◎公務機密維護宣導

機密外洩是導致作戰失利的關鍵，國內是否需禁止使用陸資的電信網路設備？

－大陸電信設備龍頭「華為」引爆「婉君」攻防戰－

臺灣遭受網路攻擊密度是全球之冠，且駭客多數來自大陸，統計遭竊取資訊就已累積兩萬多筆；這對我國資訊安全帶來無形的威脅，其危險程度與大陸沿岸布署的飛彈不相上下。國內學者林穎佑（聖約翰科技大學教授）認為大陸除了成立網路戰部隊（簡稱網軍或婉君），更以商業為後盾支援網路戰，被點名企業如大陸華為。美國眾議院情報委員會曾對大陸華為進行調查，認為華為與大陸軍方有密切關聯，因此提醒美國企業不要與大陸華為合作。

調查顯示大陸華為是由退役的解放軍任正非上校於 28 年前（1987 年）創辦，華為內部與大陸官方組織設有相對應的官職，也提供共軍網路戰部隊服務。華盛頓時報更報導華為於七年前接連三年（2008 年至 2011 年）接受大陸政府（2.28 億美金）70 億臺幣的資助，且內部高層多人捲入賄賂疑雲，然而該公司最早的註冊資本額僅十萬臺幣，至近年卻成為全球第一大電信設備商，營收超越易利信。華為與大陸軍方異常金援關係，加上收受賄賂人員都可能是大陸網軍部隊的成員；因此國內的國安局明文規定電信業者不得採購陸資廠商的電信網路設備，國家通訊傳播委員會（NCC）與電信業者一直以來避免採購華為設備，這顯然受限於國家安全法。直至去年郭台銘的國碁電子進軍 4G 電信並擬採用華為網路設備，進而將反情報問題搬上檯面，假若臺灣的電信網路設備真使用華為的電信設備，那也就等同在臺灣本土安插了巨型木馬作為內應。

巨型木馬的典故源自希臘大軍久攻特洛伊城不下，於是將士兵藏於巨型木馬之中，當木馬被運進城中便伺機開城門引大軍。隨著駭客技術的發展，以前木馬是種電腦應用程式，而今早已進化成電路隱藏在電腦或網路設備之中，又稱木馬電路，使駭客輕易地進入系統，電腦使用者本身是無法發現，這種攻擊方式的人被稱為硬體駭客，且早已有先例可循，如大陸聯想電腦的所作所為。

大陸聯想在十年前（2005 年）於大陸北京收購美國 IBM 個人電腦，事後經澳洲金融報導顯示，聯想電腦已被澳大利亞、美國、英國、加拿大、紐西蘭等五個國家的情報機構禁止使用。各國的實驗室測試顯示，聯想電腦設有內應，也就是木馬電路，可被他人在使用者不知情的情況下遠端操作。除此之外，英國和澳大利亞的多家情報和國防消息來源證實，存在一個書面禁令，禁止聯想電腦進入機密網路。禁令凸顯了對大陸公司生產電路中被植入木馬的擔憂，華盛頓布魯金斯學會的科技專家約翰教授表示，

半導體市場的全球化使得晶片被惡意隱藏木馬電路插入供應鏈中。這些木馬電路可在數月或數年之後才變身成內應。高科技研究公司的資訊技術安全行銷分析師特納表示，木馬電路如果精心設計將很難被監測到，它們通常被設計得看起來像一個小的製造缺陷。加上今日技術電腦晶片製程已成長到奈米科技，根據牛頓時報形容，地球的奈米分之一大小相當於一顆彈珠，因此可以試想像一片指甲大小內擁有 14 億電晶體，經搭配網路通訊之後使駭客能輕易從遠端控制。木馬電路需要高度專業化的實驗室方能測試，大多數組織、企業沒有足夠的資源來監測這種木馬電路的滲入，所以聯想電腦遭多國機密網路禁用。

硬體駭客利用硬體電路，並可能對華為電信設備的電路做竄改，以達到植入木馬電路，一旦成功就可以逃避所有防火牆、防毒軟體以及安全輔助工具的追蹤，再次強調即便是電腦使用者本人（管理員）也根本不會察覺，除非電腦硬體損壞，否則此木馬電路將是一個永久的內應衛哨，供駭客隨意出入不做任何查緝，而且任何防駭措施對它也無濟於事。

商人往往看到的是利潤，郭台銘曾說：惡魔藏於細節裡。原意是用來提醒忽略細微處可導致嚴重失敗，亦可以解釋當你想做的事，困難的部分都是在很多小細節的地方，然而就我來看卻有另一層含意在其中，木馬電路小到你我看不見。未來的反情報戰已經非檯面化，基於所有資訊都網路化和數位化，加上兩岸開放自由行，華為的可攜式設備也早已慢慢地在自由的國土－臺灣銷售，禁止使用陸資電信核心設備將是固樁反制的積極作為。法國的國防承包商報告：因安全考量避免木馬電路作內應，華為被排除在澳大利亞國家寬頻網路之外。美國中央情報局更不諱言指控，華為是大陸的間諜。

「黃石公三略」所云：將謀洩則軍無勢，外窺內則禍不制。機密外洩導致作戰失利進而敗亡，絕無亡羊補牢的機會，若不慎遭敵人滲透，取得機密資訊，對國家造成的損害將無法彌補。根據《陸海空軍刑法》第 63 條第一項意圖損害軍事利益，非法輸出、干擾、變更、刪除軍事電磁紀錄，或以他法妨害其正確性者，處一年以上七年以下有期徒刑。

（摘錄清流月刊楊俊彥）

台中榮民總醫院關心您也提醒您！