你使用的 APP 安全嗎？

使用智慧型手機如同使用個人電腦一般，下載軟體或登錄社群網站，皆應時時保持戒心。

◎陳婠綺

隨著智慧型手機的普及與其功能越來越強大，如同一台隨身電腦，加上使用者將許多檔案、照片也存放於手機內，因此智慧型手機延伸出的資安問題已成為國人的重要議題。

現在隨處可見的「低頭族」，人手一支智慧型手機，想要下載各種 APP 軟體只要手指輕輕一按就能搞定。APP 市場競爭激烈，不少業者紛紛祭出「免費」軟體吸引消費者，但看似免費的背後，付出的可能是親朋好友的隱私。目前免費的 APP 資安軟體與付費版本最大的差異主要是功能上的不同，免費版本主要是提供基礎的偵測與防護，進階功能則必須購買付費版本。甚至有些 APP 本來是付費軟體，卻在重新上傳後，成為免費軟體，許多人不疑有他，還以為撿到便宜，就在不知不覺中掉入陷阱。Google 雖然在 Android Police 回報後，５分鐘內就將這些軟體下架，但下載數可能已經超過五萬次。更可怕的是，Google 本來還特別提供了名為 Android Market Security Tool 的工具，用以清除那些惡意軟體對手機所做的修改，從而防止手機在感染惡意軟體後，將手機中的重要資訊上傳給不法分子；結果這些歹徒居然也將 Google 開發的反木馬工具，改變成木馬化應用程式。這個軟體不但會蒐集手機中的相關資訊，傳送到遠端的網站，還會不經使用者允許就執行某些功能和動作，包括修改通話紀錄、攔截或監控訊息，以及下載影片等，可見手機惡意軟體的可怕程度，絕對不輸給個人電腦的惡意軟體。

事實上，相較於個人電腦用戶對下載軟體已有基本戒心，而智慧型手機用戶尚未建立起相同習慣，讓中毒的可能性大增。手機資安的問題，因為越來越多的社交網站都已推出多平台移動設備用戶端，而變得更加嚴重。這些行動裝置端的安全防禦，也比個人電腦端要差很多，加上咖啡廳、機場、旅館等公共場所提供的無線網路安全問題，讓網路犯罪分子可以利用的攻擊管道，變得越來越多。

現今網路正熱門的社群網站 Facebook，也可能成為駭客釣魚的釣餌；駭客假冒 Facebook 名義，發送假警告信件給使用者，但使用者卻不知道其內含釣魚網頁連結，讓使用者誤信帳號已遭檢舉為垃圾帳號，需於 24 小時內立即點選 email 內的連結進行帳號安全性確認，否則帳號將可能遭永久停用。使用者一旦點選該網址後，使用者將被導向特定網頁，該網頁貌似 Facebook 的安全檢測系統，要求使用者輸入註冊 Facebook 的 email 帳號、密碼及生日等個人資料；輸入該網頁所要求的訊息後，使用者將再被導向另一個網頁，並被要求提供信用卡等相關資訊，最後導致個資外洩。

近來人手一支智慧型手機，使用者個人的隱私風險，也經常暴露在各種惡意程式攻擊的威脅中，智慧型手機的資安問題逐漸浮現。由於現代人將許多重要的資料、照片、訊息都存放在智慧型手機中，手機一旦遺失就可能造成重大的個資外洩問題。現今的手機未必只是一支電話，它還

可能成為個人的錢包、身分證、電話簿及家庭相薄，當我們的行動裝置具有以上用途，若遭遺失或被盜，便會造成敏感資料外洩風險。再加上使用者十分依賴各項 APP 程式的功能，根據國外媒體報導顯示，許多手機應用程式的使用條款中，允許手機程式開發商可以查閱手機用戶的個人資料，甚至查看照片、通話對象等，個人資料就在不知不覺中外洩。許多手機用戶在下載付費或是免費的 APP 程式時，未詳閱程式使用條款即按下同意，此舉可能讓手機應用程式開發商有權搜尋手機內的相片，或是手機用戶的所在位置。社群網站 Facebook、Badoo、雅虎公司和照片分享網站 Flickr，皆坦承透過搭載 Android 系統的智慧型手機應用程式，可讀取手機用戶的簡訊。其餘不知名、免費下載的應用程式，大多在使用條款及條件中，也明確寫到有權取得用戶的個人資料。

程式開發商看準個人資訊能讓社群網站的定位更明確，若能提供更貼近使用者的服務則能增添網站的魅力，因此「個資」儼然成了所有業者最垂涎的商品。一項由臉書技術支援的雅虎公司服務，要求使用者提供宗教信仰、政治傾向才能進入；網路電話 Skype 也透過使用者拿到他們朋友的臉書照片和個資。雖然臉書要求 APP 在取得使用者的個資前，必須徵求使用者的許可，但若是朋友資料遭外流，當事人也不會收到任何通知。不少人開始擔心，這些看似免費的服務，實則賠上隱私代價，反倒是握有這些籌碼的業者，能吸引廣告主、APP 開發商或是更大的商機。

隨著手持行動網路的普及，資訊安全已從傳統電腦作業系統，擴展到手持裝置系統，部分消費者也開始建立智慧手機和平板電腦的防毒功能。但資安業者還是提醒民眾，除了安裝適當的防毒軟體之外，更應養成良好的手機使用習慣，以保護自身的資料安全。

面對日益氾濫的手機病毒，手機用戶也不是沒有預防之道，只要遵守下列防毒程序，還是可以將手機病毒有效隔離：

一、慎用藍芽裝置。就像流行性感冒一樣，病毒肆虐期間，如果到公眾場合，最好暫時關閉手機上的藍芽接收功能。如果有陌生的手機，或任何擁有藍芽裝置的機器請求連接，最好不要接受；就算是收到朋友傳送的多媒體簡訊，對於來路不明的手機程式，還是不要任意安裝。

二、接收到亂碼顯示的文字簡訊和多媒體簡訊時，最好立即刪除，因為這些亂碼簡訊，很有可能暗藏惡意的程式碼。

三、確認手機下載網站的安全性。許多智慧型手機的用戶喜歡到網路上找尋免費的軟體下載，不過這些網站卻可能是暗藏手機病毒的大毒窟。為了要遠離手機病毒，最好不要到來路不明的網站下載軟體程式。

四、如同電腦一樣，安裝防毒軟體，定期掃毒，能夠減少手機遭到數位病毒感染的機率。

由於智慧型手機的普及，導致手機資訊外洩的案例屢見不鮮，加上雲端運算和虛擬化，外洩的個資無論是關於個人品德缺陷或遭敵威脅利誘，都已對國家安全造成嚴重的影響；身為基層的我們雖沒有接觸國家安全的重大機密，也不具有決定國家指導方針的權力，但我們每一個人都是

組成捍衛國土的堅實分子，所以我們必須從自身做起，並應該戒慎恐懼，攜手共同面對這項威脅，體認國家安全、匹夫有責的觀念。唯有每個人都自我要求，恪遵規定，才能建構一個堅若磐石的安全網。

(本篇摘錄自法務部調查局清流月刊 103 年 1 月號)

杜絕採購弊端建立廉能政府採購環境

法務部與工程會聯合建置「政府採購聯合稽核平台」，建立有弊即查、制度有疏漏即導正之機制。

◎陳炎輝

壹、興利除弊實施政府採購法

我國自民國 97 年 5 月起陸續推動「愛臺十二建設」，以提升並深化總體經濟發展，實施內容分為「交通基礎建設」、「產業建設」、「都市與工業區更新」，以及「環境保護與生態」等四大面向；具體項目包括全國便捷交通網、都市及工業區更新、農村再生、海岸新生、綠色造林、防洪治水、下水道建設、產業創新、桃園航空城、智慧臺灣、發展中部高科技產業新聚落、高雄自由貿易及生態港等公共工程建設。政府推動公共工程之目的，一方面是為全民建構更好的生活環境品質，使國家各項重大建設成果，成為後世子孫珍貴的資產；另一方面則是增強工程產業的國際競爭力，在兼顧自然環境保護與永續發展的前提下，融入本土及現代科技的創新思維。政府興建各項公共工程，不僅涉及經費預算籌編與執行，更牽涉財務採購作業程序，除應整合採購政策、採購制度與法令規章外，並須培訓專業採購人才，適當管理供應廠商，讓採購商情的資訊透明化，以達到興利防弊之雙重目的。

為建立政府採購制度，依公平、公開之採購程序，提升採購效率與功能，確保採購品質，我國於 87 年 5 月 27 日制定公布《政府採購法》。鑑於本法為政府採購制度的重大轉變興革，宜有適當轉換準備期間，俾供相關子法之研訂及採購人員之教育訓練，故本法第 114 條乃明定自公布一年後（即 88 年 5 月 27 日起）正式施行。本法的重點如下：（一）政府採購制度健全化，招標分為公開招標、選擇性招標及限制性招標等三種；（二）發行採購公報，讓採購資訊透明；（三）投標期間合理化；（四）決標評選明確化；（五）政府採購國際化；（六）廠商申訴制度化；（七）不法行為處罰明確化。換言之，本法精神在於：（一）建立公開、透明、公平之政府採購作業制度，以提升競爭力；（二）創造良好的競爭環境，使廠商能公平參與；（三）符合國際標準，創新政府採購作業；（四）落實分層負責之採購行政，務期建立一個機制健全、資訊透明、公平合理，兼具興利防弊的政府採購環境。

本法是我國為加入世界貿易組織（下稱 WTO），順應經濟國際化、自由化之趨勢而制定，實施至今已達 15 年，對於提升採購的行政效率，確保採購品質雖具成效，但不容諱言，收取採購回扣、洩漏底標收受賄賂、圍標綁標、偷工減料及其他不法舞弊情事，卻仍時有所聞。例如法務部調查局及臺灣臺北地方法院檢察署，查獲前內政部消防署署長黃○○涉嫌在 92 年至 98 年 10 月任內，辦理先期防救災遠距離無線電通信系統、防救災遠距離無線電通信系統建置案、防救災專用衛星通訊系統，及現場通訊救災指揮車暨整合平台建置案等鉅額採購案時，違法指示採購單位人員違反公平與公開之原則及本法相關規定，不法圖利特定廠商新臺幣（下同）1 億元以上，涉嫌收受賄賂 1,900 多萬元；案經檢調人員於 101 年 8 月 29 日發動搜索，並於其豪宅中查獲數

十個進口名牌包，以及重達 16 公斤之 19 塊金條，新聞媒體甚至以「現代版和珅」稱之；本案經檢察官於 101 年 12 月 25 日依貪污等罪嫌提起公訴，並對嫌犯黃○○具體求處無期徒刑。

貳、淺析政府採購弊案之類型

本法於 88 年 5 月 27 日施行後，不僅促進我國採購制度的興革，同時也加速完成我國加入 WTO 之目標，為政府機關辦理採購首應遵循之基本法。就公共工程採購流程而言，約可分為規劃設計、預算編列、發包訂約、履約管理、施工監造、品質控管、驗收結算等階段，每一環節都可能發生弊端。例如，發包機關於規劃設計階段，在設計圖說、施工材料或招標文件中，指定特殊規格、工法材料、施工技術或限定廠商資格條件，為將來之議價或圍標埋下伏筆；或是於預算編列階段，將可量化之工程分批計價，方便灌水提高總價，以圖利特定廠商。又如，不肖廠商於發包作業階段，透過關說賄賂等管道探求底價，甚至勾串機關內部人員洩漏底價；或是承辦人於履約管理階段，廠商違約逾期完工，卻未依合約所訂條款予以處罰，不法圖利廠商。再如，經辦人於施工監造階段，填寫不實監工日誌或竣工報告書，藉以圖利廠商蒙混過關；或於品質控管階段，蓄意將抽驗人員帶至非施工地點執行抽驗，讓工程未經確實檢驗而辦理驗收；甚至於驗收結算時，未經詳細審核即予合格驗收。綜上，公務員違法辦理採購所涉罪嫌，最主要有綁標而要求、期約或收受賄賂，或其他不正當利益之違背職務行為罪；建築或經辦公用工程或購辦公用器材、物品，浮報價額、數量、收取回扣或從中舞弊罪（諸如偷工減料、以劣品冒充上品或以贋品代替真品）；圖利罪與洩漏國防以外之秘密罪，應依《貪污治罪條例》或刑法規定論罪科刑。前述所稱綁標，乃係「無正當理由對他事業給予差別待遇」之行為，不論是綁規格或綁資格，均不以形式上之商源家數為綁標之判斷依據，而是以招標需求是否具備「必要性」為準據。

相對於不肖廠商所涉之罪嫌，最主要為圍標罪。所謂圍標，一般指多數有競爭關係之廠商約定，在政府機關招標時不參與競爭投標，而讓內定之廠商投標，或是在「以低於底價」決標之情況下，雖然參與投標但其標價較內定廠商所出標價為高，讓內定廠商順利透過「搓圓仔湯」方式得標。至於廠商圍標之型態，第一種為串通圍標、合意圍標或合意不為競爭之陪標，依本法第 87 條第 4 項規定：意圖影響決標價格或獲取不當利益，而以契約、協議或其他方式之合意，使廠商不為投標或不為價格之競爭者，處 6 月以上 5 年以下有期徒刑，得併科 100 萬元以下罰金；一般稱之為「搓圓仔湯」條款。本項所稱之不法利益，並不以金錢財物為限，例如允諾下次無償陪標或其他利益交換，亦足當之，廠商內部彼此間有償或無償之約定，亦不影響其外部所應負之刑責。第二種為單純借牌圍標，指無投標資格之廠商借用合格廠商之名義競投標，依同法條第 5 項規定：意圖影響採購結果或獲取不當利益，而借用他人名義或證件投標者，處 3 年以下有期徒刑，得併科 100 萬元以下罰金；容許他人借用本人名義或證件參加投標者，亦同。第三種稱黑道圍標、強制圍標或非法搶標，亦即透過妨害競爭對手自由意志之形成，而達其一己不正競爭之目的；依同法條第 1 項規定：意圖使廠商不為投標、違反其本意投標，或使得標廠商放棄得標、得標後轉包或分包，而施強暴、脅迫、藥劑或催眠術者，處 1 年以上 7 年以下有期徒刑，得併科 300 萬元以下罰金。最後一種則是詐術圍標，依同法條第 3 項規定：以詐術或其他非法之方法，使廠商無法投標或開標發生不正確結果者，處 5 年以下有期徒刑，得併科 100 萬元以下罰金。

參、稽核平台防範弊端

近幾年來，檢調機關不斷破獲政府採購貪瀆弊案，例如，南投縣仁愛鄉公所多件工程採購案，採「限制性招標」比率偏高，涉有收取回扣情事，經臺灣南投地方法院檢察署搜索並偵訊鄉長、鄉長胞弟與承辦技士後，發現該三位被告涉案情節重大，且有串供滅證之虞，經向所轄地方法院聲請羈押獲准。又如，法務部調查局偵辦臺灣鐵路管理局「環島鐵路整體系統安全提升計畫」等工程，發現有高層官員勾結特定廠商，進行綁標圍標，並從中收受賄賂，乃報請臺灣臺中地方法院檢察署指揮偵辦，嗣後發覺涉案之副局長、工務處長等人亦有串供滅證之虞，經向所轄地方法院聲請羈押獲准。

為打擊貪瀆不法，革新官箴風氣，建立廉能政府採購環境，並整合政府採購與法務行政主管機關之資源，具體發揮橫向聯繫功能，以遏止政府採購發生收取回扣、收受賄賂、圍標綁標、不當變更設計、不當展延工期、偷工減料及其他舞弊等貪腐行為，法務部已與行政院公共工程委員會（下稱工程會）訂定「政府採購聯合稽核平台」建置計畫（下稱本計畫），各地方法院檢察署並與工程會建立行政協調與溝通聯繫窗口，以利檢察官偵辦政府採購貪瀆弊案時，就採取緊急處分、證據保全或其他偵查作為時，能夠適時洽請工程會提供協助，同時就政府採購所涉及法令爭點，彼此交換法令見解取得共識。

本計畫業經法務部於 102 年 7 月 18 日通函所屬檢察機關、調查局及廉政署辦理，將潛在採購不法行為之查處觸角，向前端延展邁進，先期防範各種採購弊端。工程會依據本計畫，將篩選政府採購潛在異常案件資訊，提供予「政府採購聯合稽核平台」進行資訊分享，並檢視政府採購程序及履約過程，有無違反《政府採購法》等情事。此外，針對政府採購涉及機關人員行政程序或行政裁量部分提供專業意見，同時亦與法務部廉政署建立聯繫窗口，由該署針對稽核平台所提供之批次查處案件，統籌或轉請全國各政風機構實施專案稽核，建立有弊即查、制度有疏漏即導正之機制。

（作者為法務部檢察司專員）

(摘錄自法務部調查局清流月刊 103 年 1 月號)

看蘋果公司保防工作有感

規模越大的企業往往越是將保防工作發揮得淋漓盡致，那麼事關國家安全與社會安定的全民保防，則更應加受到重視。

◎吳帝瑩

乍看之下，「保密防諜」猶如是個過時的口號，如泛黃斑駁的古老車票般只存留在老一輩的記憶中。然而事實上，保密防諜不但一直存在於我們身旁，更在當今激烈的企業競爭中被發揮得淋漓盡致。我曾在「Techorange」這個撰寫科技相關網路文章的單位實習，也意外地發現一篇關於企業界的新星─蘋果電腦，如何嚴格實行保密防諜，杜絕產品資訊被他人盜用的文章。

那篇文章的作者如獵犬般細心地找尋蘋果電腦保密的幾項關鍵，並推敲背後可能之原因；其中不難發現比起防範外在敵對企業的侵入盜竊，蘋果電腦更將重心擺在自家員工與合作廠商洩密的可能性上。正如俗語所說：「保密安全沒做好，銅牆鐵壁也會倒。」若沒有先安內，那麼花再多的功夫在攘外上頭也是徒勞無功。

在文章中作者發現蘋果電腦在開發像 IPAD 這類新興產品時，由於擔心消息走漏造成商業機密外流，因此嚴格規定開發者必須要在規定的開發室內進行研發；而根據曾任職於蘋果公司的研發者指出，所謂的開發室竟是一間沒有窗戶的房間，要進入房間的門鎖也需要研發者的詳細資料才可以放行。從這樣的行為不難推敲蘋果公司的想法，他們想斷絕一切非相關研發人員與資訊的連繫，將洩密的風險降至最低。因為如此一來，就可以將洩密的可能範圍縮小至負責研發的人員身上。

而他們又是如何對待研發人員的呢？為了防範研發者有意或無意地將資訊外洩，蘋果公司在研發者的工作桌上做了不少嚴密的設計，除了讓研發人員在進行研究時只能透過特製的框架看到他負責部分的螢幕之外，更將每台開發中的 IPAD 用鍊子和開發桌鍊住，進而拍照存檔。這麼做的原因除了確保只有最高層級的主官們知道產品的原貌之外，更能透過每張桌子的不同紋路讓特定開發者與特定產品產生連繫；只要產品圖像失竊外流，便可立即追出洩密者與洩密的產品機型。

蘋果公司的保密防諜工作還不只如此，對於和他們合作的廠商也是戒慎恐懼地要求每個環節的保密工作；除了將產品的生產鏈分散於不同的工廠以確保產品資訊的分散，更嚴格要求每個代工廠必須管制員工，除了以最基本的識別證進出外，更要通過金屬探測器來確定員工是否攜帶任何不屬於他們的器具離開。

從上述例子可以發現，蘋果公司幾乎是傾盡全力在資訊安全的保護上，因為在電子產品的領域中，知識和技術幾乎就是一切獲利的來源和保證。但國家的資訊價值卻不只於此，還涉及龐大的政府資產，其中又以軍事機密關乎整體國家的安全和全國人民的生命財產，更顯得重要。然而筆者以為國軍並非不能使用如此嚴格繁瑣的形式來執行和限制各級軍事單位，而是希望透過每週

的莒光課與各級長官的宣導，將保密防諜的觀念內化至每位國軍官兵的心中。畢竟唯有真正地打從心底確信與遵守，才是最有效的保密防諜方式；否則只要洩密者有心，則百密終有一疏，國防也沒有真正安全的一天。因此，養成資安習慣，恪遵保密規範，在外部防範、內部習慣的雙層保護下，才能真正落實資訊安全。

(摘錄自法務部調查局清流月刊 102 年 12 月號)

嚴肅面對隱形的資訊戰爭

除頒布相關的資安規定與管理制度的建立之外，資訊使用人的實踐履行，方為資安工作強化精進的核心重點。

◎王百祿

根據媒體報導，海軍光六飛彈快艇去（101）年曾發生測試筆電失竊事件，相隔年餘，2部配附艦艇上用於啟動雄二飛彈的筆電，日前也不翼而飛。雄風二型攻船飛彈是由中科院量產，配載於海軍光六飛彈快艇，為國軍重要的自製武器（如圖所示）。

今（102）年8月6日戰系廠某中士登上承德艦校正火砲，並將「通用儀表紀錄器」交給某上士班長代管，不料中士19日再度登艦時，才發現紀錄器不翼而飛，海軍艦艇指揮部獲報後立刻徹查，但仍無所獲；中士及上士班長有便宜行事之嫌，相關幹部也有督導不周之責，除將懲處違失人員外，另將全案於8月21日通報高雄憲兵隊調查，並函送高雄地檢署偵辦。

海軍司令部主任聞振國表示，遺失的是無機密資訊的筆電型「通用儀表紀錄器」，用來檢測及校正軍艦上的各種火砲，在菲律賓海巡人員槍殺我國漁民洪石成案中，參加聯合護漁操演的承德艦配備雄風二型反艦飛彈及MK-15方陣快砲等武器，「通用儀表紀錄器」就是用來檢測這些裝備。「通用儀表紀錄器」屬戰系廠配備，與軍艦無關，也不儲存資料，就像汽車維修廠的檢測電腦，沒有機密敏感資訊可言。

針對海軍光六飛彈快艇發生測試筆電失竊事件，筆者曾於《清流月刊》投書發表〈移動式資訊媒體管理與資安防護〉一文（101年10月號，第21卷第4期，第48至49頁），強調筆記型電腦，因為兼具絕佳的便利性與功能性，而快速發展成科技人不可或缺的資訊配備；但也因其輕薄短小、容易攜帶的特點，往往成為有心人士覬覦的目標。近年來，全球各地機敏單位之筆記型電腦遭竊的案例，可謂屢見不鮮！專家表示，政府部門資訊保密往往由於公務員保密意識不強烈，再加上相關問責制度不夠嚴謹，導致資安防護漏洞百出，亟待相關單位嚴肅面對，全面採取「強力措施」以防止類案再生。

本案例充分說明資訊安全與資訊設備管理之重要性，除了凸顯當事人本身警覺性不足外，同時也顯示「有心人士」無所不在且無孔不入，時時刻刻皆無所不用其極地想竊取機密資訊。本案初步分析主要肇因於三項違失：（一）裝備點收及保管作業疏漏；（二）相關幹部督導不周；（三）軍品進出入管制未臻嚴謹。建議國防部除將相關人員議處外，另應針對本案違失情節製作宣導教案，全面加強人員的宣教。

在美國知名電影《劍魚》中，頂尖電腦駭客多次神乎其技地利用電腦科技在短時間內癱瘓政府部門網站，竊取國家機密，誇張的電影效果令人直呼過癮，但也不禁讓人好奇該類型的諜報動作劇情，是否存在於真實世界？中共近年來大力發展其資訊作戰的能力，作為虛擬戰場的新型態

戰鬥力量，不但藉以蒐集情資，更可直接發動駭客攻擊，利用病毒與木馬程式來破壞敵軍的資訊網路系統。美國司法部長埃里克‧霍爾德（Eric Holder）曾公開表示：「中共駭客坐在電腦桌前，就能竊取維吉尼亞州一家軟體公司的程式碼；國防承包商員工只要敲幾下鍵盤，便能盜竊價值數十億美元的設計或程式。」相較於傳統武器的研發與製造，電腦病毒及攻擊程式具備低成本、高效益及無限制等特點；換言之，只要有心，人人皆能發動資安攻擊。

為防範中共鋪天蓋地的網攻手段，美國已明文規定政府機關不得採購中國大陸生產的資訊科技硬體，並警告美國國內企業應避免與「華為」、「中興」等通訊公司進行貿易。《澳洲金融評論報》於7月29日報導指出：英美等5國情報機關組成之「五眼」情報聯盟已全面禁止使用中國大陸的聯想電腦，原因為經過多次測試確認，該電腦硬碟的電路已遭竄改，出廠前已植入後門程式。而我國軍保密工作教則中亦明確規範：國軍籌設、籌購資訊作業系統、裝備與設施，應先就保密安全評估需要，再依國產、外購順序，考量整體規劃方向及建立自力維修能量，與全般性技術轉移，以減少爾後保密安全顧慮，進而防範中共偽裝廠商進行滲透、竊密行為。國防部並於今年7月15日令頒「國軍資訊資產管理作業規定」，凡設備內含記憶體、硬碟或網路傳輸之資訊設備屬大陸地區產製者，一律禁止採購。

現今資訊科技日新月異，「雲端」、「Wifi」與「App」等新型技術或網路軟體相繼問世，訊息傳遞無遠弗屆；然而在便捷之餘，亦凸顯資訊安全的重要性。99年「維基解密」公布美國國務院的機密電文計25萬份，涵蓋內容甚為廣泛；另101年蘋果電腦公司發表ISO 6.0地圖搜尋系統，清楚地標示我國某空軍基地的位置與衛星照片，衍生營區安全後遺。可見任何「機密」一旦缺乏完善的防護機制，便可能成為「公開資訊」，嚴重威脅機密維護工作。面對中共「網路威脅」，我國軍尤應建制完備的網路防禦與資訊作戰力量。國防部通資次長室之宣導資料顯示，如同以往文書的傳遞、管理、處理與銷毀都要遵守保密規定一樣，資訊保密在不同流程與階段，也都會有相對應的保密工作；國軍全體官兵務必恪遵「進入營區禁止攜帶個人資訊設備」、「禁止公務家辦」、「軍、民網實體隔離」，以及「電腦須設定密碼並加裝防火牆與防毒軟體」等規範。全軍官兵只要確實遵守並落實各項網路使用規範，相信就算是超強駭客，也未必能夠「登堂入室」。

最後，筆者再次呼籲，資訊安全工作是一項防患未然的風險管理過程，為有效防杜敵人情蒐，根絕洩密事件肇生，各科技研發機構應制訂強化資訊安全防護體系的整體性政策，針對專案任務屬性與作業流程，嚴採相關保密檢管措施與手段，藉以明確劃分保密責任，提高機密資訊的維護強度。除頒布相關資安規定與作法外，管理制度的建立，以及資訊使用人的實踐履行，實為資安工作強化精進的核心重點。當資安保密成為每位員工的工作習慣後，機構內資訊安全防護機制與防護網路，才能達到滴水不漏的境界。

(本篇摘錄自法務部調查局清流月刊102年12月號)