香港法律改革委員會

電腦網絡罪行小組委員會

《依賴電腦網絡的罪行及司法管轄權事宜》諮詢文件

摘要

（諮詢文件載有法律改革委員會（“法改會”）轄下電腦網絡罪行小組委員會（“小組委員會”）所提出的建議及諮詢問題，供諮詢公眾意見之用。本摘要為諮詢文件內容的概要，所採用的簡稱及界定用語與諮詢文件相同，有意提出意見者宜參閱諮詢文件全文。諮詢文件可於法改會的網站下載，網址是：https://www.hkreform.gov.hk，亦可向香港中環下亞厘畢道 18 號律政中心東座 4 樓法改會秘書處索取。

回應者應於 2022 年 10 月 19 日或之前將意見送達小組委員會秘書。）

導言

研究範圍

1. 2019 年 1 月，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；
>
> (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。”

項目的三個劃定部分

2. 諮詢文件關乎項目以下三個部分的第一部分：

(a) 第一部分處理依賴電腦網絡的罪行[1] 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，[2] 並嘗試應對數碼時代的宏觀挑戰，包括數據主權，[3] 而第二部分的範圍須待適當時候再作討論；及

(c) 第三部分會處理證據及執法（程序）事宜。

第一部分研究的五類依賴電腦網絡的罪行

3. 諮詢文件研究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，即：

(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。

4. 小組委員會展開研究後，《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，[4] 小組委員會研究電腦網絡罪行這課題時已將此考慮在內。

---

1 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。例子包括黑客入侵、散播電腦病毒，以及分布式拒絕服務攻擊。

2 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。例子包括在網上散布兒童色情物品、設立仿冒詐騙網站，以及網上起底。

3 數據主權亦稱為電腦網絡、數碼或技術主權。數據主權所指的，是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這個概念。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。見 Julia Pohle & Thorsten Thiel, "Digital Sovereignty", Internet Policy Review: Journal on internet regulation (2020), Vol 9, Issue 4，第 8 頁。

4 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。

建議背後的指導原則

5. 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。

第 1 章：電腦網絡罪行的歸類

6. 在聯合國的層面，電腦網絡罪行既沒有確切的清單，也無法巨細無遺地逐一臚列。文獻列述了多種電腦網絡罪行的歸類方法，以及多組用於有關歸類的術語。聯合國毒品和犯罪問題辦公室（United Nations Office on Drugs and Crime）的網絡犯罪問題全球方案（Global Programme on Cybercrime），區分“依賴電腦網絡的罪行”及“借助電腦網絡的罪行”。[5]

7. 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》**）處理四類罪行，[6] 其中“損害電腦數據及系統的機密性、完整性和可用性的罪行”這類別大致上對應諮詢文件的重心。

8. 我們的比較研究涵蓋七個司法管轄區，當中澳大利亞、加拿大、英格蘭及威爾斯和美利堅合眾國是《布達佩斯公約》的締約方，其餘三個司法管轄區（即中國內地、新西蘭和新加坡）則與香港一樣，並非締約方。

第 2 章：非法取覽程式或數據

9. 概括而言，就非法取覽程式或數據而訂立的罪行，旨在應對損害電腦系統安全的危險威脅及攻擊，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。黑客入侵是這罪行最典型的例子。

---

5 聯合國毒品和犯罪問題辦公室，“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）。

6 這些罪行是損害電腦數據及系統的機密性、完整性和可用性的罪行、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。

香港的現行法律

10. 根據《刑事罪行條例》(第 200 章)第 161 條(“**第 161 條**”),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,

即屬犯罪。

11. 根據*律政司司長 訴 鄭嘉儀*(*Secretary for Justice v Cheng Ka Yee*),[7] 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 條。因此,舉例來說,如任何人使用自己的電腦設立仿冒詐騙網站,第 161 條並不適用。

12. 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。[8]

13. 第 161 條的“獲益”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,例如某人先前無法取覽的資料。[9]

14. 根據《電訊條例》(第 106 章)(“**《電訊條例》**”)第 27A 條(“**第 27A 條**”),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。

15. 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。

16. 案例顯示,控方傾向根據第 161 條檢控黑客入侵事件,這可能是因為控方顯然難以證明第 27A 條所訂的犯罪意念。此犯罪意念涉及兩方面,即被告人:

---

7 (2019) 22 HKCFAR 97, [2019] HKCFA 9.

8 同上,第 38 段。

9 *香港特別行政區 訴 秦瑞麟*(*HKSAR v Tsun Shui Lun*) [1999] 3 HKLRD 215, HCMA 723/1998(判決日期:1999 年 1 月 15 日),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。

(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"*。

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（25,000 元），而根據第 161 條循公訴程序定罪則可處監禁五年。

小組委員會的看法

宜制定針對電腦網絡罪行的特定法例

18. 目前，香港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。

19. 相比之下，我們的比較研究所審視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。這些司法管轄區的做法有助確保做到協調統一、周全完備和貫徹一致（例如主要概念的定義）。我們建議制定一項針對電腦網絡罪行的特定法例，當中包括我們建議的罪行，藉以全盤改革現行法律。

主要詞語的定義

20. 據我們所觀察，目前"電腦"（computer）在字典中的涵義反映現今的科技狀況。[10]我們亦有考慮"電腦"在《證據條例》（第 8 章）中的定義（該定義就在刑事法律程序中接納文件證據而擬定），[11]以及俄羅斯聯邦於 2017 年向聯合國提交的《聯合國合作打擊網絡犯罪公約》草案（Draft United Nations Convention on Cooperation in Combating Cybercrime）（**《俄羅斯公約》**）對"資訊及通訊科技器材"的定義。[12]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

---

10 見《牛津英文字典》（Oxford English Dictionary）（2022 年 3 月）。該字典指"電腦"是 *"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"*。

11 《證據條例》（第 8 章）第 22A(12)條將"電腦"界定為 *"任何用作儲存、處理或檢索資料的裝置"*。

12 《俄羅斯公約》第四條第(o)款將"資訊及通訊科技器材"界定為 *"任何用於或設計用於自動處理和儲存電子資料的硬件組件的集合體（組合體）"*。

比，“電腦”一詞的概念仍然清晰，不僅為大眾所通曉，其他司法管轄區的法例亦廣泛使用“電腦”一詞。

21. 儘管如此，我們緊記任何法定定義，包括“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演進。我們固然信任法院可因應科技進步而靈活地解釋任何定義，以盡量體現真正的立法原意，但法定定義在實際應用上仍可能會出現困難，這是因為被告人或會極力提出各種技術性論點，辯稱某“器材”在法律上並不構成立法機關原意中的“電腦”。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，然而，若政府落實我們的建議，法律草擬專員可在立法階段進一步考慮這個議題。

把純粹在未獲授權下取用或取覽定為不合法

22. 在香港（第 27A 條）及某些其他司法管轄區，純粹在未獲授權下取用或取覽已屬犯罪。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。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。

23. 我們曾詳盡討論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的情境到底有多類似。就此而言，我們必須指出，鑑於虛擬空間的設計和運作的固有特點，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。舉例來說，我們一般並不預期網上用戶須事先尋求明示授權，方可在另一用戶瀏覽的網頁上展示廣告。正如搜尋器在掃描有關互聯網規約地址前，通常不會事先取得網站的同意。我們認為，應繼續容許這些已獲視為給予默示授權的慣常做法。在這基礎上，小組委員會大多數成員認為，純粹在未獲授權下取用或取覽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。我們認為，這種做法與處理現實世界中對等行為的方式一致，並使法律明確，因為要定奪在未獲授權下取用或取覽應實際在何時定為不合法，可能並不容易（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）。

取用或取覽的未獲授權性質

24. 新法例應明文訂定，只有在未獲授權下取用或取覽，方會受禁，從而提供指引以消除不必要的爭議。至於應如何闡述取用或取覽

的未獲授權性質，我們認為，英格蘭及威爾斯的《1990 年誤用電腦法令》（Computer Misuse Act 1990，**《英格蘭誤用電腦法令》**）第 17(5)及(8)條（如上議院在 *R v Bow Street Metropolitan Stipendiary Magistrate, Ex parte United States (No 2)*[13] 所解釋），就當地的在未獲授權下取覽電腦資料罪所採用的擬定方式較為可取。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及情況而定。

25. 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。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。正如在現實世界那樣，按常理判斷這項方針應適用於定奪某項取用或取覽在電腦網絡空間上是否已獲授權。

取覽程式或數據

26. “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。[14] 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。

合理辯解可作為免責辯護

27. 我們建議訂定以合理辯解為基礎的概括性免責辯護，因為這樣能更有效兼顧公眾利益，應付未能預見的情況，並給予法院彈性。

加重罪行

28. 單靠建議的簡易程序罪行，將不足以應對犯罪者或會在取覽程式或數據後進一步帶來可能嚴重的傷害（例如安裝間諜軟件，或勒索受害人）。

29. 我們建議，在未獲授權下取覽並意圖進行其他犯罪活動，應構成加重罪行。至於哪些其他犯罪活動應藉這種加重罪行而受到懲處，《英格蘭誤用電腦法令》第 2(2)條的擬定方式可作為考慮起點。

---

13 [2000] 2 AC 216.

14 “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”*，“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”*。在非技術層面上，“數據”亦指 *“數碼形式的資料”*。見《牛津英文字典》（2022 年 3 月）。

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。

在未獲授權下為網絡安全目的而取覽

30. “網絡安全”這個概念是以保護電腦系統免受數碼攻擊的做法作為根基。[15]我們曾廣泛討論在未獲授權下為網絡安全目的而取覽，顯示有不同論據支持和反對禁止在未獲授權下為網絡安全目的而取覽，要平衡兼顧這些互相矛盾的論據實有困難。以下舉出部分相關考慮因素及背景：

(a) 在電腦網絡空間，總會有人在未獲授權下測試（例如以“連接埠掃描”的方式測試）他人的電腦。測試工具既容易獲取，又得到廣泛使用。這些測試可能是出於善意、商業目的或惡意。

(b) 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，這些公司或會從中牟利。

(c) 網絡安全是個不斷變化的領域，評審情況亦一直演變。沒有業界機構獲視為唯一權威。在香港，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。

---

15 例如，“網絡安全”一直被理解為 *“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”*。網絡安全又稱為 *“資訊科技安全”*。見 Marion and Twede, *Cybercrime: An Encyclopedia of Digital Crime* (ABC-CLIO, 2020)，第 92 頁。

(d) 禁止各種未獲授權的測試將無法阻止他人從其他司法管轄區掃描在香港的電腦系統，而且會對網絡安全公司構成影響，卻無法制止罪犯識別這些保安漏洞。

31. 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。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。

32. 我們希望指出，若網絡安全業界的專業人員獲給予免責辯護或豁免，便會出現如何可確定或核實這類專業人員的身分這個基本問題。可行方案似乎是制訂某種形式的評審制度，由法定或行政評審團體備存一份可供查閱的網絡安全專業人員名單。因此，我們邀請公眾就建議 2(a)(i)及(ii)所載的問題，對評審制度的方式、方法及運作細節發表意見。

33. 另一方面，若社會各界認為，不斷演變的評審情況會對實施正式的評審架構造成阻礙，另一可行做法，是在新訂針對電腦網絡罪行的特定法例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，前提是有可靠的方法確定某網絡安全從業員是否符合有關法定規定。我們歡迎公眾就載於下文建議 2(a)(iii)的問題提出這方面的意見。

34. 最後，由於非保安專業人員亦可能作出非法取覽程式或數據的作為，故我們邀請公眾對非保安專業人員就非法取覽罪應否有任何合法辯解這問題提出意見，正如我們亦同樣在第 5 章就非法干擾電腦系統罪徵詢公眾在這方面的意見。[16]

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：

16 見下文第 80 至 81 段。

(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）？**[17]

簡易程序案件的時效期

35. 《裁判官條例》（第 227 章）訂定一般時效期為所涉事項發生後起計的六個月，但如規管某簡易程序罪行的有關法例另有規定則除外。受害人可能在電腦網絡罪行案件發生後的兩至三個月才向警方報案，而更甚者，是事件被揭發時六個月已屆滿。警方從互聯網服務供應商取得日誌紀錄，可能需時數月。分析這些日誌紀錄可能另需數月，還須顧及達至檢控決定所需的額外時間。

36. 由於預設時效期或不足夠，我們建議把時效期如下述般延長。

---

17 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安全和完整而掃描服務供應商的系統。

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。

第 3 章：非法截取電腦數據

37. 概括而言，就截取電腦數據而訂立的罪行，旨在把在沒有法律權限的情況下進行的截取定為不合法，從而保障人們的數據通訊私隱權。

香港的現行法律

38. 《基本法》規定，香港居民享有言論自由（第二十七條），他們的通訊自由和通訊秘密受法律的保護（第三十條）。

39. 《香港人權法案》規定，任何人之私生活或通信，不得無理或非法侵擾（第十四條），以及人人有發表自由之權利（第十六（二）條）。

40. 《截取通訊及監察條例》（第 589 章）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。然而，該條例只適用於公職人員，並只規管截取在 *"傳送過程中"* 的通訊。

41. 根據《電訊條例》第 27(b)條（"**第 27(b)條**"），任何人損壞、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，即屬犯罪。

42. 雖然電腦按理應可構成"電訊裝置"，如任何人具備所訂意圖而損壞、移走或干擾電腦，第 27(b)條便會適用，但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。

43. 此外，根據第 27(b)條，擬截取的目標只限於"任何訊息的內容"。這句顯然並不涵蓋元數據（即關於通訊本身的資料，而非通訊的內容或實質內容）。考慮到元數據對通訊各方的重要性，以及它

對通訊各方以外的人的潛在價值，元數據可與“任何訊息的內容”同樣值得受到保障。

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

44. 據我們理解，任何未經編碼處理的電腦數據，如在公開網絡上傳送，便可被外界截取。電腦數據即使被截取，仍可能繼續傳送。

45. 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。

為不誠實或犯罪目的而截取

46. 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，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。

47. 我們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。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

48. 《布達佩斯公約》第三條處理非法截取電腦數據，該條並無規定有關電腦數據須為私人數據。另外，據我們理解，新西蘭的法律委員會（Law Commission）及司法部（Ministry of Justice）已提議以“通訊”取代新西蘭《2012 年搜查及監察法令》（Search and Surveillance Act 2012）中對“私人通訊”的提述。我們同樣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

49. 互聯網採用分層方式，某層的元數據可能是另一層的數據。元數據並非定義明確的概念。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

50. 某些種類的互聯網通訊採用名為“存儲轉發”傳遞的機制，即通訊可於前往目的地途中多次暫存在網絡上。由此引起的問題是：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。

51. 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，在沒有法律權限的情況下截取有關數據便應屬犯罪。訂立這項罪行的方法之一，是加入類似於澳大利亞《1979 年電訊（截取及取覽）法令》（聯邦）（Telecommunications (Interception and Access) Act 1979 (Cth)）第 5F 條的條文，以推定通訊何時視為開始經過通訊系統，以及通訊何時視為繼續經過該系統。

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）[18] 第 8 條為藍本，包括犯罪意念（即“蓄意”截取）。

18 由英聯邦（Commonwealth of Nations）經參照《布達佩斯公約》制定。

社會可能視為正當調查的行為

52. 正如我們就建議的非法取覽程式或數據罪（第 2 章），邀請公眾對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這個議題提交意見書，我們亦歡迎社會各界就建議的非法截取電腦數據罪會否無意間對社會可能視為正當調查的行為造成影響這個議題發表意見。

真實業務進行的截取

53. 另一議題是：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），應否獲准截取傳送的數據。該等數據可能有不少用途，例如分析僱員電腦內的數據，以確定他有否違反限制性契諾；以及追蹤顧客連接至購物商場內網絡系統的智能電話或平板電腦，以查探顧客的喜好。

54. 據我們所觀察，規模較大的業務一般有能力就提供 Wi-Fi 熱點或電腦供人使用而擬定周全細密的條款及條件。有關條款及條件可保留合約權利截取和使用顧客或僱員的數據。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。

55. 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。由於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，因此在應否准許第 52 及 53 段所述的各類數據截取和使用的問題上，我們邀請公眾發表意見。如意見是應准許的話，我們歡迎公眾進一步建議應准許哪類專業及業務截取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。我們冀望公眾能就以下諮詢問題發表意見，這將有助我們考慮應如何擬定建議的免責辯護或豁免。

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

56. 概括而言，就非法干擾（而非截取）電腦數據而訂立的罪行，旨在打擊蓄意損壞、刪除、更改電腦數據等行為，從而保護有關數據的完整性，確保有關數據能正常運作或使用。

57. 非法取覽罪與非法干擾數據罪息息相關，因為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。

香港的現行法律

58. 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《刑事罪行條例》第 60(1)條所訂刑事損壞的一種形式。第 60(2)條訂明的有關加重罪行，適用於意圖危害他人生命或罔顧他人生命是否會因而受到危害的被告人。《刑事罪行條例》於 1993 年修訂，藉以：

(a) 將該條例就“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……”*；[19] 及

(b) 訂明摧毀或損壞財產，就電腦而言，包括“誤用電腦”。[20]

---

19 《刑事罪行條例》第 59(1)(b)條。

20 《刑事罪行條例》第 59(1A)條將“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（而非干擾電腦系統）最為相關：

“(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。”

59. 針對電腦網絡罪行而言，已有案例展示《刑事罪行條例》第 60 條（“**第 60 條**”）成功執行。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。這兩項條文的分別之一，在於第 60 條的犯罪意念（懷有意圖或罔顧後果）可能比第 161(1)(a)至(d)條所詳述的意圖更易證明。[21]

60. 根據《電訊條例》第 25(a)條（“**第 25(a)條**”），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，如故意隱匿、扣留或阻延擬傳遞予另一人的訊息，即屬犯罪。

61. 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：

(a) 由於第 25(a)條以電訊為前提背景，故該條的擬定方式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）。

小組委員會的看法

禁止在未獲授權下蓄意干擾數據

62. 每逢有人操作電腦或電腦與互聯網有互動，數據便難免會被更改。舉例來說，電郵伺服器會移除具危險性的電郵附件。網站可能會在訪客的電腦內儲存“小型文字檔案（cookies）”，藉以在該電腦上增加數據。即使上述對電腦數據的更改是蓄意作出的（是電郵伺服器或網站管理人有意導致的），很多電腦使用者大概都會接受這類更改。

63. 與此同時，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。

64. 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。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、[22]弄壞、更改或抑制）電腦數據定為罪行。

---

21 見上文第 10 段。

22 即使可利用某些數據復原工具將數據復原。

犯罪行為、犯罪意念、合法辯解及加重罪行

65. 我們以現行法律——具體而言為《刑事罪行條例》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。

66. 我們一致認為現有體制（包括所訂的犯罪行為、犯罪意念、兩項合法辯解及加重罪行）整體上令人滿意。

把有關罪行改列於新法例

67. 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，以打擊電腦網絡罪行，同時刪除《刑事罪行條例》第 59(1)(b)及(1A)條（當初在《刑事罪行條例》加入該條，是為了就電腦而言，擴大刑事損壞財產這項一般罪行的涵蓋範圍）。

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

68. 概括而言，就非法干擾電腦系統（而非電腦數據）而訂立的罪行，旨在禁止藉使用或干擾電腦數據，阻礙合法使用電腦系統，從而確保電腦系統能正常運作。

69. 即使數據未經修改，電腦系統的運作也有可能受阻。舉例來說，如藉進行分布式拒絕服務攻擊[23] 或慢速攻擊（slow attack），阻礙取用電腦網絡或限制電腦網絡的運作，便可能導致上述情況。

70. 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，可能在於導致該結果的各方是否意圖攻擊該系統。

香港的現行法律

71. 如上文所論述，《刑事罪行條例》第 60 條所訂刑事損壞的其中一種形式，是第 59(1A)條所界定的“誤用電腦”。第 59(1A)(a)條[24] 與非法干擾電腦系統最為相關。案例已確立分布式拒絕服務攻擊可構成“誤用電腦”。[25]

72. 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*），[26] 終審法院裁定電腦按所設定的“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。案中被告人參與一次以某銀行網站為目標的分布式拒絕服務攻擊。由於該銀行的伺服器擁有足夠的剩餘容量處理有關請求，該伺服器的其他操作並未遭受影響，因此該次攻擊並不成功。儘管如此，終審法院仍裁定維持對被告人的定罪。

73. 另一方面，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第 59(1A)(c)條。[27]

---

23 分布式拒絕服務攻擊可藉“殭屍網絡（botnet）”（即一組被入侵的電腦）發動。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。有關電腦的擁有人可能是無辜並蒙在鼓裡的。

24 見註腳 20。

25 *香港特別行政區 訴 朱婷婷* [2017] 4 HKLRD 651, HCMA 33/2016（判決日期：2016 年 10 月 11 日）。

26 (2019) 22 HKCFAR 30, [2019] HKCFA 3.

27 見註腳 20，以及*香港特別行政區 訴 朱峻瑋* (2019) 22 HKCFAR 30，第 37 頁，[2019] HKCFA 3（第 18 段）。

小組委員會的看法

一致處理干擾數據及干擾系統

74. 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。現有法例的整體施行情況理想。

75. 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

76. 我們曾考慮如“誤用電腦”的概念不再屬刑事損壞罪的涵蓋範圍，而是（如建議 6(c)所提議）一項並非載於《刑事罪行條例》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。

77. 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

78. 如將相關條文從《刑事罪行條例》遷往新法例，便可藉此機會完善“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[28] 在新法例中的對等條文；及

(b) 將諸如“損害任何電腦的操作”的概念納入“誤用電腦”的定義。

---

[28] 見上文註腳 20。

建議罪行的適用範圍

79. 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下述建議 7(d)所提到的各方。

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

80. 前述部分曾提及，[29] 總會有人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。用作進行這些測試的工具唾手可得，現時已有各種各樣的測試工具可導致不同程度的入侵。關鍵問題在於如何使用有關工具。

81. 我們邀請公眾就以下問題提交意見書：掃描（或以類似的形式測試）他人的電腦，應否足以視為建議的非法干擾電腦系統罪的合法辯解。對於法律應如何平衡網絡安全從業員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。

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；[30] 及／或

[29] 見上文第 30(a)段。

[30] 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）。

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

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

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

第 6 章：提供或管有用作犯罪的器材或數據

82. 如任何人將某器材或數據（例如消磁器、破解密碼工具或進行滲透測試的軟件）實際用作干犯電腦網絡罪行，便可因干犯建議的特定依賴電腦網絡的罪行而受懲處。概括而言，就提供或管有這類器材或數據而訂立的獨立罪行，旨在遏制生產、供應和管有可在電腦網絡空間作非法用途的器材或數據，藉以防止這類器材或數據被用作干犯電腦網絡罪行。

香港的現行法律

83. 根據《刑事罪行條例》第 62 條（“**第 62 條**”），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，以摧毀或損壞財產，即屬犯罪。

84. 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，第 62 條並沒有加以區分。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。

85. 另外，第 62 條的英文文本用“anything”一詞來描述受禁物。按照一般的說法，該詞並不限於有形物，涵蓋範圍亦似乎比中文文本的對應詞“任何物品”更廣。然而，該中文用詞的慣常涵義會否明確引伸至某些無形物，例如惡意軟件及有關利用漏洞（exploit）的專門知識，則是截然不同的問題。

86. 此外，第 62 條與第 60 條所訂的刑事損壞罪相關。對於其他條文所訂罪行（例如第 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。

87. 《電訊條例》雖然並無與第 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。在該制度適用的情況下，違反有關規定，即屬犯罪。

88. 該制度可能適用於可用作干犯電腦網絡罪行的電腦或智能電話，但我們認為，該制度有所不足。舉例來說，該制度的涵蓋範圍狹窄，只適用於無線電波等電訊技術。

小組委員會的看法

應訂立兼具基本及加重形式的新罪行

89. 我們認為，新法例應加入與第 62 條相對應的條文，而該條文亦應適用於諮詢文件第 2 至 5 章所論述的全部四類依賴電腦網絡的罪行。

90. 兼具合法及非法用途的器材及數據所帶來的挑戰，與現實世界中攻擊性武器所帶來的挑戰相類似。在應用《公安條例》（第 245 章）對"攻擊性武器"的定義時：

(a) 在涉及被"製造"或"改裝"以用作傷害他人的物品的案件中，無須證明犯罪意圖。純粹在公眾地方管有該物品，便足以招致刑事法律責任；而

(b) 本屬中性的物品，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。

91. 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。

建議罪行所應適用的器材及數據

92. 我們認為，為確保能在電腦網絡空間有效執行建議的（基本形式及加重形式）罪行，該罪行應適用於有形物及無形物。鑑於已有新西蘭法例作為先例，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。根據第 62 條及*朱峻瑋*

案，建議的罪行亦應適用於任何人相信或聲稱能夠用作犯罪的器材或數據，不論該人所信或所聲稱的是否屬實。

93. 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。因此，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。

94. 我們建議，基本罪行應涵蓋被製造或改裝以用作犯罪的器材或數據。我們亦建議，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

95. “黑客工具”及相類工具存有市場。因應該類市場的蓬勃發展而採取的周全法定措施，必須針對市場各類參與者。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。

犯罪意念

96. 我們認為，任何人應僅在行事時知悉有關事實的情況下，方屬干犯建議的基本或加重罪行。由於人們管有軟件或電腦數據十分普遍，甚至在自己不知悉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。該罪行的適用範圍似乎會過於廣闊。

97. 如任何人因相信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。

98. 如任何人被控加重罪行，按照定義，除了須證明上文第 96 及 97 段所提及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

99. 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”*。[31] 為免出現過度刑事化的問題，我們認為，建

[31] 《公安條例》（第 245 章）第 33(1)條，例如管有人在表演藝術時使用長兵器。

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。

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**

(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》（Computer Misuse Act）（第 50A 章）第 8 及 10 條為藍本。

管有只可作有害用途的數據

100. 儘管勒索軟件、病毒、建立及管理殭屍網絡的軟件，以及收集軟件（harvesting software）等電腦數據只可用作進行網絡攻擊，實屬有害，但亦有論點認為，如管有該等數據的目的是用作例如教學、研究或開發防毒軟件，法律無須（或不應）把管有該等數據定為罪行。因此，我們提出以下諮詢問題。

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

101. 我們在研究與電腦網絡罪行相關的司法管轄權事宜時，集中探討香港法庭行使司法管轄權的準則。

有關司法管轄權的一般原則

普通法的做法

102. 一般而言，對於普通法罪行及法定罪行，法庭的刑事司法管轄權受地域所限，行使範圍不會延伸至涵蓋在外地所作的作為。[32]

103. 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，這些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。

104. 然而，多個普通法司法管轄區現已採納某些更具彈性的觀點。香港法庭認同英格蘭及威爾斯採納的觀點，根據該觀點，法庭可在以下情況下，行使司法管轄權：

(a) 假如最後的作為在有關司法管轄區發生，或該罪行的絕大部分在有關司法管轄區所犯；及

(b) 並無出於相互尊重的理由而令該罪行不應在有關司法管轄區審訊。

訂明司法管轄權規則的香港法例

105. 《刑事司法管轄權條例》（第 461 章）（**《刑事司法管轄權條例》**）第 2(2)條把若干欺詐和不誠實的實質罪行，界定為甲類罪行。《刑事司法管轄權條例》第 3 條規定，就任何甲類罪行而言，只要任何“有關事情”——即是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。

106. 2002 年，政府建議把三項電腦罪行[33] 列入甲類罪行。該項建議因得不到立法會相關小組委員會支持而未有落實。

---

32 然而，不少國家亦聲稱對在懸掛有關國家國旗的船舶上和根據該國法律註冊的飛機上所犯的罪行具有司法管轄權。見《電腦網絡罪行公約說明報告》（Explanatory Report to the Convention on Cybercrime）第 235 段。

33 這些罪行分別是《電訊條例》第 27A 條所訂的“藉電訊而在未獲授權下取用電腦資料”罪、《刑事罪行條例》第 59 及 60 條所訂的與誤用電腦有關的“摧毀或損壞財產”罪，以及《刑事罪行條例》第 161 條所訂的“有犯罪或不誠實意圖而取用電腦”罪。

107. 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。[34]

普遍獲接受的域外管轄權基礎

108. 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。

與電腦網絡罪行相關的司法管轄權事宜

法庭已意會電腦網絡罪行帶來的挑戰

109. 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。要決定某項事實在何處發生可能不易。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。[35]

110. 解決司法管轄權的衝突是國際間打擊跨境罪案重要的一環。實際上，受影響地方一向通過磋商解決問題，而部分地區的文書亦有就國與國之間的法律合作可考慮的因素提供指引。[36] 在香港簽訂

---

34 例子見《刑事罪行條例》第 153P 及 153Q 條（與附表 2 一併理解），以及《防止賄賂條例》（第 201 章）第 4 條。

35 舉例而言，在 *DPP v Sutcliffe* [2001] VSC 43，第 62 – 63 段，澳大利亞維多利亞最高法院（Supreme Court of Victoria）承認 *"互聯網提供了迅速快捷且相對便宜的通訊方式，讓……人互相通訊"*，以及取用 *"不只限於擁有電腦……法律須隨着這些轉變而發展。"*

36 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。

任何有關雙邊協議之前，須獲得中央人民政府授權，[37] 我們預計，如我們的建議獲落實推行，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，[38] 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。[39]

小組委員會的看法

初步考慮

111. 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。新法例應明確訂明多種適用於所訂罪行的司法管轄權規則。檢控部門保留酌情權，決定應否提出檢控，這做法亦可為公眾提供保障，切合我們的指導原則。

112. 香港依循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這國際慣例，亦屬恰當。我們參照以下事實情況，討論諮詢文件所建議的罪行：

(a) 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（比照《刑事司法管轄權條例》第 3 條）；

(b) 犯罪者是“香港人”；

(c) 受害人是“香港人”；

(d) 目標電腦、程式或數據處於香港；及

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

---

37 根據《基本法》，中央人民政府負責管理與香港有關的外交事務，而香港獲授權自行處理有關的對外事務（按照第一百五十一條的規定，即經濟、貿易、金融、航運、通訊、旅遊、文化、體育等領域）。

38 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。見第 113 至 127 段。

39 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）。

非法取覽程式或數據

113. 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)。

114. 我們不建議應用事實情況(b)，因為該情況亦涵蓋沒有任何"香港人"受害的案件。[40] 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。

115. 我們認為應用事實情況(c)，有助加強這項建議的罪行所提供的保障。由於電腦網絡罪行所涉的各方可能身處多個司法管轄區，受害人這概念應採用寬廣的定義。舉例來說，如某雲端伺服器持有的數據由另一司法管轄區的人擁有，該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。為與這項建議的罪行的焦點一致，我們的結論是贊成以此方式盡量擴大所提供的保障範圍，因為重點應是須予保護的數據。

116. 我們認為，施加雙重犯罪的規定可能有違加強保障公眾這目的。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。我們提議，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。總括來說，我們認為，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；

40 例如犯罪者（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。

(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。

非法截取電腦數據

117. 基於類似理由，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。

118. 我們不建議應用事實情況(b)，因為上文就首項建議的罪行所提出的論點——即是很可能並非“香港人”受害，以及在香港提出檢控可能並不可行——在此處同樣適用。

119. 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。這項建議的罪行類似非法取覽程式或數據的加重罪行，多於類似非法取覽程式或數據的簡易程序罪行。

建議 12

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

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

(b) **受害人是香港永久性居民、通常居於香港的人或在香港經營業務的公司；**

(c) **目標電腦、程式或數據處於香港；或**

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

非法干擾電腦數據

120. 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。

121. 由於我們不建議將事實情況(b)應用於首兩項建議的罪行，我們同樣不建議將事實情況(b)應用於這項建議的罪行。

122. 我們亦留意到，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。

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）。**

非法干擾電腦系統

123. 我們建議用相同方式處理前項罪行及這項建議的罪行。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。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）。

提供或管有用作犯罪的器材或數據

124. 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。雖然這兩種形式輕重有別，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。

125. 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)及(d)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。

126. 就*管有*器材或數據的部分而言，假如器材或數據儲存於例如雲端伺服器，若說是在管有人所處的位置管有該器材或數據，未必能反映現實。就*提供*器材或數據的部分而言，如惡意軟件被上載到互聯

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。因此，我們建議將事實情況(a)、(b)及(e)應用於這項建議的罪行。

127. 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。我們認為，相同的理據亦適用於建議的提供或管有用作犯罪的器材或數據罪，因此有關建議亦同樣適用。

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）。

第 8 章：判刑

128. 我們在研究香港法庭對電腦網絡罪行的看法後，就各項建議的罪行提出適當的最高刑罰。香港及其他司法管轄區就相應的電腦網絡罪行所訂的最高刑罰，見諮詢文件的附錄摘要。

129. 概括而言，法庭一致將入侵、損壞或誤用電腦的案件，視為嚴重案件。例如，終審法院上訴委員會指出，故意損壞電腦軟件及數據的行為，通常應判處扣押刑罰。[41]

小組委員會的看法

各項建議的較嚴重罪行

130. 鑑於諮詢文件所建議的各項非簡易程序罪行，均可造成重大傷害，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）。

131. 我們明白電腦網絡罪行所致傷害的嚴重程度差別甚大，並建議前段(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。

132. 在仔細討論時，我們考慮了以下因素：各級法庭的判刑權限、現有電腦網絡罪行的最高刑罰、《盜竊罪條例》（第 210 章）就某幾類具代表性罪行所訂的最高刑罰，以及其他司法管轄區相若罪行的最高刑罰。我們認為，我們就上文第 130 段所列的各項建議罪行而建議的最高刑罰（可處 14 年監禁），不但會發揮必要的阻嚇作用，亦不會過分偏離我們所參考的最高刑罰。

133. 我們亦認為，循簡易程序定罪的最高監禁刑期若訂為兩年，便會與我們關於循公訴程序定罪的案件的建議相稱。

建議的非法取覽程式或數據的簡易程序罪行

134. 在某程度上，這項建議的罪行與第 27A 條所訂的罪行性質相若。然而，第 27A 條甚少獲援引，而且該條的最高刑罰（第 4 級罰

---

41 *廖偉信 訴 香港特別行政區*（*Liu Wai Shun v HKSAR*），FAMC 30/2004（判決日期：2004 年 9 月 27 日），第 7 段。

款，現為 25,000 元）看來頗輕。我們認為，即使是簡易程序案件，亦應有判監的可能性。我們建議，這項建議的罪行的最高監禁刑期，應訂為兩年。

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

135. 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 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

136. 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，因此應視為嚴重罪行，並應可處七年監禁，即相關加重罪行的建議最高刑罰的一半。

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。