機密維護常識彙編（101 年 1 月份）

＊政府機關資訊系統遭承包廠商放置後門程式案例

壹、案情概述

一、某甲科技公司於 97 年 7 月至 98 年 6 月期間，承攬某部會中部辦公室資訊作業系統工程，由經理陳○○、工程師董○○2 人負責相關系統維護操作，渠 2 人未經該中部辦公室同意，於資訊系統中放置後門程式，不需帳號、密碼，即可利用該後門程式，由遠端連線進入電腦系統主機，執行資料存取、增刪、檔案上傳、下載等作業。

二、案經後續承攬該中部辦公室之科技公司，進行舊系統資料整理時，察覺有後門程式，向調查局臺北市調查處檢舉，經清查該主機網站伺服器連線紀錄，發現某甲科技公司電腦內，於 98 年 1 月至 99 年 2 月間，有數十筆與該中部辦公室連線之存取記錄，陳○○、董○○2 人涉嫌觸犯刑法妨害電腦使用罪。

三、本案於 99 年 10 月移送臺灣高雄地方法院檢察署，嗣於 100 年 3 月 19 日予以緩起訴處分，內容略以：陳○○2 人所為，係犯刑法妨害電腦使用罪等；審酌被告 2 人並無前科，係為圖一時之便而為前開犯行，所生危害非鉅，且犯後均已坦承犯行，犯罪情節尚屬輕微，爰參酌刑法第 57 條所列事項及公共利益之維護，認以緩起訴處分為適當。

貳、經驗教訓

一、缺失檢討

（一）廠商動機啟人疑竇

廠商承包政府機關電腦系統維護，私自於電腦設備植入後門程式，以遠端操控執行系統維護及修復等工作，公務機密資料即有外洩、刪除及遭竄改之虞，廠商動機啟人疑竇。

（二）承辦人員欠缺資安警覺

該中部辦公室相關承辦人員，於辦理電腦系統維修招標案件時，對廠商遠端操控作業方式欠缺警覺，未能於合約載明限制廠商使用遠端操控條款，致資安管理出現漏洞，予人可乘之機。

二、策進作為與建議

（一）落實資訊安全管制

各機關查核廠商電腦維護作業時，除應確實遵守資安流程，並應建立周延檢核監督機制，嚴防洩密事件發生。

（二）強化資安專業訓練

應經常辦理資訊安全講習，提升同仁電腦專業知能；與廠商簽訂承攬合約時，應載明限制使用遠端操控條款，並要求簽具保密切結，防範廠商伺機竊密，避免公務資料外洩。

（三）加強法紀教育宣導

少數員工常因便宜行事，未依資安規定執行公務，甚至違法而不知，須持續加強法紀宣導，俾杜絕相關事件發生，確保公務機密安全。

參、相關法規

一、刑法第三百五十八條

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，而侵入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。

二、刑法第三百五十九條

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，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。

（文摘自法務部調查局調查站）

＊慎防中共網軍遍襲全球網路

在網路運用高速發展的今天，即使科技先進如美國，對於資安防護亦不敢大意；事實上，美國早已與包含英、法在內等約六十個國家締結相同的資訊安全協定。然而

日本礙於憲法第 9 條禁止擁有集體自衛權的問題，以及可能侵犯國民的知情權及新聞自由等基本人權，因此到最近才簽署該協定。一般研判，影響日本風向球轉變的原因主要有二：首先，日本面臨北韓核武危機與中共快速擴武的外在壓力，必須加快與美國軍事同盟的建立速度，資訊安全的共同防護便顯得急迫；其次，美、日安保的核心機密頻遭日本自衛隊洩漏，使美國對日本軍事安全感到憂心，因此要求簽署協定，進而提升資安系統的水準。

根據統計，中國大陸每天製造的木馬和後門病毒已占全球該類病毒的三分之一。為因應網路攻擊威脅，維護資訊安全，各國莫不投注心力。例如：德國資訊安全局為了反制中共電腦間諜，特別製作資訊安全手冊，發放給聯邦政府，加強宣導資訊安全的重要性；美國更因是駭客組織攻擊的主要目標，尤其是針對軍事設施及人員，因此更不敢放鬆，美國國防部目前每天都要對其網路進行六百萬次的偵測。可見全球對網路安全的重視。

而同樣面臨中共高度威脅的我國，更身處資訊安全危機的第一線。中共自 2002 年至 2008 年設置了電子戰分隊、網路隊分隊、駭客分隊、信息救援分隊，並在各個產業設立國防訊息組織分隊，2006 年更在二砲內成立電子戰藍軍部隊實施攻防演習，大幅進行共軍網路攻擊演練，以提升其網軍對我之攻擊能力。面對中共網軍鋪天蓋地、無孔不入的攻勢，國防部亦先後策頒多項有關資安的規定，要求各單位確實遵行，使官兵做好個人基本防護設施，期能達到「零資安事件」的目標，以確保國軍資訊安全。

中共已是全球公認網路最大安全威脅的來源，且此一威脅隨著中共經濟力的成長，也同步增加。前美國國防部副次長勞里斯曾在美國國會作證時表示，中共利用日益繁榮的經濟所提供的資訊技術與專業知識，已在網路戰中取得重大進展。近年來，全球各地受到來自中共大陸的網路攻擊事件有增無減，也驗證了這個危險的趨勢；當全世界都在提高警覺，而面對中共最大威脅的我國，又豈能掉以輕心！

＊建立「資安防護如同作戰整備」認知

根據媒體報導，美國國防部於去(97)年 11 月下旬緊急通令全球各單位的所有軍、文職人員，立即全面禁止在公務電腦上使用隨身碟，以防止進一步遭到駭客破壞；而

為了貫徹此一指令，美國軍方已對若干儲存極機密資訊的電腦，將其 USB 槽進行設定處理，使其根本無法使用，以收「正本清源」之效。眾所皆知，伴隨著資訊科技快速發展、科技產品樣貌多變與創新、無線網路傳輸的快速與普及，使得資料存取管道及傳輸更加便利；但同樣的，機密資訊遭受竊取與破壞的風險也隨之大幅提升。網際網路已成為一個沒有邊界的無聲戰爭平台，技術卓越的網路駭客，隨時可能藉由網路侵入防護能力薄弱的電腦並進行破壞。

為了保護重要基礎建設之資訊系統免於遭受破壞性入侵的威脅，進而達成保護經濟與人民安全的目的，美國早在 2003 年就制定「確保網路安全的國家戰略」 - 即將戰略目標置於預防國家重要基礎建設遭受網路攻擊，降低遭受網路攻擊的弱點；即使遭受攻擊，亦可將損害及復原時間降到最低。除被動防護外，美國也投入大量預算，積極建置網路及資訊作戰專業部隊，對可能攻擊美國資訊基礎建設或竊取重要資料的潛在敵國，採取進行攻勢的反制行動。

根據「臺灣網路資訊中心」的調查，目前臺灣地區二千三百萬人口當中，上網人口即超過一千五百萬人，顯示網路與我們的關係真是密不可分。資訊社會的發展是人類文明發展的重要里程，然而伴隨網路連線所構成的通路，更把世界各國聯結成天涯若比鄰的地球村，為人類文明發展的軌跡開創革命性的進程。然則，資訊安全所造成的威脅，已出現在諸多層面，包括對個人、團體、企業、政府部門，乃至整個國家，幾乎無所不在。因此，如何成為耳聰目明的資訊使用者，更需要高度智慧。如若不然，網路連結等同開門揖盜，將成為資訊叢林中輕易被獵殺的小白兔，面臨的將是災難而不是甜美的滋味。

尤其在目前兩岸情勢詭譎多變的情況下，表面上，兩岸交流與互動頻繁，實際上中共以資訊為手段，對臺進行心理戰、輿論戰及統戰的手法，未曾一日稍歇；透過網路駭客針對國軍資訊系統進行資訊竊取與系統破壞的行動，從未停止。近年來，政府部門及民間企業機構迭傳遭受網路駭客攻擊的事件，雖然這類攻擊事件中有極少數是反社會分子或網路怪客的個別性攻擊行為，但是多數的攻擊行動經過查證之後，確屬中共網軍部隊所為。

也因此，面臨中共網軍無時無刻地入侵與破壞威脅之際，「保密習性」和「資安素養」的建立，已成為現代國民不可或缺的重要德行。因為在資訊科技高速發達的現代，中共未來攻臺作戰能力將不僅僅侷限於武力手段，其在發動戰爭前及實戰進行全程，必將利用衛星、網軍及信息作戰部隊，以電子干擾、電腦病毒及資訊炸彈等軟殺手法，先行對我發動資電作戰，企圖侵襲我方政府部門或重大政經建設的電腦網路系統，藉此擾亂民心士氣與抗敵意志；甚至使用網路電子干擾及信息作戰等超限戰模式，破壞民間的交通、電力、通訊與金融網路，製造臺灣社會內部的混亂與恐慌。

根據一家防毒軟體公司對 2006 年下半年全球網路惡意攻擊活動所做的調查報告指出，中國大陸占全球網路惡意活動總數的 10%，僅次於美國為全球第二。隨著大陸地區網際網路用戶的增加，駭客侵擾和網軍的間諜活動為中共帶來的龐大利益，促使中共駭客大軍和網軍仍能繼續擴大中。在如此嚴峻的網路攻擊威脅情勢中，我國防部雖早已成立資訊專業部隊，並吸納軍中與民間的高科技人才，積極防範中共網軍攻擊行動；然而我們絕不可劃地自限，尤須認清資訊安全維護的基礎，除了資訊安全建設與管理，更在於全民良好的保密習性與資訊化條件的提升。

值得一提的就是，現今國軍各級單位除了在資訊基礎建設更新與資安防護設備提升等作業上，已做了大幅度的改善外，對於人員資安防護概念教育的強化，也做了相當的努力，例如，國軍有關「加密式隨身碟」已於去年 6 月 1 日起配發至全軍使用。為落實管理，國軍公發「加密式隨身碟」，各單位應確依國防部令頒之相關規定管制使用，以符合資訊安全規範，確保資訊共通作業環境及資料傳輸安全，避免人為誤失肇生洩密情事及資安風險，建立安全無虞之資料交換環境。

總之，戰爭決策優勢來自於資訊的有利條件，而其基礎則在於資訊安全防護的確保。為有效防護電腦設備與資訊媒體之管制及安全，必須制定相關作業的管制與規範。也因此，「保密」和「資安」習性的建立，已成為全民保防不可或缺的基本素養。吾人呼籲，全民要建立「資訊安全、人人有責」的正確態度與共識，才能有效瓦解來自中共網軍資訊攻擊的威脅，也才能讓資安危害因素消弭於無形，進而確保國家整體戰力，維護國家與人民的安全。（以上二則資料摘自於清流月刊）