美國空軍電腦犯罪偵查手冊（一）

柴　漢　熙*

翻譯說明：

筆者於 1996 年網路系統開始風行之初，即以中華民國軍法官身分取得美國陸軍軍法資訊網之會員資格，因而瀏覽並下載許多美國軍法之法學論著。眾所皆知，美國為海洋法系與我國不同，許多法律實務觀點無法比附援引。然而，對於犯罪偵查之操作與思維並無二致。由於美國乃高度重視隱私權之國家，對於犯罪偵查強調證據保存、證據能力與個人隱私權之保護。此一課題亦正為我國刑事訴訟法有關改良式當事人進行主義以及證據法等項之修法趨勢。

電腦使用趨勢已成為生活必要，反觀國內實務對於電腦仍著墨於智慧財產權的保護，對於利用電腦網路之虛擬空間或電磁數據資料犯罪之有相關犯罪偵查作為少有文字資料。而現今絕大多數視覺資料多以數位化處理，均為 0 與 1 電腦碼所編撰，換言之，如改變其中一個位元數位碼，則該項資料即可能全然轉成為完全無關之資料或毀損而不可讀，此一特性亦為電腦犯罪偵查不易之原因。而電磁記錄存放於公務系統之電腦主機，該項電磁記錄究為私人所有抑或公物？取決於存放空間？或者物件性質？凡此種種多有爭議。因此著手翻譯美國空軍軍法處所出版之「電腦犯罪偵查手冊」，藉以瞭解該國軍法官如何指導調查官實施電腦犯罪偵查並相關偵查重點。透過中文翻譯，可促使我軍法同仁建立認知與電腦高科技犯罪偵查之素養。

筆者捨棄以導論方式呈現該手冊而改以全文翻譯，其目的有三：

一、兩國法系不同，在論述上如以大陸法系觀點無法完全切入，而筆者並無海洋法系實務經驗，如以海洋法系觀點並非筆者所能勝任。

二、全文翻譯可使讀者獲取第一手資訊。藉達他山之石之目的。

三、本文僅為犯罪偵查之操作手冊，並非法學著作，屬於工具書類，藉此翻譯挑起軍法同仁撰寫相關實務運作手冊之熱心。軍事檢察官為犯罪偵查主體，理當指導國軍其他具有犯罪調查權責之機關。以樹立軍法威信。

目前，美國有關電腦犯罪偵查之手冊業由司法部整合國防部、與其他聯邦偵防機關之資源，編撰「電腦扣押與搜索以及獲取電子證據之犯罪偵查」乙書（Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations），提供檢察機關與各級犯罪偵查機關參考，如有興趣可至：http://www.cybercrime.gov/s&smanual2002.htm 下載。

* 柴漢熙，美國聖母大學法律研究所碩士，前國防部軍法司軍法官，龍華科技大學企管系講師。

GUIDE OVERVIEW

This handbook is designed to assist both Office of Special Investigations (OSI) Special Agents (SAs) and Air Force Judge Advocates (JAs) in conducting computer crime investigations and prosecutions. While the term "computer crime" can conjure up colorful images of a computer committing any number of offenses, the truth is there is always a person (currently, at least) behind the keyboard. In fact, most computer crimes involve behaviors that are already prohibited (Trespass, Theft, Espionage, etc.); it just happens that a computer has been added to the equation. Despite these ties to tried and true common law concepts, computer crimes can present surprisingly complex legal issues that require a thorough understanding of not just the applicable law, but also of how computers actually function. (We have included a small Glossary (Appendix 1) which contains some of the more commonly encountered terms.) Readers are cautioned that this Guide is intended to serve as an introduction to the subject area and should not be viewed as a definitive analysis.

We also recommend that readers consult the *Department of Justice Federal Guidelines on Searching & Seizing Computers (1994) (DoJ Guidelines) as well as their 1997 Supplement To Federal Guidelines For Searching and Seizing Computers (DoJ Supplement)*. Given the high percentage of AF computer crime cases involving civilians these two documents are essential reading in any computer crime case. The full text of both the *DoJ Guidelines* and the *DoJ Supplement* can be found on DoJ's website,

手冊導覽

手冊設計目的在協助美國空軍特別調查處（以下稱特調處）的調查官與空軍軍法官，進行電腦犯罪的偵查工作。每當我們面對電腦犯罪這個名詞時，總會想像許多「電腦」去從事犯罪行為的畫面。實際上，至少就目前的情形而言，應該是自然人在電腦鍵盤上的行為。事實上電腦犯罪包含許多被禁止的行為？，諸如：無故侵入（Trespass）、竊取（Theft）、間諜（Espionage）等等。犯罪發生的時候，電腦不過被人增刪或複製某些程式。儘管所展現的面貌是案件、審判以及法律概念的組合，然而電腦犯罪所帶來的是令人驚訝的複雜性與法律爭議性，因此不僅需要全然明白法律的適用，同時也要瞭解電腦的實際運作。導覽只是主題簡介，而非詳盡的解析。

同時，我們建議讀者能夠參閱「聯邦司法部門對電腦搜索與扣押的指導要領」（Department of Justice Federal Guidelines on Searching & Seizing Computers (1994)，DoJ Guidelines）乙書，以及相關補充資料。就空軍的電腦犯罪案件而言，涉及非軍人犯罪的比例偏高，閱讀前開書籍，對於處理所有的電腦犯罪案件是非常有必要的。有關聯邦司法部門的指導要領與補充料可以透過網址 www.

www.usdoj.gov/criminal/cybercrime.

In the first chapter we start out discussing the various military laws that may be brought to bear against military computer criminals. As the reader will soon learn, the Uniform Code of Military Justice (UCMJ) does not contain any prohibitions specifically designed to deal with computer crimes. Accordingly, most military prosecutions for computer-unique crimes are brought under the federal civilian criminal statutes. Additionally, several of these same federal statutes control how we investigate computer crimes, so a thorough discussion of those statutes follows.

Anyone who works in this field will soon run headlong into a discussion of the Electronic Communications Privacy Act (ECPA), which was signed into law on 21 Oct 86 by President Reagan. Designed to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies, the Act contains three titles. Title I of the Act amended the federal wiretap statute to protect against the unauthorized interception of **real-time electronic (computer) communications**. (This portion of the ECPA is discussed in detail in Chapter 2.) Title II created a new series of statutes, 18 U.S.C. § 2701-2711, that are designed to protect **stored wire and computer communications**, such as electronic mail (e-mail), and customer records. (Discussed in Chapter 3.) The final section of ECPA, Title III, addressed pen registers and trap and trace devices, which are more fully discussed in Chapter 4.

Chapter 5 is designed to illuminate the pit-

usdoj.gov/criminal/cybercrime的網站中取得。

第一章我們討論軍事刑法對於軍中電腦犯罪案件的適用。讀者可以立即明瞭，在統一軍事法典中（the Uniform Code of Military Justice，UCMJ），並無特別為電腦犯罪訂定任何法律規範。因此，所有單純的電腦犯罪案件，都是依照聯邦法的一般刑事法起訴。此外，對於電腦犯罪的偵查手段亦由聯邦法的刑事法所規範，因此，接續詳細討論有關電腦犯罪偵查的法律規定。

任何從事電腦犯罪偵查領域的人員，必須全心全力投入電子通訊隱私權保護法案（Electronic Communications Privacy Act，ECPA）的研討，該法案於一九八六年十月廿一日由雷根總統公佈執行。本法依據變化多端的電腦電訊科技，設計出聯邦法明確且符合時代所需之保護隱私權措施與標準，本法區分三大部分，第一部分為聯邦防範竊聽保護修正條款，藉以對抗未經授權之線上攔截電子（電腦）通訊資料行為（real-time electronic /computer communications）。（這部分第二章討論）。第二部分為保護有線通訊與電腦通訊所儲存之資料（stored wire and computer communications），例如電子郵件或客戶記錄等資料，因而建立一系列法規即聯邦法第 2701-2711 條（18 U.S.C. § 2701-2711）。（第三章討論）第三部分則討論電話撥號音攔截器、設立陷阱與證據調查等項，此於第四章討論。

第五章則是討論一九八〇年的隱私權保

falls created by the Privacy Protection Act (PPA) of 1980, which is codified as 42 U.S.C. § 2000aa.

The next two chapters concentrate on the various sections of statutory law that hold special significance in the investigation of computer-related crimes. In Chapter 6, we finally get to what some agents might consider the meat of this work, the laws that are designed to deal with hackers or intruders. In this chapter, we discuss 18 U.S.C. § 1030, which was initially enacted in 1986. This statute has been amended several times since then and is designed to prohibit most intruder conduct by relying largely upon the common law of trespass. A related statute is 18 U.S.C. § 1029, which, among other things, prohibits the unauthorized use, possession, and distribution of "access devices" or as they are more commonly known in computer parlance-passwords. Passwords and their related log-ons are the currency of the hacker and are readily traded as they allow the recipient to gain unauthorized access without having to commit another break-in. A "companion" statute is 18 U.S.C. § 1028, which Congress recently amended via The Identity Theft and Assumption Deterrence Act of 1998, {Public Law 105-318, 30 Oct 98}. The increasing sophistication of personal computer (PC) publishing software coupled with high-resolution color printers has allowed criminals to create documents so as to assume another person's identity, with all the financial mischief that entails.

Chapter 7 contains a limited discussion on the laws pertaining to child pornography. 18 U.S.C. § 2552 was the original statute that dealt

護法案（Privacy Protection Act，PPA of 1980）中的陷阱，也就是聯邦法第 2000aa 條（42 U.S.C. § 2000aa 的法條。）

接續次兩章則是討論各項法規，對於電腦犯罪案件的偵防具有特殊意義的規定。第六章對許多調查員而言，則是精髓所在，換言之，有關對於電腦駭客與侵入者的法律規定，就是討論聯邦法第 1030 條（18 U.S.C. § 1030）的規定。該法於一九八六年開始執行，期間多次修正，大多依據英美法的「無故侵入」（the common law of trespass）規範，作為禁止大多數電腦侵入行為的基礎。相關法令載明於聯邦法第 1029 條（18 U.S.C. § 1029），主要規範有禁止無故使用、擁有或處分所謂的登入電腦程式的裝置，通俗的說法就是開機密碼。密碼與登錄程式對駭客而言具有財產價值，而且便於交易，使買主得以無故登入他人電腦而無須承擔無故侵入的罪責。此外討論聯邦法第 1028 條（18 U.S.C. § 1028），國會藉由「竊盜認定與妨害行為推定法案」（The Identity Theft and Assumption Deterrence Act of 1998）而修正通過的法律。由於優異印刷軟體配合使用高解析度的印表機，透過電腦可以讓犯罪者輕易的創造出他人的證明文件，使其蒙受金融上的損害。

第七章包含一些有關規範猥褻兒童圖像（child pornography）的局部性討論。聯邦法第 2552 條（18 U.S.C. § 2552）就是規範猥褻

with child pornography. In 1996, this statute was amended to include child pornography being distributed over the Internet. At the same time, a new companion statute, 18 U.S.C. 2252A, was enacted. 18 U.S.C. § 2252A was primarily designed to combat the growing problem of "morphed" child pornography images and criminalized the creation, use, and possession of such images. This new act has some controversial sections and constitutional challenges are widely anticipated.

Finally, in Chapter 8 we provide a brief refresher on some search and seizure issues, especially as they relate to computers and electronic information.

Law has historically lagged many years behind technological advances and with the rapid advances in information technology, the problem is amplified in the area of investigating and prosecuting computer crimes. We recently heard a saying that graphically illustrates this perceived shortfall -- " The Internet moves at the speed of light, while the law moves at the speed of Congress." While the future will undoubtedly bring more fine-tuning of existing laws and the enactment of new ones, we were surprised at the relatively low number of reported court decisions. We believe this dearth of cases is caused by three factors: (1) significant portions of the intruders are juveniles who are seldom prosecuted; (2) those who were prosecuted have pled guilty to obtain plea considerations from prosecutors and/or leniency from the courts; and (3) the criminal penalties associated with much of Chapter 47 in Title 18 do not lend themselves to appellate litigation.

兒童圖像的原始法條。在一九九六年，這些法條經過修正後，在網際網路上禁止提供猥褻兒童圖像的行為亦屬其中規範。同時，另一條文聯邦法第 2552A 條（18 U.S.C. § 2552A），業已修正通過付諸實施。該條文主要對抗日益滋生的猥褻兒童圖像事業，將創造、使用或持有猥褻兒童圖像行為訂為犯罪行為。該條文具有部分爭議，以及違憲挑戰的廣泛呼應。

最後，第八章我們在搜索與扣押（search and seizure）的主題上，提供簡明的更新概念，尤其是涉及電腦或電子資訊。

法律在成長上，一直落後科技進步許多年，在資訊科技的快速成長上，法律更顯遲鈍。因此在調查或起訴電腦犯罪的事務上，問題更為凸顯。我們最近聽到一種說法，如果以圖表來描繪二者的明顯差異：「當網際網路以光速向前邁進，而法律則是以國會的速度緩步向前」。無疑地，未來將會帶來更多法律修正案以及制定新法律，然而我們十分訝異法院對於電腦領域的判決是如此稀少。我們相信如此稀少的原因有三：⑴大多數的電腦駭客是少年犯，因此無法被起訴。⑵大多數的被告向檢察官以認罪協商程序獲得減刑，或者由於法官的寬宏大量。⑶由於刑罰的附屬條件無法促使被告上訴。

Accordingly, situations may arise for which there are no approved solutions, but only "educated guesses" as to how the laws may be interpreted and what procedures should be followed. Given these uncertainties, the philosophical perspective adopted in this Guide is, when in doubt, lean toward obtaining appropriate permissions or consent prior to conducting any search. Given the frequent urgency of computer crime investigations, the investigative procedures should be kept as simple as possible and the level of permissive authority (whether Installation Commander, AFOSI Commander, Air Force General Counsel, or Federal Magistrate, etc.) kept as low as possible.

Finally, while there are many technical differences between investigating computer-related crimes and investigating more traditional cases, agents should not forget their basic investigatory training. In many cases it may not be the evidence in the computer that seals the case but the notes found in the desk drawer. Agents must guard against becoming overwhelmed by the technical aspects of the case and should remain focused on the "who, what, where, why, and how" of the case.

Having said that, however, agents should be very sensitive in handling electronic evidence. Given the public's general lack of understanding in how computers work and the unique vulnerabilities and perishability of electronic evidence, special care should be exercised to ensure that the evidence is protected from damage or potential claims of alteration. Most, if not all, of these issues can be avoided if agents ensure that proper evidence handling procedures are ob-

許多訴訟上爭議發生，就是因為缺乏一套標準的解決方法，只有學術上的推論，諸如法律應該如何的解釋？法律程序應該如何進行？由於上述的不確定因素，本文的所採取的前瞻概念是：當有任何疑慮時，於搜索前先行取得適當的允准或同意。就電腦犯罪案件偵查的急迫性而言，調查程序應盡量保持單純化，而授權層級（不論是基地指揮官、特別調查處處長、空軍法律總顧問或聯邦簡易法庭法官）應越低越好。

最後，涉及電腦犯罪案件的偵查較諸一般犯罪案件，具有更多的科技性，然而調查員仍應保持基礎的調查技巧。許多案件發現，主要的證據並非直接透過電腦所發現的，而是在被告的辦公室抽屜中發現蛛絲馬跡。調查員應該提高警覺，不要被案件的科技面相所充塞，而是將焦點放案件中的人、事、地、為何、如何等重點上。

承如前述，不論如何，調查員應有敏銳的態度來處理電子證據。由於大多數人對於電腦運作並非十分清楚，同時也不了解電子證物具有脆弱與易於毀損的特性，因此在特殊案件的調查中，應加強保護電子證據免受損害，或者被篡改的可能。如果調查員能夠遵行正確的證據保護程序，許多電子證物毀損的情形就能夠避免，同時一個強而有力的

served and that a strong chain of custody is maintained. As the law evolves to deal with new technology, remember that computer cases are just like all other investigations in one critical respect; there is no substitute for sound judgment.

CHAPTER 1 -- U.C.M.J. ARTICLES RELEVANT TO COMPUTER CRIME OFFENSES

Introduction

It may surprise the reader to learn that the Uniform Code of Military Justice (UCMJ) does not contain any articles that specifically prohibit computer-unique crimes. However, this does not mean that persons subject to the UCMJ are free to commit wanton acts via a computer. Under the General Article, Article 134, UCMJ, the military is able to borrow or assimilate the federal and in some cases state statutes. This process allows the military to hold its members accountable for laws that apply to the general population while still maintaining internal discipline. Accordingly, the computer-related laws we will discuss in Chapters 5-6 and those listed in Appendix 2, have equal application to our military personnel.

Detailed Analysis

Under Article 92, UCMJ, Failure to Obey Order or Regulation, military personnel can be charged with failing to obey an order or general regulation, provided that the regulation is "punitive." Not all regulations are punitive. But even non-punitive regulations can serve to establish a

證物監管環節就得以維持。當法律開始涉及新科技時，切記，調查電腦犯罪案件與其他案件相同地具有嚴苛的一面，沒有任何事物能夠替換案件的勝訴（被告被定罪）。

第一章——美國統一軍法典對電腦犯罪的相關法律規定

簡　介

美國統一軍法典（以下簡稱軍法典）[1]對於電腦犯罪行為並無特定規範，然而並非意味著軍事人員，可以透過電腦為所欲為而無法可管。軍法典總則即第 134 條規定，軍法典未規定者得適用聯邦法律，或得適用州法律。因此本項適用規定使軍方得以約制成員遵行一般法律，同時藉此維持內部紀律。因而電腦犯罪的法律規範，當然一體適用於軍事人員，此於第五、六章討論。

細節分析

軍法典第 92 條規定：「受軍法管轄之人員無故違反命令或法規時，而該命令或法規具有刑罰性（punitive）時，即構成抗命或違反規定等罪」。但是非刑罰性法規，而其目的係為建立一項職責時，違反該項法規即為

1 the Uniform Code of Military Justice ，UCMJ

duty, the breach of which can be the basis for a dereliction charge. Further, even regulations intended to be punitive may not be worded as clearly as one might hope. Accordingly, SAs should consult with their servicing JA prior to undertaking any investigation under Article 92. As an example, AFI 33-129, *Transmission of Information via the Internet*, is a punitive regulation governing roles, responsibilities and procedures of personnel using and maintaining Internet access. The following activities, listed in paragraphs 6.1.1 - 6.1.12, are specifically prohibited:

6.1.1. Any use of government-provided computer hardware or software for other than official and authorized government business.

6.1.2. Activities for personal or commercial financial gain. This includes, but is not limited to, chain letters, commercial solicitation, and sales of personal property.

6.1.3. Storing, processing, displaying, sending, or otherwise transmitting offensive or obscene language or material. Offensive material includes, but is not limited to, "hate literature," such as racist literature, materials or symbols (for example, swastikas, neo-Nazi materials, and so forth), and sexually harassing materials. Obscene material includes, but is not limited to, pornography and other sexually explicit materials.

6.1.4. Storing or processing classified information on any system not approved for classified processing.

失職罪的構成要件。更進一步而論，許多刑罰性法規的字面的意義卻常與一般人的認知並非吻合。因而調查官著手調查第 92 條犯罪案件之前，應與軍法官保持密切聯繫，以獲得諮詢意見。試舉一例，如空軍訓令[2] 第 33-129 條（有關網際網路傳輸資訊方面）即為刑罰性法規。係針對網際網路使用者或網際網路登錄許可持有者之行為、責任以及使用程序予以規範。列舉下列條文說明之。

6.1.1 凡使用政府所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，如（非列舉）連鎖信、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。侮辱性的物品如（非列舉）激發仇恨心理之文書；種族主義刊物、資料、標誌等（例如，納粹十字標誌、新納粹文字刊物等等），以及性騷擾的物品。至於淫穢性的物品如（非列舉）色情圖像，以及其他詳細描繪性愛的物品。

6.1.4 未經核定使用分類保密資料等級的電腦系統、儲存或處理分類保密資料。

6.1.5 未經原創者或出版者同意，儲存或處分經著作權保護的物品（包含卡通圖

2 Air Force Instruction

6.1.5. Storing or processing copyrighted material (including cartoons) unless approval is obtained from the author or publisher.

6.1.6. Participating in "chat lines" or open forum discussion unless for official purposes and after approval by appropriate Public Affairs channels.

6.1.7. Using another person's account or identity without appropriate authorization or permission.

6.1.8. Viewing, changing, damaging, deleting, or blocking access to another user's files or communications without appropriate authorization or permission.

6.1.9. Attempting to circumvent or defeat security or auditing systems without prior authorization or permission (such as for legitimate system testing or security research).

6.1.10. Obtaining, installing, copying, storing, or using software in violation of the appropriate vendor's license agreement.

6.1.11. Permitting any unauthorized individual access to a government-owned or government-operated system.

6.1.12. Modifying or altering the network operating system or system configuration without first obtaining permission from the administrator of that system.

On the other hand, the original 1 March 1997 version of AFI 33-119, *Electronic Mail Management and Use*, was not issued as a punitive regulation. However, this Instruction has been updated and the new version, dated 1 March 99, is intended to be punitive. Therefore, after 1 March 99, all subsequent violations could be charged under Article 92. Paragraphs 3.1

畫）。

6.1.6 非公務所需，或結束公務後未經允准，透過公關事務頻道登入聊天網，參與公開討論事務。

6.1.7 未經授權或允准，使用他人專用密碼或識別碼登入電腦系統。

6.1.8 未經授權或允准，閱讀，更改，毀損，刪除或阻滯他人所有之登入程式或未經許可登入電腦系統或通訊系統。

6.1.9 未經授權或核准（例如以測試系統方式或檢查電腦安全系統方式等理由），企圖使用破解程式以矇騙系統程式登入或摧毀電腦的安全措施或審核程式（譯按：以程式來破解他人電腦系統的防火牆程式，駭客行為）

6.1.10 在侵害軟體經銷商的權利狀態下，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，登入政府管理或供公務用途之電腦系統。

6.1.12 未經電腦系統管理者之允准，修正或變更電腦網路作業系統或該系統之設定參數。

另一方面，1997 年 3 月 1 日頒佈的空軍訓令第 33 － 119 條（電子郵件管理與使用）原非具有刑罰性質，但是經由 1999 年 3 月 1 日之修正頒佈後反而變為刑罰性。從此之後，凡符合下列行為者就有軍法典第 92 條之適用。其中第 3.1 至 3.3 款界定使用公務電子郵件系統的範圍，並確立與電子郵件相關之犯

and 3.3 of the new version circumscribe the use of government electronic mail (e-mail) and identify e-mail-related offenses;

3.1…. Members of the Air Force or civilian employees may use a government-provided E-mail communications system only for official or authorized use. Any other use is prohibited.…

3.1.1. E-mail is subject to the requirements of the Freedom of Information Act and the Privacy Act of 1974.

3.1.2. Use caution when sending E-mail to a large number of recipients. Digital images as well as mass distribution of smaller messages may delay other traffic, overload the system, and subsequently cause system failure.

3.1.3. Use caution when sending an E-mail message to mail distribution lists. Use electronic bulletin boards or E-mail public folders for nonmission-related E-mail (e. g., 'Car Wash'). Imprudent use of address lists clogs E-mail accounts and often clutters in-boxes.

3.3…. Air Force E-mail systems are provided to support the Air Force mission. Use E-mail systems only for official uses or for authorized personal use as explained below. . ..

3.3.1…. Official use includes communications, including emergency communications, the Air Force has determined necessary in the interest of the Federal government. Official use includes, when approved by the

罪行為。

3.1 空軍官兵或聘雇人員，非於授權或公務用途之情形下，不得使用公務電子郵件系統。

3.1.1 電子郵件適用於資訊自由法案[3]與 1974 年隱私權保護法案[4]。

3.1.2 傳送大量郵件應謹慎為之。傳送數位影像或大量信件，易致網路擁塞，或使電子郵件系統超載導致當機。

3.1.3 使用群組功能傳送電子郵件應謹慎為之。非勤務用途時（例如發信給洗車公司），得使用電子公告欄（BBS）或公用電子信箱。輕率使用群組功能，易致阻塞電子郵件帳號，或致使電子信箱資訊紊亂。

3.3 空軍電子郵件系統僅供空軍官兵公務用途。所謂公務用途或授權使用之定義如下列說明。

3.3.1 公務用途包含一般通訊與緊急通訊。由空軍依據聯邦利益原則，決定通訊之需要性。空軍官兵或聘雇人員於公勤在外期間，經勤務所在地指揮官依據現況與權益考量所允准之通訊亦屬之。

3.3.1.1 下列使用公有通訊系統之行為非屬公務用途，應予禁止。

---

3 Freedom of Information Act

4 Privacy Act of 1974

theater commander in the interest of morale and welfare, those communications by military members and other Air Force employees who are deployed for extended periods away from home on official business.

3.3.1.1. The following do not constitute official use of governmental communications systems and are prohibited.

3.3.1.1.1. Distributing copyrighted materials by E-mail or E-mail attachments without consent from the copyright owner.

3.3.1.1.2. Sending or receiving E-mail for commercial or personal financial gain using government systems.

3.3.1.1.3. Intentionally or unlawfully misrepresenting your identity or affiliation in E-mail communications.

3.3.1.1.4. Sending harassing, intimidating, abusive, or offensive material to, or about others.

3.3.1.1.5. Using someone else's identity (User ID) and password without proper authority.

3.3.1.1.6. Causing congestion on the network by such things as the propagation of chain letters, broadcasting inappropriate messages to groups or individuals, or excessive use of the data storage space on the E-mail host server.

3.3.2.… An agency designee may authorize limited personal use of government-provided E-mail communication, when it:

3.3.2.1. Serves a legitimate public interest,

3.3.2.2. Conforms with theater commander-in-chief (CINC) and MAJCOM policies,

3.3.2.3. Does not adversely affect the performance of official duties,

3.3.1.1.1 非經著作權人之同意，使用電子郵件系統、或以系統之附檔功能（attachment），傳送受著作權保護之資料

3.3.1.1.2 利用公有電子郵件系統，做為私人使用、收益用途。

3.3.1.1.3 以不法之意圖，利用公有電子郵件系統，導誤個人辨識或登錄資料。

3.3.1.1.4 傳送騷擾性、濫權且具威脅性或其他相類之資料。

3.3.1.1.5 未經授權，於公有電子郵件系統使用他人的電子郵件帳號與密碼。

3.3.1.1.6 意圖阻塞網路系統而發送連鎖信或不適當資料予公眾或他人。或儲存巨量資料於電子郵件系統伺服器內，以佔據伺服器磁碟空間。

3.3.2.… 主管單位得限制個人使用公有電子郵件通訊系統，惟須符合下列情形：

3.3.2.1 符合公眾利益與法定用途。

3.3.2.2 依據戰場指揮官與空軍總部之政策。

3.3.2.3 對勤務之遂行無負面之影響。

3.3.2.4 在合理的期限與使用頻率下，限定於個人時間使用（諸如下班後或午餐時間）

3.3.2.5 使用群組方式傳送郵件，不致對通訊系統產生負載。

3.3.2.6 對於國防部或空軍不會產生鉅額支

3.3.2.4. Is of reasonable duration and frequency, and whenever possible, is made during personal time (such as after-duty hours or lunch time),

3.3.2.5. Does not overburden the communications system with large broadcasts or group mailings,

3.3.2.6. Does not create significant additional costs to DoD or the Air Force, and

3.3.2.7. Does not reflect adversely on DoD or the Air Force (such as uses involving pornography, chain letters, unofficial advertising, soliciting or selling, violations of statute or regulation, inappropriately handled classified information or other uses that are incompatible with public service).

3.3.2.8. Examples of authorized limited personal use include, but are not limited to:

3.3.2.8.1. Brief communications made while traveling on official business to notify family members of official transportation or schedule changes.

Additionally, Series 33 Policy Directives cover communication and information-related activities. Violations of some of the AFIs that fall under this series and other related AFIs might be the basis of additional charges under Article 92. For example:

AFI 33-107, Volume 3, *Strategic Automated Command Control System-Data Transmission Subsystem (SACCS-DTS) Network Security Plan;*

AFI 33-113, *Managing Messaging and Data Processing Centers;*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP));*

出；而且

3.3.2.7 對於國防部或空軍不會招致負面形象（諸如：傳送色情圖像、連鎖信、非公用之商業廣告、推銷、招募、違反法令或不當處理機密資訊等用途，或與公眾利益不符之用途）

3.3.2.8 限制個人使用之情形應予列舉，下列非屬限制情形：

3.3.2.8.1 官兵、聘僱人員於公差期間，以簡短信息，使用公有電子郵件與家屬說明公差旅運與行程變更之消息。

此外，空軍訓令第 33 條各款項之命令涵蓋通訊與資訊相關之活動。官兵如違反相關規定，即有可能依據軍法典第 92 條起訴。相關規定內容有：

空軍訓令第 33 － 107，第 3 輯，戰略自動指揮系統－資料傳輸分系統網路安全計畫。

空軍訓令第 33 － 113，通訊管理與資料處理計畫

空軍訓令第 33 － 219，電信控管與風險評估計畫

空軍訓令第 33 － 322，記錄管理計畫

空軍訓令第 51 － 902，空軍官兵、聘僱人員

AFI 33-322, *Records Management Program;*
AFI 51-902, *Political Activities by Members of the US Air Force; and*
AFI 51-903, *Dissident and Protest Activities*.

Finally, the Joint Ethics Regulation (JER) prohibits the use of government property for unofficial purposes 5 CFR 2635.101(b)(9), JER section 2-100. The standard is set out at 5 CFR 2635.704 and provides that "an employee has a duty to protect and conserve Government property and shall not use such property, or allow its use, for other than authorized purposes." Under JER 2-301.a., communications systems and equipment (including computers, telephones, and fax machines) are for *official use* and a *uthorized purposes only*. Both of these terms are defined in the JER -- official use at JER 2-301.a.(1) and authorized use at JER 2-301.a.(2) - and both contain provisions which will allow certain minimal personal use once that use is approved by a "theater commander" and "agency designee", respectively. Our readers are cautioned that not all provisions of the JER are punitive and so care must be taken when drafting charges. OpJAGAF 1996/70, 6 May 96, contains an excellent discussion on how to charge misuse of government property under the JER.

Depending upon the facts of the case, several other UCMJ articles may be of assistance in the substantive prosecution of a computer crime investigation. The following summary, which is not all inclusive, is intended to assist both SAs

參與之政治活動，或
空軍訓令第 51 － 903，與空軍、國防部之抗爭運動。

最後，聯合品德規範[5]明定，非公務目的不得使用政府財產[6]。有關標準設立於聯邦法規 2635.704 之條文中，即「政府機構之受雇人，有保護並維持政府財產之義務，且於非經授權之情形下，不得使用或允准他人使用之」。聯合品德規範 2-301, a 規定，通訊系統與設備包含電腦、電話、傳真機等，非公務用途或非經授權不得使用。有關「公務用途」與「授權」等名詞在聯合品德規範 2-301, a（1）、2-301, a（2）中有明確的定義。惟條文規定「如係經由指揮官與其主管單位同意時，於私人用途上，得有限度的使用該通訊系統與設備」。由此可知，聯合品德規範條文有例外規定，起訴違反聯合品德規範之犯罪行為時務必謹慎。可參考空軍軍法專刊：「如何起訴有關違反聯合品德規範而使用政府財物之犯罪」一文[7]，其中有專論性的研討。

歸納以往電腦犯罪案件，發現適用軍法典其他條文以起訴被告。謹摘錄部分條文，俾使軍法官與調查官在偵查電腦犯罪之始，即能注意其他相關犯罪行為。

---

5 Joint Ethic Regulation JER
6 參閱 5 CFR 2635.101(b)(9) ，JER Section 2-100
7 OpJAGAF 1996/70，1996.5.6

and JAs in focusing on the relevant violation(s) at an early point in the investigation.

Article 106a: Espionage. Any AF member who transmits a document or other information with the intent or reason to believe that the document or other information will be used to injure the United States (or to the advantage of a foreign nation), is subject to court martial for espionage. *United States v. Peri*, 33 M.J. 927 (ACMR 1991).

Article 107: False Official Statements. Using another person's password could constitute a false official statement. No distinction should be made whether the entity receiving the statement was a person or a machine. The SA should ensure whether the statement or password was required for gaining illegal access to the computer system. The focus must be on "an official statement", and whether supplying a password to gain access to a computer system is akin to making an official statement. A separate issue is whether the user inputted or caused false information to be inputted into a computer program in an attempt to defraud the government of money, goods, or services. Article 107 was one of the offenses charged in *United States v. Casey*, 45 M.J. 623 (N. M. Ct. Crim. App. 1996.) In this guilty-plea case, a military investigator was detailed to assist the defense on technical issues relating to the BEQ computer records that Casey (a billeting desk supervisor) had falsified, which formed part of the prosecution's evidence of the underlying offenses char-

第 106a 條：間諜罪（Espionage）

空軍人員於傳送文件或資訊，依據行為人主觀意圖或客觀情事，如處分該項文件或資訊足使美國政府利益受損，或對他國政府獲有利益時，此即為軍事法庭管轄之間諜罪，參閱 Peri 案件[8]

第 107 條：偽冒公務識別罪（False Official Statments）

使用他人電腦密碼即可能構成此罪，至於是否藉由人員或機器判讀，則非所問。調查官應先確認偽冒識別或密碼之目的，係為登入電腦系統。因此應將重點置於公務認證的識別物，凡是使用密碼登入公用電腦系統即為公務識別行為。因此具備二項關鍵行為即屬之：行為人輸入他人的識別碼登入電腦系統；或輸入造成誤判的資訊而登入電腦系統，而其目的通常為詐騙政府的財物或供給。第 107 條曾適用於 Casey 案件[9]。此為被告認罪案件，經查被告（職務為軍官宿舍分配督導官）以偽冒公務識別碼登入電腦系統並獲取軍官宿舍的分配記錄，而該項分配記錄即為本案犯罪證物。

---

8 United States V. Peri 33. M. J. 927

9 United States V. Casey 45. M. J. 623

ged.

Article 108: Damage to Military Property. Computer files on a laptop computer hard-drive constitute military property and can be the basis for prosecution. *United States v. Walter*, 43 M.J. 879 (N. M. Ct. Crim. App. 1996). Files on a command hard-drive are military property. *United States v. Peterson*, No. 29341, 1993 WL 52600 (A.F.C.M.R. 1993).

Article 121: Larceny and Wrongful Appropriation. Article 121 defines larceny and wrongful appropriation as the wrongful taking, obtaining, or withholding, "by any means, from the possession of the owner or any other person any money, personal property, or article of value of any kind." However, military courts have, to date, required that the object of the computer theft be tangible property, such as a printed document. In *United States v. Ramelb*, 44 M.J. 625 (A. Ct. Crim. App. 1996), the accused used his government computer to create two fictitious pay accounts which netted him approximately $28,000, a bad conduct discharge, confinement for three years and forfeiture of all pay and allowances. See also, *United States v. Meng*, 43 M.J. 801 (A.F. Ct. Crim. App. 1996).

Although *United States v. Collins*, 56 F. 3d 1416 (D.C. Cir. 1995) is not a military case, it is interesting reading on the issue of wrongful appropriation. In that case, Collins was a civilian employee for the Defense Intelligence Agency (DIA), who, for five years, used his gov-

第 108 條：毀損軍用財物罪（Damage to Military Property）

電磁記錄或硬碟中之電磁記錄屬於軍用財物，即為本條保護之客體[10]。參閱 Walter 案件與Peterson案件[11]均認定存放於硬碟（指揮系統主機）的電磁記錄屬於軍用財物。

第 121 條：竊盜與侵占罪

本條將竊盜與侵占罪定義為：「以不正當方法取得、或持有所有人或第三人所管理之金錢或具有經濟價之物」。軍事法庭的見解至今不變：藉由電腦所竊取之物必須為實體可見，例如已完成列印之文件。在Ramelb案件[12]，被告使用其持有之公務電腦，製作二個虛構人頭帳戶，被告從中獲益將近二萬八千美元。被告除以行為不檢遭撤職外，並處以有期徒刑三年，追繳其所得之不正利益。軍事法庭於 Meng 案件[13]亦採相同見解。

另外，Code案件並非軍法案件，但是司法機關對於侵占的見解值得閱讀。本案被告Code 為國防情報局（Defense Intelligence Agency D.I.A.）聘雇人員。利用其持有之公務電腦與影印機，為其所參加之交際舞社團製

10 United States V. Walter 43. M. J. 879
11 United States V. Peterson A.F.C.M.R.1993
12 United States V. Ramelb 44. M.J.623
13 United States V. Meng 43. M.J.801

ernment computer and copier to produce newsletters for his ballroom dancing group. Collins was convicted of converting government property valued at more that $100 in violation of 18 U.S.C. § 641 and appealed arguing that this statute only criminalized conversion of tangible property. The Appellate Court explicitly held that "the statute encompasses a prohibition on the conversion of intangible property" however, they found that the government had failed to prove that Collins had "converted to his own use the government's computer time and storage." (*Id*, at pages 1419-1420). On page 1420, the Court wrote: "Guided by these principles, we conclude the government provided insufficient evidence that appellant converted to his own use the government's computer time and storage. The cornerstone of conversion is the unauthorized exercise of control over property in such a manner that serious interference with ownership rights occurs." The Court did, however, sustain his conviction for the use of the government copier.

Article 123: Forgery. This Article has been used to prosecute a subject for the altering of keypunch cards before the cards were used to process payroll checks by the computer. *United States v. Langston*, 41 C.M.R. 1013 (AFCMR 1970). The subject's action allowed him to increase his payroll check. Even though the accused did not actually make false writings, his alteration of the computer input to increase the face amount of the check constituted a forgery. This analogy should hold true in all instances where a person has altered the computer's operation.

作週報達五年之久。地院判決 Code 侵占政府財產價值逾美金一百元，觸犯聯邦法第 641 條。Code 在上訴理由狀中強調，侵占罪所保護的客體必須為實體物。上訴法院明確的判決本條包含非實體財物在內。而上訴法院對於「使用公務時間」部分認定檢察機關並未提出足夠證據，證明被告以公務時間使用公務電腦製作私人週報。判決書（1420 頁）中寫道：「依據法律原則的規範，我們認定檢察官對於上訴人以公務時間使用公務電腦製作私人週報乙節，提出的證據不足以證明上訴人犯罪。侵占罪的其中要件在於非經授權，處分公用財物，因而嚴重的干擾政府所有權」。無論如何，上訴法院仍然因為上訴人使用影印機部分而維持原判。

第 123 條：偽造罪（Forgery）

本條大多適用在變更電腦薪資辨識卡之案件。例如 Langston 案件中[14]，被告藉由改變電腦薪資辨識卡來增加自己的薪資所得。整個過程中並沒有任何傳統上所認為的偽造文書行為，只是略為改變電腦輸入致使支票面額增加，此即足以構成偽造罪。因此得以推論，凡改變電腦運作方式，不論是在輸入或是程式運作階段，其效果可產生一個偽冒

14 United States V. Langston 41 C.M.R. 1013

ation, at either the input or programming states, to effect the creation of a forged (electronic or hard-copy) document. Computer-assisted forgery was also involved in *United States v. Erby*, 46 M.J. 649 (A.F. Ct Crim. App. 1997); a finance clerk used fictitious names and social security numbers on computer files and paper forms to create forged travel vouchers and orders which ultimately caused $24,000.00 to be electronically transferred into Erby's account.

Article 132: Frauds Against the United States. This article may provide a better remedy than forgery in those instances where the individual submits paperwork to set the computer crime in motion instead of altering the computer program. Entering false documents to receive a payroll or TDY check would be an example.

Article 133: Conduct Unbecoming an Officer. In *United States v. Russell*, 47 M.J. 412 (1998) the accused used his government computer to download Internet child pornography. Russell was convicted of one specification of conduct unbecoming an officer and a gentleman by using military computers to download pornographic materials, and one specification each of wrongfully receiving and possessing materials depicting minors engaging in sexually explicit conduct, in violation of Articles 133 and 134. In a pretrial statement he had admitted that he " guessed" that the females in the pictures were 13 years of age and older. Further, a pediatrician testified that, based on known medical standards, the females shown in the exhibits were

的（電子的或實體複製）文件均屬之。另外，Erby 案件[15]，被告身為財務辦事員，輸入被害人姓名與社會福利證號在電腦中建檔，並以書面表格建立冒領收據。結果使得二萬四千美元以轉帳方式落入被告的帳戶。

第 132 條：對美國政府詐欺罪（Frauds Against the United States）

當行為人提供文書資料方式藉由電腦犯罪，而非改變電腦程式。本條對於請求損害賠償比偽造罪較為周延。例如在電腦中輸入非真實的文書資料，藉以獲得薪資或出差旅費。

第 133 條：瀆職罪（Conduct Unbecoming Officer）

1998 年 Russell 案件[16]，被告使用公務電腦上網並下載猥褻兒童圖片。檢方以被告使用軍用電腦下載色情資料起訴，經判決係為瀆職，以及非法收受並持有兒童從事明確性行為圖片，分別構成第 133 條與 134 條之犯罪。預審時，被告供稱其「猜測」該圖片顯示之女性年齡約為十三歲以上。此外，婦科醫生到庭結證稱：就已知的醫學標準而言，圖片中女性不足十五歲半的年紀。最後陪審團員審查犯罪證物後，以客觀常理與經驗判

15 United States V. Erby 46 M.J. 649

16 United States V. Russell 47 .M.J. 412

not more than 15 ½ years of age. Finally, the members were able to look at the pictures and use their common sense and experience to conclude that the girls were under the age of 18. Therefore, CAAF found there was sufficient evidence from which "a rational trier of fact" could "find guilt beyond a reasonable doubt" and conclude that appellant knowingly possessed child pornography. Similar facts were the basis of a similar Article 133 charge in the landmark military computer crime case, *U.S. v. Maxwell*, 42 M.J. 568 (A.F.C.M.R. 1995.) The Court was partially upheld and partially reversed on appeal in *U.S. v. Maxwell*, 45 M.J. 406 (1996.)

Article 134: General Article. As stated earlier, this Article is used to incorporate or borrow various federal and state criminal statutes. The more commonly used federal statutes are discussed in the following chapters.

However, when the facts establish that "the accused's conduct was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces" this general article has been used for theft of intangible items such as time or services. Article 134 can be used to punish an offender caught willfully and unlawfully altering, concealing, removing, mutilating, or destroying a public record. The removal of a computer record would generally entail making a copy of the record, thereby leaving the original unaltered so as to minimize detection. Copying a computer record may be punishable under Article 134 by in-

定圖片中女性均未滿十八歲。經上訴後，空軍覆判庭認定事證明確，判決被告為「無庸質疑的有罪」。而 1996 年 Maxwell [17] 案件亦有相同的事證，符合本條犯罪要件，覆判庭判決一部駁回、一部發回更審。

第 134 條：總則條款（General Article）

承如前述，本法未規定，而聯邦法或州法有處罰規定者，適用該處罰規定。有關聯邦法適用部分將於下一章討論。

無論如何，事實證明被告行為在軍中損害命令或紀律時，或其行為本質上造成軍譽受損時，即有適用。而本條即曾適用於竊取非實體物，例如時間與勞務。不僅如此，亦適用於處罰行為人以不法之意圖，變更、隱匿、移轉、毀損、滅失公務記錄資料。行為人在移轉電腦資料時，通常都會保留原本，而進行未經許可之複製行為，在調查上也不易被查覺。此類行為之處罰適用第 134 條，其理論基礎源自 DiGilio 案件 [18]。被告未經許可，使用公務機具影印聯邦調查局之文件，

17 United States V. Maxwell 45 M.J. 406

18 United States v. DiGilio 538 F.2d 972 3rd Cir 1976 cert. Denied, 429 U.S. 1038 (1977)

corporating the same theory used in *United States v. DiGilio* 538 F.2d 972 (3rd Cir 1976), *cert. denied*, 429 U.S. 1038 (1977). In *DiGilio*, the defendant made unauthorized photocopies of FBI files using Government equipment. The unauthorized copies were considered Government records and the removal of the copies constituted theft under 18 U.S.C. § 641. The court held that "any record" under Section 641 also included the content of the record.

Now let's move our discussion to the appropriate federal laws.

該影印的資料，經認定係屬公務記錄資料，而移轉該項未經許可之影印資料與他人，即構成聯邦法第 641 條竊盜罪。法院判決指出：第 641 條所稱之「任何記錄資料」包含文件資料內容。下一章將討論聯邦法的適用。