學術講演

刑法電腦專章及案例研究*

張紹斌**

壹、刑法電腦專章制定背景概述

吳司長、各位院長、檢察長及在座的長官們，大家好！

今天很榮幸有機會到國防部向各位報告「刑法電腦專章及案例研究」，這個專章是民國 92 年 7 月開始實施的，立法背景是因應當年網路環境漸趨成熟，網路犯罪的威脅日益增加，及歐盟通過「電腦犯罪公約」等諸多背景，所以立法院透過決議向行政院要求政府機關提出防制並嚇阻的法律草案，俾供審議討論以防堵日益猖獗的電腦或網路犯罪。

在此背景之下，與網路比較有關的業務單位像是新聞局（後來因時空變遷而成立的 NCC 國家通訊傳播委員會）、內政部警政署、法務部（調查局）、交通部（電信總局）等單位，都有提出立法草案之機會，但是因為立法院的要求是防制電腦犯罪，所以最後是由法務部來負責條文的草擬。

本次報告的主軸是從刑法條文及實際案例適用的角度來看法

---

* 本文整理自 97 年 6 月 20 日國防部軍法司 97 年度第 3 次學術講演演說內容。

** 張紹斌，交通大學科技法律研究所法學碩士，臺灣臺北地方法院檢察署主任檢察官。

條，由此角度會比較容易看出法條的問題在哪裡。另外一個要跟各位說明的就是，網路犯罪專章 6 個條文的適用及解讀，除了需有一定刑法的背景、架構之外，還必須要有電腦或網路技術做為解釋的核心，否則學說及實務適用起這些法條來就會與電腦運作、網路環境格格不入，甚至與立法意旨違背。

92 年 7 月我們修正並實施刑法，整個修正條文分為兩大部分，首先是配合妨害電腦使用專章的增訂;其次是刪除刑法中將電磁記錄擬制為動產的規定。修正前的刑法 323 條第 2 項:「電磁紀錄關於本章之罪，以動產論」,是繼受自日本法， 92 年 7 月我們把這條刪除，同時增訂保護電磁記錄專章。整體來說，等於將電磁記錄的保護移動到刑法最後面那幾條來理解比較契合修正條文。

貳、從我國第一件「偷天幣」判決談起

約民國 90 年間，我寫了中華民國第一篇在線上遊戲中「偷天幣、虛擬裝備、寶物」的起訴書，法律依據就是刑法第 323 條第 2 項。由於當時的法律將電磁記錄擬制為動產，所以我依法起訴一位就讀於北部某大學的大學生竊盜虛擬貨幣的行為，臺北地方法院的法官也同意這種新犯罪型態適用竊盜電磁記錄條文的見解;由於偷線上遊戲虛擬貨幣、裝備、寶物的案件適用竊盜電磁紀錄的見解獲得法院採納，瞬間所有累積在臺灣各警察機關，及已經移送在地檢署有關偷天幣、裝備、寶物的案件全都解套；影響所及的是竊盜案件因而暴增，估計全臺灣每年平均增加約 3,000 件類此竊盜虛擬裝備、寶物及貨幣的案件，也因此波及到治安案件的計算。

因為竊盜、搶奪、強盜當然屬治安評比項目，也就是治安因為竊盜案件數量增加而發現有顯著的惡化，在當時的環境，要達到「治安零成長」的目標是很困難的事情，是以，將原刑法有關電磁記錄擬制

為動產的規定予以刪除，並藉由新增專章的方式加以填補，某種程度兼顧美化治安案件數字的目的；但是這樣會產生非常大的法秩序漏洞，本來將電磁記錄擬制為動產，因為規定在竊盜罪章，含有財產法益的特質，偷了電磁紀錄之後拿去轉賣，購買的人則是贓物罪章所要處罰的對象。因此，偷取電腦資料庫存取權限的帳號、密碼，對於一些資訊或資料庫的公司而言，就是侵奪他們的資產。

但是此次修法，將電磁記錄保護的條文從刑法第 29 章的竊盜罪章中第 323 條，搬到第 36 章電腦犯罪專章，就沒有辦法以體系解釋的法益觀點擬制它為動產，如此此類極具資產價值的帳號、密碼便會喪失上述財產上的特質。影響所及，變成蒐購帳號、密碼等電磁記錄的行為無法用贓物罪予以規範評價，只能用個人資料保護處理法去處理。

然而使用個人資料保護處理法有個大問題，那就是一定要被害人出來提出告訴，各位試想，如果你們的電子郵件帳號、密碼被偷（外洩），你願意常常出庭來告他嗎？算了，通常都是算了，改密碼就好了，弭平自己缺憾的手段太容易，但是要去法院訴訟，討回公道的財產標的價額太低且成本太高（例如交通、時間的勞費），而且被害人也無從證明帳號、密碼外洩的損失有多少，會導致沒有什麼人願意使用個人資料保護法去提告，縱使提出民事訴訟也不知道能要到多少錢，我們很多案子就是根本找不到人來告，找到人也不願意提起刑事、民事告訴，這樣的條文設計及體系編排很不好，但是條文就是這樣寫的，我們也沒辦法。

參、刑法第 358 條之行為模式分析

現在我們看一下條文，刑法第 358 條，無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦

或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。該條的行為態樣是要「入侵」，刑法第 358 條的「入侵」和刑法第 306 條侵入住宅罪的「侵入」是兩個完全不同的法觀念：侵入住宅是不作為犯舉例的典型，經命退去而不退去，就犯了刑法第 306 條的不作為犯。但是沒有聽過侵入電腦而不退去，對吧？把電拔掉、網路線拔掉它就退去了嘛。

各位先看一下最後面，無故入侵電腦罪，它的保護就是網路安全。行為模式有三個：無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，這三個行為模式大概只有第一個能用，另外兩個在實務上幾乎沒有用處。

一、無故輸入他人帳號密碼

我們以「偷天幣」的例子來說明好了，你一定要輸入遊戲中某角色的帳號密碼，才能夠控制那個角色，記得我偵辦的第一件偷天幣的案件，當事人來地檢署按鈴申告的時候，我問他要告誰，他就說他要告一個某線上遊戲第幾伺服器的玩家，我就說：「喔，那個行為人住哪裡？叫啥名字？」，他回答：「我不知道，暱稱叫做『你爸最大尾』！」我問他要告他什麼？他說要告偷他的隱形斗篷，那時候我愣住了，我問他隱形斗篷在哪裡？他說「在天堂」；隱形斗篷的作用是什麼？他說這斗篷穿上去就看不見了，我那時因為沒在玩線上遊戲，就疑惑的問：既然隱形斗蓬既然是隱形的，那遺失不就剛好可以不需要處理了嗎？

雖然是玩笑話，但以西元 2000 年時的價格計算，一件隱形斗篷價值天幣六百萬，換算成新臺幣大約是六萬元，價值相當於一般人一到兩個月的薪水，比起竊盜罪章所提出的判決、判例中曾經說明過的松木、泥土、自來水等更具經濟上的交換價值，考慮了此種電磁記錄具有財產性格後，才用這一條予以起訴；又因為要加入線上遊戲確定

要支配的角色，通常都需要經過輸入帳號、密碼的手續，因此在這裡我們可以了解，刑法第 323 條竊盜電磁紀錄關於線上遊戲這類案件，通常的前置行為就是指輸入帳號、密碼。

「無故輸入他人帳號密碼」大概已經解決了電腦犯罪一半以上的問題，在解釋上，輸入帳號密碼也可能包括電子郵件、smart card、USB、提款卡、部分通行證、電子簽章、瞳孔指紋辨識等態樣，這些都有可能在未來的案件慢慢地去建立案例。

二、破解使用電腦之保護措施

至於「破解使用電腦之保護措施」或「利用電腦系統之漏洞」這兩項，執法人員、法官沒有技術背景是辦不到的，有技術背景也很難想出來適用情況，變成條文寫在那邊閒置，雖然有先進的立法，但是實務上卻無法使用。

例如什麼叫做「破解」？我不知道，刑法上從來沒有出現過「破解」這兩個字。到底要什麼程度才叫做破解？是防禦措施的全部嗎？還是要跟這臺電腦有連線的才算？這個沒有答案，關閉作業系統 XP 的防火牆本身算不算破解？把站在門口負責看管電腦主機的衛兵殺掉算不算破解？假設電腦外面裝大鎖，把大鎖打掉算不算破解？這個「破解」存在著太多的不確定性，所以這個我是覺得很難用啦，不知道什麼時候才能用到。

三、利用電腦系統之漏洞

再來所謂「利用電腦系統之漏洞」，這個漏洞是個相對性的名詞，所有的軟體在安裝時都會告訴你，依照當時的科技水準可以做到這個程度，這樣或許就可以在民事上免責。但是「利用電腦系統之漏洞」這一點，檢察官要如何舉證？是不是漏洞要如何舉證？參考微軟的安全性報告嗎？還是行政院國家資通安全會報技術服務中心的通報？還是外國駭客組織所發佈的作業系統缺陷當作漏洞？此處沒有客觀

標準，極難有舉證可能性，但是我們沿襲了人家的立法例，這是歐盟電腦犯罪公約一個比較 rough 的立法，我們就直接引進來當作成文法的條文。

反正這一條只有「無故輸入他人帳號密碼」最好用，行為人的目的是入侵他人電腦或其相關設備，其他的行為樣態都很難用。這一條輸入他人的帳號、密碼基本上是取得別人也就是不屬於你可以控制的電腦的存取控制權，而不是去規範輸入軟體產品的註冊碼的盜版型態，這一條請不要誤用到那邊去。

另外要跟各位稍微說明一下，這一條是告訴乃論。如果有人輸入我在天堂Ⅱ的帳號密碼，那請問誰是被害人？帳號、密碼是我在管領、使用的，所以我是被害人，千萬不要期待天堂Ⅱ遊戲公司（吉恩立公司）會出來提告，雖然是入侵的對象是遊戲公司的伺服器，但是使用的是我本身的帳號、密碼，理論上會有兩個被害人，但是在實務上不會由遊戲公司出面提告，通常都是被輸入帳號、密碼的那個被害人出來告訴，遊戲公司僅會協助他去取得一些 log 檔。

這幾年來，很多偷虛擬貨幣的情形很多是從中國大陸經過馬祖、金門的中繼站，甚至透過其他電信、網路進來臺灣，如果遇到 IP 位置在國外，我們就會直接跟被害人說，對於您的遭遇我們深表同情；天幣再賺就有了、隱形斗篷再買就有了。因為就算知道是在吐魯番窪地、亞利桑那州的某一個鎮又如何？調不到 IP 資料，你要傳誰來呢？這有事實上的困難，實然面的不得已，所以當事人最後還是會放棄告訴，告到底檢察官也無能為力。

肆、刑法第 359 條之「無故取得」？

我們看一下刑法第 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。」條文要求的是「取得、刪除或變更」，這個會常常用在洩密罪；部隊裡有很多規定，比如說明天演習的簡報檔、後天去某國家的出訪名單等，這些資料我覺得都很不適合流傳出去，雖然不一定是機密，但是要當敏感資訊來處理的這種文書卻也不少，把它 copy 在個人的 USB 存取硬體後攜帶回家，違反資訊安全的規定算不算「無故取得」？你的權限、身分是可以取得的，但是將它攜帶回家，算不算？這點是我們偵辦上的一個大問題。

資安的限制是讓你只能在部隊使用，不可以未經許可攜出，但是你的身分是可以擁有這些文件的控制權。無故取得的「無故」有沒有包括資安規定與你的身分相衝突的情況？目前為止的問題是卡在檢方自己辦不下去，他違反資安規定，但是他的目的並不是洩露，他沒有洩漏的動機和目的，他只是把工作帶回家去做而已，而現在比較新的病毒會透過 USB 隨身碟來傳染，木馬程式會把電腦或者 USB 中的資料往外傳輸，現在發生的案例就是類似這一種。

伍、與刑法第 359 條有關之營業秘密法

在實務上，這個條文剛好與營業秘密法的條文有些關聯，很多公司的員工在離職之前把資料全部 copy 到光碟、USB 或者用電子郵件寄出去，包括研發計畫、測試報告等等，就全部帶走了，當然不是每一家公司的控管都很嚴格，資料取得後再伺機拿去競爭公司來販售，這是營業秘密法要禁止的，但是「營業秘密」在營業秘密法中要有一定的要件，必須是指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，還必須要有符合「非一般涉及該類資訊之人所知、或因其秘密性而具有實際或潛在之經濟價值，及營業秘密所有人已採取合理之保密措施」者，才能叫做營業秘密。

另外，營業秘密還有一個非常大的問題：違反營業秘密法只有民事責任而沒有刑事處罰規定，所以到地檢署來告違反營業秘密法是沒有用的。現在公司的資訊都電腦化了，往往來地檢署告說離職員工在離職之前把資料 copy 至光碟，然後待投效到原公司的競爭對手後，提供這些資訊給競爭對手公司，突然間便讓它多了好多個客戶，而且都是原公司的客戶，那就知道出事了嘛！你的報價、管銷成本、代理商經銷商、折扣等等，全部都被競爭對手知道，這些認為受損失的公司就用這一條來告：「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」。

檢察官在處理的時候，還是要盡量去審酌本條的立法目的，不要脫離電腦或網路犯罪的立法原意，不要機械式的用這一條去保護屬於民事爭訟範圍的營業秘密的爭執。

我們看一下刑法第 359 條條文，無故取得、刪除或變更「他人」電腦內的電磁記錄；在離職之前，取得資料是自己的電腦還是他人的電腦？是自己的電腦，所以構成要件不該當，應該為不起訴處分。那問題來了，離職之後透過網路回來入侵公司的電腦，將屬於電磁記錄的資料帶走？這時候很有可能也會牽涉到刑法第 358 條的問題—「無故輸入他人帳號、密碼」。

另外，偷天幣也一定會牽涉到這一條，輸入被害人的帳號、密碼之後，是不是要變更他人電腦紀錄，把天幣、裝備、寶物都移轉到我控制的角色來，通常犯罪態樣都是這樣。被人家清掉的電磁紀錄，例如天幣、裝備、寶物、武器都算是無故刪除或變更他人電腦或其相關設備之電磁紀錄，所以偷天幣以前是犯刑法第 323 條竊盜電磁紀錄罪這一個條文，現在是刑法第 358 條，因為要輸入帳號、密碼，還要再加上刑法第 359 條，要取得他人電磁記錄，現在會犯這兩個條文，不過刑度和以前一樣，最重都是五年以下有期徒刑，只是把條文從前面

移到後面來，差別最大的在於財產法益的變更。

陸、網路犯罪侵害了何種法益？

不過網路犯罪本身到底是刑法要保護的什麼法益？沒有深入的學說或理論支持。到底是屬於個人法益、國家法益，還是社會法益？實在難以認定，因為他三個法益都兼有。網路犯罪的特質，就是它本身是一個犯罪類型，本身也是一個犯罪方法，可以透過電腦或網路的不法手段去觸犯別的罪名；坦白說，妨害電腦使用罪章的幾個條文，放在刑法上面一定會有體系解釋上的困難。

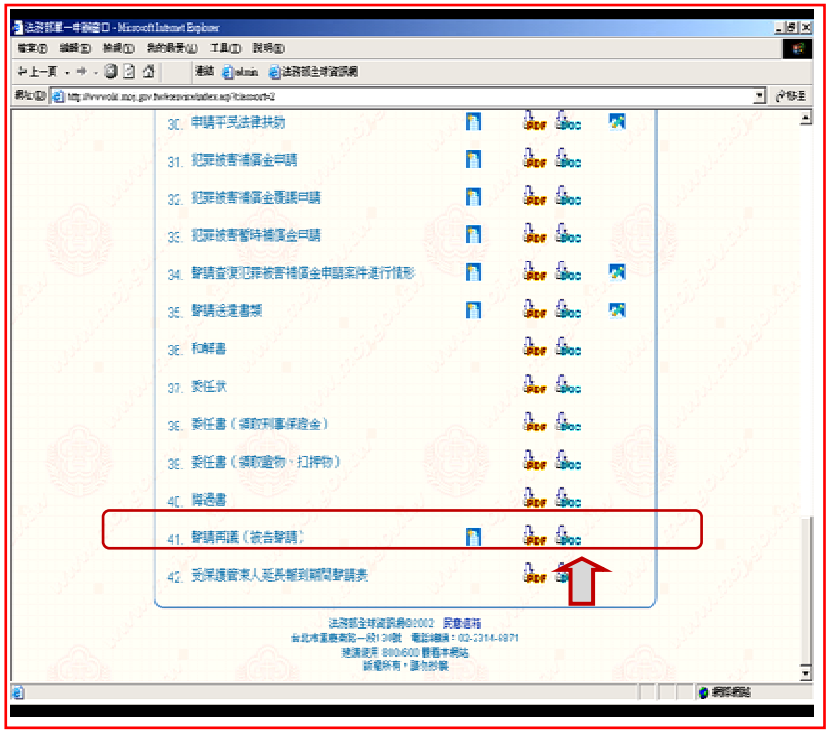
一、竄改網頁之「烏龍案」

我們來看一下 95 年度偵字第 9731 號實際案例，這是一個法務部網頁遭到竄改的案件。被告是一位駕駛計程車在支線行駛的計程車司機，他不小心在交岔路口撞到一輛在幹道行駛的摩托車，警察到現場筆錄依照告訴人講的要告計程車司機內容寫一寫、現場圖畫一畫之後就移送被告業務過失傷害，後來檢察官也認定計程車司機違反道路交通安全規則予以起訴，這個計程車司機也被法官判業務過失傷害罪有期徒刑確定。

被告一直認為警察在圖上應該畫出閃光紅燈和閃光黃燈，並且認為這樣會對他的刑度有影響，所以他認為法官認定事實沒有參考到閃光號誌而有錯誤，據此被告上訴高等法院，但是高等法院法官認為上訴沒有理由而駁回，這個案子就到此確定。

刑事訴訟法對於確定判決的救濟手段有兩種：法官對於事實的認定錯誤以再審制度來救濟，法官對於法律適用錯誤則是以非常上訴制度救濟。結果被告不知道再審書狀的例稿在哪裡，於是誤打誤撞來到法務部的網站，居然將檢察署的書狀例稿區，關於再議空白例稿拿來想用在再審上面：

在場各位法學前輩及部隊長官，我們知道，再議是對於檢察官的不起訴處分不服，向檢察官的上級檢察署也就是高等法院檢察署聲請救濟的制度，再審和再議差這麼多，一個是對於法院確定判決的事實不服，一個是對於檢察官不起訴處分表示不服。而被告在法務部的網站，找到了再議的空白例稿：



在線上開啟後填入姓名、國民身分證號碼、電話、地址等個人資料後，再使用「另存新檔」命令，在存檔的檔案名稱欄位填入「http://www.moj.gov.tw/eservice/admin/fileupload/刑事聲請再議狀(被告聲請)橫書.doc」，並將變更後的檔案以存檔方式上傳存回伺服器。

二、烏龍主因－權限設定不設限

法務部這個空白例稿系統外包給資訊廠商時，原本應該把透過網路連線外部存取的這個區域檔案權限做適當的設定，也就是應該設定成只能讀取（read）再議這個檔案，當然不能允許寫入（write）再議這個檔案，但是這個資訊廠商卻對於權限的設定沒有設限，居然設定成為 everyone，也就是每一個登入的使用者都有權限可以讀取及寫入，換句話說，就是沒有設定權限的限制。如果法務部網頁上單一申辦窗口整個區域權限都設成 everyone，則此區域的首頁也就可以更改，如果上傳一些裸照或有的沒的檔案的話，那事情就嚴重了。

因為權限設定錯誤，這樣子就可以改首頁，他現在改的是再議的空白例稿區，一般很少人會來這邊，此區的利用率老實說不是很高，被告選擇另存新檔這個命令之後，他的個人資料就被儲存在法務部的伺服器這邊，結果他隔天開啟自己的電腦想要繼續編輯昨天填完個人資料的 Word 文件，結果當然找不到，只好一錯再錯再來法務部再議例稿區，此時被告發現他的名字、國民身分證號碼、電話等資料已經填好了，問題來了，這些個人資料是誰填的？當然他自己填的，但是他會不會覺得是他自己填的？他不會，他會認為是法務部故意洩漏個人資料。各位，這個就是無故變更他人電腦內之電磁記錄！這麼烏龍的案件發生在法務部，自己草擬的法案，自己先來測試看看條文好不好用……，刑法第 359 條規範不得無故變更他人電磁記錄，這不就是無故變更他人的電磁記錄不是嗎？問題是行為人自己知不知道這樣會無故變更他人電腦的電磁記錄？

光是舉這個例子來說，變更他人電腦內的電磁記錄需不需要什麼高超的駭客手段？不用，是因為部分原因是法務部自己例稿區的權限設定不當或是錯誤所導致的。不過話說回來，我家門沒有關或是上鎖，所以你可以來偷東西對不對？好像不是，也不能這樣子講。

這個用另存新檔變更他人電磁記錄的行為人，想找法務部弄掉他的個人資料，其實，只要再次開啟同一個再議檔案，把他的資料刪掉，再來一次「另存新檔」就可以了；不過他沒有這麼做，他後來直接去找 TVBS 電視臺想要爆料，就說法務部把他的個人資料登在網站上面洩漏個人資料，TVBS 的記者上網去查證果然不假，於是就做了一則報導，下午就跟被告一起到法務部來興師問罪開記者會，資訊處處長知道他在陳情什麼事情之後，自己也上網去一窺究竟，結果真的有被告的資料，糗大了，只好出來道歉。

記者會結束之後，越想這件事越有蹊蹺，就去查那個例稿登入登出的記錄檔（log 檔），發現就是那個再議的人他自己在登入這個例稿區，半年來幾乎只有他去存取再議檔案，這是烏龍一場，就這麼簡單，還好法務部這個書狀例稿沒啥人在用，真有很多人在用登入的 IP 一大堆，案子就不好查了；所以這個案子很經典，被告自己填的個人資料，又自己來開記者會羞辱法務部，我就起訴他侮辱公署。

三、法院對「烏龍案」的看法

起訴之後，這個案子就特殊了，我們來看看法官怎麼處理。95 年度訴字第 1117 號、96 年度訴更(一)字第 1 號，地方法院的法官認為「法務部網站上之單一申辦窗口系統為數年前所開發之舊系統，網路使用者可以另存新檔方式將檔案內容修改後存回伺服器」，這是他的看法。

不過我質疑的是，法務部的網站使用新或舊系統的架設，是法院所能置喙的嗎？法官有調查架設該例稿專區網站使用何種作業系統嗎？縱使有調查，又如何評斷 UNIX、FreeBSD、Solaris、SunOS、Windows NT 等各種伺服器級作業系統含各種版本之優劣？如果法務部用免費的 Linux 來架站，就代表一定比較不安全嗎？況且，刑法第 359 條的構成要件，是被告無故變更政府機關之電磁記錄，此與法務部存放空

白例稿的資料庫，不管是軟體像是作業系統、硬體像是中央處理器、硬碟、路由器、橋接器等等設備建置是否老舊，安全性等級需否提昇有什麼關係？用被害人的電腦硬體或軟體老舊，所以會被入侵，這點顯然法官的認知比較缺乏伺服器權限的觀念。

我認為法官說「網路使用者可以另存新檔方式將檔案內容修改後存回伺服器」這部分，明顯抵觸刑法的禁止規範，根本就是錯誤的，我所持的看法與判決所採取的見解相反。

此外，法官又說「被告之教育程度為國中畢業，且曾擔任水泥工、現為計程車司機之學、經歷，其所學及專長顯與電腦及網路等相關專業知識無涉，衡情應無法輕易察知電腦程式具有漏洞」。這一部份顯然判決忽略了一件事：何以學歷或程度不好就不可以當駭客呢？駭客有規定要何種職業嗎？高學歷的人就一定是電腦高手或是就可以有駭客入侵他人電腦的能力嗎？法官用何種標準來「衡情」被告不具有改寫電磁記錄的能力？也不過就是存檔嘛，差異只是在儲存(或寫入)在自己的電腦（又叫做本機端）硬碟內，或是在別人的電腦（本件中就是指法務部的資料庫伺服器）而已，哪裡需要什麼特別技能？！又本件是資料庫的例稿電磁記錄因為權限錯誤遭外部連線寫入，跟有沒有察知電腦程式有沒有漏洞之間有什麼關係？

四、摘錄：最高法院 97 年度台非字第 285 號判決理由

非常上訴理由：「一、按判決不適用法則或適用法則不當者，為違背法令，刑事訴訟法第三百八十七條定有明文。次按刑法第三百六十一條之罪，並非告訴乃論之罪，此觀『中華民國刑法部分條文修正草案（電腦網路犯罪部分）審查會通過行政院、司法院提案現行法條文對照表』第三百六十三條說明欄所載『至於第三百六十一條之罪，因公務機關之電腦系統往往與國家安全或社會重大利益密切關聯，實有加強保護之必要，故採非告訴乃論以嚇阻不法。…審查會：照案通過。』

及所有立法院審議過程之紀錄即明(見立法院公報第九十一卷第七十七期第一頁、第九十二卷第二十一期第五十九—六十二頁、第九十二卷第二十四期第一六一—一七七頁、第九十二卷第二十六期第一三五—一三八頁、第第九十二卷第二十九期第一二八—一五二頁、第九十二卷第三十三期第一七八—一八0頁)(如附件一)。再按『侵害國家法益者,該機關有監督權之長官,得代表告訴,本件上訴人所犯刑法第三百五十四條之毀損罪,業經有監督權之楠濃林區管理處岡山工作站主任向檢察官提出告訴,原判決以其僅係告發,顯有違誤。』亦有貴院六十七年台上字第四二五七號刑事判例可考(如附件二)。而當時各林區管理處依(前)台灣省政府六十二年十二月十三日府人丙字第 124475 號令發布之(前)台灣省政府農林廳林務局各林區管理處組織規程第七條規定於轄區內設置之工作站,並非獨立之行政機關,而係內部單位,此觀該組織規程規定自明(如附件三)。另按『資訊處掌理左列事項:一、關於本部暨所屬機關資訊系統之規劃、開發及推動事項。二、關於本部暨所屬機關資訊作業之指導、監督事項。三、關於本部暨所屬機關資訊相關工作人員之訓練事項。四、關於刑事偵查、執行案件資料處理之管理事項。五、關於犯罪矯正、保護管束資料處理之管理事項。六、關於檢察法規資料之彙整、運用事項。七、關於本部資訊設施之管理、操作及維護事項。八、關於本部與其他機關間資訊交換之協調事項。九、其他有關法務資訊事項。』法務部組織法第十六條亦著有明文(如附件四)。二、本件原確定判決係以下列理由,就被告被訴妨害電腦使用部分不另為公訴不受理諭知:(一)九十二年四月二十四日立法院第五屆第三會期司法委員會第十六次全體委員會議紀錄,似未就刑法第三百六十一條是否須告訴乃論乙節有所定論。佐以立法院公報第九十二卷第二十九期第一四八頁所刊登之中華民國刑法部分條文修正草案行政院、司法院提案條文對照

表第三百六十三條說明欄第三項雖記載『至於第三百六十一條之罪，因公務機關之電腦系統往往與國家安全或社會重大利益密切關聯，實有加強保護之必要，故採非告訴乃論以嚇阻不法，…。』惟其後經總統公布修正條文時，刑法第三百六十三條之立法理由第三項業經全文刪除，此有卷附之法源法律網立法理由及上開立法院公報各一份為憑，故僅依上開立法院會議紀錄，尚難認立法者於立法時業已明確說明刑法第三百六十一條採非告訴乃論之意旨。因之公訴人起訴被告犯刑法第三百五十九條、第三百六十一條之罪，依同法第三百六十三條之規定，須告訴乃論；若未經合法告訴，公訴人即遽予起訴，依刑事訴訟法第三百零三條第三款之規定，法院自應諭知不受理之判決。（二）法務部資訊處僅為該部之內部單位，尚非獨立之行政機關，法務部資訊處縱有法益遭受侵害，仍應由法務部有監督權之首長代表提出告訴，方屬適法，本件法務部資訊處並無訴訟主體之能力，則其告訴，自難認為合法。三、惟按刑法第三百六十一條之罪並非告訴乃論之罪之理由，已如前述。至原確定判決認總統公布修正條文時，刑法第三百六十三條之立法理由第三項業經全文刪除，有法源法律網立法理由可據一節，固有法源法律網下載之立法理由可供參考，然法源法律網並非政府網站，其所載之立法理由復未載明出處，與首揭立法院公報所載內容又不符，已無可信性；況總統公布法律修正條文時，並不一併公布立法理由，此為眾所週知之事實，故原確定判決該部分之立論，並無依據，不足以推翻首開刑法第三百六十一條之罪並非告訴乃論之罪之說明。而縱認刑法第三百六十一條之罪，須告訴乃論，惟依貴院六十七年台上字第四二五七號刑事判例意旨及法務部組織法第十六條規定，法務部資訊處處長就有關法務資訊事項遭侵害時，自得合法提出告訴。查本案於法務部調查局調查中，法務部資訊處處長陳○○已於九十四年十一月十一日向該局提出委任狀載明委任黃○

○為告訴代理人，黃○○並於該局在九十四年十一月十日詢問時表明代理法務部資訊處提出告訴，有委任狀及詢問筆錄分別附於台灣台北地方法院檢察署九十五年度他字第七一０七號卷第八十七頁及第八十八—九十一頁可稽，則本案自亦已合法提出告訴。綜上說明，原確定判決以刑法第三百六十一條之罪須告訴乃論及本案未據合法告訴為由，就被告被訴妨害電腦使用部分不另為公訴不受理諭知，自有適用法則不當之違法。四、爰依刑事訴訟法第四百四十一條、第四百四十三條提起非常上訴，以資糾正。」等語。

本院按判決不適用法則或適用不當者，為違背法令，刑事訴訟法第三百七十八條定有明文。又刑法第三百六十一條及第三百六十三條分別規定：「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。」，「第三百五十八條至第三百六十條之罪須告訴乃論」，固未就同法第三百六十一條之罪，是否屬告訴乃論予以明定。惟按刑法分則所列各罪，其須告訴乃論者，以法律有明文規定者為限。又法律解釋固須探究立法者於制訂法律時所作價值判斷及其所欲實踐之目的，以推知立法之原意，惟如文義解釋已極為明確，仍應以文義解釋為先，而無庸另作論理解釋。原確定判決雖以：刑法第三百六十一條於上開司法委員會討論時，就本罪是否屬告訴乃論，已有爭議，並無定論，且其後經總統公布修正條文時，刑法第三百六十三條之立法理由第三項業經全文刪除，有卷附之法源法律網立法理由可稽，尚難認刑法第三百六十一條係採非告訴乃論之意旨，況上開規定之編排方式與同法第二百七十七條規定：「傷害人之身體或健康者，處三年以下有期徒刑、拘役或一千元以下罰金。犯前項之罪因而致人於死者，處無期徒刑或七年以上有期徒刑；致重傷者，處三年以上十年以下有期徒刑。」、同法第二百八十條規定：「對於直系血親尊親屬，犯第二百七十七條或第二百七十八條之罪者，加重其刑至二分之

一。」、及同法第二百八十七條規定：「第二百七十七條第一項、第二百八十一條、第二百八十四條及第二百八十五之罪，須告訴乃論。但公務員於執行職務時，犯第二百七十七條第一項之罪者，不在此限。」相較，兩者之規定方式均屬相同；且參照本院民國十九年上字第一九六二號判例：「本案原審及第一審判決均認上訴人毆傷某氏，係犯刑法第二百九十三條第一項之罪，依同法第三百零二條規定，該罪須告訴乃論，雖某氏係上訴人之直系尊親屬，應依同法第二百九十八條規定加重其刑，然該條既明定為對於直系尊親屬犯第二百九十三條第一項之罪者，加重本刑二分之一，是加重其刑者，而所犯者仍係第二百九十三條第一項之罪，第三百零二條復明定為第二百九十三條之罪，須告訴乃論，又係以罪而不以刑，則對於直系尊親屬犯第二百九十三條第一項之罪者，自在告訴乃論之列。」，益證刑法第三百六十一條應屬告訴乃論，本件被告被訴刑法第三百六十一條之加重破壞電磁紀錄罪部分，既僅由法務部資訊處處長提出告訴，自非合法，該被訴部分，自不得受理等旨。惟查刑法第三百六十一條於九十二年四月二十四日立法院第五屆第三會期司法委員會第十六次全體委員會議討論時，固有認應採告訴乃論之意見，然嗣經當時之法務部顏大和次長說明：「之所以第三百六十一條及第三百六十二條不採告訴乃論，是因為第三百六十一條的刑度已經有加重，所以不應該再適用告訴乃論」等語，並表明希望維持原來公訴罪之規定後，並未再有爭議。嗣經二、三讀程序，均未再作文字之修正或增刪。參諸「中華民國刑法部分條文修正草案（電腦網路犯罪部分）審查會通過行政院、司法院提案現行法條文對照表」第三百六十三條說明欄第三點所載：「至於第三百六十一條之罪，因公務機關之電腦系統往往與國家安全或社會重大利益密切關聯，實有加強保護之必要，故採非告訴乃論以嚇阻不法。……審查會：照案通過。」，有立法院審議過程之紀錄甚明（見

立法院公報第九十二卷第二十六期第一三七頁、第九十二卷第二十九期第一四八、一四九頁、第九十二卷第三十三期第一八０頁），足見立法院制定通過之刑法第三百六十一條，並未將之列為告訴乃論之罪，應無足疑。至上開條文經總統公布修正時，法源法律網就刑法第三百六十三條之立法理由雖僅登載：「一、本條新增。二、刑罰並非萬能，即使將所有狹義電腦犯罪行為均規定為非告訴乃論，未必就能有效遏止電腦犯罪行為，尤其對於個人電腦之侵害行為，態樣不一，輕重有別，如受害人無告訴意願，並配合偵查，實際上亦難達到偵查成效，故採告訴乃論，有助於紛爭解決及疏解訟源，並可將國家有限之偵查及司法資源集中於較嚴重之電腦犯罪，有效從事偵查，爰增訂本條。」，並未記載前揭第三點之說明，但既與立法院公報之上開內容未符，應係漏載，尚難認該第三點所載之說明係有意刪除。況按之首開說明：刑法分則所列各罪，其須告訴乃論者，以法律有明文規定者為限。又刑法分則之加重，係就犯罪類型變更之個別犯罪行為予以加重，成為另獨立之罪名。刑法第三百六十一條係就對象為公務機關之妨害電腦使用罪所訂之加重懲罰規定，屬刑法分則加重之獨立罪名，其是否屬告訴乃論之罪，自應以法律有無明文規定為判斷之基準。而刑法第三百六十三條既未明定第三百六十一條之罪須告訴乃論，則其非屬告訴乃論之罪，乃屬當然。本院十九年上字第一九六二號判例，所闡述之法理，自不宜適用於本條之規定，原判決予以援引，自有違誤。乃原判決見未及此，竟以刑法第三百六十一條之加重破壞電磁紀錄罪係告訴乃論，因認被告被訴違反刑法第三百六十一條部分，未據合法告訴，惟公訴意旨認此部分與論罪科刑之公然侮辱公署罪間，有裁判上一罪之牽連關係，故不另為不受理之諭知。揆諸上開說明，顯有不適用法則之違背法令。案經確定，非常上訴執以指摘，

洵有理由。惟原判決該違法部分尚非不利於被告，應由本院僅將其違背法令之部分撤銷，以資糾正。

柒、刑法第 360 條之名詞定義不明確

我們繼續看刑法第 360 條：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」所謂「干擾」，請看一下原來的舊刑法第 352 條第 2 項，「干擾他人電磁紀錄之處理，足以生損害於公眾或他人者，亦同」民國 92 年 7 月就修法了，修成這樣：「無故以電腦程式或其他電磁方式干擾」，干擾是日本法的用語，然後我們立法直接繼受。

本條增訂的立法理由指出，干擾的行為方式並不明確，用什麼手段來干擾？所以這個手段不明確、很容易產生困擾。我的問題是：「什麼叫做干擾？」心情上的不爽應該不算是干擾，因為干擾的對象必須是電磁記錄，而且心情上的干擾也沒有辦法舉證。舊法是「干擾他人電磁紀錄」，新法是「干擾他人電腦」；舊法就是搞不懂什麼叫做干擾，新法還是沒有解決這個問題，不過新法加了條文上的限制，一定要用科技手段——要用電腦程式或其他電磁方式。什麼叫「電腦程式」？什麼叫「電磁方式」？對於未曾學習電腦、不學程式的法律人來說，如何定義這些概念、名詞都是重大障礙。

如果大哥大會發射電磁波，也應該算是一種「電磁方式」，大哥大放在螢幕或主機旁邊會不會產生雜訊？如果會有雜訊，那在加護病房撥打大哥大，就會該當這一條，可不可以接受？拿大哥大在加護病房撥打幾分鐘就當現行犯加以逮捕－因為人工心肺機是屬於電腦設備，構成要件乍看之下好像也完全符合？本條到底要管制加護病房外面的行為，還是在規範電腦或網路犯罪？什麼情況之下叫做干擾？不

好定義，只好透過個案實例來予以累積。

捌、刑法第 360 條之立法理由：通訊安全

但是這一條的立法理由有說到，譬如 DDoS（阻斷攻擊）、Ping Flood（洪水攻擊）等以癱瘓網路為目的的都算干擾，換言之，通訊安全是這一條的立法理由。那問題又來了，什麼叫做 DDoS？Ping Flood？其他以癱瘓網路為目的？沒有資訊背景的人，看看就算了，了解到我們有先進的立法就好？！

目前發生的 DDoS 沒有一件可以查得出來，主要是因為幾乎是跨領域（境外）的攻擊，因為查證上幾乎不可能，且必須聚集一定攻擊能量才會有阻斷網路連線的效果，換句話說，是因為量變（數量太大）而產生質變（阻斷連線），所以就算了，還是那句話「對於您的遭遇，我們深表同情」，只能這樣，其實也是很無奈。

立法理由還有一段很有趣，它說為了避免砸毀電腦也算干擾，故需「以電腦程式或其他電磁方式」等科技手段為行為始屬之。各位，如果是警察、憲兵或者檢察官，砸毀電腦你會把它當作是干擾嗎？

立法理由又說到，廣告郵件不算是這一條的干擾。廣告郵件不算是這一條的情形，它的立法理由有說，「除非能證明行為人有破壞 ISP 系統或『灌爆』使用者信箱之故意，並致生損害於公眾或他人者」。各位，這個「灌爆」，學法律的人不應該這樣用。

刑法第 173 條以下有放火罪、第 178 條以下有決水罪，「爆炸」在刑法上是有特定意義的，對法律人來說，「灌爆」是屬於火星文；這樣的網路行話不適合用在官方文書上。

假設你是廣告商寄發電子郵件，一定是希望收電子郵件的人收得到嘛，既然希望人家收得到郵件，那你會不會把送電子郵件的郵差殺死？ISP 系統不就是幫你寄信的人嗎？假設我用 Hinet 去寄電子郵

件，立法理由要求檢察官能證明行為人寄電子郵件的目的就是希望破壞 Hinet，破壞 Hinet 那人家還收得到嗎？收不到。寄廣告電子郵件主觀上就是希望別人能收到而不是不能收到，所以是檢察官要證明行為人的目的是要妨礙郵件伺服器而寄不出電子郵件，顯然在文字表現有邏輯上的錯誤。

再來就是「灌爆」，3 年多前 hotmail 的存檔限制是 2MB，現在是 2G 甚至更高。在當年的情況下，隨便一封夾帶有影音、照片的檔案都是 1MB、2MB，對不對？那很容易就「灌爆」了。就算是現在的 2G，假設你已經使用了 1.99G 的信箱容量，只剩下 1MB 或 10MB 的容量，那麼一樣很容易就會被「灌爆」。我會不會被法辦，取決於收件人信箱的容量大小，你的感覺怎麼樣？檢察官要去證明寄信的廣告商是要把郵差殺死，或者因為收信的人的信箱容量太小導致無法收信，就要拿行為人來偵辦，這些對於行為人的主觀動機上都沒有認識可能性。結論就是，廣告郵件不算這一條規範的情形。

玖、刑法第 361 條是否為「告訴乃論」罪？

我們繼續來看刑法第 361 條：「對於公務機關之電腦或其相關設備犯前三條（刑法第 358、359、360 條）之罪者，加重其刑至二分之一」；我們都知道，依照學說及實務的一貫見解，只要加重其刑在分則加重的情形下，分則加重是屬於條文的變更，算是一個新的罪名。在刑法前三條之罪（刑法第 358、359、360 條）是告訴乃論，那這一條（刑法第 361 條）是不是告訴乃論？曾經就產生過爭議，刑法第 363 條說刑法第 358 條至 360 條是告訴乃論，就是沒有說到刑法第 361、362 條是不是告訴乃論，就會產生不同見解。根據立法理由及立法院的會議記錄，刑法第 361 條應該是非告訴乃論，最近最高法院也表示見解，在最高法院 97 年度臺非字第 285 號判決，就明確的表

示刑法第 361 條並非屬於告訴乃論之罪。

拾、「公務機關」之定義

至於什麼叫做「公務機關」？依照立法理由的說明，就是指電腦處理個人資料保護法第三條所定的依法行使公權力之中央或地方機關。

這裡提出一些問題供大家思考：請問公務機關的電腦一定放在公家機關裡面嗎？不一定，對不對？比如說國防部軍事情報局的網頁一定要放在軍事情報局本部裡的電腦嗎？可不可以去中華電信租 10MB 空間，把軍事情報局的網頁放在 Hinet 的機房裡，可不可以？當然可以！主機借用、虛擬硬碟的租用或者因為頻寬不夠而產生的主機代管都有可能發生。

所以入侵公務機關的電腦不一定是指地理上公務機關的限制，有可能這臺機器的一部分是作為公務機關的租用或借用，也有可能這臺機器就是公務機關但是放在民間的 ISP 上面，這種情況都非常有可能發生。

另外就是，警察機關有些人利用公務電腦去查人家的個人資料、利用公務機關的電腦去做妨害秘密罪章的事，這種也要加重其刑至二分之一；再來，對於公務機關的電腦犯刑法第 358、359、360 條之罪，也是加重其刑至二分之一。各位，一個是用公家機關的電腦犯罪，一個是對公家機關電腦實施入侵、變異電磁記錄、干擾或者其他行為的犯罪；這兩個是不一樣的條文，請務必區分清楚。總括的結論就是說，最高法院的見解就是刑法第 361 條屬於非告訴乃論，當然就不受告訴乃論期間 6 個月的限制。

拾壹、刑法第 362 條「駭客條款」之實務操作

刑法第 363 條是指前幾條（358、359、360）之罪，須告訴乃論的規定。再回來講到刑法第 362 條，這條是我們立法最得意的條文，屬於「駭客條款」，條文內容是：「製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，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」。

它的條文的行為有兩個：一個是寫程式--「製作專供犯本章之罪之電腦程式」，另外一個是「供自己或他人犯本章之罪」，有兩個行為。這是我們最得意的條文，不過也是我覺得最值得商榷的條文。為什麼最值得商榷？它說要「專供」犯「本章」之罪，所以不能犯「別章」。所以一旦犯了這個罪而被警察或憲兵移送到檢察官那邊，請了律師來，千不要做「無罪答辯」，而應該做「無恥答辯」，例如陳述：「我的當事人寫這個程式的目的，是想犯從刑法第一章到最後一章的罪，如果寫這支程式可以洗錢、援交、侵害著作權、妨害兵役或販毒他也想要犯；只要有刑罰規定的條文，他都想犯……」。因為這樣就不是「專供犯本章（即專指刑法第 36 章）」，他還想兼犯別章，就不會該當這一條犯罪了，這實在很弔詭，很不幸，這就是實務操作所產生的結果。

而且各位要知道，網際網路還有跨地域的特質。去美國旅遊還會先熟讀美國刑法嗎？不太可能吧。所以你有沒有辦法期待一個外國人知道本章是哪一章？通常會寫程式的不見得是本國人，對不對？還要專供犯本章，這個條文只能適用於生長於臺灣的臺灣人，因為他不能說他不知法律嘛，對於外國人你很難去期待。所以條文的目的是要處罰寫病毒、木馬程式、蠕蟲程式等惡意程式的人，但是在實務上操作的結果，這條很難去適用。

本來立法的草案是說七年有期徒刑，被立法委員改成五年，他們很難想像為什麼寫程式和搶奪罪的刑度要一樣重。各位，當時立法的

背景有連續犯，因為寫一個程式而導致上百萬臺電腦受害，依照臺灣的法制，連續犯再怎麼判也是五年以下，至多加重其刑至二分之一。現在廢掉連續犯之後，這個條文是不是還需要五年？就值得商榷了。因為只要駭一臺電腦，理論上是不同的財產法益，比如說一個電腦判三個月，500 臺電腦似乎就應該乘以 500。

拾貳、網路犯罪管轄權的歸屬問題

看了這麼多國外有關網路的民事和刑事判決，可以發現關於網路犯罪的管轄權，國外每一個法院都不斷地想辦法擴張其管轄領域；無論如何，法院的管轄權伴隨主權的擴張其範圍，現在則是透過網路不停地擴大。

刑事犯罪的法院管轄權只有兩個，一個是犯罪地、一個是被告之住所、居所地或所在地。那什麼叫做網路犯罪的犯罪地？沒有辦法界定，實務上高等法院 89 年上訴字 1175 號刑事判決已經說明：依照各國網路犯罪管轄權之通例，網路犯罪要斟酌：網頁所在地、電子郵件主機所在地、傳輸資料主機所在地，或者是交易地來決定。

這樣的結果我們知道，內湖科學園區的 seednet、廣通或者臺灣固網都在那邊，臺灣士林地方法院會因此變成一大部分得網路犯罪的承審法院，另外一個就是臺北地方法院，因為中華電信在臺北市仁愛路、信義路之間，所以臺北地方法院也會有一大半的網路犯罪案件，其他地方法院相對來講就會比較少。另外可能就是線上遊戲公司所在地，例如天堂Ⅰ、天堂Ⅱ的公司在臺北縣板橋市，所以也有可能到臺灣板橋地方法院去訴訟。

拾參、病毒、蠕蟲與木馬程式

什麼叫病毒？病毒的特性會自己複製然後再透過磁片、光碟、隨

身碟或是網路傳染、散布，但是不會去偷別人的資料。什麼叫蠕蟲？也是會傳染，主要是透過網路，其目的是在消耗電腦系統的資源（運算能力），或是消耗網路連線的頻寬。至於木馬程式，雖然會透過儲存媒介或是網路來傳染，但是通常不會自己不停的複製，而且現在的木馬程式，常常會透過 USB 隨身碟或是外接式硬碟，或者是網路寄送，也就是用寄送的方式傳染，甚至瀏覽網頁也有可能被植入類似木馬功能的惡意程式，有些程式甚至兼有木馬程式和病毒的特質。

結語

辦理電腦犯罪案件，若沒有電腦技術背景，就容易出現一些不合理而無法讓人信服的判決，這需要科技人和法律人的結合，這樣才能夠把案件處理得圓滿，謝謝大家！