美國空軍電腦犯罪偵查手冊（四）

柴　漢　熙*

第五章－未經授權登入他人電腦系統（包含電腦駭客） 聯邦法第 1030 條與 1029 條

簡　介

Thomas Ricks 的著作「迫在眉睫的資訊保衛戰」，大膽的描述 1997 年美軍事部門擁有 2 百餘萬台以上的電腦，以及 1 萬部以上的區域網路系統。根據統計百分之九十以上的軍事電子通訊是透過公眾所使用的網際網路而四處穿梭。1998 年 4 月 20 日， AOL 的副總顧問 John Ryan 在「21 世紀全國資訊基礎建設防護會議」演講時指出，1993 年全球僅有 3 百萬網際網路使用者，但是 1997 年終卻暴增一億以上，僅僅 AOL 即有 1 千 2 百萬的客戶。他更指出網際網路的流量是每百天呈倍數增長。

網際網路呈現爆炸性的成長，使得資訊變成具有經濟價值的商品，同時也有許多人認為，侵入他人的電腦系統而存取相關資訊是一件微不足道的小事。對於這類人物，社會上已經使用一些特別的名詞來稱呼他們。例如駭客（hacker）、侵入者或者是 cracker、phreaker、phracker，在不同的情境使用不同的字眼。例如，駭客通常指青少年的入侵者，具有興奮衝動的特徵，當這些人被查獲後，最典型的辯解就是入侵他人電腦，乃是為了促使對方改進電腦的安全系統，於是不論動機如何，駭客經常在電子布告欄張貼他們入侵電腦系統的戰果，其中有登入的密碼、登入的帳戶以及入侵的系統。因此，若懷有不正的念頭，即可利用這類駭客的資訊，輕易的侵入他人電腦系統。至於 Cracker 通常是指對於入侵電腦系統並加以破壞的人。這類族群具有強大破壞能力實在不容忽視。本手冊對於侵入電腦系統的人統稱「侵入者」，藉以涵蓋所有不同面貌的駭客。

細節分析

1.利用電腦連結的詐欺行為及其相關行為 聯邦法第 1030 條

聯邦法第 1030 條又稱之電腦入侵者的制裁條款。法律條文於 1986 年公布施行，又稱為「1986 年電腦詐欺與濫用防制法案」，迄今已修正三次。最新修正條文稱為：「1996 年國家基礎建設防護法案」。在法律條文中，讀者應注意其中有許多詞彙在意義與功能上具有不同的解釋。雖然大部分的詞彙均有相關條文來定義，然而某些付之闕如。大多數的名詞都是在說明電腦實際的運作與機件互動的情形。例如：「意圖登入」或者「踰越權限登入電腦系統」，後者的詞彙在聯邦法第 1030 條(e)項⑹款中有明確的定義，然而所謂「意圖登入」部分卻無。當我們檢視立法過程時，發現參議院僅將研討侷限在何謂「意圖」。當時定義「意圖登入」乙詞是：「一個明確的故意，未經適當的授權登入他人電腦檔案、資料的行為」。參議院公報更進一步的解釋「意圖」，係指「不僅是出於行為人自由意願，並且具有意識目的行為」（參閱公報第 99 期第 432 號第二次會期，1986 年第六輯）。

就現今立法而論，聯邦法第 1030 條訂定了六項重罪、五項輕罪。在未經修法前，大多數侵入軍事電腦系統的犯罪均屬本條第(a)項⑶款與(a)項⑸款(c)目的輕罪。如此的分類對於工作量大，而人手又不足的聯邦檢察官而言，的確造成相當的爭議。迫使他們將有限的精力投入在這些案件上，但是又必須獲得最大的效益。不過，對大多數的檢察官而言，他們樂於接受這些勁爆的挑戰，對

* 柴漢熙，美國聖母大學法學碩士，現任龍華科技大學企管系講師。

於追訴相關電腦犯罪相當投入。（請讀者注意，聯邦法第 1030 條的適用，對於其他相關法律之處罰並無競合的效果。特別是 Riggs 案件[1]，聯邦法院認為聯邦法第 1030 條並未排除其他相關處罰法律的適用。

依次來檢視本條各項規定，1030 條第(a)項⑴款：嚴禁利用電腦從事間諜活動。違反本項規定者屬於重罪，不論在罰金或有期徒刑的處罰上都是最高限度，最重可判處十年以下有期徒刑。有關本罪構成要件如下：

⑴行為人於侵入電腦系統時，明知其進入電腦系統係未經授權或踰越授權範圍之行為。

⑵行為人侵入電腦系統之行為，因而使其獲得分類保密資料或核武相關的情資。

⑶行為人有足夠的理由確信，使用上開資料可能對國家產生危害，或者因此使外國政府受益，而且

⑷行為人故意保留上開資料，並意圖傳輸、運送、移轉予無權接受之第三人。

就現況所知，目前尚無起訴此類犯罪行為，我們推論原因係舉證困難，尤其是利用電腦傳輸資料而構成第三、第四款的要件行為。1996 年修法後，立法者要求政府證明行為人「明知」資料的使用對國家產生危害。這項認知標準降低後本條更具實務功能。

聯邦法第 1030 條(a)項⑵款列有(A)至(C)三目。其立法目的在於保護未經分類的機密資料，避免外部（未經授權）與內部（踰越授權）人員的侵入。每一目保護的資訊各異。第 1030 條(a)項⑵款(A)目保護金融機構、信用卡公司或相關機構所保存的金融來往記錄。第 1030 條(a)項⑵款(B)目保護政府機關、部門之資訊。第 1030 條(a)項⑵款(C)目保護私人資訊且須為國內或國際之通訊。

無論如何，檢察機關在偵辦此類案件時，僅僅證明「無故登入電腦系統」的行為是不夠的，尚須證明行為人藉此存取資料。不過，「存取」行為並未在法條中訂明。美國司法部電腦犯罪防治與智慧財產處處長 Scott Charney 先生曾經對「存取」提出解釋：「僅僅閱讀資料即是，而且不論該資料是否被實體的移動或複製」。（參閱 Emory 法學院期刊 Scott Charney & Kent Alexander, Computer Crime, 45 Emory L.J. 931, 951 1996)

違反上述三目的規定均以輕罪論處，但是行為人如：1）犯罪主要目的係獲得財務上的利益或，2）犯罪的行為的目的係為展開另一次的犯罪行為或侵權行為或，3）犯罪所得超過 5000 美金。構成其中一項要件時，可判處五年以下有期徒刑併科最高額度罰金。（聯邦法第 1030 條 C 項）

無故侵入軍事電腦系統屬於聯邦法第 1030(a)項⑶款的犯罪行為。本款規定未經授權無故登入政府機關所屬非公眾使用之電腦系統，且該非法登入行為影響政府部門之使用權，即為犯罪行為。本款的重點在於檢察機關無須證明該行為具有危害性，僅需證明行為人無權登入之行為存在即可。然而，本條不足之處在於僅規範外部的侵入者，對於機關內部踰越權限登入行為卻無拘束。

聯邦法第 1030 條(a)項⑷款針對使用電腦為詐欺行為。檢察機關面對此類案件時，必須舉證行為人有詐欺的意圖，明知無權而侵入受保護之電腦系統，而且從中獲取利益。如僅獲得非財產之物件，卻以之運用於一年期間內獲益達美金 5000 元以上者，亦屬本款所規範之犯罪行為。美金 5000 元門檻不僅對較為嚴重的犯罪具有拘束力，更是為保護「超級電腦」而量身訂製。一般情形下，使用超級電腦每小時花費可達數千美元。本款規範的對象不論是外部或內部的侵入者均屬之，可判處五年以下有期徒刑併科最高額度罰金。

有關電腦資訊的「財產價值」，適用上是一個具有爭議性的問題。某些法院判決認定，凡是合理的估算方式均可列入。因此包含研究發展的費用，或是資訊在黑市中的價格。參閱 Stegora 案件的判決[2]。但是在 Czubinski 的案件[3]，聯邦第一巡迴法院有不同的見解。判決理由認定行為人透過稅務局的電腦系統蒐整納稅人資訊之行為，與聯邦法第 1030 條(a)項⑷款所定具有財產價值的要件不符。所謂資訊的「財產價值」與侵入行為人的需要以及其他客觀事證相關。

聯邦法第 1030 條(a)項⑸款亦有(A)至(C)三目。聯邦法第 1030 條(a)項⑸款(A)目針對意圖損害他

---

1 United States v. Riggs, 739 F. Supp. 414, 423, N.D., Ill, 1990

2 United States v. Stegora, 849 F.2d, 291, 8th Cir., 1988

3 United States v. Czubinski, 106 F. 3d 1069, 1st Cir., 1997

人具有保護程式的電腦系統，而傳輸、移轉該電腦系統的程式、資訊、電腦碼、或程式指令檔案。本條屬於重罪法律，第一次觸犯本罪可判處五年以下有期徒刑併科最高額度罰金，再犯者，可判處十年以下有期徒刑併科最高額度罰金。本罪要件如下：

⑴行為人明知為電腦程式、資訊、電腦碼、程式指令檔案並使之傳輸

⑵傳輸上開物件後，造成該具有保護程式的電腦系統損害，而且

⑶行為人對於前項的損害行為係非經合法授權所為。

所謂「具有保護程式的電腦系統」於本條(e)項⑵款中詳細訂明，主要可區分三大類：1）金融機構或政府機關專用電腦系統，或 2）雖非專屬系統，但金融機構或政府機關於使用時，因行為人之犯罪行為所致而妨礙其使用，或 3）適用於國內外商業用途的電腦系統。第三項可以包括任何與網際網路連接的電腦系統。

本法是因應「Morris 網蟲」病毒所制訂，參閱 Morris 案件[4]。本案被告 Morris 為大學生，設計病毒程式並在網際網路上散發，導致全美至少 6000 多部電腦系統癱瘓，其中包含教育、醫療、軍事等系統。本款對外部或內部的侵入者均一體適用。有關「損害」乙詞定義在聯邦法第 1030 條(e)項⑻款之中，在適用上應非常謹慎。「損害」的定義為：「對於電腦數據、程式、系統的整合性與適用性造成損傷，或使用電腦資訊

⑴對任何人造成財物之損失，一年累計失達 5000 美元以上者；或

⑵意圖危害他人，而修飾或毀損任何人之醫療檢驗記錄、診斷記錄、治療或照護的醫囑處方，或有修飾毀損上開資料之虞者。

⑶對任何人造成身體上的傷害。或者

⑷對於公眾的健康與安全造成威脅。」

Magnuson 案件[5]，被告是民營公司（INET）的電腦分析師。該公司經營業務為企業管理電腦系統，其中包括 Devereaux 基金會。被告被解雇後，透過家中的電腦系統，使用先前的核准的通關密碼登入基金會的電腦系統，然後癱瘓該基金會在其他七個州的電腦系統伺服器。被告被起訴後經法院以觸犯聯邦法第 1030 條之規定，判決有期徒刑二年。被告不服並以原審法院對於被害人的電腦系統的實際傷害並未敘明理由，判決顯有瑕疵而提起上訴。聯邦第四巡迴法院贊同原審法院的認定而駁回上訴。有關實際傷害部分，原審法院認為 INET 公司與基金會的維修人員每個人花費 112 至 136 小時來恢復電腦系統的運作，而每小時以美金五十元計算應屬合理。Sablan 案件[6]，被告 Sablan 小姐係被解雇的員工，以報復的手段加諸於雇主夏威夷銀行。利用公司先前核准的登入密碼，潛入銀行的電腦主機，並毀損部分銀行檔案。被告以觸犯聯邦法第 1030 條第(a)項⑸款（本條款適用期間為 1986 至 1994 年）之規定被定罪。被告以法院認定的財物損失其中包括：銀行與聯邦調查局之間的會議聯繫開支計美金 5,350 元，以及因被告毀損檔案導致銀行額外增加使用電腦的開支費用、行政管理費用與支出員工費用等項目過於浮濫而提出上訴。聯邦第九巡迴上訴法院判決認定會議聯繫費用美金 5,350 元應予刪除，但是其他費用總計美金 22,902.38 元應屬必要，維持原判。

聯邦法第 1030 條第(a)項⑸款(B)目屬於重罪範圍，規範外部人員未經允許故意侵入他人電腦系統，並且因「行為輕率」導致毀損具有保護程式的電腦系統。其中有二個要件：

⑴行為人明知未經授權或允准，故意侵入具有保護程式的電腦系統，而且

⑵侵入行為的結果，係因被告輕率的行為導致毀損該電腦系統。

聯邦法第 1030 條第(a)項⑸款(C)目則屬於輕罪範圍，其規範外部人員未經允許故意侵入具有保護程式的電腦系統，於過失的情形下毀損該電腦系統。本條在犯罪意圖上與同條款(B)目比較屬於過失。本條大多適用於侵入軍方系統的行為人，但是因為法條對損害的定義（參閱前開說明），更加限制了法條的實用性。

1996 年，美國法院在 Harvey 案件中，對於行為人將具有癱瘓系統能力的電腦碼傳輸給有權限

---

4 United States v. Morris, 928 F.2d 504 2nd Cir. 1991, cert. denied, 502 U.S. 817, 1991

5 United States v. Magnuson, 120, F. 3d, 263, 4th Cir., 1997

6 United States v. Sablan, 92 F. 3d, 865, 9th Cir., 1996

登入電腦系統之人，而有權限之人於不知的情形下，將該電腦碼載入系統導致毀損，因此對於能否適用聯邦法第 1030 條各項各款的規定發生疑議。本案原告（NTPI）公司係專門提供醫學上診斷攝影影像。而被告 Harvey 先生為另一家醫學診斷攝影影像公司（MDI）的負責人，自行研發可強化影像的電腦系統。原告向被告購買其中一套系統。雙方交易後在合約上因而引發爭執。爭議尚未解決前，被告仍繼續研發該系統而製作升級版本，並在系統中設定一組密碼防範複製使用，如無升級碼即可使系統癱瘓毀損。原告在不知的情形下載入該程式，因無升級碼而導致系統無法運作。法院判決被告的行為業已構成聯邦法第 1030 條(a)項⑸款的規定。

聯邦法第 1029 條又稱之為「防制電腦密碼詐欺法案」，不但禁止非法買賣電腦登入密碼同時也禁止持有非經授權的電腦登入密碼，而聯邦法第 1030 條(a)項⑹款為處罰非法買賣電腦登入密碼的行為。本條款係屬輕罪範圍，其主要構成要件：

⑴行為人明知其持有電腦登入密碼，並且將其移轉或配置與其他人

⑵行為人於行為時，具有詐欺的意圖，並且

⑶行為人的行為使國內或國外的商業交易受到影響，或影響所及之電腦系統為美國政府所使用。

雖然聯邦法第 1030 條對於電腦密碼並無定義，而主要的法條規範即聯邦法第 1029 條對此亦無解說，但是參議院委員會，對於電腦密碼乙詞的解釋是：「為獲准登入電腦系統所設計的一組命令或指令」。委員會指出，電腦密碼應該擴大解釋涵蓋不只是一個單字而已[7]。

聯邦法第 1030 條(a)項⑺款的規定係處罰電腦千面人，最重可判處有期徒刑五年，第一次犯罪尚須併科罰金。其構成要件如下：

⑴藉由通訊方式針對國內外商業機構以其所設定保護的電腦系統實施破壞並予以恐嚇之行為，且

⑵意圖從人員或機構獲取不正當利益或其他具有財產價值之物。

本條制訂的目的係反制真實發生的案件。電腦駭客潛入他人電腦系統，並將系統內的資料轉換成密碼，導致系統無法正常操作，藉此要求贖金來換取破解碼。

2.非法取得、買賣、持有登入他人電腦的工具或密碼, 18 U.S.C. § 1029

聯邦法第 1029 條係禁止持有非經授權的電腦登入密碼。本條主要針對信用卡或行動電話識別卡的詐欺案件，然而在名詞解釋上，有關登入裝置業已涵蓋電腦登入密碼。在 Fernandez 案件[8]，聯邦地方法院判定：「本條直接的意義，當然包含竊取或以詐欺方式取得密碼，進而使用該密碼以登入他人之電腦系統，藉電腦誤認的方式從中獲得有價之物，例如電話公司或信用卡公司的服務」。

本條為重罪，行為人故意且以詐欺的意圖持有、買賣、或使用非經授權或偽造的登入裝置，或者以詐欺的意圖而生產、買賣、實力支配、監管或持有相關製造登入裝置之器具。本條有數款規定，有關要件各有不同。

聯邦法第 1029 條(a)項⑶款係保護特定法益，禁止行為人以故意詐欺的意圖擁有十五項以上的登入裝置，而該裝置係屬非經授權製造或偽造。如前述，電腦駭客經常蒐集並相互交易他們曾經破解的電腦系統密碼資訊。就最低限度而言，擁有上述密碼，即可確認該電腦駭客業已進出不同的電腦系統，而駭客通常以此能力自誇。電腦駭客經常將一種名為 Sniffer 的軟體安裝在被侵入者的電腦系統伺服器中，以便他們蒐集更多的登入密碼。Sniffer 軟體能夠記錄其他合法登入該電腦的使用者識別碼與密碼。駭客擷取後並冒用該識別碼與密碼，宛如合法客戶一般。如果將該軟體安裝在大型的電腦網路伺服器上，即可蒐集上百筆密碼。非法安裝且使用該軟體即構成禁止竊聽法案的重罪。

電腦駭客另一項詭計就是侵入電腦系統後，下載或複製系統的密碼檔案。這類密碼檔案的用途乃是將所有合法的使用者密碼，集中在一個儲存區，基於安全的理由，這些密碼資料自動編譯成電腦碼，並以電腦碼的方式存放在某一檔案中。不幸的是有許多稱為 crack 的軟體，用來將前開電腦碼解譯還原成一般資訊碼。這類的軟體在網際網路上極易取得。因此，對於駭客而言，擁有

---

7 參閱第 432 期參議院公報，第 99 會期，第二次大會第九次會議（S. Rep. No. 432, 99th Cong., 2d Sess.9 1986）

8 United States v. Fernandez, 1993 U.S. Dist. LEXIS 3590

許多密碼或密碼檔案是一件稀鬆平常的事物。自從這類行為成為重罪規範對象，特調官對於涉嫌的駭客實施搜索電腦系統時，應該將重心放在大量的密碼資料或密碼檔案，以及屬於crack的電腦軟體。這類的證據的確能夠提高定罪率，因此大為激發檢察官的興趣。

3. 竊取身分識別的行為, 18 U.S.C. § 1028

在前述的概要中提到，因為 制訂 1998 年身分識別竊盜與偽冒防制法案而修正聯邦法第 1028 條。本條主要針對一項新穎的犯罪行為，稱之為「身分識別竊盜」。這項犯罪行為是利用電腦創建檔案的特性，建立一個偽冒他人或虛構的身分電磁資料。這種行為對於商業機構或金融機構已經造成巨額的財物損失，同時對被害人的信用額度造成長期而深遠的負面效應，現行條文主要的部分如下：（畫線為刪除部分，斜體字為增加部分）a 任何人如符合本項 c 款所指述之情形時，即

⑴明知且未經合法授權製作身分辨識電磁資料，或明知製作虛構的身分辨識電磁資料；

⑵明知該身分辨識電磁資料為盜贓物或未經合法授權所製作的，而予以傳輸；

⑶明知並以非法使用之意圖而持有或傳輸五份以上之⑴所列之虛構或偽造之身分辨識電磁資料；

⑷明知並意圖詐欺政府，而持有⑴所列之虛構或偽造之身分辨識電磁資料

⑸意圖製作偽造或虛構之身分辨識電磁資料，而製造、傳輸或持有相關之製作工具或工具母機；或

⑹持有政府之身分辨識電磁資料或相類似資料，明知該電磁資料係盜贓物或未經合法授權製作；或

*⑺非經當事人授權傳輸或而使用該當事人身分證明之方法，意圖從事、幫助、教唆任何非法行為，而該行為係觸犯聯邦法，或構成州及其所屬地區法律之重罪，*或預備從事上開活動之行為，

均應依據本項 b 款規定予以處罰。

最近立法通過的名詞定義，反映出使用電腦竊取善意第三人身分的科技能力，例如：

D：本款規定

⑴「文件製作工具」乙詞，係指任何沖軋器具、電子裝置或電腦軟硬體等項，特別設計或專用於製作身分辨識電磁資料或虛構的身分辨識電磁資料，或上開器具之工具母機。

⑵「身分辨識電磁資料」乙詞，係指經美國政府、州政府及其所屬單位、外國政府及其所屬單位、國際政府或等同國際政府組織等機構，針對特定個人之資訊、依據個人身分辨識之要求式樣或經一般認可之身分辨識，予以授權製作或核發之電磁資料。

⑶「辨識方法」乙詞，係指單獨或併同其他資訊所使用之姓名、數字，予以辨識特定個人，其包括：

(A)姓名、社會保險證號碼、出生年月日、各州或聯邦政府所製發的駕照，或辨識數字、外國人註冊號碼、護照號碼、勞工或納稅人辨識號碼；

(B)特定的生物檢定數據，例如指紋、聲紋、視網膜、虹膜影像，或其他特殊的生理表象；

(C)特定的電子辨識數字、位址、電腦碼，或

(D)電信辨識數據或登入裝置（參閱 1029 條(e)項）

⑷「個人辨識卡」乙詞，係指由州或所屬地方政府所製發之身分辨識文件，專屬身分辨識用途。

⑸「製作」乙詞，係包括修改、原創、組合。

⑹「州」係指美國任何一州、哥倫比亞特區、波多黎各自治區、或其他美屬自治區、託管地或其他美國領域。

所不同於第 1028 條的結論，本條增定(f)項處罰預備犯與陰謀犯，增訂(g)項規範沒收程序，以及有關建構的新規定（即(h)項）。

軍事上的特別考量

電腦駭客入侵的案件可能非常複雜，通常，調查官著手調查這類案件時，對於駭客為什麼要入侵電腦系統、駭客實際所在何處、駭客對電腦系統做了什麼以及多少敏感的區域已遭駭客登入、備份或破壞等等，僅有少量的情資。駭客入侵的動機從單純的增進侵入能力到間諜活動都有可能。

然而，網際網路提供全球性無遠弗屆的資訊能力，以及大量資料聚集在我們的電腦系統，對於所造成的危險性，我們將所有駭客入侵案件評估為最壞結果。

大多數駭客即使是生手，都知道電腦與其連線電腦之間，一般都會記載登錄時間、數據資料、網際網路通信協定位址。駭客為了避免留下自己的真實位址，於是運用數個第三人的電腦系統作為串接媒介物，穿越網際網路，以迂迴環繞等方式侵入被害人的電腦系統。當被害人發覺駭客侵入時，其電腦系統登錄資料僅顯示在這環鏈中與其連接的電腦系統位址。既無駭客真實所在的電腦位址，亦無所有遭駭客使用之媒介電腦位址。

以下略述電腦駭客如何運用自己的電腦與網際網路服務業。位於洛杉磯的駭客先以網際網路入侵加州大學的電腦系統，轉由加大的系統侵入芝加哥某大學的電腦系統，透過芝加哥的系統再侵入海軍總部與空軍總部的電腦系統。

空軍與海軍的系統登錄資料中僅能顯示侵入者來自芝加哥某大學的電腦系統，而非位於洛杉磯的駭客家中電腦或加大的電腦系統。雖然以回溯的方式追蹤每一部連接的電腦系統是查明駭客最直接的方式，但是聯邦法律對於此類蒐證程序卻大為複雜。一旦駭客以跨州或跨國的方式犯案，雖然在網際網路上界限是透明的，但是繁複的法律程序以及國內競爭者的利益常常混雜其中，並且消磨調查工作時效以致於無疾而終。

反制駭客

不論是電腦及時追蹤程式或者反制駭客程式，在理想的情況下，能夠追溯出駭客入侵路線，尚且需要一些運氣。但是實務上以偵查犯罪科技為名義的作為僅被核准一次。本文所述的反制駭客是一項特別的程式或是科技，藉此侵入他人的電腦主機來追查駭客，甚至可以查出其所使用的鍵盤。駭客喜歡侵入安全系統較為開放的電腦（例如學校、大學的電腦系統），藉由此類系統對目標電腦主機發動攻擊。駭客非常明白，使用愈多的電腦主機系統做為自身電腦系統與侵入目標電腦系統間之中介路徑，則其被發現的可能性愈低。因為調查官的作為必須符合聯邦法第 2703 條與 2511 條的限制規定，這二項規定在偵查中需要耗費時間來蒐證，如果駭客在中介電腦系統加入國外的網站，調查工作的複雜度將會更高。

試舉某一案例，在紐約市軍方所屬的「羅馬實驗室」，其中數部研究用途的電腦系統遭到入侵。這些電腦系統存放較為敏感的研究資料。就侵入情形，顯示駭客有系統的利用該實驗室的內部網路，去蒐整這些敏感的資料。其次，駭客利用該實驗室的電腦系統去攻擊其他電腦系統，包括國內的或國外的都有。駭客使用的科技不僅隱藏自己的真實身分，同時也使受攻擊的電腦系統誤判該項攻擊是美國軍事電腦系統所為。

當時，美國正與一些傳統上不與西方結盟的國家舉行高層會談。其中受到攻擊的電腦系統似乎位於其中的一個國家，因此引起高度重視。我們擔心該國誤認美國軍方對其電腦系統發動攻擊。經過數日努力不懈的追查，空軍特調處的探員追蹤到駭客所使用的網際網路服務公司。令人扼腕的是，業者所持有的客戶人事資料將會牽涉其中，如果以法院的命令要求業者提供，整個調查工作勢必曝光。就本案的疑難與重心，司法部最後核准使用反制駭客程式，但是也僅能查到網際網路服務業者這個階層。

反制駭客程式具有高度的侵略性，而且合法性令人質疑，似乎只有在極端急迫的狀況下，才會核准於偵查中使用。再者，偵查人員知道即便是經由相當授權使用，反制駭客程式也非萬靈丹，並不能保證一定成功。駭客通常都會修復曾經入侵的中介電腦系統，因為這類中介路徑會成為我們追蹤駭客的途徑。但是卻有許多部隊長認為反制駭客程式是捕獲駭客的最佳利器，因此軍法官必須認知這個現況，促使部隊長對於偵查駭客的作為上持有正確的期待，避免他們因為錯誤的認知而下決心，如此，偵查行動始能大有斬獲，這就是軍法官的責任。

協同偵辦

直到今日，經驗告訴我們，絕大多數的駭客都是非軍人。因此，對於駭客入侵案件通常涉及數個不同偵查機關與不同的管轄權。執法機關彼此間緊密與適切的協同偵辦，將有助於確認駭客

並將其繩之於法。

聯邦調查局（FBI）

除非有明確的證據顯示駭客為軍事人員，否則，我們建議主動聯繫聯邦調查局，因為他們對於被入侵的民間電腦系統具有管轄權。我們通常將案件進行的程度簡要的提供給聯邦調查局，由他們決定是否積極參與。即使案發時他們並不願主動參與，而事後發現犯罪者為非軍人，此刻，特調處的偵查立場如欲起訴被告時，仍需透過聯邦調查局協助。然後，特調處第二組以華府的「國家基礎建設保護中心」作為協調聯繫機關。這種機制能夠協助承辦幹員，對於聯邦調查局提供有價值的參考觀點與經驗上的指導。

軍事犯罪調查組 (Military Criminal Investigative Organization)

如果案件資訊顯示,其他軍種的電腦遭受入侵時，所屬的軍事犯罪調查組就必須立即提出簡明的摘要報告。這份資訊來源亦應送交特調處第二組，以便協調聯繫各單位軍事犯罪調查組。空軍電腦緊急應變小組亦應提供事件相關的處理細節，傳送至受害單位的電腦緊急應變小組參考。

州與地方政府〔State and Local Authorities〕

如果被侵害的機關為州或地方政府時，應考慮與該地方政府有關的電腦犯罪偵查部門聯繫，如當地並無此類部門時，則透過特調處派駐該地的調查官與地方政府聯繫。地方政府能夠提供相當的協助與人力資源，尤其是在現場履勘與搜索實施。

國際領域　〔International Aspects〕

如果在國際上與其他國家的偵查機關協同辦案時，協調聯繫的工作應儘早展開。有時某些國家的個別因素，使協調作業變的非常遲緩。國際間協同辦案應先與特調處第二組聯絡。一般而言，這類的聯繫工作都是由責任區內的電腦犯罪調查官或由特調處承辦。應經常與派駐各地的調查官保持密切的聯繫。

㈠**司法部〔DoJ〕**

如須聯絡未與美國簽訂執法條約的國家，司法部刑事處國際科建議先行聯繫該科。國際科能提供協同辦案的資訊以及該國現行法律規定。例如，瑞士法律規定對於國外執法機關，在其國境內實施犯罪偵查而與其國民接觸是非法行為。所有執法團隊的作為，例如訪談相關人員，須由瑞士的執法機關協助始可展開。請與特調處第二組聯繫，以便獲得更多有關司法部刑事處國際科的資訊。

㈡**聯邦調查局（FBI）**

聯邦調查局在大多數的國家設有分駐點，一般而言，與駐在國的執法機關保持良好互動關係，這是一個不錯的聯繫點。由於電腦犯罪案件都是急迫性質，往往需要特調處的電腦犯罪調查官直接與國外的執法機關對口單位聯繫，然而應變的時間太短，經由司法體系的運作往往使得偵查行動受挫，為了解決此一困境，透過不同的承辦單位，相互傳輸電腦犯罪有關科技細節，應可消除時間上的壓力。

㈢**國際刑事警察組織〔International Criminal Police Organization　INTERPOL〕**

國際刑警組織在跨國犯罪偵查中是一個具有相當功能性的組織。請聯繫特調處第二組獲得相關國際刑警組織的協助。

第六章－猥褻兒童圖文資料（Child Pornorgraphy），聯邦法第 2252 條與 2252A 條

簡　介

1995 年美國空軍在Hanscom基地對電腦業務實施檢查，其中發現不論是現役軍人或聘雇人員，使用公用的電腦登入有關色情或不正當的網站總計有 44,564 件。這些登入時數經過概估總計使用

743 個人力小時。（參閱該空軍基地不當使用電腦系統登入網際網路報告，1996.2.3）

空軍訓令 33-129 第 6.1.3 節 網際網路資料傳輸規定，嚴禁使用公用電腦下載色情資料，然而事與願違。就上開數據顯示以及電腦硬碟空間快速的擴張，空軍特調處已經設法減少違規案件數量，尤其是成人色情資料部分。這類事件通常屬於行政管理事務而非刑事犯罪案件，因此成為部隊長直接查詢事務。

另一方面，空軍特調處持續的追查有關猥褻兒童圖文資料的案件。依據聯邦法第 2252 條與 2252A 條的規定，對於明知為猥褻兒童圖文資料而有傳輸、持有、收受等行為應予刑罰。美國最高法院在 Osborne 案件[9]明確的指出，刑法對持有猥褻兒童圖文資料的施予處罰並無違憲的問題。此外，聯邦法第 2252 條條文中並未明示電腦這個名詞，但是卻已經適用在利用電腦傳輸資料部分（參閱 Maxwell 案件[10]），由於 Maxwell 案件判決的影響，促使立法者針對其他有關處罰妨害風化的條文，明確的將電腦傳輸列為運送的範疇，例如 1996 年的電信法案的部分條文（Telecommunications Act of 1996, Pub. L. 104-104, § 507 b, 110 Stat. 56, 137.）。立法者制定聯邦法第 2252A 條的條文內容，再次的強調電腦傳輸即屬運送行為。雖然在原條文上，藉著 1990 年犯罪控制法案的通過與修正，將電腦傳輸猥褻兒童圖文資料列入處罰，但是立法者在其他新訂的法案中，將電腦傳輸這個部分界定更為明確，因為國會議員擔心，在新的法案中如部分條文沿用舊有的禁止規定，一旦法院的判決推翻有關電腦傳輸的處罰規定，將使所有的法案都無法適用。

細節分析

聯邦法第 2252 條立法施行迄今已逾二十年，這是一個禁止在各州散佈「視覺上對於未成年人從事明確性行為的描繪」規定。本條經多次修訂，主要目的為跟上科技發展的腳步，增訂散佈行為適用在郵遞、交通運輸與電腦傳輸等方式。（諷刺的是，本條卻未使用「猥褻兒童圖文資料」乙詞，這個差異變得非常重要，討論如後）

由於電腦科技發展襲捲全球，軟體與日新月異的科技發展出一套新的圖形轉換技術（譯註：貼圖功能），致使這些猥褻兒童圖文資料的供應者利用這類圖形剪貼軟體，將實際上是成人的猥褻圖片，以剪接移植方式變成猥褻兒童圖片，最後實體上所呈現的是猥褻兒童圖片。由於聯邦法第 2252 條僅適用在「真正的」猥褻兒童圖片，因此圖形剪貼的功能反而成為犯罪者鑽研的漏洞。

國會議員針對猥褻兒童圖文資料有所回應，通過 1996 年猥褻兒童圖文資料防治法案，該法案於 1996 年 9 月 30 日公佈施行，其中有二項重大改變。第一：本法案訂定新的條文即聯邦法第 2252A 條，其中特別針對圖形剪貼軟體將成人猥褻行為移植為兒童之圖片，並且認定為「猥褻兒童圖文資料」（Child Pornorgraphy），第二：透過猥褻兒童圖文資料防治法案，明確的定義「猥褻兒童圖文資料」的意涵。這個定義納入聯邦法第 2256 條第八款以及(B)項的條文中，其中規定：以視覺所能認知的方式，描述「真實的」或「看起來可為認定」未成年人從事明確的性行為。本條對於所謂保障言論自由的憲法爭議提供明確的指引方針。

讀者須注意的是，一旦依據聯邦法第 2252 條起訴被告時，檢方必須舉證猥褻圖片中未成年人其年齡確未滿十八歲（參閱 Russell 案件與 Smith 案件[11]，如被告坦承圖片人物確未滿十八歲，此時需要一位受過 Tanner Staging 圖片鑑定法訓練的專業鑑定人來判別圖片人物年齡。Tanner Staging 圖片鑑定法是一種通識協定，針對某些身體表徵諸如：頭髮、胸部或身體其他部位發育情形來推定當事人的年齡，因此圖片中的人物必須是正面的，而且有夠大尺寸的圖片與相當品質的畫質始能進行 Tanner Staging 圖片鑑定法。特調處有數位幹員受過該訓練並能提供鑑定服務。

1998 年 10 月 30 日，柯林頓總統簽署 1998 年兒童性侵害防治法案，其中對前述法案有數項重大改變，同時也放寬對定義的解釋。大多數學者認為，其中最重要的改變是對於聯邦法第 2252 條與第 2252A 條的修正。這些修正對於持有猥褻兒童圖文資料的人士表明不再抱持寬容的態度。在

---

9 Osborne v. Ohio, 495 U.S. 103, 1989

10 United States v. Maxwell, 42 M.J. 568, 580

11 United States v. Russell, 47 M.J.,412, 1998 and United States v. Smith, 47 M.J., 588, N.M. Ct. Crim., App.,1997

此之前，檢方對於持有猥褻兒童圖文資料的罪犯，必須舉證被告持有三張以上始能定罪，如今只要查獲被告持有一張以上即可定罪。修正條文也針對持有猥褻兒童圖文資料的被告，增訂明確正當可為抗辯的理由。增訂條文列入聯邦法第 2252 條(B)項與 2252A 條(D)項。這些得為刑事犯罪抗辯理由為⑴被告擁有三張以下的猥褻兒童圖文資料而且；⑵被告並未容讓執法人員以外的其他人觀看或複製，立即本於真誠地(A)採取合理的作為銷毀每一張圖文資料，或者(B)逕向執法機關報告並使執法人員取得每一張圖文資料。

上開敘述將這二項條文差異性予以標明，以下將探討條文的定義與一般爭議事項。大多數的名詞定義規範在聯邦法第 2256 條。例如本條第一項：未成年定義為「未滿十八歲之自然人」。第二項：明確的性行為定義為「真實的或模擬的」(A)性交，不論是同性間或異性間之生殖器與生殖器、口腔與生殖器、生殖器與肛門的交合；(B)與動物性交；(C)手淫；(D)殘酷的或自虐的性虐待；(E)淫穢的（lascivious）展示自然人的生殖器官或外陰部（參閱 A 至 E 款規定）。雖然法條對於淫穢的（lascivious）乙詞並無定義，但是依據 1979 年第五版的布萊克法律大辭典 794 頁定義該詞為：「意圖激發性慾的、猥褻的、不潔的、淫蕩的或不道德的行為，在性慾的關聯上剝除人類的道德感，參閱 Swearingen 案件[12]。

上述條文部分的款項尚且處罰以跨越州際方式交易猥褻圖片。Carroll 案件[13] 可謂首件針對電子傳輸猥褻圖片，並以網際網路進行跨州交易的聯邦犯罪案件（譯註：在美國有許多犯罪行為如跨越州界後，其管轄權即屬聯邦法院，否則仍屬州立法院，例如武器、毒品的運送、販賣、綁架等）。聯邦軍事上訴法庭在 Smith 案件[14] 對相同事實持相同的意見，而且判決內容對於保護客體邁進更大一步。本案認定就網路上的虛擬空間而論，電子資訊傳輸交易不論跨州或只是隔一條街，只要經由網際網路就是屬於跨越州界交易，即使所有的聯絡方式僅僅透過內部網路系統亦同。這種的定義解釋相當寬廣，但卻非由空軍軍事法庭或聯邦地方法院所提出的。因此，精明的幹員在調查州際交易猥褻圖片時，自當知曉對於運送方式應負舉證責任。

Simpson 案件[15] 是另一有趣而且觸碰相同議題的案件，尤其是法院對電腦內部的運作，以及如何就一份已經儲存在電腦內部的電磁記錄檔案，回溯追查到該檔案在網路下載期間的痕跡，均有深入的討論。本案緣起於 Tulsa 警察局的員警，從一位聯邦調查局的幹員口中得知被告 Simpson 經常進出猥褻兒童圖片區的專屬聊天網站，被告經常在網站上提出買賣猥褻兒童圖片的要約。當警方查扣被告的電腦後，在他硬碟中發現數張猥褻兒童圖片檔案，但是檔案名稱、數據資料均與原始下載的圖片檔案不符，被告辯稱這些圖片資料與下載區的圖片數據不符，因此檢方自無認定被告州際交易猥褻兒童圖片之可能。但是上訴法院的判決認定：

> 「就檢方所提出的證據，證明被告的電腦中存放二張猥褻兒童圖檔。檔案的名稱實質上與被告在網路下載區的檔案名稱相似，縱使被告從網路所下載的圖檔已被刪除，但是依據檢方所提出的鑑定人鑑定意見指出，此類情形係因電腦使用者（被告）從網路下載檔案後予以複製，保留複製的檔案而刪除原先的下載的檔案，這是相當合理的推斷。因此，被告雖然刪除原來的證據檔案，但是卻無法除去被告犯罪行為的事實。」

最後，有關立法者對於州際交易範圍的定義，因為 Bausch 案件[16] 的判決而被放寬到極致。本案被告 Bausch 曾經分別對十五歲與十六歲的少女拍攝裸照，這些裸照不僅暴露生殖器官，同時模擬許多性愛動作其中包含口交的動作。被告不服初審判決並上訴提出答辯，認為國會無權對於屬於州立法事務予以制定法律，例如州內的違法買賣行為。被告並且提出抗辯其拍照地點並未跨越州界，亦未將照片傳送給州界以外的任何人。因此認為檢方對其跨越州際犯罪行為並無證據。雖

12 Swearingen v. United States, 161 U.S., 446, 1896
13 United States v. Carroll, 105 F., 3d 740, 742 1st Cir., 1997
14 United States v. Smith, 47 M.J. 588 N. M. Ct. Crim., App., 1997
15 United States v. Simpson, 152 F. 3d 1241 10th Cir., 1998
16 United States v. Bausch, 140 F. 3d 739, 8th Cir., 1998

然上訴法院同意被告所提出的事實，但是也認定國會對於實質上跨越州際交易的犯罪行為有立法權。同時上訴審判決同意初審判決無誤，認定被告行為屬於州際交易行為，因為被告所使用的照相機是日本製的，這台相機是經由州際或國際交易方式運送至被告。

立法者在起草修正州行政法（Public Laws）第 105-314 條時，顯然將上述判決牢記於心，這項法案於 1998 年 10 月 30 日公佈施行。另修正聯邦法第 2251 條第(a)(b)兩款，其中包括製作猥褻兒童圖文資料所使用的器具係以州際或國際交易方式經由郵遞、海陸空運或電腦傳輸方式所運送，即屬州際交易之犯罪行為。

1997 年美國聯邦第九上訴巡迴法院審理 Lacy 案件[17]，被告抗辯檢方獲得搜索票的理由已失時效性，不足以支持搜索的正當性，因此對於搜索行為以及搜索所得的證物均屬無效。但法院明確的表示，被告長期蒐集猥褻兒童圖文資料適足證明其個人癖好。本案發生緣起 United States Customs Service 公司發現某些美國的客戶自丹麥國的電子布告欄（BBS）下載猥褻兒童圖檔，該公司透過電話通聯記錄以及網路登入記錄，確認被告 Lacy 先生登入該電子布告欄 16 次，下載六份含有猥褻兒童的圖片檔案。於是該公司轉知檢方申請搜索票搜索被告住處，其中扣押被告所有之電腦、100 份以上的電腦磁片以及數種不同類型的文件資料。之後檢驗被告電腦的硬碟，發現數份未成年人從事性行為的圖檔。被告上訴時聲明，有關申請搜索票的理由在時間點上不具效力，因為被告距申請搜索票前最後一次登入該電子布告欄，已超過十個月的時間，之後其他數個類似案件亦持相同的論點抗辯。然而負責調查的檢調人員到庭證稱，「依據受訓時所教導的理念以及日後累積的辦案經驗，蒐集或製作猥褻兒童圖片的人，通常非常珍惜此類圖片，不輕易毀棄，並且將這些圖片長時期的儲存在隱密安全的處所，而家中的電腦正是最佳的存放地點」。法院判決認為此種發現犯罪後而遲延數月申請搜索票或執行搜索的理由是合法的。例如 Bateman 案件[18]（遲延 7 個月）、Rakowski 案件[19]（6 個月）、Lamb 案件（5 個月）[20]。

軍事上的特別考量

美國統一軍法典對於猥褻兒童圖文資料並無處罰規定，但是在軍法典總則條款第 134 條（Article 134, UCMJ）規定，軍法機關得準用聯邦法第 2252 條與 2252A 條。因此任何一位軍事人員如觸犯前開法律得由軍法機關或司法機關審判。

如軍事人員使用公用電腦下載猥褻兒童圖文資料圖片，即可依據軍法典第 92 條的規定論以違反命令或一般法規罪責，而空軍訓令 33-129 條網路的資訊傳輸規定即可謂命令或法規。有關特別的禁止規定集中在 6.1.1 條至 6.1.12 條。以下將集中討論適用兒童（成人）猥褻圖片的規定

6.1.1 凡使用政府提供之電腦軟硬體設施，在網際網路上從事非職務或非經授權業務範圍之行為。

6.1.2 從事私人性質或商業收益行為，包含（非僅限於）連鎖信、商業要約或買賣個人財產等行為。

6.1.3 儲存、製作、展示、傳遞或以其他方法，傳送侮辱性或淫穢性的語言、物品。侮辱性的物品包含（非僅限於）激發仇恨心裡的作品，諸如：種族主義的刊物、資料、標誌等（例如，納粹的十字標誌、新納粹文字刊物等等），以及性騷擾的物品。至於淫穢性的物品包含（非僅限於）色情圖像，以及其他詳細描繪性愛的物品。

6.1.4 於未經核定的電腦系統上，儲存或處理分類保密資料。

6.1.5 未經原創者或出版者的同意，儲存或處理著作權保護的物品（包含卡通圖畫）。

6.1.6 非公務所需，或事後未經認可，透過公關事務頻道登入聊天網，參與公開討論事務。

6.1.7 未經授權、允准，使用他人的密碼或識別碼登入電腦系統。

17 United States v. Lacy, 119 F. 3d 742, 9th Cir., 1997

18 United States v. Bateman, 805 F. Supp. 1041, 1043 D.N.H., 1992

19 United States v. Rakowski, 714 F. Supp. 1324, 1330 D. Vt., 1987

20 United States v. Lamb, 945 F. Supp. 441, 459 N.D.N.Y., 1996

6.1.8 未經授權、允准，觀看，更改，毀損，刪除或阻滯他人登入電腦系統或通信系統
6.1.9 未經事前的授權或核准（例如以正當的測試系統方式或檢查電腦安全系統方式等理由），企圖使用電腦程式以矇混方式登入或摧毀電腦的安全措施或認證程式
6.1.10 於侵害軟體販售權人的契約狀態下，獲得、安裝、複製、儲存、使用該軟體。
6.1.11 允許未經授權之個人，登入政府所有或供公務用途之電腦作業系統。
6.1.12 未經電腦作業系統管理者的允准，修正或變更電腦網路　作業系統或設定參數。

此外，軍官如違反本規定時也構成軍法典第 133 條違反官箴罪（Conduct Unbecoming an Officer）。

最後，調查官得對軍中聘雇人員實施偵查，因此聘雇人員仍然受到聯邦法或州法的管轄。依據聯合品德規範（Joint Ethic Regulation　JER）與空軍訓令第 36-704「紀律與違反規定行為」中明定，聘雇人員非因公務目的不得使用政府財產。有關標準設立在聯邦法規（Code of Federal Regulation CFR）2635.704 的條文中，即「政府機構之受雇人，有保護並維持政府財產之義務，在非經授權情形下，不應使用或允准他人使用該財產」。依據聯合品德規範（JER 2-301,a）的規定，通訊系統與設備包含電腦、電話、傳真機等，僅允許公務用途或經授權使用。有關「公務使用」與「授權後使用」這二項名詞在聯合品德規範 2-301, a⑴、2-301, a⑵均有明確定義。這二項條文規定，如分別經由指揮官與其主管單位同意時，個人於非公務用途上，得有限度的使用上開通訊系統與設備。因此，讀者們必須留意，並非所有的聯合品德規範條文是前後一貫的，因此，在起訴違反聯合品德規範等犯罪時務必謹慎。在空軍軍法專刊（OpJAGAF 1996/70，1996.5.6）有一篇相當不錯的文章可為參考，即討論如何起訴違反聯合品德規範之規定而使用政府財物之犯罪。

第七章－ 1980 年隱私權保護法案：聯邦法第 2000AA 條

簡　介

1980 年隱私權保護法案（The Privacy Protection Act of 1980）乃是立法者回應最高法院對史丹福大學日報的判決[21]所制定的法案。本案起因於史丹福大學發生學生暴動，數名持木棍的學生打傷數名警員。二天之後，史丹福大學日報（Stanford Daily）刊載一系列有關暴動的報導，其中刊登數張現場暴動的照片。由於警方僅能指認其中二名加害人，因此希望從日報所拍攝的照片來指證更多的暴民。次日，地檢署以緊急搜索方式搜索報社辦公室，希望取得相關照片、底片與膠卷，以及能夠舉證加害人施暴的證物。諷刺的是，搜索所得之相關暴動照片均已刊載報紙上，因此並無扣押物。聯邦地方法院北加州分院判決檢方執行搜索不當，因為報社並無犯罪事證，自不應成為犯罪嫌疑人。而上訴法院更進一步的認定，舉凡對新聞媒體查無犯罪事證，媒體就應得美國憲法第一修正法案（新聞自由）對於搜索限制的保護。然而最高法院卻推翻上開判決，並認定檢方執行的搜索並無瑕疵。因此導致憲法學者與新聞媒體遊說國會，以立法來維護憲法第一修正法案。

簡言之，本法案規範執法機關在缺乏緊急的情形下，必須以傳票傳喚當事人到庭的方式，藉以取得客觀上可認定之出版文案資料。除非有相當事證足認當事人持有之文案資料為犯罪物或現正從事犯罪之物。依據本法案規定，執法機關或執法人員執行搜索或扣押，如違反本法案相關規定，當事人得對機關或執法人員個人提出民事侵權損害賠償訴訟。

細節分析

雖然起初設計隱私權保護法案的目的，主要是保護一般傳統的出版業者，例如媒體以及文字出版物的作者，然而對於電腦犯罪的偵查工作卻產生不小的衝擊。參閱 Steve Jackson Games, Inc 控告美國特勤局案件。[22] 以下針對法案對於以搜索票獲得文書證物的禁止規定予以歸納四點例外情

21　Zurcher v.Stanford Daily, 436, U.S. 547,1978
22　Steve Jackson Games, Inc. v. United States Secret Service, 816 F.Supp.432, W.D. Tex., 1993

形：參閱聯邦法第 2000aa 條(b)款

⑴具有合理的事證足資認定，當事人持有的文書資料為犯罪工具或為預備犯罪之用。

⑵具有合理的事證足資認定，如立即扣押該文書資料即可避免重大的人身傷亡。

⑶具有合理的事證認定，如改以傳票方式要求當事人到庭提供該項文書證據時，恐將致該項證據資料毀損、變造或被隱匿，或

⑷ a、該項文書證據業經法院票傳當事人到庭提供卻不可得，且經一切上訴救濟方式亦不可得；b、經合理的判斷認定該拖延行為將造成司法利益受損。

對於 Steve Jackson Games, Inc 案件與 Davies 案件的搜索權限部分，必須明瞭二者案情相仿但法院判決迥異。這二件判決的差異性足以說明調查官應採取二項步驟，來避免任何潛在的法律爭議。首先，幹員應儘速對於扣押的文書資料進行檢驗工作，因為這些文書資料雖然體積龐大，但是易於發現證據，因此，快速的審查可減少不必要的法律責任。其次，幹員對於當事人請求發還扣押文書資料部分應謹慎處理。換言之，執法官員面對當事人請求時，並非儘速的辦理發還事宜，而是應立即進行文書資料查驗工作，並立即聯繫法務部門請求法律專業諮詢。調查後續發展如認定須再次扣押該項文書資料時，幹員於前次的扣押作為中，越早發還扣押物就越能減輕檢方的法律責任。

軍事上的特別考量

軍方的特調官並不常偵辦涉及隱私權保護法案的案件，然而特調官仍應對此類案件保持高度謹慎，只要有所疑慮，在採取任何偵查作為時，立即聯絡當地的特調站或空軍特調處人員請求提供諮詢意見。

第八章－搜索與扣押的討論

簡　介

當我們討論搜索與扣押時，首先必須構思：從搜索的電腦系統中究竟能夠得到什麼？應採行何種程序？現行法律並未提供所有問題的解答。犯罪調查案件，往往從案件本身尋找事實真相。軍法官依據以往諸多具有指標性的判決意旨，研擬「調查官搜索要點清單」詳如附錄。主要的目在協助調查官，將偵查焦點放在隱私權的例外情形。當一切情資蒐集齊備後，軍法官才能確認被告在本案調查的事物或地點上，是否具有合理可期待的隱私權。

第二、第三章曾分別指出，當國會通過電子通訊隱私權保護法案（ECPA）時，同時也對網路服務業者的合法用戶，創造出合理可期待的隱私權。電子通訊隱私權保護法案的條文詳盡的規範執法機關應於何時或應如何從公務電腦系統中存取資訊時，然而對於私人所有的電腦系統的規範付之闕如。更糟的是該法案對於存取公務系統資訊卻是提供一個令人混淆的指導方針，僅有少數幾份判決提及公務電腦系統的隱私權。因此，我們必須從其他的案件判決中尋找答案，但是這些案件卻與電腦系統無關。

細節分析

1.第三人所行使的同意權

調查官應注意經第三人同意的範圍內，對於搜索可能出現直接性或間接性的限制[23]。具有同意權的第三人可能會對搜索區域內與他人共同持有的電腦，提出搜索範圍的限制，或因共有約定而使第三人無權同意搜索。總之，第三人會採取一些必要步驟保護其所有財產。

a.經由主管機關同意或命令

當調查官得到當事人的同意而取得電腦系統、帳號或相關資訊數據時，此時無須申請搜索票[24]。然而，調查官仍須保持高度謹慎，電腦系統中某些區域或檔案並非屬於公開共享部分，或者

---

23 United States v. Griffin, 530 F.2d 739, 744 7th Cir. 1976; United States v. David, 756 F. Supp. 1385 D. Nev. 1991

24 Schneckloth v. Bustamonte, 412 U.S. 218, 219 1973; Military Rule of Evidence 314 d

就所有的事證顯明該電腦系統屬於專責人員權限，因此該電腦系統中仍可能具有法律上所認可的隱私權。不過，運用電腦使用警語或使用者條款（如附錄），應能解決這項爭議。

b.雇主的同意

政府機關對於人身與個人財產的保護在憲法第四修正法案有詳盡的規定，對於無令狀搜索政府機關聘雇人員，搜索範圍必須限定與工作相關或是屬於行政管理事務。因此在雇主同意的情形下，對於無令狀搜索是否恰當，應先考量當事人在聘雇的關係上是否具有合理可期待的隱私權。

c.親屬

父母、配偶以及民營的雇主可歸類於第三人，得授權准予實施搜索。就Matlock的案件與Pollock案件[25]判決結果，法院認為父母對其未成年子女實施電話監聽的行為是正當合理的。雖然判決僅針對有線通訊部分，但是依據判決的法理，同等適用於電子通訊部分。另Reister案件判決[26]，法官認定代管房屋之人有權同意檢方搜索該屋屬於房屋所有人之寢室，並得扣押其日記。

獲得同意權對於偵查犯罪有諸般利益。而同意權包含直接與間接的方式，就 Milan-Rodriguez案件判決為例[27]，當事人向警方指明門鎖鑰匙所在就是間接的同意方式。同意權必須出於自由意願[28]，而且對於自由意願有所爭執時，檢調人員須負舉證責任[29]。

2. 緊急情況

電子數據資料易於毀損，因此在電腦犯罪偵查中確立了緊急情況的法理。電子數據資料容易受到溼度、溫度、震動、數據殘裂等因素的影響，僅是單純的磁場作用，就能在數秒之間毀損數據資料。所謂緊急情況定義如下：當發生毀損證據的情況是急迫的，而且有客觀的事證認定該證據可資證明犯罪行為者，則無令狀搜索與扣押是正當的[30]，而緊急情況的法理適用於：在客觀的認定下，當執法人員認知到室內人員需要「立即的協助」，藉以避免相關事證遭受毀損、或阻止嫌犯脫逃、或避免其他執法人員無法有效達成執法任務等等[31]。在適用緊急情況的法理時，必須考量下列：

(a)緊急的程度。

(b)申請獲准搜索票所需時間，包括電話申請方式的時間。實施偵查人員如有充裕的時間（30分鐘之內）以電話申請搜索票時，緊急情況即無適用，如果於充裕時間內不以電話申請搜索票，卻以等待方式消耗時間使情勢成為緊急情況，然後據以實施無令狀搜索為無效搜索[32]。搜索之證物是否有湮滅或搬移之虞。

(c)搜索區域發生危險之可能性。有情資顯示，違禁物品持有人已經得知檢調單位開始對其實施偵查，而且該違禁物品有毀損之虞。

無令狀搜索，就一般人的客觀認知如認必要時，即具正當性[33]。如果調查人員判斷在客觀上是合理的，即使事後發現是錯誤的，通常法院認為無令狀搜索仍具正當性[34]。

雖然理論上無令狀搜索可以適用在電腦硬體設施（硬碟、主機）的搜索與扣押，但是實務上，執行搜索此類物品仍須具有搜索票[35]。以Brown案件判決為例，法院認為警方發現被告正在刪除電腦檔案時，以緊急情況逕行扣押被告電腦主機內的備忘錄程式，此種無令狀搜索與扣押是正當的，但是當警方於扣押程式後，如欲登入被告電腦主機去搜尋備忘錄所記錄的檔案時，警方則必須另行申請搜索票。法官特別把電腦主機與檔案資料，以容器與容器內裝物品比喻，以緊急情況查扣

---

25 United States v. Matlock, 415 U.S. 164 1974; Pollock v. Pollock, 154 F.3rd 601 6th Cir. 1998

26 U.S. v. Reister, 40 M.J. 666 N. M. Ct. Crim. App. 1994

27 United States v. Milan-Rodriguez, 759 F.2d 1558, 1563-64 11th Cir. 1985, cert. denied, 474 U.S. 845 1985

28 United States v. Scott, 578 F.2d 1186, 1189 6th Cir 1977, cert. denied, 439 U.S. 870 1978

29 United States v. Price, 599 F.2d 494, 503 2nd Cir. 1979

30 United States v. David, 756 F. Supp. 1385, 1392 D. Nev. 1991; United States v. Talkington, 875 F.2d 591 7th Cir. 1989

31 United States v. Arias, 923 F.2d 1387 9th Cir., cert. denied, 502 U.S. 840 1991

32 United States v. Patino, 830 F.2d 1413, 1416 7th Cir. 1987, cert. denied, 490 U.S. 1069 1989

33 United States v. Reed, 935 F. 2d 641, 642 4th Cir. 1991, cert. denied, 502 U.S. 960 1991

34 United States v. Arias, 923 F.2d 1387, 1391 1991; Reed, 935 F. 2d at 642

35 United States v. David, 756 F. Supp. 1385 D. Nev. 1991

容器的行為是正當時，並非等同獲得法律的授權，對內裝物品得實施無令狀搜索[36]。

3. 對外公開

「當事人自願的將資訊向第三人公開時，第三人再將該資訊告知政府機關時，不論是主動的方式或依據先前的約定，政府機關無須另行申請搜索票來獲得該資訊，其依據理由是當事人明知並承擔第三人向政府機關洩漏該資訊的風險」，參閱波士頓大學法學專刊論文「搜索數位化資料之要件」[37]，而實務上亦採此見解以及 Miller 案件判決[38]。此種情形自可成為個人所期待之隱私權是否合理存在的考量因素。例如Horowitz案件的判決[39]，被告將公司（惠特尼飛機製造公司）列為機密的價格資料出售給公司的競爭者（EMI 公司），這份價格資料是一份電腦檔案，經由被告非法複製並儲存至 EMI 公司的電腦。聯邦調查局對 EMI 公司執行搜索時找到這份複製的檔案，而被告辯稱他個人在這份電腦檔案中擁有合理可期待之隱私權。上訴法院在判決中反駁被告的說法：「雖然被告內心非常希望對公司隱藏他個人的惡行，但是被告以不法之所有販售公司機密資料時，即已主動的將資料向 EMI 公司公開，此時被告對這份檔案業已捨棄曾經所擁有合理可期待的隱私權。」

4. 合法逮捕後所衍生的搜索

逮捕被告後，對其所藏匿的武器實施無令狀搜索是允當的[40]，而搜索的範圍必須以受逮捕者的人身，以及在拘捕過程中受逮捕者所能掌控的區域為限。這個區域包括被逮捕者可能獲得武器或毀損證物的範圍。就 Chimel 爾案件[41] 判決可知，警方因逮捕行動而扣押某些物品，但是未必能夠逕行搜索該物品。例如，在逮捕過程中，扣押被告的呼叫器，然而這項電子產品受到 1986 年電子通訊隱私權保護法案的保護，除非警方先行獲得搜索票，否則就不得搜尋呼叫器中的資訊。這種情形亦適用於個人數位資料處理器（PDA）或掌上型電腦。

5. 一目了然原則

當檢調人員處於合法的地理位置，經由目視直接看到證物以及相關犯罪的特徵時，得以無令狀搜索的方式逕行搜索與扣押該證物[42]。就目視的觀點，經由搜索票所扣押的電腦並非當然具有證據能力。「一目了然原則」在電腦犯罪調查中佔有重要的地位，例如，發現犯罪嫌疑人正坐在電腦鍵盤前，非法的傳輸資料或者進行可疑的犯罪行為。

6. 具狀扣押電腦硬體、軟體或電子資料

檢調人員在申請搜索票前，必須具有正確的資訊足以構成申請搜索票之理由。檢調人員如欲搜索電腦、軟體或其他與電腦相關的周邊設備時，由電腦專業人員所提供的情資即能確立客觀合理的搜索理由。以 Henley 案件的判決[43] 為例，美國空軍覆判庭認定：「當正當可供參考的事證被提出時，簡易法庭的法官有權審酌並決定搜索的理由存在與否」。本案為亂倫案件，空軍指派心理學專家參與調查，該名專家審閱案件相關資料後並提出鑑驗意見，推論被告具有異常而強烈的個性，極可能將過去性侵害的行為加以記錄保存。這位心理學專家告知偵辦特調官，所有整合的資料顯示犯罪嫌疑人是戀童癖者。之後，特調官從Seth先生所寫「對於兒童的性侵害」（The Sexual Exploitation of Children by Seth Goldstein）的專論文章中反覆研究，文中敘明猥褻兒童者的共通性格中包含蒐集有關性行為的詳細資料，並保存完善，而且甚少丟棄其所蒐集的資料。經綜整上開專家的意見、被害人的指述及其他的調查情資，簡易法庭的法官終於核發搜索票搜索被告住家。搜索後發現並扣押錄影帶 1000 支以上，錄影設備含攝錄影機以及為數眾多的色情雜誌，其中有兒童裸體或同性性行為的圖片。本案經簡易法庭移送軍法後，軍法審判官判決認定司法機關的法官

36 Texas v. Brown, 460 U.S. 730, 750 1983
37 Warrant Requirement For Searches of Computerized Information, 67 B.U.L. Rev. 179, 185 1987
38 United States v. Miller, 425 U.S. 435, 442-43 1976
39 United States v. Horowitz, 806 F. 2d 1222 4th Cir. 1986
40 United States v. Robinson, 414 U.S. 218, 234-36 1973
41 Chimel v. California, 395 U.S. 752, 762-63, 768 1969
42 Horton v. California, 496 U.S. 128, 136 1990
43 United States v. Henley, 48 M.J. 864 A. F. Ct. Crim. App. 1998

（簡易法庭）核發搜索票所依據的理由充分而正當，同時駁回被告請求法庭捨棄扣押物具有正據能力的聲請。被告上訴後經空軍覆判庭以相同的理由駁回被告的聲請，判決因此確定。

a、搜索區域

搜索電腦網路系統（Networked computer）時，敘明搜索處所是相當困擾的。因為此類已經儲存的資訊在電腦網路的系統中，其所在的地理位址實際上是不明確的。如果查明這些資訊是存放之電腦系統位於同一管轄區但非屬同一網域時，檢調人員必須再行聲請搜索票。因此，在同一管轄區內有數個網點系統，雖可就一份搜索票進行多點搜查，但是在此強烈建議個別申請方式實施搜索較佳。因為同一網域跨越數個管轄區域時，檢調人員必須向簡易法庭的法官報告後始能獲得搜索票。如果資訊存放的網點不明時，法官核發搜索票前就必審慎考量。因為電腦資訊存放在不同網點時，搜索票必須加以註明。

有關搜索區域較為貼切的敘述：「持搜索票的檢調官員，憑藉著客觀合理的判斷即能標定搜索地理位址」。司法部的指導要領建議檢調人員，儘可能的針對每一個地理位置來申請搜索票。因此，以一個明確的地理位置對應一張搜索票是較佳的作為。（譯註：網域與網點位址是虛擬空間，依據所存放之主機決定其地理位置，不易描繪地理位置所在）

b、物品的扣押

檢調人員對所欲扣押之物品，應於搜索票上逐項詳列並予敘明。在大陪審團案件（Grand Jury Investigation, et al. v. United States, 130 F. 3d 853, 9th Cir. 1997) 的判決中指出，「國防部犯罪調查局、聯邦調查局與太空總署的幹員在執行對 SSDI 公司的搜索時，有關搜索的項目過於廣泛」。本案的 SSDI 公司是一家半導體供應商，負責對國防部與國防部所屬的簽約商供貨，經人檢控該公司供應非合約規格之商用半導體。調查單位的幹員，依據檢控資料所載實施搜索，法院發現上開單位所欲搜索與扣押之物品，竟是該公司過去五年內高達百分之九十的資料與貨品，其中包括電腦、電腦資料儲存設施，以及 2000 件以上的公文檔案櫃與公文檔案夾。

同樣的，有關「同意」的字眼也相當關鍵。對一位幹員而言，如欲搜索一個房間或是一列住宅，僅僅獲得個人的同意是不夠的，如果搜索一台電腦，幹員不僅需要所有人同意的意思表示，同時也要獲得其對電腦內所存放的資訊同意搜索的意思表示。因為電腦僅一單純儲存裝置，對於內部的檔案尚須明確的敘明搜索必要性，否則雖能扣押電腦，但卻無法進一步觀看內部檔案內容。在處理猥褻兒童圖片檔案時，除扣押電腦之外，與電腦搭配的螢幕、列表機應一併查扣。因為偵查人員在檢驗證物時，須確認該器具與被告在觀賞證物時的器具相同，Carey 案件[44] 可為此類狀況之範例。本案實施偵查之警員針對疑似運毒案件因被告同意對其住所實施搜索，在搜索中發現房內放置電腦一部，於是另行以搜索毒品為由聲請取得搜索票，企圖搜尋電腦內部存放與本案相關的證據。警方登入電腦主機後發現一些 jpg、bmp、gif 等規格的圖片檔案，於解碼後播放後發現均為猥褻兒童圖片，於是警方持續解碼並播放此類規格檔案。被告以持有猥褻兒童圖片罪起訴。地方法院判決認定該搜索所得之猥褻兒童圖片具有證據能力。聯邦第十上訴巡迴法院則予以判決發回更審。因為當時所核發之搜索票欲搜索扣押之物品，並未涵蓋這些猥褻圖片。同時也反駁檢調人員的論點，上訴法院認為這些猥褻圖片絕非在偶然、無意間之情形下所查獲。因為檢調人員證稱發現猥褻圖片時，即推論其他相同名稱檔案亦屬猥褻圖片，並非起初所懷疑的運毒證物。再者，上訴法院認為一旦檢調人員發現猥褻圖片時，就有義務去聲請取得另一搜索票，以修正搜索證物內容，或者取得被告同意的意思表示後，續行解碼上述檔案並扣押之，此乃為合法作為。

本案主要精神在於「搜索扣押的明確性」。憲法第四修正法案特別嚴禁檢調人員搜索扣押踰越搜索票所列載之範圍。因此在決定搜索的範圍時應謹慎考量。至於搜索密碼資訊，應先將其解碼譯成原文。如果經由當事人同意的意思表示而實施搜索，密碼資訊就成為搜索的界線，換言之，當資料無法解碼時，就應聲請傳票要求被告交出解碼資料，否則即以藐視法庭罪起訴。而被告拒絕時，軍法檢察官於起訴被告藐視法庭罪或拒絕服從法令罪時，應將被告拒絕接受搜索票所列事項交出解碼資料等情狀，予以分析詳述。

44　United States v. Carey, __F.3d ___ 10th Cir. 1999

c、物證移離搜索區域之分析

非列載區域之搜索，在合理的情形下是允許的。但須審慎考量搜索票所載區域延展限制、電腦系統設置所在建築物之型態。

如果搜索票允許的範圍是寬廣的，就能將大量的文件資料予以搬遷。反之，檢調人員則須區分搜索票列載以及未列載的資料。一般而言，搜索的處所是家庭居所，法官對於檢調人員「先扣押、再分類」的辦案態度比較寬大些。如果搜索區域是公司機關，扣押大量的資料則會導致公司機關運作癱瘓。因此搜索公司機關的電腦設施時，法官大都不同意檢調人員扣押所有與電腦相關的證據資料。因為扣押所有電腦資源後，會使無辜的員工暫時喪失工作機會。然對搜索住家，法官通常允許扣押全部物品。因此，檢調人員必須注意所謂現行「居家辦公」的普遍性，以及電信通訊的新趨勢：透過網路系統居家經營事業。再者，扣押電腦後，因檔案證物數量龐大或者扣押時技術上的失當，極可能毀損其中數據資料。有關指導原則請參考司法部所製頒的「指導方針」第四部分 H 項，以及第四部分補充要點。（DoJ Guidelines, Part IV, § H. DoJ Guideline Supplement Part IV）

d、電腦硬體與軟體的扣押

電腦成為犯罪工具且為犯罪者所擁有時，最好的方式就是扣押該設備，以阻止犯罪侵害持續進行。例如，利用電腦傳輸違禁資料，此時立即扣押電腦硬體與軟體設備即可阻止犯罪續行。犯罪證物如為數據或電腦檔案規格時，檢調人員應依據個案特定情況，另行扣押其他相關周邊設備，俾便專業人員啟動電腦觀看證物資料。例如中央處理器（CPU）、監視器、滑鼠、鍵盤。然而一般情形並不扣押列表機或數據機。一旦快速的完成審驗後，與案件無關之資料應立即發還。大多數的情形下，硬體被扣押後必須確保數據資料受到妥善的保存，並且快速檢驗相關內容。扣押軟體，相關儲存媒介亦應扣押，例如磁帶盤、磁帶、光碟等均屬之。

e、隱匿窺探式搜索票（Sneak and Peek Warrants）

檢調人員在偵查時如欲獲得資訊或犯罪情資，或查證單位內部之共犯，而不使嫌疑人察覺，可聲請隱匿窺探式搜索票（Sneak and Peek Warrants），此種搜索票允准檢調人員以隱匿不為人知的方式，登入嫌疑人的電腦系統並複製相關檔案資料後加以查證。不過偵查人員於事後必須向當事人說明搜索的情形，否則即違反聯邦法對於搜索與扣押的規定[45]。

f、無預警搜索票（No-Knock Warrants）

一般搜索的方式必須具備叩門與宣告（knock-and-announce）的要件，只有在緊急情況時例外。如果「叩門」會導致檢調人員或其他第三人受到傷害、嫌疑人逃亡或是證據可能被湮滅，此時即可使用無預警搜索票。搜索處所係為無人或房門開啟狀態時，即無必要適用叩門與宣告的要件。凡搜索電腦的案件均無適用無預警搜索之可能，除非與其他案件相牽連。有關無預警搜索票應詳載實施的必要理由。捨棄叩門與宣告的要件應具備相當合理的依據，其中所應考量的事項有：是否偵查犯罪（不論暴力或非暴力）、是否有情資顯示證物即將湮滅、當事人的年齡與科技能力純熟度以及當事人是否知悉其為偵查對象。檢調人員如欲進行無預警搜索前，均應諮詢空軍特調處軍法官，其他請參閱司法部「指導方針」第六部分B項4款之軍事上特別考量要點。（DoJ Guidelines, Part VI, § B. 4. Special Military Considerations）

g、數據位置與分析

依據上述各項搜索的限制，如搜索電腦系統時，所有的儲存裝置均應視為主要證物。其中包含硬碟、軟碟、備份磁帶、光碟片以及其他許多新開發的儲存裝置。而輸出與輸入裝置（I/O device）通常並不儲存數據資料，但電腦專家能夠從中獲得相當寶貴的資訊。此外，對於雷射印表機最後所存留的數據資料應予搜索。硬碟中所存留之列印緩衝器內的數據資料，或者是印表機內硬碟所留存的列印數據資料，以及列印捲軸在尚未完成列印時所保存的數據資料，均應當成證據予以檢驗。點陣式印表機的色帶能夠存留列印資料的印痕，監視器的螢幕因為磷化物燃燒所殘存的痕跡，亦能發現螢幕上最後所顯示的影像。此外，附有鍵盤的磁盤機、插卡與掃描器等均可視為證據的

45 United States v. Johns, 948 F.2d 599 9th Cir. 1991, cert. denied, 505 U.S. 1226 1992

來源。其他如傳真機等亦不容忽視。

電腦的使用者，不論使用何種電腦系統都會例行性的產生備份資料，有時可能將其存放在其他網站。因此證明此類備份的存在以及存放位置可能相當困難，但是對於任何電腦系統的作業程序應詳細研究與查看，檢查系統有無備份磁帶、備份磁碟或備份卡匣的資訊。

案件如涉及電腦網路系統時，應詳加策劃與思考有關數據資料存放其他網站的可能性，因為使用者在網路系統中可能使用檔案伺服器、電子郵件、電子布告欄以及語音信箱系統，由於網路系統透過網際網路的連接，幾乎能夠連接任何處所的任何一部電腦。承如前述，系統作業人員在多人使用的系統上都會例行性的備份自己的資料，然後存放在其他網站內。參閱司法部「指導方針」第四部分 F 項。（DoJ Guidelines, Part IV, §F）

h、搜索資訊

由於電腦數據資料的易損性，導致調查官搜索數據資料時，產生許多困難。因此幹員在搜索前應先控制電腦系統遠端登入口，如此即能防止嫌疑人從其他位址登入系統進行毀損作為。例如，當偵查人員著手搜索資料備份區域時，犯罪者同時從其他不同的電腦系統，登入該搜索區予以刪除資料，使得偵查人員無功而返。

i、運用專業人員

執行搜索電腦系統時，應先詳盡策劃。針對所有的可能性，先行確認電腦類型、作業系統、嫌疑人登入系統之能力。找出這些問題的答案後，再行決定專業人力之需求。聯邦法第 3105 條（18 U.S.C. § 3105 1997)規定，電腦專業人員得附隨執法人員執行搜索。這些專業人員能夠在法庭上擔當鑑定人，進行系統資料檢索、使系統正常運作、從儲存裝置救回被刪除與被覆蓋的資料、解除系統密碼、破解與辨識密碼文件以及查驗電腦病毒等項。參閱司法部「指導方針」第四部分 I 項（DoJ Guidelines, Part IV, § I）審判時運用專業人員的討論。

就空軍特別調查處的政策而言，電腦犯罪調查員（Computer Crime Investigators）應負責電腦相關證物的分析與處理，但不包括處理與分析猥褻圖文資料案件。由於電腦硬碟的容量越來越大，而且電腦犯罪調查的人力需求永無止境的擴張，空軍特調處發展出一套幹員支援體系，這些幹員對訴訟上電腦專業鑑定領域相當熟稔，他們稱之為電腦鑑驗員（Computer Forensic Field Examiners CFFE）。他們經過特別的訓練，能夠在有限的資訊傳導體上實施分析。因為涉及到不同的作業系統、複雜多元的處理過程以及龐大的資訊容量，許多案件需要特別的處理。因此，電腦鑑驗員能夠獲得國防電腦鑑驗室（Defense Computer Forensics Laboratory DCFL）的支援。該實驗室建立於 1996 年，前身即為空軍特調處的電腦鑑驗室。目前，電腦犯罪調查員、電腦鑑驗員、國防電腦鑑驗實驗室等三個單位的人員屬於空軍特調處，專責執行電腦資訊分析鑑定業務。

7. 最佳證據法則

整體而言，最佳證據法則是：「凡在審判中所提出的任何證物都必須是原本」。複製品必須在特定的條件下始准提出。聯邦證據法第 1001 條⑶款對原本的定義如下：

> 原本：文書或抄錄之「原本」，係指文書或抄錄之本身，或出於「原本」製作人或發行人之本意，使之具有相同效果之複本。照片之「原本」包括底片與其任何之印製物。如果資料儲存於電腦或類似裝置，其列印物件或輸出物件，得以經由視覺閱讀，且其反射影像資料經顯示與資料無誤者亦為原本。

軍事證據法第 1001 條⑶款規定與聯邦證據法的敘述相同。因此，幹員若能證明嫌疑人電腦所儲存的列印物件、相片、文書資料等等，其反射影像資料正確無誤，法院均認定為原本資料[46]。

由於特殊案件的大量數據資料以及電子證據的易變性，檢調人員對於被告的抗辯應保持敏銳度，這些抗辯包括證物監管體系、證據的真實性，以及權利主張變更的可能性。如果證物的控管流程嚴密，這些抗辯成立的可能性就微乎其微。

---

46 United States v. Whitaker, 127 F. 3d 595 7th Cir. 1997), cert. Denie

附錄一

Access 登入、存取	啟用電腦系統的時機。存取已儲存之電子通訊的過程。
Accreditation 授權	經由主管機關正式的公告，於特定的安全模式下，使用律定的保護程式，在可容許的風險情形下操作資訊系統。
Applet 小型應用程式	小型應用程式，通常可免費使用，執行一些簡易的功能如計算、電話撥號等。例如伴隨視窗九五的應用小程式。
ASCII 美國資訊交換標準碼	全球認可的文字版本規格。ASCII 檔案就是一份存文字檔案，其中包含英文字母、空格、英式標點符號、行列轉折、移字符號或者檔案結束符號，但是這些文字均無格式化的資訊，此類的規格是應用在程式之間的檔案轉換過程，否則程式無法一一的認知各個文件。
Assembly Language 電腦組合語言	低階的程式語言，通常一個敘述對應一項指令，經由微電腦系統處理完成。
Attack 攻擊	在電腦系統上嘗試繞過安全控制，企圖滲透或滲透電腦系統的行為，事實上，攻擊未必成功。所謂成功的程度依據電腦系統的傷害程度而定，或者是反制作為的有效程度而定。
Audit Trail 追蹤	以時間為順序之方式，記錄電腦系統作業情形，並且存入系統的檔案。這份檔案能夠經由系統管理人員查閱，即能明瞭當時系統用戶在該系統的操作過程，由於此種追蹤系統佔據相當大的硬碟空間，促使作業系統速度減緩，因此多數系統管理員並不使用，或者限量應用。
Aural Transfer 聽覺傳導	聯邦法第 2510 條第 18 項所定義之名詞，即「兩端點之間，包含起始點與收訊點之間，含有人類語音的傳導運動」。
Authorization 授權	對於電腦登入或存取權限授與系統用戶，或賦予程式或操作的程序。
Automated Security Monitoring 自動化保全監控作業	使用自動化作業程序，確保安全系統不至失效，或是使用此類工具，追蹤不當使用電腦嫌疑人所操作之行為。
Backbone 中樞鏈路	廣域網路如網際網路之高速、高容量的傳導體。應用在數千英里的距離中傳遞數據資料。許多不同種類的物理介質被使用在中樞鏈路系統中，例如微波傳遞、衛星、專用電話線等等。
Backdoor 隱匿裝置	與「天窗」同義。是隱藏式的軟體或機械設備，其功能為阻擋不當侵入或安全控制系統。
Backup 備份	檔案或程式的複製品，如軟、硬體當機後作為回復原狀之用。
Bandwidth 頻寬	頻率測量方式，通常以每秒周數（赫茲）或每秒位元數 (bps)，來表示一定數量的資訊在頻道中的流量。頻率越高，頻寬越寬。
Banner 警語、標題	告示，通常提醒電腦系統用戶在登錄使用系統前，明示系統用戶在使用時為受監控對象。
Baseband 傳輸媒介，基帶	區域網路中傳送數位訊號的方式，在傳導纜線中以直接數位方式傳遞，而沒有複雜、頻繁的變換動作。
Basic Input/Output System (BIOS) 基本輸出輸入系統	電腦程式，應用在IBM相容的個人電腦上，在唯讀記憶體（ROM）中以解碼方式運作。這套程式主控系統開機，諸如訊息輸入以及對硬體進行低階控制，這類硬體如磁碟機、鍵盤、顯視器等。
Bin 二進位制	二進位制檔案的縮寫。
Binary File 二進位制檔案	電腦檔案，包含數據或程式指令，電腦可讀取的格式。
Binary Transfer 二進位制傳輸	經過議定的檔案傳輸方式，使當事人以終端軟體將二進位制檔案傳輸至遠端電腦。
Bit 位元	電腦數據的最小單位容量
Boot 啟動電腦	電腦自動化的例行程序，進行清除記憶體資料、載入電腦作業系統，然後使電腦呈現開機狀態。

Bridge 連接器	應用於區域網路的裝置，能使二個區域網路系統進行資料交換。
Brute Force 蠻力法	在電腦編製程序中，未經精密邏輯處理，以反覆多次的簡易程序來解決較為複雜的疑難，例如拼字驗證器、駭客程式等。
Bulletin Board System (BBS) 電子布告欄	由公司或個人所設定的電腦主機，透過數據機撥通電話連接電子布告欄系統，在美國有上千家電子布告欄系統，對使用客戶提供豐富的資訊。甚至有的系統提供圖檔、共享軟體、公用軟體下載服務。
Byte 位元組	八位元。用以表示一個字母、單一數字或其他符號。
Chat 網上聊天	以鍵入文字方式在線上與其他人談話。
Chat Forum 聊天室	在電子布告欄系統或線上資訊服務系統，提供特別的區域或會議空間，容讓二位以上的人員在線上，依序鍵入文字方式同時進行會話。
Classified Information 分類保密資訊	依據美國總統第 12958 號行政命令規範或是其他繼任總統的相關行政命令，或是 1954 年原子危機法案及其修正法案之規定，對於必須受到保護且未經核准的情形下不得對外公開的資訊，必須被標示為保密狀態。
Coaxial Cable (10base2) 同軸電纜	應用於區域網路，寬頻連接電纜，軸心為絕緣電線，外圍包覆著實體或網狀電線。同軸電纜應用在寬頻系統與基帶系統（baseband systems），例如乙太網路（Ethernet）。
Command Processor 指令處理器	屬於作業系統的一部份，從系統用戶處接受輸入指令，然後顯示訊息與提示符號，例如確認或錯誤訊息。同時也稱之為指令處理編譯器。
Command.com Command 檔	在 MS-DOS 系統中，一個包含命令處理器的檔案，這份檔案必須使用在 MS-DOS 開機系統來啟動系統。
Command-line Operating System 指令操作系統	以指令驅動的作業系統，例如 MS-DOS, 以鍵盤輸入指令方式。
Compromise 洩漏資料	公開資訊與未經核准人員，或者妨害系統安全規定之行為，因而導致資訊外洩、遭到篡改、毀損或遺失等情事。
Computer Fraud and Abuse Act of 1984 一九八四年防範電腦舞弊與濫用法案	本法為聯邦法律，對於跨越州界濫用美國政府電腦系統或網路系統之行為予以處罰，其中對於未經允准登入系統、竊取財務信用資料以及故意幫助外國政府之間諜行為，施以罰金或有期徒刑之刑罰。
Computer Security (COMSEC) 電腦安全規範	有關確保電腦系統資產之嚴密性、整合性與效益所採取之措施與管制作為，電腦系統資產包含硬體設備、軟體、韌體，以及經由該系統處理、儲存、或通聯之資訊資料。
Confidentiality 嚴密性	確保資訊不會洩露給未經核准之人員或遭受未經核准之處理，或提供相關設置之用。
Config.sys 系統組態檔	MS-DOS 系統中，這是一份 ASCII 文字檔案內容為組態設定指令，存放在根目錄，當 MS-DOS 系統開機時，指令即與該檔案協調互動。
Configuration 組態	對於電腦系統的應用程式予以選項設定，以便於滿足個別系統用戶之不同需求。
Configuration File 系統組態檔案	當植入軟體時，將應用程式予以選項設定並記錄成檔案，在下一次當開機時，系統用戶能夠順暢的操作軟體。
Connect Speed 連線速度	資料傳輸的速度，當數據機運作時與其他數據機連接前，計算線上傳導雜訊後建立連線，通常連線速度低於數據機的最高速。
Connectivity 網路連通性	電腦或程式在網路設定的情形下所能運作的程度。
Contents 通訊內容	通訊的內容或文字訊息，依據聯邦法第 2510 第 8 項的定義，使用任何有線、口語或電子式通訊的內容，包含與該通訊相關之有形物質的資訊、文字意涵或意義。
Core Dump 內存信息轉儲	在大型電腦主機系統中的除錯技術，其中包含列印整個電腦的核心內容或記憶體資料。

Crack Program 解碼程式（駭客程式）	一套解除或突破電腦密碼之程式。通常系統用戶所設定的密碼，以編碼的檔案儲存在電腦系統。駭客經常製作這種解碼程式，然後輕鬆的執行程式來突破密碼的限制，一旦解密後就直接登入系統，變成正當系統用戶，由於系統用戶使用同一組密碼在不同的系統上操作，因此駭客也就能夠輕而易舉的開啟其他系統。這些程式通稱為快客（Crack）。
Cracker 駭客	一群圖謀不軌的電腦族，通常任意破壞他人電腦系統。
Crash 當機	電腦系統或程式稱之為當機，即表示該系統或程式由於硬體或軟體失效無法執行，其主因為停電、軟體編碼錯誤、電腦系統於作業時與其他系統或資料處理相衝突，導致系統鎖住。許多駭客入侵電腦系統後能夠使系統當機，不論是故意或偶發事件，大都因為駭客執行某些指令或植入與系統不相容的程式。
Critical Infrastructures 重要基礎公共建設	有關政府或經濟方面基要運作所需的實體或虛擬之系統設施。
Cryptography 密碼學	將一般資訊編譯成艱澀難懂的字碼，然後能夠將字碼回復成一般資訊的步驟、方法、原理原則之學門或藝術。
Cyberspace 虛擬空間	電腦網路的真實世界，任何人透過電腦與數據機均可進入瀏覽。每個人都能進入世界上任何一個電腦系統並且與電腦系統用戶相互溝通。
Daemon 電腦程式（屬於UNIX系統）	電腦程式，維持或執行電腦工作或功能，例如列印檔案、監控網路流量或對外通訊。
Data Encryption Standard (DES) 數據加密標準	一項由IBM 公司所開發且具有爭議性的資訊密碼編譯科技，為美國政府所採用，作為非保密資訊之用，同時被金融機構廣泛的作為鉅額資金電子轉帳之用。
Data Integrity 數據的嚴整性	數據資料存在於與原始數據相同且未經修飾、改變或毀壞的狀態。
Denial of Service 連線拒絕	由於資訊系統或其他執行傳輸之必要設施無法工作所到導致的結果，通常是失去連線或是傳輸功率降低所致。連線拒絕的情形常常衝擊到生產力，當連線拒絕的情形發生後，依據發生時間長短與天數造成費用的耗損。
Designated Approval Authority (DAA) 權責主管單位	這個名詞由美國空軍所創造的，主要是凸顯個人經由基地指揮官的任命後，執行基地電腦網路系統或某些重要部分的監督工作。依據空軍訓令（AFI）第 33-202 條專用術語彙編，DAA 就是「具有主管權責，能夠確切的認定在特定的環境下，操作資訊系統或網路系統的官員」，他們的職務規範在空軍訓令第 33-202 條第 2.7 項（Paragraph 2.7 of AFI 33-202）
Direct Memory Access (DMA) Channels 直接存儲器存取（DMA）管道	從記憶體傳輸數據資料至周邊設備的管道，例如硬碟控制器、網路配接器或磁帶備份設備。
Direct Memory Access (DMA) Controller 直接存儲器存取（DMA）控制器	從直接存儲器存取管道來控制數據資料流量的晶片。藉由控管數據資料，達到使其規律地進出管道的機制。直接存儲器存取（DMA）控制器能夠釋放微處理器能量去執行其他工作。
Domain 網域	在網際網路上，次級分類中的最高階，通常以國家為主體，以美國為例，次級分類通常以機構性質區分，例如商業部分以（com.）、教育性質以（edu.）、政府部門以（gov.與mil.）為名。
Domain Name 網路名稱	在網際網路上電腦系統名稱。網路名稱通常用來確認網際網路上的單機系統。以單字或縮寫來表明電腦主機的名稱，例如 (watt.seas.virginia.com).
Domain Name Service (DNS) 網路名稱服務	在網際網路上連接電腦系統的程式，稱之為網路名稱服務伺服器，並且能夠自動的從網路名稱與網路協定位址（IP addresses）相互轉換以便傳輸資料，此種轉換的目的又稱之為「解決方案」，在於使網際網路的用戶即使因為服務業者的網路協定位址（IP addresses）變更，仍能持續的使用熟悉的名稱來與對方連線，例如：(www.afpc.mil)。
Electronic Communication 電子通訊	這是名詞定義在聯邦法第 2510 條第 12 項中：任何屬於符號、信號、文書、影像、聲音、數據的傳輸，或者就可理解之事物，其全部或一部能夠透過導線、無線電、電磁體、電子攝影或影像視覺等傳導系統傳輸並能影響國內或國外之商業交易。但不包含下列各項（A）任何有線或口語上的通訊（B）任何經由非語音之傳呼器的通訊（C）任何從語音追蹤器（詳如聯邦法第 3117 條）所獲得的通訊 （D）在金融機構的通訊系統中所儲存的電子轉帳資訊，作為電子儲存資料或轉帳的記錄 。

Electronic Communication Service 電子通訊服務	聯邦法第 2510 條第(15)項規定：「任何提供系統用戶具有接收與發送有線或電子通訊能力之服務」。此亦包含政府所有之系統。
Electronic Communication System 電子通訊系統	聯邦法第 2510 條第(14) 項規定：「任何屬於傳輸電子通訊之有線電、無線電、電磁、視覺影像或電子影像等器材，以及任何屬於儲存電子通訊之電腦設備或相關電子設備」。
Electronic Communications Privacy Act (ECPA) 電子通訊隱私權保護法案	立法通過並於 1986 年 10 月 21 日經由雷根總統簽署的法案。該法案為修正法案，確立聯邦法有關隱私權的保護與標準，特別針對電腦與通訊科技的急劇改變。法案第一標題針對聯邦反竊聽法律中有關反制非經授權，實施攔截線上電子（電腦）通訊等作為之條文予以修正。第二標題增訂聯邦法第 2701-2711 條文，以保護業經儲存有線與電腦通訊，例如電子郵件、通訊記錄。第三標題明定電話撥號音訊與相關偵蒐追蹤等裝置。
Electronic Mail 電子郵件	簡稱 e-mail. 透過電子布告欄、電腦網路或其他電腦系統，能夠傳輸訊息給二個以上的系統用戶。對於這種訊息亦稱之為電子郵件。
Electronic Storage 電子儲存	聯邦法第 2510 條第(17)項規定：(A) 任何屬於暫時性、初級的儲存裝置，儲存伴隨電子傳輸而來的有線或電子通訊。(B)任何屬於儲存前款所稱之通訊裝置，且由電子通訊服務業者所裝設，其目的係為備份並保護上開通訊。
Expanded Memory Manager (EMM) 擴充記憶體管理器	管理擴充記憶體的工具程式，擴充記憶體藉由擴充記憶體板 (EMM386)， 裝設在 IBM 個人電腦內。
File Allocation Table (FAT) 檔案配置表	磁碟片或硬碟上所存在的隱藏配置表。檔案配置表記錄檔案如何區分並且以相連接的叢集方式存放。目錄檔案儲存檔案第一叢集的位址。在檔案配置表第一叢集的入口處即為第二叢集儲存檔案的位址，以此類推。
File Transfer Protocol (FTP) 檔案傳輸協定	在網際網路上傳輸檔案的標準模式。透過這一項協定即可將檔案在不同兩端的電腦上相互傳輸。FTP 乙詞也是電腦上檔案傳輸程式的名稱，以檔案傳輸協定為運作主體。
Finger （電腦指令）	屬於電腦網路系統的指令。在 A 電腦系統的系統用戶能夠以這項指令來核驗從 B 電腦系統登錄本機系統的用戶。這種電腦指令能夠被系統用戶予以解除。例如當 B 電腦系統系統用戶解除這項指令後，即能如隱形人一般進入 A 系統，而 A 電腦系統用戶即無法執行該指令來查驗何人登錄本機系統。
Firewall 防火牆	裝設在區域網路或網際網路系統中的安全保護程式。防火牆程式係為阻擋非經授權的系統用戶進入網路系統。防火牆程式的登入方式係藉由代理伺服器 proxy servers 以間接與仲介方式進入。
Firmware 韌體	記錄在電腦永久記憶體中與程式有關的程序指令。
Floating-Point Calculation 浮點運算	數值運算與儲存的方式，以便使十進位數值的位置以浮動的方式而非固定的方式存在。（十進位的數值在運算時，如有需要以浮動方式移動，如此能使運算方式加入更重要的數值運算。）
Flooding 溢位	因為加入巨量的數據資料，導致當機或程式不運作。
Gateway 網路閘道器	將不同網路系統連接的設備。大都為硬體裝置，又稱之為連接器，藉由電腦程式來執行翻譯不同系統的電腦語言。
Graphical User Interface (GUI) 圖形使用者界面	電腦程式的圖形設計，令系統用戶能夠以點選圖像方式來執行程式（例如 Windows 視窗與 Macintosh 麥金塔系統）。
Hack-back 追縱駭客	專門性的程式或技術，應用在調查電腦入侵者的路徑並可回溯到入侵者的本機系統或是其他轉介的主機系統。
Hacker 電腦駭客	在字典上「hacker」乙詞是俚語，用以描述辦事能力強或執行工作成功的人。在電腦界，駭客專指某些能夠花費許多時間在電腦上操作，僅僅憑著嘗試錯誤法不斷摸索而能成功，無須依賴操作手冊之人。這類人通常是電腦科技人才，例如電腦語言組合工程師或系統工程師。在今日，這個名詞具有負面意義，通常用來貶損使用電腦科技以未經允准的方式來獲得登入存取資料的能力，然後在他人電腦系統上惡作劇或毀損系統與資料庫的人。
Hardware 硬體	電腦實體部份例如監視器、鍵盤、主機、列表機、掃描器等等。

Host 網路主機	屬於傳輸控制/網路通訊協定（TCP/IP）的網路系統中的電腦主機，有時泛指網路上的任何裝置。
HyperText Markup Language (HTML) 超文字標記語言	一部約定，將文件資料部分以標記方式表示，經由電腦語法分析之後，各個標記部分呈現不同的版式。超文字標記語言是一種審定後的語言類型，呈現在全球資訊網上的是文書資料，而所謂的語法分析意即網頁瀏覽器。就標準通用標記語言規範，超文字標記語言能夠讓作者加入超連結，使瀏覽者在點選時能夠直接顯示其他的超文字標記語言格式的文書。
HyperText Transport Protocol (HTTP) 超文件傳輸協定	網際網路的協定標準，用來支援全球資訊網（WWW）上的資訊交換，藉由界定一致資源定址器（URLs）的方法，以及資源接收的方式，不僅是網頁文件同時也包括檔案傳輸協定認可的檔案資料。超文件傳輸協定能夠使網頁作者將網頁資料以超連結方式崁入。當系統用戶點選超連結時，超連結自行啟動資料的傳輸與接收，無須系統用戶再行介入操作。超文件傳輸協定在網際網路上首創清晰簡易登入網際網路的方式。
Identification 辨識	電腦系統用以確認實體設置或系統用戶的程序。
Impersonating 假冒	欺騙的方式，在線上假冒他人身分證明。
Information Operations (IO) 資訊戰	為了保護我方的資訊與電腦系統，所採取的反制敵方資訊與電腦系統的作為。
Information System 資訊系統	一套完整的基要建設或是機構組織、人事體系與相關組件，係為蒐集、處理、儲存、傳輸、散播、展示與配置資訊。
Integrated Services Digital Network (ISDN) 整合服務數位網路	一套針對家庭、學校與事務機關等場所用以傳輸數位電話或數據服務的全球性標準。整合服務數位網路業區分三項：一般性 ISDN，針對聲音、影像與數據資料具有二個每秒 64 千位元（KBPS）傳輸速率的頻道，附加一條每秒 16 千位元（KBPS） 的信號傳輸頻道，二、主要速率 ISDN ，提供 23 個具有每秒 64 千位元（KBPS）傳輸速率的頻道。三、寬頻類：能夠提供每秒 150 兆位元（MBPS）數據傳輸速率能力。
Interception 攔截	線上獲取有線、口語、或電子通訊的作為，與竊聽同義。參閱聯邦法第 2510 條。
Internet 網際網路	又稱為資訊高速公路。網際網路乙詞係為全球性的架構，卻難以簡明解釋。網際網路的資料起源於 1969 年，美國國防部所屬之高等研究計劃署 ARPA 創立了 Internet 的前身 ARPANET，這個早期的網路系統限制於軍事體系、或與軍方簽約的民間機構與教育單位使用，藉著電腦專用的電話線，在 Unix 作業系統（32 位多任務、多用戶操作系統）上相互連結。ARPANET 的主要目標係為維持軍事通訊的暢通，不因電話通訊業者的分崩離析而受影響。因此說明了網際網路高度的重複性與低度的集權性。例如介於兩台電腦的通訊受阻後，電腦會自行尋找另一條通路來傳送資訊。由於在電腦中心有數條不同的通路與運作，因此在網際網路的運作上，並無所謂的網際網路中心或是最高單位，每一個電腦位址都是一個獨立的個體，但都遵從國家或國際會議中所制定的標準運作。由於個人電腦以及商務廣告快速發展，因此遂有提供小額月付制來進入網際網路的服務。任何人只要有一個基本操作的電腦與數據機就能使用網際網路。在 1988 年 網際網路約有 33,000 部主機電腦上線。在 1993 年年尾已經擴展到 180 萬部，全球計有 500 萬個電腦系統用戶透過網際網路通訊，每個月約有 100 萬個新增用戶上網。
Internet Protocol (IP) 網路通訊協定	傳輸控制／網路通訊協定的標準規範，說明有關與網路連結的電腦，應如何將數據資料分成小包以便在網路上傳輸，以及訂定這些小包的位址，以便到達相關目的地，網路通訊協定在協定標準中係屬無連接傳輸模式。傳輸控制／網路通訊協定具體的說明，兩部網際網路線上電腦，藉由交換預設控制信號或字元的程序能夠建立確實的數據通聯。
Internet Protocol Address or IP Address 網路通訊協定位址	一連串的數值，以句點隔開，用以辨識電腦位址例如 138.194.1.3.。每一串數值均能辨識國家別、網路編號、主機編號以及個人電腦在網路中的位址。
InterNIC 管理機構（負責控制區域名稱的登記及對網友們提供教育與公眾可進入的資料庫）	經由美國國家科學基金會（NSF）的簽約，聯合兩個機構提供網路資訊服務。目前美國電話電報公司 AT&T 提供名錄與資料庫的服務，而 Network Solutions 公司提供新登記網站名稱與網路通訊協定位址的註冊服務。
Interrupt Address (IRQ) Lines 硬體裝置對 CPU 中斷要求的線路	IBM 相容的個人電腦中，硬體相連的線路（例如印表機、數據機等）能夠提醒中央處理器該裝置業已處於接收或傳送數據的準備狀態。

Intruder 入侵者	非經授權的電腦系統用戶。同時也包含越權使用電腦系統，通常與hacker、phracker、phreaker同義。
Kernel 核心	在電腦作業系統中，程式常駐記憶體的核心部分，在運作上扮演必要的執行角色，諸如控制磁碟的輸出與輸入作業、管理內部記憶體。
Keystroke Monitoring 鍵盤監控	藉由電腦操作者以鍵盤輸入方式與電腦回應方式的監控作業過程。
Local Area Network (LAN) 區域網路	此為最常見的網路系統。區域網路僅包含本地端電腦設備，例如電腦在地理位置上相鄰，如辦公室或大樓內。與廣域網路為相對名詞 Wide Area Networks (WANs).
Log 登錄	兩端電腦連接的記錄。系統作業人員除了紀錄電腦間連線的資訊，同時也能使用另一部電腦來偵測電腦通訊的問題與駭客入侵等活動。
Logic Bomb 邏輯炸彈	具有惡意的電腦程式，能夠隱藏在電腦系統中，依據特定事件開始發作，造成當機或毀壞電腦程式，例如四月愚人節程式，於四月一日發作。
Log-in or Log-on 登入	得以進入電腦存取資料的手續，通常鍵入自己的帳號與密碼即可。
Looping 循環、重複執行	電腦駭客用來掩飾其入侵路徑的方法。透過這種技術，駭客以蛙跳方式或重複迂迴執行方式進入其他的電腦系統，然後對於目的電腦系統發動攻擊。這種技術使駭客能夠掩飾其真實入侵路徑。除此之外，駭客經常使其入侵路徑跨越國界。這種透過電子的越界入侵方式，使得駭客成為其他國家司法主權管轄所及。因此在立法上與執法機關執行上必須詳加考量。
Mail Bombing 郵件炸彈	利用發送大量電子郵件給對方以達騷擾的目的，這種程式也會因為對方遭受服務拒絕，而採取的反擊作為。
Malicious Code 破壞碼	具有破壞電腦系統能力而且能夠不受支配的軟體或韌體。
Modem 數據機	調幅器與解調器的組合體。電腦經由這項設備能夠以電話線來收發資訊。當數據機發送資訊時，將電腦資訊或數位資訊轉換成類比信號（類似雛鳥尖叫的聲音）經由電話線傳遞。而收訊時，數據機將類比信號轉換成數位資訊以便電腦使用。
Name Server 伺服器名稱	連接區域網路與網際網路系統之間，電腦必須提供網域名稱，藉以銜接字母與數字之間的網路通訊協定位址。因此，如為建立與網際網路系統業者之連線，本機電腦必須提供網路通訊協定位址的伺服器名稱。
Network 網路	二台以上的電腦或主機相互連結，以便交換數據資料。網路有二種主要態樣，一為區域網路 Local Area Networks (LANs)，另一為 廣域網路 Wide Area Networks (WANs)。
Network Security 網路安全性	保護網路系統避免遭受非經允准的修改、毀損、公開或使用的作為。因此必須確保網路的運作嚴密精確，同時避免網路上的資訊被修改。
Open System Interconnection (OSI) Model Reference Model 開放系統（國際通用的電腦標準系統）的模式與相關模式	由國際標準組織 International Standards Organization (ISO)以及電機工程師學會 Institute of Electrical and Electronic Engineers (IEEE)針對區域網路系統所建立的國際標準，藉以改善網路系統的靈活性。國際標準組織所提出的模式，係將通訊過程區分為各自不同且相互絕緣的層次，例如實質硬體層（同軸纜線）、傳輸層（數據通訊的方式）、供給層（數據與程式交互作用的方式）、應用層（程式提供給網路用戶使用的方式）。
Operation Security (OPSEC) 操作安全性	針對潛在的敵人所採取的拒絕資訊措施，其中以辨識、控管與保護等作為來維護非分類保密資訊。
Oral Communication 口語通訊	聯邦法第 2510 條第(2)項規定：任何由人類所表達的口語溝通，其中含有一個期望，即在合理的情形下，該溝通內容不應成為被截聽的主體 ，但是這個名詞並未包含電子通訊。
Packet Internet Groper (PING) 測試連通性之軟體	診斷型的工具軟體，用以測試電腦與網路連接之連通性。
Password 密碼	用以識別或證明電腦系統用戶的字、詞、字串。這是登錄過程的一部份，用戶能夠登入電腦系統存取檔案、或資訊。
Penetration 突破	未經允准以凌越電腦安全保護程式之方法，登入電腦系統的行為。
Phracker 佛瑞客	結合電腦駭客與電話駭客的辭彙。專指侵入電話公司的電腦系統藉以獲得免費的通話服務之人。

Phreaker 電話駭客	專指非法獲取免費長途電話服務之人。電話駭客設計出音源器能夠模仿硬幣落入付費電話機的聲音。這種音源器有不同的名稱，例如藍盒子、黑盒子等等。然而由於科技日新月異，這些裝置已經不再使用。目前電話駭客大都是以偽造電話卡或將通話費用誤導至他人帳戶來圖利。
Point to Point Protocol (PPP) 點對點通訊協定	電腦以直撥電話方式聯通網際網路的其中標準（另一稱之為串聯線路網際網路協定SLIP）。點對點通訊協定應用更高階的數據協商、數據壓縮以及除錯功能。
Program 程式	一組電腦系統的指令，能夠使電腦執行某類特定事務。
Protocol 協定	一組由軟體用來與硬體產生相互作用的標準或規定。例如：二具數據機相互連接時，二者必須遵行相同的協定才能相互通聯。
Remote Computing Service 遠端電腦服務業	聯邦法第 2711 條第(2)項規定：藉由電子通訊方式，對公眾提供電腦儲存或使用電腦的服務。
Root (System Administrator Privileges) 源頭（又稱之為系統管理者特權）	這是一個用以描述在操作電腦上擁有特定信賴度與特權的名詞。一旦以此特權登入電腦系統之後，電腦將使用者視為主人，使當事人具有為所欲為的權限，這種特權能夠賦予從任意觀看檔案、系統控制、系統登入、任意移除檔案、下載資訊、執行程式檔案到毀損所有檔案或作業系統檔案等權限。這種特權僅限於少數經篩選的系統作業人員，他們負有維護系統、更新系統與配置系統之責任。電腦駭客亟欲獲取此種系統管理權限，不僅能夠任意存取資料，同時也能掩飾其入侵路徑。
Router 路由器	在封包交換的網路系統中（網際網路）的其中基本裝置（另一稱之為主機），路由器是電子裝置，用以檢驗所收到的每一封包的數據資料，然後依據目的地將其送往該處。
Security Administrator Tool for Analyzing Networks (SATAN) 網路安全管理工具	用以分類電腦網路安全等級的程式。該程式能夠判定何種與網路相關的軟體，不足以防護電腦駭客入侵之能力。這種軟體頗具爭議性，因為駭客與系統管理人員均能用以發掘網路疏漏。
Serial Line Internet Protocol (SLIP) 串聯線路網際網路協定	工作站或個人電腦以直撥電話連接網際網路的連通標準之一（另一為點對點通訊協定），串聯線路網際網路協定界定數據封包以非同步式電話線路傳遞方式，因此能夠使電腦以間接且非完全方式聯通網際網路，這種連接模式優於以命令解釋程序登入的方式，因為用戶能夠依據個人喜好使用網路工具，同時操作二種以上的的網路應用軟體，而且可以直接下載資料至電腦，無須其他仲介儲存裝置。
Server 伺服器	電腦網路系統中，具有分享軟體與資訊並提供服務的電腦主機，例如分配給網路用戶的電子郵件信箱。
Shell 命令解釋程序指令	配置易於使用的人機界面作業系統的程式。雖然命令檔 COMMAND.COM 技術上而言是命令解釋程序指令（應用於系統用戶與微軟磁碟機作業系統MS-DOS之間的軟體)，但是這個名詞應用於以組合指令替代一列指令語言的程式。
Sniffer 偵蒐程式	具有攔截並儲存電腦資訊功能的軟體程式。當駭客獲得電腦的控制權後，通常會在電腦內部植入這種偵蒐軟體。藉以蒐集有限的資訊，例如用戶的登錄帳戶名稱與密碼或其他文件內容。然後再以用戶密碼登入電腦內部發掘更多的資訊，使人不易發覺。再者，由於大多數的用戶在其他的系統中也使用同一組帳號與密碼，致使駭客能夠輕而易舉的進入其他系統，導致骨牌效應產生。這種行為被認定係觸犯聯邦法第 1030 條(a)項(2)款, 第 1030 條(a)項(3)款以及第 2511 條(a)項(1)款(A)目。
Software 軟體	電腦程式、作業程序、作業準據，並且伴隨著電腦操作等文件資料。
Spoofing 假冒行為	企圖獲取登入權限而偽冒成用戶，與模仿、化裝、假扮同義。
Swap File 交換暫存檔	在微軟的視窗作業系統中，一個龐大的隱藏系統檔案，其中包含有程式指令以及隨機存取記憶體 random access memory（RAM）無法存放的數據資料。
Sysop/Sysad 系統操作員／系統管理員	系統操作員／系統管理員係對電腦系統負有維護之責。主要是針對電腦系統運作順暢發揮效率，俾使用戶有效的完成工作。為能達到這項使命，系統操作員必須規律的監控網路流路以確保通暢，或者限縮用戶權限，以及保護系統資源的完整性，避免遭受侵入、變更或竊取。
T1 T1 專線	高寬頻電話幹線，傳輸數率可達 1.544 兆位元秒。
T3 T3 專線	高寬頻電話幹線，傳輸數率可達 44.21 兆位元秒。

Telnet 遠端載入工具	遠端登入的軟體程式。登入後，用戶能夠觀看遠端電腦的檔案或執行該電腦上之程式。執行這項軟體後，本機電腦啟動與遠端電腦連通，將本機電腦輸入資訊傳送到遠端系統，由遠端系統回傳輸出資訊至本機系統。
Threat Analysis 危險分析	檢驗資訊並驗證電腦系統易於侵入之盲點。
Threat Monitoring 監控潛伏危機	分析、評估並審核資訊的相關軌跡，以驗證系統所發生的事件有無危害系統的情事。
Throughput 總處理能力	評量電腦整體運作的數值，以資訊傳輸表現做為評量對象，其中包括資訊儲存裝置，例如磁碟機。
Transmission Control Protocol/Internet Protocol (TCP/IP) 傳輸控制協定／網際網路通訊協定	國際認定之網際網路通信協定，藉由此協定可使每部電腦經由網際網路相互連通。雖然傳輸控制協定 TCP 與網際網路通訊協定 IP 為兩種不同的協定，實際上使用此一名詞均以傳輸控制協定／網際網路通訊協定 TCP/IP 稱之。
Trap Door 天窗	隱藏軟體或硬體機械功能，用來規避電腦系統實施的登入控管。與後門 back door 同義。
Trojan Horse 特洛埃木馬程式	在表面上看起來是正常運作的軟體，然而在運作時卻暗自散佈破壞碼或設定破壞性的指定令，系統用戶不易察覺。駭客常使用此種軟體來改變侵入電腦的作業系統，以避免偵測。
Uniform Resource Locator (URL) 一致資源定址器	通用資源識別器的其中一種類型，由一串字元詳細的辯識網際網路上的資源類型與位址。例如 http://www.aflsa.af.mil
User 用戶	經核准使用電腦系統或於其中存取資訊之人。
User ID 用戶識別碼	電腦系統所能接受的特定的字串或符號，用以識別系統用戶。
Virus 電腦病毒	能夠自行複製具有破壞能力的電腦程式或可執行之程式，通常不易察覺。
Wide Area Network WAN 廣域網路	電腦網路系統涵蓋不同的地理區域。由於使用網路線來連接廣域網路系統的電腦是不切實際的，因此這些電腦以電話線路或透過網際網路來連接。
Wire Communication 有線通訊	聯邦法第 2510 條第(1)項規定，任何屬於聽覺的訊息傳遞，不論是部分或全部，經由通訊器材的協助如電線、纜線或其他類似從傳訊端點連接到收訊端點器具之傳輸（包含以交換機方式連接），而該器具經由人類的提供或操作，達成州內或海外通訊之目的，或達到以該通訊影響州內或海外商業交易之目的。該名詞包括任何儲存該通訊之電子裝置（例如語音信箱）
World Wide Web (WWW) 全球資訊網	全球性的超文件系統，以網際網路作為傳輸方式，系統用戶能夠以點選超連結方式瀏覽文件。
Worm 電腦病毒	具有無限複製能力的電腦程式，其目的在於耗盡電腦記憶體資源達到癱瘓電腦運作之目的，這類型的病毒程式相當活躍，透過網際網路來感染電腦。通常受感染的電腦會自行複製一隻病毒存放於作業系統，然後當病毒電腦登上網際網路後，藉網路系統感染其他電腦並繼續複製更多的病毒。

附錄二：電腦登錄使用警語

這是一部攸關美國國防部權益的電腦系統。本系統僅提供處理美國政府部門以及其他經核准之資訊用途。本系統所擁有之數據資料均為國防部或其他經授權之使用者所有，而且經權責單位核准後，該數據資料得受監控、截取、錄製、閱讀、複製或紀錄等任何方式處理之。本系統於使用時，**使用者並無隱私權保障**。如有發生觸犯刑法，或違反安全法規、或違反經由國防部偵防、保安部門所訂定之政策等規定之情事時，系統作業單位基於此種情形下，即獲得授權而提供可能相關之證據，其中可包含使用者個人資料。不論是否經由核准，凡當事人於使用本系統時，對於監控、截取、錄製、閱讀、複製與公開等作為，即發生明確的同意之意思表示。如果你不同意，請勿使用本系統。

附錄三：電腦系統用戶約定條款

電腦系統用戶約定條款

有鑑於本人經考量接受賦與（系統名稱）電腦系統（或相關主機）之使用者帳號。這項系統為美國國防部所有，依據國防部約定條款運作，本人同意以下各條款並簽名於後：

1. 本人操作之電腦與主機系統之所有權與運作權限均屬美國國防部。
2. 美國國防部所屬之電腦與電腦系統，僅限提供本人處理美國政府資訊之用。
3. 經由美國國防部之電腦或主機系統所輸入、儲存或傳送之資訊，本人對之並無可期待之隱私權。
4. 美國國防部電腦與主機系統嚴格限定為經核准人員使用，本人對於以本人帳號或身分識別所操作之行為負完全責任，本人不會允准其他人使用本人帳號或本人身分識別操作電腦。
5. 本人使用國防部之電腦或主機系統，僅於經核准後之情形下使用，本人明瞭非公務使用這項系統時有所限制，即(a)為公眾合法之利益提供服務；(b)遵守基地指揮官與部隊長所訂定之規範；(c)對於個人職務之執行並無發生妨害之情形；(d)在合理的使用範圍與使用頻率，而且不論如何，必須於本人公餘時間使用（例如非服勤時間、午餐時間）；(e)不會大量的發送數據資料或傳送群組郵件導致通訊系統超載；(f)不會使國防部或空軍負擔額外龐大的費用，亦不會對國防部或空軍產生負面形象。（例如使用含有色情資料、猥褻兒童之圖文資料、連鎖信、或進行非關公務之廣告、推銷、販售等行為，或違反法令，或其他與公務無關之行為）
6. 本人未經資訊官或主官核准，不會輸入其他任何軟體或裝置任何硬體。
7. 除非經由特別之核准，本人絕無存取資料或執行系統程式之企圖。
8. 本人於每隔九十天之期限內，至少更換登入密碼一次。
9. 本人於使用時，不會隱匿本人身分識別或使用他人身分識別，亦無此企圖。
10. 本人不會輸入超越本系統保密區分層次之機密分類資料，亦不會輸入具有專利權、專屬權或需要其他特別保護方式的資料，如經主機保安人員核准不在此限。
11. 本人如發現任何違反安全規範或誤用本系統之情事時，將立即通知本人直屬上級與主機資訊官。
12. 本人恪遵安全程序、法令與應用於電腦系統作業之管理規範。
13. 本人絕不會以任何國防部電腦系統來發送電子郵件至非軍人所有之使用帳號。
14. 本人於取得主機資訊官之書面許可前，不會裝設數據機或遠端登入設施。
15. 本人不會使用任何國防部電腦與（或）主機系統，來獲取非經核准之登入權限或意圖獲取非經核准之登入權限，如經主官明確的指示為前述行為，則不在此限。再者，本人不會使用國防部電腦與（或）主機系統來發射「拒絕服務」的假訊息程式，或意圖發射「拒絕服務」的假訊息程式，或攻擊其他電腦或電腦系統，如經主官明確的指示為前述行為，則不在此限。
16. 主機系統係經監控作為來確保資訊安全與系統嚴整，而且僅限於公務使用。本人於使用主機系統時，以明確之意思表示同意上開監控作為，包含監控本人登入其他電腦的連線過程。

而且同意本人註冊之登錄資訊可作為行政上、紀律上或刑事訴訟等程序所引用之依據。

17. 本人在此同意開放任何儲存於主機系統或任何國防部電腦之中的檔案與（或）電子郵件。

18. 本人在此明確的同意授權主機資訊官，得提供執法機關有關本人涉及濫用或誤用任何國防部電腦與（或）主機系統之任何或所有資訊。

19. 本人於離職前、永久移防駐地前或退伍前，本人會主動通知相關資訊官，藉以刪除本人之註冊帳號。

20. 本人現已提出經本人簽署之同意條款之副本，而且本人明瞭資訊官保留本人所簽署之同意條款之原本。

簽署時間：　　年　　月　　日

電腦系統用戶姓名：_____

電腦系統用戶單位、級職：_____

電腦系統用戶連絡電話：_____

電腦系統用戶駐地（番號、基地名稱）：_____

電腦系統用戶帳號名稱：_____

電腦系統用戶簽名：_____

認證人簽名：（資訊官）　資訊官連絡電話：_____

以下由資訊官填寫

主機系統名稱：_____　伺服器所在位置：_____

核准權責人員：_____　連絡電話：_____

主機系統主官：_____　連絡電話：_____

附錄四：調查官搜索要點清單

A、系統資訊

1. 電腦系統是否為政府所有？若非，何人擁有該系統？
2. 電腦系統作業人員為何人？主管為何人？
3. 電腦系統分配何人操作？
4. 管理該電腦系統之指揮官為何人？
5. 本案電腦係為網路連接性質或單機作業系統？
6. 本案電腦連接網路為何？
   a、網路系統具有分類保密區分或不具保密區分？
   b、系統上所保存的資料為何種類型？
   c、與本系統連接的電腦有多少部？儘可能的獲得與本案電腦相連接的網路系統概要圖說。
7. 電腦是否位於機密資料隔離保存區域（Sensitive Compartmented Information Facility ）
8. 登入或存取本案電腦的類型為何？
9. 本案電腦是否提供相關服務（如電子郵件）？
10. 如有電子郵件，其運作方式為何？
11. 電腦作業人員是否對系統做備份？
    a、備份何種資料？
    b、多久備份一次？
    c、備份資料存放何處？
12. 系統作業人員是否對電腦實施監控作為？
    a、實施何種監控方式？
    b、是否有監控記錄？

13.本案電腦是否使用數據機或連接數據機？

B、同意權

1.是否能夠獲取當事人的同意而非經由偵查作為？

2.有無使用者警語？

a、警語內容？取得影本乙份。

b、警語對於任何使用者是否清晰可見？或者放置於其他電腦螢幕？

3.有無其他放置於電腦外部之警語？或警語貼紙？

4.當事人是否簽署使用者約定條款？

a、使用者條款內容？取得影本乙份。

5.當事人的辦公室是否有明示之摘要或簡要說明，告知當事人在使用電腦時不具有任何隱私權保障？

6.是否能夠證明當事人知悉前項說明或摘要？或是明瞭本項政策？

7.當事人的辦公室對於電腦系統是否經常實施無預警之檢查或搜索？

a、如是，當事人的電腦是否曾經被搜索或檢查？

b、搜索或檢查時，當事人是否在場？

8.當事人的電腦是否位於機密資料隔離保存區域（Sensitive Compartmented Information Facility）？

a、若是，該處入口是否貼有同意之告示？

C、可期待之隱私權

1.當事人是否為特定電腦的唯一使用者？

2.如非。其他使用者可否存取任何資料？

3.能否非經偵查手段取得其他使用者的通訊同意權？

4.電腦是否位於專屬辦公室而非開放區域？

5.當事人是否分割硬碟？是否對檔案加密處理？是否採取特殊的方法以致於產生高度可期待之隱私權？

6.對於搜索的電腦資料，是否具有合理可認定該資料具有發行的企圖？

D、搜索類型

1.所欲搜索的資訊種類？

2.搜索資訊的存放位置？

3.如包含電子郵件，該郵件是否經當事人傳輸或仍存放於伺服器中？

4.伺服器的位置所在？

E、搜索權責

1.是否具有合理的認定可獲得搜索權？

2.是否已諮詢特調處或地區分處的軍法官？

3.對於下列人員是否完成摘要資訊？

a、電腦配置地區部隊長。

b、系統作業員或系統主管人員。

c、管理本案特定電腦系統的部隊長

d、經分配獲准之使用者。 (全文完)