

機密維護常識彙編 (96 年 7 月份)

*用情治機構辦外交 換來滿身傷疤

凱德磊案雖然宣判，但是並不會船過水無痕，反而留下美台雙邊關係的傷疤，相關人士都應該要記取這個教訓。

此案纏訟許久，主要因為涉案的四方面各有盤算，凱德磊是一方，聯邦調查局是一方，國務院是一方，台灣則是第四方；台灣希望不要扯上間諜罪名，國務院則擔心洩密若成立，直屬長官要負責，而兩國從美台關係著眼，都希望大事化小、小事化無。

無奈 F B I 為了邀功，堅持要辦，就像之前抓到國防部高官費斯與以色列間諜勾結一樣，他們見獵心喜，加上手上有證據，自認足夠讓凱德磊間諜罪名成立。

F B I 也可以接受認罪協商，但不能太離譜，前年十二月中旬，一度傳出要以認罪協商的方式結案，但是後來調查局不肯以輕罪釋放，據說條件是至少入獄服刑八年以上，從凱德磊與其律師的立場，當然不希望認罪後，還要坐這麼久的牢，訴訟進度僵持，去年六月廿三日原本要宣判的，因此延後。

期間，凱德磊與他的律師選擇的施壓方式，是透過媒體放消息，威脅台灣與國務院，要大家想辦法，否則手中資料抖出來，大家都難看。紐約不知名的小報太陽報 (New York Sun) 三不五時就有些獨家，包括凱德磊與程念慈的電郵，其中談及譚慎格與台灣的关系，警告之意甚明。

台灣國安局方面，原本認為是可以解決的了，所以前年八月特地挑選陸軍官校校長楊國強，接替涉案的黃光勳。

當時美方並沒有拒絕由楊來取代黃，但是前年下半年楊國強到華府上任後，凱德磊案開始暗潮洶湧，一方面問題越來越棘手，一方面，越來越多證據顯示，台灣確實有利用凱德磊「接觸」機密文件的情事，所以美方開始對台灣不客氣。

跡象之一是：去年七月中，回台後的黃光勳，原內定出使以色列，卻遭以方委婉拒絕，表面理由是因過去介入凱案，媒體會注意，工作受影響，但真正原因卻是美方有壓力，明確不希望以色列接受黃光勳。

跡象之二：更早前，楊國強應該就已經感受到美方的壓力，在僅僅擔任半年特派員後，於去年二月調返台灣，是否被迫提早回國，楊與國安局都否認；但是駐美特派員是艷羨的中將缺，安全局中個個少將眼紅，竟然換成文職的嚴夢漢出任，傳言所謂美方不滿，並要求以後不要再派軍職人員擔任駐美特派，看來並不是空穴來風。

國安局為了撇清運用間諜的嫌疑，薛石民日前在立法院答覆質詢時還表示，凱德磊是自己找上門來，「凱德磊代表美國國務院主動與我方接觸」，因為A I T處長包道格不願與安全局來往。

這裡是有問題的，安全局本來與國務院的接觸，就有些名不正言不順，包道格拒絕往來，不能說他錯，而以包道格中情局出身的背景，刻意避免接觸，不能不說他有先見之明。

用情治機構來作外交，是這十幾年來的畸形現象，元首倚賴情報機構的效率財力，便宜行事，不受監督，從科索沃援助案、國安密帳，到凱德磊案，已經傷疤滿身了，台灣主其事者卻還沒有得到教訓。

【中國時報/郭崇倫 / 新聞分析】

*台灣情治破洞 才震懾

呂昭隆 / 新聞分析 中共國安部宣稱獲取的我國情治系統這批機密文件，如果文件屬實，則最令人震驚的並非內容，而是國安局長簽報給總統的絕對機密文件，簽呈首頁右上方，有著代表絕對機密的「四條斜槓」印記，而且簽文時間又是今年二月廿六日，等於是最新、又最機密的文件，在第一時間，就落入中共手中，著實令人震懾。

由於這批機密文件的時間，有今年與去年的簽文，而年前外洩的國安密帳密件，時間則集中於李前總統執政時代，顯示情治單位的洩密管道，「漏洞還沒有堵住」，可能是同一管道所為，也可能是新的管道，如果是同一管道，代表「它」既能到國安密帳的機密文件，也能接觸到「業務相關」的最新密件。

這分今年二月由前國安局長簽報的絕對機密文件，頗富玄機。

首先，國安局呈給國安會的公文極少，甚或從未有過「謹呈秘書長」，再「轉呈總統」的簽文方式。一般而言，國安局呈給國安會的公文，簽呈首頁末，僅會寫著「謹呈秘書長」五個字，絕對不會接續再寫「轉呈總統」字樣。

依照國安局行文作業，呈給國安會秘書長，就是只給秘書長，如果還要給總統看，國安局會單獨再寫一分，簽呈首頁末，則寫「謹呈總統」。換言之，如果公文要同時給秘書長與總統看，國安局會打兩份文，不會採取「謹呈秘書長」再「轉呈總統」，以一分公文同時讓秘書長與總統批示。

因此，研判這份分析民運與政策建議的密件，應該是前國安會秘書長康寧祥，指示前國安局長蔡朝明辦理，蔡朝明照指示做後，打了份報告給康寧祥，但因涉及情報經費運用，與「政策建議」，而蔡朝明

也希望總統知道，所以採取了這種罕見行文方式，特別加了一個「轉呈總統」，意即，此一絕密公文，主要是給康寧祥裁示，但也讓總統過目，「知道有這麼件事」。由於二月，陳總統正忙於大選最後衝刺，是否知道此事，公文並無批示，無法得知。

不過，從公文首頁尚無批示，可以分析洩密的可能管道。由於康寧祥尚未批示密件，而文件又是要呈給國安會，所以，包括國安會與國安局，都可能是洩密的管道。如果是國安會洩密，於康寧祥未接觸公文前，所有能經手這件絕密文件的官員，都有嫌疑。但是，洩密管道也極可能是國安局，當這份文件要出門給國安會前，就已被人取得。

因為密件還沒有康寧祥的批示，所以，文還沒有走到總統府，因此，總統府內部應可排除 洩密的可能，至於國安會或國安局的洩密可能性，雖不能排除，但有國安密帳前例，加諸這次外洩文件中，還有國安局四處與會計室簽報的極機密文件，還是國安局內部洩密的可能性居多，當然，也不排除中國民運人士「意外取得」密件，並輾轉交給中共國安單位。

而國安局長簽給總統的絕密文件，如果第一時間便外洩，無論內容為何，台灣情治單位的「破洞」，顯然比外界想像的還要大。

(呂昭隆 / 新聞分析)

***教師介聘電腦駭客案件實例研析**

缺乏必要的防護機制及貪求方便，都可能給予駭客入侵機會。

一、前言

現今科技的發明，使得人們藉由無遠弗界的網路在瞬間即可跨越距離的界限，輕易到達世界上的任何一個地方，也正因如此，掌握資

訊的流通及作好訊息的防護已成為本世紀資訊戰中最要的一個課題。正因為網路的特性，使得防制滲透及機密維護扮演著國家安全、機關安定中最重要角色。近來，有些公務機關發生遭駭客入侵滲透竊取機密或竄改資料甚至癱患系統之情形，例如單純的教師介聘作業亦遭有心人士入侵竄改，顯示對於防制滲透與機密維護之觀念有待加強，因此本文僅就該案例作一探討，由實務中加強正確觀念，以求電腦駭客案件能有所減少。

二、案例介紹

(一) 緣由：教育部自民國 90 年起為辦理臺閩地區公立國中小學暨幼稚園教師申請介聘他縣市服務之作業，依「90 年臺閩地區公立國民中小學暨幼稚園教師申請介聘他縣市服務作業要點」實施相關聯合介聘作業，並以電腦作業方式行之，由教育部委託高雄縣電子資料中心(址設：高雄縣鳳山市五甲二路 424 號，五甲國小內)負責辦理相關流程。欲申請調動外縣市介聘之教師則於填寫介聘申請表後，上網至該中心所架設之「教師外縣市介聘網站」(<http://exc.ks.edu.tw/>)登錄資料。

(二) 案情概述：本案係 94 年 5 月間某國小沈姓資訊組長因其甲教師友人欲請調回臺北縣服務，不諳電腦網路操作而將其個人電腦帳號、身分證字號等資料交由沈某，由沈代為操作網路程序向電子資料中心提出介聘調動申請，沈遂於 5 月 31 日利用學校 IP 透過某大學的代理伺服器連結，進入介聘作業系統，沈先隨意試著更改不認識的某國小乙老師的積分，以及丙老師的志願，沒想到都更改成功，便更改甲姓友人和認識的丁老師兩人積分。沈自行模擬調動兩次，發現甲與丁師無法如願調成，遂將兩人資料還原，但因已忘記乙、丙老師的

資料，所以無法還原，導致兩名老師，一個積分由 131 分被竄改為 101 分，另一個的第一志願則被更改。由於乙老師一心一意想調回住家所在的臺北縣，因此對於介聘分發十分留意，時常上網查看自己積分，經發現積分由 131 分被竄改為 101 分，被介聘到其他國小，經向彰化縣教育局反映，並確認並非鍵入錯誤，轉向高縣教育局通報，才發現分發作業系統遭駭客入侵，另一名丙老師則因原本績分不足，無法調動，故不受影響。

(三) 適用法條：本案係適用《刑法》新增之第 36 章妨害電腦使用罪，其中第 359 條「無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」以及 361 條「對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一」，由於沈○○犯後即向服務學校校長坦承，透過校長向花蓮縣教育局報告，並告知高雄縣電子資料中心，表示願主動投案，全案後由高雄縣調查站及高雄警察局調查了解，因沈某屬自首行為，且犯後坦承不諱全力配合調查，經高雄縣調查站偵訊後依違反個人資料保護法移送高雄地檢署，由檢察官諭令五萬元交保，並宣告緩起訴處分。

三、缺失檢討與應有正確觀念

(一) 缺失檢討：本案係沈某利用介聘系統網站的網頁漏洞，於進入介聘系統網站之系統管理者目錄網頁後，取得系統管理者權限入侵竄改資料之權限，係因本案與防火牆的防護機制不足有關，因辨識身分之設計無法確實把關，導致遭人入侵滲透，而高雄縣電子資料中心亦表示本案係為求方便在主辦單位新竹縣教育局的遠端連線，於作業期間取消「最高管理員程式區」的 IP 限制，造成漏洞而使有心者

滲透入侵而產生，因此已要求電子資料中心在事發後緊急更改入口程式，加強阻擋駭客的入侵。因此缺乏必要的防護機制及因貪求一時之快而開方便之門都可能給予駭客入侵的最佳機會。

(二) 正確的資訊維護觀念：正確的資訊維護觀念是對付駭客入侵的重要關鍵，除了透過防毒軟體、防火牆系統等防護機制外，重要資料最好不要存放於電腦裡，並做好使用程式及瀏覽器、WORD 等應用程式和防毒軟體定期、隨時更新，以避免漏洞，並養成不隨便讀取來路不明電子郵件習慣，免得「開後門」讓駭客有可乘之機，都是正確且必要的資訊維護觀念。

四、結論

93 年大學聯考分發時，因電腦程式未把特殊條件限制寫入，造成沒通過軍事聯招智力測驗及口試的考生，考取資格不符的國防大學，該錯誤代價使得 220 名考生必須重新分發；94 年 4 月爆發了大考中心和國中基測電腦系統連續三年遭 19 歲的電腦駭客蘇○○入侵，竊取一百多萬筆考生資料，燒錄成光碟，轉賣給補習班；如今教師介聘系統也出狀況，駭客入侵公務系統及教育部相關網站已呈現其嚴重性，本次的教師介聘電腦系統案，雖僅有一位老師權益受影響，並於事後予以彌補，但其中所顯現的機制漏洞有關單位實應妥慎檢視省思，畢竟未來「電子政府」已是趨勢所在，如讓前述的駭客入侵案件一再發生，將嚴重損及我國家安全及機關安定。

(本文摘錄自清流月刊/作者：王俊傑)

*戶政雇員洩漏公務機密案例

案情概要：

某縣某戶政事所雇員甲負責辦理戶籍登記之櫃檯業務，係依據法令從事公務之人員，緣有渠在某警分局任職期間之同事某乙，在離職後開設代書事務所，因長期為客戶辦理改名，而知悉姓名條例第六條第一項第三款「同時在一縣市內居住六個月以上，姓名完全相同年齡較輕者，得申請改名」之規定較易申請改名，某乙乃利用曾任職警察熟稔警察機關內部運作規定，自民國八十四年間起迄八十六年一月止，向舊時在警分局之同事甲詢問當李之「查詢戶籍、口卡號碼」二、三次，甲明知該代號係警(戶)政單位列為機密不得對外提供之應秘密事項，而竟洩漏予乙，致使乙得據以透過電話冒用警察之名義向多處警察、戶政單位詢問得所欲查詢之同姓名人等的人別資料，再詢程序辦理改名，案經檢調單位移送法辦，本案某甲連續洩漏「查詢戶籍、口卡號碼」予乙，係觸犯刑法第一百三十二條：「公務員洩漏或交付關於中華民國國防以外應秘密之文書、圖畫、消息或物品者，處三年以下有期徒刑」，某乙所觸犯者係刑法第一百五十八條第一項：「冒充公務員而行使其職權者，處三年以下有期徒刑、拘役或五百元以下罰金」。

檢討分析：

戶政單位或其他類如警察、稅捐、電信等機關人員係依據業務職掌經管公務機密資料，理應恪遵作業規定，予以保密，不得洩漏於外，即或在人情困擾下，亦不得破例，否則民眾權益及個人隱私勢將受損，坊間多有徵信業者從事錄音、跟蹤、查址、尋人等業務，平時為包攬生意，打探隱私，勢必透過種種方式或管道向公務經管單位取得相關

資料，文中某甲將查詢代號洩漏予乙，雖屬基於私人之情誼，亦已觸犯相關法條，如係期約收賄，則必獲從重量刑，上開案例足堪身為公務員者戒。

***大哥大化身情報員（機密維護更不容輕忽）**

能拍照又可當掃描器 全錄將推出

有了這種裝備，連糊塗情報員史麥特(Maxwell Smart)也會羨慕你：具拍照功能，又可當文件掃描器的行動電話。

想像你在執行蒐集情報任務或銷售拜訪時，偷偷為合約、白板上的筆記或其他書寫的資訊拍照，稍後再轉換成另一種可供處理的格式，供影印成文件或在電腦上處理。位於法國格蘭諾伯(Grenoble)的全錄(Xerox)歐洲研究中心開發的行動文件影像軟體，可為你達成任務。這種預定今年稍晚推出市面的技術，將用在至少 100 萬像素的照相手機上，用以製作文件或簡報的數位影像。它可以檢查並修正模糊和陰影，並將影像壓縮成檔案，透過多媒體傳訊服務(MMS)或藍芽無線技術，傳輸到傳真機、另一支手機或電腦。影像稍後可列印出來。全錄歐洲研究中心資深科學家兼影像處理部經理丹斯說：「我們給測試者使用，結果大受歡迎。即使是最簡單的用途如分享文件和儲存拍攝的文件，都獲得熱烈迴響。你甚至可以手寫訊息，並傳送到別人的手機。」

全錄正透過授權代理公司與潛在的授權對象洽談，以便消費者在年中時用上這種已獲專利的技術。潛在的授權對象包括手機製造商、無線電話公司，和文件管理軟體開發商。

全錄的這套軟體牽涉四個處理步驟，丹斯說，第一是用照相手機在一

呎的距離拍攝文件，製作長 8.5 吋、寬 11 吋的影像。不過丹斯說，較小的文件較難拍攝，因為一般照相機較難近距離聚焦。

拍攝影像後，可修飾模糊，並轉換成黑白影像；也可以調整對比、去除某些紙張或文件表現產生的陰影或反光。最後，把影像壓縮成稱為 G4 的格式（體積可壓縮為十分之一），以一張相片的體積可儲存約 10 頁文件。

全錄認為，這套技術對任何工作需要蒐集情報的人都有用。例如，有人參加商展或會議時，可用手機來捕捉和儲存相關文件。丹斯說，一般人不會在小螢幕上觀看拍攝的影像，而會傳輸到電腦上，以使用光學文字辨識軟體轉換成可編輯的文件，或以 MMS 傳送文件影像給生意夥伴或家人。（編譯吳國卿/經濟日報報導）