電腦相關罪行跨部門工作小組

報告書

歡迎你的意見

政府一貫的目標，是確保我們對付罪案的法例和措施，能與時並進。電腦相關罪行跨部門工作小組因此在本年三月成立。工作小組於九月提交了報告書，這報告書現在發表作公眾諮詢。

由於電腦及互聯網的使用不斷與日俱增，我們歡迎你對報告書提出意見。有關意見請於二零零一年二月二十八日或以前，用以下任何一種方式提交給保安局：

- 郵遞地址：中環下亞厘畢道中區政府合署東座 6 樓保安局（F 組）
- 傳真號碼： 2521 2848
- 電郵地址： sbcassf@sb.gov.hk

我們鼓勵市民使用電郵，把意見傳送給我們，以減少紙張的消耗，如閣下喜歡用郵遞方式，可選擇使用在本頁底部的地址便條，以方便閣下郵寄。

本報告書現在各民政事務處派發，並可在保安局網頁 (www.info.gov.hk/sb/) 或經政府新聞處網頁 (www.info.gov.hk/) 瀏覽，我們鼓勵市民在網頁上瀏覽，以減少紙張的消耗。

如有疑問，請電 2810 2973 與保安局李家超先生聯絡。

中環下亞厘畢道
中區政府合署東座 6 樓
保安局（F 組）
保安局總助理局長收

電腦相關罪行跨部門工作小組

報告書

二零零零年九月

目錄

建議撮要

工作小組的建議撮述如下。

界定“電腦”一詞的法律定義

1. 當局應在法例中訂明一些範圍，以詮釋“電腦”這個概念，並應採納《電子交易條例》(第 553 章)所界定的“資訊系統”一詞，以取代“電腦”一詞(第 3.9 段)。為使法律用語一致，當局原則上應修訂法例中有關“電腦”一詞的所有提述(第 3.10 段)。

司法管轄權

2. 當局應考慮對整個管轄權規則問題進行徹底深入的研究，以顧及交通和通訊已大為改善的情況(第 4.10 段)。

3. 下列罪行在根據本報告書的建議作出修訂後，應納入《刑事司法管轄權條例》(第 461 章)的涵蓋範圍：

   — 藉電訊而在未獲授權下取用電腦資料(《電訊條例》(第 106 章)第 27A 條)；以及

   — 有犯罪或不誠實意圖而取用電腦(《刑事罪行條例》（第 200 章）第 161 條)

   (第 4.15 和 4.17 段)。

加密

4. 當局應引入法例，容許執法機關在有需要和有充分理由時獲取加密電腦記錄的解密工具或解密文本(第 5.14 段)。

5. 強制性披露資料的規定應受到司法審查(第 5.18 段)。為達到這個目的，當局應採用類似《有組織及嚴重罪行條

例》(第 455 章)第 4 條有關申請“提交令”的程序(第 5.22 段)。

6. 要求披露的權力應該只適用於性質比較嚴重的罪行。例如只有定罪後最高可判處不少於兩年監禁的罪行，才受披露規定的限制(第 5.25 段)。

7. 當局應提供適當法律保障，確保透過披露程序取得的資料必須保密。透過強制性披露取得的證據，應可獲得法庭接納(第 5.26 段)。

8. 違反披露規定的刑罰，原則上必須與調查中的罪行的刑罰相稱(第 5.27 段)。

保護電腦資料數據

9. 雖然就電腦資料數據而言，現行有關未獲授權而取用電腦的法例條文已可涵蓋大部分需要保護的情況，但仍應作進一步改善(第 6.18 和 6.19 段)。

10. 所有經由電腦或互聯網儲存或傳輸的電腦資料數據，不論儲存或傳輸狀態，也應包括在內(第 6.19 段)。

11. “取用電腦”一詞應闡明為包括取用電腦和取用儲存在電腦的程式及資料數據(第 6.19 段)。

12. 在未獲授權下以任何方式(非只局限於藉電訊方式)取用電腦，都應屬違法(第 6.19 段)。

13. 接收、保留及處理／販賣明知是在未獲授權下取得的電腦資料數據的行為，應予禁止(第 6.19 段)。

14. 出售、分發和提供電腦密碼或取用碼，使他本人或他人不當地用來圖利、作不法用途，或不當地用以使他人蒙受損失，也應列為違法(第 6.19 段)。

15. 立法管制黑客入侵工具並非必要，也不可行。這項建議不須再研究(第 6.23 段)。

16. 如果電腦資料數據和實體資料數據的處理方法出現不一致的情況，便有需要進行研究及作出適當糾正(第 6.25 段)。

“欺騙”電腦

17. 現行法例已足以處理“欺騙”電腦的案件(第 7.9 段)。不過，當局應考慮研究和堵塞現行法例中“欺騙”電腦以外的機器不屬違法的漏洞(第 7.10 段)。

罪行刑罰

18. 在未獲授權下取用電腦的罪行，應加入監禁刑罰。要發揮足夠的阻嚇作用，有關罪行的刑罰應不少於盜竊罪(第 2.7 和 6.22 段)。

19. 當局應修訂意圖犯罪而取用電腦(《刑事罪行條例》(第 200 章)第 161(1)(a)條)可被判監禁五年的現行罰則，使刑罰視乎罪犯所意圖觸犯罪行的嚴重程度而定(第 4.16 段)。

20. 當局應修訂《刑事罪行條例》(第 200 章)第 161 條中有關欺騙和不誠實意圖部分(即第 161(b)、(c)和(d)條)，使最高刑罰為由現行的監禁五年改為監禁十年或以上(第 7.11 段)。

互聯網服務供應商提供的協助

21. 當局應維持現行的做法，就是在有需要時，才追查懷疑涉及電腦罪案的指定帳戶的交易(第 8.22 段)。

22. 當局應鼓勵互聯網服務供應商(互網商)保存運作記錄(包括來電號碼)，作為良好的管理常規。不過，有關強制要求使用來電線路識別功能或來電號碼顯示功能追查所有互聯網交易的建議，則應暫時擱置(第 8.22 段)。

23. 當局應為互網商制訂保存記錄的行政指引，以便協助電腦罪案的調查工作。指引應包括：

- 用戶開設戶口時應查核的資料和之後須保存的資料；

- 運作記錄應載列的資料 — 最低限度應包括登入及退出時間和就互聯網交易而編配的網絡協定地址。如能包括來電者號碼則更為理想；以及

- 記錄應予保留的時間，例如六個月

(第 8.16、8.24 和 8.26 段)。

24. 制訂指引時應徵詢互網商的意見(第 8.26 段)。

25. 當局應就指引進行適當的宣傳，並鼓勵消費者選擇那些採納了載列在指引中的良好管理方法的互網商(第 8.27 段)。

26. 當局應鼓勵互聯網使用者利用公開密碼匙基礎建設來加強保安，但不應強制執行(第 8.23 段)。

27. 原則上贊同制訂移除程序，讓互網商移除涉嫌違法的材料。有關決策局應研究是否可以在保護版權、管制網上賭博及色情物品等方面，加入這些程序(第 8.30 段)。

28. 當局應促請互網商把系統預設為拒絕多重登入，而只將這項設施作為一個用戶選項，在選擇後才可使用(第 8.31 段)。

29. 如何處理網上購物信用額的問題，應繼續由市場作主導。當局毋須藉法例規定互網商必須設定互聯網交易的信用額(第 8.32 段)。

30. 應透過以下方法，加強執法機關與互網商的溝通：

- 設立交流意見的渠道，讓雙方定期會面，從宏觀的層面商討共同關注的問題；以及

- 設立聯絡人制度，好讓互網商和執法機關處理調查個別電腦罪案的要求(第 8.33 段)。

保護重要基本設施

31. 當局應就重要基本設施抵禦網上侵襲的能力進行徹底的風險評估(第 9.16 段)。

32. 當局應設立一個常設機制以統籌和協調有關保護、應變及復原計劃的擬定，以保障各項重要基本設施免受涉及電腦及互聯網方面的安全威脅(第 9.17 段)。這個機制的重點，應放在改善整體統籌工作上 — 統籌個別和整體重要基本設施受威脅和脆弱程度的評估，和協調有關保護、應變和復原計劃的擬備和定期更新(第 9.18 段)。

33. 政府的緊急應變系統演習應加入模擬本港重要基本設施遭受網上侵襲的情況(第 9.17 段)。

34. 從協助執法的角度來看，工作小組支持成立電腦緊急應變小組(應變小組)(第 9.21 段)。

35. 在應變小組成立之後，應該把重要基本設施營辦者涵蓋在內(第 9.22 段)。

36. 在應變小組成立之前，資訊科技署應與重要基本設施營辦者加強聯繫，以便迅速交流資訊，從而更妥善地應付緊急情況(第 9.22 段)。

公眾教育

37. 當局應設立一個機制，涵蓋目前從事資訊保安教育或宣傳工作的各個政府部門和其他公營機構，以便：

- 提供交流資訊的溝通渠道；
- 方便各機構參與和協辦由其他機構舉辦的計劃；
- 擔當中央統籌的角色，幫助制訂整體公營機構的資訊保安教育及宣傳策略；以及
- 統籌推動私營機構參與公營機構主導的資訊保安計劃，反之亦然

（第 10.7 段）。

私營機構的角色

38. 應繼續以市場主導，發展資訊保安設備或程式(第 11.5 段)。

39. 執法機關應把在調查電腦罪案過程中取得不法分子破解保安措施的方法，通知有關的行業。私營機構也應該讓執法機關知悉資訊保安的最新趨勢和發展，以及業界關注的保安問題(第 11.6 段)。

40. 私營機構在制訂和推行交流資訊的措施方面，也應該出一分力(第 11.6 段)。

41. 當局應鼓勵私營機構，特別是專業團體、行業組織和商會在各個層面更大力推動資訊保安的教育及宣傳工作(第 11.7 及 11.8 段)。

42. 政府部門及公營機構應盡量支持私營機構推行的資訊保安宣傳及教育措施。同樣地，當他們舉辦教育計劃時，也應積極尋求私營機構的支持(第 11.9 段)。

43. 政府應繼續讓私營機構參與制訂電腦罪案的政策，以及較定期地諮詢私營機構(第 11.10 及 11.11 段)。

44. 應探討可否為不同行業及在不同層面，制訂一套公認的審核或評估機制，以認證資訊保安的標準(第 11.12 段)。

資源和能力

45. 當局應提供足夠資源來打擊和防止電腦罪案(第 12.17 段)。

46. 執法機關應繼續密切留意是否有足夠的專才，以調查電腦罪案和鑑證電腦資料，確保這類專業人員的供求不致失衡，並應盡量利用私營機構的資源和取得它們的合作(第 12.18 段)。

47. 把各個執法機關與電腦罪案有關的所有資源匯集一起，成立一個一站式的中央單位的建議，應予擱置(第 12.19 段)。

48. 各個執法機關互相合作、交流情報和經驗的做法，應該繼續並加以深化(第 12.20 段)。

49. 執法機關應加強與本港以外對口單位的聯繫(第 12.21 段)。

50. 執法機關應密切留意國際間有關處理電腦證據程序的發展，確保有關國際標準一旦確立，香港的程序應可與之相符(第 12.22 段)。

51. 當局應盡快制訂一套處理電腦證據的標準程序，供本港各執法機關使用。即將成立的電腦資料鑑證室應負責牽頭制訂這套通用標準(第 12.23 段)。

52. 處理電腦證據的通用標準一旦制訂完成，便應告知司法人員、律師，以及有關人士和團體(第 12.23 段)。

53. 從較長遠的角度來看，當局應考慮設立一個中央電腦資料鑑證單位或鑑證室，以便統一提供電腦資料鑑證服務(第 12.24 段)。

未來的體制安排

54. 當局應在撲滅罪行委員會下成立一個小組委員會，以跟進工作小組的建議、監察這些建議的相關發展，以及評估建議對我們的政策和措施的影響(第 13.8 段)。

55. 上述小組委員會應包括執法機關的高層代表和私營機構的代表(第 13.9 段)。

其他

56. 當局在訂立新法例和修訂現有法例時，一般應留意資訊時代的需要。法例應盡量跨越個別科技或媒體的界限(第 14.4 段)。

57. 為盡量爭取市民支持和合作，當局在制訂工作小組建議的執行細則時，應徵詢公眾及有關團體的意見(第 14.5 段)。

第一章

背景及工作方針

引言

1.1 過去幾年，互聯網和電腦的應用顯著增長，令日常生活中的學習、通訊、消閑和商務等各方面，都大大提高了速度，也帶來更多方便。不過，這樣也令不法分子有機可乘。電腦相關罪案(1)增加，是國際關注的課題。

1.2 在香港，警方和海關處理的電腦罪案舉報數目，由一九九六年的 21 宗，增至一九九九年的 318 宗(2)。一九九六年以來舉報罪案的分項數字如下：

案件性質	1996	1997	1998	1999	2000 (1至6月)
黑客入侵	4	7	13	238	168
發布淫褻物品	6	6	13	32	0
刑事毀壞資料數據	4	3	3	4	6
互聯網購物詐騙	0	2	1	18	11
侵犯版權	不適用	不適用	不適用	1	43

(1) “電腦罪案”和“電腦相關罪案”是兩個通常可換用的詞語，都是指通過電腦或互聯網干犯的罪案，詳情見第二章第 2.1 段。至於是否需要就“電腦”一詞界定更精確的法律定義的問題，我們將在第三章探討。

(2) 由其他執法機關處理的電腦罪案為數極少。

案件性質	1996	1997	1998	1999	2000 (1至6月)
其他	7	2	4	25	22
總計	21	20	34	318	250

工作小組

1.3 在這背景下，電腦相關罪行跨部門工作小組(工作小組)於二零零零年三月成立。工作小組的職權範圍載於附件1。工作小組由保安局的代表擔任主席，核心成員包括政府多個局和部門的代表，詳盡的成員名單載於附件2。

1.4 在二零零零年三至八月期間，工作小組共舉行了六次正式會議。此外，工作小組成員之間，以及工作小組代表與有關私營機構(例如互聯網服務供應商)、學術界和有關法定機構之間，也進行了多次討論。工作小組有部分成員曾到美國考察，並與當地的相關政府機構、其他組織及個別人士討論各項有關問題，聽取他們的意見及經驗。此外，我們也曾向資訊基建諮詢委員會(3)簡介我們的工作，並徵詢該委員會成員的意見。由於工作小組屬於政府內部的專責小組，而我們提出的建議在實施前還須經過內部審議，因此我們沒有進行正式和全面的公眾諮詢。雖然如此，我們從與外界人士的討論中，獲益良多；對於各界在過去半年所提供的意見和協助，我們謹此衷心致謝。他們的支持有助我們衡量眾多不同的考慮因素，並制訂建議。

工作方針

1.5 我們的工作重點，是改善對付電腦罪案的執法架構或環境。因此，我們嘗試找出問題所在，並就電腦罪案的預防、蒐集證據、調查和檢控方面的問題，建議立

---

(3) 請參閱第十三章第13.6段

法或其他方面的對策。我們的最終目標，是協力提供一個有利於正當使用電腦和互聯網的環境。

1.6 我們採用宏觀的方針，盡可能找出全盤適用的對策。因此，我們不是要處理所有可能通過電腦或互聯網干犯的個別罪案。它們應繼續在有關的政策範疇內予以考慮。舉例來說，網上賭博應該是整體賭博政策中的一環，並應在這個範疇內考慮如何適當處理。不過，由於我們提出的建議會加強或有助撲滅電腦罪行的執法工作，因此對這些個別的罪案也會有影響。

1.7 在制訂建議時，我們一直注意要在促進執法與有關代價兩者之間取得平衡。我們傾向在可行情況下以行政措施取代立法，並在建議立法增加權力時，致力確保有足夠的制衡。由於互聯網並無疆界，我們在討論過程中也積極考慮國際間的相關發展和趨勢。

1.8 工作小組受命在大約半年內完成工作。在討論過程中，我們遇到一些需要較長時間作更深入研究的問題。就這些問題，我們都設法定出基本的範疇，以便作進一步研究。如有關問題需要即時的紓緩，我們也建議了一些可行的措施。

1.9 我們也遇到一些在工作小組研究範圍以外的問題，當中有些是本身需要作出跟進，有些則是因實施我們的建議之後而要作出跟進。我們在隨後各章節中會指出這些問題。

第二章

現行法例

引言

2.1 “電腦罪案”和“電腦相關罪案”是兩個通常可換用的籠統詞語，都是指下列任何一項：

(a) 直接以電腦或電腦系統為目標的罪行(例如非法闖入電腦系統，即俗稱的黑客入侵)；

(b) 利用電腦作為媒介的罪行(例如網上賭博)；以及

(c) 電腦只起附帶作用的罪行(例如在互聯網上刊登廣告，吸引顧客到書店購買色情物品)。

工作小組關注的重點是(a)類及整體(b)類罪案(而非個別案件)[4]。屬於(c)類的罪案只與電腦有些微的間接關係，在其他範疇處理會更合適。如這類罪案的調查工作涉及電腦記錄加密等的一般性問題，才會與我們目前審議的事項有關。

概況

2.2 針對電腦相關罪案的主要法例是一九九三年制訂的《電腦罪行條例》。該條例透過修訂《電訊條例》(第106章)、《刑事罪行條例》(第200章)和《盜竊罪條例》(第210章)，訂立了一些新罪行並擴大了一些現有罪行的涵蓋範圍，詳見下表。

---

(4) 請參閱第一章第1.6段

法例	條文	最高刑罰
第 106 章第 27A 條	禁止藉電訊而在未獲授權下取用電腦資料	罰款：20,000 元
第 200 章第 59 條	把財產的涵義擴大，包括電腦內或電腦儲存媒體內的任何程式或資料	不適用
第 200 章第 59 及 60 條	把刑事損壞財產的涵義擴大，包括誤用電腦程式或資料	監禁 10 年
第 200 章第 85 條	把在銀行簿冊作出虛假記項的涵義擴大，包括擅改任何銀行以電子方法所備存的帳目簿冊	終身監禁
第 200 章第 161 條	禁止有犯罪或不誠實意圖而取用電腦	監禁 5 年
第 210 章第 11 條	把入屋犯法罪的涵義擴大，包括非法地導致任何電腦以並非該電腦的擁有人所設立的電腦運作方式運作，以及更改、刪除或加入任何電腦程式或數據	監禁 14 年

法例	條文	最高刑罰
第 210 章第 19 條	把偽造帳目的涵義擴大，包括毀壞、污損、隱藏或擅改用電腦保存的記錄	監禁 10 年

2.3 此外，很多其他法例條文也有提及“電腦”或類似詞語，現列舉一些例子如下。

法例	條文
《證據條例》(第 8 章)第 20 條	藉電腦備存的銀行記錄內的記項副本，可接納為證據
第 8 章第 22A 條	在刑事法律程序中可接納來自電腦記錄的文件證據
第 8 章第 54 條	把由電腦產生的記錄包括在“記錄”的涵義
《證券（內幕交易）條例》(第 395 章)第 2 條	把任何形式的電腦輸入或輸出的材料包括在“文件”的涵義
《土地測量條例》（第 473 章）第 2 條	把電子數據記錄儀所印出的印本包括在“外業記錄”的涵義
《版權條例》(第 528 章)第 4 條	把電腦程式包括在受版權保護的作品的涵義
第 528 章第 26 條	經由互聯網提供版權作品的複製品，列作受版權所限制的作為

法例	條文
《專利條例》第 514 章第 93 條	指明用於電腦的程式不得被視為可享專利的發明
《電子交易條例》(第 553 章)	賦予電子記錄及數碼簽署與文件記錄及簽署相同的法律地位
《非政府簽發產地來源證保障條例》(第 324 章)第 10 條	賦權獲授權人員要求任何載於電腦的資料以可取去和以可見或可閱讀的形式出示
《證券條例》(第 333 章)第 83 條	任何人如故意將虛假要項儲存於電子裝置內或擅改電子裝置內的記項或銷毀電子裝置內的記錄，即屬犯罪
《吸煙(公眾衞生)條例》(第 371 章)第 13B 條	禁止將煙草廣告置於互聯網上

2.4 在很多情況下，有關條例雖無明文提到網上環境，但仍可詮釋為同時涵蓋現實世界和虛擬世界。舉例來說，《個人資料(私隱)條例》不但適用於現實環境，同樣也適用於網上環境。

檢討

2.5 工作小組檢討了《電腦罪行條例》所作的法例修訂(上文第 2.2 段)。我們相信這些修訂的***要點仍然適用***。尤其是新訂的兩項罪行，即藉電訊而在未獲授權下取用電腦資料(第 106 章第 27A 條)和有犯罪或不誠實意圖而取用電腦(第 200 章第 161 條)，讓當局可以處理多宗已舉報的電腦罪案。整體來說，《電腦罪行條例》訂立的新罪行或擴大涵義的罪行，應該繼續保留。

2.6 在第三至第七章，我們會探討電腦罪行涉及的各項法律問題。我們會深入研究應否和如何修訂或改善部分現有法例的條文，以配合我們提出的建議。

2.7 因此，在現階段，我們只希望指出目前*有一明顯不足之處*，亦即第 106 章第 27A 條黑客入侵罪行(請參閱第 2.2 段)的刑罰。目前，這項罪行的最高刑罰只是罰款 20,000 元。由於黑客入侵可能引致極其嚴重的破壞，工作小組認為目前的刑罰顯然不足以產生阻嚇作用。因此，我們*建議*這項罪行應該加入監禁刑罰。我們會在第六章深入探討有關的問題。

2.8 工作小組曾經考慮是否應該將本報告書建議的各項法例修訂納入一條單一法例之內，這樣做可能會較逐一修訂多條現行法例簡單方便。但與此同時，我們了解到電腦和互聯網的應用已非常普遍。因此，我們主張把資訊科技的使用視為整體法例中的已知事實，而不是要將它分開處理(請同時參閱第十四章)。因此，只要修訂建議的用意和實質內容清晰明確，我們會讓法律草擬人員決定如何立法才最切合有關修訂建議。

第三章

“電腦”一詞的涵義

引言

3.1 目前，本港法例基本上並無界定何謂“電腦”及“電腦系統”，這兩個名詞的涵義一向是由法庭予以詮釋。雖然本報告書的其餘部分仍會沿用這兩個簡便的名詞，我們在下文會研究在法律上是否要為這兩個名詞提供一個較為一致的定義。

現行的法律定義

3.2 在香港現行法例下，“電腦”一詞在《證據條例》(第8章)第22A條、《稅務條例》(第112章)第26A條及《商業登記條例》(第310章)第19條內被界定為：

“儲存、處理或檢索資料的器材”。

3.3 《電子交易條例》(第553章)並無試圖界定“電腦”或“電腦系統”的定義，而是採用了“資訊系統”的概念。該詞的定義如下：

“符合以下所有說明的系統：

(a) 處理資訊；

(b) 記錄資訊；

(c) 能用作使資訊記錄或儲存在不論位於何處的其他資訊系統內，或能用作將資訊在該等系統內以其他方式處理；及

(d) 能用作檢索資訊(不論該等資訊是記錄或儲存在該系統內或在不論位於何處的其他資訊系統內)”。

其他司法管轄區的例子

3.4 在歐洲議會《網上罪案公約》草案(請參閱第十四章第14.2段)內，“電腦系統”指“*任何依照程式執行自動數據處理的裝置或一組互連裝置*”。

3.5 美國《法令》第18項第1030條“與電腦有關的詐騙及相關活動”的條文中，“電腦”一詞的定義如下：

“執行邏輯運算、算術運算或儲存功能的電子、磁性、光學、電子化學、或其他高速數據處理裝置，也包括任何與上述裝置直接有關或與這些裝置共同操作的數據儲存設施或通信設施，但這個名詞不包括自動打字機或排字機、手提計算機，或其他相類的裝置。”

3.6 加拿大《刑事令》第九部有關“損害產權的罪行 — 與盜竊罪類似的罪行”的條文訂明，“電腦系統”和“電腦程式”的定義如下：

“電腦系統指一項裝置，或一組互連或相關的裝置，而其中最少有一個部分：

(a) 包含電腦程式或其他數據；以及

(b) 依照電腦程式

(i) 執行邏輯運算及控制功能；以及

(ii) 可以執行其他功能，

電腦程式指代表指令或語句的數據，在電腦系統中執行時可使電腦系統執行某項功能。”

考慮因素

3.7 從狹義來說，“電腦”一詞通常使人聯想到一台包括顯示器、鍵盤及中央處理器的獨立機器。不過，隨着

互聯網、電子個人數據助理器等設施和無線應用規約(WAP)等技術的發展，這個詞語的含義愈來愈廣，所指的物品種類繁多，包括聯網電腦系統和多種流動電子通訊器材。

3.8 至於“電腦”一詞是否要有明確的法律定義的問題，有兩種不同的意見。一種意見認為，科技發展日新月異，十年前這個名詞所指的不過是獨立桌上電腦或巨型主機系統，現在則指很多不同的器材。因此，有關的法律定義可能會流於太過籠統或可能要經常更新。另一種意見則認為，如果完全依賴法庭作出詮釋，則可能會因個別法官的取向不同而出現差異甚大的判決。

3.9 總的來說，工作小組認為應在法例中訂明一些範圍，以詮釋“電腦”這個概念。有關的定義不應過於狹窄，以免不能涵蓋新的器材或技術。定義應能涵蓋獨立電腦、電腦系統及流動通訊／資訊設備等不同器材。由於“電腦”一詞的含義可能過於狹窄，未能符合現今情況，我們建議以一個涵蓋面較廣的詞語表述有關的法律範圍。工作小組*建議*採納《電子交易條例》(第 553 章)(上文第 3.3 段)所界定的“資訊系統”一詞，以取代“電腦”一詞。據我們所知，“資訊系統”一詞的定義在界定時，已兼顧到國際上最新的資訊科技發展情況。有關定義不久前在立法機關討論《電子交易條例草案》時經過審議。(草案已於二零零零年一月通過。)此外，我們知悉資訊科技及廣播局會定期檢討該條例，以配合有關的發展。如果“資訊系統”一詞的定義是以第 553 章所用者為準，日後任何對後者的修訂，都會自動適用於前者。

3.10 我們檢視過本港的法律，發現“電腦”一詞曾在 35 條條例共 76 項條文中出現。(這些條文的一覽表載於附件 3。)經瀏覽有關條文後，我們認為當可把其中“電腦”一詞改為“資訊系統”。為使法律用語更為一致，我們原則上應把所有有關條文的用語劃一。不過，我們考慮到在某些條文中，使用“電腦”一詞可能涉及一些我們不知的政策因素。因此，我們*建議*應

先要求政府各局檢討其職權範圍內的有關條文，若它們同意修訂，我們*建議*把法例內“電腦”一詞改為“資訊系統”。

簡便用語

3.11 嚴格來說，法律上並無“黑客入侵”這項罪名，有關罪行是以“未經批准循電訊途徑進入電腦”或“有犯罪或不誠實意圖而取用電腦”等方式表述。同樣，我們在上文第 3.9 及 3.10 段提出的建議，無非是為了使人容易明白“電腦”及“電腦系統”等概念的法律意義，因為這些概念在法律上的表達方式須較日常生活所用的精確。為方便提述起見，本報告書的其餘部分仍會沿用“電腦”及“電腦系統”等詞語，作為簡便用語，但其含義仍應按《電子交易條例》中“資訊系統”一詞的定義來理解。

第四章

司法管轄權

引言

4.1 電腦罪案並無地域界限之分。這種跨境性質使我們要以一個新的觀點看待司法管轄權的傳統概念。我們會在下文研究有關問題。

目前情況

4.2 在現實世界中，犯案者通常都是身處犯罪現場或是在附近地方。因此，傳統上司法管轄權的概念與地理疆界密切相關。除非特別指明，法院的司法管轄權只適用於在有關國家或地區的地理疆界內發生的罪行。一般來說，根據普通法，若構成罪案的最後行為或事件在某地發生，則該罪案會被視為在當地干犯，而司法管轄權也由干犯罪案當地的機關行使。

4.3 隨著通訊方法日趨進步，跨境罪案亦相應而生。處理這個問題的一個方法，是與其他司法管轄區訂立雙邊刑事事宜司法互助協定，目的是確保締約雙方都可以獲得對等的待遇，以及加強國際合作打擊跨境罪案。司法互助協定涵蓋的主要協助項目通常包括：

- 辨認和追尋疑犯及證人；
- 送達文件；
- 取得證據；
- 執行搜查及檢取物品的要求；
- 提供有關刑事事宜的文件證據；
- 移交有關人士以便作供或協助充公事宜；以及

- 追查、約制及充公用作犯罪的財產或犯罪所得的財產。

4.4 司法互助有助蒐集跨境罪案的證據，並對偵破跨境網上罪案有一定幫助。不過，如果與罪案有關的交易及事件在一個以上的司法管轄區發生，司法互助本身也不能解決司法管轄權的問題。

4.5 香港在一九九四年十二月制訂了《刑事司法管轄權條例》(第 461 章)。該條例旨在處理國際詐騙案涉及的司法管轄權問題。該條例賦予香港法院對詐騙和不誠實罪案有如下司法管轄權：

(a) 如為使罪行定罪而須予證明的任何行為(包括不作為)或其產生的後果的任何部分在香港發生，則香港法院擁有司法管轄權。

(b) 企圖在香港犯罪的行為可在香港審訊，不論該企圖犯罪的行為是在香港或任何其他地方作出，亦不論該行為是否在香港產生作用。

(c) 在香港企圖或煽惑他人在任何地方犯罪的行為，可在香港審訊。

(d) 串謀在香港犯罪的行為可在香港審訊，不論該串謀行為是在什麼地方作出，亦不論有否在香港作出任何事情以促進或助長該串謀行為。

(e) 在香港串謀在任何地方進行一些若在香港進行會構成罪行的事情，則該串謀行為可在香港審訊，但擬進行的行為必須在擬進行該行為的司法管轄區內屬於犯法的行為。

條例所適用各項罪行可由行政長官會同行政會議藉命令予以修訂，但命令的草稿必須先獲立法會通過。對於《電腦罪行條例》所訂立的罪行(請參閱第二章第 2.2 段)，《刑事司法管轄權條例》只涵蓋透過電腦偽造帳目這項罪行。

4.6 《刑事司法管轄權條例》未有涵蓋的許多電腦罪案，顯然也有可能屬於跨境性質，例如黑客入侵、通過更改或刪抹電腦程式或數據構成刑事損壞，以及網上賭博等。司法管轄權的問題必須非常認真處理。

其他司法管轄區的法例

4.7 英國相當早便已認識到電腦罪案涉及的司法管轄權問題。英國的 1990 年《不當使用電腦令》訂明，如罪案受害人或犯案人身處英國，則英國法院對該法令所涵蓋的罪行享有司法管轄權。該法令涵蓋的罪行包括未獲授權下取用電腦程式或數據、未獲授權下進入系統意圖干犯或協助干犯繼發罪行(5)，以及未獲授權下改動電腦的任何內容。

4.8 同樣，新加坡的《不當使用電腦令》准許對在新加坡境內或境外干犯的電腦相關罪行提出檢控。如有人在新加坡境外任何地方觸犯該法令所涵蓋的罪行，則該人會如在新加坡境內觸犯該罪行般受到制裁。就有關罪行而言，該法令適用於以下情況：

- 案發時被告人身處新加坡；或
- 案發時涉案的電腦、程式或數據在新加坡境內。

新加坡的《不當使用電腦令》所涵蓋的罪行包括未獲授權下取用電腦資料、取用電腦意圖干犯或協助干犯罪行(6)、未獲授權下改動電腦資料、未獲授權下使用或截取電腦服務、未獲授權下妨礙他人使用電腦，以及未獲授權下披露取用電腦的密碼。

4.9 歐洲議會於二零零零年四月發表的《網上罪案公約》草案(請參閱第十四章第 14.2 段)籲請各成員國就於其境內發生，或在懸掛該國國旗或在該國註冊的船隻、

---

(5) 繼發罪行指可以對 21 歲或以上人士判處五年或以上監禁的罪行。

(6) 涵蓋的罪行包括涉及財產、詐騙、不誠實行為或傷害他人身體，在定罪後可判處不短於兩年監禁的罪行。

飛機、或衞星上發生，或由其國民在任何國家管轄區以外干犯的電腦相關罪行，確立司法管轄權。

考慮因素

4.10 鑑於跨境罪案(不論是否與電腦有關)有所增加，現行的管轄權規則可能會造成不必要的約束。我們曾考慮是否要徹底修訂《刑事司法管轄權條例》的適用範圍。我們曾考慮，與其像現行做法般逐一臚列該條例涵蓋的每項罪行，倒不如採用較為簡單的方法，例如採用“所有可循公訴程序審訊的罪行”這個概括性提述。此舉可以省卻麻煩，毋須逐一辨別一般管轄權規則不適用的每項罪行。可是，這樣會徹底改變管轄權規則的基本原則。《刑事司法管轄權條例》旨在就常規以外的例外情況制訂條文。徹底更改條例的涵蓋範圍至實際上幾乎包括了所有刑事罪行，是不應輕率嘗試的，而且也超出了工作小組的職責範圍。司法管轄權是一個牽涉複雜法律概念的重大問題。要審視這問題，必須對既定的法律原則和不斷演變的判例法進行仔細詳盡的探討，再輔以大量的法律研究和分析。為確保法例的一致性，我們應採用全面而非片面的方式處理。因此，工作小組*建議*，應考慮對整個管轄權規則問題進行徹底深入的研究，以顧及交通和通訊已大為改善的情況。這應是如法律改革委員會等組織的一個合適課題。

4.11 由於牽涉的法律問題複雜，上文第 4.10 段建議的深入檢討需要一段時間才能完成。但工作小組相信，有關電腦罪案的問題需更迫切解決。我們要確保能把電腦罪犯繩之於法，防止他們利用現存的漏洞。我們會在下文闡述如何以妥善的方法，達到這個目的。

4.12 其中一個方案是找出所有可以透過電腦或互聯網干犯的罪行，然後把這些罪行納入《刑事司法管轄權條例》的涵蓋範圍。不過，這類罪行可能為數甚多。此外，這個方案可能導致不同的管轄權規則適用於本質相同而只在有否使用電腦或互聯網這方面有差別的罪

行。舉例來說，有可能出現一套管轄權規則適用於一般賭博罪行而另一套則適用於網上賭博罪行的情況。

4.13 上文第 4.12 段提及的情況使我們更加相信，整個司法管轄權問題應該全面地處理。在現階段，我們認為應盡可能以現有的條文為基礎，然後作出改善。

4.14 我們選擇的方案，是以《刑事罪行條例》第 161(1)(a)條為基礎。該條規定，任何人意圖犯罪而取用電腦，即屬犯罪。後者的罪行與英國和新加坡的繼發罪行在概念上相同，主要的分別在於司法管轄權的問題——在英國和新加坡，有關罪行受延伸的司法管轄權規則所涵蓋(請參閱第 4.7 和 4.8 段)，而在香港則不是。

4.15 如情況許可，追究原來的罪行既是理所當然，又較為簡單直接，無怪乎《刑事罪行條例》第 161(1)(a)條至今從未被引用。不過，倘若司法管轄權延伸，我們便可以引用意圖犯罪而取用電腦這項罪名，打擊那些我們原本無權過問的犯罪行為。舉例來說，倘若一個身處香港以外地方的人透過電子郵件恐嚇另一個身在香港的人，聲言要傷害他的人身、聲譽或財產，有關案件便可交由香港法院審理。因此，我們的第一步*建議*，是把意圖犯罪而取用電腦這項現有罪名(《刑事罪行條例》第 161(1)(a)條)，納入《刑事司法管轄權條例》的涵蓋範圍。換言之，只要取用電腦犯罪的人身在香港或被取用進行犯罪的電腦是在香港，香港法院便有權審理有關案件。

4.16 目前，意圖犯罪而取用電腦的刑罰是監禁五年。我們完全明白，這項刑罰並非針對罪犯意圖觸犯的罪行本身。不過，我們認為針對某行為的刑罰必須與所意圖觸犯罪行的嚴重程度相稱，刑罰才能有足夠的阻嚇能力。如果所意圖觸犯罪行的刑罰是終身監禁，針對含此意圖的行為的刑罰看來也不應以監禁五年為上限。因此，我們*建議*修訂意圖犯罪而取用電腦這項罪行的罰則，使刑罰視乎罪犯所意圖觸犯罪行的嚴重程度而定，但當然不應超逾該意圖觸犯罪行的最高刑罰。由於上述考慮因素並不適用於《刑事罪行條例》第 161(1)

條的其餘部分，當局可考慮讓上述罪行自成一項，並對第 161(1)條作出相應修訂。

4.17 我們曾經研究，除了意圖犯罪而取用電腦這項罪行之外，是否還有其他罪行應該納入《刑事司法管轄權條例》的涵蓋範圍。基於上文第 4.10 及 4.12 段所述的考慮因素，我們在現階段不建議大幅擴闊該條例的涵蓋範圍。不過，我們*建議*下列罪行在根據本報告書的建議作出修訂後，也應納入該條例的涵蓋範圍：

- 藉電訊而在未獲授權下取用電腦資料(《電訊條例》第 27A)；以及

- 除上文第 4.15 段所述者外，有犯罪或不誠實意圖而取用電腦這項罪行的其餘部分，即不誠實地意圖欺騙；目的在於使其本人或他人不誠實地獲益；或不誠實地意圖導致他人蒙受損失(《刑事罪行條例》第 161(1)(b)、(c)及(d)條)。

這些罪行可以稱為“純粹”或“直接”的電腦罪行，因為電腦是這些案件的主體而非只起附帶的作用。《刑事司法管轄權條例》的規定應適用於這些罪行，以待對司法管轄權規則進行全面檢討。

第五章

加密

引言

5.1 加密科技發展一日千里，也愈來愈普及。作為一項保安工具，加密技術對保護機密或個人資料非常有用。舉例來說，加密技術是確保人們對電子商貿具有信心的主要關鍵。然而，罪犯也同樣會利用加密技術來保護他們的電腦記錄和電郵通信。如果沒有正確的解密鍵，要偵查受保護的交易和抽取可接納的證據來提出檢控，縱使並非完全無從入手，亦會是困難重重。下文會探討涉及的問題。

目前情況

5.2 對於用作證據或供調查之用的電腦記錄可能經過加密的問題，香港有關電腦記錄的法例通常都沒有作出規定。即使有規定，在法律上也往往只要求有關電腦資料須“以可見和可讀的形式提出，並且可以拿取”。就這個問題，附件 4 臚列有關的法例條文。

5.3 現行電腦資料須以可見和可讀的形式提出的法律表述方式，並未受到充分考驗。但是，這表述方式是否能圓滿解決加密的問題，實有相當疑問。這方面的現行法例，並無任何條文明確規定需要提供*經解密*的資料或明碼文本。因此，有人可能認為只要將代碼及符號列印出來，便可符合目前有關可見和可讀資料的要求。當然，這些代碼及符號對於調查或檢控工作的幫助極微。

其他司法管轄區的例子

5.4 其他司法管轄區為解決加密鍵的問題，曾研究或採取以下措施：

- 禁止在未獲授權下進行加密；

- 將利用加密技術促致干犯刑事罪行、隱瞞刑事不當行為、或妨礙政府調查刑事罪行的行為，列為罪行；

- 規定設立強制性的加密鍵託管機構；以及

- 賦予權力，可藉由手令或命令要求提交加密鍵。

以下我們會研究一些例子。

5.5 中國內地，俄羅斯和沙特亞拉伯全都禁止在未獲授權下使用加密產品。

5.6 瑞典於一九九九年五月發表的密碼政策文件表示，由用者自願把私人加密鍵存放於託管機構，讓當局可循合法途徑取用，是平衡執法者和使用者需要的解決辦法。

5.7 在美國，一九九八年的《追索密碼鍵法例草案》、一九九八年的《電子私隱令》、一九九九年的《通過加密達到保安和自由的目的令》和一九九九年的《推廣可靠的聯機交易以促進商貿令》，全都訂有條文，把使用加密技術以促致干犯刑事罪行或掩飾罪行列為犯罪。據我們所知，所有這些條文仍未通過成為法律。

5.8 在新加坡，根據《不當使用電腦令》，獲警察總監書面授權的警務人員，可以取用任何資料、代碼或科技，藉以把加密資料數據重新變換或整理成可閱讀和理解的形式。

5.9 在馬來西亞，《數碼簽署令》准許持搜令進行搜查的警務人員取用電腦資料數據，以及獲取所需的密碼、加密代碼、解密代碼、軟件、硬件及其他工具以解讀該電腦資料數據。

5.10 在英國，最近通過的《2000 年規管調查權力令》讓獲授權人可發出通知書，要求有關人士交出受加密保護資料數據的明碼本或解讀資料數據的解密鍵。發出通知書的權力將視乎有關資料的性質，由國務大臣或法官賦予。

5.11 荷蘭及比利時均已擬備條例草案，規定第三者須披露加密鍵，但卻不會強迫任何人提供可使自己入罪的證據。

考慮因素

(a) 改變的需要

5.12 有人可能認為，調查人員的工作之一，正是弄懂所蒐集證據的意義。目前，市面上有不少解密程式售賣，調查人員也自行編寫了一些專門解讀加密資料數據的程式。因此，一個選擇是繼續依賴這些工具。

5.13 不過，由於加密程式種類繁多，可能採用的加密方法更是多不勝數，以致破解加密代碼的工作變得愈來愈困難。更重要的是，我們關注的是從加密數據之中抽取可在法律程序中獲得接納的證據，而不是為收集情報而解讀資料。就前者而言，我們必須在無合理疑點的情況下，證明所用的解密程式或方法正確無誤，以及證明經解密的資料數據就是正確的資料數據。

5.14 有人建議應從根本解決這個問題，即從起初就規管使用加密方法。我們認為這種規管方法本身的成效有限。如果案件已涉及使用加密鍵，這個方法也無法令調查人員取得有關的解密鍵。同樣地，罪犯亦不大可能把解密鍵存放在一個託管戶口。更重要的是，加密技術可用於完全正當的用途，在自由經濟體系內全盤規管使用加密方法是矯枉過正的做法。我們認為，容許執法機關在***有需要和有充分理由時***獲取解密工具或經解密的文本(包括所有圖像和聲音)，會是較為適當和直接的做法。我們***建議***通過法例以達致這一目的。

(b) 方案

5.15 純粹從方便執法的角度來說，負責調查工作的執法機關如果在取用解密鍵或解密文本方面毋須受到太多限制，固然會較為理想。在大部分情況下，執法機關已經掌握有關的電腦記錄，問題只在於能否把代碼解讀。未能及時掌握解密鍵或解密文本，足以導致錯失拘捕從犯或檢取犯罪得益的良機。

5.16 與此同時，我們不應掉以輕心，必須確保要求披露解密鍵的權力不會被濫用。因此，我們根據上文第 5.5 至 5.11 段列舉的其他司法管轄區的例子，研究了幾個可行的方案。

5.17 方案一建議把強迫披露解密鍵或解密文本的權力，授予有關執法機關的高級人員。舉例來說，當局可以規定，只有獲得有關執法機關首長親自以書面授權的人員，才可以行使該項權力。此外，每項授權均只應適用於指定的某宗案件。方案二與方案一大同小異，分別只是把該項權力授予一名局長。舉例來說，如案件涉及《刑事罪行條例》下的罪行，便授權予保安局局長；如案件涉及《版權條例》下的罪行，則授權予工商局局長。方案三則建議引入司法審查，以加強制度上的制衡，確保執法機關不會輕率行使權力要求披露解密鍵或解密文本。

5.18 首兩個方案在執行上應當較為迅速，對於講求速度的電腦罪案調查工作會很有用。把權力授予執法機關的首長或局長，可以確保該項權力不會任意行使。這兩個方案的任何一個都理應足夠。不過，我們認為，任何規定如果涉及強迫他人披露資料，特別是披露一些可能導致披露者本人入罪的資料，在處理上便須更為審慎。不令自己入罪、私隱及資料保密等個人權利，應該盡量尊重。把強迫披露資料的權力授予一個非執法機關，可以令人覺得有適當的制衡。經衡量各種因素後，工作小組*建議*對披露資料的規定引入某種形式的司法審查。

(c)“提交令”程序

5.19 在擬定司法審查程序時，我們參考了《有組織及嚴重罪行條例》(第 455 章)中俗稱“提交令”的條文。根據該條例第 4 條，律政司司長或獲授權人可向原訟法庭提出單方面申請，要求發出命令，以便為偵查有組織罪行或與有組織罪行有關連的罪行而要求提交或取覽有關物料。法庭須信納該項申請已符合某些條件，才會發出這項命令。舉例來說，如偵查的是某項有組織罪行，法庭須信納有合理理由：

(a) 懷疑有人已犯該有組織罪行；

(b) 相信與申請有關的物料相當可能與偵查有關，而且並不包括享有法律特權的物品；以及

(c) 相信要求提交或取覽有關物料是符合公眾利益的。

5.20 受制於“提交令”的人可向法庭申請撤銷或更改該命令，但不得以提交有關物料可能使他獲罪為理由而不予遵從。任何人如不遵從該命令，即屬犯罪，可處罰款最高十萬元及監禁一年。

5.21 實際上，“提交令”申請須經律政司司長審慎研究案情後，才由其本人或獲授權人提出。如屬證據確鑿的案件，調查人員可以在徵詢律政司司長的意見後擬備誓章，然後向原訟法庭提出申請。如屬較難以確定或複雜的案件，申請會由律政司司長提出。這個程序加上司法審查的規定，應足以保證此類申請只在有需要及有充分理由的情況下才會提出和批准。

5.22 工作小組*建議*，准許取覽與偵查有關的加密電腦資料的命令，亦應採用類似第 455 章第 4 條有關申請“提交令”的程序。取覽的方式可以是提供明碼或解密文本，或者是提供可以解讀有關電腦資料的密碼、加密代碼、解密代碼、軟件、硬件及其他方法。

5.23 擬議法例有數個可能的適用範圍。首先，擬議法例或可適用於《有組織及嚴重罪行條例》(第 455 章)訂明的提交令所涵蓋的有組織及嚴重罪行。不過，這只會涵蓋與黑社會活動有關、或涉及兩人或以上所策劃和組織的罪行。就我們的目的而言，這個範圍過於狹窄。

5.24 另一個可能，是對在刑事調查過程中檢取或獲取的已加密電腦資料，都引用披露規定。這個做法比較容易實行，並可確保處理方法一致，但潛在缺點是範圍可能太闊。舉例來說，有人可能認為強迫披露解密鍵的規定，不應適用於一些“輕微”的電腦罪行，而只應適用於較嚴重的罪行。鑑於這項措施的嚴厲性，可能涉及披露導致披露者入罪的證據，我們贊同這項意見。

5.25 基於上述考慮因素，我們*建議*制訂額外的保障措施，限定要求披露的權力只適用於性質比較嚴重的罪行。例如只有定罪後最高可判處不少於兩年監禁的罪行，才受這項規定限制。

5.26 如果上文第 5.22 及 5.25 段的建議獲得通過，我們會進一步*建議*提供適當法律保障，確保透過披露程序取得的資料必須保密。法例亦應訂明，透過強迫披露取得的證據可以獲得法庭接納。

5.27 擬議法例必須有實際效力，這點非常重要。由於披露規定適用的案件可能牽涉數額龐大的金錢，當局必須制訂嚴厲的刑罰，以處理未有合理理由而不遵照命令准許取覽已加密資料的情況。純粹罰款未必是有效的阻嚇措施，因為罰款可被視為一項運作成本。我們*建議*，有關刑罰原則上必須與調查中的罪行的刑罰相稱。

第六章

保護電腦資料數據

引言

6.1 我們在本章探討電腦和互聯網的發展如何令資料數據保護的問題更形嚴重，並會評估是否需要加強保護，防止電腦資料數據在未獲授權下被取用及使用。

目前情況

6.2 目前，只有《個人資料(私隱)條例》界定“資料”一詞的法律定義。該條例第 2 條訂明，“資料”指“*在任何文件中資訊的任何陳述(包括意見表達)，並包括個人身分標識符*”。按這個定義，資料的涵義極廣，包括例如版權作品、個人資料、信用卡資料、商業秘密、密碼等等。

6.3 目前，一些已明確界定類別的資料，例如版權作品、個人資料和證券交易的內幕消息，均受到特定法例的規管，但沒有法例保障所有的資料。涉及不受特定法例保障的資料的侵權行為，會視乎情況以不同方式處理。舉例來說，如事情涉及洩漏在機密情況下告知的敏感商業資料，當事人可能會訴諸民事訴訟。又如事情涉及盜用信用卡資料進行購物騙案，則通常會列作行騙案或盜竊信用卡案處理，因此，“盜竊”資訊的問題並沒有受到正視。

6.4 政府早在一九九三年已認識到有需要保護電腦資料數據，因而制訂了《電腦罪行條例》。舉例來說，“財產”的涵義擴大後，《刑事罪行條例》(第 200 章)所指對財產的刑事損壞罪行，現已包括濫用電腦數據(更改、刪抹或增添電腦內的數據)。《盜竊罪條例》(第 210 章)所指的“入屋犯法罪”經修訂後，現在亦包括侵入建築物內，意圖非法地更改、刪除或加入電腦數據的行為。此外，根據《電訊條例》(第 106 章)，任何

人藉電訊致使電腦執行功能，在未獲授權下取用該電腦所保存的數據，即屬犯罪。

6.5 儘管如此，在現行法例下，“盜竊”電腦資料數據這項行為本身並非刑事罪行。此外，接收、處理或複製未獲授權下取得的電腦資料數據，亦毋須受到法律制裁。

其他司法管轄區的法例

6.6 其他司法管轄區保護電腦資料數據的法例，主要是保障電腦資料數據不會在未獲授權下被人取用。受保護的可以是一般或特定的資料數據，對於後者而言，電腦密碼是保護的重點。下文第 6.7 至 6.13 段列舉一些例子。

6.7 在英國，根據《不當使用電腦令》，任何人如致使電腦執行功能，意圖在未獲授權下取用電腦保存的資料數據，即屬犯罪。

6.8 在美國，屬聯邦法例的美國《法令》第 18 項標題第 1030(a)(b)條訂明，凡明知及有欺騙意圖而非法買賣可以在未獲授權下取用電腦的密碼或類似資料，即屬犯罪。

6.9 根據加拿大的《刑事令》，任何人藉欺詐手段及在未獲授權下取用電腦服務、截取電腦系統功能、利用電腦系統干犯與電腦資料數據或程式有關的損害罪行，即屬犯罪。

6.10 在德國，任何人在未獲授權下取用並非供他使用的資料數據，而這些資料數據是受到特別保護以防有人在未獲授權下取用的，即觸犯“刺探資料數據間諜活動”罪行。這項罪行所指的資料數據，指明限於用電子或磁力方式或以不能直接可見方式儲存或傳送的資料數據。

6.11 根據馬來西亞的 1997 年《電腦罪行令》，任何人直接或間接把可以取用電腦的號碼、代碼、密碼或其他方式傳達給一名他未獲正式授權傳達的人士，即屬犯法。

6.12 在新加坡，《不當使用電腦令》規定，在未獲授權下取用電腦資料，即屬犯法。此外，該法令又禁止在未獲授權下披露密碼或取用碼，以取用任何電腦程式或資料數據作任何不當的圖利行為、不法用途，或不當地引致他人蒙受損失。

6.13 歐洲議會在二零零零年四月發表的《網上罪案公約》草案(請參閱第十四章第 14.2 段)籲請成員國保護用以取用電腦系統的電腦密碼或代碼，以免在未獲授權下被使用。

考慮因素

(a) 保護的需要

6.14 資料保護並非網上世界獨有的問題。舉例來說，信用卡資料可以透過實際竊取信用卡而盜取，不一定要在未獲授權下闖入信用卡資料庫或盜取網上購物交易的資料。不過，電腦和互聯網的發展令多方面的問題惡化，詳情如下：

(a) 虛擬資料數據來往的流通量和速度均明顯增加。

(b) 大量資料數據被取用及複製以供日後在未獲授權下使用的危機大增。這類罪案的規模可能相當宏大。整個資料數據庫的內容可在數秒之內被複製或受到干擾。要是實體資料數據，這種情況不大可能出現。

(c) 有關“損失”也許不能即時發覺，受害者通常要較遲才發覺或根本不發覺有損失。如果損失的是實物，例如是信用卡，受害者很容易便會發覺。

(d) 借助傳統法例作出補救的可行性愈來愈受到局限。舉例來說，在網上世界，要“盜取”信用卡資料也不一定要取去有關的信用卡。任何人如實際偷取信用卡，可按現行法例被控以“盜竊”罪，但如果他在未獲授權下透過互聯網取用信用卡資料，則可能毋須受到制裁。

6.15 在網上世界，未獲授權而取用資料的行為，可能引致極大的經濟損失，也可能大大削弱消費者的信心，以致影響電子商貿的進一步發展。附件 5 列舉了一些這方面的例子。雖然保護資料並非網上世界獨有的問題，我們仍須採取措施，確保藉電腦和互聯網儲存和傳送的資料數據獲得充分保護。

(b) 方案

6.16 我們曾考慮能否把電腦資料數據作為可竊取的財產看待。這樣的話，《盜竊罪條例》(第 210 章)中“財產”一詞[7]的現有定義便須作出修訂，以涵蓋電腦資料數據。《刑事罪行條例》(第 200 章)中這個詞語的定義，即“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”，正好作為合適的基礎。這項安排有現有法例可循，表面看來是較為直接的方法。修訂《盜竊罪條例》中“財產”一詞的定義，會使該條例的其他條文適用於盜取電腦資料數據。這項修訂也可使該條例中“財產”一詞的定義，與《刑事罪行條例》中該詞的定義一致。

6.17 不過，經仔細研究後，我們發現第 6.16 段的方法也非毫無漏洞。問題正是來自“盜竊”一詞的概念。根據《盜竊罪條例》(第 210 章)，如任何人不誠實地挪佔屬於另一人的財產，“意圖永久剝奪該另一人的財產”，即屬犯盜竊罪。很明顯，這個概念不經修訂的話將難以適用於電腦資料數據，因為在網上環境，“盜竊”資料數據總是指在未獲授權下取用或複製資

(7) “財產”一詞在第 210 章的現有定義為“金錢及所有其他土地及非土地財產，亦包括據法權產及其他無形財產”。

料數據，這些資料數據不論是否會供日後使用，都不會發生永久剝奪的問題。此外，如果要把盜竊的概念應用於電腦資料數據，便可能產生電腦資料數據屬誰所有和是否必須懷有不誠實意圖的問題。經衡量各種情況後，我們認為，利用現有的電腦資料數據保護條文(第 6.4 段)作為基礎，再加以增添修訂，會是較有效的做法。

6.18 我們首先以現行《電訊條例》訂定的罪行作為出發點，即藉電訊而在未獲授權下取用電腦數據，即屬違法。我們留意到該條例第 27A 條明確闡釋未獲授權取用數據的概念：

"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。"

只要是藉電訊作出未獲授權而取用資料的行為，便無須證明有犯罪或不誠實意圖。此外，根據《刑事罪行條例》第 161 條，任何人取用電腦，不論是否已獲授權，如目的在於使其本人或他人不誠實地獲益，或不誠實地意圖導致他人蒙受損失，即屬違法。條例並無指明取用的方法，因此應包括任何方法。再者，根據《刑事罪行條例》第 60 條，在無合法辯解或罔顧後果情況下濫用電腦，包括更改、刪抹或增添電腦內的數據，即屬犯罪。

6.19 我們認為，上述條文綜合起來已可涵蓋大部分需要保護的情況。我們*建議*實行下列改善措施：

(a) 就涵蓋範圍而言，現行條文顯然已涵蓋所有儲存於電腦*內*的資料數據。為免生疑問，這些條文應闡明資料數據還包括所有透過電腦或互聯網傳輸或正在傳輸的資料數據。這樣便能涵蓋例如未獲

授權的截取行為。這個構思是要把所有在各個儲存和傳輸階段的電腦資料數據包括在內，而且不用界定需要保護的各類資料數據的定義(例如信用卡資料)。

(b) 為免生疑問，“取用電腦”一詞應闡明為包括取用電腦[8]和取用儲存在電腦的程式及數據。

(c) 現行《電訊條例》第 27A 條把未獲授權下取用電腦的罪行，局限於藉電訊取用電腦的行為。這項規定的局限性太大。其實無論有否利用電訊，以任何方式(舉例來說，藉“偷來的密碼”)在未獲授權下取用電腦，都應屬違法。如果這個擴大的範圍獲得接納，我們便要考慮《電訊條例》是否仍是處理這項罪行的最佳工具。這個問題應在法律草擬階段解決。

(d) 接收、保留及處理／販賣明知是在未獲授權下取得的電腦資料數據的行為，應予禁止。這樣可堵塞目前第三者理論上可以購買“偷來”的電腦資料數據而不屬犯罪的漏洞。

(e) 出售、分發，以至提供電腦密碼或取用碼作非法用途，也應列為違法。這樣便可應付以下列舉的情況：心懷不滿或不誠實的僱員把執行職務時得知的密碼提供予未獲授權的人士；或“交易商”自各方取得這類密碼，然後售予他人作非法用途。由於分發密碼作完全合法用途的情況甚多，這項罪行應訂明違法者當時知悉：

- 所作的披露並未獲得授權；以及
- 密碼會被他本人或他人不當地用來圖利、作不法用途，或不當地用以使他人蒙受損失。

---

(8) 見第三章關於“電腦”的定義。

此外，密碼、取用碼和類似詞語的含意，應該清楚界定為可以直接使用、毋須再經處理即可取用電腦的資料。這樣可令定義不至過於廣泛，以免把要經過細意處理才可能間接地導致在未獲授權下取用電腦的程式或其他資料也涵蓋在內。(所謂“黑客入侵工具”的問題，會在下文第 6.23 段探討。)

6.20 非法取用電腦和取用電腦內的程式和資料數據，可能會造成嚴重損失。因此，我們在第二章第 2.7 段已指出，任何人違反現行《電訊條例》第 27A 條所指的黑客入侵罪行，應該判罰監禁。有人或會質疑，如果只為滿足好奇心或純粹因為“貪玩”而在未獲授權下取用電腦，是否也要判罰監禁？還是施行教育或處以象徵式罰款就已足夠？

6.21 我們絕對同意應在教育方面多加努力，勸止電腦用戶(特別是較年輕一代)不可在未獲授權下取用他人的電腦系統和資料數據。(請參閱第十章有關教育在防止電腦罪案方面的功能。)儘管如此，我們認為不應無意間為犯事者提供擋箭牌，或傳遞某些黑客入侵行為並不嚴重的錯誤信息。在未獲授權下取用他人的電腦程式或資料數據，至低限度已侵犯了他人將資料保密的權利。由於這項行為幾乎全都涉及蓄意干擾電腦的保安措施，所以絕少是無心之失。打個比喻來說，這並非偶然打開沒有鎖上的門，而是蓄意闖入門上了鎖和有保安系統的房子。此外，不管入侵黑客的用意為何，我們很難保證被取用的程式和資料數據完全未受感染。舉例說，它們很可能感染了黑客的電腦病毒。黑客入侵電腦的行為削弱了用戶的信心，阻礙電子商貿的發展。

6.22 在未獲授權下取用電腦資料數據可能造成的嚴重後果，眾所周知，故意不理這些後果至少也屬罔顧後果的行為。一如上文第 6.16 段所指出，這種行為在概念上可視為與盜竊類同。目前，盜竊罪行一經循公訴程序定罪，最多可判處監禁十年。表面看來，未獲授權下取用電腦程式和資料數據的罪行應處以不少於盜竊

罪的刑罰，才能發揮足夠的阻嚇作用。因此，我們*建議*相應提高這項罪行的最高刑罰。當然，每宗個案須按個別情況處理，只要有理可據，法院絕對有權判處較輕的刑罰。

(c) 黑客入侵工具

6.23 有人建議把生產、分發、售賣和使用黑客入侵工具(即可用來在未獲授權下取用電腦程式或資料數據的程式)，列作違法行為。工作小組曾考慮這項建議。不過，我們相信，很多所謂的黑客入侵工具其實也可以用於正當用途。舉例來說，系統管理人員可能利用這些工具來測試系統是否容易被入侵，從而加強保安措施。要確定黑客入侵工具甚麼時候是純粹用於非法入侵用途、甚麼時候是用於教育或其他正當用途，實在非常困難。因此，我們認為立法管制黑客入侵工具並不可行。我們*建議*不再研究這項建議。

(d) 整體資料的保護

6.24 在作出上述建議時，工作小組曾廣泛討論，我們會否在無意中以不一致的方式對待電腦資料數據和實體資料數據。我們承認，如果販賣在未獲授權下取用電腦而取得的資料屬於犯罪，但販賣通過另一途徑取得的同樣資料則不屬犯罪，便很可能出現不一致的情況。不過，經過審慎考慮後，我們相信電腦資料數據包含的一些特性，未必同樣適用於以其他媒體儲存的資料數據(請參閱第 6.14 段)。據我們所知，其他司法管轄區保護電腦資料數據的法例，通常也不會延伸至非電腦資料數據。目前，《電訊條例》訂定的在未獲授權下取用電腦資料數據的罪行，也是採用這個做法。

6.25 從工作小組的角度看，保護電腦資料數據這個問題值得優先處理，我們也就此提出相應的建議。至於應否及如何處理整體資料的保護問題，已超出了工作小組的職權範圍。儘管如此，我們仍想指出，如果出現不一致的情況，應要進行研究及作出適當糾正。

第七章

“欺騙”電腦

引言

7.1 根據普通法的原則，一台機器不可能受到欺騙。鑑於電腦也是機器的一種，我們有需要探討這項原則對電腦罪案有何影響。

目前情況

7.2 就法律而言，一台機器(包括電腦在內)不可能受到欺騙。欺騙罪必須有人受騙才能成立。不過，現今的電腦的確可以“作出決定”，例如電腦可以依照預設程式接受網上購物訂單。故此，上述的普通法原則帶出了一個問題，就是能否對經互聯網提供虛假資料(包括偷來的密碼和信用卡資料)以從受害人獲取貨品、服務和信貸的人提出檢控。這普通法原則仍未經香港法庭考驗。

7.3 利用電腦行騙的行為，已載列於現行《刑事罪行條例》(第 200 章)第 161 條訂明的有犯罪或不誠實意圖而取用電腦的罪行之中。該條的內容如下：

> *“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,可處監禁五年。"

事實上,第 161(1)(b)條自制訂以來從未引用過。反之,在解決該項普通法原則所導致的潛在問題時,曾經引用(c)及(d)款。根據該兩款條文,任何人如取用電腦以向另一方提供虛假資料,藉以使他本人或他人獲益、或導致他人蒙受損失,罪行即告成立。因此,根本毋須證明有關的機器(即電腦)曾受欺騙。

其他司法管轄區的例子

7.4 按照英國的盜竊罪法例,必須有人受騙才可以使欺騙罪成立,因此,這裏存在一個法律漏洞。英國法律委員會曾再三考慮是否有需要堵塞這個漏洞。委員會認為,雖然有理據支持修訂法例來堵塞漏洞,但這個漏洞並不嚴重,因為不誠實地利用機器犯罪的案件往往涉及其他罪行,例如盜竊、製造虛假文書、偽造帳目等。任何人利用電腦並提供他人的信用卡資料以獲取財產,即屬犯了盜竊罪。購買物品的款項稍後會在信用卡持有人的帳戶中扣除,該項扣除便構成一宗盜竊信用卡發卡機構與顧客之間據法權產的罪行。該委員會在一九九九年一份關於詐騙及欺騙罪行的諮詢文件中,初步認為"欺騙"機器應按盜竊案而非欺騙案處理。

7.5 據工作小組所知,美國阿拉斯加州是唯一一處地方通過訂立法例,明文否定上述普通法原則可作為抗辯理由。《阿拉斯加法例》第 11 項《刑事法》第 6 章針對財產的罪行的條文訂明:

"在根據本章提出有關包含'欺騙'成分的罪行的檢控中,辯方不得以欺騙或意圖欺騙的對象是機器作為抗辯理由。就本條而言,'機器'一詞包括售賣機、電腦、入場機或自動櫃員機。"

考慮因素

7.6 正如上文第 7.3 段所指出，機器不可能受騙這項普通法原則可能引致的問題，可以利用第 161 條第(1)(c)和(d)款來解決。我們也知悉，《刑事罪行條例》第 161 條制訂以來，該條第(1)(b)款從未被引用。因此，就電腦罪案而言，工作小組相信該項普通法原則至今還沒引起過棘手問題。

7.7 雖然第 161(1)(b)條從未被引用，但我們認為該條仍有用處。舉例來說，如取用電腦的目的，是要欺騙負責處理從該電腦所得資料的人，而取用是否引致獲益或損失又難以證實，則可引用該條。不過，基於該項普通法原則，若人們就所得資料應如何處理編入預設程式內，而處理資料的過程本身又不經人手，則該條並不適用。因此，工作小組曾考慮應否修訂該條，訂明欺騙的對象可以是人或是機器。

7.8 一方面，隨着技術發展，電腦可藉設定程式執行很多以往由人負責的工作，由電腦“作出”決定的情況愈來愈多。概念上，電腦由於能夠執行人的指令，因此也應可被“欺騙”。有見及此，堅守只有人才可被欺騙這項原則，似乎限制過大。

7.9 另一方面，鑑於《刑事罪行條例》第 161(1)條的條文，該項普通法原則造成的漏洞僅屬輕微。實際上，我們並未遇到任何不能藉該條(c)或(d)段處理的重大“欺騙”電腦案件。因此，***就電腦而言***，工作小組認為現行法例已足以涵蓋“欺騙”電腦而非人類的案件。

7.10 儘管如此，如果我們把目光放於電腦以外，而欺騙行為涉及的是服務而非貨物或財產，則的確存在“欺騙”機器的問題。。舉例來說，如有人不付所需費用而“欺騙”投幣擦鞋機替自己擦鞋，他並不屬違法，因為目前並無類似《刑事罪行條例》第 161(1)(c)和(d)條的法例用以規管所有的機器。工作小組雖然明白此事超出了我們的職權範圍，但也***建議***當局應考慮審慎

研究此事和修補這個漏洞。這個問題至少有兩個處理方法。一是涵蓋所有的機器。舉例來說，我們可以規定機器可被欺騙，或明文規定不得以欺騙對象為機器作為抗辯理由。另一個處理方法是像現時處理停車收費錶一般，列明某些機器如有人濫用和欺騙，即屬違法。我們建議，這個議題適宜由法律改革委員會等機構，在研究整體的詐騙和盜竊法例時加以探討。

7.11 如上文所示，我們關注網上行騙案和實際行騙案的處理方法是否一致。基於同一關注，我們認為有需要檢討懷有犯罪或不誠實意圖取用電腦這項罪行(《刑事罪行條例》第 161(1)(b)、(c)和(d)條)中有關欺騙和不誠實意圖部分的現行刑罰是否足夠。(第 161(1)(a)條的刑罰已在第四章另行討論。)這類罪行目前的最高刑罰是監禁五年。不過，我們注意到《盜竊罪條例》中涉及行騙罪的最高刑罰為監禁十至 14 年。鑑於透過電腦或互聯網行騙造成的破壞不會少於實際行騙案造成的破壞，我們***建議***，懷有犯罪或不誠實意圖取用電腦這項罪行中有關欺騙和不誠實意圖部分的最高刑罰，原則上不應輕於《盜竊罪條例》中類似性質罪行的最高刑罰，即至少監禁十年。正如第六章所指出，法庭絕對有權在法律訂明的最高刑罰之內，判處較輕的刑罰，但我們不應給予公眾錯誤印象，令人以為透過電腦行騙，其嚴重性較以其他方式行騙輕微。

第八章

互聯網服務供應商提供的協助

引言

8.1 很多電腦罪案都是透過互聯網進行，因此，我們應研究互聯網服務供應商(互網商)應否及如何協助打擊或防止電腦罪案。下文探討各項有關事宜。

背景

8.2 在調查牽涉互聯網的罪行時，客戶的帳戶記錄和上網時段記錄都是有用的資料。帳戶記錄提供帳戶持有人的身分資料，包括用戶姓名、身分證明文件內容、聯絡方法及付款方法。上網時段記錄則提供有關互聯網交易的細節，主要包括進入和退出系統的時間，以及獲編配的網絡協定地址(請參閱第 8.3 段)。在某些情況下，用戶曾經取覽的網頁地址、電郵地址和上網的來電號碼(如有來電顯示功能)也會記錄下來。因此，上網時段記錄可以用來找出某項互聯網交易源自哪個用戶，如具備來電者辨別功能，更可找出該項交易源自哪個地點。

8.3 追尋電腦罪犯的一項重要線索，是其帳戶獲編配的網絡協定地址。在撥號上網系統中，每次有人進入系統上網時，互網商便會給他編配一個地址碼。該人退出系統後，該地址碼便會重新編配給其他人。要確定某一地址碼在某段時間編配給什麼人，唯一方法是查閱互網商的運作記錄(如有的話)。租用專線的帳戶則獲編配固定的網絡協定地址。

目前情況

8.4 當局目前並無規定持牌互網商(截至二零零零年七月底，互網商約有 200 間)必須保留運作記錄。不過，我

們知悉互網商現行確有保存撥號上網帳戶的運作記錄，但保存期則長短不一。根據香港互聯網供應商協會對某些互網商進行的非正式調查所得，記錄的保存期由一個月至三年不等。此外，主要的互網商(它們的總市場佔有率超逾八成)往往保存運作記錄達六個月或更長時間。保留運作記錄，主要是為發單收費之用。互網商保存運作記錄的期限，主要視乎其電腦系統的容量而定。由於租用專線的帳戶是以定額方式而非按進入系統時間的長短支付服務費用，互網商不會保存這類帳戶的運作記錄。此外，互網商保存作記帳用途的用戶資料，亦各有不同。

8.5 除商營互網商外，大學也會提供上網服務，但這項設施只限其教職員及學生使用。據我們了解，儘管這項服務是免費的，但大學的電腦系統仍保留用戶的運作記錄，理由如下：

- 保安：進行監察，以防外人非法進入系統；
- 內部審計：進行監察，以防系統被人濫用；以及
- 研究與發展：找出資源分配的先後次序，較受歡迎的網站可能獲分配較多資源。

關注問題

8.6 每個互網商都有自己保存記錄的方法。有些記錄會在發單收費程序完成不久後銷毀，從協助執法的角度來看，保存期可能並不夠長。互網商保存的資料亦各有不同。此外，國際上，互網商免費提供上網服務已漸趨普遍。這樣一來，互網商為發單收費而保存運作記錄的需要便會日益減少。執法機關當然希望互網商不但繼續保存足夠的上網時段和帳戶記錄，而且還把資料最低限度保存一段時間，例如六個月。除運作記錄外，執法機關亦建議保存來電號碼。電腦罪行調查人員希望互網商保存的記錄種類，載於附件 6 的建議清單。

8.7 另外，有人建議互網商迅速移除涉嫌違法的網站，以協助打擊或防止電腦罪行，亦有人建議互網商禁止多重登入，以減低帳戶在未獲授權下被人盜用的可能。另一項建議是為互聯網上使用信用卡付款的交易設定信用限額，從而減低遇到網上購物騙案時的損失。

其他司法管轄區的例子

8.8 一九九九年九月，歐洲委員會的資料數據保護工作小組(工作小組)就互網商保存通訊資料數據以助執法提出建議。工作小組強調保護個人資料的私隱，因此着眼於互網商應保存客戶記錄的最長而非最短期限。工作小組建議歐洲委員會提出適當措施，劃一電訊營運商和互網商可保存通訊資料數據的期限。有關期限必須足以讓顧客就帳單提出質詢。但除此以外則必須盡量縮短，以免令營運商和互網商的負擔過重。

8.9 二零零零年四月，歐洲議會公布了《網上罪行公約》的初稿讓公眾討論(請參閱第十四章第 14.2 段)。該公約草案涵蓋的其中一個範疇，是規定成員國透過立法或其他措施，強制要求某人保存某次通訊的資料數據以協助刑事調查。這項規定若果實施，只會適用於特定的要求，而不會作為要求互網商保存所有記錄的一般規定。

8.10 二零零零年三月，美國總統指派的互聯網非法行為工作小組(小組)發表報告書，指出有部分互聯網業者保存某些系統資料數據的期限過短，不足以讓執法機關找到網上罪犯。不過，小組不贊成實施強制要求保存資料數據的規定，反而建議業界在考慮市場需要、消費者私隱的保障和公眾安全等因素後，評估保存資料數據的成本效益。小組建議業界應充分考慮，保存某些有助拘捕違法者的資料對業界本身及社會可帶來的好處。

8.11 二零零零年五月在巴黎舉行的八大工業國(G8)會議，討論了強制要求互網商保存客戶記錄的建議。這項建議

受到互網商的代表強烈反對，他們指嚴格的規管會令業界承擔額外成本，並窒礙電子商貿的發展。

8.12 至於互網商其他形式的合作，一九九八年通過的《美國數碼千禧年版權令》訂明聯機服務供應商須遵守的通知和移除程序，藉以打擊侵犯版權的物品。版權擁有人如相信某網站載有濫用其版權的物品，可通知有關的聯機服務供應商。聯機服務供應商在接到通知或自行發現有侵犯版權的情況後，必須盡快移除有關材料或阻止公眾取覽該網站。如聯機服務供應商出於真誠遵守有關法例規定，法律便會豁免其向用戶和第三者須負的法律責任。如用戶提出正式的“反對通知”，證明他合法使用有關材料，則聯機服務供應商必須迅速通知版權擁有人，並於 14 個營業日內復載有關材料，除非該事件已轉交法庭處理。

考慮因素

(I) 互網商保存的記錄

8.13 調查網上罪案時，通訊資料數據和用戶詳情肯定是重要的工具。互網商目前採用的保存記錄方法雖然各有不同，但他們都會為本身的需要保存帳戶記錄和上網時段記錄。各執法機關可以根據規管其機關運作的法例，獲取記錄作調查之用。在有需要時，執法機關可以向法庭申請搜查令。如果記錄包含個人資料，它們可以依據《個人資料(私隱)條例》(第 486 章)第 58 條獲得豁免。直至目前為止，執法機關在有需要時取用資料方面，並未遇到無法解決的問題。雖然如此，我們也曾考慮是否需要改善現有的安排，以及一些改善建議是否切實可行。

(a) 用戶資料

8.14 目前，互網商用不同的方法核實準用戶的個人資料，例如記下用戶身分證明文件的詳情和覆核其住址證明(例如要求出示公用服務公司的收費帳單)。不過，在我們與一些互網商舉行非正式討論時，有意見認為，如

果法律明文規定他們必須保留用戶身分證明文件的影印本，將有助他們核實用戶的身分。

8.15 我們知悉，私隱專員公署已發出了《*身分證號碼及其他身分代號實務守則*》，該守則訂明在什麼情況下可以保存他人的身分證副本。我們相信該守則已可為各有關人等，包括互網商，提供處理個人資料時須遵從的指引。此外，如有需要和理由，互網商在查核資料時，可以記下準用戶的身分證詳情。因此，在現有安排之外再以法例規定互網商須保存用戶身分證的影印本，看來不會有多大效用。

8.16 有人可能指出，互網商或會因恐防準用戶轉投其競爭對手而不積極查核用戶的資料，立法規定則可以防止這個情況出現。不過，要處理這個問題，較佳的治本方法是一開始便審慎查核用戶的資料。互網商如不堅守一些基本的良好管理措施，不僅其收入及聲譽可能受影響，其系統及／或用戶系統的保安也可能受損。立法規管一些可以藉行政措施解決的問題，似乎不是恰當的做法。不過，我們*建議*，執法機關應與互網商的代表合作制訂一套行政指引，訂明用戶新開戶口時應查核的資料類別，以及在戶口有效期間和在戶口結束後一段合理時間內須保存的資料。這套指引應符合《個人資料(私隱)條例》的規定。

(b) 來電者號碼

8.17 工作小組曾深入探討，應否藉法例規定互網商記錄所有網上交易的來電者識別資料。很多電腦罪案的犯事者都是盜用他人戶口上網，因此，僅能顯示哪個戶口獲編配涉及電腦罪案的網絡協定位址的運作記錄，並無多大幫助。反之，如來電者號碼屬於一條固定的電話線，能提供來電者號碼的記錄便能顯示某項互聯網信息或指令的實際發出位置。因此，這些記錄對追查涉及電腦罪案的過往事件來說，是十分寶貴的線索。

8.18 另一方面，工作小組也知道這項建議並非全無問題。首先是成本的問題。裝置來電者身分顯示設施，每條

線的成本估計為每月約 25 元[9]，而互網商擁有的電話線，往往有數百至數千條。此外，儲存獲取的資料也需額外的成本。這些成本相信最終會轉嫁消費者身上。在與我們非正式磋商時，部分互網商的代表指出，來電者號碼並非他們營業所需的資料；如果純粹為協助執法而施行這項規定，則應考慮由政府負擔有關開支。我們不能單看表面就接納這個論點，因為以此推論，將意味政府必須支付所有因守法而需付的費用。我們留意到有一些司法管轄區，例如澳洲和英國，確實有授權政府為通訊機構和服務供應商訂定最低限度的技術標準，並在符合一定條件下分擔部分費用。不過，這是為了在必須行使某些調查權力時確保有足夠的技術能力，而非規定保留所有交易的來電號碼。據我們所知，沒有一個已發展國家把後者定為一項法定要求。

8.19 另一更值得關注的事項涉及建議的成效問題。如果來電者在進入系統前先撥“133”，則來電號碼顯示功能便會失效。我們也曾考慮，要求互網商拒絕向無法記錄其號碼的來電者提供服務。不過，如互網商把系統如此設定，會出現以下問題。

- 來電號碼顯示功能只能顯示本地來電的號碼。外遊的用戶因此便無法通過長途電話接通香港的互網商以使用其服務。

- 來電號碼顯示功能未必能夠顯示通過專用電話交換機系統來電的號碼，這類用戶可能無法使用互網商的服務。

8.20 工作小組曾研究一個類似的建議，就是由固定線路電話公司而非互網商保存來電線路識別資料數據。利用來電線路識別功能，即使來電者撥了“133”，也可被追尋得到。我們從主要的固定線路電話公司得知，目前來電線路識別功能只用來記錄海外來電的情況，以便發單收費。如果要保存所有來電的線路識別資料數

(9) 這是主要的固定線路電話公司在獲得電訊管理局批准後徵收的收費。

據，由於每日須保存的記錄為數極多，成本將會十分高昂。此外，我們也不肯定這個辦法在技術上是否可行。電話撥號帳戶的用戶需致電互網商才可接通互聯網，而互網商的系統會編配一個網絡協定位址給用戶。我們事後能否把網絡協定位址與來電者身分配合起來，實成疑問。

8.21 除了成本的考慮因素外，來電線路識別功能也非萬無一失。如用戶使用預先繳費的手機組別記認卡，或通過專用電話交換機系統或電腦咖啡室等致電，便可避過來電線路識別功能的偵測。此外，如互聯網交易涉及海外的互網商，則除非該海外互網商亦記錄了來電者的身分，否則來電線路識別功能的作用不大。正如上文第 8.18 段所述，工作小組沒有發現有任何司法管轄區要求其互網商保存所有互聯網交易的來電者身分記錄。

8.22 因此，在衡量各方面的情況後，我們*建議*維持現行的做法，就是在有需要時，才追查懷疑涉及電腦罪案的指定帳戶的交易。此外，當局應鼓勵互網商保存運作記錄(包括來電號碼)，作為良好的管理常規。不過，有關強制要求使用來電號碼顯示功能或來電線路識別功能追查所有互聯網交易的建議，在現階段暫不實行。目前，我們應研究是否有適當辦法解決上文提及的問題和規避偵測方法，並就調查工作因缺乏來電號碼顯示或來電線路識別功能而受影響的案件，蒐集資料。

(c) 數碼匙

8.23 有人曾經建議，要求互網商的所有用戶向一個公開密碼匙基礎建設(公匙基建)[10]核證機構登記及領取密碼匙。這個安排可以防止不法之徒假冒他人非法進入互網商的系統，有助提供可靠的線索，有利於電腦罪案的調查。不過，這項安排會令訪港旅客因沒有所需的密碼匙而無法使用互網商的服務，而且也不能配合世

(10)公開密碼匙基礎建設屬一種資訊保安安排，好處是令電子交易的一方可以利用數碼證書和核證機構提供的服務來確認交易對方的身分，確保傳送的資料可靠和保密，以及避免對方藉詞拒絕履行交易。

界各地互網商提供的國際漫遊服務。基於以上各點，我們*建議*，政府和互網商應鼓勵互聯網使用者利用公匙基建來加強保安，但不應強制執行。

(d) 運作記錄

8.24 目前，互網商須向固定線路電話公司繳付公共非專利電訊服務收費[11]。一般來說，互網商把使用網絡的費用轉嫁其用戶，而公共專利電訊服務的收費會在顧客的帳單內分開列明。只要繼續有這項收費，互網商便要保存撥號上網戶口的運作記錄，以便向用戶發單收費。我們不肯定電訊管理局會否在不久將來改變這項收費機制，但即使機制改變，相信互網商仍須保存某類運作記錄以供審計之用，因為屆時互網商的主要收入將來自廣告贊助商，而後者需要知道互網商服務的使用情況。因此，預料在未來的好一段日子，互網商保存的運作記錄，最低限度仍可顯示登入及退出時間和編配的網絡協定地址。我們*建議*當局促請互網商將這些記錄保留一段合理時間，例如六個月。

(e) 總結

8.25 如果參考外國的經驗，強制要求互網商備存記錄似屬相當少有，指定備存記錄的種類和保存期限，就更加罕見。根據法律意見，當局必須引入新的法例，才可強制要求互網商保存執法機關所需的記錄。不過，此舉會涉及不少資料數據私隱和其他法律問題。

8.26 考慮到互網商現行的慣常做法、業界的合作態度、遵循規定所涉及的社會和財政成本、外國在這方面缺乏經驗，以及法律上的問題，我們認為現階段不宜強制要求互網商保存記錄。反之，我們*建議*當局制訂保存記錄的行政指引讓互網商遵從，好讓互網商向執法機關提供適當的協助。指引的內容除了涵蓋用戶資料、

(11) 公共非專利電訊服務收費是增值服務供應商(包括互網商)繳付給本地固定線路電話公司的一項接駁費，用來支付增值服務供應商的客戶以撥號上網方式透過固定網絡連接至服務供應商設施的開支。主要固定線路電話公司收取的公共非專利電訊服務收費的水平，由電訊管理局釐定。

來電號碼和運作記錄等事宜(上文第 8.14 至 8.24 段)外，還可訂明步驟，劃一執法機關目前索取資料的慣常做法。如此的話，互網商將可以更快對有關要求作出回應。我們又*建議*，制訂指引時應徵詢互網商代表的意見。

8.27 這些指引制訂之後，我們*建議*當局進行適當的宣傳，尤其是鼓勵互網商提供一份聲明或核對清單，以顯示其遵守指引的程度。當局也應鼓勵消費者選擇那些採納了載列在指引中的良好管理方法的互網商。

(II)其他事宜

(a) 移除程序

8.28 我們認為，互網商與其他內容供應商一樣，應對所提供的內容負責。不過，作為一個承載機構，互網商原則上毋須對純粹經由它們承載的內容或網站的內容負責。

8.29 目前，互網商在知悉某涉嫌違法的網站正被執法機關調查後，可能會把該網站移除。嚴格來說，互網商在網站證實違法之前把它移除，可能要負上民事責任，但這要視乎個別互網商的服務條件而定。鑑於法律訴訟可能要一段時間才能完結，為免涉嫌違法的網站繼續傳播有關資訊，盡快移除有關網站應有好處。工作小組認為，應該研究是否採取與《美國數碼千禧年版權令》(上文第 8.12 段)相似的做法，進一步澄清互網商在這些情況下的法律責任。

8.30 我們認為，從表面來看，制訂移除程序會使互網商有更穩固的法理基礎移除網上懷疑違法的材料和網站，因此原則上應該支持。要達到這個目的，有兩個方法可供選擇。就第一個方法而言，由於我們關注的，主要是透過互聯網傳送侵犯版權物品、非法賭博活動和色情物品的問題，因此，透過有關保護版權、網上賭博活動及管制色情物品的政策處理這些問題，或許已經足夠。我們留意到，在*“保護青少年免受淫褻及不*

雅物品荼毒：二零零零年檢討《淫褻及不雅物品管制條例》”諮詢文件中，其實已經採取類似的做法。至於第二個方法，就是考慮制訂一般性的賦權條文，授權互網商在接獲當局通知正對某些涉嫌違法的材料進行刑事調查後，可以移除該等物品。這個方法固然會較全面，但可能令人覺得涉及的範圍過廣。這項權力如果不限定適用於某幾類指明的罪行，便可能被濫用，甚至令人憂慮當局藉此進行審查。工作小組考慮各方面的情況後，認為第一個選擇較為可取，並*建議*有關決策局研究是否可以在保護版權、管制網上賭博及色情物品等方面，加入移除涉嫌違法材料或網站的程序。

(b) 多重登入

8.31 目前，不少互網商都將系統設定為容許用戶多重登入，即多名使用者可在同一時間利用同一個撥號帳戶上網。對帳戶持有人來說，這項設定有一些好處，例如只須支付一個帳戶的費用，便可讓自己和同伴在不同時間或同時上網。不過，當某帳戶被人在未獲授權下取用來上網時，由於該帳戶的持有人仍然可以在同一時間使用同一帳戶上網，他便會無法即時察覺。雖然多重登入設施可以為部分用戶帶來一些方便，但對廣大用戶來說，這項設施並無用處，他們甚至根本不知道有此設施存在。鑑於這項設施有一定的保安風險，我們*建議*促請互網商把系統預設為拒絕多重登入，而只將這項設施作為一個用戶選項，在選擇後才可使用。

(c) 信用額

8.32 工作小組認為，信用額的多寡，主要是持卡人與發卡銀行之間的事情。近日的發展顯示，信用卡行業其實已開始發展供網上購物用的新產品。舉例來說，部分主要銀行已提供信用額遠較正常低的信用卡帳戶，以供互聯網交易之用。這樣，即使持卡人的信用卡資料被人盜用以在互聯網上進行詐騙，持卡人也可以減少損失。網上交易採用毋須輸入信用卡資料的聰明卡，

亦日趨流行。如何處理網上購物信用額的問題，應繼續由市場作主導。因此，我們認為這個問題毋須透過法例處理。

(III) 互網商的回應和合作

8.33 正當的互聯網用戶應可期望在一個安全的環境下進行網上交易。因此，互網商和執法機關都應以此作為共同目標。在某些情況下，互網商本身也是電腦罪案的受害者。因此，互網商協助打擊或預防電腦罪行，對其本身也有好處。當有關建議涉及互網商在本港以至全球的經營環境時，互網商的回應對評估這些建議尤其重要。為了加強執法機關與互網商的溝通，以及鼓勵雙方就網上保安問題交流意見，我們*建議*：

(a) 設立交流意見的渠道，讓互網商和執法機關定期會面，商討共同關注的問題。這個機制應該用來處理一些宏觀的問題，例如可以先着手擬定第8.26段建議的行政指引；以及

(b) 設立聯絡人制度，以處理調查個別電腦罪案的要求。每家互網商和每個執法機關都應該為此設定聯絡人。這些聯絡人都應該熟悉調查涉及互網商的電腦罪案的程序。這個制度可讓聯絡人更恰當地編排個別要求的緩急次序，和促進雙方溝通。它可以作為上文(a)段建議的溝通渠道的一個環節。

第九章

保護重要基本設施

引言

9.1 本章旨在研究與本港重要基本設施有關的電腦保安及執法問題，並評估是否有需要加強防護措施，以配合資訊時代的發展。

目前情況

9.2 每個社會都有若干重要的基本設施，其服務對經濟和政府的暢順運作至為重要。這些設施如果受到重大破壞或損害，便會嚴重影響社會多個部分的運作甚至穩定。重要基本設施的例子，包括電力供應系統、食水供應系統、公共交通網絡、通訊網絡、主要公眾衞生系統和國防系統。

9.3 目前，我們並沒有一份有關香港重要基本設施的確切名單。不過，各間公用事業公司、公共交通工具營辦者(例如地下鐵路)及通訊網絡營辦者，都採取了各種保安措施，防止它們的物業或設施受到襲擊。警方負責收集、整理及發布這方面的情報，並與基本設施營辦者合作應付保安事故。

9.4 在緊急事故或災難方面，香港設有一個三級制的緊急應變系統(應變系統)，應付各類威脅市民生命財產或公眾安全的緊急事故。除了天災之外，應變系統還適用於影響我們日常生活的主要系統因失靈而引致的事故。至於要採取哪一級的應變措施，須視乎緊急事故的嚴重程度而定。對於較輕微的緊急事故，採取第一級應變措施，即由救援部門完全在本身所屬指揮單位的統籌下採取行動，或許已經足夠。這是如常運作的情況，政府部門各自按所訂的例行程序採取行動。如果發生重大事故，以致對市民生命財產及社會安穩構

成重大威脅，需要政府全面展開救援工作，便會採取第三級應變措施。在此情況下，緊急事故監察及支援中心會投入運作，在中央層面統籌個別指揮單位採取緊急應變行動。如有需要，監察水平和人員編制比例也會按情況提升。

9.5 到目前為止，重要基本設施的保安問題，仍然主要針對實質方面的保安。一向以來，我們保護這些設施的方針，都着重預防或應付個別設施的實質攻擊(外圍防護)。但是，隨着電腦科技迅速發展，以及社會日漸倚賴互聯網作通訊、商業、研究及消閑用途，我們在評估重要基本設施的保安方面也加添了新的考慮。這些基本設施在網上世界究竟有多安全？透過互聯網及電話線互相連接促進交流的環境，會否讓罪犯或恐怖分子有機會侵佔機密檔案、展開資訊戰爭、或破壞某項重要基本設施的運作？總括來說，在這個無疆界的網上世界裏，我們是否要更加留意基本設施互相依存的情況？

9.6 在其他司法管轄區，曾經發生罪犯和恐怖分子利用資訊科技侵入或破壞重要基本設施的例子。例如在一九八六至八九年間，一羣西德黑客從美國和日本多部軍方及工業電腦竊取密碼和資料，然後轉售給蘇聯國家安全委員會(特務機關)。外國政府部門、機構或公用事業公司的伺服器或網頁被黑客入侵，或受到其他破壞(例如令致服務癱瘓的攻擊)，此等例子不勝枚舉。理論上來說，不論在何處，只要有一部電腦、一具數據機和一條電話線，便有可能關閉機場的航空交通控制系統，破壞整個社區的緊急服務系統，甚至啟動導彈系統，只要這些系統是直接或間接地接上互聯網或電話線。

9.7 目前，人們對這些新問題已有一定程度的認識。在香港，資訊科技署負責統籌確保政府電腦網絡的安全。但大部分的重要基本設施並非由政府營運。至於應變系統方面，它基本上是一個應急機制，專門應付突發的嚴重災難。我們要研究香港現有的保護措施是否足以應付新的問題。在這個資訊時代，要保護重要的基

本設施，我們需要更迅速的應變、更緊密的協調、更頻密的檢討和更新保護和應變計劃。傳統以來針對個別事故及裝置／設施較被動的應變方法，或須加以補充改善。

其他司法管轄區的例子

(a) 重要基本設施的保護

9.8 有關這個問題的文獻，大多集中討論美國方面的經驗。美國在一九九八年公布的保護重要基本設施政策，主要特點如下：

- 制訂一個經過協調的國家基本設施保障計劃，涵蓋公營和私營機構各個界別；
- 設立一所國家中心，為重要的基本設施評估威脅，發出警告，執行法例和作出應變；
- 建立一個國家單位，協助推行國民教育和宣傳計劃，並統籌立法和公共事務；以及
- 鼓勵私營機構設立聯絡中心，促進國家中心與業界交流保安資訊。

有關政策的實施詳情載於附件 7。

9.9 首份美國國家保護資訊系統計劃書在二零零零年一月發表。計劃書包括 10 項計劃，目的是要達到三個主要目標，即“準備及預防”、“偵查及應變”和“建立穩固基礎”。這些計劃包括：

- 確定重要的基本設施資產和它們互相依存的程度，以及應付設施可能受襲擊的問題。
- 偵查襲擊和未獲授權的侵入行為。

- 發展強大的情報收集和執法能力，以保護重要的資訊系統。
- 及時交流襲擊警告及有關資料。
- 發展應變、重建及復原的能力。
- 加強研究及發展工作，以支援有關計劃。
- 訓練及聘用足夠的資訊保安專家。
- 大力宣傳，提高人們改善網上保安的意識。
- 通過法例和撥款，以支援有關計劃。
- 計劃書的各個步驟和環節，都應確保公民自由、私隱權和保障專利資料數據的權利得到充分保障。

(b) 緊急應變

9.10 根據美國的模式，緊急應變是整個重要基本設施保護計劃中不可或缺的部分。不過，在其他經濟體系中，也有例子是電腦緊急應變小組(應變小組)以獨立形式運作，與較大型的重要基本設施保護計劃並無直接聯繫。應變小組的特定功能因司法管轄區而異，但它們的主要功能一般包括蒐集、整理和公布有關黑客入侵及電腦病毒對電腦網絡構成威脅的資訊和警告。其他附屬功能包括教育市民認識電腦保安問題和防止破壞電腦保安。此外，有些應變小組還提供增值服務，為個別電腦系統解決問題。附件 8 列出一些海外應變小組的功能詳情。

考慮因素

(a) 資訊保安／保證的需要

9.11 對於在日常運作中需要應用資訊科技的機構來說，確保資訊系統以及資訊本身安全的工作，應是機構策略的一個重要環節。高水平的資訊保安或保證有助機構有效和圓滿地達到目標。相反，鬆懈的資訊保安可能會令機構的信譽，利潤和生產力等蒙受重大損失，不只威脅到機構的生存，還會影響其他與機構有來往人士的利益。舉例來說，一間公司如屢次遭受襲擊以致服務癱瘓，則其在維繫客戶、供應商和債權人信心方面的能力，便會削弱。公共醫療系統的病人資料數據如被搗亂，便要先進行大規模的重新檢查和測試，然後才可施手術或配給藥物。在未獲授權下披露刑事罪案調查情報以至商業洽談等機密資料，不僅會令被取用資料的受害人利益受損，還會令其他有關人士受害。

9.12 資訊保安或保證包括以下三個基本部分：

- 獲授權人士取用資料的可靠性 — 使用者經核實和確認身分後，可在有需要時取用服務和資料；
- 資料的完整性 — 資料數據不會受到干擾；以及
- 機密性 — 資料只供獲授權人士取用。

經上述分析後，可以清楚看到，資訊保安的主要決定因素在於用戶機構本身。有關機構應備有確保資訊安全的政策，這點相當重要。制訂政策時必須顧及機構本身的需要，而且要有必需的資源(人力、技術器材和軟件)及程序支援。除了確保本身的資訊安全之外，政府在這方面主要是負起促進和推廣的責任，並提供所需的規管以處理違法事宜。政府也致力推動資訊基本設施的發展，包括公匙基建。此外，政府透過教育工作(請參閱第十章)，提高市民對這些事項的認識。不

過，在確保機構的資訊安全方面，政府不應也不能取代社會上各大小機構管理層在這方面的重要責任。

(b) 保護重要基本設施

9.13 上文第 9.11 和 9.12 段提及的考慮因素，很多都適用於本港的重要基本設施。確保這些設施的資訊安全，是各有關設施營辦者的責任。不過，鑑於這些設施對整體社會有特別的重要性，政府有理由要確保這些設施的資訊保安計劃能夠趕得上不斷改變的情況。因此，工作小組就保護重要基本設施的問題，進行了探討。

9.14 原則上，本港的重要基本設施應該作好準備，以便同樣有效地應付實質攻擊及虛擬或網上的侵襲。事實上，隨着科技發展，不同系統之間互相依存(不一定是互相連接)的情況愈來愈普遍。舉例來說，電力供應全面故障一段長時間，便會嚴重影響供水和交通運輸系統，而影響程度也較從前，例如數十年前，嚴重得多。

9.15 本港重要基本設施現有的保護及應變計劃，或許基本上已足以應付可能發生的網上侵襲或電腦破壞，又或者只須對計劃稍作修改即可達到要求，這個可能性在現階段不能否定。不過，據工作小組所知，並未有就這個問題進行過任何整體評估。此外，即使個別設施已制訂保護及應變計劃，但各項計劃之間欠缺協調，很可能出現脆弱環節或配合欠佳等問題。

9.16 由此可見，及早確定目前情況和找出脆弱之處非常重要。根據美國的經驗，這項工作顯然超出了工作小組的能力範圍[12]。因此，我們*建議*的第一步，是為此目的進行一次徹底的評估，包括：

- 找出須進行研究的基本設施；

---

(12) 美國總統設立的保護重要基本設施委員會由約 20 名委員和超過 60 名輔助人員組成，並用了 16 個月時間完成報告書。

- 確定這些設施是否已就有關裝置／設施／系統制訂保護、應變及復原計劃，以防系統個別地(指獨立的系統)或集體地(指互相依存或聯網的系統)遭受網上侵襲；

- 進行威脅／脆弱程度評估；以及

- 根據上項的評估結果衡量上述計劃是否足夠。

9.17 我們雖然無意過早對初步評估的結果作出判斷，但相信所得結果很可能顯示我們目前的準備工作不足。即使個別計劃本身策劃周全，但在宏觀的層面卻欠缺協調。鑑於重要的基本設施高度互相依存，這點本身已是一脆弱的環節。此外，基本設施如按商業原則經營，營辦商往往只注重賺取利潤和維持競爭優勢，對防範網上侵襲的保護措施可能並不那麼經常重視。有見及此，我們*建議*設立一個常設機制，以統籌和協調有關保護、應變及復原計劃的擬定，以保障各項重要基本設施免受涉及電腦及互聯網方面的安全威脅。我們必須參照現行機制配合欠佳或不足之處，再深入研究中央機制的合適組織架構。不過，我們的整體原則是，該機制的運作必須與現行應付大型緊急事故的保護、應變及復原機制配合，並盡量利用現有的專業知識。應付網上侵襲和實質攻擊兩方面的工作很可能要同時進行，並應合併處理。舉例來說，政府定期進行跨部門演習以測試緊急應變系統能否有效和迅速地應付緊急事故。這些演習應加入模擬本港重要基本設施遭受網上侵襲的情況，以測試及加強我們所做的預備工作。

9.18 為保障重要基本設施免受網上侵襲，工作小組*建議*上述常設中央統籌機制應具備下列主要職能或目標：

- 確定和定期檢討重要基本設施的名單；

- 確保個別重要基本設施的營辦者會評估其設施遭受網上侵襲的威脅和脆弱程度；

- 統籌評估各個互相依存的重要基本設施遭受網上侵襲的威脅和脆弱程度；

- 確保個別重要基本設施的營辦者，會擬備並定期更新其設施的保護、應變和復原計劃，以應付可能針對其個別設施的網上侵襲；

- 統籌各個互相依存的重要基本設施，確保它們會擬備和定期更新為應付網上侵襲而設的保障、應變和復原計劃；以及

- 發生網上侵襲引致的事故時，統籌或參與統籌緊急應變工作。

這個機制的重點，是使整體的統籌工作做得更好，而不是要加設另一重官僚架構。因應千年蟲問題而做的統籌工作，是一個可以借鏡的例子。

9.19 這個中央機制當然要得到公營及私營重要基本設施營運者的緊密合作。此外，這個機制如要妥善地履行主要職能，必須與本地及海外的相關資訊系統保安機構密切聯絡。其他附屬職能還應包括與業界協商合作，加深私營機構對資訊保安的認識。

(b) 緊急應變措施

9.20 據悉，本港已有兩間機構申請撥款在香港設立電腦緊急應變小組，它們分別是香港生產力促進局和資訊及軟件業商會有限公司。資訊科技及廣播局會協助在香港成立電腦緊急應變小組。

9.21 如能迅速加深各界對電腦病毒和黑客侵襲的認識，將有助阻止問題的蔓延。電腦緊急應變小組也可以提供有關電腦罪行趨勢和發展的有用資料，甚至提供線索協助追查受害人和犯事者。不論是否另設專責機制保障重要基本設施免受網上或電腦引致的侵襲，應變小組都有其存在價值。因此，從協助執法的角度來看，工作小組原則上*支持* 在香港成立電腦緊急應變小組。

9.22 我們***建議***，在應變小組成立之後，應該把重要基本設施營辦者涵蓋在內。我們並***建議***，在應變小組成立之前，資訊科技署應與重要基本設施營辦者加強聯繫，以便迅速交流資訊，從而更妥善地應付緊急情況，雙方的溝通程序也應當盡量簡化。

第十章

公眾教育

引言

10.1 本章檢討政府及其他公營機構如何教育市民，使其認識到防止和偵查電腦罪案的重要性和相關措施，並研究是否需要和如何改善現行的教育工作。

目前情況

10.2 防止罪案是撲滅罪行整體工作的一個重要環節。通過教育可提高保安意識和操守，對於遏止電腦罪案來說，這預防工作尤其重要。舉例來說，一般電腦用戶可以因加深認識如何保護電腦系統免被黑客入侵而獲益。聯網電腦系統管理人員有需要按照良好的管理措施管理電腦系統。家長和教師需要特別的工具，以保護子女和學生免受色情物品荼毒。網上購物者也需獲得指導，以免誤墮網上騙局陷阱。從以上列舉的幾個例子可見，提高保安意識非常重要。

10.3 在現今的資訊時代，幾乎所有範疇的日常事務，都愈來愈多在網上或由電腦處理，由此更顯出使用電腦操守的重要性。鑑於聯網電腦系統互連程度極高，一次的侵襲可足以影響全球數以萬計的電腦系統，造成重大的金錢及生產力損失。就以今年五月發生的電腦病毒“愛虫” ("Love Bug") 侵襲事件為例，據估計該事件造成的損失高達 100 億美元。然而，令人感到無奈的是，發動這些侵襲的人可能並非對侵襲的對象懷有怨懟，他們的作為可能只是要在黑客界中“揚名”。由此可見，透過教育令市民，特別是年青一輩，認識這類電腦罪行的嚴重性，實在極為重要。

目前的工作

10.4 目前已有多間機構參與資訊保安和電腦操守的宣傳和教育工作。這些機構通常透過下列途徑宣揚訊息：

(a) 學校講座；

(b) 為公司舉辦的簡介會；

(c) 公開研討會；

(d) 展覽；

(e) 課程檢討；

(f) 網站；以及

(g) 行業指引。

個別機構的工作詳情載於附件 9。由該附件可見，雖然大部分工作都是由個別機構獨力推行，但也有部分工作是由多個機構共同參與。

考慮因素

10.5 工作小組得悉各機構在宣傳資訊保安意識和操守的重要性方面不遺餘力，感到十分鼓舞。這些機構顯然已在這方面付出不少努力，日後還會推行更多工作。它們所作的種種努力，已大致涵蓋有關的主題和受眾。令人感到欣慰的是，在籌劃一些教育及宣傳活動時，各有關機構曾多次攜手合作。

10.6 儘管如此，工作小組認為，現行的安排仍有可以改善之處。目前，個別機構均十分主動地推行其工作，但在統籌方面，卻有欠妥善。舉例來說，兩、三間不同機構可能各自到同一所學校舉辦講座，以及提出內容不盡相同但範圍重疊的課程修訂建議；又或者多間機構在同一次展覽中各自擺設不同的攤位推廣資訊保

安。因此，日後的工作在安排上應加以改善，務求善用有限資源和取得最大成效。我們應考慮集結各機構的資源和力量，以改善成效。各機構若加強彼此間的對話，可以促進資訊交流，並令它們可以更全面的角度考慮各項工作。

10.7 基於上述各點，工作小組*建議*設立一個機制，涵蓋目前從事資訊保安教育或宣傳工作的各個政府部門和其他公營機構，例如香港生產力促進局和消費者委員會。電腦緊急應變小組(請參閱第九章)成立後，也應參與這項工作。這個擬設機制的大致架構如下：

(a) 這個機制應為各參與機構提供溝通的渠道，讓它們可以為其即將推行的教育或宣傳計劃交流資訊。

(b) 各參與機構仍繼續主力負責制訂和推行其教育或宣傳計劃。透過這個資訊交流機制，各參與機構應盡可能允許和鼓勵其他機構參與和協辦這些計劃。為達到這個目的，主辦機構應將籌備中各項計劃的詳情，預早通知其他機構。

(c) 這個機制應能讓各參與機構評估它們的工作和計劃如何與整體工作配合。因此，這個機制適宜擔當中央統籌的角色，幫助制訂公營機構的資訊保安整體教育及宣傳策略。個別計劃應能與這項策略的主要範疇和主題緊密配合。應盡量提倡匯集資源，以代替片面推行有關工作。

(d) 這個機制應統籌推動私營機構參與公營機構主導的資訊保安教育和宣傳計劃，反之亦然。(請參閱第十一章私營機構在教育和宣傳工作中的角色。)

第十一章

私營機構的角色

引言

11.1 得不到市民大眾的參與和協助，執法機關便無法有效地撲滅罪行。本章探討私營機構在撲滅和防止電腦罪行方面擔當的角色。

目前情況

11.2 正如第九章第 9.11 至 9.12 段所指出，每個機構都有責任確保本身的資訊安全。雖然公營機構有時候也會成為侵襲的對象，但電腦罪案的受害者其實多數是私營機構或個別市民。這些罪案造成的經濟和金錢損失，亦大多由私營機構承受。因此，確保電腦罪行受到遏制，顯然是符合私營機構的利益。

11.3 私營機構事實上已在好幾方面對網上罪案作出回應。舉例來說，市面上有對抗電腦病毒程式出售或供人免費使用，亦有專業人員設計專用的保安措施，保護聯網的電腦系統。與版權有關的行業也致力保護業內人士的作品不會經互聯網非法傳遞。市場上又有過濾程式或“保姆”程式，保護兒童免被互聯網上發布的不雅或淫褻材料荼毒。在設計互聯網瀏覽器程式時，保安功能也是必備的一環。

11.4 儘管如此，一般人都認同，整體來說，社會上對資訊保安的認識以及在採取資訊保安措施方面，仍有不少可以改善之處。舉例來說，如有定期為資料數據製作備份，便可能避免慘重的損失和毋須艱辛地重建資料數據。很多時候，電腦使用者都沒有遵從一些簡單的保安步驟，例如經常更改密碼、不要告訴他人自己的密碼、在接駁互聯網前先退出內聯網系統等。商業機構現在仍未一致認識到，在資訊保安設備上的投資是

商業經營中一項必不可少的營運開支。同樣地，有些時候，費用方面的考慮，可能令尊重知識產權和使用正版應用程式的需要淪為次要。

考慮因素

11.5 對於***資訊保安設備或程式***，第 11.3 段列舉的例子足以說明，即使政府沒有提供什麼協助，私營機構其實也有能力作出回應。私營機構緊貼市場，可以對不論是大企業還是個別市民的消費者的需要，迅速作出回應。我們認為沒有理由改變這個基本上由市場主導的做法。

11.6 不過，我們認為政府在這方面仍可以擔當一定的角色，就是交流資訊。在調查電腦罪案的過程中，執法機關可能取得不法分子破解保安措施的詳細資訊。我們***建議***當局把這些資訊通知有關的行業，例如軟件業和電訊裝置製造商，讓它們可以採取跟進行動。同時，私營機構也應該讓執法機關知悉資訊保安的最新趨勢和發展，以及業界關注的保安問題。視乎案件的性質而定，這些資訊可以個別(只向個別商號)交流，也可以集體(透過行業組織或代表)交流。不過，我們要強調，私營機構之間互相交流資訊也同樣甚或更加重要。各商會、專業團體和行業組織應該制訂和推行措施，同在這一方面出一分力。

11.7 工作小組認為，私營機構在推動資訊保安的***教育及宣傳***工作方面，應可擔當一個更重要及更積極的角色。要宣揚的信息本身相當簡單，就是每名用戶都有責任保護自己的電腦系統和資料數據。要使這個信息深入民心和發揮效用，單靠政府的力量並不足夠。私營機構理所當然地應在不同層面推展教育及宣傳工作，例如：

(a) 在個別行業內 —— 專業團體和行業組織可按業內情況擬備實務守則或舉辦保安研討會；

(b) 在各個界別之間 —— 商會、中小型企業代表或有關法定團體可為中小型企業擬定指引或設立支援熱線；

(c) 在業界與消費者之間 —— 服務供應商(例如銀行、互網商和網上零售商)可主動向客戶宣揚保安資訊；以及

(d) 在整個社會上 —— 有關各方可舉辦有助提高資訊保安意識的活動。

上述工作的主題是確保資訊安全(取用資料的可靠性、資料數據的完整性和機密性) (請參閱第九章)。工作的細節自然會因不同的層面而異，但通常應圍繞以下主題：

(a) 資訊保安作為機構策略中一個重要環節；

(b) 使用電腦的操守；

(c) 預防措施，以盡量減低電腦遭受侵襲的機會，以及把侵襲的破壞減低；

(d) 對某些特定行業而言，例如網上銀行業、網上零售業等，最佳的管理守則或實務守則；

(e) 在產品研發方面保安功能的重要性(這對例如資訊科技業和版權有關行業來說尤其重要)；

(f) 資訊交流的重要性；以及

(g) 與執法機關合作的需要，例如舉報電腦罪案、提供意見等。

11.8 我們*建議*當局鼓勵私營機構依照上文第 11.7 段所述的主題，在各個層面更大力推動教育及宣傳工作，特別是呼籲專業團體、行業組織和商會為這共同目標作出貢獻。

11.9 雖然在教育及宣傳方面，私營機構本身可做的工作不少，但仍有一些由私營機構推行的措施，是政府及其他公營機構可以參與的，而很多公營機構推行的措施，也要得到私人機構的支持。我們*建議*，如果資源許可，有關的政府部門和公營機構應盡量支持私營機構推行的措施。同樣地，我們*建議*，政府部門或公營機構舉辦教育及宣傳計劃時，應積極尋求私營機構在金錢或實質上(包括提供意見)給予支持。(請參閱第十章。)

11.10 私營機構不但深受政府的電腦罪案政策影響，更對有關政策奏效與否發揮關鍵作用，因此，它們對制訂政策方面自然有相當興趣。工作小組*建議*，政府應繼續讓私營機構參與*制訂政策*。我們留意到，目前的做法大致上已是如此。除諮詢市民大眾外，當局也就直接影響有關行業的建議徵詢業界的意見。舉例來說，當局會就不雅及色情材料透過互聯網傳送的問題諮詢互網商。雖然如此，我們考慮過應否較定期地諮詢私營機構，讓它們多發表意見。舉例來說，我們應否設立一個由政府、有關法定團體和私營機構三方代表組成的討論會，商討電腦罪案問題？這做法的好處在於能夠以較宏觀的角度研究整體問題；弊處在於人們可能會認為這種討論會只尚空談，實質的成效不大。

11.11 權衡利弊後，我們認為，在商討及研究實質而非一般性問題時才徵詢私營機構的意見，會來得有用得多。若在設立適當架構處理電腦罪案問題時，已兼顧到需要預留空間，讓私營機構的意見得到考慮，較成立一個純粹蒐集私營機構意見的專責小組，更為有效。有關整體架構安排的問題，會在第十三章探討。如果該章內所載建議的方向獲得接納，我們認為毋須另外制訂諮詢私營機構的安排。

11.12 隨着資訊保安的意識日濃，我們愈來愈有需要根據一些公認的標準來評定保安預備工作的妥善程度。因此，較長遠來說，我們*建議*探討可否為不同行業及在不同層面，制訂一套公認的*審核或評估*資訊保安標準的機制。舉例來說，這機制可以是一個品質標記制

度，評審機構為一個業內組織、專業團體或獨立個體。只有資訊系統符合特定保安標準的公司，才可以獲授品質標記或獲得認證。香港會計師公會推廣的網譽認證[13]服務，便是朝這方向發展的一個例子。誠然，推行評審或認證制度這構思，必須與國際間在這方面的發展相配合。如果能付諸實行，這個制度將有助激勵私營機構在與貿易伙伴及個別消費者交易時使用適當的保安措施，以保護本身的資訊系統。舉例來說，資訊保安措施是否足夠，可以是釐定私營公司保險費的一個因素。同樣地，愈來愈精明的消費者在選擇貨品及服務供應商時，亦會考慮這個因素。

(13) 網譽認證是一個以電子商貿為本的保證印鑑服務，旨在建立消費者在網上購物和使用服務的信心。這項服務由美國會計師公會、加拿大會計師公會和一個提供數碼證書及加密服務的機構聯合提供。符合網譽認證原則和準則的網站可獲授予網譽認證印鑑，這些原則和準則包括技術（例如保安）及業務運作（例如盡量減低詐騙風險、保障客戶個人資料、履行銷售承諾等）兩方面。

第十二章

資源和能力

引言

12.1 本章檢討本港執法機關在打擊電腦相關罪案方面可以動用的資源，以及評估是否需要作出改善。

目前情況

(a) 部門的工作

12.2 自一九九三年起，*香港警務處*在商業罪案調查科之下成立了一個電腦罪案組(電腦組)，負責調查電腦相關罪案。這個由 18 名人員組成的電腦組亦就其他警隊單位調查案件所涉及的電腦證據，提供中央資料鑑證服務。該組與本地及其他司法管轄區的執法機關保持緊密聯繫，監察罪案趨勢和加強調查能力。警務處現正計劃在二零零一年年中或之前，提升電腦組的指揮階層和大幅擴充其人手。

12.3 為加強調查電腦罪案的能力，警務處在一九九九年十二月成立一個共有 83 人的電腦罪案調查支援組(支援組)，成員來自各個警區和其他單位。他們協助前線警隊單位調查電腦罪案，包括檢取電腦證物和初步評估電腦罪案現場。電腦組則負責統籌支援組的調動、對後者的調查工作提供所需技術支援，以及處理較嚴重的或跨境性質的案件。

12.4 電腦組每月為支援組的成員及其他有關執法機關的人員舉辦為期一日的訓練課程，教導學員調查電腦罪案的最新知識。

12.5 電腦組正籌辦一所電腦資料鑑證室，以便對刑事調查中檢獲的電腦證物進行數碼證據鑑證。當局已初步撥款 270 萬元購買計劃所需的硬件和軟件。

12.6 防止罪案科已成立一個電腦保安小組，為公司、學校及個別市民提供防止電腦罪案的意見。

12.7 在國際合作方面，電腦組與許多香港境內及境外的機構和組織均有聯繫，包括與日本、美國、加拿大及英國的駐港聯絡員，以及新加坡、美國及英國的電腦罪案調查員保持聯絡。

12.8 *廉政公署*(廉署)在一九九九年四月成立了一個電腦資料鑑證及資訊科技研究組(研究組)。這個由七名人員組成的研究組除了進行電腦資料鑑證外，亦負責就電腦資料鑑證事宜與外間聯絡，以及為廉署人員安排有關訓練。

12.9 研究組為廉署調查人員舉辦為期一日的內部訓練課程，內容包括電腦資料鑑證的基本原理，以及搜查和撿取電腦證物的程序。

12.10 廉署與加拿大、美國、英國及新加坡執法機關的電腦罪案專家均有保持非正式聯繫。

12.11 自二零零零年一月起，*香港海關*的版權及商標調查科成立了一支反互聯網盜版活動特遣隊。特遣隊由七名人員組成，負責調查有關互聯網上侵犯知識產權的投訴。

12.12 香港海關已經與美國和英國專門調查電腦罪案的機關建立聯繫。

12.13 *入境事務處*正籌備成立一個電腦罪案調查小組，以處理利用電腦偽造旅行證件的罪案。

12.14 自二零零零年一月起，*律政司*刑事撿控科轄下的商業罪案組成立了一個電腦罪案組，負責處理電腦案件。該組的主要職責包括為執法機關提供有關刑事起訴電腦罪案的法律意見，以及在法庭上檢控這類罪案。至今為止，商業罪案組主要透過警方的電腦組向海外機

構索取資料，本身尚未與其他司法管轄區的對口單位建立聯繫。

(b) 跨部門及機關的工作

12.15 警隊、廉署及香港科技大學於一九九八年年底聯合成立了一個電腦資料鑑證工作小組，目的是設計一套專業的電腦資料鑑證訓練課程。

12.16 “電腦罪案調查及電腦資料鑑證課程”在二零零零年一月七日至二十五日舉行，學員包括來自警務處、廉署、海關、入境事務處和律政司的 23 名人員。該課程旨在把適用於多個部門及機關的電腦資料鑑證最新發展情況，共冶一爐，是亞洲首個同類課程。這個課程在二零零零年六月及七月再舉辦了三次，共有 28 名來自廉署、海關、律政司及稅務局的人員參加。當局正考慮於二零零一年一月舉辦類似的訓練課程。

考慮因素

12.17 過去數年，各執法機關已紛紛主動採取措施對付電腦罪案，例如大多數電腦罪案專責單位都在近期設立，工作小組對此感到十分鼓舞。這些單位的人手*和設備配置*當然要遵照資源分配的一般程序。不過，我們希望*強調*，確保負責打擊和防止電腦罪案的專責單位以及參與其事的其他單位有足夠的資源，是十分重要的。電腦罪犯可以獲得市面上最新的科技。執法機關如果未能迎頭趕上，他們偵查電腦罪案的能力必然會受打擊。因此，當局應該盡量容許在購置所需器材方面有較大的靈活性。

12.18 電腦罪案調查和電腦資料鑑證工作，都需要相當特殊的*專業知識*。因此，我們曾考慮目前的安排，是否已足以確保專業人員的數目能應付日漸增加的需求。執法機關向我們保證，目前已有足夠的後備支援。儘管如此，根據外國的經驗，在聘用及挽留電腦人才方面，政府往往要跟私營機構競爭。此外，我們還得顧及因事業發展而出現的人手調動問題。因此，我們*促*

*請*各執法機關繼續密切留意這個課題，確保專業人員的供求不致失衡。我們也*建議*應盡量利用私營機構的資源和取得它們的合作，例如可以考慮推出人才交流計劃。

12.19 有人提議把各個執法機關與電腦罪案有關的所有資源匯集一起，成立一個中央的*一站式單位*，工作小組曾經考慮這項提議。表面看來，這項提議可以提高經濟效益，但仔細分析下，卻有若干弊病。不同執法機關有不同的法定權力，行使權力時須受不同的約制。如不大幅修改法例，便無法由一個新設單位處理所有利用電腦干犯的罪案。再者，一如上文所述，即使在同一機關之內，又或即使已設有對付電腦罪案的專責單位，調查電腦罪案的工作也不可以由某個單位完全負責。因此，什麼資源應匯集供建議的一站式單位使用，什麼資源應留下供原來的機關運用，確實極難決定。除非職責的劃分既清晰又易於執行，否則日後溝通的程序將變得複雜，這會延誤案件的處理。有鑑於此，我們不支持設立一站式單位的提議，並*建議*擱置這項建議。

12.20 儘管如此，工作小組同意，各執法機關盡量*互相合作*、*交流情報和經驗*，實在非常重要。據悉，各機關在調查工作方面，已經時常互相合作和交流資訊。我們*建議*，這個做法應該繼續，並加以深化。具體來說，這方面的合作應包括互相交換聯絡人名單、到外地考察電腦罪案之後為其他機關舉行滙報會、到海外參加電腦罪案研討會後傳閱會上發表的報告，更重要的，是交流處理真實案件時汲取的經驗和教訓。這類交流活動必須有系統地舉行，才能發揮作用。在第十章，我們研究過各機關應否及如何在推行公眾教育工作方面加強合作；在第十三章，我們將探討是否需要制訂一個涉及執法機關和其他組織的常設安排，以處理電腦罪案政策事宜。各執法機關之間加強合作和交流資訊，會對有關工作起相輔相成之效。

12.21 *與其他司法管轄區的執法機關合作*，對應付不受地理疆界限制的電腦罪案至為重要。儘管司法互助協定(見第

四章)已為跨境罪案的搜集證據工作奠下良好基礎，但由於電腦侵襲的蔓延速度快，且較其他罪案易於隱藏或消滅線索，因此為國際合作的問題帶來了新要求，就是有關各方必須迅速作出回應。能夠在短時間內確定並聯絡上有關的負責單位，便顯得十分重要。因此，我們*促請*本港的執法機關加強與海外對口單位的聯繫，務求能夠：

- 迅速處理個別案件；
- 交流經驗及知識；以及
- 密切注意有關事態的發展，包括立法建議。

我們也應積極支持多邊合作打擊電腦罪案的工作，並適當地參與有關的國際行動。

12.22 ***電腦證據的檢驗工作***須以特別方式處理。電腦記錄與實物記錄不同，技術上來說，每次取用都可視作“更新”電腦記錄。因此，要透過“凍結”記錄來保存電腦證據，使其獲得法庭接納，甚具挑戰性。電腦證據的處理方法是一個正在演進中的課題，據工作小組所知，國際上仍未有一套公認的處理電腦證據標準程序。因此，我們的最終目標，是確保有關的國際標準一旦確立，香港的程序應可與之相符。為此，各執法機關都應密切留意國際間有關事態的發展。

12.23 不過，工作小組相信，我們較短期的目標應是盡快制訂一套標準程序，供本港各執法機關使用。鑑於警隊電腦資料鑑證室即將成立，我們*建議*該鑑證室負責牽頭，與其他執法機關、律政司，以及本地和海外的大學和有關專業組織磋商，以制訂一套通用標準。這樣既可避免工作重複，又可善用現有資源。通用標準一旦制訂完成，便應告知司法人員(他們須審理涉及電腦罪案的法庭案件)、律師(他們須參與這類案件的辯護或檢控工作)，以及互網商等的有關人士和團體(他們可能須協助電腦罪案的調查工作)。

12.24 電腦資料鑑證牽涉專門訓練和專業知識。此外，為求公正無私，電腦資料鑑證也應與實物證據鑑證一樣，須與案件的調查工作分開進行。因此，從較長遠的角度來看，當局應考慮設立一個中央電腦資料鑑證單位或鑑證室，以便統一提供這項服務。這個做法也會較符合經濟效益。

第十三章

未來的體制安排

引言

13.1 本章探討是否需要一常設架構，以處理電腦罪案問題。

考慮因素

13.2 工作小組是一個有時限的專責小組。我們不能夠一次過徹底處理所有與電腦罪案有關的執法和防止罪行問題。故此，有需要考慮怎樣才能最有效地跟進工作小組的建議、監察這些建議的相關發展，以及評估建議對我們的政策和措施的影響。在這方面，我們曾經研究幾個擬議方案。

13.3 第一個方案是把有關工作重新納入主體架構。這並非不尋常的途徑。很多專責小組完成工作後，獲得當局接納的建議往往都交由負責有關範疇的現行架構負責執行。就本工作小組而言，這個方案的主要缺點是電腦罪行瞬息萬變，故極需要密切監察其不斷的發展。此外，如果沒有一個明確的負責單位，或許較難邀請私營機構定期參與有關工作。

13.4 第二個方案是設立一個電腦罪案常務委員會。這方案的優點是令這個機制的身分清晰、工作目標明確。一個獨立的委員會亦較易匯集這方面的專家以及與海外的對口單位建立聯繫。不過，有人可能認為這個委員會的大部分實質工作都會由其秘書處負責，故設立新的委員會用處有限。

13.5 第三個方案是採取中庸之道，由當局指派一個現有的委員會負起整體監察之責，細節的跟進工作則由有關的決策局和部門及其他相關組織執行。這個方法既可

控制工作質素，又不會把太多細節工作加諸委員會身上。

13.6 就以上第三個方案，工作小組特別研究了現行兩個和撲滅罪行及資訊科技事宜有關的諮詢機構的工作。第一個機構是由政務司司長擔任主席的撲滅罪行委員會。這個高層次的委員會由政府和非政府代表組成，負責監察香港的罪案問題。有需要時，該委員會可以成立小組委員會處理特別的事宜。撲滅罪行委員會的職權範圍和成員名單載於附件 10。第二個有關的委員會是由資訊科技及廣播局局長擔任主席的資訊基建諮詢委員會。這個委員會負責就資訊科技及電訊方面的政策、監管、技術及其他事宜向政府提供意見，其非官方成員有不少來自資訊科技及電訊業界和學術界。這個委員會的職權範圍及成員名單載於附件 11。

13.7 上文第 13.5 及 13.6 段所述的第三個方案，可避免當局成立太多委員會，而更重要的，是可以在一個較宏觀而又相關的背景下(對撲滅罪行委員會而言是罪案的整體情況，對資訊基建諮詢委員會而言是資訊基建的發展)，研究電腦罪行的問題。鑑於資訊基建諮詢委員會關注推動資訊科技業的發展多於撲滅和防止罪行，因此，撲滅罪行委員會也許是更適合的主體組織。

13.8 工作小組相信，由一個身分清晰、工作目標明確的組織負責有關工作，更能達到上文第 13.2 段所述的目的(即跟進工作小組的建議、監察這些建議的相關發展，以及評估建議對我們的政策和措施的影響)。與此同時，這個機制又可在防止和偵測罪行的整體政策範疇內運作，從而得益。因此，在衡量各項因素後，我們*建議*在撲滅罪行委員會下成立一個小組委員會以確保各項跟進工作得以落實。這個安排應至低限度在初期實施，及後小組委員會是否需要繼續存在，當局可參照其工作進度及電腦罪案的發展而不時加以檢討。

13.9 工作小組並無討論有關安排的具體細節，例如小組委員會的組成和支援。就這些事宜，當局必須考慮各項因素，例如可用資源，然後作出最終決定。不過，我

們*建議*該小組委員會應包括執法機關內對電腦罪行的政策和運作有全面認識的高層代表。此外，鑑於電腦罪行對私營機構的影響，小組委員會亦應有私營機構的代表參與。（請參閱第十一章有關私營機構的角色）。

第十四章

結語

14.1 工作小組在本報告書內勾劃了一個擬議框架，以改善目前對付電腦罪案的措施。這個框架絕非可以解決一切問題的萬應靈丹，而我們在上文各章中已指出其中一些局限。不過，我們希望它可以成為日後工作的基礎。

14.2 由於電腦罪案具有跨境的特性，我們也特別注意要確保建議的框架與國際間對這問題的見解一致。因此，在研究個別課題時，我們參考了現有的國際先例。為確保研究工作更加完備，我們曾把歐洲議會《網上罪案公約》草案(14)的條文與香港的現況作一比較，該公約是體現國際間對電腦罪案見解的一份重要文件。該份比較表載於附件 12。從中可見，香港現有的措施加上工作小組的建議，已大體上與公約草案的精神一致。我們應該繼續監察國際間有關事態的發展，確保我們的電腦罪案對策與時並進。

14.3 在商討過程中，我們發覺工作小組的一些建議可能影響電腦罪案以外的問題。我們在第一章和個別章節中已指出，有需要對這些影響進行研究。較長遠來說，我們認為必須消除電腦罪案法例與實質罪案法例之間的隔閡。若我們的法例能夠顧及資訊時代的需要，同樣適用於以傳統方式或在網上世界作出的行為，應是最理想的做法。

14.4 要實現第 14.3 段所述的長遠目標，絕非易事，可能要對目前的既定法律概念和原則進行根本性的檢討。有關司法管轄權規則的問題便是一個好例子(請參閱第四

---

(14)歐洲議會是一個擁有 41 個成員國的國際組織，目標之一是鼓勵成員國採納共通的慣例和標準以加強法治。議會在二零零零年四月發表公約草案，公開徵詢意見。公約的文本會在二零零零年十二月由一組專家敲定，而部長委員會最早可於二零零一年秋季通過文本並邀請成員國簽署。

章)。這類檢討需時甚久，而且可能要與其他普通法司法管轄區的發展同步進行。在實施根本性的改變前，我們 ***建議*** 在訂立新法例和修訂現有法例時，一般應留意資訊時代的需要。法例應盡量跨越個別科技或媒體的界限。

14.5 鑑於網上世界不斷演變，我們打擊電腦罪案的努力着實不容稍歇。我們希望獲政府接納的工作小組建議，可以盡早落實執行。為盡量爭取市民支持和合作，當局在制訂執行細則時應徵詢公眾及有關團體的意見。

附件1

電腦相關罪行跨部門工作小組

職權範圍

在顧及電腦和互聯網發展一日千里並有機會被利用進行犯罪活動的情況下，

(a) 找出上述發展對執法工作造成的困難，例如在蒐集證據和進行檢控方面的困難；

(b) 檢討現行法例和有關行政措施是否足以應付上述(a)項工作所找出的困難；

(c) 研究這方面的國際發展和趨勢，並視乎情況讓香港從中借鏡；以及

(d) 提出建議解決發現的不足之處。有關建議必須能夠一方面促進執法工作，另一方面顧及在財政或其他方面所須付出的代價。

附件 2

電腦相關罪案跨部門工作小組

成員名單

保安局

副局長(特別職務)張少卿女士 (主席)

助理局長(F1)吳世權先生 (秘書)

工商局

首席助理局長(5)陳鈞儀先生

助理局長(5)A 黃宗殷先生

資訊科技及廣播局

首席助理局長(C)蕭如彬先生(直至二零零零年七月)

首席助理局長(C)譚惠儀女士(二零零零年七月開始)

助理局長(C1)鄭青雲先生

民政事務局

助理局長(5)2 丘卓恒先生

律政司

副法律政策專員(法律意見)黃繼兒先生

高級助理刑事檢控專員唐立品先生

高級助理法律政策專員(人權)鄭佩蘭女士

高級助理法律政策專員(法律政策)單格全先生

署理高級助理刑事檢控專員／高級政府律師單偉琛先生

政府律師吳雪晶女士

香港警務處

商業罪案調查科總警司盧奕基先生

商業罪案調查科高級警司艾樂善先生

保安部高級警司卓振賢先生

保安部警司劉日雄先生

商業罪案調查科總督察陳國雄先生

商業罪案調查科督察葉嘉儀女士

廉政公署

執行處助理處長陳德成先生

首席調查主任(K)張華邦先生

總調查主任(K)5 鍾紀英先生

香港海關

海關助理關長(管制及知識產權)潘揚光先生

版權及商標調查科監督歐陽可樂先生

商標調查組助理監督陳耀華先生

管理事務科參事(法例課)李振輝先生

管理事務科助理參事(法例課)邵學斌先生

入境事務處

調查科主管梁炳焜先生

助理首席入境事務主任何仲偉先生

入境事務主任羅趙存先生

資訊科技署

助理署長(基本建設)麥鴻崧先生

總系統經理(基本建設)莫桂英女士

高級系統經理陳志賢先生

電訊管理局

助理總監(規管)劉光祥先生

規管事務經理許靜芝女士

附件 3

提及“電腦”一詞的法律條文

條例	條目
第 1 章 《釋義及通則條例》	第 88 條
第 8 章 《證據條例》	第 20、22A、22B、54 及 77F 條
第 41 章 《保險公司條例》	附件 3 及 8
第 52 章 《電視條例》	附表 1C
第 60 章 《進出口條例》	第 20、21 及 33A 條
第 61 章 《借款條例》	第 4 條
第 106 章 《電訊條例》	第 27A 條
第 112 章 《稅務條例》	第 16G、26A 及 51C 條
第 155 章 《銀行業條例》	第 2 及 137B 條
第 174 章 《生死登記條例》	第 2、5A、13、22、25、27 及 32 條
第 200 章 《刑事罪行條例》	第 59 及 161 條
第 210 章 《盜竊罪條例》	第 2、11 及 19 條
第 232 章 《警隊條例》	第 39 條
第 310 章 《商業登記條例》	第 19 條
第 318 章 《工業訓練(製衣業)條例》	第 31A 條

條例	條目
第 324 章 《非政府簽發產地來源證保障條例》	第 6A 及 10 條
第 333 章 《證券條例》	第 2 條
第 395 章 《證券(內幕交易)條例》	第 2 條
第 440 章 《提單及相類裝運單據條例》	第 2 條
第 444 章 《香港教育學院條例》	第 4 條
第 445 章 《集成電路的布圖設計(拓樸圖)條例》	第 2 條
第 486 章 《個人資料(私隱)條例》	第 8 條
第 493 章 《非本地高等及專業教育(規管)條例》	附表 2
第 494 章 《航空保安條例》	第 58 條
第 503 章 《逃犯條例》	附表 1
第 514 章 《專利條例》	第 93 條
第 522 章 《註冊外觀設計條例》	第 3 及 8 條
第 526 章 《大規模毀滅武器(提供服務的管制)條例》	第 5、6、7 及 9 條
第 528 章 《版權條例》	第 4、11、17、22、25、29、60、61、91、93、116、121、154、161、198 及 199 條 附表 2 及 5
第 542 章 《立法會條例》	第 20Z 條

條例	條目
第 553 章 《電子交易條例》	第 2 條
第 1053 章 《香港大學條例》	附表
第 1126 章 《香港浸會大學條例》	第 7 條
第 1145 章 《香港公開大學條例》	第 4 條
第 1165 章 《嶺南大學條例》	第 6 條

附件 4

規定以「可看見及可閱讀形式」

交出電腦資料的法律條文

法例	條文
《釋義及通則條例》(第 1 章)第 88 條	就由藏於電腦的資料所構成的材料而言，由原訟法庭或區域法院發出檢取新聞材料的命令規定，有關材料必須以可看見、可閱讀及可帶走的形式交出。該命令亦讓申請人取用以可看見及可閱讀形式出示的材料。
《有組織及嚴重罪行條例》(第 455 章)第 4 條	為偵查有組織罪行，律政司司長或獲授權人可向原訟法庭提出單方面申請，要求發出命令，飭令其覺得是控制與偵查有關的物料的人，在指明的期限內將物料提交給獲授權人或讓獲授權人取覽該物料。 凡與該命令有關的物料為並非以可閱讀形式記載的資料，該物料須以可以看到、可以閱讀及可以帶走的形式提交。任何人不遵從該命令，即屬犯罪，可處罰款最高達 100,000 元及監禁一年。
《非政府簽發產地來源證保障條例》(第 324 章)第 10 條	獲授權人員可規定，與本條例所訂罪行有關的電腦資料，須以可取去和以可見及可閱讀的形式出示。 任何人不遵從獲授權人員所作出的規定，即屬犯罪，可處罰款最高達 10,000 元及監禁 6 個月。

法例	條文
《大規模毀滅武器(提供服務的管制)條例》(第 526 章)第 5 條	任何海關人員及獲授權人員均可規定，與本條例所訂罪行有關的電腦資料，須以可取走和以可見和可閱讀的形式呈示。
第 6 及 7 條	海關人員或獲授權人員可獲裁判官簽發搜查令，以便到某處地方搜查藏有與本條例所訂罪行有關資料的電腦。該等人員可規定該等電腦資料須以可取走和以可見和可閱讀的形式呈示。

附件 5

“盜竊”電腦資料數據：案例

一九九四年六至十月期間，俄羅斯一名男子利用一部個人電腦和偷來的密碼，接通一間美國銀行的現金管理系統 40 次以上。他和同黨從三名銀行客戶的戶口中，將超過 1,000 萬美元的款項轉入在美國加州和多個歐洲國家的其他銀行戶口。該名男子及四名同黨最終在美國被捕和受審。他們全部承認控罪。該間美國銀行其後起回大部分失款。

2. 二零零零年三月，英國威爾士當局拘捕了兩人，他們涉嫌侵入多個國家的電子商業網址，並盜取超過 26 000 個帳戶的信用卡資料。據美國聯邦調查局估計，這宗案件引致的損失可能高達 300 萬美元。

3. 二零零零年年初，香港三名年青黑客利用電腦程式記錄了 127 名與他們同時上網的互聯網用戶的登入名稱及密碼。他們得到一名拆家協助，將有關帳戶和密碼的資料，以每宗港幣 350 元的價錢賣給熱衷於玩網上遊戲的人。由於有帳戶被盜用，11 間本地互聯網服務供應商向警方報案，聲稱合共損失港幣 197,490 元。最後，三名犯案者被法院起訴並被裁定罪名成立。

附件 6

互聯網服務供應商應保存的各類記錄

建議清單

以下的建議清單僅作示範之用。這份清單綜合了本港各執法機關希望互聯網服務供應商保存的有用記錄種類。

項目	上網時段記錄	帳戶記錄
(a) 利用數據機撥號上網	• 使用者名稱 • 進入時間 • 退出時間 • 獲編配的網絡協定位址 • 來電線路號碼 • 電郵信息識別號(連同相應的網絡協定位址、使用的時間及日期) • 網絡新聞傳輸協定記入標識(連同相應的網絡協定位址、使用的時間及日期) • 網頁位址(連同上次的上載時間、網絡協定位址和該頁的圖像)	• (經核實的)用戶姓名 • (經核實的)香港身分證號碼或商業登記／公司註冊號碼 • 用戶地址 • 聯絡人 • 聯絡電話號碼 • 開立／結束帳戶日期 • 服務種類 • 連線種類，例如 (i) 租用專線 (ii) 撥號線路 (iii) 寬頻 WAP • 登入識別號 • 電郵帳戶名稱 • 互聯網域名 • 靜態網絡協定位址(如有的話) • 付款方法： (i) 銀行帳戶資料 (ii) 信用卡帳戶資料 • 客戶帳戶配置，例如 (i) 郵件伺服器名

項目	上網時段記錄	帳戶記錄
		稱 (ii) 收件伺服器名稱 (iii) 郵箱容量
(b) 利用以太網／異步傳輸協定(透過電話線進行電腦連線)寬頻上網	同上，另加： • 專用的以太網／異步傳輸協定用戶識別號	同上，另加： • 安裝地址 • 安裝設備的電話線號碼
(c) 客戶的個別審計記錄	• 進入／退出時間 • 每次進入的動態網絡協定位址 • 偵測侵入的記錄 • 電郵重新導向	
(d) 電郵信息	• 信息內容(已閱讀及未閱讀的郵件，包括附件) • 信息路徑記錄	

附件 7

美國在保護重要基本設施方面的經驗

國家基本設施保障計劃

就美國經濟體系中每個易受攻擊的主要界別，美國政府有關當局都指派一名高級官員與私營機構合作制訂有關界別的計劃，藉以：

- 評估該界別遭受網上或實質攻擊的脆弱程度；
- 建議一套消除重大脆弱之處的方案；
- 建議設立一套可辨認及防止有人企圖發動大規模攻擊的制度；
- 制訂一套計劃，既能在遇襲時發出警告，以及阻止和抵擋攻擊，又能在受襲後迅速復原主要的服務。

2. 至於政府的重要基本設施，每個部門都委任一名總資訊主任，負責資訊保證工作。此外，還設有一名總基本設施保障主任，負責保護部門其他各方面的基本設施。每個部門均須制訂保護本身重要基本設施的計劃。國家保安、基本設施保護和反恐怖主義聯絡員(國家聯絡員)，則負責統籌保護重要基本設施整體政策的施行，以及確保不同界別和政府部門的計劃在整體上能夠協調配合，尤其注重設施之間互相依存的問題。已經施行的計劃必須每兩年更新一次。

國家基本設施保護中心

3. 國家基本設施保護中心是一個為全國重要基本設施進行威脅評估，發出警告，進行執法調查和作出應變的專責單位。它的職責範圍包括訓練、推廣和技術工具的應用。該中心的調查員來自聯邦調查局、美國特工處、國防部，並包括其他對電腦罪案和基本設施保護有豐富經驗的國家安全調查

員。這個中心旨在成為蒐集基本設施所受威脅資料的全國中心，而且是協助及協調聯邦政府對事故作出應變、減低受襲影響、調查恐嚇案件，以及監察重建工作的主要機構。

重要基本設施保證局

4. 在商業部之下成立重要基本設施保證局，目的是協助國家聯絡員把不同界別的計劃納入國家計劃之內。該局負責統籌美國政府對各項基本設施依賴程度的分析工作、協助推行國民教育和宣傳計劃，並統籌立法和公共事務。

資訊交流分析中心

5. 美國政府鼓勵私營機構代表成立多個資訊交流分析中心，以蒐集、分析、整理私營機構的資訊，並向業界和國家基本設施保護中心發放這些資訊。這些中心也蒐集和分析從國家基本設施保護中心得到的資訊，並向私營機構發放這些資訊。一九九九年成立的財經事務資訊交流分析中心，便是一個例子。這個由公營和私營機構合辦的中心，旨在促進財經事務界交流關於網上威脅的資訊。這個中心提供了迅速發放這類威脅資訊的渠道，使業界更有能力防止和偵查對其技術基本設施的襲擊，並對攻擊作出回變。

6. 美國這一系列措施背後的理念，是國家和經濟安全已經成為政府和業界共同承擔的責任。政府必須蒐集適當的資訊與業界交流；私營機構則須採取合理措施防止黑客入侵。

資料來源： 克林頓政府的保護重要基本設施政策：總統決策指引第 63 項

附件 8

電腦緊急事故應變小組

美國

設於美國卡內基馬林大學的電腦緊急事故應變小組統籌中心，與互聯網社羣合作對電腦問題作出應變、提高人們對電腦保安問題的認識，以及防止破壞電腦保安。該中心在一九八八年成立，由美國國防部撥款資助。

日本

2. 日本電腦緊急事故應變小組統籌中心在一九九六年成立。該中心是統籌各專家在電腦保安受破壞的網站進行善後工作的獨立中心機構。專家負責為保安受損的網站提供技術支援，該中心則促進他們合作解決面對的保安問題。不過，該中心不會提供維修或諮詢服務。

新加坡

3. 新加坡電腦緊急事故應變小組在新加坡資訊發展局及新加坡國立大學撥款及促成下，在一九九七年成立。這個處理保安事故的綜合中心提供以下服務：

- 發布警告、公告以及保安資料。
- 主動檢查或探測系統，並提供偵測電腦被入侵的工具。
- 舉辦保安課程、講座及工作坊，藉以提高保安意識。
- 與銷售商或其他電腦緊急事故應變小組合作，尋求解決保安事故的方法。

加拿大

4. 加拿大電腦緊急事故應變小組在一九八八年由一間私人公司成立，並獲得加拿大政府認可。這小組除了蒐集和發放有關電腦受威脅的資訊外，還以收費形式為客戶提供保安支援服務。

澳洲

5. 澳洲電腦緊急事故應變小組由昆士蘭大學管理，與設於卡內基馬林大學的美國電腦緊急事故應變小組統籌中心、其他國際電腦緊急事故應變小組，以及澳洲聯邦警隊均保持緊密聯繫。該小組協助受影響的團體溝通、根據過往經驗提供建議，並向其他可能面對危機的團體發放警告。

附件 9

宣傳和教育工作

香港警務處

警務處防止罪案科和電腦罪案組(電腦組)一直致力提高公眾的電腦保安意識和推行電腦保安教育計劃。防止罪案科經常派員到學校為師生及家長舉行講座，並會應邀訪問私營機構，向員工及管方講解電腦保安和制訂良好保安政策的事宜。防止罪案科和電腦組人員亦出席一般電腦保安事宜的公開研討會。防止罪案科除了在香港大多數的大型電腦展覽設置攤位，以提高市民的電腦保安意識外，還製作多款電腦保安宣傳品，包括單張、滑鼠墊、貼紙和海報，以便在公眾教育活動的場合中派發給市民。此外，市民亦可以在該科網址參閱有關電腦保安的資料。

2. 防止罪案科正計劃聯同教育署檢討現行的資訊科技課程綱要，擴大有關電腦保安、電腦使用者操守和責任等科目的課程，以及加入詳釋有關電腦罪案法例的內容。該科亦計劃與互網商合作，向被確認曾不當使用互聯網連接服務的用戶發警告信，以及提醒寬頻服務的用戶，由於他們的網上身分穩定不變，故此有較大的保安風險。

資訊科技及廣播局和資訊科技署

3. 資訊科技及廣播局和資訊科技署推行和策劃了多項公眾教育計劃。詳情載於本附件的附錄 A。

電訊管理局

4. 二零零零年二月，電訊管理局、香港互聯網供應商協會和個人資料私隱專員公署聯合舉辦一項反濫發電郵運動。有關方面發出新聞公告，宣布引入互聯網供應商業界實務守則，以對付互聯網上濫發電郵的活動。電訊管理局經諮詢香港互聯網供應商協會和個人資料私隱專員公署後，擬備了一份宣傳小冊子並已派發給公眾。該小冊子為互聯網用戶提供

實用的資料，以盡量減低濫發電郵造成的滋擾。電訊管理局的網頁載有反濫發電郵的資料，而宣傳小冊子則在所有民政事務處和各大郵政局派發。

5. 電訊管理局與消費者委員會緊密合作，於二零零零年四月發出新聞公告，提醒公眾慎防一些海外網站的詐騙手法。那些網站會把互聯網撥號連接轉為透過國際直撥電話連接。

個人資料私隱專員公署

6. 一九九八年一月，個人資料私隱專員公署分別為互聯網的機構用戶和個別用戶印製了兩本小冊子，提供有關互聯網上個人資料私隱的指引。供機構用戶參閱的小冊子，旨在協助網站營運者透過互聯網收集、展示或傳送個人資料時，遵守《個人資料(私隱)條例》的規定；供個別用戶參閱的小冊子，則旨在令用戶更多認識在互聯網上私隱受侵犯的風險。這些小冊子就保障個人資料提議可行的預防措施。

7. 一九九九年二月，個人資料私隱專員公署印製了第三本小冊子，為網站營運者提供遵守《個人資料(私隱)條例》的實用指引。

工商局／知識產權署

8. 知識產權署是推行保護知識產權教育工作的行政機關。一九九七年至二零零零年六月期間，知識產權署曾於 260 間中學舉辦講座，提醒學生尊重知識產權的重要性。講座闡述電腦軟件的用戶許可權協議，以及從互聯網下載免費軟件或共享軟件的問題。該署亦為其他行業的人士(包括公務員)舉辦同類的講座。

9. 一九九九年，知識產權署與香港知識產權協會攜手籌辦一個國際座談會，探討知識產權與資訊科技的關係。

香港生產力促進局

10. 除與資訊科技署(請參閱附錄 A)聯合舉辦活動外，香港生產力促進局也為商界提供下列教育機會，加深他們對資訊保安的認識。

(a) 一九九九年十一月舉辦一個資訊保安研討會，講者來自香港警務處、香港互聯網供應商協會和香港科技大學，有 450 人參加。

(b) 一九九九年十月至二零零零年七月間舉辦了八項實施互聯網／內聯網保安的課程，有超過 550 人參加。

(c) 二零零零年二月與香港郵政合作成立電子核證推廣及資訊中心，推廣電子核證的使用。

(d) 二零零零年四月舉辦為期三天的“資訊保安展覽”，共有 11 間機構向 4 000 多名參觀者展示它們的資訊保安服務。該局同時安排了 16 次研討會，讓參觀者加深對電腦黑客入侵有關事宜的認識。

(e) 二零零零年三月與資訊科技及廣播局合辦香港 e 大賞，推廣商業網站保障消費者的重要性。

(f) 二零零零年三月舉辦一個公開密碼匙基礎建設管理訓練課程，有 40 多人參加。

(g) 二零零零年二月至七月間舉辦了六次為期半天的研討會，推廣電子保安辦法。

(h) 二零零零年九月和十一月將會舉辦更多有關資訊保安的研討會。

(i) 二零零零年四月發表《網上私隱及消費權益保障指南》教育單張。這項計劃由消費者委員會和個人資料私隱專員公署協辦。

消費者委員會

11. 除暑假前到學校舉辦互聯網保安講座外，消費者委員會自一九九八年六月開始，在《選擇》月刊登載了多篇以互聯網一般及專門知識為題的文章，所涉獵的主題包括：

- 濫發電郵；
- 網上證券交易；
- 網上購物；
- 電子商貿付款系統；
- 搜尋發放可疑醫療廣告網站的掃網行動；
- 國際直撥電話服務圈套，即一些有問題的網站把互聯網撥號連接轉為以國際直撥電話服務駁至海外的伺服器；
- 電子商貿的消費者資料數據保障；以及
- 如何在網上空間核證交易對方的身分。

附件 9 附錄 A

資訊科技及廣播局／資訊科技署推行的公眾教育活動

有關資訊保安的公眾教育計劃 —— 已舉行的活動

編號	活動	日期	形式／次數	目標	活動對象
1.	資訊保安研討會 (由資訊科技署和香港生產力促進局合辦)	1999年 11月10日	研討會／ 一次	加深參加者對資訊保安的認識。	資訊科技專業人士和使用者。 (參加者約有400名)
2.	“家長認識資訊科技”計劃 (講者來自教育署、香港中文大學和香港警務處)	1999年 12月12日 展開 (計劃推行後的覆檢於二零零零年五月進行)	視像光碟及資料單張／在1999至2000學年舉行	為家長提供資訊科技教育，協助他們教導子女正確使用資訊科技。 主要目標之一是提醒家長留意使用互聯網可能帶來的影響和涉及的法律問題。	中學生家長。 (約有130間中學參加) (計劃小組參考中學的意見後，會探討以另一種方式把這項計劃介紹給小學生家長)

編號	活動	日期	形式／次數	目標	活動對象
3.	中小型企業電子貿易研討會	2000年3月8日	研討會及小型展覽／一次	為中小型企業介紹市面上與電子商貿有關的服務。 香港郵政的講者應邀向參加者講解資訊保安和法律事宜。	本地的中小型企業。 (參加者約有700名)
4.	電子商貿網上訓練計劃	2000年4月	視像光碟	推廣電子商貿。 公開密碼匙基礎建設是視像光碟的題材之一。	市民大眾。 (派發了約14萬張視像光碟)
5.	電腦保安和黑客入侵問題研討會 (由資訊科技署和香港電腦學會合辦)	2000年4月1日	研討會／一次	加深參加者對資訊保安的認識。	資訊科技專業人士和使用者。 (參加者約有250名)

編號	活動	日期	形式／次數	目標	活動對象
6.	資訊保安展覽 (由香港生產力促進局舉辦，資訊科技署協辦)	2000年4月12至14日	研討會及展覽／一次	加深參加者對資訊保安的認識和介紹現有的保安辦法。	資訊科技專業人士和使用者。 (參觀者約有4 000名)
7.	互聯網網頁寄存 — 電腦病毒 — 資訊保安	1999年4月 2000年3月	持續進行	加深市民對資訊保安和電腦病毒的認識，並提供有關資訊保安和電腦病毒預防措施及警告的指引。	市民大眾。
8.	電子貿易新紀元講座	2000年5月31日	研討會／一次	加深本地中小型企業對電子商貿的認識和知識。 香港郵政的講者應邀解釋資訊保安和法律事宜。	本地的中小型企業 (參加者約有400名)

編號	活動	日期	形式／次數	目標	活動對象
9.	在數碼21新紀元網站(www.digital21.gov.hk)設立公開密碼匙基礎建設網頁	2000年8月14日	網頁	提供有關公開密碼匙基礎建設、《電子交易條例》、數碼證書及其他相關概念的資料。	市民大眾。
10.	公開密碼匙基礎建設宣傳短片／聲帶啟播 (宣傳短片／聲帶由資訊科技及廣播局製作)	2000年7月10日	宣傳短片／聲帶／一次	推廣使用公開密碼匙基礎建設和數碼證書進行穩妥的電子交易。	市民大眾。
11.	互聯網及資訊保安專題講座 (由資訊科技署和香港生產力促進局合辦)	2000年7月12日	研討會／一次	加深參加者對資訊保安的認識。	資訊科技專業人士和使用者。 (參加者約有450名)

編號	活動	日期	形式／次數	目標	活動對象
12.	2000年網上商業博覽	2000年7月27至29日	展覽／一次	推廣公共服務電子化計劃和相關的服務(例如公開密碼匙基礎建設和對資訊保安的認識)。	資訊科技專業人士和市民。
13.	由資訊科技及廣播局和消費者委員會合辦的推廣公開密碼匙基礎建設記者招待會 (由資訊科技署協助資訊科技及廣播局進行示範)	2000年8月15日	記者招待會／一次	推廣公開密碼匙基礎建設和公布《選擇》月刊會登載一篇以公開密碼匙基礎建設為題的文章。	市民大眾。
14.	印發有關防止病毒入侵的單張／小冊子	2000年7月17日	小冊子／一次	加深市民對防止病毒入侵的認識和提供有關保護電腦免受病毒入侵良策的指引。	市民大眾。

編號	活動	日期	形式／次數	目標	活動對象
15.	在《選擇》月刊登載一篇以公開密碼匙基礎建設為題的文章	2000年8月15日	文章／一次	加深市民對公開密碼匙基礎建設的認識。	市民大眾。

有關資訊保安的公眾教育計劃 —— 將會舉行的活動

編號	活動	日期	形式／次數	目標	活動對象
1.	一連串以資訊保安為題的研討會 (將由資訊科技署和香港生產力促進局合辦)	2000年9月15日和11月16日	研討會／一次	加深參加者對資訊保安的認識。	資訊科技專業人士和使用者。
2.	印製資訊保安資料單張／小冊子	2000年8月	小冊子／一次	加深市民對資訊保安的認識和提供有關保障資訊保安良策的指引。	市民大眾。

編號	活動	日期	形式／次數	目標	活動對象
3.	第三輪公共服務電子化計劃流動展覽(公共屋邨)	2000年8月中至9月中	流動展覽／一次(6個地點)	推廣公共服務電子化計劃和相關服務(例如公開密碼匙基礎建設和加深對資訊保安的認識)。	市民大眾。
4.	印製公開密碼匙基礎建設和數碼證書資料單張／小冊子	2000年9月	小冊子／一次	推廣公開密碼匙基礎建設和數碼證書。	市民大眾。
5.	在數碼21新紀元網站(www.digital21.gov.hk)設立公開密碼匙基礎建設網頁	2000年9月	網頁	改善網頁，加設問答部分和互動遊戲。	市民大眾。
6.	2000年亞太區資訊科技展	2000年9月27至30日	展覽／一次	推廣公共服務電子化計劃和相關的服務(例如公開密碼匙基礎建設和對資訊保安的認識)	市民大眾。

編號	活動	日期	形式／次數	目標	活動對象
7.	電腦軟件展覽二千	2000年11月15至18日	展覽／一次	推廣公共服務電子化計劃和相關的服務(例如公開密碼匙基礎建設和對資訊保安的認識)。	市民大眾。
8.	第四輪公共服務電子化計劃流動展覽(政府合署)	2000年12月中至2001年1月底	流動展覽／一次(6個地點)	推廣公共服務電子化計劃和相關的服務(例如公開密碼匙基礎建設和對資訊保安的認識)。	市民大眾。

資訊科技署
二零零零年八月

附件10

撲滅罪行委員會

職權範圍

(1) 制訂計劃，協力減少罪案；

(2) 統籌各有關部門及機構進行上述計劃的工作；

(3) 收集各有關部門及機構所提交的報告，並根據這些報告，評估各項計劃的進展和成效；

(4) 訂定方法，鼓勵市民協助減少罪案；

(5) 收集及整理各方面提出有關如何減少罪案的意見；

(6) 建議制訂減少罪案所需的立法及行政措施；以及

(7) 每年向行政長官報告工作進展一次。

成員名單(截至二零零零年八月)

政務司司長(主席)

律政司司長(副主席)

保安局局長

民政事務局局長

衞生福利局局長

教育統籌局局長

警務處處長

懲教署署長

王葛鳴議員，JP

劉健儀女士，JP

涂謹申先生

龐創先生，JP

潘展鴻先生

周偉淦先生，JP

石丹理教授，JP

鄭成業先生

保安局首席助理局長(E)(秘書)

附件11

資訊基建諮詢委員會(委員會)

職權範圍

為實現政府的目標，令香港在資訊科技新紀元着着領先，委員會將會就如何協助香港資訊基建的發展，尤其是涉及下列範疇的政策、規管、技術及其他相關事宜，向政府提供意見：

(1) 進一步發展及加強香港的實體通訊基礎設施；

(2) 在已經建立通訊網絡上發展開放及共通介面、讓個人、商界、政府都能夠使用本身的系統方便地互通資訊，而需要保密的資料也不會外泄；

(3) 發展有效使用共通介面的應用系統；

(4) 訂定香港在國際和區內組織及討論場合上就全球及區內資訊基建及電子貿易事宜所採取的立場和參與程度；以及

(5) 提高社會人士對資訊科技的認識及向各界推廣靈活應用資訊科技。

成員名單(截至二零零零年七月)

資訊科技及廣播局局長(當然主席)

張啟洲先生

錢玉麟教授

周文耀先生

方　鏗先生

簡永基博士

高　錕教授

盧永仁博士，JP

呂博聞先生

莫乃光先生

單仲偕先生

丁午壽先生，JP

曾勵強先生

于均諾博士

葉賜添先生

余國雄先生

教育統籌局局長或其代表(當然委員)

工商局局長或其代表(當然委員)

電訊管理局總監或其代表(當然委員)

資訊科技署署長或其代表(當然委員)

附件12

歐洲議會《網上罪案公約》草案*

比較表

歐洲議會公約草案		香港的情況
條文	簡略說明	
1.	公約內所用詞彙。	不適用。
2.	公約的每個締約成員必須把未獲授權下取用電腦系統列為罪行。	《電訊條例》(第106章)第27A條訂明藉電訊而在未獲授權下取用電腦資料的罪行；《刑事罪行條例》(第200章)第161條訂明有犯罪或不誠實意圖而取用電腦的罪行。工作小組建議加強這些罪行的法例。
3.	公約的每個締約成員必須把未獲授權下蓄意截取非公開傳輸的電腦資料數據列為罪行。	工作小組建議闡明現行法律條文的涵蓋範圍，使所有在各個儲存或傳輸階段的電腦資料數據均獲保障，以免在未授權下被人取用。
4.	公約的每個締約成員必須把未獲授權下蓄意干擾電腦資料數據列為罪行。	《刑事罪行條例》(第200章)第60條的刑事損壞罪行已涵蓋此點。
5.	公約的每個締約成員必須把未獲授權下蓄意干擾電腦系統運作列為罪行。	香港有關刑事損壞的罪行已涵蓋此點。
6.	公約的每個締約成員必須把生產、分發或管有專門用以或意圖用以違犯第2至5條所指罪行的裝置或密碼列為罪行。	工作小組研究過有關問題，並建議不應立法禁止管有黑客入侵工具，因為這些工具也可以用於正當用途。不過，我們已建議加強法例，保障包括密碼在內的電腦資料數據免受非法販賣。
7.	公約的每個締約成員必須把偽造電腦資料數據列為罪行。	《盜竊罪條例》(第210章)第19條訂明的偽造帳目罪行，已包括偽造作會計用途的資料。涉及誤用電腦的刑事損壞罪行(第200章第60條)也與此有關。

* 二零零零年四月二十五日發表的十九號文本。

歐洲議會公約草案		香港的情況
條文	簡略說明	
8.	公約的每個締約成員必須把透過操縱電腦資料數據或干擾電腦系統藉以行騙列為罪行。	《刑事罪行條例》第161條與此有關 ——有犯罪或不誠實意圖而取用電腦。
9.	公約每個締約成員必須把透過或在電腦系統製作、分發和管有兒童色情物品列為罪行。	兒童色情物品防止條例草案處理這方面的問題。
10.	公約每個締約成員必須把未獲授權下蓄意利用電腦系統複製及分發受版權保護的作品以作商業用途的行為列為罪行。	《版權條例》(第528章)第26及118條已涵蓋這些罪行。
11.	公約每個締約成員必須把企圖觸犯和協助及教唆他人觸犯第2至10條所載罪行列為罪行。	香港已經將企圖觸犯和協助及教唆他人觸犯這類罪行列為罪行。
12.	公約每個締約成員必須就公約所訂明罪行的共同法律責任作出規定。	香港已有類似條文。
13.	上述刑事罪行的刑罰，必須是有效、與罪行嚴重程度相稱，並能起阻嚇作用的制裁和措施。	本港法例也是按類似原則制訂罰則。工作小組亦曾建議修改某些罪行的罰則，以更準確反映罪行的嚴重程度。
14.	主管當局應獲授權搜查及檢取電腦系統和資料數據，以供刑事調查或訴訟之用。	調查人員可根據有關法例獲發手令搜查和檢取證據。
15.	主管當局應獲授權命令有關人士交出刑事調查及訴訟所需的電腦資料數據。	《有組織及嚴重罪行條例》(第445章)所指的提交令與此有關。工作小組亦曾建議，對較嚴重的罪案採取強迫披露加密電腦資料數據的程序。
16.	為進行刑事調查或訴訟，主管當局應獲授權要求有關人士保存由他控制的指定儲存資料數據，並須將保存資料數據一事保密。	現行法例條文已包括這項規定。

歐洲議會公約草案		香港的情況
條文	簡略說明	
17.	依據第16條，有關當局必須以法例或其他措施，確保盡快保存某次指定通訊的往來資料數據。	現行法例條文已包括這項規定。
18.	尚在商討中 —— 未有詳細資料	不適用
19.	每個締約成員必須就在該國司法管轄區內發生，或其國民在其領土外干犯的上述第2至11條所載的罪行，確立司法管轄權。	工作小組已就司法管轄權的問題進行研究和提出建議，只要取用電腦的人身在香港或被取用的電腦是在香港，香港法院便可享有司法管轄權。
20.	締約成員必須在調查電腦相關罪案和蒐集刑事罪案的電子證據方面互相提供協助。	我們積極回應香港以外對口單位提出的協助要求。
21.	第3至5條及7至11條所訂立的刑事罪行，是可以在各締約方之間引渡的罪行。	《逃犯條例》(第503章)附表1所說明的罪行均屬可以引渡的罪行，包括*與電腦數據有關的損害*和*涉及非法使用電腦的罪行*。
22.	締約成員必須在協助電腦相關罪案的調查和訴訟方面，以及蒐集刑事罪案的電子證據方面盡量互相提供協助。	這適用於和香港已簽訂司法互助協定的司法管轄區。
23.	公約的每個締約成員之間若果沒有簽訂互助條約或協定，便應各自制訂有關互助要求的程序。	這項建議與我們目前的做法一致。
24.	締約成員必須採取一切適當措施，當另一締約成員要求時，盡快保存指定的資料數據。就回應要求而言，雙重犯罪並不是應提供保存資料數據協助的一項條件，但可以是披露資料數據給對方的一項條件。	欠缺雙重犯罪這項因素，意味着該活動在香港可能不構成犯罪。如果情況如此，能夠取得手令或法庭頒令以保存資料數據的機會將會極微。試圖為這類案件保存資料數據，看來會徒勞無功。不過，盡快保存資料數據這項一般原則，與我們的目標一致。

歐洲議會公約草案		香港的情況
條文	簡略說明	
25.	被要求方在執行根據第24條提出的要求時，如發現有關通訊的傳輸涉及第三國的服務供應商，便須盡快向要求方披露足夠的通訊資料數據，以便確定該服務供應商的身分和有關通訊傳輸所經的路徑。	這與我們目前的做法一致。
26.	遇有另一方要求搜查、檢取或獲取由電腦系統保存的資料數據時，被要求方須盡快執行有關要求。	這與我們目前的做法一致。
27.	如果資料數據可供公眾查閱，或資料數據的當事人已同意讓某締約成員取用資料數據，則該成員可向另一司法管轄區索取數據。	這與我們目前的做法一致。
28.	尚在商討中 —— 未有詳細資料	不適用
29.	公約的每個締約成員必須指定一個能夠每周七天每天24小時都聯絡得上的單位，以確保能為其他締約成員即時提供下列協助： (a) 提供技術意見； (b) 盡快保存資料數據；以及 (c) 蒐集證據、提供法律資訊和追尋疑犯。	這屬歐洲議會成員國之間的內部安排。雖然如此，如果有類似安排而又非只限適用於主權國，香港應探討可否參與。