連接埠掃描是否構成取用目標電腦，是頗具爭議的問題。但就概念而言，以概括方式擬定的在未獲授權下取覽罪似乎可能適用於連接埠掃描。《英格蘭誤用電腦法令》第 1 條所訂罪行便是一例，當中“取覽”一

89　舉例來說，英國政府的國家網絡安全中心（National Cyber Security Centre）把網絡安全形容為*“個人及組織減低網絡攻擊風險的方式”*，並指網絡安全的核心功能是保護*“所有人均使用的器材（智能電話、手提電腦、平板電腦和電腦），以及人們在上網和工作時均會取用的服務，使之免遭盜竊或損壞”*。同樣地，美國政府的網絡安全及基礎設施安全局（Cybersecurity and Infrastructure Security Agency）把網絡安全界定為*“保護網絡、器材及數據免受未獲授權的取用或取覽或免被用作犯罪的技巧，以及確保資料機密、完整和可用的常規。”*分別見 https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security 及 https://www.cisa.gov/uscert/ncas/tips/ST04-001#:~:text=Cybersecurity%20is%20the%20art%20of,integrity%2C%20and%20availability%20of%20information（於 2022 年 5 月 3 日瀏覽）。

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

91　見上文註腳 81。

詞按第 17(2)條解釋。

(d) 人們測試他人的電腦，可能是出於善意、商業目的或惡意。舉例來說：

(i) 於 2017 年“WannaCry”事件期間，[92] 一些網絡安全專家進行測試，並提醒相關電腦用戶其電腦須安裝修補程式以免遭受感染。這些專家的工作顯然惠及社會。

(ii) 某人進行連接埠掃描，可能是為了得知某電腦是否已安裝最新的修補程式、某伺服器的哪個連接埠編號可供連接等。若識別到問題，該人或會就此收取高昂的修復費用。這些資料亦可能利便其他犯罪活動，例如以惡意軟件感染有關電腦。

就連接埠掃描而言，單憑日誌紀錄無法洞悉某人進行掃描的背後意圖。缺乏科技知識的電腦用戶，甚至無從知曉自己的電腦已被掃描。

(e) 一些網絡安全公司從不間斷地掃描互聯網，以確定網絡攝影機、網頁伺服器等是否有某些常見的保安漏洞。若識別到保安漏洞，這些公司或會主動提出作收費修復。他們的客戶亦可訂閱已識別保安漏洞的資料，這些漏洞所涉及的互聯網規約地址可能是由客戶本身使用，亦可能是由其他人使用。

(f) 網絡安全是個不斷變化的領域，評審情況亦一直演變。對網絡安全從業員來說，活躍於香港以至國際的業界機構眾多，沒有機構獲視為唯一權威。[93]

(g) 不少網絡安全從業員均具備實際經驗，但資格未經正式審定，至少在香港如是。若干年前，香港金融管理局在推行網絡防衛計劃以提高銀行業抵禦網絡攻擊的能力時，曾承

---

92 “WannaCry”是一款加密勒索軟件，會透過網絡掃描存在某種 Microsoft Windows 保安漏洞而未經修補的電腦，然後作出攻擊。全球多處地方，包括香港的電腦用戶均受到影響。例如見香港生產力促進局屬下的香港電腦保安事故協調中心於 2017 年 5 月 13 日發布的新聞稿，登載於 https://www.hkcert.org/tc/press-center/hkcert-security-alert-watch-out-for-wannacry-ransomware（於 2022 年 5 月 3 日瀏覽）。

93 香港網絡安全團體的一些例子，包括專業資訊保安協會和資訊保安及法證公會。其他與本港資訊科技專業人員有關的團體包括：香港電腦學會、香港資訊科技商會、香港資訊科技聯會和香港互聯網供應商協會。

認本港經審定的網絡安全專業人員數目有限。[94]

(h) 在香港商界，預防性網絡安全服務顯然不太流行。企業往往在發生網絡安全事故後，才會尋求協助以採取補救行動和加強它們的電腦系統。

(i) 香港固然可選擇訂立新罪行，藉以禁止各種未獲授權的電腦測試，但即使訂立該罪行，事實上也無法阻止他人從其他司法管轄區掃描在香港的電腦系統。

(j) 無論如何，罪犯一般使用自己的網絡來掃描互聯網以尋找保安漏洞，而並非依賴網絡安全公司。禁止各種未獲授權的測試，只會對網絡安全公司構成影響，卻無法制止罪犯識別這些漏洞。

2.113 基於上述各點，對於應如何在獲准許與不獲准許的取覽之間劃定界線，似乎難免會意見紛紜。某些人可能認為，若各種未獲授權的電腦測試不論因由，亦不論測試是否造成損壞，均可產生刑事法律責任，我們所建議的罪行便會過於廣闊。

2.114 因此，我們曾考慮在未獲授權下為網絡安全目的而取覽，在新法例下應否有免責辯護或豁免。應注意的是，舉例而言，在保障資料方面的現有法律下，《個人資料（私隱）條例》（第 486 章）第 61 條[95] 就“新聞活動”訂有豁免。考慮到即使未獲授權取覽是為了

---

94 見時任香港金融管理局總裁於 2016 年 5 月 18 日發表的網絡安全峰會主題演辭，第 8 段，登載於 https://www.hkma.gov.hk/chi/news-and-media/speeches/2016/05/20160518-2/。

95 *“(1) 由——*
(a) 其業務或部分業務包含新聞活動的資料使用者持有；及
(b) 該使用者純粹為該活動（及任何直接有關的活動）的目的而持有，
的個人資料，獲豁免而——
(i) 不受第 6 保障資料原則及第 18(1)(b)及 38(i)條的條文所管限，除非及直至該資料已發表或播放（不論在何處或藉何方法）；
(ii) 不受第 36 及 38(b)條的條文所管限。
(2) 在以下情況，個人資料獲豁免而不受第 3 保障資料原則的條文所管限——
(a) 該資料的使用包含向第(1)款所提述的資料使用者披露該資料；及
(b) 作出該項披露的人有合理理由相信（並合理地相信）發表及播放（不論在何處及藉何方法）該資料（不論是否實際有發表或播放該資料）是符合公眾利益的。
(3) 在本條中——
新聞活動（*news activity*）*指任何新聞工作活動，並包括——*
(a) 為向公眾發布的目的而進行——
(i) 新聞的搜集；
(ii) 關於新聞的文章或節目的製備或編纂；或
(iii) 對新聞或時事所作的評析；或
(b) 向公眾發布——
(i) 屬新聞的或關於新聞的文章或節目；或
(ii) 對新聞或時事所作的評析。”

網絡安全目的，亦有不同論據支持和反對禁止這類取覽，要平衡兼顧這些互相矛盾的論據實有困難，因此我們不擬在現階段確定立場，而是歡迎公眾就下文建議 2(a)所載的諮詢問題提出意見。

2.115 我們希望指出，若我們的法律應給予網絡安全業界的專業人員免責辯護或豁免（待我們收到公眾意見後才能決定這一點），便必須處理如何可確定或核實這類專業人員的身分這個基本問題。如上文所述，[96] 香港的網絡安全從業員目前未經任何評審團體或專業團體正式認可，故此，可行方案之一是制訂某種形式的評審制度，為網絡安全專業人員提供認證機制，若屆時有人須倚賴任何建議的免責辯護或豁免，便能以此輕易識別出這些專業人員。為方便公眾提出有據可依的意見，以助我們制訂未來方向，隨後各段概述了其他司法管轄區所採用的認證或以其他方式識別網絡安全從業員的機制。

2.116 在英國，國家網絡安全中心已制訂“認證網絡專業人員保證服務”（Certified Cyber Professional assured service，簡稱“**CCP 制度**”），務求建立由認可網絡安全專業人員組成的社群。[97] 要根據 CCP 制度取得認證，申請人須持有某些資歷或會員資格，以證明他們能廣泛應用網絡安全基礎知識。其後，他們或會獲授予在網絡安全不同專門範疇執業的認可。[98] 在中國內地，中國網絡安全審查技術與認證中心在《中國網絡安全法》的批准範圍內承擔網絡安全從業員的評審工作。[99] 我們亦注意到，新加坡網絡安全局（Cyber Security Agency of Singapore）已推行一項計劃，藉以培訓網絡安全專業人員並提升其技能，該等人員均須符合資訊及通訊科技方面有關資歷及工作經驗的正式規定。[100]

2.117 另一方面，我們理解到，並無制訂評審或認證制度的司法管轄區或會依據國際標準（例如**國際認可論壇**（International Accreditation Forum）[101] 所訂明的國際標準）來識別合資格的網絡安全人員。

---

96 第 2.112(f)及(g)段。

97 見 https://www.ncsc.gov.uk/information/certified-cyber-professional-assured-service（於 2022 年 5 月 3 日瀏覽）。國家網絡安全中心是英國在網絡安全領域的國家級技術機構。

98 同上。

99 見 https://www.isccc.gov.cn/zxjs/zxjs/index.shtml#intro（於 2022 年 5 月 3 日瀏覽）。中國網絡安全審查技術與認證中心於 2006 年成立。《網絡安全法》第十七條訂明：*“國家推進網絡安全社會化服務體系建設，鼓勵有關企業、機構開展網絡安全認證、檢測和風險評估等安全服務。”*

100 見新加坡網絡安全局網站，網址為 https://www.csa.gov.sg/Programmes/CSAT（於 2022 年 5 月 3 日瀏覽）。

101 國際認可論壇是一個由評審團體及其他團體組成的全球組織，這些團體均着眼於不同領域（管理系統、產品、服務，以及最重要是人員）的合格評定。見 https://iaf.nu/en/about/（於 2022 年 5 月 3 日瀏覽）。據我們理解，國際認可論壇所認可的認證均獲世界各地政府廣泛接受。

2.118 若公眾屬意法律應為網絡安全從業員提供免責辯護或豁免，而香港應為此設立評審制度，我們便須考慮該制度實際上應如何運作。一些初步構思包括：評審團體可以屬法定性質或行政性質，負責備存一份可供查閱的網絡安全專業人員名單。我們邀請公眾回應建議 2(a)(i)及(ii)所載的問題，就以下兩方面發表意見：評審方式和方法（例如評審準則及可能訂定的持續進修規定），以及評審制度的運作細節（例如若任何經審定人士未能符合持續進修規定，評審團體可否將該人除名或拒絕將其審定資格續期；以及評審團體以外的人應否獲准查閱經審定人士名單）。

2.119 但若社會各界認為，不斷演變的評審情況[102]會對實施正式的評審架構造成阻礙，則我們傾向認為，針對電腦網絡罪行的特定法例可訂明任何人應符合某些規定，方可享有法律就在未獲授權下為網絡安全目的而取覽所容許的免責辯護或豁免。一些基本規定可能關乎某人的培訓資歷、工作經驗和正直品格，例如該人是否適合及適當人選。儘管如此，任何立法訂明的準則要在實際上行之有效，似乎需要有一些可靠的方法來確定某特定網絡安全從業員是否符合有關規定。我們歡迎公眾就設立評審制度以外，任何能達到同樣目的（即讓人識別可享有所建議免責辯護或豁免的網絡安全專業人員）的可行替代方案提出意見，相關問題載列於下文建議 2(a)(iii)。

2.120 最後，我們知道非保安專業人員亦可能作出非法取覽程式或數據的作為。這類非法取覽代表着入侵電腦系統的初期。正如我們將在第 5 章解釋，在其後干擾有關電腦系統可能構成罪行，故我們邀請公眾對非保安專業人員就該罪行應否有任何合法辯解這問題提出意見。[103] 鑑於第 2 及 5 章所建議的罪行息息相關，我們亦在這方面就非法取覽程式或數據罪徵詢公眾意見（見下文建議 2(b)）。

建議 2

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：

102 第 2.112(f)段。

103 第 5 章建議 8(b)。

(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）？**[104]

簡易程序案件的時效期

2.121 根據《裁判官條例》（第 227 章）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。第 27A(4)條[105] 便是一例，該條把時效期延長至 *"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）"*。

2.122 我們理解到，《裁判官條例》（第 227 章）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的兩至

---

104 建議 8(b)所述的例子是：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。

105 於上文第 2.11 段引述。

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經已屆滿。警方從互聯網服務供應商取得日誌紀錄，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。

2.123 鑑於上文所述，我們建議把建議罪行的時效期延長至發現所涉事項後的兩年，但維持其簡易程序性質，即就該罪行更改《裁判官條例》（第 227 章）第 26 條。按照邏輯，如循簡易程序就我們在本諮詢文件所建議的任何罪行提出檢控，經延長的同一時效期應亦適用。

建議 3

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。

犯罪法人團體的高級人員的刑事法律責任

2.124 我們察覺到，法人團體可在其董事或其他相類高級人員同意或縱容下犯電腦網絡罪行。故此，我們考慮了應否在新法例加入明文規定，使刑事法律責任可在某些情況下直接歸於出任有關職位的人。[106]

2.125 現時，《刑事訴訟程序條例》（第 221 章）第 VI 部就公司的董事和其他高級人員的法律責任訂有一般條文。[107] 我們認為，這項一般條文足以處理涉及電腦網絡罪行的情況。此外，我們相信若我們有關訂立在未獲授權下取覽程式或數據罪的建議獲接納，則可在進行立法程序時，才更具體地考慮有否需要就董事和擔任管理職位的人

106 舉例來說，《版權條例》（第 528 章）第 125(1)條訂明：*"凡任何法人團體就任何作為而犯了本條例所訂的罪行，而該罪行經證明是在該法人團體的任何董事、經理、秘書或其他相類高級人員或本意是以任何該等身分行事的任何人同意或縱容下犯的，或經證明是可歸因於該法人團體的任何董事、經理、秘書或其他相類高級人員或本意是以任何該等身分行事的任何人本身的任何作為的，則上述的人及該法人團體均屬犯該罪行。"*其他香港法例亦有許多相類似的條文。

107 《刑事訴訟程序條例》（第 221 章）第 101E 條訂明：*"凡犯了任何條例內的罪項的人是一間公司，一經證明罪行是得到公司董事或與公司管理有關的其他高級人員同意、縱容，或得到宣稱是以該董事或高級人員身分行事的人同意、縱容而犯的，則該董事或高級人員亦屬犯了該項罪行。"*

的法律責任作出明文規定。[108] 因此，我們的結論是現階段無需就這個議題作出具體建議。對於本諮詢文件第 3 至 6 章所建議訂立的其他罪行，我們也抱持同樣的立場。

[108] 《香港法律草擬文體及實務指引》（律政司，2012 年），第 6.2.12 段。

第 3 章　非法截取電腦數據

引言

3.1　我們會在本章探討第二類依賴電腦網絡的罪行，即非法截取電腦數據。概括而言，就此主題而訂立的罪行，旨在更明確地：

(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；

(b) 從而保障人們的數據通訊私隱權。

3.2　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。[1] 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”[2] 或安裝間諜軟件。

香港的現行法律

《基本法》

3.3　一般而言，禁止非法取覽罪及禁止非法截取罪分別關乎“靜止數據”及“傳遞中的數據”。假若法律應保障前者的話，那麼對後者亦應一視同仁。

3.4　此外，“傳遞中的數據”及“通訊”這兩個概念密不可分，本章宜引述適用於一般通訊的《基本法》第二十七條及第三十條作為引子：

(a) *“香港居民享有言論……自由……。”*[3]

(b) *“香港居民的通訊自由和通訊秘密受法律的保護。除因公共安全和追查刑事犯罪的需要，由有關機關依照法律程序對通訊進行檢查外，任何部門或個人不得以任何理由侵犯*

1　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。

2　後門程式是 *“電腦系統的特點或缺陷，容許在未獲授權下暗中取覽數據。”*見：Oxford University Press, “Lexico.com”（2021 年），網址為 https://www.lexico.com/definition/back_door（於 2022 年 5 月 3 日瀏覽）。

3　第二十七條。

居民的通訊自由和通訊秘密。”[4]

《香港人權法案》

3.5 《香港人權法案》第十四條(*“對私生活、家庭、住宅、通信、名譽及信用的保護”*)及第十六(二)條(*“意見和發表的自由”*)[5]同樣有關：

(a) *“任何人之私生活……或通信，不得無理或非法侵擾……對於此種侵擾或破壞，人人有受法律保護之權利。”*[6]

(b) *“人人有發表自由之權利；此種權利包括……尋求、接受及傳播各種消息及思想之自由。”*[7]

《截取通訊及監察條例》（第 589 章）

條例目的

3.6 《截取通訊及監察條例》（第 589 章）（**《截取通訊及監察條例》**）補充上述《基本法》及《香港人權法案》的條文，該條例：

> “……就授權和規管執法機構為防止或偵查嚴重罪案和保障公共安全的目的而進行的截取通訊及秘密監察，訂立法定機制。”[8]

3.7 《截取通訊及監察條例》着眼於規管執法機構（“**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。[9]

“傳送過程中”的通訊

3.8 只有第一類行動（即截取通訊）與本章主旨有關。根據《截取通訊及監察條例》第 2(1)條：

---

4 第三十條。
5 《香港人權法案條例》（第 383 章）第 8 條。
6 第十四條。
7 第十六（二）條。
8 截取通訊及監察事務專員秘書處網站，網址為 https://www.sciocs.gov.hk/tc/ordinance.htm（於 2022 年 5 月 3 日瀏覽）。
9 《截取通訊及監察條例》第 2 條。

"***'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；

'通訊'（communication）指——

(a) 任何藉郵政服務傳送的通訊；或

(b) 任何藉電訊系統傳送的通訊"。

3.9 根據上述定義，《截取通訊及監察條例》只規管截取在*"傳送過程中"*的通訊。第 2(5)(b)條以下述措辭解釋傳送何時結束，換言之，就是《截取通訊及監察條例》不再適用於有關通訊之時：

"就本條例而言……如藉電訊系統傳送的通訊，已被該通訊的傳送對象接收，或被該傳送對象所管控或可取用的資訊系統或設施接收，則不論他有否實際閱讀或聽見該通訊的內容，該通訊不得視為是在傳送過程中。"

"截取作為"的目標

3.10 如上文所述，"截取作為"的目標界定為*"通訊的某些或所有內容"*。根據《截取通訊及監察條例》第 2(6)條：

"……藉電訊系統傳送的任何通訊的內容，包括聯同該通訊一併產生的任何數據。"

3.11 這些數據似乎主要是元數據，即關於通訊本身的資料，而非通訊的內容或實質內容。連同電郵內容一併傳送的電郵傳送人和接收人的相關資料，便是電腦網絡空間上元數據的例子。《截取通訊及監察條例》的實務守則闡述如下：

"在通訊的傳送過程中截獲該等資料[10] 亦同樣視為截取，即使沒有取用通訊的實際訊息亦是如此。然而，在

---

10 有關條例及實務守則分別提述"數據"及"資料"。雖然就本章而言，似乎無需區分兩詞，但兩者技術上並不相同。國際標準化組織對"數據"的定義是*"為便於交流、解釋或處理，對資訊的可再獲解讀的形式化表述"*，而對"資料"的定義則是*"關於客體（如事實、事件、事物、過程或思想，包括概念）的知識，而該知識在特定場合中具特定意義"*。見登載於以下網址的定義：
https://www.iso.org/obp/ui/#iso:std:iso:10782:-1:ed-1:v1:en（於 2022 年 5 月 3 日瀏覽）。

傳送通訊後取得的紀錄（例如通電紀錄及電話帳單）並非截取作為。這類資料的紀錄可藉搜查令取得。”[11]

《電訊條例》（第 106 章）

蓄意損壞電訊裝置——第 27(b)條

3.12 《截取通訊及監察條例》只適用於公職人員。在執法情況以外，*任何人*均可能犯《電訊條例》（第 106 章）第 27 條所訂的以下罪行：

> “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。”

可能適用於電腦網絡空間

3.13 《電訊條例》於 1963 年生效，最初或者是參照二十世紀六十年代的電話而採用“電訊”及有關詞句，但該等詞句的定義廣闊，而近數十載科技發展日新月異，[12] 按理電腦如今應可構成“電訊裝置”。[13] 因此，如任何人損壞、移走或干擾這樣的電腦，而意圖是 *“截取或找出任何訊息的內容”*，第 27(b)條便會適用。

並非針對電腦網絡罪行的特定條文

3.14 縱然上述如此，第 27(b)條始終並非針對截取電腦數據的特定條文。該條文的措辭及定義預設電訊背景，並不完全適用於電腦網絡空間。以下例子可說明這一點：

---

11 保安局局長，《依據〈截取通訊及監察條例〉（第 589 章）第 63 條而發出的實務守則》（2016 年 6 月），第 10 段。

12 例如透過採用稱為非對稱數碼用戶線路的技術，以往用來連接電話的銅線現在可支援連接互聯網。

13 第 2(1)條將“電訊裝置”界定為 *“為電訊網絡、電訊系統或電訊服務或與電訊網絡、電訊系統或電訊服務相關而維持的器具或設備”*。
雖然加拿大最高法院在 *R v McLaughlin* [1980] 2 SCR 331 裁定，電腦系統不屬當時《刑事法典》（Criminal Code）第 287 條所指的“電訊設施”，但該裁決建基於舊時的電腦科技及用途，應審慎評估該案如今是否具說服力的案例。

"***干擾***（interference）指由任何或任何組合的發射、輻射或感應所引起的無用能量對電訊網絡、電訊系統或電訊裝置的接收的影響，表現為性能下降、以及資訊（如沒有上述無用能量則可從該電訊網絡、電訊系統或電訊裝置中提取出者）的誤解或遺漏；

訊息（message）指藉電訊傳送或接收的任何通訊，或交由電訊人員藉電訊傳送的或交由電訊人員傳遞的任何通訊"。[14]

3.15 基於上述法定定義，假如某人具備所需意圖而干擾電腦，因而根據第 27(b)條被起訴，控方或需援引專家證據，以證明(a)有關電腦構成電訊裝置，以及(b)被告人的行為構成該條文所定義的干擾。

3.16 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，因為《電訊條例》（第 106 章）中並沒有與《截取通訊及監察條例》第 2(6)條（於上文引述）對等的條文。儘管元數據可與"任何訊息的內容"同等重要，在有關通訊各方以外的人眼中亦可能具有價值，但元數據似乎不受第 27(b)條保障。

《布達佩斯公約》訂定罪行的標準

3.17 《布達佩斯公約》[15] 第一節之下的第一篇第三條（引述如下）處理本章的主題事宜：

"各締約方均應採取必要的立法及其他措施，在其本土法律中將下列行為定為刑事罪行：在無權的情況下蓄意以技術截取往來電腦系統或在電腦系統內的非公開傳送電腦數據（包括由電腦系統發出載有該等電腦數據的電磁發射）。任何締約方可規定，有關罪行須具不誠實意圖，或須與連接至另一電腦系統的電腦系統有關。"

3.18 《說明報告》對第三條的評註如下：

"51. 本條旨在保障數據通訊的私隱權。有關罪行相當於傳統竊聽和記錄人們口頭電話對話的侵犯通訊私隱行為。《歐洲人權公約》（European Convention on Human Rights）第八條體現通訊私隱權，第三條所訂罪行正是將這項原

---

14 《電訊條例》（第 106 章）第 2(1)條。

15 有關《布達佩斯公約》的背景資料，見導言第 11 段，以及第 1 章第 1.6 至 1.10 段。

則應用於所有形式的電子數據傳輸（不論是藉電話、傳真、電郵或檔案傳輸）。

……

53. 以‘技術’截取，是指直接透過取覽和使用電腦系統，或間接透過使用電子偷聽或竊聽器材，以監聽、監測或監察通訊的內容和取得數據的內容。截取亦可能包含記錄。技術包括裝設在傳輸線及器材上用以收集和記錄無線通訊的技術器材，可包括使用軟件、密碼及編碼。使用技術這項規定是具限制性的要求，目的是避免造成過度刑事化的情況。

54. 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。構成‘非公開傳送電腦數據’的僱員通訊，不論是否為了業務目的，亦會受第三條保障，使該通訊免遭他人在無權的情況下截取……

55. 以傳送電腦數據形式進行的通訊，可在單一電腦系統內（例如由中央處理器傳送至屏幕或打印機）進行，亦可在同一人擁有的兩個電腦系統之間進行，或在兩部互相通訊的電腦之間或電腦與人之間（例如透過鍵盤）進行。不過，締約方仍可規定，通訊須在遠程連接的電腦系統之間傳送，作為額外罪行元素。

56. 應注意的是，雖然‘電腦系統’這個概念亦可包含無線電連接，但任何無線電傳送如以相對公開和易於取用的方式進行，因而可被截取（例如被無線電業餘愛好者截取），則即使無線電傳送屬‘非公開’傳送，亦不代表締約方有責任把截取這類無線電傳送定為罪行。

……

58. 非法截取須是‘蓄意’和在‘無權’的情況下進行，方會招致刑事法律責任。例如，假若進行截取的人有權如此行事，或他是按照有關傳送的參與者的指示或

授權行事（包括獲授權的測試或參與者同意的保護行動），或假若調查機關為維護國家安全或偵查罪行而合法授權監察，有關作為便是有理可據的。由於使用‘小型文字檔案（cookies）’等這類常見的商業做法不屬在‘無權’的情況下進行截取，故這類做法本身亦不擬定為罪行。對於第三條所保障的非公開僱員通訊（見上文第 54 段），本土法律可訂明合法截取這類通訊的理由。根據第三條，在這些情況下進行的截取會視為在‘有權’的情況下進行。

59. 在某些國家，截取可能與在未獲授權下取用電腦系統罪關係密切。為確保有關法律的禁止事項和適用範圍貫徹一致，如這些國家根據第二條，規定須具不誠實意圖，或規定有關罪行須與連接至另一電腦系統的電腦系統有關，則亦可在本條就招致刑事法律責任訂下類似的規限元素。這些元素應與有關罪行的其他元素（例如‘蓄意’和‘無權’）一併詮釋和應用。”[16]

靜止數據的兩類特例

“靜止數據”及“傳遞中的數據”

3.19 我們於上文評述，概括而言，禁止非法取覽罪及禁止非法截取罪分別關乎“靜止數據”及“傳遞中的數據”。兩者概念截然不同，卻又（如《說明報告》第 46 及 59 段[17] 所揭示）息息相關。

3.20 除了儲存於電腦用戶儲存媒體內的數據這個明顯例子外，數據還可能在兩類情況下靜止不動。我們會於下文先討論這類靜止數據，並以舉例方式簡略探討若干司法管轄區的法例如何處理這類數據，隨後再就非法截取電腦數據這個課題展開比較研究。

在傳送期間暫時靜止的數據

3.21 第一類特例之所以出現，是因為某些種類的互聯網通訊所採用的技術。名為“存儲轉發”傳遞的機制，是指通訊可於前往目的地途中多次暫存在網絡上。[18]

---

16 《說明報告》第 51、53 至 56、58 及 59 段。

17 分別於第 1 章及本章較前部分引述。

18 “存儲轉發”傳遞可與網上視像片段等串流媒體作對比。

3.22 問題是：當數據在傳送期間有一剎那暫時靜止，截取罪應否適用於該數據。對於這個問題，並非所有司法管轄區均有法例處理，但澳大利亞法律以《1979 年電訊（截取及取覽）法令》（聯邦）（Telecommunications (Interception and Access) Act 1979 (Cth)，**《電訊（截取及取覽）法令》**）第 5F 條的推定條文給予肯定答案，該條文的內容如下：

> "就本法令而言，通訊：
>
> (a) 在發送該通訊的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，直至該通訊的傳送對象可取覽該通訊為止。"

3.23 根據這項條文，截取罪適用於整個傳送過程中的通訊（不論在該通訊被指稱截取時，構成該通訊的數據恰巧是暫時靜止還是正在傳遞中）。

3.24 如沒有這項條文，控方便可能需要極為技術性的證據，方可證明有關罪行的元素。例如，被控截取罪的人可能就其所取得的數據在關鍵時間是否正在傳遞中這個事實問題提出爭議（因為倘若有關數據當時是暫時靜止，原則上非法取覽的控罪會較為恰當）。要在排除合理疑點的情況下證明這一點，未必直接簡單。

儲存於通訊系統的數據

3.25 第二類特例涉及到達通訊終點後，在通訊系統內靜止並可供傳送對象取覽的數據。日常例子包括儲存於手提電話用戶語音留言信箱內的訊息，[19] 以及儲存於網上電郵服務供應商伺服器內的電郵。這類數據顯然不受《截取通訊及監察條例》規限，因為該條例不再適用於處於以下狀況的通訊：

> "如……已被該通訊的傳送對象接收，或被該傳送對象所管控或可取用的資訊系統或設施接收，則不論他有否實際閱讀或聽見該通訊的內容"。[20]

3.26 在澳大利亞的相關概念是"儲存通訊"，這概念在《電訊（截取及取覽）法令》第 5 條界定為：

---

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

20 《截取通訊及監察條例》第 2(5)(b)條（於上文引述）。

"……符合以下說明的通訊：

(a) 並非正在經過電訊系統；及

(b) 由傳送者操作和管有的設備所持有；及

(c) 在沒有傳送者的僱員的協助下，通訊各方以外的人不能在該設備上取覽該通訊。"

3.27 從《布達佩斯公約》的罪行歸類而言，處於這個狀況的數據應屬禁止非法取覽（而非禁止非法截取）的焦點。然而，不同司法管轄區根據性質各異的法規（這些法規未必是專門針對電腦網絡罪行的法例）把非法截取定為罪行。

3.28 例如，英格蘭及威爾斯的《2016年調查權力法令》（Investigatory Powers Act 2016，**《調查權力法令》**）訂明多項條文，當中包括合法截取通訊的情況和非法截取通訊的情況。就此而言，不論構成通訊的數據是靜止不動還是在傳遞中，在概念上應差異無幾。

3.29 由此，就《調查權力法令》而言，"截取"一詞不一定與電腦網絡罪行法例（即《英格蘭誤用電腦法令》）中的"取覽"概念互作對比。由於《調查權力法令》中的"截取"一般可理解為取得構成通訊的數據，因此即使有關數據是靜止不動，概念上亦無不協調之處。

3.30 上文為《調查權力法令》第4(4)[21]及(5)[22]條定下背景，該等條文的實際效果，是把第3(1)條所訂的截取罪應用於在澳大利亞視為"儲存通訊"的通訊。這個概念意義重大，因為：

"……隨着網上電郵服務日漸普及，這代表取覽的複本愈來愈可能是儲存於傳送者[23]的設備中，而非下載至接收人的電腦。"[24]

---

21 *"在本條中，就藉電訊系統傳送的通訊而言，'有關時間'指——*
(a) 該通訊傳送期間的任何時間，及
(b) 該通訊於該系統內儲存或由該系統儲存期間的任何時間（不論是在該通訊傳送之前或之後）。"

22 *"就本條而言，通訊的任何內容須視為已在有關時間提供予某人的情況，包括以下情況：在有關時間轉發或記錄該通訊的任何部分，以便在該時間後向某人提供該通訊的任何內容。"*

23 傳送者是傳送通訊服務的供應商，一般是電訊網絡操作人。

24 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第187頁。

3.31　概念上，當通訊已獲下載或儲存於接收人的電腦（即不再留在任何通訊系統內），若有人非法取覽構成該通訊的數據，便會受第 2 章所檢視的非法取覽程式或數據罪所規管。

其他司法管轄區的法定體制

澳大利亞

《刑事法典》（聯邦）並不相關

3.32　在澳大利亞，《刑事法典》（聯邦）（Criminal Code (Cth)）第 10.7 部處理電腦罪行。正如第 2 章所述，該部定為不合法的主要行為種類有：在未獲授權下取覽電腦數據、在未獲授權下修改電腦數據，以及在未獲授權下損害電子通訊。根據第 476.1(1)條：

> "**損害往來某電腦的電子通訊**包括：
>
> (a)　阻止進行上述通訊；或
>
> (b)　在該電腦所使用的電子聯網或網絡上損害上述通訊；
>
> 但不包括純粹截取上述通訊。"

3.33　上述但書顯示《刑事法典》（聯邦）與本章主旨並不相關。

《電訊（截取及取覽）法令》所訂的截取罪

3.34　《電訊（截取及取覽）法令》的條文反而相關。根據第 7(1)條，除非例外情況適用，否則：

> "任何人不得：
>
> (a)　截取；
>
> (b)　授權、容許或准許另一人截取；或
>
> (c)　作出任何作為或事情，使其本人或另一人能截取；
>
> 正在經過電訊系統的通訊。"

3.35　第 7(2)至(10)條接着詳細列出例外情況。《電訊（截取及取覽）法令》第 105 條訂定，違反第 7(1)條屬可公訴罪行，最高可處兩年監禁。

3.36　第 7(1)條與第 5F 條一併施行。我們於上文考慮在傳送期間暫時靜止的數據時提到，第 5F 條實際上是把第 7(1)條應用於整個傳送過程中的通訊（不論構成該通訊的數據恰巧是暫時靜止還是在傳遞中）。

儲存通訊

3.37　當通訊可供接收人取覽，該通訊即屬《電訊（截取及取覽）法令》第 3 章所規管的“儲存通訊”。[25] 我們在探討儲存於通訊系統的數據時，已在上文第 3.26 段討論這個詞語的法定定義。

元數據

3.38　除非任何例外情況適用，否則《電訊（截取及取覽）法令》第 4 章一般禁止取覽大體上是元數據的“電訊數據”：

> “電訊數據是關於電訊的資料，但電訊數據並不包括通訊的內容或實質內容……就互聯網的應用而言，電訊數據包括使用時段所用的互聯網規約（IP）地址、曾到訪的網站，以及每節使用時段的開始和結束時間。”[26]

《電訊（截取及取覽）法令》可能有其局限

3.39　與香港《電訊條例》（第 106 章）第 27(b)條一樣，《電訊（截取及取覽）法令》對“電訊”的提述亦可能限制其應用範圍。有評論員認為：

> “有關在未獲授權下截取通訊的罪行並非新事，在各個司法管轄區均可見。這些罪行一般由關於在公共電訊網

25　除非屬訂明例外情況，否則《電訊（截取及取覽）法令》第 108 條禁止在儲存通訊的傳送人或傳送對象不知情的情況下，取覽該通訊。

26　澳大利亞聯邦國會（Parliament of the Commonwealth of Australia）眾議院（House of Representatives），《2007 年電訊（截取及取覽）（修訂）法案》摘要說明（Explanatory Memorandum for the Telecommunications (Interception and Access) Amendment Bill 2007），登載於 https://www.legislation.gov.au/Details/C2007B00124/Explanatory%20Memorandum/Text（於 2022 年 5 月 3 日瀏覽）。

絡上截取電話通話的條文演變而來，這帶來的種種挑戰，不少與將這些罪行應用於數碼通訊方面有關。”[27]

加拿大

《1985 年刑事法典》第 342.1(1)(b)條

3.40 在第 2 章，我們提到加拿大《1985 年刑事法典》（Criminal Code 1985）第 342.1(1)條。該條文的四個部分中，(b)段與本章最為相關。根據(b)段，任何人意圖欺詐並在無表面權利的情況下藉電磁、聲音、機械或其他器材截取 *“某電腦系統的任何功能”*，或導致藉電磁、聲音、機械或其他器材截取 *“某電腦系統的任何功能”*，即屬犯罪，一經循公訴程序定罪，最高可處十年監禁。

3.41 我們在第 2 章亦可見《1985 年刑事法典》第 342.1(2)條對“功能”及“電腦系統”的寬廣定義，特別是“功能”包括（但不限於）*“往來某電腦系統或在某電腦系統內的通訊或電訊”*。從表面看，第 342.1(1)(b)條所訂罪行的犯罪行為可涵蓋多種情況。

3.42 該罪行的犯罪意念（*“意圖欺詐並在無表面權利的情況下”*）則相對明確。例如，單是知悉（自己截取或導致截取“某電腦系統的任何功能”）或罔顧後果，並不足以入罪。

《1985 年刑事法典》第 184(1)條

3.43 《1985 年刑事法典》第 VI 部第 184(1)條（*“侵犯私隱”*）訂立另一項與本章相關的罪行：

> “任何人藉任何電磁、聲音、機械或其他器材，故意截取[28]私人通訊，[29] 即屬
>
> (a) 犯可公訴罪行，可處為期不超過 5 年的監禁；或
>
> (b) 犯可循簡易程序定罪而懲處的罪行。”

---

27 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 149 頁。

28 《1985 年刑事法典》第 183 條對“截取”的定義包括 *“監聽、記錄或獲取通訊，或獲取通訊的實質內容、涵義或大意”*。

29 《1985 年刑事法典》第 183 條將“私人通訊”界定為：
“由身處加拿大的發訊人作出或發訊人擬讓身處加拿大的人接收的任何口頭通訊或電訊，而該通訊或電訊在發訊人合理預期不會被他擬讓其接收的人以外的任何人截取的情況下作出，私人通訊包括為了阻止有關通訊被發訊人擬讓其接收的人以外的任何人以清楚易明的形式接收，而藉電子或其他方式處理的任何無線電電話通訊”。

3.44 第 184(2)及(3)條接着列出若干豁除條文。例如，第 184(2)(c)條規定，第 184(1)條並不適用於：

> "從事向公眾提供電話、電報或其他通訊服務，並在以下情況下截取私人通訊的人：
>
> (i) 該項截取對提供該服務而言屬必需，
>
> (ii) 該項截取在服務觀察或抽樣監察的過程中進行，而該服務觀察或抽樣監察對機械或服務質量控制檢查而言屬必需，或
>
> (iii) 該項截取對保障該人與提供該服務直接有關的權利或財產而言屬必需"。

比較第 342.1(1)(b)條與第 184(1)條

3.45 第 342.1(1)(b)條與第 184(1)條所訂罪行的犯罪方式大致相同，它們均是"藉〔任何〕電磁、聲音、機械或其他器材"進行截取。這兩項條文分別訂定的犯罪行為，顯然均可涵蓋針對電腦系統而進行的截取。檢控當局只有在指稱具有"意圖欺詐並在無表面權利的情況下"這項所需的犯罪意念時，方可選擇以第 342.1(1)(b) 條屬較具體的條文為理由，支持根據該條向針對電腦系統進行上述截取的人提出檢控。

3.46 與此同時，如某人並非針對電腦系統而進行截取，即使該人意圖欺詐並在無表面權利的情況下行事，亦只能根據第 184(1)條[30] 被檢控，而不會根據第 342.1(1)(b)條[31] 被判處較重的最高刑罰。有人或會認為，是否涉及電腦系統這一因素，並非具充分說服力的理由解釋這兩項條文不同的最高刑罰。

---

30 *"任何人藉任何電磁、聲音、機械或其他器材，故意截取私人通訊，即屬*
(a) 犯可公訴罪行，可處為期不超過 5 年的監禁；或
(b) 犯可循簡易程序定罪而懲處的罪行。"

31 *"任何人意圖欺詐並在無表面權利的情況下……(b)藉電磁、聲音、機械或其他器材直接或間接截取某電腦系統的任何功能，或導致藉電磁、聲音、機械或其他器材直接或間接截取某電腦系統的任何功能，即屬犯可公訴罪行，可處為期不超過 10 年的監禁，或屬犯可循簡易程序定罪而懲處的罪行"。*

英格蘭及威爾斯

《調查權力法令》第 3(1)條

3.47 在英格蘭及威爾斯，專門對付電腦網絡罪行的法例（《英格蘭誤用電腦法令》）並無條文禁止截取電腦數據，反而《調查權力法令》第 3(1)條（*"非法截取罪"*）才是相關的法規。該條之下共有七款，在此引述首兩款已足夠：

> "(1) 如——
>
> (a) 任何人蓄意在通訊[32]藉以下方式傳送的過程中截取該通訊，
>
> (i) 公共電訊系統，
>
> (ii) 私人電訊系統，[33] 或
>
> (iii) 公共郵政服務，
>
> (b) 該項截取是在聯合王國進行的，及
>
> (c) 該人並無合法權限進行該項截取，
>
> 則該人即屬犯罪。
>
> (2) 但任何人如在通訊藉私人電訊系統傳送的過程中截取該通訊，而該人——
>
> (a) 是有權管控該系統的操作或使用的人，或
>
> (b) 在上述的人明示或默示同意下進行該項截取，
>
> 則不屬犯第(1)款所訂罪行。"

---

32 根據《調查權力法令》第 261(2)條：
"就電訊操作人、電訊服務或電訊系統而言，'通訊'包括——
(a) 任何類別的語言、音樂、聲音、影像或數據所組成的任何事物，及
(b) 用於在人與人之間、人與物之間或物與物之間傳遞任何事物的訊號，或用於開動或控制任何器具的訊號。"

33 該法令第 261 條對"公共電訊系統"及"私人電訊系統"的定義並不特別精闢獨到。不過，該法令顯然預先假定電腦數據可藉電訊系統傳送。例如，第 62(7)條將"互聯網連接紀錄"界定為：
"……為取覽或驅動電腦檔案或電腦程式而藉電訊系統傳送通訊至某電訊服務時，可用於識別……該電訊服務的通訊數據……"。

3.48 《調查權力法令》第 4、5 及 6 條分別解釋“截取”的涵義、在甚麼情況下截取視為在英國進行，以及在甚麼情況下某人有合法權限進行截取。

儲存通訊

3.49 正如我們在上文談及如何處理儲存於通訊系統的數據時提到，《調查權力法令》第 4(4)及(5)條實際上是把第 3(1)條所訂的截取罪應用於在澳大利亞視為“儲存通訊”的通訊。

元數據

3.50 有別於公共郵政服務，在關乎電訊系統的個案中，《調查權力法令》第 4(1)條（載於下文）實際上是把第 3(1)條所訂罪行局限於截取通訊的“內容”：

> “就本法令而言，任何人在以下情況下並僅在以下情況下，方屬在通訊藉電訊系統傳送的過程中截取該通訊——
>
> (a) 該人就該系統作出有關作為，及
>
> (b) 該有關作為的效果，是在有關時間向該通訊的傳送人或傳送對象兩者以外的人提供該通訊的任何內容。
>
> 就通訊而言，‘內容’的涵義見第 261(6)條。”

3.51 《調查權力法令》第 261(6)條內容如下：

> “‘內容’……指該通訊的任何元素，或該通訊所附帶的任何數據，或邏輯上與該通訊相聯的任何數據，而該元素或數據顯露可合理認為是該通訊的涵義（如有的話）的任何事物，但——
>
> (a) 該通訊一事本身所產生的任何涵義，或與傳送該通訊有關的任何數據所產生的任何涵義，均無須理會；及
>
> (b) 任何屬系統數據[34]的事物，均不屬內容。”

---

[34] 《調查權力法令》第 263(4)條將“系統數據”界定為：

3.52 簡言之，通訊的“內容”似乎並不包括元數據。《調查權力法令》就元數據使用“通訊數據”一詞，並在第 261(5)條對該詞作出詳盡定義，“通訊數據”主要涵蓋第 261(3)及(4)條分別界定的“實體數據”及“事件數據”。根據《調查權力法令》第 11(1)條：

> “有關人士如無合法權限而故意或罔顧後果地從電訊操作人或郵政操作人取得通訊數據，即屬犯罪。”

3.53 第 11(2)條將“有關人士”界定為在《調查權力法令》“*（第 3 部所指的）有關公共機構出任職位、職級或崗位的人*”，這顯示第 11(1)條並不適用於由一般大眾進行的截取，對“通訊數據”的保障因此有限。

《2006 年無線電訊法令》第 48(1)(a)條

3.54 另外，我們亦應提及《2006 年無線電訊法令》（Wireless Telegraphy Act 2006，**《無線電訊法令》**）第 48 條（*“截取和披露訊息”*）。根據第 48(1)(a)條，任何人在以下情況，即屬犯罪：

> “……無合法權限而使用無線電訊器具，[35] 並意圖取得與某訊息（不論該訊息是否藉無線電訊發送）的內容、傳送人或收訊人有關的資料，而他本人或由他代表行事的人均並非該訊息的傳送對象”。

3.55 有些行為似乎可同時根據《無線電訊法令》第 48(1)(a)條和《調查權力法令》第 3(1)條被檢控。第 48(3A)條訂定《調查權力法令》實際上凌駕《無線電訊法令》，從而確認了這觀點：

“……使以下任何一項能運作或利便其運作的任何數據，或對於使以下任何一項能運作或利便其運作所關連的任何事物作出識別或說明的任何數據——

(a) 郵政服務；

(b) 電訊系統（包括組成該系統的任何器具）；

(c) 藉電訊系統提供的任何電訊服務；

(d) 有關系統（包括組成該系統的任何器具）；

(e) 藉有關系統提供的任何服務。”

[35] 《無線電訊法令》第 116(2)及 117(1)條將“無線電訊器具”界定為發射或接收以下（在訂明頻率範圍內的）電磁能的器具，而所經途徑並非由為此目的而建造或安排的物料提供：

(a) 用作傳遞訊息、聲音或影像（不論實際上是否有人接收該等訊息、聲音或影像），或用作操作或控制機械或器具的電磁能；或

(b) 在與釐定位置、方位或距離有關連的情況下使用，或為了獲取有關某物件或某類物件是否存在或其位置或移動情況的資料而使用的電磁能。

根據上述定義，該詞語似乎包括 Wi-Fi 路由器及可連接藍芽或 NFC（近距離無線通訊）的智能電話等器材。

"如任何人的行為——

(a) 構成《2016 年調查權力法令》第 3(1)條所訂罪行（非法截取罪），或

(b) 假若沒有（該法令第 6 條所指的）合法權限，便會構成該法令第 3(1)條所訂罪行，

則該人不會因該行為而犯本條所訂罪行。"

中國內地

《中國刑法》第二百八十五條第二款

3.56 第二百八十五條第二款訂定，如*"違反國家規定，侵入〔國家事務、國防建設、尖端科學技術領域的系統〕以外的計算機信息系統……，獲取該計算機信息系統中存儲、處理或者傳輸的數據"*，即屬犯罪。

（底線後加）

截取目標

3.57 第二百八十五條第二款泛指被侵入的計算機信息系統所傳輸的數據，並無區分通訊內容及元數據。因此，第二百八十五條第二款似乎適用於元數據。

3.58 此外，由於第二百八十五條第二款同樣保障計算機信息系統中存儲和處理的數據，因此有關罪行亦適用於靜止數據，例如是在傳送期間暫時靜止的數據，以及儲存於通訊系統的數據。

新西蘭

《新西蘭法令》第 216B 條

3.59 相關的法例條文是《新西蘭法令》第 216B 條（*"禁止使用截取器材"*）。該條文載於關於侵犯個人私隱罪行的《新西蘭法令》第 9A 部，而非載於處理涉及電腦罪行的第 248 至 252 條之中。第 216B 條內容如下：

"(1) 除第(2)至(5)款另有規定外，任何人蓄意藉截取器材截取任何私人通訊，可處為期不超過 2 年的監禁。

(2) 如截取私人通訊的人——

(a) 是該私人通訊的其中一方；或

(b) 依據由以下法令向該人賦予的任何權限，或根據以下法令向該人賦予的任何權限，並按照該權限的條款進行截取——

(i) 《2012 年搜查及監察法令》（Search and Surveillance Act 2012）；或

(ii) 《2017 年情報及保安法令》（Intelligence and Security Act 2017）第 4 部；或

(iii) 《1987 年國際恐怖主義（緊急權力）法令》（International Terrorism (Emergency Powers) Act 1987），

則第(1)款並不適用。

(3) 〔廢除〕

(4) 第(1)款不適用於根據《2004 年懲教法令》（Corrections Act 2004）第 113 條對囚犯通話進行的任何監測，亦不適用於根據該法令第 189B 條授權對私人通訊進行的任何截取。

(5) 在以下情況下，第(1)款不適用於從事向公眾提供互聯網或其他通訊服務的人所操作的任何截取器材對私人通訊進行的截取——

(a) 該項截取是由向公眾提供該互聯網或其他通訊服務的人的僱員，在執行該人職責的過程中進行；及

(b) 該項截取是為了維持該互聯網或其他通訊服務而進行；及

(c) 該項截取就維持該互聯網或其他通訊服務而言屬必需；及

(d) 該項截取僅用於維持該互聯網或其他通訊服務。

(6) 如根據第(5)款所取得的資料不再需用於維持有關互聯網或其他通訊服務，則該等資料須即時銷毀。

(7) 如任何人持有在協助執行根據《2012 年搜查及監察法令》發出的監察器材手令期間取得的任何資料，則該等資料須在該手令屆滿時——

(a) 即時銷毀；或

(b) 交予執行該手令的機關。”

3.60 《新西蘭法令》第 216C 至 216F 條繼而訂明相關事宜，例如禁止披露非法截取的私人通訊，以及禁止處理截取器材。

主要詞語的法定定義

3.61 第 216A(1)條廣泛界定第 216B 條所用的三項詞語：

“就私人通訊而言，**截取**包括在——

(a) 該通訊進行期間；或

(b) 該通訊傳送期間，

聽見、監聽、記錄、監測、獲取或接收該通訊。

截取器材——

(a) 指用於或可用於截取私人通訊的任何電子、機械、電磁、光學或光電工具、器具、設備或其他器材；但

(b) 不包括——

(i) 助聽器或相類器材……；或

(ii) 獲總督會同行政局豁免受本部條文規管的器材……

私人通訊——

(a) 指在可合理視為顯示通訊任何一方意欲將該通訊局限於該通訊各方的情況下作出(不論是以口頭或書面形式或其他形式作出)的通訊;但

(b) 如任何一方理應合理預期通訊可能會被某些未經任何一方明示或默示同意可截取該通訊的其他人截取,則不包括在這些情況下發生的通訊。"

3.62 "通訊"一詞並無獨立定義。無論如何,截取目標均是"進行中"或"傳送中"的私人通訊。這顯然不包括傳送期間暫時靜止的數據,以及在澳大利亞相當於"儲存通訊"的數據。

截取罪的豁除條文

3.63 第 216B(2)至(5)條的豁除條文,主要與執法以及互聯網或其他通訊服務供應商必需進行的截取有關。

3.64 有關第 216B(2)(a)條豁除條文(即截取私人通訊的人是該通訊的其中一方)的指引,見於第 216A(3)條:

"凡在本部提述私人通訊的其中一方,即提述——

(a) 該通訊的任何發訊人,以及發訊人擬讓其接收該通訊的任何人;及

(b) 在該通訊的任何發訊人明示或默示同意下截取該通訊的人,或在發訊人擬讓其接收該通訊的任何人明示或默示同意下截取該通訊的人。"

法律委員會與司法部的聯合研究

3.65 新西蘭的法律委員會(Law Commission)與司法部(Ministry of Justice)於 2016 年 11 月 8 日發表聯合議事文件,[36] 當中提及多個有關《2012 年搜查及監察法令》內"截取"及"私人通訊"定義的問題,這些定義與《新西蘭法令》第 216A(1)條中的定義幾乎完全一樣。

---

[36] 法律委員會及司法部,*Review of the Search and Surveillance Act 2012 (IP40)*,登載於 https://www.lawcom.govt.nz/our-projects/search-surveillance-act-2012(於 2022 年 5 月 3 日瀏覽)。見第 4 章。

3.66 雖然《新西蘭法令》第 216B 條的用字顯示，該條文本擬適用於多種情況，包括針對電腦而進行的截取，但該議事文件提出以下各點：

> "4.11 ……斷定何謂'私人'的測試，取決於通訊任何一方是否'理應合理預期該通訊可能會被截取'……假若國家截取通訊變得普遍平常，便幾乎總可合理預期通訊可能會被截取。
>
> ……
>
> 4.19 另一類很可能不屬'私人通訊'定義範圍的通訊例子，是元數據或機器類型通訊。概括而言，元數據是關於電子活動的資料，與其內容無關。元數據包括進行各種形式的電子通訊時所產生的數據，例如電話通話或電郵的時間及日期、各方電郵地址或電話號碼，以及收發通訊的單元塔或互聯網規約地址。元數據亦可包括互聯網使用者曾到訪的網站。
>
> 4.20 元數據可顯露與關係、位置、身分及活動有關的資料，這些資料可能是寶貴的調查工具。例如，元數據可讓警方證明疑犯與犯罪組織成員通訊，或曾到訪顯示不良材料的網站。
>
> 4.21 然而，元數據似乎並不符合'私人通訊'的定義，因為該定義提述通訊各方及他們的意圖，意味着有關通訊必須在兩人或多於兩人之間進行。"（斜體乃原文所有）

3.67 法律委員會與司法部在 2018 年 1 月 30 日發表的報告[37] 內提出多項建議，其中包括以下建議。下文提述的法令雖是《2012 年搜查及監察法令》，但就《新西蘭法令》第 216B 條而言，這些建議似乎亦大致適用：

(a) 法令應修訂為提述截取"技術"而非"器材"。有關定義應重新草擬，以涵蓋使用電腦程式、器材和其他技術輔助工具。[38]

---

37 登載於新西蘭法律委員會網站，網址為 https://www.lawcom.govt.nz/our-projects/search-surveillance-act-2012（於 2022 年 5 月 3 日瀏覽）。

38 建議 14。

(b) “私人通訊”的定義應予廢除。現時使用“私人通訊”一詞之處應以“通訊”取代，因此需要修訂“截取”及“截取器材”的定義。[39]

(c) 法令應加入條文，將“通訊”界定為包括任何人或機器在任何媒介製造、發送、接收、處理或持有的符號、訊號、脈衝、文字、圖像、聲音、資料或數據。[40]

(d) 新西蘭政府應考慮新西蘭應否加入《布達佩斯公約》。[41]

3.68 法律委員會與司法部的報告有待新西蘭政府回應。

新加坡

《新加坡誤用電腦法令》第 6 條

3.69 《新加坡誤用電腦法令》第 6 條（*“在未獲授權下使用或截取電腦服務”*）規定如下：

“(1) 除第(2)款另有規定外，任何人——

(a) 為了直接或間接取得任何電腦服務，在沒有權限的情況下，故意取用任何電腦；

(b) 在沒有權限的情況下，故意藉電磁、聲音、機械或其他器材直接或間接截取某電腦的任何功能，或故意導致藉電磁、聲音、機械或其他器材直接或間接截取某電腦的任何功能；或

(c) 為了犯(a)或(b)段所訂罪行，故意直接或間接使用電腦或任何其他器材，或故意導致直接或間接使用電腦或任何其他器材，

即屬犯罪，一經定罪——

(d) 可處不超過$10,000 的罰款或為期不超過 3 年的監禁，或兩者兼處；及

---

39 建議 24。讀者會備悉《布達佩斯公約》規定禁止截取非公開傳送的電腦數據。

40 建議 25。

41 建議 44。

(e) 如屬第二次或其後每次定罪，則可處不超過$20,000的罰款或為期不超過5年的監禁，或兩者兼處。

(2) 如因本條所訂罪行而導致任何損壞，被裁定犯該罪行的人可處不超過$50,000的罰款或為期不超過7年的監禁，或兩者兼處。

(3) 就本條而言，未獲授權的取用或截取並非針對——

(a) 任何特定程式或數據；

(b) 任何種類的程式或數據；或

(c) 存於任何特定電腦內的程式或數據，

均屬無關重要。”

3.70 《新加坡誤用電腦法令》第6條以加拿大《1985年刑事法修訂法令》（Criminal Law Amendment Act 1985）第301.2(1)條為藍本，第301.2(1)條已成為於上文引述的《1985年刑事法典》第342.1(1)條。

3.71 《新加坡誤用電腦法令》第6(1)條的三個部分中，(b)部分對應本章的主題事宜。該部分對犯罪行為的擬定方式，特別是“藉電磁、聲音、機械或其他器材”截取“某電腦的任何功能”，與《1985年刑事法典》第342.1(1)(b)條[42]的相似之處顯而易見。《新加坡誤用電腦法令》第2(1)條更逐字逐句採用加拿大《1985年刑事法典》第342.1(2)條對“功能”的寬廣定義。

3.72 儘管新加坡與加拿大的法規有上述相類之處，它們亦有重大差異：

(a) 就犯罪意念而言，根據新加坡的條文，知悉便已足夠。加拿大的條文則規定，犯罪者須“意圖欺詐並在無表面權利的情況下”行事。

(b) 根據新加坡的條文，有關截取必須“在沒有權限的情況下”進行。從加拿大的條文表面上看，這並非罪行元素，儘管按道理，該條文使用“在無表面權利的情況下”等字

---

42 *“任何人意圖欺詐並在無表面權利的情況下……藉電磁、聲音、機械或其他器材直接或間接截取某電腦系統的任何功能，或導致藉電磁、聲音、機械或其他器材直接或間接截取某電腦系統的任何功能，即屬犯……罪……”*。

眼，這意味着只有在沒有權限的情況下進行截取，方屬違法。

《1999 年電訊法令》第 61(b)條

3.73 另外，根據新加坡《1999 年電訊法令》（Telecommunications Act 1999）第 61 條（*"蓄意損壞用於電訊的裝置或工業裝置"*）：

> "任何人意圖——
>
> (a) 為阻止或妨礙任何訊息的傳送或傳遞；
>
> (b) 為截取或令其本人知悉任何訊息的內容；或
>
> (c) 為導致損害，
>
> 而損壞、移除、干預或觸摸屬於公共電訊持牌人而用於電訊的任何裝置或工業裝置（或其任何部分），或干擾公共電訊持牌人的無線電通訊服務或系統，[43] 即屬犯罪。"

3.74 這條文的(b)部分可對照香港《電訊條例》（第 106 章）第 27(b)條。第 27(b)條提述某人的意圖是"截取或找出任何訊息的內容"，顯然並不涵蓋截取與訊息有關的元數據。較後這一點似乎亦適用於新加坡《電訊法令》第 61(b)條。

比較加拿大法律與新加坡法律

3.75 如上文所述，[44] 加拿大《1985 年刑事法典》第 342.1(1)(b)及 184(1)條所訂罪行似乎均適用於電腦網絡空間，但只有後者涵蓋並非針對電腦系統而進行的截取。由於兩項罪行的犯罪意念有別（"意圖欺詐並在無表面權利的情況下"相對"故意"），而且最高刑罰不一（監禁十年相對五年），兩者不同的涵蓋範圍或會造成不公。

3.76 反之，《新加坡誤用電腦法令》第 6(1)(b)條和《1999 年電訊法令》第 61(b)條所訂罪行均沒有規定犯罪意念標準與"意圖欺詐"同樣地高（條文分別只要求"故意"和"意圖"）。若根據當中

---

43 根據該法令第 6 條：
"有關當局〔資訊通訊媒體發展局〕可在部長批准下，指定根據第 5 條獲批出牌照作為公共電訊持牌人的任何人，根據本法令履行全部或任何關乎在新加坡經營和提供電訊系統及服務的職能（屬發展局專有特權所管限範圍內者）。"

44 第 3.45 至 3.46 段。

任何一條定罪，均可處不超過 10,000 新加坡元的罰款或為期不超過三年的監禁，或兩者兼處。[45] 這兩項條文將類似的行為定為不合法，並附帶相同的最高刑罰，而這些刑罰與條文訂定的相應犯罪意念大致相若。

3.77 就前兩段所引的法規而言，新加坡法律似乎比加拿大法律較少不一致的問題。

美國

概覽

3.78 以下學術觀點對美國有關法例的看法頗為負面：

> "某著名評論員曾將美國的監察法例形容為'若非徹底難明費解，其錯綜複雜也是人所共知'，而法院亦指有關法例'繁複晦澀'、'含混不清且毫不明確'，是一場'舉證惡夢'。截取法例隨着《1986 年電子通訊私隱法案》（Electronic Communications Privacy Act 1986，《電子通訊私隱法案》）制定而經歷重要改革，但由於這條法案早於互聯網及萬維網面世前擬訂，故不少困難由此而生。因此，現有法律框架並不適合應對現代的通訊形式，'普遍視為落後過時'。"[46]

3.79 該著者亦指出，有關截取法例的複雜之處、辯論及改革，大多與執法部門進行監察的能力有關，而美國的案例及評註主要關乎美國憲法《第四條修正案》對免受不合理搜查和檢取的保障。[47]

3.80 美國的相關法例現時由三部分組成，分別為規管截取通訊內容的《搭線竊聽法案》（Wiretap Act）、[48] 規管取覽儲存通訊的《儲存通訊法案》（Stored Communications Act），[49] 以及規管取覽流量數據（一種元數據）的《通訊紀錄器法案》（Pen Register Act）。[50]

---

45 《新加坡誤用電腦法令》第 6(1)條及《1999 年電訊法令》第 85 條。

46 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 155 頁（書內引文省略）。

47 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 150 頁。

48 《電子通訊私隱法案》第 I 篇，編纂於《美國法典》第 18 篇第 2510 至 2523 條。

49 《電子通訊私隱法案》第 II 篇，編纂於《美國法典》第 18 篇第 2701 至 2713 條。

50 《電子通訊私隱法案》第 III 篇，編纂於《美國法典》第 18 篇第 3121 至 3127 條。

《搭線竊聽法案》內的《美國法典》第 18 篇第 2511(1)條

3.81　就本章而言，可集中研究《美國法典》第 18 篇第 2511(1)條：

"除本章[51]另有特別規定外，任何人如——

(a) 蓄意截取、嘗試截取或促致任何其他人截取或嘗試截取任何有線、口頭或電子通訊；

(b) 蓄意使用、嘗試使用或促致任何其他人使用或嘗試使用任何電子、機械或其他器材，以截取任何口頭通訊……；

(c) 蓄意向任何其他人披露或嘗試向任何其他人披露任何有線、口頭或電子通訊的內容，並知悉或有理由知悉有關資料是在違反本款的情況下透過截取有線、口頭或電子通訊而取得的；

(d) 蓄意使用或嘗試使用任何有線、口頭或電子通訊的內容，並知悉或有理由知悉有關資料是在違反本款的情況下透過截取有線、口頭或電子通訊而取得的；或

(e) (i) 蓄意向任何其他人披露或嘗試向任何其他人披露……截取的任何有線、口頭或電子通訊的內容，

(ii) 並知悉或有理由知悉有關資料是在與刑事調查相關的情況下，透過截取上述通訊而取得的，

(iii) 並在與刑事調查相關的情況下取得或接收有關資料，及

(iv) 意圖不正當地妨礙、阻撓或干擾妥為授權的刑事調查，

---

51 《美國法典》第 18 篇（罪行及刑事法律程序）第 I 部（罪行）第 119 章（有線及電子通訊截取和口頭通訊截取）（Chapter 119 (Wire and Electronic Communications Interception and Interception of Oral Communications), Part I (Crimes), Title 18 (Crimes and Criminal Procedure), United States Code）。

則須按照第(4)款的規定懲處，或按照第(5)款的規定被起訴。”

有線、口頭及電子通訊的涵義

3.82 第 2511(1)條把有線、口頭及電子通訊區分開來。第 2510 條界定這些詞語：

> “(1) ‘有線通訊’指任何符合以下說明的聽覺傳訊：該傳訊之全部或部分是透過使用……通訊傳送設施，借助導線、電纜或其他在來源點與接收點之間的類似接駁裝置……而作出的；
>
> (2) ‘口頭通訊’指某人說出的任何口頭通訊，而該人在有理由預期該通訊不會被截取的情況下，展示出他如此預期，但該詞不包括任何電子通訊；
>
> (12) ‘電子通訊’指符號、訊號、文字、圖像、聲音、數據或消息（不論任何性質）的任何傳訊，而該傳訊之全部或部分是透過影響州際貿易或對外貿易的導線、無線電、電磁、光電子或光學系統而傳送的，但不包括——
>
> (A) 任何有線或口頭通訊；
>
> (B) 任何透過只具音頻系統的傳呼器材作出的通訊；
>
> (C) 任何由追蹤器材……發出的通訊；或
>
> (D) 金融機構在用作電子儲存及資金轉帳的通訊系統中儲存的電子資金轉帳資料”。

截取目標

3.83 第 2511(1)(a)條禁止截取“任何有線、口頭或電子通訊”，而第 2511(1)(c)、(d)及(e)條則適用於在訂明情況下披露和使用截取通訊的“內容”。儘管用字有所不同，但基於第 2510 條以下定義，第 2511(1)(a)條定為不合法的截取，其目標似乎亦只限於通訊的內容：

> “(4) ‘截取’指透過使用任何電子、機械或其他器材，聽取或以其他方式獲取任何有線、電子或口頭通訊的內容；

(8) ‘內容’用於任何有線、口頭或電子通訊時，包括關於該通訊的實質內容、大意或涵義的任何資料”。

在傳送期間暫時靜止的數據

3.84 特別就“電子通訊”而言，該詞語的法定定義中“傳訊”及“傳送”等文字顯示該詞語指傳遞中的通訊。然而，聯邦上訴法院第一巡迴法庭（Court of Appeals for the First Circuit）在 *United States v Councilman* 一案裁定，該詞語 *“包括通訊過程中固有的短暫電子儲存”*。[52]

罪行的豁除條文

3.85 第 2511(1)條所訂罪行不適用於因着第 2511(2)條而獲豁除者。這些獲豁除者主要是：

(a) 有線或電子通訊服務的供應商；

(b) 聯邦通訊委員會（Federal Communications Commission）履行執法（監察）職責的人員、僱員或代理人；

(c) 進行獲授權電子監察的美國人員、僱員或代理人；

(d) 有關通訊的其中一方；及

(e) 獲有關通訊其中一方事先同意進行截取的人。

《儲存通訊法案》（《美國法典》第 18 篇第 2701 至 2713 條）

3.86 簡言之，《儲存通訊法案》：

> “……保障服務供應商所存檔案的內容及服務供應商所持的用戶紀錄（例如用戶姓名、帳單紀錄或互聯網規約地址）的私隱。”[53]

---

52 *United States v Councilman*, 418 F 3d 67 (1st Cir 2005)，第 85 頁。

53 司法協助局（Bureau of Justice Assistance），“Electronic Communications Privacy Act of 1986 (ECPA)”，登載於：https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285（於 2022 年 5 月 3 日瀏覽）。

3.87 《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，則須按照本條第(b)款的規定懲處。"

3.88 《美國法典》第 18 篇第 2701(c)條所載的例外情況包括：

"(1) 提供有線或電子通訊服務的人或實體所授權的行為；

(2) 有關服務的使用者就其本人的通訊所授權的行為，或就以該使用者為對象的通訊所授權的行為；或

(3) 本篇第 2703、[54] 2704[55] 或 2518[56] 條所授權的行為。"

《通訊紀錄器法案》（《美國法典》第 18 篇第 3121 至 3127 條）

3.89 有關法例將《通訊紀錄器法案》內兩個主要詞語（即*"通訊紀錄器"*及*"監測追蹤裝置"*）界定如下：

"(3) '通訊紀錄器'一詞指記錄或解譯從傳送有線或電子通訊的儀器或設施傳送的撥號、發訊路線、發訊對象或訊號資料的器材或過程，但該等資料不包括任何通訊的內容……；

(4) '監測追蹤裝置'一詞指獲取正輸入的電子或其他脈衝資料的器材或過程，以識別來源號碼或其他

---

54 *"規定須披露客戶通訊或紀錄"*。

55 *"備份保存"*。

56 *"截取有線、口頭或電子通訊的程序"*。

撥號、發訊路線、發訊對象及訊號資料，而該等資料合理地相當可能會識別某項有線或電子通訊的來源，但該等資料不包括任何通訊的內容”。[57]

3.90 《通訊紀錄器法案》首先一律禁止使用通訊紀錄器及監測追蹤裝置：

> “除本條另有規定外，任何人如沒有事先根據本篇第3123條或《1978年外國情報監察法案》(Foreign Intelligence Surveillance Act of 1978)（《美國法典》第50篇第1801條及其後段落）取得法庭命令，或沒有事先從受行政協議（獲司法部長斷定並向國會證實符合第2523條者）所規管的海外政府取得命令，則不得安裝或使用通訊紀錄器或監測追蹤裝置。”[58]

3.91 下一條接着規定，代表美國政府的律師可向法庭申請授權或批准安裝通訊紀錄器或監測追蹤裝置，或申請授權或批准使用通訊紀錄器或監測追蹤裝置。[59]

小組委員會的看法

把在未獲授權下截取電腦數據定為不合法

3.92 我們於本章起首指出，既然靜止數據應受保障，使其免遭非法取覽，那麼傳遞中的數據亦應受保障，使其免遭非法截取。兩者不但會引起私隱方面的關注，[60]亦可能會帶來其他潛在問題，例如被截取的數據如遭利用，可能會造成財務損失。[61]

3.93 據我們理解，任何未經編碼處理的電腦數據，如在開放連接的網絡上傳送，便可被外界截取。[62] 電腦數據即使被截取，仍相當可能繼續傳送。人類傳送或接收該等數據所構成的通訊，未必會察覺通訊已被截取，有關截取作為可能只有經第三方才會曝光。

---

57 《美國法典》第18篇第3127條。

58 《美國法典》第18篇第3121(a)條。

59 《美國法典》第18篇第3122(a)(1)條。

60 《個人資料（私隱）條例》（第486章）只適用於可識別在世的個人的身分的資料，而該條例所訂的刑罰亦相對較輕。

61 例如，信用卡資料在傳送至賣方期間，被截取作不當用途。

62 很多網上通訊採用稱為HTTPS（保密超文本傳輸規約）的規約，數據會在傳送前先經過編碼處理。雖然有人或可截取部分通訊，但該部分不會是純文字，而且必須加以解密。

3.94 為保存通訊完整無損，我們認為應把在未獲授權下截取電腦數據定為罪行，亦應禁止在未獲授權下披露或使用截取的數據。由於現今使用不同器材均會經常牽涉傳遞中的數據（即可能遭他人在未獲授權下截取的數據），我們希望建議的罪行有助並鞏固器材之間的可靠連接。隨着量子計算時代來臨，所有數據或可通通保留，我們亦因此預期建議的罪行會變得更為重要。

3.95 我們對香港及多個其他司法管轄區現行法例所進行的研究顯示，多項與非法截取電腦數據相關的法規並行共存，背後原因顯然是有需要立法涵蓋對各式通訊的截取，包括電腦網絡空間內外的通訊。

3.96 根據小組委員會的職權範圍，我們建議訂立適用於電腦數據的截取罪，但同時保留立法規管現實世界中對應罪行的可能性，以留待政府從長計議。我們相信，建議的罪行會補足只適用於公職人員的《截取通訊及監察條例》。

為不誠實或犯罪目的而截取

3.97 現代網絡器材的運作方式難免牽涉截取。有鑑於現時的科技，我們承認假如純粹在未獲授權下截取電腦數據便會招致刑責，則我們建議的罪行範圍未免不合理地寬廣。例如，即使以下現象可能牽涉在未獲授權下進行截取，我們相信沒有很多人會認為它們有不妥：

(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個網站。

(b) 在日常運作中，互聯網服務供應商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。此外，某些種類的數據（例如有關域名系統查詢的通訊）只屬暫時性質，但其他種類的數據（例如域名系統紀錄、登入數據及電郵事項）則不然。

3.98 我們就建議的罪行的犯罪意念提出多個可能性後，總結認為不應堅持須證明有犯*某項特定罪行*的意圖，因為這樣可能會令執法過於困難。

3.99 我們建議，在建議的罪行下，有關截取須“為不誠實或犯罪目的”而進行。

罪行適用範圍不限於私人通訊

3.100 我們提到，《布達佩斯公約》第三條所訂罪行適用於“非公開”傳送電腦數據。[63] 如《說明報告》所述，“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。[64] 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。

3.101 我們亦留意到在新西蘭，其法律委員會及司法部：

(a) 認為在決定通訊是否屬私人通訊時，參照通訊任何一方是否“理應合理預期該通訊可能會被截取”的做法並不理想；[65] 及

(b) 提議以“通訊”取代《2012 年搜查及監察法令》中對“私人通訊”的提述。[66]

3.102 我們認為，儘管法律委員會及司法部的提議是建基於新西蘭對“私人通訊”的法定定義，他們強調不宜聚焦於通訊各方的預期[67]這一理據，對其他司法管轄區而言確是真知灼見。

3.103 基於以上考慮，我們贊成訂立能保障一般通訊（而並非只保障私人通訊）的截取罪。

罪行涵蓋包括元數據在內的所有數據

3.104 大體來說，通訊的元數據可與通訊的內容相對照。電腦網絡空間內的元數據通常與規約層面或系統層面的事物有關。

3.105 然而，從技術角度而言，現實的情況更為複雜，尤其是互聯網採用分層方式，某層的元數據可能是另一層的數據。例如，中繼信息在網絡層面屬數據，但就電郵而言卻是元數據。元數據並非定義明確的概念。

3.106 另外，雖然在某些司法管轄區內，截取罪似乎不適用於元數據，但原因可能是這些罪行在多年前引入，而當代的元數據概念尚未在電子或電腦通訊的背景下出現。

---

63 第 3.17 段。

64 《說明報告》第 54 段（於上文第 3.18 段引述）。

65 法律委員會及司法部，*Review of the Search and Surveillance Act 2012 (IP40)*，第 4.11 段（於上文第 3.67 段引述）。

66 第 3.67(b)段。

67 如第 3.82 段所述，美國對“口頭通訊”的法定定義亦提述通訊方預期的事宜。

3.107　考慮到上述因素，我們建議，建議的罪行應一般適用於數據（不論有關數據是否元數據）。

罪行適用於整個傳送過程中的數據

3.108　關於在傳送期間暫時靜止的數據，我們已於上文[68]討論有關問題。

3.109　為簡易起見，我們建議只要有關數據是在傳送人一端前往傳送對象一端的途中，截取有關數據便應屬犯罪。訂立這項罪行的方法之一，是加入類似於上文第 3.22 段所載的《電訊（截取及取覽）法令》第 5F 條的推定條文。

3.110　至於儲存於通訊系統內的數據，我們於上文提到，這類數據顯然不受《截取通訊及監察條例》規管。[69] 因此我們提議，建議的非法截取罪不應適用於這類數據（我們認為這類數據反而應受第 2 章建議的非法取覽罪規管）。

香港法例的藍本

3.111　我們研究的所有司法管轄區中，相關法規各有不同。就作為香港的參考對象而言，《示範法》第 8 條（*"非法截取數據等"*）與我們的構思最為相近：

> "任何人如在無合法辯解或理由的情況下，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非公開傳送；或
>
> (b) 來自某電腦系統並載有電腦數據的電磁發射；[70]
>
> 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。"

68　第 3.21 至 3.24 段。

69　第 3.25 段。

70　《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"。

3.112　上述罪行的擬定方式須加以修改，以反映我們的其他建議。舉例來說，香港的條文：

(a) 應訂定該條文適用於在沒有“權限”下進行的截取，而非沒有“理由”依據的截取（後者的概念似乎較廣）；

(b) 不應只限適用於“非公開”傳送；及

(c) 應包含有關截取須“為不誠實或犯罪目的”而進行這個犯罪意念。

建議 4

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）第 8 條為藍本，包括犯罪意念（即“蓄意”截取）。

社會可能視為正當調查的行為

3.113 在第 2 章，我們提到建議的非法取覽罪可能會對網絡安全從業員造成影響。我們在建議 2 提出以下問題：在未獲授權下為網絡安全目的而取覽，應否有特定的免責辯護或豁免。[71]

3.114 我們在考慮建議的非法截取罪時，同樣亦討論到該罪行會否無意間對社會可能視為正當調查的行為造成影響。

3.115 我們歡迎社會各界就這個議題發表意見。

真實業務進行的截取

真實業務進行截取的情況普遍

3.116 儘管大多數人很可能會同意惡意截取他人數據是不當行為，例如藉着設置虛假 Wi-Fi 熱點（可能利用具誤導性的服務設定識別碼），提供 Wi-Fi 熱點或電腦供顧客或僱員使用的真實業務（咖啡店、酒店、購物商場、僱主等），在提供網絡連接之餘，還應否獲准截取傳送的數據，這個問題值得商榷：

(a) 隨着數據分析面世，即使是真實業務，也可能有動機截取屬於或關於顧客的數據，並可能從中獲益，而顧客卻未必察覺這些能夠進行（據我們理解是經常進行）的數據分析何其深入。

(b) 在僱傭關係中，僱主可能會懷疑僱員有若干行為（例如犯罪，或違反僱傭合約的限制性契諾，向競爭對手或準僱主披露機密商業資料），因此或會想截取和分析往來僱員電腦的數據傳送。

被截取的數據的用途

3.117 在上述例子和類似情況下被截取的數據可能有不少用途，我們在下文概述部分用途：

(a) 網絡系統供應商一直向購物商場的東主推銷一種新業務。具體而言，購物商場內的網絡系統可追蹤連接至該系統的器材（購物商場顧客的智能電話、平板電腦等）所在

---

71 第 2.110 至 2.114 段。

位置，藉此追蹤持有這些器材的顧客的活動。這些位置數據可：

(i) 顯示這些器材的使用者較常光顧哪些商店（他們便會是這些商店的目標顧客）；[72] 及

(ii) 利便按照位置提供服務（例如“推送”相關廣告這項服務現已相當普遍）。

(b) 網絡器材設有一項標準功能，顯示在該等器材所提供網絡服務的用戶當中，哪些網站最受歡迎。互聯網服務供應商便可把所截取的用戶數據提供予內容排名公司進行分析。

條款及條件

3.118 上述業務可根據若干條款及條件提供 Wi-Fi 熱點或電腦供人使用，而有關條款及條件可保留權利截取和使用顧客或僱員的數據（例如進行流量分析和其他種類的數據分析）。這類截取和使用數據的權限屬於合約性質。

3.119 在某些情況下，實在無從確定有多少顧客或僱員會細閱或明白這些條款及條件。其中有關考慮是，儘管不論有關業務規模大小，同一行為（截取數據）原則上理應導致同一法律後果，規模較大的業務一般有能力擬定周全細密的條款及條件，而這些條款及條件往往不容協商，並且向有關業務傾斜。

3.120 可更有效保障顧客和僱員的其中一個方法，是規定業務須具有法定權限，方可合法截取數據，即截取必須符合法例施加的若干規定。不過，假如只有根據法定權限方可進行數據分析，而不能根據合約權限進行該分析，我們預見不少數據分析工作將須終止。有人或會認為這樣過分嚴苛。

徵詢公眾回應

3.121 在上述各段中，[73] 我們已概述多個可能出現的例子和情況，說明各類專業及真實業務可能截取數據和使用截取或傳送的數據。我們竭力確保我們的建議公平對待各方持份者，並公正地平衡兼顧他們的利益，因此在應否准許上述各段所識別的各類數據截取和使

---

72 購物商場的東主或會認為，這類資料有助優化租戶組合和決定適當的租金水平等。

73 第 3.113 至 3.120 段。

用的問題上，我們希望收到公眾的意見。若公眾在這方面的回應是肯定的，我們亦歡迎公眾進一步建議應准許哪類專業及業務截取數據和使用截取或傳送的數據，以及建議有關准許應否附帶任何條件或限制。假如能夠全面識別相關的例子及情況，我們便可更周詳考慮應如何擬定建議的免責辯護或豁免（例如新訂的電腦網絡罪行法例是否可藉參照公認的法律概念，比如有合理目的或合法權限及不含惡意，從而對這些例子及情況作一般描述），以及這些免責辯護或豁免應如何施行（例如如何履行舉證責任）。

3.122 我們冀望公眾能就以下建議5內的諮詢問題發表意見。

建議5

小組委員會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實業務（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）？

第 4 章　非法干擾電腦數據

引言

4.1　我們會在本章探討第三類依賴電腦網絡的罪行，即非法干擾電腦數據，而非法干擾電腦系統則會在下一章集中討論。概括而言，就此主題而訂立的罪行，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。

4.2　第 2 章建議訂立的非法取覽罪，所針對的是入侵電腦系統的初期。隨着入侵更進一步，干擾數據便可能構成本章所討論的罪行。這兩項罪行息息相關，特別是因為以下原因：

> "……其中一項支持把純粹在未獲授權下取用系統定為罪行的論據，是該項取用能夠造成非蓄意的損壞。"[1]

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。

香港的現行法律

《刑事罪行條例》（第 200 章）

第 60 條

4.4　現時，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一種形式。根據《刑事罪行條例》（第 200 章）第 60(1)及(2)條（*"摧毀或損壞財產"*）：

1　Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press, 2007)，第 3.268 段。

"(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) 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。"

4.5 與第 60(1)條相比，第 60(2)條所訂罪行顯然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。"

1993 年的立法修訂

4.6 《1993 年電腦罪行條例》（1993 年第 23 號）將《刑事罪行條例》（第 200 章）就"財產"一詞所採用的涵義，擴至包括 *"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。"*[2]

4.7 《1993 年電腦罪行條例》繼而在《刑事罪行條例》（第 200 章）加入第 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；

---

[2] 《刑事罪行條例》（第 200 章）第 59(1)(b)條。

(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)部分與本章最為相關。

4.8 此外，《1993 年電腦罪行條例》：

(a) 將在銀行簿冊等作出虛假記項罪適用於在電腦作出的記項；[3]

(b) 將入屋犯法罪的適用範圍，擴大至包括作為侵入者進入任何建築物，意圖誤用在該建築物內的電腦／電腦程式或數據的人；[4] 及

(c) 將偽造帳目罪適用於用電腦保存的紀錄。[5]

展示成功執法的案例

4.9 *HKSAR v Chan Chi Kong*[6] 是首宗根據 1993 年修訂的《刑事罪行條例》（第 200 章）而檢控誤用電腦的案件。[7] 被告人承認無合法辯解而銷毀其僱主在客戶辦事處安裝的電腦檔案。高等法院上訴法庭在審理被告人就判刑提出的上訴時裁定，儘管受影響的電腦系統後來得以還原，令有關檔案失而復得，原審法庭仍有充分理由判處扣押刑罰。[8]

4.10 在 *HKSAR v Ko Kam Fai*，[9] 男被告人對兩名女受害人的電郵帳戶進行黑客入侵，更改受害人電腦的數據，令受害人的電郵帳戶無法操作。他又向受害人發送含有淫褻內容及強姦威脅的電郵。他承認多項刑事恐嚇和刑事損壞的控罪，分別違反《刑事罪行條例》（第 200 章）第 24 及 60(1)條。

---

3 藉在《刑事罪行條例》（第 200 章）加入新的第 85(2)條。
4 藉在《盜竊罪條例》（第 210 章）加入新的第 11(3A)條。
5 藉在《盜竊罪條例》（第 210 章）加入新的第 19(3)條。
6 [1997] 3 HKC 702, CACC 245/1997（判決日期：1997 年 9 月 25 日）。
7 根據被告人代表大律師的陳詞（見判詞第 706 頁 H 行）。
8 然而，判刑由區域法院所判的監禁兩年八個月，縮短至監禁一年九個月。
9 [2001] 3 HKC 181, CACC 83/2001（判決日期：2001 年 6 月 20 日）。

4.11 由於案中電腦所受損壞屬短期性質，故被告人就八項刑事損壞控罪的每一項被判處監禁四個月。兩項刑事恐嚇的控罪則較為嚴重，所判處的刑期亦較長（各為監禁 12 個月，這兩項控罪的刑期與各項刑事損壞控罪的刑期同期執行）。被告人只針對刑事恐嚇的判刑提出上訴，但被駁回。上訴法庭指出，就刑事損壞控罪的較輕判刑而言，*"雖然所判刑期表面上似乎較短，但在本案的特別情況下，刑事恐嚇的控罪才是罪行重點"*。[10]

與第 161 條作比較

4.12 雖然《刑事罪行條例》（第 200 章）第 60 條所訂最高刑罰（通常是監禁十年）較第 161 條所訂最高刑罰（監禁五年）為重，但這兩項條文均適用於電腦網絡空間。據我們所理解，被控第 161 條所訂罪行的人，偶爾也會被控第 60 條所訂罪行，作為交替控罪。控方可視乎案情而將第 60 條視為第 161 條的合適後備條文：

(a) 如某電腦因足夠穩健而未受損壞，只要有證據證明某人在未獲授權下蓄意取用或操作該電腦，便足以根據第 161 條提出控罪。

(b) 然而，若有關證據只顯示對電腦數據的更改是源自某些互聯網規約地址（可沿該等地址追查犯罪者的身分），根據第 60 條提出控罪可能更為恰當。

(c) 懷有意圖或罔顧後果均足以構成第 60 條的犯罪意念。這可能比第 161(1)(a)至(d)條所詳述的意圖更易證明。[11]

《電訊條例》（第 106 章）

第 25(a)條

4.13 《電訊條例》（第 106 章）第 25(a)條（*"電訊人員以外的人隱匿訊息等"*）訂立了以下簡易程序罪行：

> "任何不屬電訊人員或不屬雖非電訊人員但其公務與電訊服務相關者的人，如——

---

10 同上，第 185 頁。

11 根據第 161(1)條，任何人不得有下述意圖或目的而取用電腦：
"(a) 意圖犯罪；
(b) 不誠實地意圖欺騙；
(c) 目的在於使其本人或他人不誠實地獲益；或
(d) 不誠實地意圖導致他人蒙受損失"。

(a) 故意隱匿、扣留或阻延擬傳遞予另一人的訊息；或

(b) 〔……〕

即屬犯罪，一經循簡易程序定罪，可處第 4 級罰款[12] 及監禁 12 個月。”

並非針對電腦網絡罪行的特定條文

4.14 第 25(a)條的措辭看來足以禁止他人抑制構成“訊息”的電腦數據（藉電訊）傳送。然而，第 25(a)條在應用於電腦數據時會有限制，這些限制與第 3 章所論述關於第 27(b)條的限制相類似：[13]

(a) 由於第 25(a)條以電訊為前提背景，故該條的擬定方式——包括對“電訊人員”、“訊息”[14] 等的提述——並未能有效應用於電腦網絡空間。

(b) 第 25(a)條的犯罪行為只涵蓋隱匿、扣留或阻延訊息，並無涵蓋其他干擾電腦數據的方式（例如刪除數據或將數據加密）。

《布達佩斯公約》訂定罪行的標準

4.15 就本章而言，《布達佩斯公約》[15] 的相關條文是第一節之下的第一篇第四條：

“1. 各締約方均應採取必要的立法及其他措施，在其本土法律中將下列行為定為刑事罪行：在無權的情況下蓄意損壞、刪除、弄壞、更改或抑制電腦數據。

2. 任何締約方可保留權利，規定第 1 段所述的行為須造成嚴重傷害。”

---

12 根據《刑事訴訟程序條例》（第 221 章）附表 8，現為 25,000 元。

13 第 3.14 至 3.16 段。

14 “訊息”的法定定義載於第 3.14 段。

15 有關《布達佩斯公約》的背景資料，見導言第 11 段，以及第 1 章第 1.6 至 1.10 段。

4.16 《說明報告》中有關第四條的內容如下：

"60. 本條旨在對電腦數據及電腦程式提供免遭蓄意損壞的保護，使其所受的保護與有體物所受的保護相若。這裏受保護的法定權益，是所儲存電腦數據或電腦程式的完整性，以及有關數據或程式的正常運作或使用。

61. 在第1段，'損壞'數據和'弄壞'數據這兩種重疊的作為，尤其涉及對數據及程式的完整性或資訊內容作出不利的更改。'刪除'數據等同於摧毀有體物，即是把數據銷毀至難以辨識。抑制電腦數據指以下行動：阻止或終止可取用電腦或數據載體的人獲取儲存於電腦或數據載體的數據。'更改'一詞指修改現有數據。因此，本段既涵蓋輸入病毒和特洛伊木馬等惡意程式碼，也涵蓋對數據因此而造成的修改。

62. 上述作為只有在'無權'的情況下作出，方可予以懲處。網絡設計中固有的常見活動或普遍的操作或商業慣例，例如在擁有人或操作人的授權下測試或保護電腦系統的安全性，又或在系統操作人獲取新軟件（例如准許接達互聯網但會停用先前安裝的相類程式的軟件）時重新設定電腦的作業系統，均是在有權的情況下作出的，因此不會被本條定為罪行。為方便進行匿名通訊（例如匿名郵件轉發系統的活動）而修改流量數據，或為進行安全通訊（例如將數據加密）而修改數據，原則上應視為對私隱的合法保障，故應視為在有權的情況下進行。然而，締約方不妨把某些涉及匿名通訊的濫用行為（例如更改數據包的標頭資料以隱藏犯罪者身分）定為罪行。

63. 此外，犯罪者須'蓄意'行事。

64. 第2段容許締約方就有關罪行作出保留，使締約方可規定有關行為須造成嚴重傷害。至於何謂嚴重傷害，則留待本土法律解釋……"[16]

16 《說明報告》第60至64段。

其他司法管轄區的法定體制

澳大利亞

主要概念的法定定義

4.17 讀者可能記得第 3 章提到，《刑事法典》（聯邦）（Criminal Code (Cth)）第 10.7 部定為不合法的主要行為種類有：在未獲授權下取覽電腦數據、在未獲授權下修改電腦數據，以及在未獲授權下損害電子通訊。[17]

4.18 我們在研究有關罪行前，宜先研究第 476.1(1)條如何界定第二類及第三類非法行為（"損害往來某電腦的電子通訊"的定義已在第 3 章列明，但值得在此重述）：

> "**電子通訊**指藉導向電磁能或無導向電磁能而以任何形式傳達資料。"
>
> "就存於某電腦內的數據而言，**修改**指：
>
> (a) 更改或移除該等數據；或
>
> (b) 對該等數據作出增補。"
>
> "**損害往來某電腦的電子通訊**包括：
>
> (a) 阻止進行上述通訊；或
>
> (b) 在該電腦所使用的電子聯網或網絡上損害上述通訊；
>
> 但不包括純粹截取上述通訊。"

4.19 根據上述定義，上述以粗體表示的詞語與非法干擾電腦數據相對應，儘管該等詞語涉及該罪行不同的層面。

---

17 第 3.32 段。

《刑事法典》（聯邦）第 477.1 條

4.20 第 477.1 條（*"在未獲授權下作出取覽、修改或損害，並意圖干犯嚴重罪行"*）已在第 2 章論述，討論側重於有關在未獲授權下取覽電腦數據的第 477.1(1)(a)(i)條。[18]

4.21 第 477.1(1)(a)(ii)及(iii)條與本章相關，規定任何人如導致"在未獲授權下修改存於某電腦內的數據"，或導致"在未獲授權下損害往來某電腦的電子通訊"，而該人知悉該行為未獲授權，並意圖藉該行為而干犯（或利便干犯）違反聯邦、各州或領地法律的嚴重罪行，即屬犯罪。

4.22 "嚴重罪行"是可處終身監禁或為期五年或以上監禁的罪行。[19] 任何人違反第 477.1(1)條，可處不超過適用於嚴重罪行的刑罰。

《刑事法典》（聯邦）第 477.2 條

4.23 如證據未能證明有干犯（或利便干犯）嚴重罪行的意圖，則第 477.2 條（*"在未獲授權下修改數據，以導致損害"*）仍可能適用：

> "(1) 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。
>
> 刑罰：監禁 10 年。
>
> (3) 即使沒有實際上損害或不會實際上損害：
>
> (a) 對存於某電腦內的數據的取覽；或

---

18 第 2.21 段。

19 《刑事法典》（聯邦）第 477.1(9)條。

(b) 上述數據的可靠性、保安或操作，

任何人仍可被裁定犯違反本條的罪行。

(4) 違反本條罪行的定罪判決，可作為違反第 477.3 條罪行（在未獲授權下損害電子通訊）的控罪的交替裁決。”

4.24 第 477.2(3)條似乎旨在明確地表明，任何人如罔顧自己在未獲授權下作出的修改會否實際上造成第 477.2(3)條所描述的損害，即屬干犯第 477.2(1)條所訂罪行。然而，由於第 477.2(1)(c)(ii)條採用了廣泛的措辭來表達損害的對象，因此任何人譬如在電腦系統引入類似計時炸彈的軟件（即經設計以在未來某時間無需進一步干預而損害數據，或在某事件發生時損害數據的軟件），便可能干犯第 477.2(1)條所訂罪行。我們亦於下文第 4.73 段對美國的相關法例提出類似觀點。

《刑事法典》（聯邦）第 477.3 條

4.25 相反，如根據第 477.3 條（*“在未獲授權下損害電子通訊”*）提出控罪，實際損害則是重要元素：

“(1) 任何人在以下情況，即屬犯罪：

(a) 該人導致在未獲授權下損害往來某電腦的電子通訊；及

(b) 該人知悉該項損害未獲授權。

刑罰：監禁 10 年。

(3) 違反本條罪行的定罪判決，可作為違反第 477.2 條罪行（在未獲授權下修改數據，以導致損害）的控罪的交替裁決。”

4.26 根據第 477.2(4)及 477.3(3)條，第 477.2(1)及 477.3(1)條所訂罪行（分別適用於修改數據和損害通訊）互為法定交替罪行。由於這兩項罪行均最高可處十年監禁，被告人能夠指稱因作出交替裁決而可能造成不公的機會不大。然而，我們並不清楚為何有關法例就違反第 477.2(1)條的非法干擾（即使沒有導致實際損害）和違反第 477.3(1)條的非法干擾，訂定相同的法定最高刑罰。第 477.2(1)條所訂的罪責，是歸因於罔顧在未獲授權下修改數據是否可能導致實際損害，而

第 477.3(1)條則規定電子通訊須受損害，但沒有明確提到犯罪者“意圖導致該項損害”。[20]

《刑事法典》（聯邦）第 478.1 條

4.27 第 478.1 條（*“在未獲授權下取覽或修改受限數據”*）及第 478.2 條（*“在未獲授權下損害存於電腦紀錄碟等內的數據”*）可視為另一組分別處理修改和損害的條文。雖然這些條文所訂立的罪行並非法定交替罪行，但兩者的最高刑罰相同，均最高可處兩年監禁。

4.28 第 478.1 條規定如下：

> “(1) 任何人在以下情況，即屬犯罪：
>
> (a) 該人導致在未獲授權下取覽或修改受限數據；及
>
> (b) 該人意圖導致該項取覽或修改；及
>
> (c) 該人知悉該項取覽或修改未獲授權。
>
> 刑罰：監禁 2 年。
>
> (3) 在本條中：
>
> ***受限數據***指符合以下說明的數據：
>
> (a) 存於某電腦內；及
>
> (b) 其取覽受與該電腦任何功能相關的存取控制系統所限。”

4.29 第 477.2 及 478.1 條所訂罪行均適用於在未獲授權下修改數據。兩者的共通點是就犯罪意念而言，犯罪者須知悉有關修改未獲授權。然而：

---

[20] 《2001 年電腦網絡罪行法案》（Cybercrime Bill 2001）在《刑事法典》加入第 477.2 及 477.3 條，該法案的摘要說明解釋了這兩項條文把最高刑罰訂為監禁十年的背景。第 477.2 條的刑罰相等於《刑事罪行法令》（Crimes Act）當時所訂電腦罪行的刑罰，以及《刑事法典》所訂欺詐罪及偽造罪的刑罰。至於第 477.3 條的刑罰，則 *“確認了利用電腦進行可靠通訊的重要性，以及如該等通訊受到損害，即可造成相當大的損壞”*。然而，並無其他二手資料解釋為何第 477.2 及 477.3 條的犯罪行為不同，最高刑罰卻相同。

(a) 犯罪者只要罔顧後果，便足以符合第 477.2(1)(c)條的規定，但要符合第 478.1(1)(b)條的規定，犯罪者須意圖導致有關修改。

(b) 此外，第 477.2(1)(a)條並沒有如第 478.1(1)(a)條那樣，規定有關數據須屬“受限數據”。

第 477.2 條所訂罪行的最高刑罰較重，顯示第 477.2 條的罪行理應較第 478.1 條嚴重，但上述兩點看來與此不符。

《刑事法典》（聯邦）第 478.2 條

4.30 正如上文所述，第 478.1 及 478.2 條所訂罪行的最高刑罰相同，均最高可處兩年監禁。後述條文的內容如下：

“任何人在以下情況，即屬犯罪：

(a) 該人導致在未獲授權下損害存於以下事物內的數據的可靠性、保安或操作：

(i) 電腦紀錄碟；或

(ii) 信用卡；或

(iii) 其他用作以電子方式儲存數據的器材；及

(b) 該人意圖導致該項損害；及

(c) 該人知悉該項損害未獲授權。

刑罰：監禁 2 年。”

4.31 第 477.3 及 478.2 條所訂罪行分別適用於在未獲授權下損害電子通訊，以及在未獲授權下損害數據的可靠性、保安或操作。這兩項罪行的共通元素，是犯罪者知悉有關損害未獲授權。

4.32 儘管如此，第 477.3 條並沒有如第 478.2(b)條那樣，提述犯罪者意圖導致有關損害，這似乎有違常理，因為前者大概是為了訂立較嚴重的罪行，才訂明較重的最高刑罰。

加拿大

《1985 年刑事法典》第 430(1.1)條

4.33 與澳大利亞法例相比，加拿大法例較為精簡。相關條文是《1985 年刑事法典》（Criminal Code 1985）第 430(1.1)條（*"與電腦數據有關的損害"*）：

> "任何人如故意
>
> (a) 銷毀或更改電腦數據；
>
> (b) 使電腦數據變得無意義、無用或無效；
>
> (c) 妨礙、中斷或干擾合法使用電腦數據；或
>
> (d) 妨礙、中斷或干擾正在合法使用電腦數據的人，或拒絕讓有權取覽電腦數據的人取覽電腦數據，
>
> 即屬導致損害。"

與《示範法》的相似之處

4.34 《1985 年刑事法典》第 430(1.1)條就犯罪行為訂定的條文，措辭幾乎與《示範法》第 6 條（*"干擾數據"*）的下述條文相同：

> "(1) 任何人無合法辯解或理由而蓄意或罔顧後果地作出任何以下作為：
>
> (a) 銷毀或更改數據；
>
> (b) 使數據變得無意義、無用或無效；
>
> (c) 妨礙、中斷或干擾合法使用數據；或
>
> (d) 妨礙、中斷或干擾正在合法使用數據的人；或
>
> (e) 拒絕讓有權取覽數據的人取覽數據，
>
> 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。
>
> (2) 不論上述人士的作為所造成的影響屬暫時性或永久性，第(1)款亦適用。"

第 430(1.1)條所指的損害

4.35 《1985 年刑事法典》第 430(1.1)條就“損害”所訂的某些特點值得留意：

(a) 就犯罪行為而言，第 430(1.1)條針對的是受禁後果，而沒有把任何特定行為定為不合法，該條亦無提述獲得授權或未獲授權的概念。該條看來適用於故意藉不作為（即不作出某行為）而導致受禁後果的被告人。[21] 另外，該條的法律措辭似乎足以涵蓋以物理手段損壞電腦數據的情況（例如把強力磁鐵放在舊式軟磁碟附近）。

(b) 就犯罪意念而言，被告人須故意導致有關損害。根據第 429(1)條：

> “就本部而言，如任何人藉作出某作為或不作出該人有責任作出的作為而導致某事件發生，而該人知悉該作為或不作為頗有可能會導致該事件發生，並罔顧該事件是否發生，則該人須視為故意導致該事件發生。”

導致損害的刑事後果

4.36 《1985 年刑事法典》第 430 條訂明在不同情況下導致“損害”的刑事後果。根據第 430(5)條：

“任何人導致與電腦數據有關的損害，即屬

(a) 犯可公訴罪行，可處為期不超過 10 年的監禁；或

(b) 犯可循簡易程序定罪而懲處的罪行。”

4.37 此外，某些其他款亦可能適用於與電腦數據有關的損害。舉例來說，第 430(2)條有以下規定：

> “任何人如導致損害以致生命受到實際危害，即屬犯可公訴罪行，可處終身監禁”。

---

21 《1985 年刑事法典》第 430(5.1)條提供支持這項解釋的依據。根據該條：
“任何人故意作出某作為或故意不作出該人有責任作出的作為，而如該作為或不作為相當可能構成損害導致生命受到實際危害，或構成與財產或電腦數據有關的損害……”
即屬犯罪。

英格蘭及威爾斯

《英格蘭誤用電腦法令》第 3 條

4.38 《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"*）及第 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"*）顯示兩層式的做法。我們會先研究第 3 條：

"(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；及

(c) 下文第(2)款或第(3)款適用。

(2) 如上述人士意圖藉作出有關作為而——

(a) 損害任何電腦的操作；

(b) 阻止或阻礙取覽存於任何電腦內的任何程式或數據；或

(c) 損害上述程式的操作或上述數據的可靠性；或

(d) 致使上述(a)至(c)段提述的任何事宜得以作出，

則本款適用。

(3) 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。

(4) 上文第(2)款所提述的意圖，或上文第(3)款所提述的罔顧後果，不一定要涉及——

(a) 任何特定電腦；

(b) 任何特定程式或數據；或

(c) 任何特定種類的程式或數據。

(5) 在本條中——

(a) 凡提述作出某作為，即包括提述導致作出某作為；

(b) '作為'包括一連串作為；

(c) 凡提述損害、阻止或阻礙某些事宜，即包括提述暫時如此行事。

(6) 任何人犯本條所訂罪行——

(a) 一經在英格蘭及威爾斯循簡易程序定罪，可處為期不超過 12 個月的監禁或不超過法定最高罰款，或兩者兼處；

(b) 〔……〕

(c) 一經循公訴程序定罪，可處為期不超過 10 年的監禁或罰款，或兩者兼處。"

展示成功執法的案例

4.39 *R v Victor Lindesay*[22] 是根據《英格蘭誤用電腦法令》第 3 條成功執法的例子。該案的案情與 *HKSAR v Chan Chi Kong* 相似。[23] 林德賽（Lindesay）先生承認三項導致在未獲授權下修改電腦內容的控罪。雖然所造成的損壞並非永久，但他被判處監禁九個月。

4.40 英格蘭上訴法院維持判刑，並指出：

> "……不管上訴人的不滿是多麼實在，不管上訴人是多麼出於一時衝動而作出報復，也不管上訴人須對這些作為負責是多麼難免會被揭發，事實畢竟是上訴人利用自己的技術及對前僱主業務的認識，給完全無辜的機構帶來大量工作、不便及憂慮。依本院判斷，判處即時執行的監禁刑罰以反映上訴人破壞誠信，實屬恰當。"[24]

---

22 [2001] EWCA Crim 1720; [2002] 1 Cr App R (S) 86.

23 第 4.9 段。

24 見上文註腳 22，第 373 頁（第 15 段）。

《英格蘭誤用電腦法令》第 3ZA 條

4.41　任何人違反第 3 條，可處為期不超過十年的監禁或罰款，或兩者兼處。第 3ZA 條所訂的最高刑罰嚴重得多，該條內容如下：

"(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——

(a) 對任何地方的人類福祉的損害；

(b) 對任何地方的環境的損害；

(c) 對任何國家的經濟的損害；或

(d) 對任何國家的國家安全的損害，

即屬'關鍵性'損害。

(3) 就第(2)(a)款而言，某作為只有導致以下情況，方屬導致對人類福祉的損害——

(a) 人命損失；

(b) 人類患病或受傷；

(c) 貨幣、食物、水、能源或燃料的供應受到干擾；

(d) 通訊系統受到干擾；

(e) 交通設施受到干擾；或

(f) 關乎衞生的服務受到干擾。

(4) 就第(2)款而言，某導致損害的作為是否——

(a) 直接導致該損害；

(b) 該損害的唯一或主要成因，

均屬無關重要。

(5) 在本條中——

(a) 凡提述作出某作為，即包括提述導致作出某作為；

(b) '作為'包括一連串作為；

(c) 凡提述某國家，即包括提述某地區，以及提述某國家或地區的任何地方、部分或區域。

(6) 除非第(7)款適用，否則任何人犯本條所訂罪行，一經循公訴程序定罪，可處為期不超過 14 年的監禁或罰款，或兩者兼處。

(7) 如任何人——

(a) 因導致第(3)(a)或(3)(b)款所述種類的人類福祉嚴重損害的作為而干犯本條所訂罪行，或因產生導致該損害的重大風險的作為而干犯該罪行；或

(b) 因導致國家安全嚴重損害的作為而干犯本條所訂罪行，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。"

第 3 及 3ZA 條的犯罪行為

4.42 這兩項條文的犯罪行為均包括 *"就某電腦作出任何未獲授權的作為"*。就第 3ZA 條而言，該作為還須導致 *"關鍵性嚴重損害"*，或產生導致 *"關鍵性嚴重損害"* 的重大風險。

4.43 "作為"一詞示明任何人不會因着不作為而干犯上述任何條文所訂罪行。另外，按照這兩項條文的草擬方式，似乎無須證明實際損害，方能定罪。

4.44 此外，似乎物理作為亦可構成這兩項條文的犯罪行為。在這方面，我們在上文討論加拿大法律時曾舉出把強力磁鐵放在舊式軟磁碟附近的例子。[25] *R v Nicholas Alan Whiteley*[26] 指出，在《英格蘭誤用電腦法令》實施前，這樣做可能構成《1971 年刑事損壞法令》(Criminal Damage Act 1971）第 1(1)條（*"摧毀或損壞財產"*）所訂的罪行。[27] 該法令第 10(5)條現須加以考慮：

> "就本法令而言，修改電腦的內容不得視為損壞任何電腦或電腦儲存媒體，但如該項修改對該電腦或電腦儲存媒體的影響，是損害其物理狀況，則作別論。"

4.45 鑑於第 10(5)條，修改電腦的內容而沒有損害電腦的物理狀況，應根據《英格蘭誤用電腦法令》而非《1971 年刑事損壞法令》提出檢控。

第 3 及 3ZA 條的犯罪意念

4.46 至於犯罪意念方面，這兩項條文均規定被告人須知悉其作為未獲授權，並規定被告人須：

(a) 意圖導致（如屬第 3 條）指明類型的損害[28] 或（如屬第 3ZA 條）"關鍵性嚴重損害"；[29] 或

(b) 罔顧上述損害會否發生。

中國內地

《中國刑法》第二百八十六條第二款

4.47 根據《中國刑法》第二百八十六條第二款：

> "違反國家規定，對計算機信息系統中存儲、處理或者傳輸的數據和應用程序進行刪除、修改、增加的操作，後果嚴重的，依照前款的規定處罰。"
>
> （底線後加）

---

25 第 4.35(a)段。

26 (1991) 93 Cr App R 25.

27 *"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。"*

28 損害任何電腦的操作、阻止或阻礙取覽任何程式或數據、損害上述程式的操作，或損害上述數據的可靠性（第 3(2)條）。

29 第 3ZA(2)及(3)條。

展示成功執法的案例

4.48 在最高人民檢察院第九批指導性案例的第 34 號案例，[30] 被告人冒用其他互聯網使用者的身分登錄他們的購物網站帳戶，刪改這些互聯網使用者在某網購平台上給予一些網上賣家的劣評。被告人因為對計算機信息系統內的數據（即該網購平台上的劣評）進行修改，被裁定犯了第二百八十六條第二款所訂罪行。法院將該等差評數據視為該購物平台計算機信息系統的“重要組成部分”。

新西蘭

《新西蘭法令》第 250(2)條

4.49 新西蘭的法例方案與英格蘭及威爾斯的相類似，有關法例既訂有基本罪行，亦訂有加重形式，後者以被告人的作為所導致的更嚴重後果為基礎。

4.50 《新西蘭法令》第 250(2)條（*“損壞或干擾電腦系統”*）訂立以下基本罪行。就本章而言，第 250(2)條規定如下：

> “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。”

4.51 第 250(2)(c)條會在第 5 章探討。

刪除電腦數據或軟件

4.52 第 250(2)(a)及(b)條提述多種作為，其中包括刪除電腦數據或軟件。相關的問題是，這是否意味着要令有關數據或軟件不可復原（“擦除”），還是即使有關數據或軟件可輕易復原，仍會產生刑事法律責任？後述情況的例子如下：

---

30 李駿傑等破壞計算機信息系統案。

(a) 如某人正使用文字處理器編輯文件，而另一人在未獲授權下刪除當中某些內容，“復原”功能可能有助復原被刪除的內容。

(b) 在某人刪除電腦內的檔案後，或可在“資源回收筒”、“垃圾桶”或同等位置找到有關檔案，再把它復原。

(c) 如相關儲存媒體存有備份或影像，便能夠還原被刪除的檔案。[31]

4.53 某評論員注意到，*Police v Robb*[32] 一案強調了擦除和可復原的刪除之間的分別。正如基督城（Christchurch）地區法院所指，有關電腦檔案看來：

> “……只是被刪除，而不是被擦除。擦除涉及在刪除前先將檔案的數據蓋寫。人們普遍認為被擦除的檔案無跡可尋，亦無法復原。”[33]

4.54 上述評論員將該法院的裁定概述如下：

> “根據法官的說法，刪除本身並不構成損壞或干擾電腦系統而違反〔《1961 年刑事罪行法令》（Crimes Act 1961）〕第 250 條。另外，要證明損壞或干擾電腦系統的刑事罪行，便須豁除數據是在無意或意外的情況下刪除。法官指出，擦除檔案要求在單純刪除之外再另作有意的決定，但檔案是否被故意刪除，並不能用法證方法斷定。”[34]

4.55 對於該法院裁定須證明 *“故意採取步驟確保有關數據無法復原，即擦除數據”*，[35] 該評論員有以下批評：

> “國會在〔《1961 年刑事罪行法令》第 250(2)條中〕使用‘刪除’一詞的用意，不可能是表示該檔案的全部或部分須完全無法復原……國會的用意……不可能是電腦的正常操作可包括在他人蓄意進行旨在妨礙某機器或

---

31 一如 *HKSAR v Chan Chi Kong* 的情況（引用於第 4.9 段）。

32 [2006] DCR 388（該書面決定似乎沒有網上版）。

33 同上，第 27 段，引述於：
David Harvey, *internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015)，第 7.92 段。

34 David Harvey, *internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015)，第 7.93 段。

35 *Police v Robb*，第 40 段，引述於 David Harvey, *internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015)，第 7.93 段。

系統妥善操作的活動後採取介入補救步驟，使該機器或系統可以操作。”[36]

4.56 除非根據上述評論員的論點而採取較寬鬆的解釋，否則按照 *Police v Robb*[37] 所裁定對第 250(2)條的解釋，假如 *HKSAR v Chan Chi Kong*[38]（該案中被刪除的檔案最終還原，不過是在即時啟動緊急應變程序之後）在新西蘭發生，該條相當可能會不適用於該案的案情。

第 250(2)條的犯罪意念

4.57 第 250(2)條以“蓄意或罔顧後果地”行事，形容進行犯罪行為的犯罪意念，而有關未獲授權的犯罪意念，則是知悉或罔顧後果。有兩點觀察可以提出：

(a) 該法例雖然可提述被告人是“故意或罔顧後果地”進行犯罪行為，但卻選用了“蓄意或罔顧後果地”。有學者認為，就新西蘭的刑事法律而言，*“顯然‘故意’可用作‘意圖’的同義詞”*。[39] 與此比較，根據美國法學會（American Law Institute）的《模範刑法典》（Model Penal Code）：[40]

> “除第 2.05 條另有規定外，任何人除非就某罪行的每項關鍵元素特意、[41] 故意、[42] 罔顧後果地[43] 或疏忽[44] 行事（視乎法律規定），否則該人不屬犯罪。”[45]

---

36 見上文註腳 34，第 7.94 段。

37 [2006] DCR 388.

38 第 4.9 段。

39 Kris Gledhill, “The Meaning of Knowledge as a Criminal Fault Element: Is to Know to Believe?” (2019) 45(2) University of Western Australia Law Review 216，第 228 頁。

40 《模範刑法典》並非法律，但正如美國法學會所指，該法典 *“對於美國實體刑事法律的廣泛修訂和編纂，發揮了重要作用”*。見美國法學會，《模範刑法典》，登載於 https://www.ali.org/publications/show/model-penal-code/（於 2022 年 5 月 3 日瀏覽）。

41 *“任何人在以下情況，即屬就某罪行的關鍵元素特意地行事：*
(i) 如該元素涉及該人的行為的性質或後果，該人有意識地以進行屬該性質的行為或導致該後果為目的；及
(ii) 如該元素涉及伴隨情況，該人察覺到該等情況存在，或相信或希望該等情況存在。”（第 2.02(2)(a)條）

42 *“任何人在以下情況，即屬就某罪行的關鍵元素故意地行事：*
(i) 如該元素涉及該人的行為的性質或伴隨情況，該人察覺到其行為屬該性質，或察覺到該等情況存在；及
(ii) 如該元素涉及該人的行為的後果，該人察覺到其行為實際上肯定會導致該後果。”（第 2.02(2)(b)條）

43 *“凡任何人有意識地不理會某罪行的關鍵元素存在的重大不合理風險，或有意識地不理會其行為會導致該關鍵元素的重大不合理風險，即屬就該關鍵元素罔顧後果地行事。該風險須具有以下性質及程度：在顧及行事者行為的性質及目的，以及該人所知的情況後，該人*

因此根據該法典，“特意”（界定為性質與“蓄意”相類似）與“故意”屬不同概念。

(b) 相比之下，罔顧後果的涵義更為清晰。新西蘭最高法院在 *Cameron v R*[46] 中裁定：

> “在……的案件中，如並非以規定至少實際知悉或懷有意圖的字眼來界定所涉罪行，我們認為〔 *R v G*[47] 〕所闡釋的罔顧後果，將（至少通常甚或定當）足以符合情況及後果這兩方面的犯罪意念規定。就上述目的而言，如有以下情況，即構成罔顧後果：
>
> (a) 被告人意識到：
>
> i. 其行動確實可能會引致受禁後果；及／或
>
> ii. 受禁情況確實可能存在；及
>
> (b) 考慮到該風險後，該等行動屬不合理。”[48]

《新西蘭法令》第 250(1)條

4.58 至於加重罪行方面，根據《新西蘭法令》第 250(1)條：

> “任何人蓄意或罔顧後果地摧毀、損壞或更改任何電腦系統，並知悉或理應知悉相當可能會導致生命受危害，可處為期不超過 10 年的監禁。”

4.59 表面上，該條文只涵蓋摧毀、損壞或更改電腦系統，但不涵蓋電腦數據。然而，在一些被告人的作為“相當可能會導致生命受危

不理會該風險涉及嚴重偏離守法的人如處於行事者的情況便會遵守的行為標準。”（第 2.02(2)(c)條）

44 *“凡任何人應察覺到有某罪行的關鍵元素存在的重大不合理風險，或察覺到其行為會導致該關鍵元素的重大不合理風險，即屬就該關鍵元素疏忽地行事。該風險須具有以下性質及程度：在顧及行事者行為的性質及目的，以及該人所知的情況後，該人沒有意識到該風險涉及嚴重偏離合理的人如處於行事者的情況便會採取的謹慎標準。”*（第 2.02(2)(d)條）

45 第 2.02(1)條。

46 [2017] NZSC 89.

47 [2003] UKHL 50; [2004] 1 AC 1034.

48 *Cameron v R*，第 73 段，引用於 Nick Chisnall, “Case Note: *Cameron v R* [2017] NZSC 89 – Controlled Drug Analogues, Indeterminacy and *Mens Rea* under the Misuse of Drugs Act 1975” [2017] NZCLR 256，第 262 頁。

害”的案件中，可以想像到該人除摧毀、損壞或更改了整體電腦系統之外，應該亦銷毀、損壞或更改了電腦數據。事實上，該條文可說是與第 4 章及第 5 章同時相關。

4.60 另一方面，獲得授權這概念顯然與第 250(1)條無關，這與第 250(2)條有所不同。鑑於前者涉及生命受危害，這點可以理解。

《新西蘭法令》第 258(1)條

4.61 第 250(1)條所訂罪行的最高刑罰（監禁十年）與第 258(1) 條（*“意圖欺騙而更改、隱藏、銷毀或複製文件”*）所訂的相同。第 258(1)條載列如下：

> “任何人——
>
> (a) 更改、隱藏或銷毀任何文件，或導致任何文件被更改、隱藏或銷毀；或
>
> (b) 製造文件或導致文件被製造，而該文件的全部或部分屬任何其他文件的複製文本，
>
> 並意圖以欺騙手段取得任何財產、特權、服務、金錢利益、得益或有值代價，或意圖導致任何其他人蒙受損失，可處為期不超過 10 年的監禁。”[49]

4.62 法院在 *R v Johannes Hendrik Middeldorp*[50] 中裁定，在上文引述的第 258(1)(b)條中，“文件”一詞包括儲存於電腦硬碟的電腦檔案（代表掃描影像），以及已發送或接收的電郵的附件（代表影像）。按邏輯推斷，第 258(1)(a)條中“文件”一詞亦應同樣詮釋。基於這一點，凡電腦數據被更改、隱藏或銷毀，有關條文亦會適用。

4.63 如將第 250(1)條針對電腦的罪行與第 258(1)條適用於一般情況的罪行加以比較，便可見以下潛在的重大差異：罔顧後果足以構成前述條文的犯罪意念，但不足以構成後者的犯罪意念。

---

49 第 258(2)條闡述如下：
“在有第(1)款所提述的意圖而作出有關更改或製造有關文件後，違反該款的罪行即告完成，即使犯罪者未必有以下意圖亦然——
(a) 某特定的人應使用被更改或製造的文件，或應按照該文件行事；或
(b) 某特定的人應基於被隱藏或銷毀的文件並不存在而行事；或
(c) 某特定的人應被誘使作出或不作出任何行為。”

50 [2015] NZHC 951.

新加坡

《新加坡誤用電腦法令》第 5 條

4.64 《新加坡誤用電腦法令》第 5 條(*"在未獲授權下修改電腦資料"*)與本章相關:

> "(1) 除第(2)款另有規定外,任何人知悉任何作為會導致在未獲授權下修改任何電腦的內容,並作出該作為,即屬犯罪,一經定罪——
>
> (a) 可處不超過$10,000 的罰款或為期不超過 3 年的監禁,或兩者兼處;及
>
> (b) 如屬第二次或其後每次定罪,則可處不超過$20,000 的罰款或為期不超過 5 年的監禁,或兩者兼處。
>
> (2) 如因本條所訂罪行而導致任何損壞,被裁定犯該罪行的人可處不超過$50,000 的罰款或為期不超過 7 年的監禁,或兩者兼處。
>
> (3) 就本條而言,如有關作為並非針對——
>
> (a) 任何特定程式或數據;
>
> (b) 任何種類的程式或數據;或
>
> (c) 存於任何特定電腦內的程式或數據,
>
> 均屬無關重要。
>
> (4) 就本條而言,未獲授權的修改是否屬永久性或僅屬暫時性,或是否擬屬永久性或擬僅屬暫時性,均屬無關重要。"

未獲授權的修改

4.65 至於犯罪行為方面,該法令第 2(7)及(8)條闡釋未獲授權的修改這個主要概念:

> "(7) 就本法令而言,如藉着操作有關電腦或任何其他電腦的任何功能——

(a) 存於有關電腦內的任何程式或數據遭更改或刪抹；

(b) 在該電腦所收納的內容上任何程式或數據有所增加；或

(c) 發生任何會損害任何電腦的正常操作的作為，

即屬出現修改任何電腦的內容，而造成導致上述修改的任何作為，須視為導致該項修改的作為。

(8) 凡有人因其作為而導致第(7)款所提述的修改，而該人——

(a) 本身無權決定應否作出該項修改；及

(b) 未獲有此權利的人同意該項修改，

該項修改即屬未獲授權。”

犯罪意念

4.66 該法令訂明的犯罪意念，是知悉犯罪者的作為會導致未獲授權的修改。因此，單是罔顧後果，並不足以招致刑事法律責任。

如涉及“受保護電腦”可加重懲罰

4.67 上文所詳細論述的司法管轄區均訂有基本罪行，並訂有以更嚴重後果（例如犯罪者意圖或導致生命受危害）為基礎的加重罪行。

4.68 《新加坡誤用電腦法令》則採用另一做法。除了第 5(1)條（該條訂明適用於再犯者的最高刑罰較重）及第 5(2)條（根據該條可對導致“任何損壞”的犯罪者判處更重的最高刑罰）之外，第 11(1)條還把最重的最高刑罰預留給涉及取用“受保護電腦”的案件：

“(1) 如有人在干犯第 3、5、6 或 7 條所訂罪行的過程中取用任何受保護電腦，被裁定干犯該罪行的人可處不超過$100,000 的罰款或為期不超過 20 年的監禁，或兩者兼處，以代替該等條文所訂明的刑罰。

(2) 就第(1)款而言，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或程式或數據是在與下述各項有直接關連的情況

下使用的，或對下述各項屬必要的——

(a) 新加坡的安全、防務或國際關係；

(b) 與執行刑事法律有關的機密資料來源的存在或身分；

(c) 提供與通訊基礎建設、銀行及金融服務、公共事業、公共交通或公開密碼匙基礎建設直接有關的服務；或

(d) 保障公眾安全，包括與必要緊急服務（例如警務、民防及醫療服務）有關的系統。

(3) 為根據本條提出的檢控的目的，已就有關電腦、程式或數據而言，如被告人獲展示電子警告或其他警告，而該警告述明在未獲授權下取用該電腦或取覽該程式或數據，可根據本條處以較重刑罰，則須推定被告人知悉第(2)款提述的所需事實，直至相反證明成立。”

4.69 《新加坡誤用電腦法令》述明在制訂加重罪行時，涉及某類數據或電腦系統可作為加重刑罰的因素。

美國

《電腦欺詐及濫用法案》內的《美國法典》第 18 篇第 1030(a)(5)條

4.70 正如第 1 章[51] 及第 2 章[52] 所指，《電腦欺詐及濫用法案》（Computer Fraud and Abuse Act，《美國法典》第 18 篇第 1030 條）是美國應對電腦網絡罪行的主要聯邦法例。任何人如作出與第 1030(a)條所述各種情境有關的作為，可按第 1030(c)條的規定予以懲處。

4.71 《美國法典》第 18 篇第 1030(a)(5)條訂立與本章相關的罪行，該條分為三個部分：

“(A) 故意導致向某受保護電腦傳送程式、資料、代碼或指令，並因着該行為而在未獲授權下蓄意導致該電

---

51 第 1.10(b)段。

52 第 2.81 段。

腦損壞；

(B) 在未獲授權下蓄意取用某受保護電腦，並因着該行為而罔顧後果地導致損壞；或

(C) 在未獲授權下蓄意取用某受保護電腦，並因着該行為而導致損壞及損失。”

對受保護電腦所導致的損壞

4.72 以上三個部分均關乎對“受保護電腦”所導致的“損壞”。《美國法典》第 18 篇第 1030(e)(8)條把“損壞”界定為*“對數據、程式、系統或資料的完整性或可用性造成任何損害”*。

4.73 在這寬廣的定義下，某人如作出某些行為（例如蓄意地散播電腦病毒，或安裝類似計時炸彈的軟件），儘管這些行為不會即時導致損壞，它們已等同實際干擾電腦數據，帶來在較後時間發生損壞的風險，有關罪行似乎也適用於該人。雖然上述干擾可能仍未發生，但該人的作為已損害數據的完整性。“損壞”的定義，亦會涵蓋在未獲授權下將數據加密而損害數據可用性的情況。

4.74 《美國法典》第 18 篇第 1030(e)(2)條把“受保護電腦”界定為：

“(A) 某財務機構或美國政府專用的電腦，或如屬並非如此專用的電腦，則指由某財務機構或美國政府所使用或為其而使用的電腦，而構成有關罪行的行為會影響由該財務機構或美國政府對該電腦的使用或為其而對該電腦的使用；

(B) 用於或影響州際或對外貿易或通訊的電腦，包括位於美國境外而以影響美國州際或對外貿易或通訊的方式使用的電腦；或

(C) 符合以下說明的電腦——

(i) 屬投票系統的一部分；及

(ii) (I) 用作聯邦選舉的管理、支援或行政；或

(II) 曾在州際或對外貿易中運作或在其他方面影響州際或對外貿易”。

未獲授權

4.75 《美國法典》第 18 篇第 1030(a)(5)條中三個部分均訂有*"未獲授權"*的規定，但所聯繫的元素並不相同，其中(A)部分是導致損壞，而(B)及(C)部分則是取用受保護電腦。因此，就(A)部分而言，*"即使有關傳送已獲授權，如所導致的損壞未獲授權，被告人仍可能須負上法律責任"*。[53]

4.76 《美國法典》第 18 篇第 1030(a)(5)條的三個部分都沒有提述被告人在超逾授權範圍下行事的情境，而《美國法典》第 18 篇第 1030(a)(1)、(a)(2)及(a)(4)條卻明確考慮到該情境。[54]

4.77 由於這個分別，聯邦上訴法院第五巡迴法庭（Fifth Circuit Court of Appeals）在 *US v Phillips*[55] 中得出以下結論：《美國法典》第 18 篇第 1030(a)(5)條*"只適用於對〔相關電腦〕完全沒有取用授權的使用者"*。該法庭引用述明《美國法典》第 18 篇第 1030(a)(5)條會*"針對'外界人士'"*的國會紀錄，並指出：

> "國會藉使入侵行為的性質局部取決於電腦使用者所具備的授權級別，從而區分'獲授權取用電腦的內部人員'與'入侵電腦的外界黑客'。"[56]

(A)部分的傳送

4.78 (A)部分的"傳送"一詞已有司法解釋。看來：

(a) 該詞涵蓋*"通過電訊線路或藉着直接輸入"*而感染電腦的情況；[57] 及

(b) *"只要導致所需的損壞，即便是打字和蓋寫數據的作為，該條文也可涵蓋"*。[58]

---

53 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 117 頁，引用 *Lockheed Martin Corp v Speed*, 2006 US Dist LEXIS 53108 (MD Fla 2006)，第 21 頁。

54 第 2.83 至 2.88 段探討在未獲授權下行事的人與在超逾授權範圍下行事的人有何分別。

55 477 F 3d 215 (5th Cir 2007).

56 同上，第 219 頁。

57 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 121 頁，引用 *Lloyd v US*, 2005 US Dist LEXIS 18158 (D NJ 2005)。

58 同上，第 122 頁，引用 *International Airport Centers LLC v Citrin*, 440 F 3d 418 (7th Cir 2006)。

(C)部分的損失

4.79 (C)部分規定，被告人的作為須導致“損壞及損失”。根據《美國法典》第 18 篇第 1030(e)(11)條：

> “‘損失’一詞指任何受害人的合理費用，包括對某罪行作出回應的費用、進行損壞評估的費用，以及將有關數據、程式、系統或資料還原至該罪行發生前狀態的費用，還包括因服務受阻而損失的收入、招致的費用或引致的其他相應損害賠償”。

犯罪意念

4.80 《美國法典》第 18 篇第 1030(a)(5)條的三個部分的犯罪意念，可概述並對照如下：

(a) 根據(A)部分，被告人須故意導致傳送程式等，並蓄意導致損壞。

(b) (B)部分規定，取用受保護電腦須是蓄意的，並規定被告人須罔顧後果地導致損壞。

(c) (C)部分亦規定，取用受保護電腦須是蓄意的，但並無就導致損壞及損失訂明任何意念元素。

小組委員會的看法

禁止在未獲授權下蓄意干擾數據

4.81 在討論開首，我們便意會到更改電腦數據實屬常見。每逢有人操作電腦（例如啟動或登入電腦）或電腦與互聯網有互動，數據便難免會被更改。常見的更改數據例子如下：

(a) 社交媒體平台會在使用者張貼照片或網頁連結時，檢查該使用者提供的數據。該平台可能會修改或移除部分數據（例如照片的元數據）。

(b) 電郵伺服器會掃描電郵的附件，如發現附件具危險性，便會將之移除。

(c) 網站可能會在訪客的電腦內儲存“小型文字檔案（cookies）”，[59] 藉以更改該電腦的數據或在該電腦上增加數據。

4.82 雖然數據會遭蓄意更改（因為這些更改是社交媒體平台、電郵伺服器或網站管理人有意導致的），但很多電腦使用者大概都會認為上述情境可以接受。

4.83 更改數據可能已獲適用的條款及條件授權，但亦有可能未獲明確授權。舉例而言，據我們了解，互聯網服務供應商在營運電郵服務或對其基礎設施進行升級時，如使用者數據的內容仍然完整無損，就不一定會把數據在形式上的改變通知使用者。

4.84 與此同時，如 *HKSAR v Chan Chi Kong*[60] 之類的案件顯示了干擾電腦數據可帶來的傷害。原則上，法律應禁止可能導致或已導致傷害的干擾。按照邏輯，這類干擾會屬未獲授權，亦可能是蓄意作出的。

4.85 接下來的問題是，法定的干擾數據罪應採用甚麼準則，令該罪行只針對涉及（潛在或實際）傷害的案件，而非針對獲普遍接受的情況（如上述社交媒體平台、電郵伺服器及網站的例子）。鑑於現行針對刑事損壞的法例，我們認為問題的癥結最終在於有關干擾是否有合理辯解支持。

4.86 因此，我們建議應將無合法權限或合理辯解而蓄意干擾（損壞、刪除、[61] 弄壞、更改或抑制）電腦數據定為罪行。議定這個大方向後，我們再以現行法律——具體而言為《刑事罪行條例》（第 200 章）與刑事損壞有關的第 59 至 64 條——為藍本，討論建議罪行的各個方面。

犯罪行為

4.87 就犯罪行為而言，我們認為，《刑事罪行條例》（第 200 章）第 59(1A)條所詳述的“誤用電腦”概念[62] 似乎大致上足以涵蓋與本章相關的想像情境。

---

59 *“網頁伺服器發送給瀏覽器的數據包，瀏覽器其後每次接達同一伺服器時會將該數據包發還，用作識別使用者或追蹤使用者接達伺服器的情況。”*見：Oxford University Press, “Lexico.com”（2021 年），網址為 https://www.lexico.com/definition/cookie（於 2022 年 5 月 3 日瀏覽）。

60 第 4.9 段。

61 即使可利用某些數據復原工具將數據復原。

62 第 4.7 段。

4.88 雖然第 59(1A)條並不包括加拿大《1985 年刑事法典》第 430(1.1)(b)條所示的一般條文，[63] 但看來沒有情境受該一般條文所涵蓋，卻未被納入上述香港條文的涵蓋範圍。該一般條文大概反映加拿大對損壞電腦本質上屬損壞電腦數據的看法。

犯罪意念

4.89 目前，“誤用電腦”屬刑事損壞的一種形式。這樣合乎情理，因為該項誤用情形與刑事損壞實體財產類同。為保持一致，這兩種刑事損壞的形式應採用相同的犯罪意念(即懷有意圖或罔顧後果)。

4.90 香港訂立刑事損壞罪的法例，主要是以英格蘭及威爾斯《1971 年刑事損壞法令》為藍本，而該法令則是根據法律委員會(Law Commission)的建議而制定的。[64] 正如法律委員會的報告書所解釋，[65] 前身法例《1861 年惡意損壞法令》(Malicious Damage Act 1861)所訂的大部分罪行，均規定被告人須“非法及惡意”行事。法律委員會不建議採用該等字眼；[66] 我們認為並無任何理由恢復舊例，規定須懷有惡意干犯建議的罪行。

合法辯解

4.91 法律委員會在同一份報告書中，將(當時建議的)刑事損壞罪背後的理念描述如下：

> “雖然被告人不必提出有合法辯解的爭論點，但只有在被告人確實提出該爭論點，或證據顯示可能有合法辯解時，有關問題方會出現。該罪行的定義所用措辭，旨在訂明如有關問題出現，控方有責任證明無合法辯解。”[67]

4.92 在香港，《刑事罪行條例》(第 200 章)第 64(2)條就兩項合法辯解訂定條文，並同時保留任何獲法律承認的其他合法辯解或免責辯護。

---

63 使電腦數據*“變得無意義、無用或無效”*(見第 4.33 段)。

64 法律委員會，*Criminal Law Report on Offences of Damage to Property*(1970 年)，法律委員會第 29 號，登載於 https://www.lawcom.gov.uk/project/criminal-law-report-on-offences-or-damage-to-property/(於 2022 年 5 月 3 日瀏覽)。

65 同上，第 16 頁(第 42 段)。

66 同上，第 17 頁(第 44 段)及第 18 頁(第 48 段)。

67 同上，第 18 頁(第 48 段)。

4.93　第一項合法辯解適用於以下情況：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，或會予以同意。後者指的是無須實際上獲得同意。被告人只要是誠實地相信有關事情，則即使沒有充分理由支持，也可以援引這項合法辯解，[68] 但在現實中，被告人相信的事情亦不應過於牽強。這項合法辯解看來足以涵蓋上述社交媒體平台、電郵伺服器及網站的情況。[69] 另一假設情境是，技術人員在未事先取得電腦擁有人的同意下，對電腦套用最新的保安修補程式。

4.94　第二項合法辯解則以需要保護財產、財產權利或財產權益為基礎。這似乎適用於以下例子：某人須移除電腦內的病毒，以保護該電腦的數據。

4.95　我們的結論是，維持上述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，實屬恰當。

加重罪行

4.96　我們在上文提到，在加拿大，與電腦數據有關的損害可處為期不超過十年的監禁，而任何人導致損害以致生命受到實際危害，則可處終身監禁。[70] 這些最高刑罰與香港適用於刑事損壞罪（包括“誤用電腦”）的最高刑罰相同。[71]

4.97　我們認為，加拿大及香港對涉及和不涉及生命受危害的案件加以區分，是有據可依的。一個涉及生命受危害的假設情境是，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。

4.98　我們認為保留《刑事罪行條例》（第 200 章）第 60(2)條所訂的加重罪行較為可取。

把有關罪行改列於新法例

4.99　總括而言，我們一致認為現有體制整體上令人滿意。鑑於我們建議制定一項針對電腦網絡罪行的特定法例，[72] 我們提議有關“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。

68　《刑事罪行條例》（第 200 章）第 64(3)條。
69　第 4.81 段。
70　第 4.36 至 4.37 段。
71　第 4.5 段。
72　第 2.90 段。

建議 6

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。

第 5 章　非法干擾電腦系統

引言

5.1　我們會在本章探討第四類依賴電腦網絡的罪行，即非法干擾電腦系統。概括而言，就此主題而訂立的罪行，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。

5.2　鑑於非法干擾電腦數據與非法干擾電腦系統息息相關，本章會在第 4 章討論的基礎上再作探討。以下學術評論，可謂貼切恰當：

> "雖然電腦系統的運作受阻通常是因為數據曾被修改，但即使數據未經修改，若對電腦的取用受阻或電腦的運作受限，上述情況也有可能發生；拒絕服務攻擊便是一例。"[1]

5.3　本章所探討的各種不當行為之中，最佳例子就是拒絕服務攻擊，這涉及*"中斷獲授權使用者取用某電腦網絡，通常是出於惡意而導致的"*。[2] 這類攻擊還有一種分散進行的加強模式，稱為分布式拒絕服務攻擊，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"*。[3]

5.4　分布式拒絕服務攻擊通常（但並不一定）藉"殭屍網絡（botnet）"發動。犯罪者可在網上散布惡意軟件（例如透過在網頁提供帶有病毒的超連結，讓不虞有詐的互聯網使用者點擊），令被入侵的電腦受暗中控制。每台被入侵的電腦稱為"殭屍電腦（bot）"（即機械人），因此，"殭屍網絡"一詞指一組被入侵的電腦，而殭屍電腦越多，則殭屍網絡越強大。舉例來說，犯罪者可遙距指示殭屍網絡內所有電腦同時重複向同一網頁發出請求。如寄存該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。有關電腦的擁有人很可能是無辜的，在出現這種情況時還蒙在鼓裡。

1　Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 113 頁。

2　Oxford University Press, "Lexico.com"（2021 年），網址為 https://www.lexico.com/definition/denial_of_service（於 2022 年 5 月 3 日瀏覽）。

3　同上。

5.5 若某電腦系統看來受到分布式拒絕服務攻擊，關鍵的事實爭論點，可能在於共同導致該結果的各方是否意圖攻擊該系統。舉例而言，透過電腦系統提供的緊急熱線服務可能會被大量來電佔線。究竟是很多人碰巧同時致電該熱線，還是有人控制成百上千台電腦一起致電該熱線，必須加以區分。後者與分布式拒絕服務攻擊較為類近。

5.6 除分布式拒絕服務攻擊外，還出現了一種干擾電腦系統的新方式，稱為慢速攻擊（slow attack）。分布式拒絕服務攻擊與餐廳有多名顧客同時點餐的情況相類似，而慢速攻擊則猶如餐廳某名顧客用多枚小額硬幣結帳，令餐廳的正常服務受到干擾。分布式拒絕服務攻擊會導致目標電腦系統產生大量日誌紀錄，而慢速攻擊則可能只令目標電腦系統長時間忙於處理有關請求。

香港的現行法律

《刑事罪行條例》（第 200 章）

第 60 條

5.7 正如第 4 章所述，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。”

從上文提述 *“(a)、(b)或(c)段”* 可見，這三段並非相連。第 4 章考慮過當中的(b)及(c)段，而(a)段則與本章最為相關。

涉及分布式拒絕服務攻擊的案例

5.8 案例已確立分布式拒絕服務攻擊可構成第 59(1A)條所界定的"誤用電腦"。在*香港特別行政區 訴 朱婷婷*這宗裁判法院上訴案件，[4] 高等法院原訟法庭法官黃崇厚裁定，原審裁判官的以下裁斷*"絕無問題"*：[5] 由於被告人在 49 分鐘之內由一個互聯網規約地址發出七千多次嘗試瀏覽網站<www.police.gov.hk>的分布式拒絕服務攻擊，該網站的伺服器已符合第 59(1A)(a)條中被刑事損壞的涵義。

5.9 被告人獲裁定上訴得直，主要理由是案中證據未能證明被告人是引發該次攻擊的人。因此，無須考慮犯罪意念的問題。儘管如此，黃崇厚法官在指出*"定罪基礎是上訴人罔顧後果"*，[6] 並提述罔顧後果的一般準則後[7]（該等準則由終審法院在*冼錦華 訴 香港特別行政區*〔*Sin Kam Wah v HKSAR*〕訂立），[8] 對於應如何處理犯罪意念的問題，提出以下看法：

> "以本案而言，如果事實裁定是上訴人〔即被告人〕是在相關情況下按了〔被告人進入國際黑客組織網頁後版面所示的按鈕而〕引致警方網站被損壞的人時，即使已確立了她知悉風險，顧及她所做的只是按了一個按鈕，那是版面所示的唯一的按鈕，不過那是什麼按鈕在證據上沒有細節，上訴人見到的版面有什麼也須細察。她的行為是否屬不合理，〔裁判法院〕是必須小心考慮而作出裁定的。"[9]

5.10 分布式拒絕服務攻擊能阻礙正常取用電腦或限制電腦的預定運作，但第 59(1A)(a)條所用的措辭則更為廣泛。在*香港特別行政區 訴 朱峻瑋*（*HKSAR v Chu Tsun Wai*，***"朱峻瑋案"***），[10] 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

---

4 [2017] 4 HKLRD 651, HCMA 33/2016（判決日期：2016 年 10 月 11 日）。

5 同上，第 656 頁（第 22 段）（*"這裁定絕無問題"*）。

6 同上，第 664 頁（第 79 段）。

7 同上，第 664 頁（第 81 及 82 段）。

8 任何人在以下情況，即屬罔顧後果地行事：
(1) (a) ……就某情況而言，該人察覺到有該情況存在或將會存在的風險；
(b) ……就某結果而言，該人察覺到有該後果將會產生的風險；而
(2) ……在該人所知的情況下，承擔該風險屬不合理
（*冼錦華 訴 香港特別行政區* (2005) 8 HKCFAR 192, FACC 14/2004〔判決日期：2005 年 5 月 26 日〕）。

9 見上文註腳 4，第 665 頁（第 91 段）。

10 (2019) 22 HKCFAR 30, [2019] HKCFA 3.

受影響，因此該次攻擊並不成功。終審法院對第 59(1A)(a)條的解釋及應用如下：

> "本席認為，電腦按所設定的運作方式運作，關鍵並不在於電腦如何運行（或未能運行），而是在於電腦擁有人擬用電腦去**辦**什麼**事情**。電腦如何運行視乎生產商如何製造電腦而定，但該法規的關鍵則是在於電腦擁有人設定電腦去辦什麼事情。有關的網站和伺服器旨在提供銀行服務，而非用以處理大量旨在對該銀行及其客戶帶來不便和為攻擊者引來公眾關注的請求。"[11]（強調之處乃原文所有）

5.11 終審法院又提到，進行分布式拒絕服務攻擊在某程度上與向收件人發送大量電郵相類似。[12] 後一情境見於 *Director of Public Prosecutions v Lennon*，[13] 案中英格蘭高等法院分庭（Divisional Court）指出，電腦擁有人就收取電郵所給予的一般同意：

> "……顯然並不涵蓋並非為與該擁有人通訊，而是為干擾該擁有人正常操作及使用其系統而發送的電郵。"[14]

5.12 終審法院的結論是，將*朱峻瑋*案所涉的分布式拒絕服務攻擊*"形容為誤用該銀行的電腦相當貼切"*，[15] 並應維持根據第 59(1A)(a)條對被告人所作的定罪。終審法院的判決理據顯示，若 *Director of Public Prosecutions v Lennon* 的案情在香港發生，第 59(1A)(a)條很可能同樣適用。

5.13 雖然*香港特別行政區 訴 朱婷婷*[16] 沒有引用第 59(1A)(c)條，但由於目標電腦系統會因應分布式拒絕服務攻擊而產生日誌紀錄，這類攻擊原則上也可能涉及該條。*朱峻瑋*案間接顯示，第 59(1A)(c)條可能與分布式拒絕服務攻擊相關。[17]

---

11 同上，第 36 頁（第 13 段）。終審法院的判決由非常任法官賀輔明勳爵（Lord Hoffmann）頒布，而其他所有法官均表示同意。

12 同上，第 37 頁（第 14 段）。

13 [2006] EWHC 1201 (Admin).

14 同上，第 9 段。

15 見上文註腳 10，第 37 頁（第 15 段）。

16 [2017] 4 HKLRD 651, HCMA 33/2016（判決日期：2016 年 10 月 11 日）。

17 見上文註腳 10，第 37 頁（第 18 段）。

《布達佩斯公約》訂定罪行的標準

5.14 根據《布達佩斯公約》第一節之下的第一篇第五條：[18]

> "各締約方均應採取必要的立法及其他措施，在其本土法律中將下列行為定為刑事罪行：在無權的情況下蓄意藉輸入、傳送、損壞、刪除、弄壞、更改或抑制電腦數據，從而嚴重阻礙電腦系統的運作。"

5.15 《說明報告》對第五條的評註如下：

> "65. 上述行為在〔歐洲委員會（Council of Europe）關於電腦相關罪行的〕第(89) 9號建議內稱為破壞電腦。本條旨在把蓄意藉使用或影響電腦數據，阻礙合法使用電腦系統（包括電訊設施）定為罪行。這裏受保護的法定權益，是電腦系統或電訊系統的操作人及使用者能夠讓系統正常運作的權益。有關文本以中立的方式擬定，確保各種功能均受保護。
>
> 66. '阻礙'一詞指干擾電腦系統正常運作的行動。該項阻礙須藉輸入、傳送、損壞、刪除、更改或抑制電腦數據而造成。
>
> 67. 該項阻礙還須是'嚴重'的，方可處以刑事制裁。各締約方應自行決定該項阻礙應符合甚麼準則，才可視為'嚴重'。舉例來說，任何締約方可規定該項阻礙須導致某最低限度的損壞，方可視為嚴重。草擬人員將以下阻礙視為'嚴重'：向某系統發送數據，而發送的形式、規模或頻密程度會對擁有人或操作人使用該系統或與其他系統通訊的能力，有重大的不利影響，例如藉着會產生'拒絕服務'攻擊的程式、會妨礙或大大減慢該系統的操作的惡意代碼（如病毒），或會向收件人發送大量電子郵件以阻斷該系統通訊功能的程式。
>
> 68. 該項阻礙須在'無權'的情況下造成。網絡設計中固有的常見活動或普遍的操作或商業慣例，均是在有權的情況下作出的。這些活動或慣例的例子包括：在擁有人或操作人的授權下測試或保護電腦系統的安全

---

[18] 有關《布達佩斯公約》的背景資料，見導言第 11 段，以及第 1 章第 1.6 至 1.10 段。

性，又或在系統操作人安裝會停用先前安裝的相類程式的新軟件時，重新設定電腦的作業系統。因此，這類行為即使造成嚴重阻礙，也不會被本條定為罪行。

69. 為商業或其他目的而發送非應邀的電郵，尤其是大量發送或頻密地發送這類訊息（‘濫發訊息’），可能會對收件人造成滋擾。草擬人員認為，只有在通訊受蓄意及嚴重阻礙的情況下，才應把這類行為定為罪行。然而，締約方可在本土法律中以另一方式處理上述阻礙，例如可將特定的干擾作為定為行政罪行，或訂明該等作為須受制裁。有關文本留待締約方在本土法律中決定，有關系統的運作應受到何種程度——局部或全面、暫時或永久——的阻礙，才能達到足以處以行政制裁或刑事制裁的傷害門檻。

70. 該罪行須是蓄意干犯的，即犯罪者須有造成嚴重阻礙的意圖。”[19]

其他司法管轄區的法定體制

澳大利亞

《刑事法典》（聯邦）第 477.3 條

5.16 第 1 章[20] 指出，《刑事法典》（聯邦）（Criminal Code (Cth)）中的電腦網絡罪行條文，乃源於 2001 年發表的《示範法典委員會報告書》。根據該報告書的建議，《示範刑事法典》（Model Criminal Code）第 4.2.6 條所訂罪行 *“針對的是拒絕服務攻擊”*，[21] 以及 *“發送大量電郵，令收件郵箱容量不勝負荷以致系統崩潰等手段”*。[22] 該報告書闡述如下：

“並不是凡通訊受損都會對數據造成損害……攻擊可透過各種不同形式進行：可向系統發送大量不需要的訊息，阻斷連接目標電腦的通訊鏈路，亦可誘使目標電腦產生足夠的訊息量來阻止進行通訊，還可更改位址，以及將訊息重新導向。以上述及類似方式損害通訊，統稱

19 《說明報告》第 65 至 70 段。
20 第 1.10(g)段。
21 《示範法典委員會報告書》第 91 頁。
22 同上，第 137 頁。

為‘拒絕服務攻擊’。雖然有些攻擊涉及損害數據，有些則不會。”[23]

5.17 《示範法典委員會報告書》所建議的相關罪行，後來制定為《刑事法典》(聯邦)第 477.3 條(*“在未獲授權下損害電子通訊”*)，第 4 章已介紹該條。[24] 根據第 477.3 條，任何人如導致 *“在未獲授權下損害往來某電腦的電子通訊”*，而該人知悉該項損害未獲授權，即屬犯罪。

5.18 正如第 4 章提到，[25]《刑事法典》(聯邦)第 476.1 條把 *“損害往來某電腦的電子通訊”* 界定為包括 *“阻止進行上述通訊”* 或 *“在該電腦所使用的電子聯網或網絡上損害上述通訊”*，但不包括 *“純粹截取上述通訊”*：

(a) 由於上述定義並非詳盡無遺，第 477.3 條不只適用於干擾系統的案件，亦適用於其他情況。《示範法典委員會報告書》支持此觀點，據該報告書所述，現已制定為第 477.3 條的建議罪行旨在有：

> “……極之廣泛的適用範圍，由涵蓋短暫及輕微的傷害，以至涵蓋造成嚴重經濟損失或導致業務活動、政府活動或社會活動受嚴重干擾的行為。行為只要損害單一無關重要訊息的通訊，即屬違反有關禁止規定……一旦接受應就蓄意損害電子資料施加刑事法律責任，那麼損害收取或傳送該等資料的能力的行為，便須同樣納入受禁範圍。”[26]

(b) 不過，第 476.1 條提述 *“阻止”* 或 *“損害”*[27] 通訊，可能意味着假如攻擊電腦系統失敗(像 *朱峻瑋案* 那樣)，便不會構成第 477.3 條所訂罪行。

5.19 《示範法典委員會報告書》所建議的罪行及制定為第 477.3 條的罪行，均規定被告人須知悉某項損害未獲授權。然而，前者還規定，被告人須意圖損害往來有關電腦的電子通訊或罔顧會否造成上述損害，第 477.3 條則沒有這項規定。

---

23 同上，第 171 頁。
24 第 4.25 至 4.26 段。
25 第 4.18 段。
26 《示範法典委員會報告書》第 171 頁。
27 第 3.32 段。

《刑事法典》（聯邦）第 477.1 條

5.20 第 477.1 條（*"在未獲授權下作出取覽、修改或損害，並意圖干犯嚴重罪行"*）已在第 2 章[28] 及第 4 章[29] 論述；該條亦與本章相關。

5.21 根據第 477.1(1)(a)(iii)條，任何人如導致 *"在未獲授權下損害往來某電腦的電子通訊"*，而該人知悉該項損害未獲授權，並意圖藉該項損害而干犯（或利便干犯）違反聯邦、各州或領地法律的 *"嚴重罪行"*，即屬犯罪。

5.22 第 477.1(1)(a)(iii)條可視為在第 477.3 條之上，引入意圖干犯或意圖利便干犯 *"嚴重罪行"* 的規定。因此，諸如分布式拒絕服務攻擊等不當行為，除可能構成第 477.3 條所訂罪行外，也可能構成第 477.1(1)(a)(iii)條所訂罪行。

5.23 *"嚴重罪行"* 是可處終身監禁或為期五年或以上監禁的罪行。[30] 任何人根據第 477.1(1)(a)(iii)條被定罪，可處不超過適用於嚴重罪行的刑罰。[31]

加拿大

分布式拒絕服務攻擊的判例

5.24 加拿大《1985 年刑事法典》（Criminal Code 1985）第 430(1.1)條（*"與電腦數據有關的損害"*）與《示範法》第 6 條（*"干擾數據"*）的相似之處，已在第 4 章指出。[32] 然而，該法典看來並沒有與《示範法》第 7 條（*"干擾電腦系統"*）相對應的條文。第 7 條載列如下：

> "(1) 任何人無合法辯解或理由而蓄意或罔顧後果地：
>
> (a) 阻礙或干擾某電腦系統的運作；或
>
> (b) 阻礙或干擾正在合法使用或操作某電腦系統的人；

---

28 第 2.21 段。
29 第 4.21 段。
30 《刑事法典》（聯邦）第 477.1(9)條。
31 同上，第 477.1(6)條。
32 第 4.34 段。

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。

在第(1)款中，就電腦系統而言，‘阻礙’包括但不限於：

(a) 截斷電腦系統的電力供應；

(b) 導致對電腦系統的電磁干擾；

(c) 以任何方式破壞電腦系統；及

(d) 輸入、刪除或更改電腦數據。”

5.25 加拿大皇家騎警（Royal Canadian Mounted Police）所處理的下述事件，說明了在加拿大可如何向須為分布式拒絕服務攻擊負責的人提出檢控：

> “2012 年，皇家騎警〔即加拿大皇家騎警〕對某分布式拒絕服務攻擊進行調查，該次攻擊源自下議院屬下辦事處，針對魁北克政府的門戶網站‘www.gouv.qc.ca’，導致該網站超過兩天無法被進入。在刑事調查期間，皇家騎警使用登錄名稱、建築物進出紀錄、監察影像及數碼證據（被檢取的電腦設備）來識別疑犯的身分，該疑犯是獲得‘www.gouv.qc.ca’的管理權限而上載惡意軟件的政府網絡管理員。2013 年，該疑犯就兩項在未獲授權下使用電腦控罪及一項損害控罪，被裁定罪名成立，判處軟禁。”[33]

《1985 年刑事法典》第 342.1(1)條

5.26 雖然關於上述分布式拒絕服務攻擊的法院文件似乎未能供公眾查閱，但“在未獲授權下使用電腦”的控罪頗有可能是根據第 2 章所提述的《1985 年刑事法典》第 342.1(1)條（*“在未獲授權下使用電腦”*）提出的：[34]

---

33 加拿大皇家騎警，*Cybercrime: an overview of incidents and issues in Canada*（2014 年），第 8 頁，登載於 http://www.rcmp-grc.gc.ca/en/cybercrime-an-overview-incidents-and-issues-canada（於 2022 年 5 月 3 日瀏覽）。

34 第 2.28 段。

"任何人意圖欺詐並在無表面權利的情況下作出以下作為，即屬犯可公訴罪行，可處為期不超過 10 年的監禁，或屬犯可循簡易程序定罪而懲處的罪行：

(a) 直接或間接取得任何電腦服務；

(b) 藉電磁、聲音、機械或其他器材直接或間接截取某電腦系統的任何功能，或導致藉電磁、聲音、機械或其他器材直接或間接截取某電腦系統的任何功能；

(c) 直接或間接使用某電腦系統，或導致直接或間接使用某電腦系統，意圖干犯(a)或(b)段所訂罪行，或就電腦數據或某電腦系統干犯第 430 條所訂罪行；或

(d) 使用、管有、非法傳送或准許他人取覽某電腦密碼，而該密碼會使某人能夠干犯(a)、(b)或(c)段所訂罪行。"

《1985 年刑事法典》第 430(1)條

5.27 在上述分布式拒絕服務攻擊中，《1985 年刑事法典》第 430(1)條（*"損害"*）可作為提出損害控罪的依據，該條的內容如下：

"任何人如故意

(a) 摧毀或損壞財產；

(b) 使財產變得危險、無用、無法操作或無效；

(c) 妨礙、中斷或干擾合法使用、享用或操作財產；或

(d) 妨礙、中斷或干擾正在合法使用、享用或操作財產的人，

即屬導致損害。"

5.28 第 430(1)條適用於與一般財產有關的損害，其措辭與第 4 章所介紹的第 430(1.1)條（*"與電腦數據有關的損害"*）相類似。[35] 由

---

[35] 第 4.34 段。

於《1985 年刑事法典》已訂有第 430(1)條，這或可解釋為何該法典並無針對非法干擾電腦系統的特定條文。

英格蘭及威爾斯

在《英格蘭誤用電腦法令》制定時的第 3 條

5.29 《英格蘭誤用電腦法令》於 1990 年 8 月 29 日生效時，第 3 條（*"在未獲授權下修改電腦資料"*）訂立以下罪行：

> "(1) 任何人在以下情況，即屬犯罪——
>
> (a) 該人作出任何作為，導致在未獲授權下修改任何電腦的內容；及
>
> (b) 該人在作出該作為時，具所需的意圖及所需的知悉。
>
> (2) 就上文第(1)(b)款而言，所需的意圖，指意圖導致修改任何電腦的內容，並藉如此行事而——
>
> (a) 損害任何電腦的操作；
>
> (b) 阻止或阻礙取覽存於任何電腦內的任何程式或數據；或
>
> (c) 損害上述程式的操作或上述數據的可靠性。
>
> (3) 有關意圖不一定要針對——
>
> (a) 任何特定電腦；
>
> (b) 任何特定程式或數據，或任何特定種類的程式或數據；或
>
> (c) 任何特定修改或任何特定種類的修改。
>
> (4) 就上文第(1)(b)款而言，所需的知悉，指知悉該人意圖導致的任何修改未獲授權。

(5) 就本條而言，未獲授權的修改或其屬上文第(2)款所述類別的任何預定影響是否屬永久性或僅屬暫時性，或是否擬屬永久性或擬僅屬暫時性，均屬無關重要。

(6) 就〔1971 年第 48 章〕《1971 年刑事損壞法令》（Criminal Damage Act 1971）而言，修改電腦的內容不得視為損壞任何電腦或電腦儲存媒體，但如該項修改對該電腦或電腦儲存媒體的影響，是損害其物理狀況，則作別論。

(7) 任何人犯本條所訂罪行——

(a) 一經循簡易程序定罪，可處為期不超過 6 個月的監禁或不超過法定最高罰款，或兩者兼處；及

(b) 一經循公訴程序定罪，可處為期不超過 5 年的監禁或罰款，或兩者兼處。”

5.30 某評論員指出，對於上述條文是否適用於分布式拒絕服務攻擊及類似不當行為這問題，當時有*“相當激烈的爭辯”*。[36] 此外，在*Director of Public Prosecutions v Lennon*[37]（以案件呈述方式提出的上訴），法院裁定當時的第 3 條可適用於電郵轟炸，至於裁定該條並不適用的初審裁決則*“備受傳媒廣泛批評”*。[38]

《2006 年警察及司法法令》所帶來的改革

5.31 在上述背景下，《2006 年警察及司法法令》（Police and Justice Act 2006）第 36 條藉新條文（標題是*“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”*）取代原有的《英格蘭誤用電腦法令》第 3 條。制定為《2006 年警察及司法法令》的法案的註釋述明：

“301. 這項修訂旨在確保訂定完備的條文，將各種形式的拒絕服務攻擊定為罪行。在此等攻擊中，攻擊者拒絕受害人取用特定資源，方法通常是阻止某項服務

---

36 Neil MacEwan, “The Computer Misuse Act 1990: lessons from its past and predictions for its future” [2008] Crim LR 955，第 959 頁。

37 引用於*朱峻璋案*第 36 頁（第 14 段）。見上文第 5.11 段。

38 見上文註腳 36，第 960 頁。

的合法使用者取用該項服務（例如藉發送電郵等行動，令某網站的互聯網服務供應商不勝負荷）……。”

現行的《英格蘭誤用電腦法令》第 3 條

5.32　2008 年 10 月 1 日，英格蘭及威爾斯實施新的第 3 條。其後，《2007 年嚴重刑事罪行法令》（Serious Crime Act 2007）及《2015 年嚴重刑事罪行法令》（Serious Crime Act 2015）再進一步修訂該條。第 4 章已載述第 3 條的現行版本，[39] 但我們在此再引述該條，以便與原有版本作比較：

“(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；及

(c) 下文第(2)款或第(3)款適用。

(2) 如上述人士意圖藉作出有關作為而——

(a) 損害任何電腦的操作；

(b) 阻止或阻礙取覽存於任何電腦內的任何程式或數據；或

(c) 損害上述程式的操作或上述數據的可靠性；或

(d) 致使上述(a)至(c)段提述的任何事宜得以作出，

則本款適用。

(3) 如上述人士罔顧有關作為是否會造成上文第(2)款(a)至(c)段所述的任何事宜，則本款適用。

(4) 上文第(2)款所提述的意圖，或上文第(3)款所提述的罔顧後果，不一定要涉及——

(a) 任何特定電腦；

---

[39] 第 4.38 段。

(b) 任何特定程式或數據；或

(c) 任何特定種類的程式或數據。

(5) 在本條中——

(a) 凡提述作出某作為，即包括提述導致作出某作為；

(b) '作為'包括一連串作為；

(c) 凡提述損害、阻止或阻礙某些事宜，即包括提述暫時如此行事。

(6) 任何人犯本條所訂罪行——

(a) 一經在英格蘭及威爾斯循簡易程序定罪，可處為期不超過 12 個月的監禁或不超過法定最高罰款，或兩者兼處；

(b) 〔……〕

(c) 一經循公訴程序定罪，可處為期不超過 10 年的監禁或罰款，或兩者兼處。"

5.33 由於目標電腦的操作不必受到實際損害，故現行的第 3 條可能適用於如*朱峻瑋*案中失敗的分布式拒絕服務攻擊。根據第 3(2)及(3)條，如攻擊者意圖導致有關損害或罔顧會否造成有關損害，便已足夠。

《英格蘭誤用電腦法令》第 3ZA 條

5.34 如非法干擾電腦系統導致《英格蘭誤用電腦法令》第 3ZA 條所指的*"關鍵性嚴重損害"*，或產生導致該條所指的*"關鍵性嚴重損害"*的重大風險，該項干擾便可能構成第 3ZA 條所訂罪行。由於第 4 章已探討該條，[40] 似乎沒必要在此再論述該條。

---

40 第 4.41 至 4.46 段。

中國內地

《中國刑法》第二百八十五及二百八十六條

5.35 《中國刑法》第二百八十五條第二款訂明：*"違反國家規定，……對〔不屬國家事務、國防建設、尖端科學技術領域的〕計算機信息系統實施非法控制"*，須給予處罰。

（底線後加）

5.36 第二百八十六條第一款，是另一項關於干擾電腦系統的條文，針對令該系統無法正常運行的行為：

> "違反國家規定，對計算機信息系統功能進行刪除、修改、增加、干擾，造成計算機信息系統不能正常運行，後果嚴重的，處五年以下有期徒刑或者拘役；後果特別嚴重的，處五年以上有期徒刑。"

（底線後加）

犯罪行為

5.37 第二百八十五條第二款與第二百八十六條第一款的分別，在於對計算機信息系統進行的行為，即*"實施非法控制"*與*"對……功能進行刪除、修改、增加、干擾，造成……系統不能正常運行"*。實際上，這兩條看來可作為檢控案件的交替理由。

5.38 在中國最高人民法院發布的第 26 批指導性案例的第 145 號案例，[41] 犯罪者通過向網站服務器植入木馬程序，對計算機信息系統內的數據進行增加、修改，以提高賭博網站廣告被搜尋引擎命中機率。法院裁定，這種行為只導致犯罪者對該系統實施非法控制，但未造成該系統功能的破壞，或不能正常運行，因此裁定這種行為並未符合第二百八十六條第一款的規定。然而，犯罪者就第二百八十五條第二款所訂罪行，被裁定罪名成立。[42]

5.39 另外，最高人民檢察院第九批指導性案例的第 35 號案例[43]作出以下指示：通過修改計算機信息系統（即案中的智能手機）的登

---

41 《最高人民法院關於案例指導工作的規定》第七條規定，中國最高人民法院發布的指導性案例，各級人民法院審判類似案例時應當參照。

42 張竣傑等非法控制計算機信息系統案。

43 曾興亮、王玉生破壞計算機信息系統案。

錄密碼而鎖定有關設備，導致合法使用者不能取用或正常使用的行為，亦構成第二百八十六條第一款所訂罪行。

新西蘭

《新西蘭法令》第 250(2)(c)條

5.40 我們在第 4 章介紹《新西蘭法令》第 250(2)條（*"損壞或干擾電腦系統"*）時，提到本章會探討第 250(2)(c)條。[44] 根據第 250(2)(c)條：

> "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……
>
> (c) 導致任何電腦系統——
>
> (i) 發生故障；或
>
> (ii) 拒絕向任何獲授權使用者提供服務，
>
> 可處為期不超過 7 年的監禁。"

5.41 第 250(2)條以 *"蓄意或罔顧後果地"* 行事，形容進行犯罪行為的犯罪意念，而有關未獲授權的犯罪意念，則是知悉或罔顧後果。關於犯罪意念的問題，我們在第 4 章[45] 提出的各點均適用於第 250(2)條各段，包括(c)段，故不必在此重複。

5.42 就第 250(2)(c)條適用的情境而言，某評論員有以下評析：

> "7.96 第 250(2)(c)條的適用範圍廣泛。舉例而言，如軟件被拙劣地或罔顧後果地編入缺損程式，根據該條，軟件生產商可能須負上法律責任。此外，任何人罔顧後果地透過電郵發送病毒，亦須負上法律責任，但有意見認為使用者應該安裝最新的防毒軟件，亦應對他們轉發的電郵格外謹慎。
>
> ……
>
> 7.98 該款亦可能適用於濫發電郵者。濫發電郵者如對於發送大量電郵對郵件伺服器可能造成的影響掉以輕

---

44 第 4.50 至 4.51 段。

45 第 4.57 段。

心，罔顧後果這項元素便頗有可能適用。非應邀的郵件必須大量湧入，才能拖垮互聯網服務供應商的郵件伺服器，導致服務發生故障或拒絕提供服務。因此，第250(2)(c)條不會普遍適用於所有濫發電郵者。”[46]

《新西蘭法令》第 250(1)條

5.43 第 4 章亦有提及第 250(1)條，[47] 這是另一項針對非法干擾電腦系統的條文：

> “任何人蓄意或罔顧後果地摧毀、損壞或更改任何電腦系統，並知悉或理應知悉相當可能會導致生命受危害，可處為期不超過 10 年的監禁。”

5.44 上文引述的評論員將第 250(1)及(2)條比較如下：

> “……第 250(1)條可適用於已獲授權取用電腦系統的人，但第 250(2)條規定，取用電腦系統的人須未獲授權，並：
>
> (1) 知悉自己未獲授權；或
>
> (2) 罔顧自己是否已獲如此授權。
>
> 換言之，任何獲授權對系統作出某些行為（如移動或刪除檔案）的人（例如系統管理員），均可干犯第 250(1)條所訂罪行。第 250(2)條則規定，有關行為元素須缺乏權限，或須涉及罔顧是否已獲授權這項元素。”[48]

5.45 該評論員重點評論有關授權的問題，凸顯了在涉及第 250(2)條及其他司法管轄區相類法規的情況下，獲得授權的重要性。舉例而言，流動數據服務供應商可能會因公平使用政策而獲得合約權利，可在數據使用量超過指明限額時，限制客戶的數據傳輸速度，或暫停某些數據服務。雖然這些安排會限制客戶透過其器材正常使用數據服務，但客戶接納公平使用政策，實際上對施加這些限制給予授權。若然服務供應商在公平使用政策所預期的情況下啟動這些安排，便不必擔心會招致潛在的刑事法律責任。

---

46 David Harvey, *internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015)，第 7.96 及 7.98 段。

47 第 4.58 段。

48 見上文註腳 46，第 7.90 段。

新加坡

《新加坡誤用電腦法令》第 7 條

5.46 《新加坡誤用電腦法令》第 7 條(*"在未獲授權下妨礙使用電腦"*)訂明相關罪行如下:

> "(1) 任何人在沒有權限或合法辯解的情況下——
>
> (a) 故意干擾、中斷或妨礙合法使用某電腦;或
>
> (b) 故意阻撓或阻止取覽儲存於某電腦的任何程式或數據,或損害該程式或數據的效用或效能,
>
> 即屬犯罪,一經定罪——
>
> (c) 可處不超過$10,000 的罰款或為期不超過 3 年的監禁,或兩者兼處;及
>
> (d) 如屬第二次或其後每次定罪,則可處不超過$20,000 的罰款或為期不超過 5 年的監禁,或兩者兼處。
>
> (2) 如因本條所訂罪行而導致任何損壞,被裁定犯該罪行的人可處不超過$50,000 的罰款或為期不超過 7 年的監禁,或兩者兼處。"

5.47 雖然《新加坡誤用電腦法令》的罪行條文主要是建基於加拿大和英格蘭及威爾斯的相應條文,但該法令並沒有加入任何註釋,指其他司法管轄區的任何法例條文是第 7 條的藍本(該法令對其他條文則有這樣做)。

沒有權限或合法辯解的情況

5.48 若按第 7 條的字面理解,如在具有權限或合法辯解的情況下作出(a)及(b)段所載的行為,則不屬犯罪。*"沒有權限"*一詞,亦見於第 3 條(*"在未獲授權下取覽電腦資料"*)及第 6 條(*"在未獲授權下使用或截取電腦服務"*)。就取覽電腦程式或數據的情況而言,第 2(5)條對該詞解釋如下:

> "就本法令而言，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，即屬未獲授權取覽或在沒有權限的情況下取覽——
>
> (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。"

若以類似方式理解第 7 條的 *"沒有權限"*，似乎屬合理之舉。

5.49 在《新加坡誤用電腦法令》中，*"合法辯解"*一詞僅在第 7 條出現一次，亦沒有定義。這與香港《刑事罪行條例》（第 200 章）第 64(2)條形成對比，該條就刑事損壞（包括 *"誤用電腦"*）的控罪，訂定兩項合法辯解。[49]

第 7 條的適用範圍

5.50 《新加坡誤用電腦法令》第 7 條措辭寬廣。在概念上，該條的應用並不限於分布式拒絕服務攻擊及類似的不當行為。某評論員對一宗相關案件有以下描述：

> "一名曾受僱於 SMC Marine Services 的系統工程師，被控離職前秘密地在他開發的程式內設定密碼，涉嫌令前僱主無法對有關系統進行檢查、修改或升級。這可構成《〔誤用電腦〕法令》第 5 條（在未獲授權下修改）或第 7 條（在未獲授權下妨礙）所訂罪行。案中公司亦在高等法院展開民事訴訟，尋求禁制令防止其機密資料外洩。"[50]

5.51 案中前僱主成功申請臨時禁制令，防止其指稱的版權外洩及遭侵犯，[51] 而有關民事訴訟據報亦告完結。案中系統工程師被控非法修改電腦系統，但最終因法院裁定控方 *"未有在排除合理疑點的情況下履行舉證責任"*而獲判無罪。[52]

---

49 第 4.92 至 4.94 段。

50 Gregor Urbas, "An Overview of Cybercrime Legislation and Cases in Singapore" (ASLI Working Paper No 001, Dec 2008)，第 14 頁。

51 *SMC Marine Services (Pte) Ltd v Thangavelu Boopathiraja and Others* [2008] SGHC 29.

52 The Straits Times, "Man cleared of sabotage"（2009 年 6 月 3 日），登載於 https://www.asiaone.com/News/AsiaOne%2BNews/Crime/Story/A1Story20090603-145841.html（於 2022 年 5 月 3 日瀏覽）。

不同情況的最高刑罰

5.52 《新加坡誤用電腦法令》就所訂罪行訂明一致的最高刑罰。以下概述的最高刑罰量刑基準，同樣適用於根據第 5 條（*"在未獲授權下修改電腦資料"*）[53] 或第 7 條被定罪的人：

(a) 初犯者可處不超過 10,000 新加坡元的罰款或最多三年監禁，或兩者兼處。

(b) 對再犯者訂定的最高刑罰較重（不超過 20,000 新加坡元的罰款或最多五年監禁，或兩者兼處）。

(c) 導致實際損壞的犯罪者的最高刑罰，包括不超過 50,000 新加坡元的罰款或最多七年監禁，或兩者兼處。

(d) 如犯罪者取用任何 *"受保護電腦"*，[54] 則《新加坡誤用電腦法令》第 11(1)條訂明更重的最高刑罰（不超過 100,000 新加坡元的罰款或最多 20 年監禁，或兩者兼處）。

美國

《電腦欺詐及濫用法案》內的《美國法典》第 18 篇第 1030(a)(5)條

5.53 雖然有人認為，發動分布式拒絕服務攻擊如同靜坐示威[55]（即示威者佔據某地方後拒絕離開，直至他們的要求得到滿足的抗議形式），[56] 應屬合法，[57] 但看來美國已清楚確立這樣做可能會違反下文所載的《美國法典》第 18 篇第 1030(a)(5)條。正如第 4 章所述，[58] 任何人如作出以下作為，可按第 1030(c)條的規定予以懲處：

---

53 第 4.64 段。

54 有關法定定義載於第 4.68 段。

55 例子見 Chris Peterson, "In Praise of [Some] DDoSs?"（2009 年 7 月 21 日），登載於 http://www.cpeterson.org/2009/07/21/in-praise-of-some-ddoss/（於 2022 年 5 月 3 日瀏覽）：*"在某程度上，分布式拒絕服務攻擊如同靜坐。兩者的核心概念均包括過度利用稀缺資源（前者利用伺服器週期，後者則利用櫃檯空間）來將他人排除在外，以達到政治效果。兩者均屬非暴力，但有損經濟。兩者均可具有政治性質，有關罪行因而可置於上述背景下考慮。"*

56 Oxford University Press, "Lexico.com"（2021 年），網址為 https://www.lexico.com/definition/sit-in（於 2022 年 5 月 3 日瀏覽）。

57 例子見 Mike Masnick, "Anonymous Launches White House Petition Saying DDoS Should Be Recognized As A Valid Form Of Protest"（2013 年 1 月 11 日），登載於 https://www.techdirt.com/articles/20130111/08053821642/anonymous-launches-white-house-petition-saying-ddos-should-be-recognized-as-valid-form-protest.shtml（於 2022 年 5 月 3 日瀏覽）。

58 第 4.70 至 4.71 段。

"(A) 故意導致向某受保護電腦傳送程式、資料、代碼或指令，並因着該行為而在未獲授權下蓄意導致該電腦損壞；

(B) 在未獲授權下蓄意取用某受保護電腦，並因着該行為而罔顧後果地導致損壞；或

(C) 在未獲授權下蓄意取用某受保護電腦，並因着該行為而導致損壞及損失。"

美國的分布式拒絕服務攻擊

5.54 舉例而言，某網上期刊載有以下記項，該記項的日期為2001年1月19日：

> "美國阿拉斯加地區法院的前電腦系統管理員史葛．丹尼斯（Scott Dennis）因為對美國紐約東區地區法院的伺服器發動三次拒絕服務攻擊，被阿拉斯加地區法院判處監禁六個月以及履行240小時的社會服務……丹尼斯承認一項違反《美國法典》第18篇第1030(a)(5)(C)條的非重刑罪。谷柏（Cooper）補充說：'美國地區法院系統並非首次受到攻擊'；華盛頓州西區地區法院也曾受攻擊。丹尼斯已不再於美國地區法院任職。亦見聯邦調查局的新聞公報。"[59]

5.55 涉及分布式拒絕服務攻擊的案件持續在美國發生。某宗矚目案件的犯罪者承認：

> "……一項故意導致向某受保護電腦傳送程式、資料、代碼及指令，並因着該行為而蓄意導致該電腦損壞的控罪。"[60]

這顯然是根據《美國法典》第18篇第1030(a)(5)(A)條提出的控罪。犯罪者被判處監禁六年。[61]

---

59 Tech Law Journal, "News Briefs from January 11-20, 2001"，登載於 http://www.techlawjournal.com/home/newsbriefs/2001/01b.asp（於2022年5月3日瀏覽）。

60 克利夫蘭聯邦調查局（Federal Bureau of Investigation Cleveland），"Akron Man Arrested and Charged for DDoS Attacks"（2018年5月10日），登載於 https://www.fbi.gov/contact-us/field-offices/cleveland/news/press-releases/akron-man-arrested-and-charged-for-ddos-attacks（於2022年5月3日瀏覽）。

61 美國司法部，"Akron man sentenced to six years in prison for launching denial of service attacks that shut down web sites for the city of Akron and the Akron Police Department"（2019年10月3日），

令語音信箱系統及電郵系統不勝負荷

5.56 上述案件的法院文件似乎沒有網上版。要了解《美國法典》第 18 篇第 1030(a)(5)條如何把非法干擾電腦系統定為不合法，參考 *Pulte Homes, Inc v Laborers' International Union of North America*[62] 會有所啟發，縱使該案屬源自勞資糾紛的民事案件。[63]

5.57 普爾特公司（Pulte）是這宗案件的僱主，它指稱工會 LIUNA *"以數以千計的電話來電及電郵，轟炸普爾特公司的銷售辦事處及其中三名營業主任"*，[64] 引致以下後果：

> "這些來電堵塞了普爾特公司的語音信箱系統，令客戶無法聯絡該公司的銷售辦事處及營業代表，而該公司的一名僱員甚至被迫關掉工作手機。電郵所造成的破壞更加嚴重：這些電郵令該公司的系統（該系統對收件匣的電郵數目設有限制）不勝負荷，以致該公司的僱員無法查閱與業務有關的電郵，或向客戶及供應商發送電郵，正常業務運作因而陷入停頓。"[65]

5.58 聯邦上訴法院第六巡迴法庭處理《美國法典》第 18 篇第 1030(a)(5)條的全部三個部分，並就普爾特公司根據《美國法典》第 18 篇第 1030(a)(5)(A)條提出的 *"傳送申索"*，作出以下裁定：

(a) 在應用"損壞"的法定定義（即 *"對數據、程式、系統或資料的完整性或可用性造成任何損害"*）時：[66]

> "……凡進行的傳送會削弱健全的電腦系統（或同樣地，進行的傳送會降低原告人使用數據或系統的能力），即屬導致損壞。LIUNA 的一連串來電及電郵，正被指稱有如此效果。"[67]

登載於 https://www.justice.gov/usao-ndoh/pr/akron-man-sentenced-six-years-prison-launching-denial-service-attacks-shut-down-web（於 2022 年 5 月 3 日瀏覽）。

62 648 F 3d 295 (6th Cir 2011). 聯邦上訴法院第六巡迴法庭（Court of Appeals for the Sixth Circuit）的意見書（即判詞），日期為 2011 年 8 月 2 日，登載於其網站，網址為 http://www.ca6.uscourts.gov/opinions.pdf/11a0200p-06.pdf（於 2022 年 5 月 3 日瀏覽）。

63 《美國法典》第 18 篇第 1030 條同時訂立若干電腦網絡罪行，並訂明民事訴訟因由。

64 見上文註腳 62，第 2 頁。

65 見上文註腳 62，第 3 頁。

66 《美國法典》第 18 篇第 1030(e)(8)條。

67 見上文註腳 62，第 7 頁。

(b) 進行初審的地區法院，要求普爾特公司 *"指稱 LIUNA **知悉** 其來電及電郵會對普爾特公司的電腦系統造成傷害"*[68]，或 *"LIUNA 完全清楚其電郵活動的**實際**後果"*[69]（強調之處乃原文所有），實屬錯誤。普爾特公司只要：

> "……指稱 LIUNA 是有意識地為了對普爾特公司的電腦系統導致法定意義上的損壞而行事——此標準並不要求完全知悉有關事實"，[70]便已足夠。

因此，上訴法院恢復普爾特公司在初審時被駁回的 *"傳送申索"*。

5.59 然而，上訴法院確認地區法院以下裁定：普爾特公司未能根據《美國法典》第 18 篇第 1030(a)(5)(B)及(C)條就 *"取用申索"* 作出陳述。上訴法院裁定：

> "為了就取用申索作出陳述，原告人必須作出多項指稱，其中包括被告人'在未獲授權下蓄意取用某受保護電腦。'（《美國法典》第 18 篇第 1030(a)(5)(B)、(C)條）。……我們無須決定 LIUNA 的來電及電郵有沒有取用普爾特公司的電腦，因為即使有，普爾特公司也沒有指稱該項取用是'在未獲授權下'作出的。"[71]

> "LIUNA 使用非受保護公共通訊系統，這推翻了普爾特公司指稱 LIUNA'在未獲授權下'取用其電腦的說法。普爾特公司容許所有公眾人士聯絡其辦事處及營業主任：該公司並沒有指稱例如 LIUNA 或任何其他人需要密碼或代碼，才能致電或發送電郵給該公司。反之，普爾特公司的電話系統及電郵系統，一如非受保護網站，'是向公眾開放的，故〔LIUNA〕獲授權使用〔這些系統〕。'見〔*Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418，〕第 420 頁。另外，普爾特公司雖有就通訊的數目、頻密程度及內容作出投訴，但對於一個或數個來電，或一封或數封電郵，卻連一項未獲授權指稱也沒有。因此，普

---

68 見上文註腳 62，第 8 頁。
69 見上文註腳 62，第 9 頁。
70 見上文註腳 62，第 9 頁。
71 見上文註腳 62，第 10 頁。

爾特公司的投訴，充其量只算是指稱 LIUNA 超逾獲授權的取用範圍。”[72]

5.60 正如上訴法院在 *Pulte* 案所指，[73] 最高法院在 *Leocal v Ashcroft*[74] 裁定，任何法規不論應用於刑事或非刑事案件，解釋須一致。因此，可以預計法院在非法干擾電腦系統（例如藉着對網站發動分布式拒絕服務攻擊）的檢控中，亦會以同樣方式解釋《美國法典》第 18 篇第 1030(a)(5)條。

小組委員會的看法

一致處理干擾數據及干擾系統

5.61 正如第 4 章及上文所論述，現時香港法律處理非法干擾電腦數據及非法干擾電腦系統的主要方式，是將兩者視為 *“誤用電腦”*，即刑事損壞的一種形式。由於這兩類不當行為部分互相重疊，故上述法律立場實屬合理。

5.62 從案例可見，現有法例的整體施行情況理想。舉例來說，*朱峻璋*案展示了但凡干擾電腦系統，不論成功與否，均可能招致刑事法律責任。這與我們的方針一致：純粹在無權的情況下取用整台電腦或其任何部分，應定為罪行，如意圖進行其他犯罪活動而取用電腦，則應構成加重罪行。

5.63 我們認為，針對干擾數據及干擾系統的現行體制有貫徹一致的優點，應予保存。因此，我們建議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。

新法例應採用現有條文

5.64 我們在建議 6(c)提出，應把《刑事罪行條例》（第 200 章）第 59(1A)及 60 條關於“誤用電腦”的部分改列於新法例。

5.65 我們在擬訂該項建議時，曾考慮如“誤用電腦”的概念不再屬刑事損壞罪的涵蓋範圍，而是一項並非載於《刑事罪行條例》（第 200 章）的新訂獨立罪行，是否仍可引用以有關“誤用電腦”的現行法律為依據的案例（例如*朱峻璋*案）。

---

72 見上文註腳 62，第 11 至 12 頁。

73 見上文註腳 62，第 8 頁。

74 543 US 1 (9 Nov 2004).

5.66 我們認為，只要在草擬新法例時小心謹慎，並適當參考現行的法例措辭(尤其是藉機會將相關案例的基本法律原則編纂為法例條文)，我們便可相信新法例的目的會如實反映，在建議的修改落實後，“誤用電腦”背後的政策及立法原意亦因此能保持清晰明確。

可釐清“誤用電腦”一詞

5.67 假設建議 6(c)得以落實，便可藉着將相關條文從《刑事罪行條例》(第 200 章)遷往新法例的機會，完善 *“誤用電腦”* 的法定概念。舉例而言，以下做法似乎會有好處：

(a) 釐清如攻擊的破壞力巨大，導致目標電腦完全不能運作，這會否涉及第 59(1A)(a)條 —— *“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”* —— 在新法例中的對等條文；及

(b) 將諸如 *“損害任何電腦的操作”*[75] 的概念納入 *“誤用電腦”* 的定義。

建議罪行的適用範圍

5.68 最重要的是，新法例應保留現有法律的廣度，不宜過於局限。舉例來說，除了現有法律已涵蓋的情境外，我們認為建議的罪行應適用於上述比較研究所提到的以下各方：

(a) 攻擊電腦系統失敗的人；[76]

(b) (如軟件被蓄意或罔顧後果地編入缺損程式)軟件的生產商；[77] 及

(c) 故意並在未獲授權下對電腦系統作出任何更改的人，而該項更改可能導致合法使用者不能取用或正常使用系統。[78]

---

75 根據《英格蘭誤用電腦法令》第 3 條，任何人如 *“就某電腦作出任何未獲授權的作為”*，而該人知悉該作為未獲授權，並意圖 *“損害任何電腦的操作”* 等，或罔顧是否會引致上述後果，即屬犯罪。見第 5.32 段。

76 見第 5.33 段，內容關乎《英格蘭誤用電腦法令》第 3 條。

77 見第 5.42 段，內容關乎《新西蘭法令》第 250(2)(c)條。

78 見第 5.50 段，內容關乎《新加坡誤用電腦法令》第 7 條。

建議 7

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。

合法辯解

5.69 讀者可能會記得，第 2 章曾提及在環球層面，總會有人（包括但不限於網絡安全從業員）在電腦網絡空間測試他人的電腦，而目標電腦的擁有人往往並不知情，更不用說授權測試。[79]

5.70 用作進行這些測試的工具唾手可得，在互聯網搜尋一下便可輕易找到，不只在暗網才有。現時已有各種各樣的測試工具可導致不同程度的入侵。有些工具只會掃描電腦系統一次，不會對系統造成損壞，但另一些工具則可持續進行掃描（比方說持續掃描幾小時）。另

[79] 第 2.112(a)段。

外還有一些工具可對電腦系統造成重大損壞。關鍵問題在於如何使用有關工具。

5.71 基於上述背景，我們詳細討論了因任何理由而掃描（或以類似的形式測試）他人的電腦，在新法例下應否足以視為建議的非法干擾電腦系統罪的合法辯解。就使用測試工具的網絡安全從業員而言，對於法律應如何平衡他們的利益與社會大眾的利益這問題，我們初步認為，實行較嚴格的規管體制可能對網絡安全從業員造成損失，而在未獲授權下使用測試工具可能對目標電腦系統的管理人及擁有人造成損壞或損失，兩者比較之下，前者的損失看來沒有那麼廣泛。

5.72 公眾對建議 8 所載的諮詢問題發表意見，會有助我們確定立場。具體而言，(a)段主要針對網絡安全專業人員，而(b)段則涉及非保安專業人員（例如搜尋器營運人、電腦終端使用者等）。

建議 8

小組委員會邀請公眾就以下問題提交意見書：

(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；[80] 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）：

80 RFC6335 的資料登載於互聯網工程專責組（Internet Engineering Task Force）的網站，網址為 https://datatracker.ietf.org/doc/rfc6335/（於 2022 年 5 月 3 日瀏覽）。

(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？

第 6 章　提供或管有用作犯罪的器材或數據

引言

6.1　我們會在本章探討導言所提及的第五類（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。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。

6.2　如任何人實際使用器材或數據，舉例來說對電腦進行黑客入侵，即會構成非法取覽罪的犯罪行為。本章的重點，是應否將純粹提供或管有有關器材或數據（例如管有存有勒索軟件的記憶棒）定為獨立的罪行，以及如應該的話，應如何擬定該罪行。

6.3　這類器材及數據的例子，包括：

(a) 用於測試網絡的軟件，例如某些軟件可通過進行滲透測試，評估電腦系統對分布式拒絕服務攻擊的承受能力；

(b) 破解密碼工具，該工具可能是軟件，亦可能是實物器材；及

(c) 消磁器，它可通過消除磁性儲存媒體（例如硬碟）的磁性，銷毀該媒體中的數據。

6.4　任何人可能不需要任何特別硬件，僅是使用軟件也能干犯電腦網絡罪行。

香港的現行法律

《刑事罪行條例》（第 200 章）

第 62 條

6.5　對於第 2 至 5 章所論述的依賴電腦網絡的罪行，香港處理該等罪行的法例條文主要載於《刑事罪行條例》（第 200 章）及《電訊

條例》（第 106 章）。按照邏輯，如任何條文與本章相關，並擬適用於前數章所介紹的依賴電腦網絡的罪行，該等條文固然應載於該兩條條例內。

6.6 我們宜先審視《刑事罪行條例》（第 200 章）。第 59(1A)條訂明在該條例的第 VIII 部中，*"摧毀或損壞財產（to destroy or damage any property），就電腦而言，包括誤用電腦"*。因此，第 VIII 部第 62 條（*"管有任何物品意圖摧毀或損壞財產"*）所訂可處監禁十年的以下罪行，[1] 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。"

實際上可能產生的問題

6.7 第 62 條適用於意圖摧毀或損壞財產的人，如有人意圖導致或意圖准許他人摧毀或損壞財產，該條亦適用。對於兼具合法及非法目的之物品，以及只可作非法用途的物品，該條並沒有加以區分。

6.8 至於保管或控制有關物品的人，是否須負上法律責任，主要視乎該人的意圖。由於人的意念屬主觀性質，在執法過程中可能出現舉證問題。

對受禁物的解釋

6.9 第 62 條的英文文本用 *"anything"* 一詞來描述受禁物，而中文文本的對應詞則是 *"任何物品"*。

6.10 按照一般的說法，*"anything"* 一詞並不限於有形物，如從以下角度考慮，該詞的涵蓋範圍似乎比 *"任何物品"* 更廣：雖然實物顯然屬於 *"任何物品"* 的範圍，但該詞的慣常涵義會否明確引伸至某些可利便干犯第 62 條所訂罪行的無形物，則是截然不同的問題。就干犯 *"誤用電腦"* 罪的情況而言，下述例子可帶出該問題：

---

[1] 《刑事罪行條例》（第 200 章）第 63(2)條。

(a) 電腦軟件或數據（例如惡意軟件及登入憑證）；

(b) 提供黑客入侵服務或類似服務；及

(c) 有關利用漏洞（exploit）的專門知識。

6.11 如 *"anything"* 與 *"任何物品"* 的涵蓋範圍可能不同，《釋義及通則條例》（第 1 章）第 10B 條（*"兩種法定語文本條例的釋疑"*）即可發揮作用：

"(1) 條例的中文本和英文本同等真確，解釋條例須以此為依據。

(2) 條例的兩種真確本所載條文，均推定為具有同等意義。

(3) 凡條例的兩種真確本在比較之下，出現意義分歧，而引用通常適用的法例釋義規則亦不能解決，則須在考慮條例的目的和作用後，採用最能兼顧及協調兩文本的意義。"

6.12 在 *T 訴 警務處處長*（*T v Commissioner of Police*），[2] 終審法院須審理的主要爭論點是：在《公眾娛樂場所條例》（第 172 章）下 *"公眾娛樂"* 的定義[3] 中，*"admitted"* 一詞應如何解釋。雖然這宗上訴主要是依據該法例的英文文本來爭辯，[4] 但終審法院就該爭論點作出裁定時，亦考慮了 *"admitted"* 的中文對應詞 *"讓……入場"*。[5] 舉例而言，終審法院常任法官李義接納以下看法：

"……'公眾娛樂'定義的中文文本，尤其是'入場'一詞的使用，帶有'特定地點'的涵義，而……英文文本並不帶有這個涵義……由於兩個真確文本之間存在差異，所以便須……解決……"[6]

---

2 (2014) 17 HKCFAR 593.

3 即 *"……讓公眾入場的任何娛樂，而不論是否收取入場費"*（第 2 條）。

4 見上文註腳 2，第 679 頁（第 284 段）（終審法院非常任法官廖柏嘉勳爵〔Lord Neuberger of Abbotsbury〕）。

5 見上文註腳 2，第 607 頁（第 11(5)段）（終審法院首席法官馬道立）、第 625 頁（第 82 段）（終審法院常任法官李義）、第 648 頁（第 166 段）（終審法院常任法官鄧國楨）、第 666 頁（第 232 段）及第 671 頁（第 253 段）（終審法院常任法官霍兆剛），以及第 679 頁（第 284 段）（終審法院非常任法官廖柏嘉勳爵）。

6 見上文註腳 2，第 625 頁（第 82 段）（終審法院常任法官李義）。

6.13 終審法院亦確認了下述重要原則：

> "……法庭不能夠對一項法例條文作出該條文所使用的經按照其文意和法定目的理解的語言所不能承載的解釋"。[7]

6.14 終審法院大比數裁定，*"admitted"*一詞應解釋為*"在主動意義上表示出給予某人准許進入或出入或讓人入內"*。[8] 該法例的中文文本似乎比英文文本更為具體，如中文文本未有影響法院有關裁決，它至少為該裁決提供支持。

6.15 在解釋《刑事罪行條例》（第 200 章）第 62 條時，一種可能的說法是，該條的文意及目的均要求*"anything"*及*"任何物品"*涵蓋有形物及無形物，但有人可能會認為這樣解釋該條，似乎會令*"任何物品"*的慣常涵義過度延伸。另一個可能性，是把*"anything"*及*"任何物品"*一併理解為只傳達兩者兼具的概念。根據該論點，若採取這種做法，無形物便可能被排除在第 62 條的範圍外，這無助於將第 62 條應用於電腦網絡空間。

第 62 條與刑事損壞罪相關

6.16 此外，《刑事罪行條例》（第 200 章）第 62 條禁止保管或控制任何意圖用作摧毀或損壞財產的物品，亦即用作干犯該條例第 60 條所訂罪行的物品。對於其他條文所訂罪行（例如該條例第 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。

《電訊條例》（第 106 章）

6.17 《電訊條例》（第 106 章）雖然並無與《刑事罪行條例》（第 200 章）第 62 條相對應的條文，但該條例設立了無線電通訊器具的發牌制度。[9] 就本諮詢文件而言，似乎沒有必要詳細描述該制度。我們只需指出，在該制度適用的情況下，違反有關規定，即屬犯罪。[10]

---

7 見上文註腳 2，第 655 頁（第 195 段）（終審法院常任法官霍兆剛），類似看法見第 607 頁（第 12 段）（終審法院首席法官馬道立）。

8 見上文註腳 2，第 670 頁（第 250 段）（終審法院常任法官霍兆剛）。

9 《電訊條例》（第 106 章）第 8(1)及 9 條；《電訊（電訊器具）（豁免領牌）令》（第 106Z 章）第 5 及 7 條。

10 見下文第 6.20 段，1-a-i。

6.18 該制度可能適用於可用作干犯《電訊條例》（第 106 章）第 27A、27(b)及 25(a)條所訂罪行的電腦或智能電話，而我們在第 2、3 及 4 章分別論述建議的非法取覽罪、非法截取數據罪及非法干擾數據罪時，已提及該等條文。[11]

6.19 我們認為，現有的發牌制度並不足以打擊電腦網絡罪行。舉例來說，該制度的其中一個限制是涵蓋範圍狹窄，只適用於無線電波等電訊技術。現行法律的不足，正是應訂立特定的新罪行的部分原因。

《布達佩斯公約》訂定罪行的標準

6.20 根據《布達佩斯公約》第一節之下的第一篇第六條：[12]

> "1 各締約方均應採取必要的立法及其他措施，在其本土法律中將下列在無權的情況下蓄意作出的行為定為刑事罪行：
>
> a 生產、出售、為使用而獲取、輸入、分發或以其他方式提供：
>
> i 經設計或改裝以主要用作干犯第二至五條所訂任何罪行的器材[13]（包括電腦程式）；
>
> ii 可藉以取用整個電腦系統或其任何部分的電腦密碼、取用碼或類似數據，
>
> 並意圖使該器材、電腦密碼、取用碼或數據用作干犯第二至五條所訂任何罪行；及
>
> b 管有上文 a i 或 ii 段所提述的物品，並意圖使該物品用作干犯第二至五條所訂任何罪行。任何締約方可依法規定須管有一定數量的這類物品，方會招致刑事法律責任。
>
> 2 如本條第 1 段所提述的生產、出售、為使用而獲取、輸入、分發或以其他方式提供或管有，並非以

---

11 第 2.11、3.12 及 4.13 段。

12 有關《布達佩斯公約》的背景資料，見導言第 11 段，以及第 1 章第 1.6 至 1.10 段。

13 本章所論述罪行涵蓋的器材，亦可能構成無線電通訊器具，故須受《電訊條例》（第 106 章）的發牌制度所規限。

干犯本《公約》第二至五條所訂罪行為目的（例如是為了在獲授權下測試或保護電腦系統），則本條不得解釋為施加刑事法律責任。

3 各締約方可保留不應用本條第 1 段的權利，但該項保留不得涉及出售、分發或以其他方式提供本條第 1 a ii 段所提述的物品。”

6.21 《說明報告》對第六條的評註如下：

“71. 本條將蓄意作出關乎某些可被誤用作干犯……〔《布達佩斯公約》第二至五條所訂〕……罪行的器材或取用數據的特定非法作為，另行規定為獨立的刑事罪行。由於犯這些罪行往往需要管有取用方法（‘黑客工具’）或其他工具，因此獲取該等工具作犯罪之用的誘因強烈，以致可能形成一種生產及分發該等工具的黑市……

72. 第 1(a)1 段把生產、出售、為使用而獲取、輸入、分發或以其他方式提供……器材……定為罪行。‘分發’指將數據轉發給他人的主動作為，‘提供’則指將器材放在網上供他人使用……所包括的‘電腦程式’指以下例子：經設計以更改甚至銷毀數據或干擾系統操作的程式……或經設計或改裝以取用電腦系統的程式。

73. 草擬人員曾詳盡討論，應否將有關器材限於經設計為專門或特別用作犯罪的器材……有意見認為這樣是過於狹窄……至於把所有（即使是合法生產及分發的）器材納入涵蓋範圍的替代方案，亦遭否決。只有意圖干犯電腦罪行這項主觀元素，將成為判處刑罰的決定性因素……《公約》將其範圍限於涉及經客觀設計或改裝以主要用作犯罪的器材的案件……

74. 第 1(a)2 段把生產、出售、為使用而獲取、輸入、分發或以其他方式提供可藉以取用整個電腦系統或其任何部分的……數據，定為罪行。

75. 第 1(b)段把管有列於第 1(a)1 或 1(a)2 段的物品定為罪行。締約方獲准……依法規定管有一定數量的這類物品。所管有物品的數量，可直接證明有犯罪意圖……

76. 該罪行須是在無權的情況下蓄意干犯的……還須有特定（即直接）意圖，將有關器材用作干犯《公約》第二至五條所訂任何罪行。

77. 第 2 段清楚列明，為了在獲授權下測試或保護電腦系統而製作的工具，並不受該條所涵蓋……

78. ……第 3 段容許締約方根據所作保留……在本土法律中規限該罪行的範圍。然而，各締約方有責任至少把出售、分發或提供第 1 (a) 2 段所述的……數據，定為罪行。”[14]

其他司法管轄區的法定體制

澳大利亞

《刑事法典》（聯邦）第 478.3 條

6.22 澳大利亞《刑事法典》（聯邦）（Criminal Code (Cth)）第 478.3 條（*“管有或控制數據，並意圖干犯電腦罪行”*）訂有一項與本章相關的罪行：

> “(1) 任何人在以下情況，即屬犯罪：
>
> (a) 該人管有或控制數據；及
>
> (b) 該人作出該項管有或控制的意圖，是使該等數據被該人或他人：
>
> (i) 用作干犯違反第 477 分部的罪行；或
>
> (ii) 用作利便干犯該罪行。
>
> 刑罰：監禁 3 年。
>
> (2) 即使干犯違反第 477 分部的罪行並不可能，任何人仍可被裁定犯違反本條的罪行。

[14] 《說明報告》第 71 至 78 段。

企圖犯罪不屬犯罪

(3) 企圖干犯違反本條的罪行，不屬犯罪。

管有或控制數據的涵義

(4) 在本條中，凡提述某人管有或控制數據，即包括提述該人：

(a) 管有任何存有或載有該等數據的電腦或數據儲存器材；或

(b) 管有任何記錄該等數據的文件；或

(c) 控制存於他人管有的電腦內的數據(不論是在澳大利亞境內或境外)。”

6.23 《刑事法典》(聯邦)第 478.3(1)(b)(i)條所提述的第 477 分部(*“嚴重電腦罪行”*)，包括：

(a) 第 477.1 條(*“在未獲授權下作出取覽、修改或損害，並意圖干犯嚴重罪行”*)；

(b) 第 477.2 條(*“在未獲授權下修改數據，以導致損害”*)；及

(c) 第 477.3 條(*“在未獲授權下損害電子通訊”*)。

這些罪行實質上與第 2 至 5 章所論述的建議罪行相對應。

《刑事法典》(聯邦)第 478.4 條

6.24 除《刑事法典》(聯邦)第 478.3 條外，第 478.4 條(*“生產、供應或取得數據，並意圖干犯電腦罪行”*)亦與本章相關。這兩項條文的結構相類似：

“(1) 任何人在以下情況，即屬犯罪：

(a) 該人生產、供應或取得數據；及

(b) 該人作出上述作為的意圖，是使該等數據被該人或他人：

(i) 用作干犯違反第 477 分部的罪行；或

(ii) 用作利便干犯該罪行。

刑罰：監禁 3 年。

(2) 即使干犯違反第 477 分部的罪行並不可能，任何人仍可被裁定犯違反本條的罪行。

企圖犯罪不屬犯罪

(3) 企圖干犯違反本條的罪行，不屬犯罪。

生產、供應或取得數據的涵義

(4) 在本條中，凡提述某人生產、供應或取得數據，即包括提述該人：

(a) 生產、供應或取得存於或載於電腦或數據儲存器材內的數據；或

(b) 製作、供應或取得記錄該等數據的文件。”

6.25 第 478.3 及 478.4 條源於《示範法典委員會報告書》*“為配合”《布達佩斯公約》“第六條的規定”*而建議的《示範刑事法典》（Model Criminal Code）第 4.2.7 及 4.2.8 條。[15] 第 478.3 及 478.4 條所訂立的罪行成為一組，具有以下共通點：

(a) 兩項罪行均規定須有以下意圖：被告人或他人將數據用作干犯違反《刑事法典》（聯邦）第 477 分部的罪行，或將數據用作利便干犯該罪行。罔顧後果或僅是知悉數據可用作上述目的，並不足夠。

(b) 兩項罪行均只針對數據，而非針對任何實物。然而，兩者均把管有或控制數據（第 478.3 條）或生產、供應或取得數據（第 478.4 條），界定為包括某些涉及有形物的情境。

15 《示範法典委員會報告書》第 92 頁。

加拿大

《1985 年刑事法典》第 342.1(1)條

6.26 第 2 及 3 章曾提及加拿大《1985 年刑事法典》(Criminal Code 1985)第 342.1(1)條(*"在未獲授權下使用電腦"*)。[16] 第 342.1(1)(d)條訂明,任何人:

> "意圖欺詐並在無表面權利的情況下……使用、管有、非法傳送或准許他人取覽某電腦密碼,而該密碼會使某人能夠干犯(a)、(b)或(c)段所訂罪行",

即屬犯罪。

6.27 第 342.1(1)(a)、(b)及(c)條分別處理:

(a) 取得任何電腦服務;

(b) 截取某電腦系統的任何功能;及

(c) 使用某電腦系統,意圖干犯(a)或(b)段所訂罪行,或就電腦數據或某電腦系統干犯第 430 條所訂罪行。

6.28 根據第 342.1(2)條,就電腦密碼而言,*"非法傳送"*指*"出售、從加拿大輸出、向加拿大輸入、分發或以任何其他方式處理"*。該條把*"電腦密碼"*界定為*"任何可藉以取得電腦服務或使用電腦系統的電腦數據"*。該定義範圍雖廣,但顯然不包括比如有關利用漏洞的專門知識。

《1985 年刑事法典》第 342.2(1)條

6.29 若要更廣泛地規管用作干犯電腦網絡罪行的*"器材"*,便須改用第 342.2(1)條(*"為在未獲授權下使用電腦系統或導致損害而管有器材"*)。根據該條,任何人:

> "無合法辯解而製造、管有、出售、要約出售、輸入、為使用而取得、分發或提供經設計或改裝以主要用作干犯第 342.1 或 430 條所訂罪行的任何器材,並知悉該器材已用作或擬用作干犯該罪行",

即屬犯罪。

---

16 第 2.28 及 3.40 段。

6.30 第 342.2(4)條以非盡列無遺的方式，將 *"器材"* 界定為包括 *"(a)某器材的零件；及(b)第 342.1(2)款所指的電腦程式"*。就 *"器材"* 一詞而言，某評論員引用兩宗案例，[17] 並提出以下評析：

> "該條通常不適用於諸如並非**主要**為干犯相關罪行而設計的電腦等物品。然而，法院曾經裁定，該條適用於為了記錄與信用卡帳戶有關的個人身分號碼而安裝的數碼攝像機。"[18]（強調之處乃原文所有）

6.31 第 342.2(1)條的措辭與第 327(1)條（*"管有器材以取得使用電訊設施或服務"*）相同，但後者適用於：

> "經設計或改裝以主要用作在沒有支付合法費用下使用電訊設施或取得電訊服務的任何器材"。

《1985 年刑事法典》第 191(1)條

6.32 我們還應提述第 191(1)條（*"管有等"*），該條是關乎截取通訊（而非電腦網絡罪行）的條文。根據第 191(1)條，任何人：

> "管有、出售或購買任何電磁、聲音、機械或其他器材或其任何零件，並知悉該器材的設計使該器材主要對暗中截取私人通訊有用"，

即屬犯罪。

6.33 第 191(1)及 342.2(1)條均引入某器材的*主要*用途這個概念，而關乎電腦密碼的第 342.1(1)(d)條則沒有此概念。

英格蘭及威爾斯

《英格蘭誤用電腦法令》第 3A 條

6.34 在英格蘭及威爾斯，《2006 年警察及司法法令》（Police and Justice Act 2006）第 37 條在《英格蘭誤用電腦法令》加入新的第 3A 條。制定為《2006 年警察及司法法令》的法案的註釋，概述該新訂條文，並如下解釋條文的背景：

---

17 *R v Singh* 2006 ABPC 156 及 *R v Coman* 2004 ABPC 18。

18 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 140 頁。

"302. ……新訂條文訂立三項新罪行，各項罪行一經循公訴程序定罪，可處監禁兩年或罰款，或兩者兼處。這些罪行是：

- 製造、改裝、供應或要約供應某物品，意圖使該物品用作干犯(或用作協助干犯)第 1 條[19] 或第 3 條[20] 所訂罪行（新訂條文的第(1)款）；

- 供應或要約供應某物品，並相信該物品相當可能會被如此使用（第(2)款）；

- 取得某物品，以使該物品被供應作如此使用（第(3)款）。

如任何人就多項物品而被控第(2)款所訂罪行，控方便須就該等物品中任何一件或多於一件特定物品，證明其案情屬實。若只證明該人相信某部分涉案物品相當可能會在與第 1 或 3 條所訂罪行有關連的情況下使用，並不足夠。

303. 訂立這些新罪行的背景，是由於電子工具（例如可用作對電腦系統進行黑客入侵的'黑客工具'）現成市場不斷擴張，而且越來越多人在與有組織罪行有關連的情況下，使用這類工具。此外，《2001 年歐洲委員會電腦網絡罪行公約》（2001 Council of Europe Cybercrime Convention）第 6(1)(a)條規定，須把分發或提供可藉以取用電腦系統的電腦密碼或類似數據，並意圖犯罪這行為定為罪行。這些新罪行是為了實施這項規定而訂立的……。"

6.35 《英格蘭誤用電腦法令》加入第 3A 條後，《2015 年嚴重刑事罪行法令》（Serious Crime Act 2015）第 41(2)條在《英格蘭誤用電腦法令》加入第 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"*），第 4 及 5 章已論述該條。[21] 因此，第 3A 條提述 *"第 1、3 或 3ZA 條所訂罪行"*，作為意圖使用某 *"物品"* 而干犯的罪行。此外，《2015 年嚴重刑事罪行法令》第 42 條亦擴大了《英格蘭誤用電腦法令》第 3A(3)條的範圍。

---

19 在未獲授權下取覽電腦資料。

20 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。

21 第 4.41 及 5.34 段。

6.36　經上述修訂後，《英格蘭誤用電腦法令》第 3A 條（*"製造、供應或取得用於第 1、3 或 3ZA 條所訂罪行的物品"*）的現行內容如下：

"(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。

(5) 任何人犯本條所訂罪行——

(a) 一經在英格蘭及威爾斯循簡易程序定罪，可處為期不超過 12 個月的監禁或不超過法定最高罰款，或兩者兼處；

(b) 〔……〕

(c) 一經循公訴程序定罪，可處為期不超過 2 年的監禁或罰款，或兩者兼處。"

有關罪行的範圍

6.37 《英格蘭誤用電腦法令》實施 30 年後，部分社會人士開始提倡改革該法令。[22] 舉例而言，某跨行業組織在其報告書中認為，第 3A 條有 *"過度刑事化的顯著風險"*，[23] 並對此闡述如下：

> "3.54 ……首先，《誤用電腦法令》第 3A 條沒有將'物品'局限於為用作犯罪而設計或製作的物品，更遑論將'物品'局限於'主要'為該目的而設計或製作的物品。即是說，只要有關事物用作犯罪，就連虛擬私有網絡軟件（VPN）及讓通訊得以安全進行的洋蔥路由器（the onion router，簡稱 Tor）亦會納入該罪行的範圍內……
>
> 3.55 第二，如有關行為是供應或要約供應工具，第 3A 條只規定須證明某人'相信相當可能'該等工具會被非法使用……這較廣泛的意念元素的主要問題，在於所有保安及威脅研究人員均**知悉**（而非僅是相信）不法之徒'相當可能'會使用黑客工具或像 VPN 這樣的匿名工具來利便犯罪，因此，保安及威脅研究人員也會落入該罪行的範圍內。
>
> 3.56 第三，第 3A 條並無提及……正當理由……
>
> 3.57 第四，第 3A 條並沒有將管有單獨定為罪行。管有只是作為其他行為（即製造、供應、要約供應及取得）的一部分而間接獲視為罪行……
>
> 3.58 這些規定的綜合效果，是令那些同時供應或要約供應具有雙重用途的黑客工具、VPN 及 Tor 的人，及／或那些取得該等工具以作自用或供應予他人的人，受第 3A 條約束。以下人士也會因而落入該罪行的範圍內：保安及威脅情報研究人員；可能取得 VPN 或 Tor 以確保通訊安全的舉報者，以便他們透露在未獲授權下取覽的數據（《誤用電腦法令》第 1 條）；以及供應這類工具（例如 SecureDrop）並相信有關工具會用作收取數據（特

---

22 例子見 Cyber Up 運動，網址為 https://www.cyberupcampaign.com/cma-30th-birthday（於 2022 年 5 月 3 日瀏覽）。

23 Criminal Law Reform Now Network, *Reforming the Computer Misuse Act 1990*（2020 年），第 2 章，第 4.23 段，登載於 http://www.clrnn.co.uk/publications-reports/（於 2022 年 5 月 3 日瀏覽）。

別來自舉報者的數據)的新聞工作者(第 3A(2)條)。”[24]
(強調之處乃原文所有)

展示成功執法的案例

6.38 以上負面評論並不適用於犯罪者明顯難逃其責的情況。在 *R v Lewys Martin*[25] 這宗相關案件,被告人承認多項控罪,包括兩項根據第 3A 條提出的控罪,這兩項控罪關乎被告人電腦上兩項名為 Jaindos 及 CyberGhost 的程式。Jaindos 可發動拒絕服務攻擊,CyberGhost 則可提供具誤導性的互聯網規約地址位置資料,讓使用者匿名。

《2006 年欺詐罪法令》第 6 及 7 條

6.39 《2006 年欺詐罪法令》(Fraud Act 2006)第 8(1)條界定第 6 條(*“管有用作欺詐的物品等”*)及第 7 條(*“製造或供應用作欺詐的物品”*)中 *“物品”* 一詞的方式,與《英格蘭誤用電腦法令》第 3A(4)條相同,即包括 *“以電子形式所存的任何程式或數據”*。因此,在某程度上,《2006 年欺詐罪法令》第 6 及 7 條顯然與《英格蘭誤用電腦法令》第 3A 條互相重疊。

6.40 上述對過度刑事化風險不滿的跨行業組織,將這些條文比較如下:

> “從檢控人員的角度來看,要根據〔《英格蘭誤用電腦法令》〕第 3A 條提出控罪,看來須證明有關物品可用作干犯第 1 或 3〔或 3ZA〕條所訂罪行。若採用《2006 年欺詐罪法令》第 6 或 7 條,便須證明有關工具可用作干犯欺詐罪……”[26]

《2003 年通訊法令》第 126 條

6.41 為求完整,以下條文值得一提:

(a) 《2003 年通訊法令》(Communications Act 2003)第 126(1)條將以下行為定為不合法:管有或控制可用作取得電子通訊服務,或管有或控制可在與取得該服務有關連的情況下使用的任何事物,並意圖以第 126(3)條所詳述的方式誤用該事物;及

---

24 同上,第 2 章,第 3.54 至 3.58 段。
25 [2014] 1 Cr App R (S) 63.
26 見上文註腳 23,第 1 章,第 4.6 段。

(b) 第 126(2)條訂立以下罪行：供應或要約供應同類事物，並知悉或相信其收取人意圖以第 126(3)條所詳述的方式誤用該事物。

6.42 《2003 年通訊法令》第 126(3)條提述某人的下述意圖：

(a) 使用有關事物，以不誠實地取得電子通訊服務；

(b) 將有關事物用作與不誠實地取得上述服務有關連的目的；

(c) 不誠實地容許將該事物用作取得上述服務；或

(d) 容許將該事物用作與不誠實地取得上述服務有關連的目的。

中國內地

6.43 《中國刑法》第二百八十五條第三款載有以下罪行：

> "提供專門用於侵入、非法控制計算機信息系統的程序、工具，或者明知他人實施侵入、非法控制計算機信息系統的違法犯罪行為而為其提供程序、工具，情節嚴重的，依照前款的規定處罰。"
>
> （底線後加）

6.44 就提供程序或工具，第二百八十五條第三款訂有兩部分，即(i)*"專門用於"*侵入、非法控制計算機信息系統，以及(ii)明知他人會將程序或工具用於該等目的。

6.45 關於第一部分，根據法釋〔2011〕19 號第二條，具有下列情形之一的程序、工具，應當認定為第二百八十五條第三款規定的*"專門用於侵入、非法控制計算機信息系統的程序、工具"*：

> "（一）具有避開或者突破計算機信息系統安全保護措施，未經授權或者超越授權獲取計算機信息系統數據的功能的；
>
> （二）具有避開或者突破計算機信息系統安全保護措施，未經授權或者超越授權對計算機信息系統實施控制的功能的；

（三）其他專門設計用於侵入、非法控制計算機信息系統、非法獲取計算機信息系統數據的程序、工具。”

6.46 至於第二部分，如被告人明知他人會將本屬中性的程序或工具用於侵入、非法控制計算機信息系統，則提供該程序或工具亦可干犯該罪行。因此，該部分除要求須證明有《中國刑法》第十四條所規定的意圖外，還要求證明知悉這項額外意念元素。

6.47 《中國刑法》第二百八十六條第三款是另一項相關罪行條文：

“故意製作、傳播計算機病毒等破壞性程序，影響計算機系統正常運行，後果嚴重的，依照第一款的規定處罰。”

（底線後加）

6.48 根據法釋〔2011〕19號第五條，具有下列情形之一的程序，應當認定為*“計算機病毒等破壞性程序”*：

“（一）能夠通過網絡、存儲介質、文件等媒介，將自身的部分、全部或者變種進行複製、傳播，並破壞計算機系統功能、數據或者應用程序的；

（二）能夠在預先設定條件下自動觸發，並破壞計算機系統功能、數據或者應用程序的；

（三）其他專門設計用於破壞計算機系統功能、數據或者應用程序的程序。”

新西蘭

《新西蘭法令》第 251 條

6.49 《新西蘭法令》第251條（*“製作、出售、分發或管有用作犯罪的軟件”*）訂立兩項罪行，該等罪行關乎令人能夠在未獲授權下取用電腦系統的軟件或其他資料。

6.50 第251(1)條訂立首項罪行。該條側重於上述軟件或資料的供應層面，將任何人（“**甲方**”）的以下作為定為不合法：

(a) 邀請另一人獲取上述軟件或資料；或

(b) 要約出售或要約供應該軟件或資料，或為出售或供應而展示該軟件或資料；或

(c) 同意出售或供應該軟件或資料；或

(d) 出售或供應該軟件或資料；或

(e) 為出售或供應而管有該軟件或資料，

前提是甲方：

(i) 知悉該軟件或資料的唯一或主要用途，是用作犯罪；或

(ii) 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（不論甲方是否也宣傳該軟件或資料對任何其他目的有用）。

6.51 第 251(2)條則針對需求層面，將管有上述軟件或資料並意圖用它犯罪，定為第二項罪行。

6.52 第 251(1)及(2)條均提述可能犯 *"罪"*。這似乎可以是任何性質的罪行，而無須是電腦網絡罪行。

《新西蘭法令》第 216D 條

6.53 第 216D(1)條（*"禁止處理截取器材等"*）亦與本章相關。該條所禁止的作為與第 251(1)條所指明的作為（列於上文）相同，但第 216D(1)條關乎符合以下說明的任何 *"截取器材"*：

(a) 任何人知悉該截取器材的唯一或主要目的，是暗中截取私人通訊；或

(b) 該人表示該截取器材對暗中截取私人通訊有用（不論該人是否也表示該截取器材對任何其他目的有用）。

6.54 根據第 216A(1)條，*"截取器材"*指：

> "用於或可用於截取私人通訊的任何電子、機械、電磁、光學或光電工具、器具、設備或其他器材"

但不包括助聽器或相類器材，或獲總督豁免的器材。

6.55 《新西蘭法令》第 216D(1)(ii)及 251(1)(b)條將宣傳或表示某軟件、資料或截取器材對非法目的有用的行為，定為不合法。有學者就第 251(1)(b)條提出以下看法，而該看法同樣也適用於第 216D(1)(ii)條：

> "實際上，該條的目標徒勞無益。任何人只需為可能屬非法的程式宣傳用作某種合法目的，餘下的留給別人想像便可。"[27]

6.56 上述批評看來理據充分。假設被告人沒有作出上述宣傳或表示，控方便需要依賴（第 216D(1)(i)條或第 251(1)(a)條所訂的）交替法律責任基礎，即被告人知悉該軟件或資料的唯一或主要用途，是用作犯罪，或被告人知悉該截取器材的唯一或主要目的，是暗中截取私人通訊（視乎屬何情況而定）。

新加坡

《新加坡誤用電腦法令》第 8 條

6.57 《1998 年誤用電腦（修訂）法令》（Computer Misuse (Amendment) Act 1998，1998 年第 21 號）第 7 條在《新加坡誤用電腦法令》加入新的第 6B 條，該條現已重編為第 8 條（*"在未獲授權下披露取用碼"*），內容如下：

> "(1) 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。
>
> (2) 任何人犯第(1)款所訂罪行，一經定罪——
>
> (a) 可處不超過$10,000 的罰款或為期不超過 3 年

---

27 David Harvey, *internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015)，第 7.112 段。

的監禁，或兩者兼處；及

(b) 如屬第二次或其後每次定罪，則可處不超過$20,000的罰款或為期不超過5年的監禁，或兩者兼處。”

《新加坡誤用電腦法令》第10條

6.58 《2017年誤用電腦及電腦網絡安全（修訂）法令》（Computer Misuse and Cybersecurity (Amendment) Act 2017）第3條進一步在《新加坡誤用電腦法令》加入新的第10條（*“取得用於某些罪行的物品等”*），其規定如下：

“(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。

(3) 任何人犯第(1)款所訂罪行，一經定罪——

(a) 可處不超過$10,000的罰款或為期不超過3年的監禁，或兩者兼處；而

(b) 如屬第二次或其後每次定罪，則可處不超過$20,000的罰款或為期不超過5年的監禁，或兩者兼處。”

6.59 《新加坡誤用電腦法令》第8(1)及10(1)(b)條看來有部分互相重疊。控方或須決定案件應根據哪一條處理。在現實中，這大概不會對被告人造成不公，因為該兩條所訂的最高刑罰相同。由於我們會在下文建議新法例應以《新加坡誤用電腦法令》第8及10條為藍本，[28]因此可能有空間將這些條文重組或合併，以訂立一個更井然有序的法律體制。這方面留待法律草擬專員決定。

與《示範法》作比較

6.60 《新加坡誤用電腦法令》第10條另一值得注意的特點是，該條指明適用物品時所採用的措辭，近似《示範法》第9條（*“非法器材”*），但比後者範圍更廣。以下列出《示範法》第9(1)條，以作比較：

“任何人在以下情況，即屬犯罪：

(a) 該人無合法辯解或理由而蓄意或罔顧後果地生產、出售、為使用而獲取、輸入、輸出、分發或以其他方式提供：

(i) 經設計或改裝以用作干犯違反第5、6、7或8條的罪行的器材（包括電腦程式）；或

(ii) 可藉以取用整個電腦系統或其任何部分的電腦密碼、取用碼或類似數據；

並意圖使該器材、電腦密碼、取用碼或數據被任何人用作干犯違反第5、6、7或8條的罪行；或

(b) 該人管有(a)(i)或(a)(ii)節所提及的任何物品，並意圖使該物品被任何人用作干犯違反第5、6、7或8條的罪行。”

---

28 第6.88(b)段。

美國

《電腦欺詐及濫用法案》內的《美國法典》第 18 篇第 1030(a)(6)條

6.61 根據《美國法典》第 18 篇第 1030(a)(6)條，任何人：

> "意圖欺詐並故意非法傳送（定義見第 1029 條）任何密碼或類似資料，而透過該密碼或資料可在未獲授權下取用電腦，如——
>
> (A) 該非法傳送會影響州際或對外貿易；或
>
> (B) 有關電腦是由美國政府所使用或為美國政府而使用的"，

即可按《美國法典》第 18 篇第 1030(c)條的規定予以懲處。

6.62 根據《美國法典》第 18 篇第 1029(e)(5)條的定義，*"非法傳送"*指*"轉讓予另一人或以其他方式處置而轉予另一人，或意圖作出轉讓或處置而取得控制"*。

6.63 有關法例並無界定*"可透過密碼或類似資料，在未獲授權下取用電腦"*。該用語的慣常涵義包括登入憑證等資料，而視乎*"類似"*一詞應如何解釋，大概亦會包括有關利用漏洞的專門知識。然而，該用語是否涵蓋用作在未獲授權下取用電腦的軟件，則似乎有商榷餘地。

《美國法典》第 18 篇第 1029 條

6.64 無論如何，《美國法典》第 18 篇第 1030(a)(6)條不適用於實物這觀點，應不受爭議。《美國法典》第 18 篇第 1029(a)條反而就多種行為訂立十項獨立罪行，其中包括管有、生產、使用及販運*"取用器材"*。

6.65 以下是《美國法典》第 18 篇第 1029(e)(1)條中*"取用器材"*的定義，該定義包括有形物及無形物：

> "可單獨使用或與其他取用器材一併使用，以取得金錢、貨物、服務或任何其他有價值事物，或可用作提出資金轉帳（僅藉紙本文書作出的轉帳除外）的任何卡、字牌、代碼、帳戶號碼、電子編號、流動識別號碼、個

人身分號碼，或其他電訊服務、設備或工具標識，或其他取用帳戶的方法”。

6.66 對於《美國法典》第 18 篇第 1029 條的一些典型適用範圍，美國司法部電腦罪行及知識產權組（Computer Crime and Intellectual Property Section）解釋如下：

> “檢控人員通常會根據第 1029 條，對多種‘仿冒詐騙（phishing）’案件及‘使用失竊卡資料（carding）’案件提出檢控，前者涉及被告人使用詐騙電郵取得銀行帳戶號碼及密碼，後者則涉及被告人購買、出售或轉讓盜取的銀行帳戶、信用卡或扣帳卡資料。”[29]

《美國法典》第 18 篇第 2512 條

6.67 除《美國法典》第 18 篇第 1029 條外，*“器材”*一詞亦出現在《美國法典》第 18 篇第 2512(1)條，該條本質上禁止任何人蓄意製造、分發、管有和宣傳：

> “任何電子、機械或其他器材，而該人知悉或有理由知悉該器材的設計使該器材主要對暗中截取有線、口頭或電子通訊有用”。

6.68 《美國法典》第 18 篇第 2512(1)條對某器材的主要用途（而非比如是唯一用途或可能用途）的提述，亦見於《布達佩斯公約》第六條、[30] 加拿大《1985 年刑事法典》第 191(1)及 342.2(1)條，[31] 以及《新加坡誤用電腦法令》第 10(2)(a)條[32]（這些條文均於上文論述）。

小組委員會的看法

應訂立兼具基本及加重形式的新罪行

6.69 現時，《刑事罪行條例》（第 200 章）第 60 及 62 條共同把刑事損壞定為不合法。如按建議 6(c)所提議，將該條例關於 *“誤用電*

---

29 H Marshall Jarrett, Michael W Bailie, Ed Hagen and Scott Eltringham, *Prosecuting Computer Crimes* (Office of Legal Education, Executive Office for United States Attorneys, 2nd edition, 2010)，第 102 至 103 頁，登載於 https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf（於 2022 年 5 月 3 日瀏覽）。

30 第 6.20 段。

31 第 6.29 及 6.32 段。

32 第 6.58 段。

腦”的條文改列於新法例，在新法例加入與第 62 條[33] 相對應的條文，實屬正確之舉。我們亦認為，該條文亦應適用於第 2 至 5 章所論述的全部四類依賴電腦網絡的罪行。

6.70 在討論過程中，我們設法解決兼具合法及非法用途的器材及數據所帶來的挑戰。第 6.3(c)段所提及的消磁器便是一例，財務機構會使用消磁器清除舊硬碟的內容，以策安全。我們相信，在該情況下管有消磁器不會引起任何問題，這點無可爭議。相反，如管有消磁器並意圖將它用作非法目的（例如破壞），施加刑事法律責任則屬合理。

6.71 在現實世界中，*“攻擊性武器”*這概念亦有同樣的考慮。根據《公安條例》（第 245 章），*“攻擊性武器”*[34] 的定義區分以下物品：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、*“適合”*[35] 用作造成傷害的物品，或 *“擬供”*用作造成傷害的物品。在應用該定義時：

(a) 在涉及例如下述物品的案件中，無須證明犯罪意圖。純粹在公眾地方管有下述物品，便足以招致刑事法律責任：

(i) 槍、開山刀或蝴蝶刀（因為以性質而論，這類物品屬 *“被製造……以用作傷害他人”*）；或

(ii) 裝有刺刀的雨傘，或削尖並裝有尖釘的手杖（因為該雨傘或手杖已被“改裝”以用作造成傷害）。

(b) 然而，鑑於比如水果刀或“瑞士軍刀”這類物品本屬中性，有關物品只有在 *“由管有或控制該物品的人擬將之作攻擊性用途”*的情況下，方屬攻擊性武器。

6.72 借鏡上述分類方法，我們認為應把建議的罪行分為基本及加重兩種形式。在個別案件中，除了根據某器材或數據是否被製造或改

---

33 *“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。”

34 第 2(1)條將 *“攻擊性武器”*界定為：
“任何被製造或改裝以用作傷害他人，或適合用作傷害他人的物品，或由管有或控制該物品的人擬供其本人或他人作如此用途的任何物品”。

35 在 *R v Chong Ah Choi & Ors* [1994] 3 HKC 68, HCMA 281/1994（判決日期：1994 年 10 月 4 日），上訴法庭基本上裁定（第 7G 段），*“攻擊性武器”*定義中 *“適合”*用作造成傷害的部分應不再適用。

裝以用作非法用途，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（例如已有人開始利用圖像卡來挖掘加密貨幣），故單靠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。

建議罪行所應適用的器材及數據

就建議罪行的基本及加重形式而言

6.73 電腦網絡罪行可藉實物器材而干犯，但沒有實物器材亦可干犯有關罪行。舉例而言，在網上故意散布勒索軟件已可造成破壞。將勒索軟件、病毒、其源碼及類似事物稱為電腦網絡武器，其實也不為過。為確保能在電腦網絡空間有效執行建議的罪行，我們認為該罪行應適用於有形物及無形物。

6.74 另一方面，鑑於已有新西蘭法例作為先例，[36] 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。

6.75 我們也考慮過建議的罪行應否適用於主要用作犯罪的器材或數據，不論該器材或數據能否用作任何合法目的。我們認為，建議的罪行若只適用於沒可能有任何合法用途的器材或數據，會過於局限。同樣道理，不論被告人的主觀意圖，任何器材或數據的主要用途，應以客觀方式界定。總的來說，我們認為建議的罪行應適用於主要用作（以客觀方式界定）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。

6.76 我們亦曾討論，建議的罪行應否適用於獲相信或聲稱能夠（但實際上不能）用作犯罪的器材或數據，例如：

(a) 不正確的密碼；或

(b) 據稱能夠在十分鐘內破解密碼的破解密碼工具，但由於該工具設計不良或有缺陷，經過長久得多的時間後，該工具仍未能破解密碼。

6.77 鑑於《刑事罪行條例》（第 200 章）第 62 條並無明確規定有關物品須實際上能夠摧毀或損壞財產，我們總結認為，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

---

36 見第 6.50 及 6.51 段，當中提述《新西蘭法令》第 251(1)及(2)條。

屬實，亦應足以構成罪行。此立場符合我們基於*朱峻瑋*案所達成的共識，即刑事法律責任不應取決於網絡攻擊成功與否。

就基本罪行而言

6.78 我們亦建議：

(a) 基本罪行應涵蓋被製造或改裝以用作犯罪的器材或數據；及

(b) 應依據有關器材或數據的主要用途（以客觀方式界定，不論被告人的主觀意圖為何）評估是否符合(a)項的準則。

6.79 同時，我們建議的做法，將本屬中性（例如上文所論述的消磁器）[37] 但被意圖用作導致傷害的器材或數據排除在外，原因是如沒有該意圖，似乎沒有理由將有關行為定為罪行。相反，如有該意圖，加重罪行便會適用。

就加重罪行而言

6.80 基於上文所解釋的看法，我們建議加重罪行應適用於能夠用作犯罪的器材或數據，或犯罪者相信或聲稱能夠用作犯罪的器材或數據。

犯罪行為

6.81 《布達佩斯公約》的《說明報告》[38]，以及制定為《2006年警察及司法法令》的法案的註釋，[39] 均提到存在*"黑客工具"*及相類工具的市場。為確保法例周全起見，我們相信因應該類市場的蓬勃發展而採取的法定措施，必須針對市場各類參與者，不論他們是該市場的供應方還是需求方。

6.82 因此，我們的建議是，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。

---

37 第 6.70 段。

38 第 6.21 段所引述的《說明報告》第 71 段。

39 第 6.34 段所引述的註釋第 303 段。

犯罪意念

就建議罪行的基本及加重形式而言

6.83 我們認為，任何人應僅在蓄意提供或管有上文所述的器材或數據的情況下，方屬犯罪。由於很多人都管有軟件或電腦數據，甚至在自己不察覺的情況下向他人提供軟件或電腦數據，若採用較低的門檻——比如只須罔顧後果，或者完全無須有任何特定意念，似乎不宜。舉例而言：

(a) 不法之徒可遙距對不知情人士的電腦植入惡意軟件或數據。

(b) 某人可能管有已受到惡意軟件感染的電腦檔案，但對此毫不知情。該人可能把該檔案上載至網上儲存空間，以為只有自己才能檢索該檔案。在現實中，該儲存空間的管理人相當可能可取覽該檔案。如該儲存空間不受保護或所受保護不足，該檔案甚至可供整個互聯網社群取覽。

如有關罪行沒有規定必須知悉，而單是罔顧後果，或不論被告人的意念如何，亦足以干犯該罪行，該罪行便可能適用於上文情境(a)中毫不知情的人士，以及情境(b)所述的人。該罪行的適用範圍似乎會過於廣闊。

就基本罪行而言

6.84 如任何人因相信[40]有關器材或數據可用作犯罪而被控基本罪行，該信念即構成須由控方證明的犯罪意念之一部分。

就加重罪行而言

6.85 如任何人被控加重罪行，按照定義，除了須證明上文第 6.83 及 6.84 段所論述的犯罪意念的所有其他方面外，還須證明該人意圖將有關器材或數據用作犯罪。

建議讓合理辯解作為法定免責辯護

6.86 在公眾地方管有攻擊性武器並不構成犯罪，前提是具有*"合法權限或合理辯解"*[41]（例如管有人在表演藝術時使用長兵器）。

---

40 第 6.76 至 6.77 段。

6.87 我們認為，建議的罪行應同樣加入合理辯解這項法定免責辯護，因為任何人或機構可以有各種合法理由而需要可用作犯罪的器材或數據。我們認為，建議的免責辯護，有助避免像上述批評《英格蘭誤用電腦法令》的跨行業組織所談及的過度刑事化問題。[42]

建議條文的藍本

6.88 上文所審視的其他司法管轄區，在草擬罪行方面差異甚大，顯示多種不同的可能性。在擬定香港的新法例時，我們提議借鑑以下條文，並將它們加以完善：

(a) 《英格蘭誤用電腦法令》第 3A 條；及

(b) 《新加坡誤用電腦法令》第 8 及 10 條。

6.89 我們曾詳加考慮，*"管有"*這概念是否切合建議的罪行擬適用於數據等無形物的用意。說明*"管有"*這法律概念性質的案例，現確立已久。*Archbold Hong Kong 2021* 的以下段落，描述了該概念的要素：

> "如有足夠證據證明某人實質控制某事物，即該人有能力在可行範圍內及法律規限下，隨意使用該事物並有能力禁止他人使用該事物，亦有意圖行使該控制權，該人便可被裁定為管有該事物。"[43]
>
> （底線後加）

6.90 換言之，*"管有"*表示有權控制某事物，而該事物並非必定是有形的。事實上，就其他法例而言，*"管有"*亦已特別適用於涉及電腦程式或數據的罪行，例如是《版權條例》（第 528 章）所訂的管有侵犯版權物品罪，[44] 以及《防止兒童色情物品條例》（第 579 章）所訂的管有兒童色情物品罪。[45] 另外，據我們觀察，在我們所比較研究的部分司法管轄區，*"管有"*亦適用於同屬無形物的數據、資料、

---

41 《公安條例》（第 245 章）第 33(1)條。

42 第 6.37 段。

43 *Archbold Hong Kong 2021*，第 29 – 39 段。

44 根據《版權條例》（第 528 章）第 118(2A)條，任何人如*"未獲本款適用的版權作品的版權擁有人的特許，而為任何貿易或業務的目的或在任何貿易或業務的過程中，管有該作品的侵犯版權複製品，以期令某人可為該貿易或業務的目的或在該貿易或業務的過程中，使用該侵犯版權複製品"*，即屬犯罪。憑藉第 118(2B)條，第 118(2A)條亦保障屬"電腦程式"的版權作品。

45 根據《防止兒童色情物品條例》（第 579 章）第 3(3)條，任何人管有兒童色情物品，即屬犯罪。第 2(1)條將"兒童色情物品"界定為包括*"以任何方式貯存並能轉為"*對兒童作色情描劃的照片、影片、電腦產生的影像或其他視像描劃*"的資料或數據"*。

電腦程式及軟件。[46] 基於上述理由，我們認為*"管有"*作為建議罪行的元素，實屬恰當。

建議 9

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

---

46 舉例而言，澳大利亞《刑事法典》（聯邦）第 478.3 條把意圖犯電腦罪行而*"管有"*或控制數據，定為罪行（見第 6.22 段）。加拿大《1985 年刑事法典》第 342.2(1)條將多項行為定為罪行，包括*"管有"*經設計或改裝以主要用作干犯第 342.1 或 430 條所訂罪行的器材，而*"器材"*則包括電腦程式（見第 6.29 至 6.30 段）。《新西蘭法令》第 251(1)條將多項行為定為罪行，包括*"管有"*用作犯罪的軟件或資料（見第 6.50 段）。美國《電腦欺詐及濫用法案》第 1029(a)條將多項行為定為罪行，包括*"管有"*、*"取用器材"*，而憑藉第 1029(e)(1)條，*"取用器材"*則包括無形物及數據（見第 6.64 至 6.65 段）。

(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。

管有只可作有害用途的數據

6.91 我們已在上文建議合理辯解可作為一般免責辯護。在結束本章前，我們謹提出以下問題：新法例應否同時就蓄意管有只可用作進行網絡攻擊的電腦數據（軟件或源碼）這項罪行，再認可一項特定的免責辯護或豁免。這類電腦數據的例子包括：

(a) 勒索軟件；

(b) 病毒；

(c) 建立及管理殭屍網絡的軟件；及

(d) 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）。[47]

6.92 儘管這幾類電腦數據可能有害，但亦有論點認為，比如在以下情況下，法律無須（或不應）把管有該等數據定為罪行：

(a) 大學保存惡意軟件，作教學或研究之用；

(b) 開發防毒軟件；

(c) 使用惡意軟件訓練互聯網服務供應商電郵伺服器的垃圾郵件過濾器；[48] 及

---

47 上述跨行業組織報告書舉出第三及第四項例子。見 Criminal Law Reform Now Network, *Reforming the Computer Misuse Act 1990*（2020 年），第 1 章，第 3.24 段。

48 採用人工智能技術的垃圾郵件過濾器可接受訓練，久而久之其性能便可改善。

(d) 其他資訊科技從業人員透過逆向工程，對惡意代碼進行研究。

6.93 至於分界線應訂於何處，一切視乎情況而定。以現實世界的例子作比擬，任何人即使對研究有興趣，也不大可能以此為理由，在家中保存爆炸品。在闡述這些意見後，我們期望公眾就以下問題提交意見書。

建議 10

小組委員會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？

(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？

第 7 章　香港法庭行使司法管轄權的準則

引言

7.1　本章討論與電腦網絡罪行相關的司法管轄權事宜，並集中探討香港法庭行使司法管轄權的準則。本章宜先從一般原則着手，繼而轉談國際間電腦網絡罪行法例處理司法管轄權事宜方面的經驗。

7.2　有評論員[1]識別出以下三個各自獨立卻又環環相扣的司法管轄權範疇：

(a) 規範的司法管轄權，該權關乎立法機關規管若干行為的能力；

(b) 審判的司法管轄權，該權關乎若干行為可否由法庭審理；及

(c) 執行的司法管轄權，該權關乎法律體制要求遵守規定或懲處違規行為的權限。

有關司法管轄權的一般原則

普通法的做法

7.3　一如終審法院在*香港特別行政區　訴　黃得強*（*HKSAR v Wong Tak Keung*，“***黃得強案***”）中述明：

> “一般規則是法庭的刑事司法管轄權受地域所限……這規則適用於普通法罪行及法定罪行。沒有域外法律效力的有力推定，在解釋訂立罪行的法例時適用。”[2]

1　Susan W Brenner and Bert-Jaap Koops, “Approaches to Cybercrime Jurisdiction” (2004) Vol 4, No 1, Journal of High Technology Law，第 5 頁；Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 475 頁；David Harvey，*internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015)，第 6.206 段；以及 Alisdair A Gillespie, *Cybercrime: Key Issues and Debates* (Routledge, 2016)，第 21 頁。

2　(2015) 18 HKCFAR 62，第 74 及 75 頁（第 27 及 28 段），FACC 8/2014（判決日期：2015 年 1 月 9 日）。

7.4　因此，一般而言，*"刑事司法管轄權的行使範圍不會延伸至涵蓋在外地所作的作為"*。[3] 加拿大最高法院（Supreme Court of Canada）在 *Libman v The Queen* 中評述如下：

> "……刑事法的屬地管轄原則，是法庭為了回應兩項實際考慮而建構的。首先，一個國家一般與外地不法分子的行動甚少會有直接關係。其次，假如某國試圖規管那些全部或絕大部分在別國境內發生的事宜，別國或會理所當然感到不悅。基於這些原因，法庭採納法律在領土以外不適用的推定……"[4]

7.5　除了整體上遵守屬地管轄原則外，不少國家亦聲稱對在懸掛有關國家國旗的船舶上和在該國註冊的飛機上所犯的罪行具有司法管轄權，因為這些船舶和飛機*"經常視為該國領土的延伸"*。[5] 在香港，法例確認這類延伸的屬地概念：

(a)　根據《航空保安條例》（第 494 章）第 3(1)條：

> "在正在航行但並非在香港境內或上空航行的香港控制的飛機上發生的任何作為或不作為，假如在香港境內發生便會構成香港法律下的某罪行的，即構成該罪行。"

(b)　根據《刑事罪行條例》（第 200 章）第 23B(1)條：

> "任何人的任何作為如——
>
> (a)　在處於公海的香港船舶上作出；及
>
> (b)　無本條則不屬一項罪行；及
>
> (c)　在香港作出的情況下，根據香港法律會構成一項罪行，
>
> 則在符合第(5)及(7)款的規定下，無論該人具有何種公民身分或屬何種國籍，該作為均構成該項罪行。"

3　*Treacy v DPP* [1971] AC 537，第 552 頁。

4　*Libman v The Queen* [1985] 2 SCR 178，第 208 頁 f 行。

5　《說明報告》第 235 段。

7.6 不幸的是，罪案*"的源頭及影響已不再局限於以本地為主"*，而且*"正在以國際規模謀劃"*。[6] 某項罪行相當可能只有部分元素在某司法管轄區內發生，而其他元素則在其他地方發生。在"後果罪行"的案件中：

> "如被告人作出受禁行為，造成受禁後果……而有關行為及後果在兩個不同的司法管轄區內發生……傳統觀點認為，這一類罪行須當作僅在罪行完成的地點所犯——也就是最終主要元素發生的地方——這通常稱為'終點觀點'。"[7]

7.7 然而，加拿大最高法院在 *Libman* 案中採納較具彈性的觀點，拉福里斯特法官（La Forest J）代表該法院說明如下：

> "本席對於屬地限制的觀點或可概括如下：本席認為，若要某罪行受本國法庭的司法管轄權規限，所需的是構成該罪行的活動的重大部分在加拿大發生。正如現代學者指出，罪行與這個國家之間有'真實及密切聯繫'便已足夠，這是國際公法及國際私法中眾所周知的驗證標準……"[8]

7.8 其他普通法司法管轄區自此相繼仿效，採納某些比墨守屬地管轄原則更具彈性的觀點。例如：

(a) 在 *Lipohar v R* 中，[9] 具關鍵性的事實牽涉多個澳大利亞州份，因而涉及多個司法管轄區。高等法院的多數法官裁定維持上訴人（被告人）在南澳大利亞的定罪，並對司法管轄權的問題評論如下：

> "在本案中，爭論點是控罪的主要內容與南澳大利亞之間是否有足夠聯繫。那是探究聯繫的因素是否足夠的問題，當中不涉假定或推定……應靈活應用有關聯繫的規定，只要與有關司法管轄區有真實聯繫便已足夠。"[10]

(b) 在英格蘭及威爾斯，上訴法院（刑事法庭）（Court of Appeal

---

6 *Liangsiriprasert v United States* [1991] 1 AC 225，第 251 頁 C 行。
7 見上文註腳 2，第 77 頁（第 33 段）。
8 [1985] 2 SCR 178，第 212 頁 j 行至 213 頁 a 行。
9 [1999] HCA 65。
10 [1999] HCA 65，第 122 及 123 段。

(Criminal Division)）在 *R v Smith (Wallace Duncan)(No 4)*中裁定，英格蘭的法庭可在以下情況下，行使司法管轄權：

> "……假如最後的作為在英格蘭發生，或該罪行的絕大部分〔在英格蘭〕所犯，而且並無出於相互尊重的理由而令該罪行不應〔在英格蘭〕審訊。"[11]

(c) 在香港，終審法院在*黃得強*案認同英格蘭及威爾斯採納的觀點：

> "……暫委法官司徒冕在 *HKSAR v Chan Shing Kong* 中認為，這項源自 *R v Smith (No 4)*的較寬鬆觀點比較可取，上訴法庭在 *HKSAR v Krieger* 的附帶意見中亦表示贊同，兩者依我們看來皆是正確之舉。"[12]

訂明司法管轄權規則的香港法例

7.9 終審法院在*黃得強*案中亦指出，法庭的刑事司法管轄權受地域所限這一般規則，*"可經法律修改"*。[13] 例如，根據《刑事司法管轄權條例》（第 461 章）（**《刑事司法管轄權條例》**）：

(a) 第 2(2)條把《盜竊罪條例》（第 210 章）及《刑事罪行條例》（第 200 章）所訂若干欺詐和不誠實的實質罪行，界定為甲類罪行；[14] 及

(b) 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)"

是在香港發生的，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。

---

11 [2004] QB 1418，第 1434 頁 H 行。

12 見上文註腳 2，第 81 頁（第 45 段）。

13 同上，第 75 頁（第 29 段）。

14 與串謀、企圖犯罪及煽惑他人的初步罪行（即第 2(3)條的乙類罪行）互相對照。

7.10 概念上，《刑事司法管轄權條例》第 3 條至少涵蓋下述兩種情況：

(a) 在香港的人，對在香港境外的受害人（個人）或目標（電腦等物件）作出甲類罪行的部分犯罪行為；及

(b) 在香港境外的人，對在香港的受害人或目標作出部分犯罪行為。

7.11 前段第一種情況大致對應上文所討論的普通法較寬鬆觀點。第二種情況則可視為反映“客觀屬地管轄原則”，法庭可據此聲稱對*“在外地作出而在有關司法管轄區內造成影響的作為”*具有司法管轄權。[15]

7.12 2002 年，政府將《2002 年刑事司法管轄權條例（修訂第 2(2)條）命令》擬稿提交予立法會批准。該命令擬稿旨在把以下三項電腦罪行列入甲類罪行：

(a) 《電訊條例》（第 106 章）第 27A 條所訂的“藉電訊而在未獲授權下取用電腦資料”罪；[16]

(b) 《刑事罪行條例》（第 200 章）第 59 及 60 條所訂的與誤用電腦有關的“摧毀或損壞財產”罪；[17] 及

(c) 《刑事罪行條例》（第 200 章）第 161 條所訂的“有犯罪或不誠實意圖而取用電腦”罪。[18]

然而，由於立法會相關小組委員會不支持這份命令擬稿，上述建議最終未有落實。[19]

7.13 除了《刑事司法管轄權條例》外，某些其他條例亦載有條文，就特定罪行訂明司法管轄權事宜。例如：

---

15 Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press, 2007)，第 5.27 段；類似看法見 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 477 頁。

16 於第 2 章（第 2.11 段）論述。

17 於第 4 章（第 4.7 段）和第 5 章（第 5.7 段）論述。

18 於第 2 章（第 2.6 段）論述。

19 根據立法會小組委員會於 2004 年 6 月 25 日的報告，一名委員不支持該命令擬稿，因為她認為就電腦罪行的擴大司法管轄權訂定的條文，應編在新訂的綜合條例內，而非在《刑事司法管轄權條例》內。其他某些委員亦同意她的看法。另一委員認為，修訂《刑事司法管轄權條例》所載罪行的機制（即由行政長官會同行政會議制定命令，但須事先提交立法會以決議通過），不及三讀程序可取。

(a) 《刑事罪行條例》（第 200 章）附表 2 載有一系列性罪行條文，凡若干類別的人干犯該等罪行，或該等罪行是就若干類別的人而干犯的，該等罪行條文便會具有域外法律效力。

(b) 根據《防止賄賂條例》（第 201 章）第 4 條，任何人 *"（不論在香港或其他地方）"* 無合法權限或合理辯解，提供任何利益；或任何公職人員 *"（不論在香港或其他地方）"* 無合法權限或合理辯解，索取或接受任何利益，作為（例如）誘因或報酬，即屬犯罪。

普遍獲接受的域外管轄權基礎

7.14 域外管轄權有四個普遍獲接受的基礎：

(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。[20]

與電腦網絡罪行相關的司法管轄權事宜

電腦網絡罪行帶來的挑戰

7.15 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供應商（例如社交媒體或通訊軟件的營運者）。

---

[20] 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。

7.16 就電腦網絡罪行而言，要決定某項事實在何處發生可能不易。例如，雲端計算的運作方式，是*"所要求的數據未必處於單一位置，而是分散於多個位置"*。[21] 在受害人儲存於雲端的數據被非法取覽的案件中，聯合國毒罪辦《網絡犯罪綜合研究》（Comprehensive Study on Cybercrime）的以下評述恰當貼切：

> "雲數據的處理涉及多個分佈在不同國家法域的數據場所或數據中心，而且涉及到不同的私有數據控制者和處理者。在當前條件下，儘管數據地點從技術上講是可知的，但雲計算用戶並非總會被告知自己的數據到底存於'何處'。而且，各國對待有關雲服務提供商所持數據的數據保護機制和對待關於國家執法偵查活動的管轄方式非常複雜。"[22]

法庭確認電腦網絡罪行的挑戰

7.17 法庭早已意會經常在電腦網絡罪行出現的司法管轄權事宜。例如，英格蘭上訴法院在 *R v Governor of Brixton Prison and Another, Ex parte Levin* 中有以下論述：

> "如某項指令幾乎是即時性的，並旨在於有關電腦所處的地方生效，若然把指令輸入磁碟這事視為只是在鍵盤所處的遙遠地方進行，我們認為未免流於牽強。"[23]

7.18 澳大利亞維多利亞最高法院（Supreme Court of Victoria）的基爾勒法官（Gillard J）在 *DPP v Sutcliffe* 中亦表達類似意見：

> "科技已發展至通訊可於一秒內遍達全球的階段。互聯網提供了迅速快捷且相對便宜的通訊方式，讓可以取用電腦及電話線的人互相通訊。取用不只限於擁有電腦，企業紛紛以低廉收費提供接達互聯網的服務。法律須隨着這些轉變而發展。"[24]

7.19 *R v Sheppard and Whittle* 的上訴人（被告人）被裁定發布煽動種族仇恨材料罪名成立，違反英格蘭及威爾斯《1986 年公安法令》（Public Order Act 1986）第 19 條。涉案材料在互聯網上發布。以下在判詞中提

---

21 Alisdair A Gillespie, *Cybercrime: Key Issues and Debates* (Routledge, 2016)，第 25 頁。

22 聯合國毒罪辦，《網絡犯罪綜合研究》（2013 年 2 月），第 167 頁。

23 *R v Governor of Brixton Prison and Another, Ex parte Levin* [1997] QB 65，第 82 頁 E 行。上議院後來維持上訴法院的判決，見[1997] AC 741。

24 [2001] VSC 43，第 62 及 63 段。

到的大律師陳詞，闡明要斷定發布內容應視為在何處發布，有多種可能性：

> "戴維斯先生（Mr Davies）在陳詞指出，關於互聯網上的發布，主要有三套法學理論。第一，發布只可在其寄存的網頁伺服器所在的司法管轄區內審理——來源國理論。第二，互聯網上的發布，可在能夠下載該項發布的任何司法管轄區內審理——目的國理論。第三，發布除了必然可在其寄存的網頁伺服器所在的司法管轄區內審理之外，亦可在該項發布所針對的司法管轄區內審理——指向和針對理論。"[25]

7.20 *Dow Jones and Co Inc v Gutnick*[26] 雖是民事案件，但引述此案亦有助說明。案情關於指稱的誹謗性材料在位於美國新澤西的道瓊斯（Dow Jones）網頁伺服器上發布，但在澳大利亞下載。澳大利亞高等法院裁定，這宗誹謗申索可由澳大利亞的法庭審理，理由是：

> "如屬萬維網上的材料，直至某人使用網頁瀏覽器把該材料從網頁伺服器下載至電腦，該材料才會以可理解的形式提供。也就是在該人下載該材料的地方，聲譽才可能會受到損害。因此，該處通常是誹謗侵權行為發生的地方。"[27]

7.21 網上材料在世上任何地方均可能下載得到。假若指稱誹謗性的網上發布關乎某在多個司法管轄區均享有聲譽的人，如該等司法管轄區各自的法庭採用澳大利亞高等法院的上述理據，便可主張對該項發布具有司法管轄權。*Gutnick* 案的判決*"引起不少爭議"*，[28] 例如有評論員警告，該項判決可能會*"對互聯網上的言論造成寒蟬效應"*，[29] 另一評論員亦指，該項判決*"凸顯澳大利亞與美國法律在互聯網司法管轄權上的分歧"*。[30]

---

25 [2010] 1 Cr App R 26，第 402 頁。英格蘭上訴法院因應案情而信納它具有司法管轄權，因此拒絕進一步探討該大律師提出的理論。

26 (2002) 210 CLR 575。

27 同上，第 607 頁（第 44 段）。

28 Richard Garnett, "*Dow Jones & Company Inc v Gutnick*: An Adequate Response to Transnational Internet Defamation?" (2003) 4(1) Melbourne Journal of International Law 196。*Gutnick* 案判決後，學術界多年來對該案一直爭論不休。例如見 David Rolph, "Publication, Innocent Dissemination and the Internet after *Dow Jones & Co Inc v Gutnick*" (2010) 33(2) UNSW Law Journal 562 這文章。

29 Nathan W Garnett, "*Dow Jones & Co v Gutnick*: Will Australia's Long Jurisdictional Reach Chill Internet Speech World-Wide?" (2004) 13 Pac Rim L & Pol'y J 61，第 62 頁。

30 Brian Fitzgerald, "*Dow Jones & Co Inc v Gutnick*: Negotiating 'American Legal Hegemony' in the Transnational World of Cyberspace" (2003) 27(2) Melbourne University Law Review 590。

7.22 不論採用哪一套司法管轄權原則，行使域外管轄權均須合乎情理，以免涉及*"在沒有充分理由下干預別國主權"*。[31] 國際間打擊跨境罪案時，應務求避免和解決司法管轄權的消極衝突（即沒有國家聲稱對某宗罪案具有司法管轄權）及司法管轄權的積極衝突（即多個國家聲稱對某宗罪案具有司法管轄權）。[32] 實際上，解決後一類衝突亦可防止有關司法管轄區出現一罪兩審的問題。[33]

《布達佩斯公約》的司法管轄權規則

7.23 《布達佩斯公約》[34] 第二十二條訂明成員國應如何處理有關第二至十一條所訂罪行的司法管轄權事宜。

> "1 在下列情況下，各締約方均應採取必要的立法及其他措施，對按照本公約第二至十一條訂立的任何罪行確立司法管轄權：
>
> a 該罪行發生在其領土內；或
>
> b 該罪行發生在懸掛該締約方旗幟的船舶上；或
>
> c 該罪行發生在根據該締約方法律註冊的飛機上；或
>
> d 該罪行由其國民所犯，而該罪行根據犯罪地點的刑事法律可予懲處，或該罪行在任何國家的領域管轄權以外發生。
>
> 2 各締約方可保留權利，完全不應用或只在特定案件或條件下才應用本條第 1.b 至 1.d 段或其任何部分所訂的司法管轄權規則。

---

31 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 483 及 485 頁。

32 Susan W Brenner and Bert-Jaap Koops, "Approaches to Cybercrime Jurisdiction" (2004) Vol 4, No 1, Journal of High Technology Law，第 40 及 41 頁。

33 如某人就某項罪行曾獲判無罪或被定罪，而後來又被控以同一罪行，禁止一罪兩審的規則即告適用，控方因而不得檢控該人。這項規則亦適用於在另一司法管轄區曾被定罪或獲判無罪的情況。正如終審法院在*楊振邦及其他人 訴 律政司司長*（*Yeung Chun Pong & Others v Secretary for Justice*）(2009) 12 HKCFAR 867 中確認，如*"某人面臨第二次審訊，而該次審訊源於與較早前審訊相同或大致相同的事實，不論該較早前審訊是在同一司法管轄區內進行，還是在另一司法管轄區具管轄權的法院內進行"*，法庭亦有酌情決定權，以司法程序遭濫用為理由而擱置檢控（第 21 段）。

34 有關《布達佩斯公約》的背景資料，見導言第 11 段，以及第 1 章第 1.6 至 1.10 段。

3　　各締約方均應採取必要的措施，在指稱罪犯在其領土內，而其在接獲引渡請求後僅因該人的國籍而不予引渡至另一締約方時，確立其對本公約第二十四條第1段所指罪行的司法管轄權。

4　　本公約不排除締約方根據其本土法律行使的任何刑事司法管轄權。

5　　如多於一個締約方聲稱對按照本公約訂立的某項指稱罪行具有司法管轄權，有關締約方須在適當的情況下進行磋商，以期決定最適合提出檢控的司法管轄區。"

7.24　　第二十二條第1a至1c段體現屬地管轄原則，並顯示這項原則延伸至船舶和飛機，上文在考慮司法管轄權的一般原則時，已討論此點。第1d段則以主動屬人管轄原則為前提。

7.25　　第1d段的第一項限制條款（*"而該罪行根據犯罪地點的刑事法律可予懲處"*），揭示不少國家的引渡法律均有雙重犯罪的規定。如在香港應用有關規定，即是指根據某作為作出的地方的法律，以及根據香港法律，該作為均須屬罪行，香港的法庭方可行使司法管轄權。[35] 就引渡而言，上議院在 *Norris v Government of the United States of America*[36] 中述明，雙重犯罪規定的背後理念是：*"人身自由不得因被請求國根本不承認屬刑事的罪行而受到限制"*。[37]

7.26　　《說明報告》對第二十二條其他部分的評註如下：

"237. 第2段容許締約方就第1段b、c及d項定下的司法管轄權基礎作出保留。然而，對於根據a項確立領域管轄權，或對於根據第3段在屬於'引渡或檢控'（'*aut dedere aut judicare*'）原則下的情況（即該締約方因指稱罪犯的國籍而拒絕引渡，而該罪犯身處其領土內）確立司法管轄權的責任，則不得作出保留。根據第3段確立司法管轄權有其必要，以確保如請求引渡的締約方提出要求，拒絕引渡國民的締約方在法律上有能力依

35　《刑事司法管轄權條例》並沒有就甲類罪行（一般傳統欺詐及不誠實罪行）施加雙重犯罪的規定。

36　[2008] 1 AC 920。

37　同上，第954頁H行。

據本公約第二十四條（‘引渡’）第 6 段的規定在其本土進行調查和法律程序作為替代。

……

239. 在使用電腦系統犯罪的情況下，有時候會有多於一個締約方對有關罪行的部分或全部參與者具有司法管轄權。例如，不少利用互聯網進行的病毒攻擊、欺詐及侵犯版權行為均以多國的受害人為目標。為免工作重疊、對證人造成不必要的不便，或令有關各國的執法官員互相競爭，又或是為了利便法律程序高效公平地進行，受影響的締約方應進行磋商，以決定適合提出檢控的地方。在某些情況下，有關國家選擇單一檢控地是最有效的做法；在另一些情況下，最佳做法則可能是由某國家檢控部分參與者，另一（些）國家則檢控其他參與者。兩個結果皆為這一段所准許。最後，進行磋商並非一項絕對責任，而是應‘在適當的情況下’進行。因此，假如其中一個締約方知道進行磋商並無必要（例如，它獲另一締約方確認，該方並無計劃採取行動），或假若有締約方認為進行磋商會有損它進行的調查或法律程序，則可延遲或拒絕進行磋商。”[38]

7.27 上述《說明報告》內的評註反映國際間的普遍做法。根據聯合國毒罪辦《網絡犯罪綜合研究》，各國表示，*“它們通常會通過與其他國家的正式和非正式磋商來解決管轄權糾紛這一問題，從而防止雙重調查和管轄權衝突”*。[39] 儘管各國普遍並無為解決電腦網絡罪行案件的司法管轄權衝突而制定特定法例，[40] 部分地區的文書就國與國之間的法律合作可考慮的因素提供指引。[41]

---

38 《說明報告》第 237 及 239 段。

39 聯合國毒罪辦，《網絡犯罪綜合研究》（2013 年 2 月），第 240 頁。

40 見上文註腳 39。

41 例如，《歐洲聯盟理事會關於攻擊信息系統行為的第 2005/222/JHA 號框架決定》（Council Framework Decision 2005/222/JHA on attacks against information systems in the European Union）第 10(4)條及《阿拉伯國家打擊信息技術犯罪問題公約》（Arab Convention on Combating Information Technology Offences）（2010 年 12 月 21 日）第 30(3)條列出以下因素：

(i) 有關罪行擾亂其安全或利益的國家；
(ii) 有關罪行在其境內發生的國家；
(iii) 犯罪者是其國民的國家；
(iv) 在其境內發現犯罪者的國家；及
(v) （如情況類似）首個請求引渡的國家。

7.28　根據《基本法》，[42] 中央人民政府負責管理與香港有關的外交事務，而香港獲授權依照《基本法》自行處理有關的對外事務。[43] 因此，如香港在有關的對外事務範圍以外與外國政府磋商和簽訂任何雙邊協議，須獲得中央人民政府授權，並由中華人民共和國外交部駐香港特派員公署（"**外交部駐港公署**"）協助。[44] 在任何有關協議簽訂之前，我們預計，如我們的建議獲政府落實推行，相關執法機構及檢控機關便會援引新訂電腦網絡罪行法例分別就五類依賴電腦網絡的罪行訂明的司法管轄權規則，[45] 而禁止一罪兩審的規則適用於在另一司法管轄區曾被定罪或獲判無罪的情況，如同適用於在香港曾被定罪或獲判無罪的情況。[46]

其他司法管轄區的法定體制

澳大利亞

《刑事法典》（聯邦）第 15.1 條

7.29　在澳大利亞，《刑事法典》（聯邦）（Criminal Code (Cth)）第 476.3 條訂明，詳列於第 15.1 條的 *"擴大地域司法管轄權——甲類"* 適用於第 10.7 部所訂罪行（即各項電腦罪行）。第 15.1 條篇幅甚長，無需在此列出全文。先從第 15.1(1)條看起：

> "如聯邦法律規定本條適用於某罪行，除非有以下情況，否則任何人不屬干犯該罪行：
>
> (a) 構成有關指稱罪行的行為：
>
> (i) 全部或部分在澳大利亞發生；或
>
> (ii) 全部或部分在澳大利亞的飛機或澳大利亞的船舶上發生；或

42　見第十三條及第七章。

43　按照第一百五十一條的規定，有關的對外事務包括在經濟、貿易、金融、航運、通訊、旅遊、文化、體育等領域同世界各國、各地區及有關國際組織簽訂有關協議。

44　外交部駐港公署的主要職責載於其網站，網址為 http://www.fmcoprc.gov.hk/chn/zjgs/gszn/202109/t20210903_8903490.htm（於 2022 年 5 月 3 日瀏覽）。

45　就該五類依賴電腦網絡的罪行所建議的司法管轄權規則，分別概述於建議 11、12、13、14 及 15。有關這些規則的考慮，詳情見第 7.71 至 7.100 段。

46　見上文註腳 33。

(b) 構成有關指稱罪行的行為，全部在澳大利亞境外發生，而該行為的後果：

(i) 全部或部分在澳大利亞發生；或

(ii) 全部或部分在澳大利亞的飛機或澳大利亞的船舶上發生；或

(c) 構成有關指稱罪行的行為，全部在澳大利亞境外發生，而：

(i) 在有關指稱罪行發生時，該人是澳大利亞公民；或

(ii) 在有關指稱罪行發生時，該人是藉或根據聯邦法律或某州份或某領地的法律成立為法團的法人團體；或

(d) 符合以下所有條件：

(i) 有關指稱罪行屬附帶罪行；

(ii) 構成有關指稱罪行的行為，全部在澳大利亞境外發生；

(iii) 構成該附帶罪行所關乎的主要罪行的行為，或該行為的後果，全部或部分在澳大利亞發生，或全部或部分在澳大利亞的飛機或澳大利亞的船舶上發生，或該人意圖該行為或該行為的後果全部或部分在澳大利亞發生，或全部或部分在澳大利亞的飛機或澳大利亞的船舶上發生。”

7.30 概括第 15.1(1)條而言，澳大利亞的法庭可按以下原則，聲稱對主要罪行具有司法管轄權：

(a) 屬地管轄原則（包括延伸至澳大利亞的船舶及飛機）；

(b) 客觀屬地管轄原則（構成罪行的行為在澳大利亞境外發生，但其後果在澳大利亞發生）；及

(c) 主動屬人管轄原則(適用於澳大利亞的公民及法人團體)。

7.31 第 15.1(2)條接着訂定適用於主要罪行的免責辯護：

"如聯邦法律規定本條適用於某罪行，則在以下情況下，任何人不屬干犯該罪行：

(aa) 有關指稱罪行屬主要罪行；及

(a) 構成有關指稱罪行的行為，全部在外國發生，但並非在澳大利亞的飛機或澳大利亞的船舶上發生；及

(b) 該人：

(i) 並非澳大利亞公民；亦

(ii) 並非藉或根據聯邦法律或某州份或某領地的法律成立為法團法人團體；及

(c) 在：

(i) 發生構成有關指稱罪行的行為的外國；或

(ii) 發生構成有關指稱罪行的行為的外國的部分；

並無該外國的有效法律或該外國部分的有效法律，訂立任何相當於首述罪行的罪行。"

7.32 第 15.1(4)條的條文與第 15.1(2)條相若，但適用於附帶罪行。[47] 簡言之，凡是在澳大利亞境外發生的行為，如發生該行為的司法管轄區並無任何法律把該行為定為罪行，第 15.1(2)及(4)條共同為這類行為訂立免責辯護。這兩款大致上對應《布達佩斯公約》之下的雙重犯罪規定。[48]

《刑事法典》（聯邦）第 16.2 條

7.33 《刑事法典》（聯邦）第 16.2 條（*"當行為視為部分在澳大利亞發生"*）進一步規定如下：

---

47 《刑事法典》（聯邦）末端的字典將附帶罪行界定為*"(a)違反第 11.1、11.4 或 11.5 條的罪行；或(b)違反聯邦法律的罪行，但以因第 11.2、11.2A 或 11.3 條實施而產生的罪行為限"*。維多利亞司法學院（Judicial College of Victoria）在其《維多利亞刑事法律程序指南》（Victorian Criminal Proceedings Manual）中述明，附帶罪行一詞主要*"關乎企圖犯罪、煽惑他人、串謀，或依據合謀或共同目的或利用不知情的人而犯的罪行"*（第 1.3 節第 56 段）。

48 關於《布達佩斯公約》第二十二條第 1d 段的第一項限制條款，見第 7.25 段。

“ 發送物件

(1) 〔……〕

發送電子通訊

(2) 就本部而言，任何人如將電子通訊或導致將電子通訊：

(a) 從澳大利亞境外某點發送至澳大利亞某點；或

(b) 從澳大利亞某點發送至澳大利亞境外某點；

則該行為視為部分在澳大利亞發生。

某點

(3) 就本條而言，**某點**包括流動或可能流動的某點，不論是在陸上、地底、大氣中、水底、海上或任何其他地方。”

7.34 如某人身處澳大利亞，並發送或導致發送電子通訊，則該行為即屬在澳大利亞發生，類似於第 16.2 條的推定條文，並非必要。這顯示第 16.2 條旨在適用於某人在作出有關行為時身處澳大利亞境外的情況。

7.35 如以廣義解釋第 16.2(2)條，該條實際效果似乎如下：

(a) 只要某人發送或導致發送的電子通訊以 *“澳大利亞某點”* 為來源地或目的地，即視為符合該人的行為 *“部分在澳大利亞發生”* 的司法管轄權準則。

(b) 就傳入的電子通訊而言（即第 16.2(2)(a)條的情況），無需證明該通訊已進入澳大利亞。

(c) 就輸出的電子通訊而言（即第 16.2(2)(b)條的情況），該通訊是否已離開澳大利亞無關宏旨。

7.36 另一解讀可能是，須先證明有關電子通訊在部分關鍵時間，於澳大利亞出現，某人發送或導致發送該電子通訊的行為方可視為完成。這解讀可能對傳入電子通訊的情況有較大影響。

加拿大

《1985 年刑事法典》第 477.1 條

7.37 在加拿大，根據《1985 年刑事法典》（Criminal Code 1985）第 477.1 條（*"加拿大境外的罪行"*）：

> "如任何人作出某作為或不作為，而假使該作為或不作為在加拿大發生，便會屬……聯邦法律所訂罪行，則在以下情況下，該人即當作在加拿大作出該作為或不作為：
>
> (a) 在加拿大專屬經濟區內，
>
> (i) 為了勘探或開採、保存或管理該加拿大專屬經濟區的天然資源……而身處該加拿大專屬經濟區的人作出該作為或不作為，及
>
> (ii) 該作為或不作為由身為加拿大公民或……永久性居民的人作出，或就身為加拿大公民或……永久性居民的人作出；
>
> (b) 該作為或不作為在加拿大的大陸架內的某地方或大陸架上方的某地方作出，而憑藉《海洋法令》（Oceans Act）第 20 條，該作為或不作為在該地方屬犯罪；
>
> (c) 該作為或不作為在加拿大境外，在根據任何國會法令註冊或領牌或獲發識別號碼的船舶上作出，或藉根據任何國會法令註冊或領牌或獲發識別號碼的船舶作出；
>
> (d) 該作為或不作為在加拿大境外於緊追期間作出；或
>
> (e) 加拿大公民在任何國家的領土外，作出該作為或不作為。"

7.38 上文第(a)至(e)段訂明的情況當中，體現出主動屬人管轄原則的(e)段似乎與電腦網絡罪行案件最為相關。

《1985 年刑事法典》第 476(d)條

7.39 凡某罪行是在飛行中的飛機上所犯的，《1985 年刑事法典》第 476(d)條（*"特別司法管轄區"*）將該罪行視為在以下領域分區所犯：

> "(i) 該次飛行開始的領域分區，[49]
>
> (ii) 該飛機在該次飛行中經過其上空的任何領域分區，或
>
> (iii) 該次飛行結束的領域分區"。

加拿大法庭作出審判的司法管轄權

7.40 《1985 年刑事法典》第 481.2 條（*"加拿大境外的罪行"*）訂明，對於受加拿大法律的域外管轄權所規管的罪行，加拿大法庭審判該罪行的司法管轄權如下：

> "除本國會法令或任何其他國會法令另有規定外，如某作為或不作為在加拿大境外作出，而根據本國會法令或任何其他國會法令，該作為或不作為如在加拿大境外作出即屬犯罪的話，則不論被告人是否在加拿大，亦可在加拿大任何領域分區內就該罪行展開法律程序，並控告、審訊和懲處被告人，其方式猶如該罪行是在該領域分區內所犯一樣。"

7.41 *Libman* 案中定下的普通法原則（於上文引述[50]）補充上述條文。根據該原則，加拿大的法庭會對與加拿大有*"真實及密切聯繫"*的罪行行使司法管轄權。

英格蘭及威爾斯

概覽

7.42 《英格蘭誤用電腦法令》：

> (a) 在第 1、2、3、3ZA 及 3A 條訂立五項罪行；並

---

49 《1985 年刑事法典》第 2 條將"領域分區"界定為包括*"文意所適用的任何省、郡、聯合郡、鎮區、市、鎮、教區或其他司法分區或地方"*。

50 第 7.7 段。

(b) 在第 4 至 9 條處理司法管轄權事宜。

7.43 由於《英格蘭誤用電腦法令》所訂的五項罪行各有不同司法管轄權規則，要概述該等規則並不直接簡單。概括而言，根據第 4 條（*"本法令所訂罪行的領域範圍"*）：

(a) 須 *"與本地司法管轄權有重大聯繫"*，方屬犯以下條文所訂罪行：

(i) 第 1 條（*"在未獲授權下取覽電腦資料"*）；

(ii) 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"*）；

(iii) 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"*）；

就上述罪行而言，就定罪而須予以證明的任何作為或其他事情是否在 *"有關原屬國"*[51] 發生，或被告人當時是否身在該處，均無關重要。[52]

(b) 至於第 2 條所訂罪行（*"在未獲授權下取覽，並意圖干犯或意圖利便干犯其他罪行"*），當中的在未獲授權下取覽無需 *"與本地司法管轄權有重大聯繫"*。[53] 然而，第 2(2)條[54] 顯示，意圖干犯的其他罪行，須屬可根據英格蘭法律審訊的罪行。

(c) 如第 3A 條所訂罪行（*"製造、供應或取得用於第 1、3 或 3ZA 條所訂罪行的物品"*）*"與本地司法管轄權有重大聯繫"*，則被告人在就該罪行定罪而須予以證明的任何作為或其他事情發生時，是否身處 *"有關原屬國"*，亦無關重要。[55]

---

51 《英格蘭誤用電腦法令》適用於英格蘭及威爾斯時（該法令同樣適用於蘇格蘭及北愛爾蘭），第 4(6)條將這詞語界定為英格蘭及威爾斯。

52 《英格蘭誤用電腦法令》第 4(1)條。

53 《英格蘭誤用電腦法令》第 4(3)條。

54 *"本條適用於以下罪行——*
(a) 刑罰為法律所固定的罪行；或
(b) 任何年滿 21 歲（就英格蘭及威爾斯而言，則為年滿 18 歲）且無定罪紀錄的人，可處為期 5 年監禁的罪行（或在英格蘭及威爾斯，假若沒有《1980 年裁判法院法令》〔Magistrates' Courts Act 1980〕第 33 條所施加的限制，則可被如此判刑的罪行）。"

55 《英格蘭誤用電腦法令》第 4(4A)條。

"與本地司法管轄權有重大聯繫"的涵義

7.44 《英格蘭誤用電腦法令》第 5 條解釋何謂*"與本地司法管轄權有重大聯繫"*。表面看來，這詞組是一項統一概念，適用於第 1、3、3ZA 及 3A 條所訂各項罪行。然而，*"與本地司法管轄權有重大聯繫"*的確切涵義及其含意，卻視乎有關罪行而有所不同。這種聯繫可按第 5 條指明的以下其中一種形式體現：

(a) 被告人是英國國民，當時身處英國以外的國家，而根據該作為發生的國家的法律，被告人的作為構成罪行[56] —— 這種形式是基於主動屬人管轄原則，適用於第 1、3、3ZA 或 3A 條所訂罪行；

(b) 被告人於作出有關作為時，身處*"有關原屬國"*[57] —— 這種形式反映屬地管轄原則，適用於第 1、3 或 3ZA 條所訂罪行；

(c) 目標電腦在*"有關原屬國"*[58] —— 這種形式包含客觀屬地管轄原則，適用於第 1、3 或 3ZA 條所訂罪行；或

(d) 未獲授權的作為在*"有關原屬國"*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[59] —— 這種形式體現了保護管轄原則，只適用於第 3ZA 條所訂罪行。

7.45 鑑於上述機制錯綜複雜，第 4 及 5 條難免較為複雜。

雙重犯罪

7.46 《英格蘭誤用電腦法令》所訂的五項罪行有一個共通點，就是在英格蘭及威爾斯的法庭可行使司法管轄權的多個可能事實情況當中，只有一個事實情況有雙重犯罪的規定。至於雙重犯罪的規定如何適用，該五項罪行可分為以下兩組：

(a) 就第 1、3、3ZA 或 3A 條所訂罪行而言，上文介紹的*"與本地司法管轄權有重大聯繫"*的第一種可能形式[60] ——

---

56 《英格蘭誤用電腦法令》第 5(1A)條。
57 《英格蘭誤用電腦法令》第 5(2)(a)、(3)(a)及(3A)(a)條。
58 《英格蘭誤用電腦法令》第 5(2)(b)、(3)(b)及(3A)(b)條。
59 《英格蘭誤用電腦法令》第 5(3A)(c)條。
60 第 7.44(a)段。

基於主動屬人管轄原則——含有雙重犯罪元素，當中規定根據該作為發生的國家的法律，被告人的作為須構成罪行。

(b) 就第 2 條所訂罪行而言，如上文所述，[61] 當中的在未獲授權下取覽無需*"與本地司法管轄權有重大聯繫"*。然而，第 8 條在以下情況下適用：

(i) 有人被指稱犯了第 1 條所訂罪行；而

(ii) 該罪行*"與本地司法管轄權有重大聯繫"*。[62]

第 8(1)條包含雙重犯罪的規定：

> "如任何人意圖作出或意圖利便的事會涉及犯一項該事或其任何部分擬發生的地方的有效法律所訂罪行，則該人只有在此情況下方被判犯了可憑藉上文第 4(4)條審訊的罪行。"[63]

中國內地

《中國刑法》

7.47 適用於電腦網絡罪行的司法管轄權規則，載於《中國刑法》第六至八條：

> "第六條 凡在中華人民共和國領域內犯罪的，除法律有特別規定的以外，都適用本法。
>
> 凡在中華人民共和國船舶或者航空器內犯罪的，也適用本法。
>
> 犯罪的行為或者結果有一項發生在中華人民共和國領域內的，就認為是在中華人民共和國領域內犯罪。

---

61 第 7.43(b)段。

62 《英格蘭誤用電腦法令》第 4(4)條。

63 第 8(3)條的條文相若，但適用於該條詳列的企圖犯罪罪行：
"如任何人所構想的事會涉及犯該事或其任何部分擬發生的地方的有效法律所訂的罪行，則該人只有在此情況下方被判犯了可憑藉《1981 年企圖犯罪法令》(Criminal Attempts Act 1981)第 1(1A)條審訊的罪行。"

第七條　中華人民共和國公民在中華人民共和國領域外犯本法規定之罪的，適用本法，但是按本法規定的最高刑為三年以下有期徒刑的，可以不予追究。

中華人民共和國國家工作人員和軍人在中華人民共和國領域外犯本法規定之罪的，適用本法。

第八條　外國人在中華人民共和國領域外對中華人民共和國國家或者公民犯罪，而按本法規定的最低刑為三年以上有期徒刑的，可以適用本法，但是按照犯罪地的法律不受處罰的除外。"

7.48　簡言之，《中國刑法》容許法庭根據以下原則，對刑事罪行行使司法管轄權：

(a) 屬地管轄原則（依據第六條包括犯罪的行為或結果在中國發生的情況，亦延伸至中國的船舶及飛機）；

(b) 主動屬人管轄原則（依據第七條適用於任何中國公民）；及

(c) 被動屬人管轄原則及保護管轄原則（依據第八條適用於針對中國公民及中國的犯罪，前提是有關罪行可處不少於三年有期徒期，並且符合雙重犯罪的規定）。

新西蘭

《新西蘭法令》第 7 條

7.49　下列的《新西蘭法令》第 7 條（*"犯罪地點"*），可與香港的《刑事司法管轄權條例》第 3 條對照：

"就司法管轄權而言，如任何作為或不作為構成任何罪行的部分，並在新西蘭發生，或完成任何罪行所必要的任何事情在新西蘭發生，則不論被控該罪行的人在該作為、不作為或事情發生時是否身處新西蘭，該罪行亦須當作在新西蘭干犯。"

7.50　新西蘭法律委員會（New Zealand Law Commission）在其有關誤用電腦的報告書內，對第 7 條評述如下：

"……我們認為，《1961 年刑事罪行法令》（Crimes Act 1961）現有的司法管轄權條文，並不足以處理誤用電腦活動。首先，雖然有些情況是涉案黑客或電腦均並非位於新西蘭，但誤用電腦的影響卻可出現在這個國家。在這些情況下，或不可能每次按照《1961 年刑事罪行法令》第 7 條的條文，均成功爭辯'構成〔有關〕罪行的部分的任何作為或不作為，或完成〔有關〕罪行所必要的任何事情'是在新西蘭內發生的。其次，在不少案件中，根本不可能判斷涉案黑客在誤用電腦活動發生時身在何處……我們建議應訂立條文，賦予新西蘭的法庭司法管轄權，審理在任何地方所犯的誤用電腦罪行。"[64]

7.51 有評論員並不同意法律委員會這項建議，[65] 該項建議亦顯然未有落實。雖然《新西蘭法令》於 2002 年加入新訂的第 7A 條（*"有關若干跨國罪行的域外管轄權"*），[66] 但該項條文只適用於該法令訂明的某些罪行，而當中並不包括第 249 至 252 條所訂涉及電腦的罪行。

雙重犯罪

7.52 《新西蘭法令》第 7 條並無包含雙重犯罪的原則，但該法令第 8 條（*"有關對新西蘭境外船舶或飛機上的罪行的司法管轄權"*）卻基於該項原則訂定免責辯護，在此引述第 8(1)及(2A)條便足夠：

"(1) 本條適用於在新西蘭境外——

(a) 任何人在任何英聯邦的船舶上作出的任何作為或不作為；或

(b) 任何人在任何新西蘭的飛機上作出的任何作為或不作為；或

(c) 任何人在任何船舶或飛機上作出的任何作為或不作為，而該人在作出該作為或不作為的旅程途中或終結時，在該船舶或飛機上到達新西蘭；或

---

64 新西蘭法律委員會，*Computer Misuse: Report 54* (May 1999)，第 26 及 27 頁。

65 David Harvey, *internet.law.nz selected issues* (LexisNexis NZ Limited, 4th edition, 2015)，第 6.221 段，註腳 239（*"……筆者認為這項〔建議〕適得其反……訂立普遍的司法管轄權會在法律的灰色地帶立下危險先例"*）。

66 第 7A 條反映延伸至船舶和飛機的屬地管轄原則、主動屬人管轄原則和被動屬人管轄原則。

(d) 任何英籍人士在處於公海的任何外國船舶(並非該人所屬的船舶)上作出的任何作為或不作為,或在處於任何英聯邦國家領海內的任何該等船舶上作出的任何作為或不作為;或

(e) 任何新西蘭公民或通常居於新西蘭的人在任何飛機上作出的任何作為或不作為:

但如某非英籍人士在任何船舶或飛機上作出該作為或不作為,而該船舶或飛機當時正用作非英聯邦國家的任何武裝部隊的船舶或飛機,則(c)段並不適用。

(2A) 凡憑藉本條賦予的司法管轄權進行任何法律程序,如證明根據在有關作為或不作為發生時被告人屬其國民或公民的國家的法律,該作為或不作為假若在該國發生便不屬犯罪,即可以此作為免責辯護。"

新加坡

《新加坡誤用電腦法令》第 13 條

7.53 在新加坡,適用於《新加坡誤用電腦法令》的司法管轄權規則載於第 13 條(*"本法令所訂罪行的領域範圍"*):

"(1) 除第(3)款另有規定外,本法令的條文對新加坡內外的任何人均具有效力,不論該人屬何種國籍或具有何種公民身分。

(2) 如任何人在新加坡境外任何地方犯本法令所訂罪行,則可對該人作出處置,猶如該罪行是在新加坡所犯一樣。

(3) 為施行本條,本法令在以下情況下適用——

(a) 就有關罪行而言,被告人在關鍵時間處於新加坡;

(b) 就有關罪行(即第 3、4、5、6、7 或 8 條所訂罪行)而言,有關電腦、程式或數據在關鍵時間處於新加坡;或

(c) 該罪行導致在新加坡的嚴重損害，或產生導致在新加坡的嚴重損害的重大風險。

(4) 在第(3)(c)款中，*"在新加坡的嚴重損害"*指——

(a) 在新加坡的個人患病、受傷或死亡；

(b) 干擾新加坡任何主要服務供應，或嚴重削弱公眾對新加坡任何主要服務供應的信心；

(c) 干擾政府、國家機關、法定委員會（或政府、國家機關或法定委員會的任何部分）執行任何職務或職能或行使任何權力，或嚴重削弱公眾對政府、國家機關、法定委員會（或政府、國家機關或法定委員會的任何部分）執行任何職務或職能或行使任何權力的信心；或

(d) 損害新加坡的國家安全、防務或對外關係。

……

(5) 就第(3)(c)款而言，導致在新加坡的嚴重損害的罪行是否——

(a) 直接導致該損害；或

(b) 該損害的唯一或主要成因，

均屬無關重要。

(6) 在第(4)(b)款中，'主要服務'指以下任何服務：

(a) 與通訊基礎建設、銀行及金融服務、公共事業、公共交通、陸上運輸基礎建設、航空、船運或公開密碼匙基礎建設直接有關的服務；

(b) 警務、民防或衞生服務等緊急服務。

(7) 在第(4)(c)款中，'法定委員會'指由任何公共法令成立以執行或履行公共職能的法團或並非法團的團體，或根據任何公共法令成立以執行或履行公共職能的法團或並非法團的團體。"

7.54 學術界對第 13 條發表以下意見：

> "第 1 及 2〔款〕賦予該法令無限的域外法律效力，但第 3〔款〕則可理解為限制第 1 及 2〔款〕的適用範圍。只有與罪行有關的犯罪者、電腦、程式或數據在罪行發生時處於新加坡，該法令方會適用。不過，法令的適用範圍依然甚廣。數據在關鍵時間須處於新加坡這項規定，可與西弗吉尼亞訂明數據須在傳送中經過該州的規定比照。" [67]

在新加坡的嚴重損害

7.55 如上文所示，《新加坡誤用電腦法令》第 13(4)條訂明存在*"在新加坡的嚴重損害"*的四種情況。該法令就該等情況，在第 13(4)(b)及(c)條提供以下例子：[68]

> "例 1.——以下例子中的作為，嚴重削弱公眾對主要服務供應的信心，或產生嚴重削弱公眾對這方面的信心的重大風險：
>
> (a) 向公眾發布新加坡某醫院的病人醫療紀錄；
>
> (b) 向公眾提供查閱新加坡某銀行的客戶帳戶號碼的途徑。
>
> 例 2.——以下例子中的作為，嚴重削弱公眾對政府、國家機關、法定委員會（或政府、國家機關或法定委員會的任何部分）執行任何職務或職能或行使任何權力的信心，或產生嚴重削弱公眾對這方面的信心的重大風險：
>
> (a) 向公眾提供查閱屬政府某部門的機密文件的途徑；
>
> (b) 向公眾發布屬於某法定委員會的電腦的取用碼。"

---

67 Susan W Brenner and Bert-Jaap Koops, "Approaches to Cybercrime Jurisdiction" (2004) Vol 4, No 1, Journal of High Technology Law，第 21 頁。

68 根據《詮釋法令》（Interpretation Act）第 7A 條（*"例子及說明"*）：
"如某法令包括某條文施行的例子或說明——
(a) 該例子或說明不得視為並無遺漏；及
(b) 如該例子或說明與該條文不相符，則以該條文為準。"

7.56 有關司法管轄權乃基於*"罪行導致在新加坡的嚴重損害，或產生導致在新加坡的嚴重損害的重大風險"*[69]提出，這體現了保護管轄原則。

美國

《電腦欺詐及濫用法案》（《美國法典》第 18 篇第 1030 條）

7.57 正如之前各章所述，在美國，規管電腦網絡罪行的主要聯邦法例是《電腦欺詐及濫用法案》（Computer Fraud and Abuse Act），編纂於《美國法典》第 18 篇第 1030 條。

7.58 《電腦欺詐及濫用法案》所訂的罪行，不少是指（或包括）作出侵害*"受保護電腦"*的特定刑事作為。第 1030(e)(2)條將*"受保護電腦"*界定為：

> "(A) 某財務機構或美國政府專用的電腦，或如屬並非如此專用的電腦，則指由某財務機構或美國政府所使用或為其而使用的電腦，而構成有關罪行的行為會影響由該財務機構或美國政府對該電腦的使用或為其而對該電腦的使用；
>
> (B) 用於或影響州際或對外貿易或通訊的電腦，包括位於美國境外而以影響美國州際或對外貿易或通訊的方式使用的電腦；或
>
> (C) 符合以下說明的電腦——
>
> (i) 屬投票系統的一部分；及
>
> (ii) (I) 用作聯邦選舉的管理、支援或行政；或
>
> (II) 曾在州際或對外貿易中運作或在其他方面影響州際或對外貿易"。

7.59 上文引述的第 1030(e)(2)(B)條中，*"對外"*一詞在 *United States v Ivanov*[70] 中解釋為國際的意思。有評論員提出以下論點：

> "這可能會大幅擴大聯邦域外法律的適用範圍，因為任何連接上互聯網的電腦均可說是用於或影響州際或對

---

69 《新加坡誤用電腦法令》第 13(3)(c)條。

70 175 F Supp 2d 367 (D Conn 2001)。

外通訊，而有關電腦甚至無需位於美國。只要該電腦連接上互聯網，便可形容為以影響美國州際通訊或內外通訊的方式使用。”[71]

7.60 儘管案例已釐清《電腦欺詐及濫用法案》的域外範圍，但如要加入有關域外法律效力的提述，*“受保護電腦”*的法定定義似乎並非最適當的位置。本章檢視的其他司法管轄區，均已訂立特定法例條文，以處理司法管轄權事宜。

案例中的客觀屬地管轄原則

7.61 另外，法庭在 *Ivanov* 案中亦確認了客觀屬地管轄原則：

> “本案中，伊雲洛夫（Ivanov）在公訴書內被控的實質罪行，其擬造成或實際造成的不利影響全部在美國境內發生……縱使〔目標〕電腦是被人藉着從〔美國境外的〕遠處發起和控制的繁複程序所取用，亦不改取用電腦的行為（即法規禁止的部分不利影響）是在該等電腦實際所在的地方（即位於康涅狄格弗農〔Vernon〕……）發生這一事實。”

小組委員會的看法

初步考慮

新法例應訂明司法管轄權規則

7.62 在電腦網絡罪行案件中，犯罪者在一個實際地點進行的作為，可透過互聯網在短時間內影響多個實際地點的無數受害人，當中可能涉及電腦網絡空間的大量通訊。我們認為，電腦網絡罪行的性質，充分支持香港法律適用於域外範圍。

7.63 為防止日後的法律程序出現爭議，新法例應明確訂明適用於所訂罪行的司法管轄權規則。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，便會知道香港的法律立場。

---

71 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2nd edition, 2015)，第 479 頁；類似看法見 Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press, 2007)，第 5.18 段（*“這實際上是把領域範圍延伸至全球，因為任何連接上互聯網的電腦均可能包括在內”*）。

7.64 例如，假若新法例應規定在香港境外的人如入侵在香港的電腦，便屬干犯香港法律所訂罪行，那麼該人若前往香港，便可被拘捕。如該人一直留在香港的司法管轄區範圍以外，香港的執法機關可適時向其他司法管轄區的執法機關尋求協助。

7.65 在上述例子中，我們明白該人的作為在該作為作出的地方，可能並不構成罪行。撇開可能與雙重犯罪原則相關的問題不談，我們認為，如該作為對香港造成影響，便有理由支持根據香港法律將該作為定為罪行。[72] 按照我們指導原則的精神，[73] 任何人作出任何作為的權利，須與保障公眾免因該作為而可能受害的需要互相平衡，當中須衡量該作為所造成的傷害，與法律對該人作出該作為的權利所擬施加的限制比較，是否更為重大和帶來更嚴重損害。

有理由制定限制較少的司法管轄權規則

7.66 當執法機關決定是否向其他司法管轄區尋求協助時，實際上會考慮該等司法管轄區的執法機關會如何回應。我們知悉，由於大規模的電腦網絡罪行案件在香港並不常見，因此這類協助請求通常並不可行。即使案中損失總額龐大，每名受害人所涉的金錢價值可能不高。

7.67 在上述背景下，據我們理解，如新法例包含多種司法管轄權規則，執法機關及檢控部門均認為會有用處。背後的想法是，假如司法管轄權規則設有太多限制，以致香港的罪行不適用於若干應受譴責的行為，便會完全無法提出檢控。相比之下，假若罪行適用於這些行為，而檢控部門保留酌情權，決定應否提出檢控，這做法較為可取，亦可為公眾提供保障，切合我們的指導原則。

應專門制定切合各項罪行的司法管轄權規則

7.68 與此同時，我們的比較研究顯示，國際慣例是司法管轄區在合理範圍內，為其法律的任何域外應用訂定條文，這與普通法一般奉行屬地管轄原則的做法一致。例如：

(a) 新西蘭法律委員會曾建議新西蘭的法庭對於在任何地方所犯的誤用電腦罪行一律具有司法管轄權，但這項建議顯然未有落實。[74]

---

72 例如因為目標電腦處於香港。

73 導言第 12 段。

74 第 7.50 至 7.51 段。

(b) 雖然《新加坡誤用電腦法令》第 13(1)及(2)條似乎賦予該法令無限的域外法律效力，但該等條文的適用範圍受第13(3)條所限。[75]

如有關電腦網絡攻擊與香港並無任何事實聯繫及因果聯繫，香港法律似乎並無理據規管在其他司法管轄區發動，並針對第三方司法管轄區內目標的電腦網絡攻擊。

7.69 我們認為，香港依循上述國際慣例，亦屬恰當。在相互尊重的原則下，香港應能夠向其他司法管轄區據理解釋其法律立場。我們亦緊記需要顧及不同持份者的利益，而該利益可能會視乎有關罪行而有所不同。因此，我們參照以下事實情況，依次討論本諮詢文件所建議的罪行：[76]

(a) 罪行的任何“主要元素”[77] 在香港發生，即使其他“主要元素”在其他地方發生；[78]

(b) 犯罪者是“香港人”；[79]

(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）。

7.70 我們在討論期間緊記一點，就是決定是否提議採用某種事實情況很大程度上涉及主觀判斷，並無絕對答案。就各項建議的罪行，我們所建議採用的司法管轄權規則載於下文。

---

75 第 7.53 至 7.54 段。

76 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。

77 如以術語表達，即如《刑事司法管轄權條例》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）”*。

78 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。

79 其他司法管轄區的法例可能提述有關司法管轄區的國民或公民。就香港的情況而言，我們參考其他法律範疇的現有罪行，建議“香港人”這概念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。

非法取覽程式或數據

事實情況(a)、(d)及(e)

7.71 我們認為將事實情況(a)、(d)及(e)應用於這項建議的罪行，應無爭議。我們會於下文討論事實情況(b)及(c)。

事實情況(b)

7.72 支持將事實情況(b)[80]應用於建議的非法取覽程式或數據罪的論點是：香港法律應阻嚇香港人非法取覽儲存於例如雲端伺服器的數據（不論該伺服器實際位於何處），因為在電腦網絡空間上，實際位置通常無關重要。例如，網上電郵系統普遍盛行，一般採用雲端技術。雲端伺服器已成為罪犯的主要目標，雲端儲存的重要性可能於未來數年超越普通儲存。

7.73 然而，我們留意到，事實情況(b)亦涵蓋犯罪者（儘管是“香港人”）、其作為、所用器材、有關數據和受害人全部處於香港境外的案件，而沒有任何“香港人”受害。香港的執法機關或難以取證和證明犯罪者的作為。正面來看，如案情嚴重，受影響司法管轄區的執法機關可能會採取行動，香港的執法機關會適時提供協助。

7.74 權衡所有因素之下，我們不建議將事實情況(b)應用於建議的非法取覽程式或數據罪。

事實情況(c)

7.75 就這項建議的罪行而言，事實情況(c)[81]引起誰是受害人的問題。舉例來說，如某人在非洲對歐洲的雲端伺服器進行黑客入侵，而該伺服器持有的數據由不同人（包括“香港人”）擁有，那麼受害人應是該雲端伺服器的擁有人，還是該等數據的擁有人？特別考慮到案中的黑客入侵不一定是針對該雲端伺服器的任何特定使用者。

7.76 我們認為，受害人這概念應採用寬廣的定義。在上述情況中，該雲端伺服器的擁有人及該等數據的擁有人均應視為潛在受害人。此外，為與這項建議的罪行的焦點（非法取覽*程式或數據*）一致，重點應是須予保護的數據，而不管最終應視誰人為受害人。

---

80 犯罪者是“香港人”。

81 受害人是“香港人”。

7.77 我們繼而得出結論，將事實情況(c)應用於建議的非法取覽程式或數據罪，是會有用處的。如採納前段的考慮因素，只要雲端伺服器的擁有人或有關數據的擁有人是“香港人”，這項建議的罪行便會基於事實情況(c)而適用。這個法律立場能盡量擴大這項建議的罪行所提供的保障範圍。

雙重犯罪

7.78 就這項建議的罪行而言，有人或會認為施加雙重犯罪的規定是合理的做法，因為技術上來說，取覽程式或數據可輕易發生。如某人在香港境外某地方所作的作為，在該地方並不構成罪行，若要求該人因着該作為而在香港就這項建議的罪行負上法律責任，未必恰當。

7.79 然而，相反的論點是，施加雙重犯罪的規定可能有違加強保障公眾這目的。除了檢控部門需要證明被告人的作為，根據該作為作出的地方的法律屬罪行之外，另一相關因素是，某些司法管轄區的法律標準未必能與香港的法律標準比擬。如設有雙重犯罪的規定，有人或會故意在電腦網絡攻擊並不構成罪行的地方發動攻擊，藉此逃避法律責任。香港可能最終會更易遭受這類電腦網絡攻擊。

7.80 我們的比較研究顯示，其他司法管轄區對於在電腦網絡罪行法例中是否施加雙重犯罪的規定，並沒有任何主流或統一的做法。我們認為，要解決上述難題，關鍵在於意會*就嚴重罪行而言*，支持*不*施加雙重犯罪的規定之理據較為有力。我們決定採取折衷方法，即雙重犯罪的規定應適用於非法取覽程式或數據的*簡易程序*罪行，但不適用於*加重*罪行。由於後者涉及被告人在取覽有關程式或數據後，意圖進行其他犯罪活動，被告人難以辯稱不施加雙重犯罪的規定，會造成不公。

7.81 我們得出建議的非法取覽程式或數據的簡易程序罪行應設有雙重犯罪的規定這看法時，整體上採納了《刑事司法管轄權條例》第 7 條的精神，[82] 該條體現了香港法律下雙重犯罪的概念。此外，我

---

82 《刑事司法管轄權條例》第 7 條對乙類罪行的定罪施加雙重犯罪規定，乙類罪行即第 6(1)條所指的串謀犯甲類罪行或串謀詐騙，以及第 6(2)條所指的企圖犯甲類罪行或煽惑他人犯甲類罪行。第 7 條的內容是：

“(1) 如為實施所協定的行為過程而會在某個階段涉及——

(a) 一方或超過一方的作為或不作為；或

(b) 其他事情的發生，

而根據在該作為、不作為或事情擬發生的地方的有效法律，該作為、不作為或事情是構成一項罪行的，則任何人只有在此情況下方被判犯了可憑藉第 6(1)條審訊的罪行。

們認為，如犯罪者因在香港境外所作的作為而被控這項建議的簡易程序罪行，該作為本身或連同就該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。

---

(2) *如任何人所構想的事會涉及犯一項該事或其任何部分擬發生的地方的有效法律所訂的罪行，則該人只有在此情況下方被判犯了可憑藉第6(2)條審訊的罪行。"*

非法截取電腦數據

事實情況(a)、(c)、(d)及(e)

7.82 基於上文就首項建議的罪行（非法取覽程式或數據罪）所提出的類似理由，我們建議將事實情況(a)、(c)、(d)及(e)應用於建議的非法截取電腦數據罪。

事實情況(b)

7.83 事實情況(b)是犯罪者是“香港人”。就建議的非法截取電腦數據罪而言，其特色傾向支持將新法例的阻嚇作用視為重點，這支持採納事實情況(b)這觀點：

(a) 這項建議的罪行不受地域限制。

(b) 假設建議 4(a)獲採納，[83] 便須就這項建議的罪行證明被告人懷有不誠實或犯罪目的。

7.84 然而，上文就反對首項建議的罪行採納事實情況(b)所提出的論點，[84] 在此處同樣適用，這些論點扼要覆述如下：

(a) 在只符合事實情況(b)的案件中，很可能並非傷害“香港人”，而是傷害其他司法管轄區的人。由該等司法管轄區的執法機關檢控犯罪者，是較為理想的做法。

(b) 由於需要向其他司法管轄區取證，故此在香港提出檢控可能並不可行（尤其是當案情錯綜複雜）。

7.85 此外，雖然有人或會認為香港的法庭應對事實情況(b)的案件具有司法管轄權，因為任何被截取的數據其後均可能在香港被不當使用，但相反的論點則指出，香港的法庭應只在該等數據實際被不當使用時才行使司法管轄權。

7.86 衡量上述考慮因素後，我們不建議將事實情況(b)應用於建議的非法截取電腦數據罪。

---

83 第 3 章。

84 第 7.73 段。

雙重犯罪

7.87 儘管在電腦網絡空間，數據截取難免因着該空間所涉技術而發生，建議的非法截取電腦數據罪只針對懷有不誠實或犯罪目的而行事的人。因此，這項建議的罪行類似非法取覽程式或數據的加重罪行，[85] 多於類似非法取覽程式或數據的簡易程序罪行。[86]

7.88 為貫徹一致，我們認為不應就這項建議的罪行施加雙重犯罪的規定。我們提出這項建議，旨在避免罪犯利用該規定，因着他們的作為在香港境外某些地方並不構成罪行（例如因為當地的法律體制未盡完善），而故意在該等地方作出該作為。

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）。

非法干擾電腦數據

事實情況(a)、(c)、(d)及(e)

7.89 同樣地，我們相信將事實情況(a)、(c)、(d)及(e)應用於建議的非法干擾電腦數據罪這點並無爭議。我們因此提出相應建議，並提

---

85 我們就此建議不施加雙重犯罪的規定（第7.80段）。

86 我們就此建議應施加雙重犯罪的規定（第7.80段）。

議將事實情況(d)[87]應用於這項建議的罪行時，重點應放在目標程式或數據的位置，而非儲存目標程式或數據的電腦的位置。

事實情況(b)

7.90 只有事實情況(b)[88]有待討論。讀者會記得我們不建議將事實情況(b)應用於首兩項建議的罪行。經考慮後，我們同樣不建議將事實情況(b)應用於建議的非法干擾電腦數據罪。

雙重犯罪

7.91 我們留意到，如雙重犯罪的規定不適用於這項建議的罪行，便會與我們就首兩項建議的罪行所提出的建議一致。如是者，任何人如在另一司法管轄區干擾數據，不論該項干擾在當地是否構成罪行，亦可能須根據香港法律負上法律責任。

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）。**

---

87 目標電腦、程式或數據處於香港。

88 犯罪者是“香港人”。

非法干擾電腦系統

事實情況

7.92 我們建議用相同方式處理前項罪行及這項建議的罪行，[89] 故此我們此處可以相對簡略。這兩項建議的罪行關係密切，顯示兩者的司法管轄權範圍應該一致，但將事實情況(d)[90] 應用於建議的非法干擾*電腦系統*罪時，重點應放在目標電腦的位置，而非任何程式或數據的位置。

雙重犯罪

7.93 我們亦不建議對這項建議的罪行施加雙重犯罪的規定。

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）。**

---

89 第 5 章建議 7(a)及(b)。

90 目標電腦、程式或數據處於香港。

提供或管有用作犯罪的器材或數據

建議的罪行的基本及加重形式，應採用相同的司法管轄權規則

7.94 我們建議，這項建議的罪行應包括基本形式及加重形式，視乎被告人是否意圖任何人將有關器材或數據用作犯罪。[91]

7.95 然而，我們認為，由於這項基本罪行適用於被製造或改裝以用作犯罪的器材或數據，因此即使是基本罪行，亦應視為嚴重。雖然這項建議的罪行的兩種形式輕重有別，但當中差距不至於足以支持兩者有不同的司法管轄權規則。我們提議將同一套司法管轄權規則套用於這兩種形式。

事實情況(c)及(d)

7.96 這項建議的罪行的案件未必涉及任何受害人或任何目標電腦、程式或數據，但事實情況(c)[92] 及(d)[93] 分別以這些元素為前提，因此，我們認為這些事實情況並不適合這項建議的罪行。

事實情況(a)、(b)及(e)

7.97 在考慮其他事實情況時，我們緊記這項建議的罪行有兩部分：

(a) 就*管有*器材或數據的部分而言，有人或會認為管有這個概念會伴隨個人，而個人處於實際位置。然而，假如器材或數據儲存於例如雲端伺服器，若說是在實際位置管有該器材或數據，未必能反映現實。

(b) 就*提供*器材或數據的部分而言，如實際位置在香港境外的人上載惡意軟件到互聯網，理論上這套惡意軟件可提供予世界上每個角落任何能接達互聯網的人。這項建議的罪行所規管的器材和數據，不少都非常有可能在暗網上找到，而買賣雙方的實際位置均無從追蹤。

7.98 在上述前提下，加上我們認為這項建議的罪行性質較其餘四項建議的罪行獨特，[94] 我們建議將事實情況(a)[95] 、(b)[96] 及(e)[97] 應用於這項建議的罪行。

---

91 第 6 章建議 9(a)及(d)。

92 受害人是“香港人”。

93 目標電腦、程式或數據處於香港。

雙重犯罪

7.99 我們建議首四項建議的罪行均不應施加雙重犯罪的規定，非法取覽程式或數據的簡易程序罪行則除外。

7.100 我們認為，儘管建議的提供或管有用作犯罪的器材或數據罪性質獨特，相同的理據亦適用於該罪行，因此有關建議亦同樣適用。我們留意到，我們的建議有助各項建議的罪行貫徹一致。

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）。

---

94 雖然《英格蘭誤用電腦法令》所訂罪行大多規定須*"與本地司法管轄權有重大聯繫"*，但就第 3A 條所訂罪行而言（*"製造、供應或取得用於第 1、3 或 3ZA 條所訂罪行的物品"*），這似乎並非必要。見第 7.43 段。

95 罪行的任何"主要元素"在香港發生，即使其他"主要元素"在其他地方發生。

96 犯罪者是"香港人"。

97 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）。

第 8 章　判刑

引言

8.1　在前面各章，我們建議訂立五類依賴電腦網絡的罪行，並建議應適用於每類罪行的司法管轄權規則。本章：

(a) 載述源自香港案例的相關原則、觀點及其他附帶意見，表達法庭對電腦網絡罪行的看法；

(b) 讓讀者了解本諮詢文件的附錄，當中概述香港及其他司法管轄區的現行法律就有關罪行所訂的最高刑罰；並

(c) 列出我們就建議的罪行所建議的適當最高刑罰。

香港法庭對電腦網絡罪行的看法

8.2　*HKSAR v Chan Chi Kong*[1] 涉及首宗根據《刑事罪行條例》（第 200 章）第 59(1A)及 60(1)條就 *"誤用電腦"* 提出的檢控。[2] 高等法院上訴法庭有以下論述：

> "香港特別行政區是舉世聞名的國際商業及金融中心，商業和銀行業的各個範疇均倚賴現代電腦科技。對於那些相當可能損害或有可能損害他人對本港的信任和信心的案件，法院有責任確保施以具阻嚇性的刑罰，以防止有類似傾向的其他人犯這類罪行……我們強調，這些罪行均相當嚴重，必須施以合乎案件情況的刑罰。"[3]

8.3　在 *香港特別行政區　訴　秦瑞麟*（*HKSAR v Tsun Shui Lun*），[4] 被告人根據第 161 條被定罪。高等法院首席法官陳兆愷雖然判他刑期上訴得直，但卻駁回他就定罪提出的上訴，並指出：

> "在現代社會，我們的生活均離不開電腦。現今的日常活動均高度倚賴電腦，實難想像沒有電腦會是怎樣的情況。人們不僅透過電腦進行商業交易，亦以電腦儲存機

1　[1997] 3 HKC 702, CACC 245/1997（判決日期：1997 年 9 月 25 日）。
2　根據被告人代表大律師的陳詞（見判詞第 706 頁 H 行）。
3　見上文註腳 1，第 709 頁 C – E 行。
4　[1999] 3 HKLRD 215, HCMA 723/1998（判決日期：1999 年 1 月 15 日）。

> 密甚至秘密的資料，醫院的電腦化運作更是拯救無數生命。若電腦被誤用或濫用，或姑息有犯罪或不誠實意圖或目的而取用電腦的行為，便可能會引致嚴重後果。這些情況均必須避免……
>
> 第 161 條涵蓋種類極為廣泛的犯罪和不誠實活動。時至今日，透過取用他人的電腦並摘取當中所載資料，便可犯非常嚴重的罪行或欺詐罪，一些例子包括：竄改銀行紀錄、把大額款項從某一帳戶轉往另一帳戶，以及偷竊顧客名單和業務紀錄等秘密程式及數據。有關活動可能非常嚴重，有這類意圖或為這類目的而取用電腦的嚴重性亦不遜於此。
>
> 第 161 條所訂最高刑罰為五年監禁……本席認為，若為犯罪或進行欺詐而取用電腦，或該項取用的意圖是產生巨大獲益或導致他人蒙受嚴重損失（不論是在經濟上或所有權上的損失，還是其他方面的損失），便應判處即時監禁刑罰。若取用並非為個人利益，而是為了破壞他人的系統或者令他人深感尷尬和困擾，也不可排除判監的可能性。但在這宗特別案件中，本席不適宜就第 161 條所訂罪行制定判刑指引。”[5]

8.4 在*香港特別行政區 訴 譚曦倫及其他人*（*HKSAR v Tam Hei Lun & Ors*），[6] 上訴法庭同樣拒絕就第 161 條頒布判刑指引，因為當時(a)曾根據第 161 條提出的檢控少於十宗，而且(b)受該條規管的各類罪行均很大機會未為人認識或了解。[7] 然而，該法庭有以下評析：

> “法院就《刑事罪行條例》第 60 及 161 條所訂罪行決定適當的刑罰時，無疑須考慮許多因素：首要考慮的，是對受害人造成的損失及損壞，另外是有關罪行對受害人的嚴重性。有關取用的目的，以及取用者在經濟上或其他方面的任何獲益，亦會是相關因素。
>
> 就目前情況而言，我們認為只需指出，若有人為了獲益或某種其他理由而取用他人的電腦，該作為在多方面均與入屋犯法類似。實際發生的情況是，有人曾取用他人的電腦，猶如某人進入某住房或辦公室後翻弄抽屜或檔

---

5 同上，第 228 頁 H 行－第 229 頁 F 行。

6 [2000] 3 HKC 745, HCMA 385/2000（判決日期：2000 年 10 月 9 日）。

7 同上，第 749 頁 C 行。

案櫃一樣。入屋犯法罪的某些層面，無疑並不見於在未獲授權下取用電腦，故上述的類比絕非完美。儘管我們表示認為不適宜在目前制定指引，但亦希望指出，除非有極不尋常的情況，否則不適宜就違反第 161 條的罪行判處非扣押刑罰。”[8]

8.5 在 *HKSAR v Ko Kam Fai*，[9] 被告人承認多項（涉及兩名受害人的）刑事恐嚇控罪和（涉及該等受害人的電腦及電郵帳戶的）刑事損壞控罪，分別違反《刑事罪行條例》（第 200 章）第 24 及 60(1)條。鑑於前段所引述*譚曦倫*案中的附帶意見，主審法官把這些罪行如同根據第 161 條提出檢控的罪行看待，並判處具阻嚇性的即時監禁刑罰。上訴法庭讚揚這種做法。[10]

8.6 鑑於*譚曦倫*案中的附帶意見，包鍾倩薇法官亦在 *HKSAR v Choy Yau Pun*[11] 作出以下裁定：

“……即使就犯罪者的情況而言，社會服務令是可行的判刑選擇，亦必需有極不尋常的情況，才可以把社會服務令或任何其他形式的非扣押刑罰視為適當選擇，以替代違反第 161 條的罪行的扣押刑罰……

……但實情是他犯了違反第 161 條的罪行，而他更是背叛了顧客的信任而犯罪（這位顧客把自己的電腦交給他維修）。若如同本案的情況，恰當判刑的作用既是阻嚇以一般方式違反第 161 條的行為，亦是阻嚇背叛信任的話，要把社會服務令視為適當的刑罰便會比平常更難。”[12]

8.7 同樣地，在*李聞偉 訴 律政司司長*（*Li Man Wai v Secretary for Justice*），[13] 終審法院表示，第 161 條所訂罪行可屬嚴重性質：

“根據《刑事罪行條例》第 161 條可判罰的該類罪行無疑非常嚴重——該類罪行可視為一種盜竊，每每造成嚴重後果，而受害人卻一直無從得知事情的始末緣由。隨着電腦被廣泛使用及科技進步，這種非常有用的設備已

8 同上，第 749 頁 F 行－第 750 頁 A 行。
9 [2001] 3 HKC 181, CACC 83/2001（判決日期：2001 年 6 月 20 日）。
10 同上，第 183 頁 H 行及第 185 頁 B 行。
11 [2002] 3 HKLRD 156, HCMA 450/2002（判決日期：2002 年 6 月 24 日）。
12 同上，第 159 頁 H－I 行及第 160 頁 D－E 行。
13 (2003) 6 HKCFAR 466, FACC 6/2003（判決日期：2003 年 11 月 6 日）。

> 成為我們日常生活的一環。因此，保護電腦的完整性，尤其是稅務局電腦系統的完整性，就愈發重要。然而，現行法例並非一律懲處在未獲授權下取用電腦的各種情況，而是只禁止在未獲授權下不誠實地提取和使用資料。案中是否涉及不誠實的情況，正是陪審團須就每宗案件裁斷的事實問題。”[14]

8.8 在*廖偉信 訴 香港特別行政區*（*Liu Wai Shun v HKSAR*），[15] 任職軟件發展人員的被告人被僱主開除，為了報復僱主，被告人刪除一些電腦檔案，令擁有相關軟件的僱主無法使用該軟件。被告人根據《刑事罪行條例》（第 200 章）第 60(1)及 161(1)(a)條被判罪名成立，判處罰款。高等法院原訟法庭駁回他的上訴。終審法院上訴委員會拒絕其上訴許可申請，並論述如下：

> “我們希望就刑罰指出以下一點：故意損壞電腦軟件及數據的行為，當然可對使用有關軟件及數據的機構在經濟及其他方面造成極大傷害。本案所造成的損壞可以補救，主要是因為申請人的前僱主採取了防範措施，申請人在這點上算是走運了。這類案件所判處的刑罰，應恰當地反映所造成損壞的嚴重性。若所引致的損壞更加嚴重，罰款便不會是足夠的刑罰。據我們得悉，上訴法庭已表明這類案件通常應判處扣押刑罰，我們認為上訴法庭的這一表述甚是恰當。”[16]

8.9 在 *HKSAR v Luk Wa*，[17] 法官在判刑時的以下論述，與上述案例相符一致：

> “電腦及互聯網的使用，是現代日常生活的重要一環。幾乎各行各業均須依靠電腦及互聯網，才能操作和暢順運作。電腦和互聯網使用的完整性不容破壞，實屬至關重要。故此，法院一向極為嚴肅看待關於不誠實使用電腦的罪行。”[18]

---

14 同上，第 474 頁 H – J 行。
15 FAMC 30/2004（判決日期：2004 年 9 月 27 日）。
16 同上，第 7 段（終審法院常任法官李義）。
17 DCCC 17/2011（判決日期：2011 年 2 月 18 日）。
18 同上，第 29 段（邱智立法官）。

8.10 同時，正如另一位法官在*香港特別行政區 訴 梁禮仲*（*HKSAR v Leung Lai Chung*）[19] 判刑時指出，不同案件的判刑會有差異。尤其是，*"循公訴程序起訴的罪行，有別於循簡易程序審訊的罪行"*。[20]

香港及其他司法管轄區的現行法律

8.11 本諮詢文件的附錄，旨在綜述香港及其他司法管轄區各項電腦網絡罪行的最高刑罰，並附有相關條文的編號（以粗體表示）及標題（以斜體表示）。前面各章已詳細探討這些罪行。附錄並無提述《示範法》，這是因為《示範法》沒有就當中建議的罪行提出最高刑罰建議。

小組委員會的看法

各項建議的較嚴重罪行

宜訂定劃一的最高刑罰

8.12 我們在第 7 章建議，除了建議的非法取覽程式或數據的簡易程序罪行外，本諮詢文件所建議的各項罪行，均不應施加雙重犯罪的規定。這項建議反映了我們認為建議的各項非簡易程序罪行，均可造成重大傷害這個觀點。經討論後，我們贊成以下罪行應訂定劃一的最高刑罰：

(a) 建議的非法取覽程式或數據的加重罪行（第 2 章）；

(b) 建議的非法截取電腦數據罪（第 3 章）；

(c) 建議的非法干擾電腦數據的基本罪行，以及非法干擾電腦系統的基本罪行（第 4 及 5 章）；及

(d) 建議的提供或管有用作犯罪的器材或數據的加重罪行（第 6 章）。

---

19 DCCC 416/2009（判決日期：2010 年 2 月 1 日）。

20 同上，第 17 段（源麗華法官）。

循簡易程序定罪及循公訴程序定罪

8.13 我們亦明白電腦網絡罪行所致傷害的嚴重程度差別甚大，既可輕微至不造成關鍵性傷害，亦可嚴重至令某重要系統（例如供電系統或鐵路系統）完全癱瘓。由於導致的後果可以如此迥異，故我們建議，前段(a)、(b)、(c)及(d)項中每項建議的罪行，應訂有兩項最高刑罰：一項適用於循簡易程序定罪，另一項則適用於循公訴程序定罪。

循公訴程序定罪的最高刑罰

8.14 在仔細討論時，我們考慮了以下因素：

(a) 裁判法院及區域法院可判處的最高刑罰分別為三年及七年監禁，[21] 高等法院則可判處較重的刑罰。

(b) 建議的非法取覽程式或數據的加重罪行，與第 161 條所訂現有罪行[22] 性質類似，該現有罪行的最高刑罰為五年監禁。若這項建議的加重罪行的犯罪者意圖作出的其他作為，與使（比如說）香港的公共交通系統癱瘓同樣令人髮指，上述的最高刑罰便似乎與刑責程度並不相稱。[23]

(c) 《電訊條例》（第 106 章）第 27(b)條[24] 只就損壞、移走或干擾電訊裝置，而意圖是截取或找出任何訊息的內容，訂立*簡易程序*罪行。另外，該條並非針對截取*電腦數據*的特定條文。[25] 因此，該條所訂最高刑罰（第 4 級罰款[26] 及兩年監禁）的參考價值有限。

---

21 見司法機構，《法庭服務簡介——裁判法院》：
"裁判法院的最高刑罰一般為監禁 2 年和罰款 10 萬元。但是，當法庭同時處理兩項或以上的可公訴罪行時，裁判官可判處最高 3 年的刑期。就某些條例而言，單一罪行可判處監禁 3 年和罰款 500 萬元。"
亦見司法機構，《法庭服務簡介——區域法院》：
"區域法院可審理除謀殺、誤殺和強姦外的所有嚴重刑事案件，可判處的最長監禁刑期是七年。"

22 *"有犯罪或不誠實意圖而取用電腦"*（見第 2.6 段）。

23 我們同意，大多數案件的案情都可能較為輕微，故法院無須判處最高刑罰。2015 年至 2020 年 9 月期間，被裁定犯第 161 條所訂罪行的犯罪者被判感化令、社會服務令、罰款或監禁 10 日至 1 年零 8 個月不等。

24 *"蓄意損壞電訊裝置"*（見第 3.12 段）。

25 第 3.14 至 3.16 段。

26 根據《刑事訴訟程序條例》（第 221 章）附表 8，現為 25,000 元。

(d) 建議的非法干擾電腦數據罪及非法干擾電腦系統罪，均關乎目前由《刑事罪行條例》（第 200 章）第 60 條所處理的行為。[27] 根據該條，犯罪者通常可處十年監禁，如案件涉及危害生命，則可處終身監禁。[28]

(e) 建議的提供或管有用作犯罪的器材或數據的加重罪行，與《刑事罪行條例》（第 200 章）第 62 條所訂罪行[29] 類同，後者可處十年監禁。[30]

(f) 至於第 8.12 (a)、(b)、(c)及(d)段所述的各項建議罪行，在刑責程度上與相若罪行如何比較，可參考《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：

(i) 盜竊罪可處 10 年監禁；[31]

(ii) 欺詐罪可處 14 年監禁；[32]

(iii) 勒索罪可處 14 年監禁；[33]

(iv) 入屋犯法罪可處 14 年監禁；[34]

(v) 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；[35] 及

(vi) 搶劫罪可處終身監禁。[36]

(g) 我們的比較研究顯示，其他司法管轄區的最高刑罰各有差異，原因是該等刑罰反映有關罪行的不同定義。其他司法管轄區的判刑原則，亦可能與香港有別。

---

27 *"摧毀或損壞財產"*（見第 4.4 及 5.7 段）。
28 《刑事罪行條例》（第 200 章）第 63 條。
29 *"管有任何物品意圖摧毀或損壞財產"*（見第 6.6 段）。
30 《刑事罪行條例》（第 200 章）第 63(2)條。
31 《盜竊罪條例》（第 210 章）第 9 條。
32 同上，第 16A(1)條。
33 同上，第 23(3)條。
34 同上，第 11(4)條。
35 同上，第 12(3)條。
36 同上，第 10(2)條。

8.15 不論我們所建議的監禁年期長度如何，某程度上總有武斷成分。我們建議，第 8.12 (a)、(b)、(c)及(d)段所述各項建議罪行的最高監禁刑期應訂為 14 年。[37] 我們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)《盜竊罪條例》（第 210 章）所訂的上述罪行，[38] 以及(b)其他司法管轄區的有關罪行。[39]

循簡易程序定罪的最高刑罰

8.16 我們認為，循簡易程序定罪的最高監禁刑期若訂為兩年，便會與關於循公訴程序定罪的案件的上述建議相稱。故此我們建議，循簡易程序定罪的最高監禁刑期，應訂為兩年。

建議的非法取覽程式或數據的簡易程序罪行

8.17 在某程度上，這項建議的罪行與第 27A 條所訂的罪行[40] 性質相若。然而，第 27A 條甚少獲援引，而且我們認為該條的最高刑罰（第 4 級罰款）[41] 頗輕，故建議的罪行不宜採納該刑罰。雖然這項建議的罪行適用於在未獲授權下取覽本身，犯罪者只是“看看”目標電腦的程式或數據，並沒有造成干擾，但我們的看法是，即使是簡易程序案件，亦應有判監的可能性。

8.18 我們建議，建議的非法取覽程式或數據的簡易程序罪行的最高監禁刑期，應訂為兩年，因此該罪行將可在裁判法院審訊。

---

37 除了訂立有關罪行的法例外，可能亦須參閱其他法例條文，才能了解所有可供採用的判刑選擇。舉例來說，即使訂立有關罪行的法例沒有提述罰款或補償，裁判官或法庭亦具有司法管轄權：
(a) 根據《裁判官條例》（第 227 章）第 92 條或《刑事訴訟程序條例》（第 221 章）第 113A 條，判處罰款；及
(b) 根據《裁判官條例》（第 227 章）第 98 條或《刑事訴訟程序條例》（第 221 章）第 73 條，命令支付補償。

38 第 8.14 (f)段。

39 本諮詢文件的附錄。

40 *“藉電訊而在未獲授權下取用電腦資料”*（見第 2.11 段）。

41 根據《刑事訴訟程序條例》（第 221 章）附表 8，現為 25,000 元。

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

8.19 正如第 4 及 5 章[42] 所論述，我們：

(a) 認為保留《刑事罪行條例》（第 200 章）第 60(2)條所訂的加重罪行較為可取；並

(b) 建議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。

8.20 為求與刑事損壞罪保持貫徹一致，我們提議就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，採納《刑事罪行條例》（第 200 章）第 63(1)條現時訂明的最高刑罰，亦即終身監禁。

建議的提供或管有用作犯罪的器材或數據的基本罪行

8.21 正如第 6 章所建議，這項建議的罪行與相關加重罪行的重要區別，在於被告人是否意圖使有關器材或數據用作犯罪。[43] 這兩種形式可讓人們知道不同的刑罰會適用於以下兩項罪行：一項是蓄意提供或管有用作犯罪的器材或數據，並意圖使該器材或數據如此使用，另一項是蓄意提供或管有用作犯罪的器材或數據，但沒有意圖使該器材或數據如此使用。

8.22 我們在考慮這項建議的基本罪行的最高刑罰時，曾提出兩個方案：

(a) 方案一是五年監禁，這參考了第 161 條所訂現有罪行。

(b) 方案二是七年監禁，即相關加重罪行的建議最高刑罰[44] 的一半。

8.23 我們認為，由於這項基本罪行適用於被製造或改裝以用作犯罪的器材或數據，因此即使是基本罪行，亦應視為嚴重罪行。[45] 基於以上原因，我們最終選擇了方案二。

---

42 第 4.96 至 4.98 及 5.61 至 5.63 段。
43 建議 9(d)(ii)。
44 第 8.15 段。
45 第 7.95 段。

建議 16

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。

第 9 章　綜合建議及諮詢問題

引言

9.1　本章綜述按本諮詢文件所建議的五類罪行而劃分的各項建議及諮詢問題。這些建議及諮詢問題並非依照它們在前面各章出現的次序逐一羅列，我們希望這種編排方式有助讀者對這些建議及諮詢問題作出全面整體的考慮。

9.2　為方便讀者參閱本諮詢文件中的相關討論，我們會在每類建議的罪行之下，分別標示有關建議。

非法取覽程式或數據

——建議 1、2、11 及 16(a)

建議

9.3　在未獲授權下取覽程式或數據，應在新訂針對電腦網絡罪行的特定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。*〔建議 1(a)〕*[1]

9.4　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。*〔建議 1(b)〕*[2]

9.5　在以下情況下，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

1　第 2.89 至 2.106 段。

2　第 2.107 至 2.108 段。

(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 11*〕[3]

9.6 犯罪者應可處下述最高刑罰：

(a) 如屬簡易程序罪行，可處兩年監禁；或

(b) 如屬加重罪行，一經循公訴程序定罪，可處 14 年監禁。〔*建議 16(a)*〕[4]

9.7 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）第 1、2 及 17 條為藍本。〔*建議 1(c)*〕[5]

諮詢問題

9.8 在未獲授權下取覽，應否有任何特定的免責辯護或豁免？

9.9 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：

(a) 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？

(b) 如(a)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？

---

3 第 7.71 至 7.81 段。
4 第 8.12 至 8.18 段。
5 第 2.109 段。

(c) 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？

9.10 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)[6]所述的例子）？〔*建議2*〕[7]

非法截取電腦數據

——建議4、5、12及16(b)

建議

9.11 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。〔*建議4(a)*〕[8]

9.12 建議的罪行應：

(a) 保障一般通訊，而並非只保障私人通訊；

(b) 一般適用於數據（不論有關數據是否元數據）；及

(c) 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。〔*建議4(b)*〕[9]

9.13 在以下情況下，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；

6 第9.30段。
7 第2.110至2.120段。
8 第3.92至3.99段。
9 第3.100至3.110段。

(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 12*〕[10]

9.14 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。〔*建議 16(b)*〕[11]

9.15 除上文第 9.11 及 9.12 段另有規定外，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）。〔*建議 4(c)*〕[12]

諮詢問題

9.16 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）？

9.17 提供 Wi-Fi 熱點或電腦供顧客或僱員使用的真實業務（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）？〔*建議 5*〕[13]

非法干擾電腦數據

——建議 6、13 及 16(c)

建議

9.18 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。

---

10 第 7.82 至 7.88 段。
11 第 8.12 至 8.16 段。
12 第 3.111 至 3.112 段。
13 第 3.113 至 3.122 段。

9.19 新法例應採用《刑事罪行條例》（第 200 章）所訂的以下特點：

(a) 第 59(1A)(a)、(b)及(c)條所訂犯罪行為；[14]

(b) 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）；

(c) 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

(d) 第 60(2)條所訂加重罪行。

9.20 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。〔*建議 6*〕[15]

9.21 在以下情況下，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 13*〕[16]

---

14 第 59(1A)條把“誤用電腦”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。”

15 第 4.81 至 4.99 段。

16 第 7.89 至 7.91 段。

9.22 犯罪者應可處下述最高刑罰：

(a) 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

(b) 如屬加重罪行，可處終身監禁。〔*建議 16(c)*〕[17]

非法干擾電腦系統

——建議 7、8、14 及 16(c)

建議

9.23 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。

9.24 《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。

9.25 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。

9.26 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：

(a) 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）；

(b) 在軟件生產時，在軟件編入缺損程式；及

(c) 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。〔*建議 7*〕[18]

9.27 在以下情況下，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；

---

17 第 8.12 至 8.16、8.19 至 8.20 段。

18 第 5.61 至 5.68 段。

(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 14〕*[19]

9.28 犯罪者應可處下述最高刑罰：

(a) 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

(b) 如屬加重罪行，可處終身監禁。*〔建議 16(c)〕*[20]

諮詢問題

9.29 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？

9.30 就這項建議的罪行而言，非保安專業人員應否有合法辯解，例如：

(a) 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

(b) 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）：

(i) 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

19 第 7.92 至 7.93 段。

20 第 8.12 至 8.16、8.19 至 8.20 段。

(ii) 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*〕[21]

提供或管有用作犯罪的器材或數據

——建議 9、10、15 及 16(d)

建議

9.31 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。〔*建議 9(a)*〕[22]

9.32 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。〔*建議 9(b)*〕[23]

9.33 建議的罪行應適用於：

(a) 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

(b) 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。〔*建議 9(c)*〕[24]

9.34 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）：

(a) 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

(b) 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。〔*建議 9(d)*〕[25]

---

21 第 5.69 至 5.72 段。
22 第 6.73 至 6.79、6.83 至 6.84、6.86 至 6.87 段。
23 第 6.81 至 6.82 段。
24 第 6.76 至 6.77、6.84 段。
25 第 6.73 至 6.80、6.83、6.85 至 6.87 段。

9.35 在以下情況下，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）。*〔建議 15〕*[26]

9.36 犯罪者應可處下述最高刑罰：

(a) 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

(b) 如屬加重罪行，一經循公訴程序定罪，可處 14 年監禁。*〔建議 16(d)〕*[27]

9.37 建議的條文應以英格蘭及威爾斯《1990 年誤用電腦法令》（Computer Misuse Act 1990）第 3A 條，以及新加坡《1993 年誤用電腦法令》（Computer Misuse Act 1993）第 8 及 10 條為藍本。*〔建議 9(e)〕*[28]

諮詢問題

9.38 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？

9.39 如以上問題的答案是“應該”的話，

(a) 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？

---

26 第 7.94 至 7.100 段。

27 第 8.12 至 8.16、8.21 至 8.23 段。

28 第 6.88 段。

(b) 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？〔*建議 10*〕[29]

簡易程序的時效期

建議

9.40 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。〔*建議 3*〕[30]

[29] 第 6.91 至 6.93 段。

[30] 第 2.121 至 2.123 段。

建議的罪行	香港	澳大利亞	加拿大	英格蘭及威爾斯	中國內地	新西蘭	新加坡	美國
(a) 非法取覽程式或數據	**《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 4 級罰款，即港幣 25,000 元（《刑事訴訟程序條例》（第 221 章）附表 8）	**《刑事法典》（聯邦）（Criminal Code (Cth)）第 477.1(1)(a)(i)條**——*"在未獲授權下作出取覽、修改或損害，並意圖干犯嚴重罪行"*[1] • 不超過適用於有關嚴重罪行的刑罰	**《1985 年刑事法典》（Criminal Code 1985）第 326(1)(b)條**——*"盜取電訊服務"* • （循簡易程序定罪）5,000 加元罰款或 2 年減 1 日的監禁，或兩者兼處[2] • （如損失不足 5,000 加元，並循公訴程序定罪）2 年監禁 • （如損失超過 5,000 加元，並循公訴程序定罪）10 年監禁	**《1990 年誤用電腦法令》（Computer Misuse Act 1990）第 1 條**——*"在未獲授權下取覽電腦資料"* • （循簡易程序定罪）不超過法定最高罰款[3] 或 12 個月監禁，或兩者兼處 • （循公訴程序定罪）罰款[4] 或 2 年監禁，或兩者兼處	**《中國刑法》第二百八十五條第一款** • 3 年徒刑或者拘役	**《1961 年刑事罪行法令》（Crimes Act 1961）第 249 條**——*"為不誠實目的而取用電腦系統"* • （作出取用，意圖取得財產等或導致損失）5 年監禁 • （作出取用，並藉此取得財產等或導致損失）7 年監禁	**《1993 年誤用電腦法令》（Computer Misuse Act 1993）第 3 條**——*"在未獲授權下取覽電腦資料"* • 5,000 新加坡元罰款或 2 年監禁，或兩者兼處 • （第二次或其後每次定罪）10,000 新加坡元罰款或 3 年監禁，或兩者兼處	**《美國法典》第 18 篇第 1030(a)(1)至(4)條（18 USC 1030 (a)(1) to (4)）**——*"與電腦有關的欺詐及相關活動"* • 第(a)(1)款所訂罪行 - （通常）罰款[5] 或 10 年監禁，或兩者兼處 - （如以往曾被裁定干犯《美國法典》第 18 篇第 1030 條所訂其他罪行）罰款或 20 年監禁，或兩者兼處

1 《刑事法典》（聯邦）第 477.1(9)條將"嚴重罪行"界定為"可處終身監禁或為期 5 年或以上監禁的罪行"。

2 《1985 年刑事法典》第 787(1)條。

3 《2012 年法律援助、罪犯判刑及懲罰法令》（Legal Aid, Sentencing and Punishment of Offenders Act 2012）第 85 條顯示，*"不超過法定最高罰款"*現時指任何款額（即款額無限）的罰款。

4 《2012 年法律援助、罪犯判刑及懲罰法令》第 85 條顯示，沒有列明最高款額的罰款，指任何款額（即款額無限）的罰款。

5 《美國法典》第 18 篇第 3571 條（18 USC 3571）訂明罰款的最高款額（就個人而言，最高為 250,000 美元，就機構而言，最高為 500,000 美元，或以下數額中的較大者：從有關罪行所得總金錢收益的兩倍，或對被告人以外的人所造成總損失的兩倍）。

建議的罪行	香港	澳大利亞	加拿大	英格蘭及威爾斯	中國內地	新西蘭	新加坡	美國
	《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"* • （循公訴程序定罪）5 年監禁	**《刑事法典》（聯邦）第 478.1 條**—— *"在未獲授權下取覽或修改受限數據"* • 2 年監禁	**《1985 年刑事法典》第 342.1(1)條**—— *"在未獲授權下使用電腦"* • （循簡易程序定罪）5,000 加元罰款或不超過 2 年減 1 日的監禁，或兩者兼處 • （循公訴程序定罪）10 年監禁	**《1990 年誤用電腦法令》第 2 條**—— *"在未獲授權下取覽，並意圖干犯或意圖利便干犯其他罪行"* • （循簡易程序定罪）不超過法定最高罰款或 12 個月監禁，或兩者兼處 • （循公訴程序定罪）罰款或 5 年監禁，或兩者兼處	**《中國刑法》第二百八十五條第二款** • （情節嚴重的）3 年徒刑或者拘役，並處或者單處罰金 • （情節特別嚴重的）3 年以上 7 年以下徒刑，並處罰金	**《1961 年刑事罪行法令》第 252 條**—— *"在未獲授權下取用電腦系統"* • 2 年監禁	• （如導致損壞）50,000 新加坡元罰款或 7 年監禁，或兩者兼處 • （如取用受保護電腦）[6] 100,000 新加坡元罰款或 20 年監禁，或兩者兼處 **《1993 年誤用電腦法令》第 4 條**—— *"意圖犯罪或意圖利便犯罪而取覽"* • 50,000 新加坡元罰款或 10 年監禁，或兩者兼處	• 第(a)(2)款所訂罪行 - （通常）罰款或 1 年監禁，或兩者兼處 - （如為商業利益或私人財務利益等而犯罪）罰款或 5 年監禁，或兩者兼處 - （如以往曾被裁定干犯《美國法典》第 18 篇第 1030 條所訂其他罪行）罰款或 10 年監禁，或兩者兼處

[6] 根據《新加坡誤用電腦法令》第 11(2)條：
"……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或程式或數據是在與下述各項有直接關連的情況下使用的，或對下述各項屬必要的——
(a) 新加坡的安全、防務或國際關係；
(b) 與執行刑事法律有關的機密資料來源的存在或身分；
(c) 提供與通訊基礎建設、銀行及金融服務、公共事業、公共交通或公開密碼匙基礎建設直接有關的服務；或
(d) 保障公眾安全，包括與必要緊急服務（例如警務、民防及醫療服務）有關的系統。"

建議的罪行	香港	澳大利亞	加拿大	英格蘭及威爾斯	中國內地	新西蘭	新加坡	美國
				《2003 年通訊法令》（Communications Act 2003）第 125 條—— *"不誠實地取得電子通訊服務"* • （循簡易程序定罪）不超過法定最高罰款或 6 個月監禁，或兩者兼處 • （循公訴程序定罪）罰款或 5 年監禁，或兩者兼處				• 第(a)(3)款所訂罪行 - （通常）罰款或 1 年監禁，或兩者兼處 - （如以往曾被裁定干犯《美國法典》第 18 篇第 1030 條所訂其他罪行）罰款或 10 年監禁，或兩者兼處 • 第(a)(4)款所訂罪行 - （通常）罰款或 5 年監禁，或兩者兼處 - （如以往曾被裁定干犯《美國法典》第 18 篇第 1030 條所訂其他罪行）罰款或 10 年監禁，或兩者兼處

建議的罪行	香港	澳大利亞	加拿大	英格蘭及威爾斯	中國內地	新西蘭	新加坡	美國
								《美國法典》第 18 篇第 2701 條（18 USC 2701）——*"非法取覽儲存通訊"* • 如犯罪目的在於獲得商業利益、作出惡意摧毀或損壞等： - （首次犯罪）罰款或 5 年監禁，或兩者兼處 - （其後每次犯罪）罰款或 10 年監禁，或兩者兼處 • 如屬任何其他情況： - （首次犯罪）罰款或 1 年監禁，或兩者兼處 - （如以往曾被裁定干犯《美國法典》第 18 篇第 2701 條所訂其他罪行）罰款或 5 年監禁，或兩者兼處

建議的罪行	香港	澳大利亞	加拿大	英格蘭及威爾斯	中國內地	新西蘭	新加坡	美國
(b) 非法截取電腦數據	**《電訊條例》（第 106 章）第 27 條**——*"蓄意損壞電訊裝置"* • （循簡易程序定罪）第 4 級罰款（即港幣 25,000 元）及 2 年監禁	**《1979 年電訊（截取及取覽）法令》（聯邦）（Telecommunications (Interception and Access) Act 1979 (Cth)）第 7(1)條**——*"不得截取電訊"*[7] • （循簡易程序定罪）6 個月監禁 • （循公訴程序定罪）2 年監禁	**《1985 年刑事法典》第 184(1)條**——*"截取"〔私人通訊〕* • （循簡易程序定罪）5,000 加元罰款或不超過 2 年減 1 日的監禁，或兩者兼處 • （循公訴程序定罪）5 年監禁	**《2016 年調查權力法令》（Investigatory Powers Act 2016）第 3 條**——*"非法截取罪"* • （循簡易程序定罪）罰款 • （循公訴程序定罪）罰款或 2 年監禁，或兩者兼處	**《中國刑法》第二百八十五條第二款** 見上文。	**《1961 年刑事罪行法令》第 216B 條**——*"禁止使用截取器材"* • 2 年監禁	**《1993 年誤用電腦法令》第 6 條**——*"在未獲授權下使用或截取電腦服務"* • 10,000 新加坡元罰款或 3 年監禁，或兩者兼處 • （第二次或其後每次定罪）20,000 新加坡元罰款或 5 年監禁，或兩者兼處 • （如導致損壞）50,000 新加坡元罰款或 7 年監禁，或兩者兼處 • （如取用受保護電腦）100,000 新加坡元罰款或 20 年監禁，或兩者兼處	**《美國法典》第 18 篇第 2511(1)條（18 USC 2511(1)）**——*"禁止截取和披露有線、口頭或電子通訊"* • 罰款或 5 年監禁，或兩者兼處

[7] 《1979 年電訊（截取及取覽）法令》（聯邦）第 105 條訂明違反第 7(1)條的最高刑罰。

建議的罪行	香港	澳大利亞	加拿大	英格蘭及威爾斯	中國內地	新西蘭	新加坡	美國
(c) 非法干擾電腦數據	**《刑事罪行條例》（第 200 章）第 60 條**——*"摧毀或損壞財產"* • （第 60(1)條所訂罪行，循公訴程序定罪）10 年監禁 • （第 60(2)條所訂加重罪行，循公訴程序定罪）終身監禁 **《電訊條例》（第 106 章）第 25 條**——*"電訊人員以外的人隱匿訊息等"* • （循簡易程序定罪）第 4 級罰款（即港幣 25,000 元）及 12 個月監禁	**《刑事法典》（聯邦）第 477.2 條**——*"在未獲授權下修改數據，以導致損害"* • 10 年監禁 **《刑事法典》（聯邦）第 477.3 條**——*"在未獲授權下損害電子通訊"* • 10 年監禁 **《刑事法典》（聯邦）第 478.2 條**——*"在未獲授權下損害存於電腦紀錄碟等內的數據"* • 2 年監禁	**《1985 年刑事法典》第 430(1.1)條**——*"與電腦數據有關的損害"* • （循簡易程序定罪）5,000 加元罰款或 2 年減 1 日的監禁，或兩者兼處 • （循公訴程序定罪）以下年期的監禁： - （通常）2 年 - （如損失超過 5,000 加元）10 年 - （如導致生命受到實際危害）終身監禁	**《1990 年誤用電腦法令》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"* • （循簡易程序定罪）不超過法定最高罰款或 12 個月監禁，或兩者兼處 • （循公訴程序定罪）罰款或 10 年監禁，或兩者兼處 **《1990 年誤用電腦法令》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"* • （通常）罰款或 14 年監禁，或兩者兼處	**《中國刑法》第二百八十六條第二款** • （後果嚴重的）5 年徒刑或者拘役	**《1961 年刑事罪行法令》第 250 條**——*"損壞或干擾電腦系統"* • （通常）7 年監禁 • （如犯罪者知悉或理應知悉相當可能會導致生命受危害）10 年監禁 **《1961 年刑事罪行法令》第 258(1)條**——*"意圖欺騙而更改、隱藏、銷毀或複製文件"* • 10 年監禁	**《1993 年誤用電腦法令》第 5 條**——*"在未獲授權下修改電腦資料"* • 10,000 新加坡元罰款或 3 年監禁，或兩者兼處 • （第二次或其後每次定罪）20,000 新加坡元罰款或 5 年監禁，或兩者兼處 • （如導致損壞）50,000 新加坡元罰款或 7 年監禁，或兩者兼處 • （如取用受保護電腦）100,000 新加坡元罰款或 20 年監禁，或兩者兼處	**《美國法典》第 18 篇第 1030(a)(5)條（18 USC 1030 (a)(5)）**——*"與電腦有關的欺詐及相關活動"* • 第 (a)(5)(A) 款所訂罪行 - （通常）罰款或 1 年監禁，或兩者兼處 - （如導致《美國法典》第 18 篇第 1030 (c)(4)(A)(i)條所指明的傷害）罰款或 10 年監禁，或兩者兼處 - （如以往曾被裁定干犯《美國法典》第 18 篇第 1030 條所訂其他罪行）罰款或 20 年監禁，或兩者兼處 - （如犯罪者企圖導致或故意或罔顧後果地導致身體受嚴重損傷）罰款或 20 年監禁，或兩者兼處

建議的罪行	香港	澳大利亞	加拿大	英格蘭及威爾斯	中國內地	新西蘭	新加坡	美國
		《刑事法典》（聯邦）第 477.1(1)(a)(ii)及(iii)條、第 478.1 條 見上文。		• （如： - 因導致第(3)(a)款所述種類的人類福祉嚴重損害（人命損失）或第(3)(b)款所述種類的人類福祉嚴重損害（人類患病或受傷）的作為而干犯該罪行，或因產生導致該損害的重大風險的作為而干犯該罪行；或 - 因導致國家安全嚴重損害的作為而干犯該罪行，或因產生導致該損害的重大風險的作為而干犯該罪行） 罰款或終身監禁，或兩者兼處				- （如犯罪者企圖導致或故意或罔顧後果地導致死亡）罰款或任何刑期的監禁或終身監禁，或兩者兼處 • 第 (a)(5)(B) 款所訂罪行 - （通常）罰款或 1 年監禁，或兩者兼處 - （如導致《美國法典》第 18 篇第 1030 (c)(4)(A)(i)條所指明的傷害）罰款或 5 年監禁，或兩者兼處 - （如以往曾被裁定干犯《美國法典》第 18 篇第 1030 條所訂其他罪行）罰款或 20 年監禁，或兩者兼處

建議的罪行	香港	澳大利亞	加拿大	英格蘭及威爾斯	中國內地	新西蘭	新加坡	美國
								• 第 (a)(5)(C) 款所訂罪行 - （通常）罰款或 1 年監禁，或兩者兼處 - （如以往曾被裁定干犯《美國法典》第 18 篇第 1030 條所訂其他罪行）罰款或 10 年監禁，或兩者兼處

建議的罪行	香港	澳大利亞	加拿大	英格蘭及威爾斯	中國內地	新西蘭	新加坡	美國
(d) 非法干擾電腦系統	**《刑事罪行條例》（第 200 章）第 60 條** 見上文。	**《刑事法典》（聯邦）第 477.2、477.3、477.1(1)(a)(ii)及(iii)、478.1 及 478.2 條** 見上文。	**《1985 年刑事法典》第 430(1.1)條及第 430(4)條** 見上文。	**《1990 年誤用電腦法令》第 3 及 3ZA 條** 見上文。	**《中國刑法》第二百八十五條第二款** 見上文。 **《中國刑法》第二百八十六條第一款** • （後果嚴重的）5 年徒刑或者拘役 • （後果特別嚴重的）5 年以上徒刑	**《1961 年刑事罪行法令》第 250 及 258(1)條** 見上文。	**《1993 年誤用電腦法令》第 7 條——** *"在未獲授權下妨礙使用電腦"* • 10,000 新加坡元罰款或 3 年監禁，或兩者兼處 • （第二次或其後每次定罪）20,000 新加坡元罰款或 5 年監禁，或兩者兼處 • （如導致損壞）50,000 新加坡元罰款或 7 年監禁，或兩者兼處 • （如取用受保護電腦）100,000 新加坡元罰款或 20 年監禁，或兩者兼處	**《美國法典》第 18 篇第 1030(a)(5)條** 見上文。

建議的罪行	香港	澳大利亞	加拿大	英格蘭及威爾斯	中國內地	新西蘭	新加坡	美國
(e) 提供或管有用作犯罪的器材或數據	**《刑事罪行條例》（第 200 章）第 62 條**——*"管有任何物品意圖摧毀或損壞財產"* • （循公訴程序定罪）10 年監禁	**《刑事法典》（聯邦）第 478.3 條**——*"管有或控制數據，並意圖干犯電腦罪行"* • 3 年監禁 **《刑事法典》（聯邦）第 478.4 條**——*"生產、供應或取得數據，並意圖干犯電腦罪行"* • 3 年監禁	**《1985 年刑事法典》第 191(1)條**——*"管有〔用作截取私人通訊的器材〕等"* • （循簡易程序定罪）5,000 加元罰款或不超過 2 年減 1 日的監禁，或兩者兼處 • （循公訴程序定罪）2 年監禁 **《1985 年刑事法典》第 327(1)條**——*"管有器材以取得使用電訊設施或服務"* • （循簡易程序定罪）5,000 加元罰款或不超過 2 年減 1 日的監禁，或兩者兼處 • （循公訴程序定罪）2 年監禁	**《1990 年誤用電腦法令》第 3A 條**——*"製造、供應或取得用於第 1、3 或 3ZA 條所訂罪行的物品"* • （循簡易程序定罪）不超過法定最高罰款或 12 個月監禁，或兩者兼處 • （循公訴程序定罪）罰款或 2 年監禁，或兩者兼處 **《2003 年通訊法令》第 126 條**——*"管有或供應用作違反第 125 條〔即不誠實地取得電子通訊服務〕的器具等"* • （循簡易程序定罪）不超過法定最高罰款或 6 個月監禁，或兩者兼處 • （循公訴程序定罪）罰款或 5 年監禁，或兩者兼處	**《中國刑法》第二百八十五條第三款** • （情節嚴重的）3 年徒刑或者拘役，並處或者單處罰金 **《中國刑法》第二百八十六條第三款** • （後果嚴重的）5 年徒刑或者拘役	**《1961 年刑事罪行法令》第 216D 條**——*"禁止處理截取器材等"* • 2 年監禁 **《1961 年刑事罪行法令》第 251 條**——*"製作、出售、分發或管有用作犯罪的軟件"* • 2 年監禁	**《1993 年誤用電腦法令》第 8 條**——*"在未獲授權下披露取用碼"* • 10,000 新加坡元罰款或 3 年監禁，或兩者兼處 • （第二次或其後每次定罪）20,000 新加坡元罰款或 5 年監禁，或兩者兼處 **《1993 年誤用電腦法令》第 10 條**——*"取得用於某些罪行的物品等"* • 10,000 新加坡元罰款或 3 年監禁，或兩者兼處 • （第二次或其後每次定罪）20,000 新加坡元罰款或 5 年監禁，或兩者兼處	**《美國法典》第 18 篇第 1030(a)(6)條（18 USC1030 (a)(6)）**——*"與電腦有關的欺詐及相關活動"* • （通常）罰款或 1 年監禁，或兩者兼處 • （如以往曾被裁定干犯《美國法典》第 18 篇第 1030 條所訂其他罪行）罰款或 10 年監禁，或兩者兼處 **《美國法典》第 18 篇第 2512(1)條（18 USC 2512(1)）**——*"禁止製造、分發、管有和宣傳有線、口頭或電子通訊的截取器材"* • 罰款或 5 年監禁，或兩者兼處

建議的罪行	香港	澳大利亞	加拿大	英格蘭及威爾斯	中國內地	新西蘭	新加坡	美國
			《1985 年刑事法典》第 342.2(1) 條——*"為在未獲授權下使用電腦系統或導致損害而管有器材"* • （循簡易程序定罪）5,000 加元罰款或不超過 2 年減 1 日的監禁，或兩者兼處 • （循公訴程序定罪）2 年監禁					