香港法律改革委員會

《依賴電腦網絡的罪行及司法管轄權事宜》報告書

摘要

（本摘要為報告書內容的概要。報告書可於法律改革委員會（法改會）的網站下載，網址是：https://www.hkreform.gov.hk，其文本亦可向香港中環花園道 3 號冠君大廈 9 樓法改會秘書處索取。）

諮詢過程

1. 法改會轄下的電腦網絡罪行小組委員會（“**小組委員會**”）在 2022 年 7 月發表《依賴電腦網絡的罪行及司法管轄權事宜》諮詢文件（“**諮詢文件**”），所研究的範圍如下：

> “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；
>
> (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。”

2. 小組委員會在公眾諮詢期間收到 65 份意見書。我們十分感謝所有曾提出意見的**回應者**。回應者的名單載於報告書附件。

報告書的結構

3. 報告書關乎小組委員會的研究的第一部分，[1] 共有九個章節，處理 16 項最終建議：

(a) 第 1 章描述國際機構和舉措如何將電腦網絡罪行歸類。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》**）所處理的 *"損害電腦數據及系統的機密性、完整性和可用性的罪行"*，[2] 大致上對應報告書的重心。

(b) 第 2 至 6 章分別處理五類依賴電腦網絡的罪行，即：

(i) 非法取覽程式或數據；

(ii) 非法截取電腦數據；

(iii) 非法干擾電腦數據；

(iv) 非法干擾電腦系統；及

(v) 提供或管有用作干犯電腦網絡相關罪行的器材、程式或數據。

(c) 第 7 章處理香港法庭行使司法管轄權的準則。

(d) 第 8 章處理這些罪行的判刑事宜。

(e) 第 9 章總結我們的最終建議。

第 2 章：非法取覽程式或數據（"取覽罪"）

4. 諮詢文件建議 1 提出，在未獲授權下取覽程式或數據應定為簡易程序罪行，而作出這類取覽並意圖進行其他犯罪活動應構成加重罪行。有關條文應以英格蘭及威爾斯《誤用電腦法令》（Computer Misuse Act，**《英格蘭誤用電腦法令》**）第 1、2 及 17 條為藍本。回應者普遍贊成建議 1，但部分回應者質疑純粹在未獲授權下取覽（即"沒有

---

1 由於小組委員會的研究範圍廣泛，我們的研究分為三個階段。研究的第二部分會涵蓋借助電腦網絡的罪行，該部範圍再作討論。第三部分會處理證據事宜及執法（程序）事宜。

2 該公約所處理的其他罪行類別，是電腦相關罪行（包括電腦相關偽造及欺詐）、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），以及關於侵犯版權和相關權利的罪行。

犯罪意圖”）應否構成罪責。其他回應者則提議釐清“合理辯解”免責辯護的涵蓋範圍。

取覽罪的意念元素[3]

5. 值得注意的是，就簡易程序罪行及加重罪行的犯罪意念而言，控方均必須證明，被告人在作出未獲授權的取覽時，知悉該項取覽未獲授權，這與《英格蘭誤用電腦法令》第 1(1)條的規定一致。

6. 我們同意，鑑於電腦網絡空間的設計和運作特點，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，並且應繼續容許在使用電腦網絡空間時已普遍接受的情況下，無須就取用或取覽事先尋求明示授權的慣常做法。另一些涉及默示授權的情況例子，包括但不限於以下情況：因設計緣故和實際需要而進行自動連接，並由此而發生取覽程式或數據。[4]

7. 因此，我們仍然認為，把某人知悉有關取覽未獲授權定為取覽罪的先決條件，是公允的做法。最終法庭會在考慮案件的整體情況後，裁定是否可從證據作出被告人知悉該項取覽未獲授權的必然推論。[5]

純粹在未獲授權下取覽應屬犯罪[6]

8. 各回應者就取覽罪的意念元素所提出的意見，關乎純粹在未獲授權下取覽程式或數據應否被定罪這問題，諮詢文件已對此作出討論。[7]

9. 由於黑客的企圖入侵所造成的不確定性及成本，《英格蘭誤用電腦法令》所訂的純粹在未獲授權下取覽罪當時所回應的，是人們需要保護電腦系統的完整及安全，使其免受未獲授權人士攻擊，不論這些人有何意圖。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。

10. 由於互聯網如今滲透大部分公共和私人生活，因此更有需要確保電腦系統及網絡完整，使其免受未獲授權的取用或取覽。簡易程序罪行及加重罪行旨在共同發揮作用，以有效阻嚇各種形式的未獲授

---

3 報告書第 2.18 至 2.24 段。
4 報告書第 2.25 及 2.26 段。
5 請參閱報告書第 2.23 及 2.24 段的說明例子。
6 報告書第 2.25 至 2.31 段。
7 第 2.4、2.5、2.96 至 2.101 段。

權取覽。故此，我們維持原先看法，認為純粹在未獲授權下取覽程式或數據應構成罪行。

合理辯解一般免責辯護及特定的免責辯護[8]

11. 我們認為，嘗試在電腦網絡罪行法例中詮釋“合理辯解”，甚或提供一份例子清單，以闡明有關立法原意，均可能會無意中收窄合理辯解免責辯護的範圍。

12. 雖然我們的結論是不應界定“合理辯解”，但我們建議應另外加入特定的免責辯護，以豁除我們認為顯然不應屬非法的各類行為。[9] 這樣會消除公眾對某些活動是否屬合理辯解免責辯護範圍的疑惑，從而使新法例更為清晰明確。

執法機關進行的合法活動[10]

13. 部分回應者尋求澄清以下一點：執法機關在有手令或無手令的情況下為刑事調查目的而取覽電腦程式或數據，會否獲豁免刑事法律責任。由於取覽罪並非旨在影響執法機關進行的任何合法活動，我們建議將“無合法權限”納入為該罪行的元素。個別案件中是否有“合法權限”這問題關乎事實。警務人員如已為搜查流動電話或其他電子器材而取得裁判官所發出的搜查令，或有合理依據支持在無手令的情況下搜查這些器材，因而符合*岑永根 訴 警務處處長*[11]中訂立的規定，便屬有*“合法權限”*而取覽程式或數據。此外，不論是否有合法權限，在迫切情況下取覽程式或數據，本身便可能屬於合理辯解免責辯護的範圍。因此我們認為，如未能提供充分理由而在無手令的情況下取覽程式或數據，即使是為了執法目的，也應構成取覽罪，實屬適當。

14. 因此，我們的**最終建議 1** 如下：

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

---

8 報告書第 2.32 至 2.34 段。
9 見本摘要第 18 至 33 段。
10 報告書第 2.35 至 2.37 段。
11 [2020] 2 HKLRD 529, CACV 270/2017（判決日期：2020 年 4 月 2 日）。

(b) 這項建議罪行的犯罪意念是：

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

(ii) 被告人在取覽有關程式或數據時，知悉該項意圖作出的取覽未獲授權。

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

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

建議 2 之中的諮詢問題

15. 諮詢文件建議 2 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。該問題由以下幾部分組成：

“(a) 對於為網絡安全目的而取覽而言，如答案是應該的話，應有甚麼條款？舉例來說：

(i) 該免責辯護或豁免應否只適用於經認可專業團體或評審團體審定的人士？

(ii) 如(i)段的答案是應該的話，評審制度應如何運作……？

(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）？”

16. 絕大多數回應者均支持訂定特定的網絡安全免責辯護，因為他們認為，白帽黑客及其他網絡安全專業人員在偵測網絡安全威脅及保安漏洞方面的工作，的確有其價值。另一方面，少數回應者則反對訂定該項特定的免責辯護，不贊成免責辯護實際上帶來一個“享有特權的界別”。他們認為，該項特定的免責辯護應適用於所有人，而非只適用於經由認可專業團體或認可團體認可的人士，不論這些人有何意圖。

17. 明顯大多數回應者均同意應設立認可制度。這結果與回應者普遍認為適宜為在未獲授權下取覽訂定特定免責辯護的意見相符。部分回應者同意，設立一個認可團體讓網絡安全專業獲得適當認可，會為香港帶來長遠裨益。

為經認可的網絡安全從業員提供特定的免責辯護 [12]

18. 我們認為，為資訊科技行業內某界定類別的人士訂定特定免責辯護，是合理而務實的做法。我們建議，經認可的網絡安全從業員如為真正的網絡安全目的而行事，應有特定的免責辯護或豁免。然而，在顧及整體情況後，被告人的目的和行為必須是合理的。

經認可或持牌網絡安全從業員

19. 鑑於為網絡安全目的而取覽程式或數據的入侵程度，以及網絡安全目的這寬廣概念，我們認為應只有持牌或經認可的從業員（即應具備一定水平的專業技能和正直品格者），才可為網絡安全目的而作出取覽。

20. 應設有一套獨立的制度，以對網絡安全從業員進行認可，並監督他們的紀律事宜。我們同意回應者所言，認可制度可以不同方式落實。其中一種方式是指定由某法定主管當局進行認可；另一種方式則是，任何人如是聲譽良好的資訊科技專業團體或國際資訊科技協會的成員，即會獲得認可。

21. 視乎所採用的模式，認可制度對網絡安全業界和電腦網絡空間用戶的影響，並不限於網絡安全專業人員的供應和收費。如何落實認可制度的細節問題，本質上屬政府的政策事宜，故這些細節問題（包括對網絡安全專業人員的認可要求、從業員須遵行的備存紀錄責任、

12 報告書第 2.63 至 2.74 段。

認可團體是由資訊科技行業還是其他主管當局管理，以及應如何為認可制度提供資金）適宜留待政府決定。[13]

真正的網絡安全目的

22. “真正的網絡安全目的”這額外規定，意味着被告人的認可資格或身分不應具決定性。我們的有關建議擬達到以下效果：舉例來說，經認可的網絡安全從業員如並非為真正的網絡安全目的而取覽自己子女電話內的數據，則只能援引“為保障兒童利益而取覽”作為免責辯護，這會在下文第 24 至 27 段討論。

在顧及整體情況後，被告人的行為必須是合理的

23. 我們亦建議在該項特定免責辯護加入“合理性”要求，從而提供穩妥和一致的規範，以界定一名明理的人所能接受的行為。若認可團體公布任何道德守則，法庭當然可參考該守則，以評定被告人的行為是否合理。

取覽罪的其他特定的免責辯護

為保障兒童利益而取覽 [14]

24. 在諮詢期間，有人提出關於家長應否獲准取用子女電腦的意見。我們認為，把“為保護 16 歲以下兒童而取覽”明文豁除於取覽罪之外，會是明智之舉。雖然這項特定免責辯護可能會削弱 16 歲以下兒童的私隱權，但鑑於這些兒童的互聯網滲透率甚高，我們認為訂有此免責辯護會符合保障他們利益的原則。

25. 為提供最大保障，這項建議的免責辯護是否成立，視乎尋求作出有關取覽的人的主觀目的而定，而非視乎該人與有關兒童的關係而定。

26. 為避免這項免責辯護被濫用，取覽作為應限於在顧及案件的整體情況後為保障兒童利益而合理所需者。我們已指明這項免責辯護的以下兩個制定方案：

---

13 為方便政府考慮認可制度，我們已在報告書第 2.67 至 2.70 段對認可建議及它可能造成的影響提出看法。

14 報告書第 2.75 至 2.91 段。

(a) 涵蓋範圍較廣的免責辯護：為保障兒童利益而取覽程式或數據；及

(b) 涵蓋範圍較窄的免責辯護：為防止兒童受到身體、情緒或心理傷害而取覽程式或數據。

27. 我們已在報告書分析這兩個方案的優劣利弊。[15] 小組委員會稍微佔多的成員屬意採用涵蓋範圍較廣的方案一。由於政府若決定落實我們這項建議，可進一步徵詢公眾意見，因此這議題最好由政府在考慮社會意見後再作定奪。

28. 由於精神上無能力的成年人可能容易遭受剝削，因此我們進一步建議，這項在未獲授權下取覽程式或數據的特定免責辯護應延伸至保護易受傷害人士，即《精神健康條例》（第 136 章）所界定的精神紊亂的人[16] 及弱智人士。[17]

為真正的研究目的而取覽 [18]

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

30. 我們同意，由於這些研究或許能得出有用的分析或資訊，[19] 因此提供“為研究目的而取覽程式或數據”這項特定免責辯護，屬合理之舉。我們認為，就各項兒童色情物品罪行所訂的免責辯護[20] 可用作藍本，把上述建議的免責辯護制定為“為真正的教育、科學或研究目的而取覽程式或數據”。為免被濫用，該免責辯護應訂有以下要求：取覽須屬合理，而該取覽不得超過為達到有關目的而所需者。這項“合理性”要求作為客觀準則，用以裁定被告人的取覽是否適度或合理。

---

15 第 2.85 至 2.87 段。

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

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

18 報告書第 2.92 至 2.94 段。

19 例如研究人員或網絡安全從業員確定在香港未受保護的電腦數目。

20 《防止兒童色情物品條例》（第 579 章）第 4(2)(a)及(3)(a)條。

《刑事罪行條例》第 64(2)條所訂、關於非法干擾電腦數據罪及非法干擾電腦系統罪（“干擾罪”）的免責辯護 [21]

31. 由於干擾電腦數據及／或干擾電腦系統通常只在取覽程式或數據後發生，因此我們認為，《刑事罪行條例》第 64(2)條（“**第 64(2)條**”）所訂的同意免責辯護及保護財產免責辯護[22]（兩者均適用於干擾罪），[23] 應同樣適用於取覽罪。

32. 鑑於同意免責辯護及保護財產免責辯護均適用於干擾罪，我們認為，取覽罪的免責辯護應採用統一的處理方式。將第 64(2)條所訂的免責辯護改列於電腦網絡罪行法例時，我們建議提高援引有關免責辯護的門檻，在上述兩項免責辯護加入客觀驗證標準：

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

(b) 就保護財產免責辯護而言，被告人必須合理地相信有關財產需即時保護。

33. 上述調整會使同意免責辯護及保護財產免責辯護，與我們就取覽罪所建議的其他特定免責辯護看齊，即所有免責辯護均一致採用“合理性”要求。

34. 因此，我們提出**最終建議 2** 如下：

> “就建議的非法取覽程式或數據罪而言，我們建議除合理辯解可作為法定免責辯護外：
>
> (a) 在未獲授權下為網絡安全目的而取覽，應有特定的免責辯護，但須符合以下條件：

---

21 報告書第 2.95 至 2.102 段。

22 根據《刑事罪行條例》（第 200 章）第 64(2)條，任何被告人被控以刑事損壞罪，在下述情況下均須被視為有合法辯解：

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

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

(i) 該財產需即時保護；及

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

23 見本摘要第 62 至 64 段。

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

(ii) 被告人必須為真正的網絡安全目的而行事;及

(iii) 在顧及整體情況後,被告人的行為必須是合理的。

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

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

(ii) 在顧及整體情況後,被告人對程式或數據的取覽必須是合理的。

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

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

(i) 第64(2)條所訂的兩項免責辯護涵蓋以下情況:

(1) 被告人在取覽程式或數據時,相信其作為已獲同意或會獲同意;或

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

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

延長循簡易程序檢控五類依賴電腦網絡罪行的時效期 [24]

35. 《裁判官條例》（第 227 章）第 26 條訂定提出檢控的一般時效期為六個月。由於六個月或不足以調查電腦網絡罪行案件，[25] 因此諮詢文件建議 3 提出，新訂的電腦網絡罪行法例應把時效期延長至兩年。

36. 大多數回應者均支持建議 3，而少數回應者則屬意維持六個月的期限，以鼓勵執法機關保持警惕。我們希望澄清一點，建議 3 僅旨在延長時效期，以確保即使由於本身涉及的難題，以致有關指稱罪行的調查按理不能在預設的六個月期限內完成，隨後提出檢控的時限也不會屆滿，而非因為我們不相信執法機關能在公平情況下盡速處理電腦網絡罪行案件。

37. 因此，我們建議保留諮詢文件建議 3 作為**最終建議 3**：

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

第 3 章：非法截取電腦數據

38. 明顯大多數回應者均支持諮詢文件建議 4，該建議提出，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定為罪行。然而，部分資訊科技團體憂慮，建議的截取罪會對網絡安全從業員所進行涉及截取的合法作為（例如網絡入侵偵測、滲透測試，以及為找出攻擊或分析網絡通訊而進行的網絡監察）帶來潛在不確定性。

---

24 報告書第 2.106 至 2.110 段。

25 正如諮詢文件所解釋，受害人可能在電腦網絡罪行案件發生後兩或三個月才向警方報案，而更甚者，六個月在事件被揭發時經已屆滿。警方從互聯網服務提供者取得日誌紀錄，可能需要幾個月。分析這些日誌紀錄可能再需要幾個月，還須顧及達至檢控決定所需的額外時間。

“為不誠實或犯罪目的”這項規定適當[26]

39. 正如諮詢文件所述，[27] 我們強調，我們完全知悉現代網絡器材的運作方式難免牽涉截取，而網絡安全公司在正常業務中亦可能會以各種方式截取數據。這解釋了諮詢文件為何建議把 *“為不誠實或犯罪目的”* 而截取列為規定之一。這項意念元素旨在訂立較高的門檻，避免所訂罪行的範圍不合理地廣泛，以免日常使用電腦網絡科技時正常進行的數據截取會被定罪。

40. 我們亦承認，若干臨界情況的行為或會出現一些不確定性。在該等情況下，某人是否犯截取罪會視乎案件的特定情況而定，包括被告人截取的目的和牽涉的數據。[28]

41. 採用 *“為不誠實目的”* 這標準的好處在於法庭可以考慮眾多因素，以決定截取行為是否屬於可接受的界限內。權衡之下，我們的結論是，*“為不誠實或犯罪目的”* 這個犯罪意念門檻屬適當，能夠避免令無惡意進行截取的人無意間誤墮法網。

在未獲授權下披露或使用數據[29]

42. 諮詢文件建議 4 擬禁止在未獲授權下披露或使用“截取的數據”，原因在於其後披露或使用截取的數據，可能會引起私隱方面的關注及其他潛在問題。[30] 經再三檢視後，若罪行是基於為不誠實或犯罪目的而在未獲授權下披露或使用“任何數據”（不限於截取的數據），則未免過於廣泛，因為這項罪行實質上會適用於我們日常數碼生活中接觸到的各類數據。

43. 鑑於在未獲授權下披露或使用電腦數據這項一般罪行[31] 影響甚廣，為審慎起見，我們應先在研究的第二部分[32] 深入探討這

---

26 報告書第 3.30 至 3.36 段。

27 第 3.97 段。

28 相關例子見報告書第 3.34 及 3.35 段。

29 報告書第 3.25 至 3.29 段。

30 例如在電子商貿交易中，倘若信用卡資料在傳送至賣方期間被截取作不當用途，持有人可能會蒙受財務損失。見諮詢文件第 3.92 及 3.94 段。

31 在未獲授權下披露或使用電腦數據的罪行，只要涉及個人資料，就更當屬個人資料私隱專員公署（“**私隱專員公署**”）檢視的範疇。最近一次在 2021 年的立法修訂工作中（即制定《2021 年個人資料（私隱）（修訂）條例》），私隱專員公署特別聚焦於“起底”罪行，務求遏止在未獲同意下披露個人資料（見該修訂條例的詳題）。“起底”罪行的犯罪意念非常局限於特定範圍。

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

議題，然後才就應否建議訂立這方面的新罪行（以及如應該的話，如何訂立）發表任何確定意見。例如，可進一步斟酌該項罪行應否局限於截取的數據，因為有人或會認為，某人如 *"為不誠實或犯罪目的"* 而披露或使用電腦數據，該項行為本身便應構成罪責，不論有關數據是在獲授權下截取而獲得，或是在未獲授權下截取（或以任何其他方式）而獲得。

44. 基於上述理由，我們提出**最終建議 4** 如下：

"我們建議：

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

(b) 建議的罪行應：

(i) 保障一般通訊，而並非只保障私人通訊；

(ii) 一般適用於數據（不論有關數據是否元數據）；及

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

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

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

該罪行的免責辯護 [33]

45. 諮詢文件建議 5 邀請公眾就以下問題提交意見書，有關意見在某程度上互相重疊：

---

[33] 報告書第 3.54 至 3.64 段。

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

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

46. 大多數回應者認為，任何專業如需在合法業務的通常運作過程中截取數據和使用截取的數據，均應享有免責辯護。他們提議，有關免責辯護應涵蓋特定類別的專業或活動。[34] 至於真正業務應否獲准截取和使用傳送中的數據，而無須負上刑事法律責任，有關回應則意見不一。

47. 我們審慎衡量回應者的意見書及建議的非法截取電腦數據罪的元素後，認為無須為需在合法業務的通常運作過程中截取和使用電腦數據的人士，訂定任何特定免責辯護或豁免，主要理由如下：

(a) 理論上，就已明確規定須證明*"不誠實或犯罪目的"*的罪行提供任何免責辯護，似乎不合邏輯；

(b) 在這前提下，某專業或真正業務如為不誠實或犯罪目的而截取電腦數據，則不應只是因為它經營某專業或業務，便獲豁免刑事法律責任；

(c) 為日常工作經常需要使用和處理截取的數據的機構提供免責辯護，實際上便會向某些專業或業務（例如私家偵探社或傳媒機構）給予截取數據的無限制授權；及

(d) 在針對電腦網絡罪行的特定法例內為特定類別的專業或人士提供免責辯護，或會暗示法例內未有指明的其他專業

---

[34] 報告書第 3.54 段。回應者建議的六個類別是：(a)互聯網服務提供者；(b)日常工作經常需要使用和處理截取的數據的機構；(c)純粹為偵測安全威脅而截取其本身網絡的公司；(d) 執法機關就犯罪活動及國家安全事宜進行的調查；(e)為公眾利益或為日後法律程序搜證而真誠地進行的舉報活動；及(f)合理相信有損害其利益的活動正在進行的業務或機構。

或人士截取數據必然是不合法，繼而令有關法律更為含糊，而非更為清晰。

48. 我們的結論是，任何業務如有意截取客戶或消費者的數據，均可向後者索取截取數據的授權。倘若截取的數據用於獲授權目的以外的其他目的，則會由法庭根據個別案件的證據，決定有關截取是否為不誠實或犯罪目的而進行。

49. 因此，我們提出**最終建議 5** 如下：

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

第 4 章：非法干擾電腦數據

50. 極大多數回應者均支持諮詢文件建議 6，該建議提出，《刑事罪行條例》第 59(1A)、60 及 64(2)條關於 *"誤用電腦"* 的現行制度應改列於新法例，從而將無合法權限或合理辯解而蓄意干擾電腦數據定為罪行。

建議罪行的意念元素 [35]

51. 部分資訊科技相關團體認為，"惡意"應是建議罪行的所需元素。某法律專業團體則尋求澄清，為何"罔顧後果"這項意念規定屬恰當或相關。

52. "惡意"是陳舊用語，過去曾造成詮釋上的困難。[36] 另外，《刑事罪行條例》第 60 條所訂的現行刑事損壞罪採納"意圖"及"罔顧後果"作為意念元素，而憑藉第 59(1)(b)及(1A)條，該罪行引伸而適用於 *"誤用電腦"*。[37] 作為一般原則，在刑事法中，

---

35 報告書第 4.14 至 4.22 段。

36 英格蘭及威爾斯法律委員會（Law Commission of England and Wales）在檢討關於損壞財產的罪行時，發現難以處理"惡意"一詞，導致後來制定了《1971 年刑事損壞法令》（Criminal Damage Act 1971，香港的刑事損壞罪亦以該法令為藍本）。見英格蘭法律委員會，*Criminal Law Report on Offences of Damage to Property*（1970 年），英格蘭法律委員會第 29 號，第 44 段。

37 《刑事罪行條例》第 59(1A)條把 *"誤用電腦"* 界定為以下作為，當中(b)及(c)段與非法干擾電腦數據（相對於非法干擾電腦系統）最為相關：

"罔顧後果"這概念要求證明被告人察覺有關風險，而在被告人所知的情況下，承擔該風險並不合理。[38] 不少刑事罪行已一併採納"罔顧後果"與"意圖"或"知悉"作為過失元素。

53. 就電腦網絡罪行而言，"罔顧後果"這概念強調小心謹慎及負責任地使用電腦科技的重要性，即當事人必須保持警惕，注意其網上行為可能帶來的後果（包括這些行為可能對他人造成的影響）。

54. 因此，我們建議就非法干擾電腦數據罪保留建議 6(b)(ii)的犯罪意念元素，即 *"須懷有意圖或罔顧後果，但無須懷有惡意"*。

加重罪行及危害國家安全的行為

55. 某回應者建議，除《刑事罪行條例》第 60(2)條所述元素外，*"任何意圖危害國家安全的行為或活動，或罔顧國家安全是否會因而受到危害"*，亦應視為加重罪行。

56. 我們的分析詳載於報告書第 4.23 至 4.31 段。概括而言，我們留意到，《中華人民共和國香港特別行政區維護國家安全法》（**《國安法》**）多項條文的範圍似乎相當寬闊，足以包括非法干擾電腦數據（以及非法干擾電腦系統）的作為。當中，《國安法》第二十四（四）條清楚涵蓋干擾及損壞互聯網電子控制系統的作為。由於《國安法》構成我們法律制度不可或缺的部分，所以重要的一點，是針對電腦網絡罪行的特定法例不得與《國安法》有任何抵觸或衝突，即使並非有意亦然。

57. 《維護國家安全條例》（"**《基本法》第二十三條立法**"）在 2024 年 3 月制定。《基本法》第二十三條立法所訂罪行包括以下罪行：意圖危害國家安全（或罔顧是否會危害國家安全）而進行破壞活動，損壞或削弱公共基礎設施（包括組成該設施的軟件）；[39] 更具體的是，意圖危害國家安全，而在沒有合法權限下，就某電腦或電子系統作出某項作為。[40]

"(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。"

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

39 《維護國家安全條例》第 49 條（危害國家安全的破壞活動）。

40 同上，第 50 條（就電腦或電子系統作出危害國家安全的作為）。

58. 考慮到《基本法》第二十三條現已藉本地立法的方式落實(包括引入特定罪行，涵蓋電腦網絡空間當中的國家安全風險），我們認為，政府更具條件全面評估所有現存國家安全相關罪行是否足夠，並考慮我們的建議，以研究應否建議任何可完善之處。

特定的免責辯護

為網絡安全目的而干擾電腦數據 [41]

59. 由於干擾電腦數據（或電腦系統）通常會在取覽程式或數據後發生，因此我們曾考慮，適用於第 2 章所討論的取覽罪的免責辯護，應否同樣適用於干擾罪。合乎邏輯的結論是，為網絡安全目的而干擾電腦數據這項免責辯護[42] 應同時適用於這兩類罪行，而我們亦如此建議。

為保障兒童或易受傷害人士的利益而干擾電腦數據 [43]

60. 雖然家長、監護人或其他人士或會要求取覽兒童或易受傷害人士的程式或數據，以保護該兒童或易受傷害人士免受網上危害，但據我們理解，這種取覽並不涉及更改或干擾電腦數據(或電腦系統)。況且，准許某人取覽任何程式或數據，絕不表示該人獲授權更改或以其他方式干預有關數據。因此，我們認為，無須為保障兒童或易受傷害人士的利益而就干擾罪提供特定的免責辯護。

為真正的研究目的而干擾電腦數據 [44]

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

改列《刑事罪行條例》第 64(2) 條的免責辯護 [45]

62. 諮詢文件建議 6 建議採納現時《刑事罪行條例》第 64(2)條所訂的兩項“合法辯解”。就干擾罪而言，由於回應者普遍歡迎採納《刑事罪行條例》所設的現行制度，我們建議維持建議 6，但須在

---

41 報告書第 4.34 至 4.35 及 5.23 至 5.24 段。
42 見本摘要第 18 至 23 段。
43 報告書第 4.36 至 4.37 及 5.25 至 5.26 段。
44 報告書第 4.38 及 5.27 段。
45 報告書第 4.39 至 4.44 及 5.28 段。

同意免責辯護及保護財產免責辯護加入客觀驗證標準（和上文第 32 段所討論的取覽罪一樣）。

63. 我們留意到現時《刑事罪行條例》第 64(2)(b)條之下的“合法辯解”僅限於保護財產，但不包括保護人命。我們曾考慮，就干擾罪而言，應否為保護生命及／或防止對他人造成身體傷害訂定特定的免責辯護。我們相信，如有人為保護生命及／或防止身體傷害而干擾電腦數據（或電腦系統），建議 6 的“合理辯解”一般免責辯護能夠應對這種情況，因此未必需要為此特定目的建議另一項免責辯護。我們贊成在這方面維持第 64(2)(b)條的現狀。

64. 我們的**最終建議 6** 如下：

“我們建議：

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

(b) 新法例應採用《刑事罪行條例》（第 200 章）所訂以下特點：

(i) 第 59(1A)(a)、(b)及(c)條所訂犯罪行為；

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

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

(iv) 第 60(2)條所訂加重罪行。

(c) 第 64(2)條所涵蓋的兩項免責辯護適用於以下情況：

(i) 被告人在干擾電腦數據時，相信其作為已獲同意或會獲同意；或

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

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

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

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

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

(ii) 被告人必須為真正的網絡安全目的而行事；及

(iii) 在顧及整體情況後，被告人的行為必須是合理的。”

第 5 章：非法干擾電腦系統

65. 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方式，是將兩者視為 *“誤用電腦”*（即刑事損壞的一種形式）。因此，諮詢文件建議 7 建議，關於非法干擾電腦數據及非法干擾電腦系統的條文，應採用一致的措辭。

66. 由於非法干擾電腦系統罪與非法干擾電腦數據罪息息相關，建議 7 同樣得到絕大多數回應者支持，他們對建議 7 的回應與對建議 6 的大致相似。我們重申上文第 51 至 63 段的分析，並提出**最終建議 7** 如下：

“我們建議：

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

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

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

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

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

(ii) 在生產軟件時，在軟件編入缺損程式；及

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

67. 諮詢文件建議 8 主要就以下活動應否足以視為建議的非法干擾電腦系統罪的合法辯解，徵詢公眾意見：

(a) 掃描（或以類似的形式測試）他人的電腦；

(b) 非保安專業人員的行動，例如由機械人進行網頁抓取（web scraping）（即利用電腦自動程式〔bots〕從網站提取內容及數據的過程），或由互聯網資訊收集工具（例如搜尋器）啟動網絡爬蟲（web crawlers）（即為建立索引而有系統地瀏覽網頁的電腦自動程式），在未獲授權下從伺服器收集數據。

建議 8(a)：特定的免責辯護 [46]

68. 由於兩項干擾罪息息相關，我們同樣建議，就非法干擾電腦系統罪而言，為網絡安全目的而干擾電腦系統應可作為免責辯護。我們在上文第 59 至 63 段列出為非法干擾電腦數據罪提供特定免責辯護的理據，該等理據同樣適用於非法干擾電腦系統罪。

---

[46] 報告書第 5.23 至 5.28 段。

建議 8(b)：無須為非保安專業人員建議免責辯護 [47]

69. 有些活動不一定會達致網絡安全目的，但本身卻存在於電腦網絡空間的運作之中，或是電腦器材或系統之間的互動之中。電腦網絡空間內有不少我們認為是數碼生活中不可或缺，因而可以接受的合法活動，但是要把這些活動詳盡無遺地全數列出，是不可能的，尤其是鑑於科技發展步伐之快，情況更是如此。我們同意諮詢文件所述，認為當某人選擇連接互聯網，便應視為默示同意任何在使用電腦網絡空間時可合理預期會發生的互動。我們應避免無意中使一些廣為接受的互聯網做法變成違法行為，而由於互聯網或電腦系統的正常運作所需，這些做法應予准許。再者，其他國家雖然制定了非法干擾電腦系統罪及取覽罪，但這些國家的電腦網絡罪行法例並沒有為非保安專業人員（如操作搜尋器）提供任何特定的免責辯護。

70. 故此，我們認為無須就電腦網絡空間日常運作中所遇到的非保安代理提供特定的免責辯護，因為有關情況應能夠與電腦網絡攻擊區分開來。[48]

71. 我們的**最終建議 8** 如下：

> "(a) 為網絡安全目的而非法干擾電腦系統，應有特定的免責辯護，但須符合以下條件：
>
> (i) 被告人必須是經認可的網絡安全從業員（認可制度的細節本質上屬政策事項，最好留待政府考慮）；
>
> (ii) 被告人必須為真正的網絡安全目的而行事；及
>
> (iii) 在顧及整體情況後，被告人的行為必須是合理的。
>
> (b) 就建議的非法干擾電腦系統罪而言，無須為非保安專業人員提供任何特定的免責辯護（例如由機械人進行網頁抓取或由互聯網資訊收集工具啟動網絡爬蟲，從而藉着連接指定的協定埠，在未獲授權下從伺服器收集數據），理由是根據默示授權的

---

47 報告書第 5.29 至 5.33 段。

48 例如在一分鐘內向某特定郵箱發送 10,000 封電郵，使郵箱及相應伺服器不勝負荷。

原則，構成互聯網或電腦系統正常運作一部分的活動應繼續獲准。”

第 6 章：提供或管有用作干犯電腦網絡相關罪行的器材、程式或數據

72. 諮詢文件建議 9 建議訂立一項獨立的罪行，即提供或管有用作犯罪的器材或數據，這建議在市民大眾之間引發不少爭論。多名回應者關注到基本罪行的廣度，為釋除這些疑慮，我們已全盤檢討建議 9，並建議作出以下修訂：

在罪行加入“程式”，即“器材、程式及數據”[49]

73. 建議罪行的目的在於打擊電腦網絡罪行，我們認為將“程式”加入為建議罪行的標的之一，是適當的做法。這立場亦與《布達佩斯公約》訂定罪行的標準相符。[50]

將罪行的適用範圍限於使用器材、程式或數據以干犯電腦網絡相關罪行（而非一般任何罪行）[51]

74. 假如器材、程式或數據的非法用途並不局限於干犯電腦網絡罪行，則建議 9 在現實世界的適用範圍便會無遠弗屆。[52] 此外，在諮詢文件所討論的其他司法管轄區，電腦網絡罪行法例均一致將建議罪行的範圍限制於干犯依賴電腦網絡的罪行。如任何人使用器材、程式或數據，以干犯並非電腦網絡罪行的其他一般罪行，該項構成罪責的行為可根據香港各項法定罪行及普通法罪行來處理。

75. 因此我們建議，建議的罪行應只適用於以下情況：透過提供器材、程式或數據（或為提供該器材、程式或數據而管有它）而干犯罪行，而該罪行屬於電腦網絡相關罪行，即第 2 至第 5 章所討論的另外四類依賴電腦網絡的罪行其中之一。[53]

---

49 報告書第 6.24 至 6.25 段。

50 《布達佩斯公約》第六條規定，各締約方應採取措施將以下行為定為刑事罪行：*“生產、出售、為使用而獲取、輸入、分發或以其他方式提供經設計或改裝以主要用作干犯第二至五條所訂任何〔依賴電腦網絡的〕罪行的器材（包括電腦程式）。”*（底線後加）

51 報告書第 6.26 至 6.36 段。

52 例如任何人撰寫電郵，試圖勒索受害人，但最終決定不送出電郵，只保留草稿，該人也屬於管有可用作干犯“罪行”的數據，因而觸犯諮詢文件建議 9 的建議罪行。

53 即非法取覽程式或數據罪、非法截取電腦數據罪、非法干擾電腦數據罪及非法干擾電腦系統罪。在研究涵蓋借助電腦網絡的罪行的第二部分，我們會考慮還有哪些罪行（如有的話）亦應納入“電腦網絡相關罪行”的清單內，並載於針對電腦網絡罪行的特定法例的附表。

重寫罪行關於管有的部分 [54]

76. 我們認同，人們可能會在各種情況下管有惡意程式或數據，但並無意圖使用該程式或數據以干犯電腦網絡相關罪行。[55] 為避免造成過度刑事化的情況，我們建議將建議 9(a)關於管有的部分的範圍限於 *"為向他人提供被製造或改裝以用作干犯電腦網絡相關罪行的器材、程式或數據而管有它"*。根據這項形式較為狹隘的管有罪，某人如在不構成罪責的情況下管有被製造或改裝以用作干犯電腦網絡相關罪行的器材、程式或數據，便不會純粹因管有該器材、程式或數據而招致刑事法律責任；但某人如管有有關器材、程式或數據供自用，以干犯電腦網絡相關罪行，則會觸犯有關罪行。

在罪行加入額外的犯罪意念規定 [56]

就器材、程式或數據的性質的所知所信等

77. 任何人未必可準確知悉或了解某器材、程式或數據的主要用途。[57] 如程式的有害性質並非可輕易識別，又或該有害程式並非廣為人知，情況更是如此。我們認為，如某人誤解該器材、程式或數據的性質，或不知悉該器材、程式或數據主要用作犯罪用途，該人便不應因建議的罪行而須負上法律責任。因此我們建議，控方必須證明被告人知悉、相信或聲稱某器材、程式或數據主要用作（以客觀方式界定）干犯電腦網絡相關罪行。

保留"提供"這項基本罪行

78. 就為"提供"而管有而言，我們必須先考慮建議的罪行是否應規定被告人須"知悉"他人或"意圖"由他人將有關器材、程式或數據用作犯罪（即被告人必須知悉該器材、程式或數據實際擬作的用途）。訂立這項規定，實際上等同摒棄諮詢文件所建議的基本罪行，並導致某些有害器材、程式或數據的供應者成為漏網之魚，原因是供應者可純粹在暗網提供該等器材、程式或數據，而不顧或不知買家意圖如何使用它們。建議的罪行旨在遏制供應和管有可在電腦網絡空間作非法用途的器材或數據，為免破壞這個目標，我們認為應保留這項基本罪行，但須按上文第 76 及 77 段的建議作出修改。

---

54 報告書第 6.37 至 6.40 段。

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

56 報告書第 6.41 至 6.51 段。

57 例如某人可能以為程式無害而下載。

替代精神意念元素：有合理理由相信某器材、程式或數據的主要用途構成罪責[58]

79. 雖然管有如電腦程式的被告人或許實際並不知悉該程式內含勒索軟件或病毒（而可用作干犯電腦網絡相關罪行），但情況可能相當可疑，足以令被告人有合理理由如此相信。[59] 蓄意提供用作干犯電腦網絡罪行的器材、程式或數據，以及蓄意為提供任何上述物品而管有它們，均帶有相當程度的刑責。遏止這種行為與建議罪行的更廣泛目標相符，即防止有害器材、程式或數據被用作干犯電腦網絡罪行。

80. 為加強法律的阻嚇作用，我們建議，建議的罪行亦應涵蓋*"有合理理由相信"*某器材、程式或數據主要用作干犯電腦網絡相關罪行的人。

提供或管有惡意器材、程式或數據的部分[60]

81. 隨着科技進步，程式或數據能夠分散（例如在星際檔案系統〔InterPlanetary File System〕等分散式檔案系統，或區塊鏈技術[61]）儲存、取覽及分享。犯罪者可能只持有整體數據的一部分，此舉本身並非犯罪，但利用科技能夠聚集儲存於多個地點的數據，並向任何人提供綜合的惡意數據。

82. 為使法例更具彈性，我們建議改進建議 9，指明對*"器材、程式或數據"*的提述會包括該器材、程式或數據的部分。這項修改根本上沒有改變建議罪行的性質，因為要產生刑事法律責任，控方必須在毫無合理疑點下證明相同的犯罪意念元素，即有關的人(i)知悉自己管有某器材、程式或數據（或其任何部分）；及(ii)知悉、相信、有合理理由相信，或聲稱某器材、程式或數據（或其任何部分）主要用作干犯電腦網絡相關罪行。

---

58 我們的論點詳載於報告書第 6.48 至 6.51 段。

59 例如陌生人將某程式交予被告人，要求被告人於指明日期的特定時間上載該程式至某電腦系統，以換取大額金錢報酬，但不作任何解釋。

60 報告書第 6.52 至 6.54 段。

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

"合理辯解"作為法定免責辯護 [62]

83. 一如第 2 章所討論的取覽罪，我們認為無須提供一份例子清單，列舉會屬於建議罪行的"合理辯解"一般免責辯護範圍內的合法活動。我們建議訂立多項特定的免責辯護，該等免責辯護將於下文第 85 至 93 段討論。

84. 根據諮詢文件建議 9（稍經修改），我們提出**最終建議 9** 如下：

"(a) 在新法例下，蓄意提供被製造或改裝以用作干犯電腦網絡相關罪行[63] 的器材、程式或數據（或其部分），或蓄意為提供該器材、程式或數據而管有它，不論它是有形物或無形物（例如勒索軟件、病毒或其源碼），應定為基本罪行，而合理辯解可作為法定免責辯護。

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

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

(d) 建議罪行的犯罪意念規定為：

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

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

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

---

62 報告書第 6.57 至 6.59 段。

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

亦應屬犯罪，猶如任何人即使就所販運物質的性質構成罪責的信念原來出錯，亦屬干犯企圖販運危險藥物罪一樣。

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

(i) 該器材、程式或數據能夠用作干犯電腦網絡相關罪行，或犯罪者知悉、相信[64] 或聲稱該器材、程式或數據能夠用作干犯電腦網絡相關罪行；及

(ii) 犯罪者意圖任何人將該器材、程式或數據用作干犯電腦網絡相關罪行。

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

(i) 該器材、程式或數據能夠用作干犯電腦網絡相關罪行，或犯罪者知悉、相信[65] 或聲稱該器材、程式或數據能夠用作干犯電腦網絡相關罪行；及

(ii) 犯罪者意圖將該器材、程式或數據用作干犯電腦網絡相關罪行。

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

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

特定的免責辯護

為網絡安全目的提供有害器材、程式或數據（或為了為網絡安全目的提供該器材、程式或數據而管有它）[66]

85. 一如取覽罪及干擾罪，我們建議，為網絡安全目的提供有害器材、程式或數據（或為了為網絡安全目的提供該器材、程式或數據而管有它），應有特定的免責辯護。由於器材、程式或數據可由經認可的網絡安全從業員以外的人管有或提供，[67] 我們建議，網絡安全免責辯護應延伸至網絡安全從業員以外，以涵蓋獲網絡安全從業員事先批准或授權，為網絡安全目的而管有或提供器材、程式或數據的人。

為教育、科學或研究目的提供有害器材、程式或數據（或為上述目的提供該器材、程式或數據而管有它）[68]

86. 我們同意回應者所言，建議的罪行應有為教育或研究目的而設的免責辯護，而且該免責辯護適用於電腦科學領域的教師及學生，以及為自行研究而取得或製造有害電腦程式（例如特洛依木馬）的業餘愛好者。我們理解到，從事電腦科學研究可出於善意或惡意，但法律應留有空間，以促進對有害器材、程式或數據的研究。為預防濫用，我們建議，援引這項免責辯護的人的行為必須是合理的，且不得超過為達到有關目的而所需者。

為互聯網服務提供者提供免責辯護[69]

87. 互聯網服務提供者為個人及機構提供互聯網連接及相關服務（如網頁寄存）。由於互聯網服務提供者所分配的互聯網規約地址可能寄存多個網站及 URL，互聯網服務提供者要使被製造或改裝以用作干犯電腦網絡相關罪行的有害網站、程式或數據（如偽冒銀行網站）不能被接達並非總是可行，因為此舉可能擾亂向其他互聯網使用者提供的服務。

88. 考慮到互聯網服務提供者的處境，我們建議採用由歐洲聯盟部長理事會通過的《數位服務法案》（Digital Services Act）第 4 條所訂的純導管免責辯護（mere conduit defence）為藍本，並採納如《版權條例》

---

66 報告書第 6.71 至 6.75 段。

67 例如在開發防毒軟件的公司，其技術人員、銷售員及其他非專業人員的僱員在履行職務期間也可能管有電腦病毒。

68 報告書第 6.76 至 6.79 段。

69 報告書第 6.82 至 6.87 段。

（第 528 章）第 65A(2)條中“服務提供者”那般廣闊的定義，[70] 為互聯網服務提供者提供免責辯護。互聯網服務提供者作為服務提供者，如證明以下事項，即為免責辯護：

(a) 它並無啟動傳送有關器材、程式或數據（統稱“**違法內容**”）；

(b) 它並無選定該項傳送的接收人；及

(c) 它並無選定或修改該項傳送所載的違法內容。

為儲存及／或發布器材、程式或數據提供免責辯護 [71]

89. 在數碼時代，寄存服務提供者、雲端服務提供者及數據儲存設施均提供各種各樣的互聯網服務。為使針對電腦網絡罪行的特定法例臻於完善，我們建議以《數位服務法案》第 6 條[72] 為藍本訂立免責辯護，不同的“服務提供者”如服務包括“儲存”及／或“發布”服務對象所提供的器材、程式或數據，均可受惠於這項免責辯護。這種處理方式會涵蓋該等服務提供者，而無須將它們加以區別。

90. 上述服務提供者移除違法內容或使違法內容不能被接達，並非總是技術上可行，因為會造成連鎖效應，影響其他使用者。因此我們建議，上述服務提供者如證明以下事項，即為免責辯護：

(a) 它知悉或有合理理由相信服務對象已提供違法內容後，已在合理地切實可行的範圍內盡快移除該違法內容或使該違法內容不能被接達；或

---

70 《版權條例》（第 528 章）第 65A(2)條訂明“服務提供者”是*“藉電子設備或網絡（或同時藉兩者），提供任何聯線服務或為任何聯線服務操作設施的人”*。根據第 65A(2)(a)至(c)條，“聯線服務”包括：

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

(b) 寄存使用者能接達的資料或材料；及

(c) 在使用者能接達的系統或網絡儲存資料或材料。”

71 報告書第 6.88 至 6.92 段。

72 《數位服務法案》第 6(1)條內容如下：

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

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

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

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

以自動化科技提供器材、程式或數據的免責辯護[73]

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

92. 凡某些違法內容純粹藉某自動化程序、工具或科技而提供，則任何人如證明以下事項，即為免責辯護，我們認為是公平的：

(a) 他並無蓄意參與設計、製作或產生上述違法內容；及

(b) 他並無蓄意參與使上述違法內容成為該自動化程序一部分的過程。

93. 這項免責辯護會參照“自動化程序”以一般通用的方式擬定，而非述明任何特定科技，原因是隨着科技繼續演變，或會出現區塊鏈及電腦自動程式的替代品。

94. 我們的**最終建議 10** 如下：

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

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

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

---

73 報告書第 6.93 至 6.96 段。

(ii) 在顧及整體情況後，該網絡安全從業員的目的和行為必須是合理的；及

(iii) 這項免責辯護應延伸至：

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

(2) 協助網絡安全從業員履行其專業職務的人。

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

(c) 以歐洲聯盟《數位服務法案》（Digital Services Act）第 4 條為藍本，規定凡任何互聯網服務提供者[74] 作為提供有關器材、程式或數據（或為提供該器材、程式或數據而管有它）的純導管，則該提供者如證明以下事項，即為免責辯護：

(i) 它並無啟動傳送該器材、程式或數據（“**違法內容**”）；

(ii) 它並無選定該項傳送的接收人；及

(iii) 它並無選定或修改該項傳送所載的違法內容。

(d) 以《數位服務法案》第 6 條為藍本，規定凡任何服務提供者[75] 的服務包括儲存及／或發布服務對象所提供的器材、程式或數據，而該服務提供者察覺或有合理理由相信，服務對象已提供違法內容或已提供途徑接達（不論以直接或間接方式）該違法

74 我們建議採納如《版權條例》（第 528 章）第 65A(2)條中“服務提供者”那般廣闊的定義，以涵蓋大大小小的服務提供者，以及設立網上空間（例如論壇或網站）以寄存或儲存程式或數據的個人。見本摘要第 88 段。

75 同上。

內容，則該服務提供者如證明以下事項，即為免責辯護：

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

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

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

(i) 他並無蓄意參與設計、製作或產生該違法內容；及

(ii) 他並無蓄意參與使該違法內容成為該自動化程序一部分的過程。”

第 7 章：香港法庭行使司法管轄權的準則

電腦網絡罪行的司法管轄權規則 [76]

95. 基於香港適宜依循國際慣例，而國際慣例是司法管轄區應在合理範圍內，為其法律的任何域外應用訂定條文，諮詢文件建議 11 至 15 參照以下事實情況，就五類依賴電腦網絡的罪行訂明司法管轄權規則：

(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；

(b) 犯罪者是“香港人”；

(c) 受害人是“香港人”；

(d) 目標電腦、程式或數據處於香港；及

---

76 報告書第 7.2 至 7.6 段。

77 如以術語表達，即如《刑事司法管轄權條例》（第 461 章）第 3(1)條所述明：*“就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）”*。

(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）。

擴大事實情況(c)的範圍：受害人是“香港人”[78]

96. 我們獲得絕大多數回應者支持，將建議的電腦網絡罪行法例適用於域外範圍。至於上一段所述的事實情況(c)，諮詢文件建議“香港人”的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。

97. 因應某回應者的提議，我們深思香港法庭應為電腦網絡罪行的受害人提供多大的保障範圍。我們明白，各有原因而暫時在香港工作或逗留的人（例如外籍家庭傭工、遊客及其他在香港短暫逗留的訪客，在身處香港時遇上建議的依賴電腦網絡的罪行），亦應受到香港法律保障。

98. 故此，我們建議將事實情況(c)改進如下：

> “受害人是香港永久性居民、通常居於香港的人，<u>或於相關罪行發生時身處香港</u>，又或是在香港經營業務的公司。”

對危害國家安全行為的司法管轄權[79]

99. 至於是否需要就依賴電腦網絡的罪行訂定針對危害國家安全行為的域外法律效力條文，而非只是針對威脅*“香港的安全”*的作為立法，我們的分析詳載於報告書第 7.33 至 7.40 段。總括而言，《基本法》第二十三條立法已解決上述問題，該項立法清楚訂明凡任何其他條例提述*“特區的安全”*（或意義相同的詞句），[80] 須理解為包括法例所界定的“國家安全”。[81] 此外，當電腦網絡罪行案件涉及《國安法》規定的任何罪行時，顯而易見，一般原則是香港法庭可根據《國安法》第四十條[82] 對案件行使司法管轄權。最後，鑑於電腦網絡罪行案件如危害國家安全，有關案件的司法管轄權因著《國安法》

---

78 報告書第 7.25 至 7.28 段。

79 報告書第 7.33 至 7.40 段。

80 第 8(2)條。

81 第 4 條。

82 第四十條訂明，*“香港特別行政區對〔《國安法》〕規定的犯罪案件行使管轄權，但〔《國安法》〕第五十五條規定的情形除外。”*

第五十五[83]及五十六條[84]的規定而並不完全歸於香港法庭，我們認為並不適合在針對電腦網絡罪行的特定法例中訂立司法管轄權規則，訂明香港法庭對有關案件行使司法管轄權。

證據事宜及程序事宜[85]

100. 部分回應者提出證據事宜及程序事宜，包括從其他司法管轄區搜集證據、保存取自雲端環境的證據及該等證據是否可接納呈堂，以及應否修訂《刑事事宜相互法律協助條例》（第 525 章）（**《相互法律協助條例》**）下任何條文。由於我們的研究第三部分會處理執法及程序事宜，這些事宜為一大議題，我們會緊記回應者幫忙識別的問題。考慮到《相互法律協助條例》的相關修訂，最終會取決於建議的電腦網絡罪行法例的制定形式，而且或需與其他司法管轄區商討，以促進跨司法管轄區的合作，我們若對《相互法律協助條例》的相應修訂作出任何建議，實屬言之尚早。有關修訂最好留待政府適時按需要決定。

101. 基於以上原因，我們保留諮詢文件建議 11 至 15，並擴大事實情況(c)的範圍，從而提出**最終建議 11 至 15** 如下：

> "<u>最終建議 11</u>
>
> 我們建議，在以下情況下，就建議的非法取覽程式或數據罪，香港的法庭應具有司法管轄權：
>
> (a) 就該罪行定罪而須予以證明的任何作為或不作為或其他事情（包括一項或多項作為或不作為所產生的任何後果）在香港發生，即使其他有關作為、不作為或事情在其他地方發生；
>
> (b) 受害人（目標電腦的擁有人、有關數據的擁有人或兩者）是香港永久性居民、通常居於香港的人，或

---

83 第五十五條訂明，*"有以下情形之一的，經香港特別行政區政府或者駐香港特別行政區維護國家安全公署提出，並報中央人民政府批准，由駐香港特別行政區維護國家安全公署對〔《國安法》〕規定的危害國家安全犯罪案件行使管轄權：*
（一） 案件涉及外國或者境外勢力介入的複雜情況，香港特別行政區管轄確有困難的；
（二） 出現香港特別行政區政府無法有效執行〔《國安法》〕的嚴重情況的；
（三） 出現國家安全面臨重大現實威脅的情況的。"

84 第五十六條訂明，*"根據〔《國安法》〕第五十五條規定管轄有關危害國家安全犯罪案件時，由駐香港特別行政區維護國家安全公署負責立案偵查，最高人民檢察院指定有關檢察機關行使檢察權，最高人民法院指定有關法院行使審判權。"*

85 報告書第 7.20 至 7.22、7.31 及 7.32 段。

於該罪行發生時身處香港，又或是在香港經營業務的公司；

(c) 目標電腦、程式或數據處於香港；或

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

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

最終建議 12

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

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

(b) 受害人是香港永久性居民、通常居於香港的人，或於該罪行發生時身處香港，又或是在香港經營業務的公司；

(c) 目標電腦、程式或數據處於香港；或

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

最終建議 13

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

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

的任何後果）在香港發生，即使其他有關作為、不作為或事情在其他地方發生；

(b) 受害人是香港永久性居民、通常居於香港的人，或於該罪行發生時身處香港，又或是在香港經營業務的公司；

(c) 目標程式或數據處於香港；或

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

最終建議 14

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

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

(b) 受害人是香港永久性居民、通常居於香港的人，或於該罪行發生時身處香港，又或是在香港經營業務的公司；

(c) 目標電腦處於香港；或

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

最終建議 15

我們建議，在以下情況下，就建議的提供用作干犯電腦網絡相關罪行的器材、程式或數據罪（或為提供用作干犯電腦網絡相關罪行的器材、程式或數據而管有罪），香港的法庭應具有司法管轄權：

(a) 就該罪行定罪而須予以證明的任何作為或不作為或其他事情(包括一項或多項作為或不作為所產生的任何後果)在香港發生,即使其他有關作為、不作為或事情在其他地方發生(例如身處香港的人在暗網上提供用作干犯電腦網絡相關罪行的器材、程式或數據);

(b) 犯罪者是香港永久性居民、通常居於香港的人,或在香港經營業務的公司;或

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

第 8 章:判刑

102. 諮詢文件建議 16 載列就五類依賴電腦網絡的罪行所建議的最高刑罰。概括而言,回應者均支持引入一套較現有電腦相關罪行的罰則更重的罰則,因為此舉將有助阻嚇依賴電腦網絡的罪行,而良好穩健的網絡安全制度亦會促進香港的商業地位。

簡易程序形式的取覽罪 [86]

103. 因應某回應者的提議,我們已考慮就簡易程序形式的取覽罪處以最高兩年監禁是否具足夠阻嚇性。總括而言,把最高刑罰訂為兩年監禁,便能彰顯簡易程序形式的取覽罪的嚴重性:任何人一旦干犯該罪行,即使沒有足夠證據證明該人在未獲授權下取覽程式或數據後意圖進行其他犯罪活動,法律旨在保護的有關目標系統的不可侵犯性或有關資料的機密性,也已經受到侵害。我們認為建議的最高刑罰是適當的,因為這樣可給予判刑法院足夠權力,判處能恰當地反映罪行重點的刑罰。

把干擾罪的加重罪行最高刑罰訂為終身監禁的背後理念 [87]

104. 訂明最高刑罰為終身監禁,僅旨在與現行《刑事罪行條例》第 63(1)條就刑事損壞的加重罪行所訂的刑罰保持貫徹一致。若把第 63(1)條與《刑事罪行條例》第 60(2)(b)條[88] 一併閱讀,便可確保

---

86 報告書第 8.9 至 8.13 段。

87 報告書第 8.14 至 8.18 段。

88 《刑事罪行條例》第 60(2)條規定:

所施加的刑罰足以處理涉及意圖危害生命的財產損壞或摧毀的情況。由於干擾罪可能會危害數以千計的人的生命，[89] 因此有充分理由處以嚴厲的最高刑罰。事實上，視乎案情而定，非法干擾電腦數據及／或非法干擾電腦系統的行為可能已構成刑事損壞的加重罪行，該罪行現時的最高刑罰為終身監禁。新訂的電腦網絡罪行法例的用意，只是使這些已在《刑事罪行條例》設想的現有干擾罪在該法例中得以反映。

105. 經全盤檢討建議 16，我們信納有關建議不但會發揮必要的阻嚇作用，足以打擊電腦網絡罪行，亦不會過分偏離以下罪行的最高刑罰：(a)《盜竊罪條例》（第 210 章）所訂的罪行，[90] 以及(b)其他司法管轄區的有關罪行。[91] 因此，我們保留諮詢文件建議 16，作為**最終建議 16**：

"我們建議：

(a) 就建議的非法取覽程式或數據罪而言，犯罪者應可處下述最高刑罰：

(i) 如屬簡易程序罪行，可處兩年監禁；或

(ii) 如屬加重罪行，一經循公訴程序定罪，可處 14 年監禁。

(b) 就建議的非法截取電腦數據罪而言，犯罪者一經循簡易程序定罪，應可處兩年監禁，一經循公訴程序定罪，應可處 14 年監禁。

(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：

"任何人無合法辯解而摧毀或損壞任何財產（不論是屬於其本人或他人的）——
(a) 意圖摧毀或損壞任何財產或罔顧任何財產是否會被摧毀或損壞；及
(b) 意圖藉摧毀或損壞財產以危害他人生命或罔顧他人生命是否會因而受到危害，即屬犯罪。"（底線後加）

89 例如干擾機場控制塔系統、鐵路信號系統、發電廠等所處理的電腦數據。

90 用作參考的具代表性罪行類別：《盜竊罪條例》（第 210 章）所訂的盜竊罪、欺詐罪、勒索罪、入屋犯法罪、嚴重入屋犯法罪及搶劫罪。

91 見諮詢文件的附錄，當中概述香港及其他司法管轄區的現行法律就建議的五類依賴電腦網絡的罪行所訂的最高刑罰。

(i) 如屬基本罪行，一經循簡易程序定罪，可處兩年監禁，一經循公訴程序定罪，可處 14 年監禁；或

(ii) 如屬加重罪行，可處終身監禁。

(d) 就建議的提供用作干犯電腦網絡相關罪行的器材、程式或數據罪（或為向他人提供該等器材、程式或數據而管有罪）而言，犯罪者應可處下述最高刑罰：

(i) 如屬基本罪行，一經循簡易程序定罪，可處兩年監禁，一經循公訴程序定罪，可處七年監禁；或

(ii) 如屬加重罪行，一經循公訴程序定罪，可處 14 年監禁。”