【莒光園地】確遵資安保密 杜絕機密外洩

2019 年 8 月 19 日

政治作戰局保防安全處供稿

壹、前言

根據《數位時代》雜誌報導，2018 年全球網路用戶平均每日上網時數為 6 小時 42 分鐘，相當於每人一天有四分之一的時間都在上網。在資訊快速傳遞及享受生活便利的同時，也帶來駭客攻擊、網路詐騙及假消息傳散等威脅，不僅造成社會治安危害，更威脅臺灣的民主發展與國家安全。總統蔡英文女士在今年的「臺灣資訊安全大會」上表示「資安就是國安」，也強調「資安維護是不能孤軍奮戰的」。因此如何做好資安保密、杜絕機密外洩，必須仰賴平時全體官兵確遵資安保密規定，養成良好保密習性，才能維護個人資訊及單位機密的安全。

貳、案例檢討與分析

今年漢光 35 號演習也因應現代戰爭趨勢，特別將反制中共的假訊息攻擊納入操演科目，戰時除面對中共的軍事威脅，對於中共網軍影響民眾心防、國家主權認知等假消息資訊攻擊，國軍也應相對採取必要之反制作為。面對未來戰場的資訊化，國防部長嚴德發先生在工作檢討會中，強調保密的重要性，要求所屬做好資安防護工作，以維護機密資訊安全。以下援引案例，供各級參考與省思：

一、貪圖作業方便，衍生洩密風險

近期某單位人員將一般公務資訊以手機翻拍後，再分別透由「Snapfax」、「Fax886」等 App 手機軟體，傳送至營外傳真器材，轉為實體紙本輸出。相關資訊雖非機密資訊，惟已違反「國軍營內民用通信資訊器材管理要點」，當事人須依「國軍資通安全獎懲規定」核予記大過處分；另查案述 App 手機軟體所屬公司及伺服器機房，均設置大陸地區，恐衍生資訊外流疑慮。

二、違反資安規定，洩漏演習資訊

某中校日前參與實彈射擊任務時，逕以個人智慧型手機拍攝射擊過程，並貪圖作業方便，私自以通訊軟體 LINE 傳輸相關影像，遭有心人士將影片上傳群組，致使影像在網路散布流傳，衍生廣大媒體輿論，嚴重斲喪軍譽；相關當事人均依規定予以懲處。

參、國軍官兵應有的體認與作為

國防部長嚴德發先生於今年 3 月主持國軍高階幹部保密安全講習時表示，國軍就是保衛國家安全最重要的守護者，在從事國防事務工作時，保密警覺最為重要，保密安全是我們幹部的基本功。面對中共和戰兩手策略，應秉持「毋恃敵之不來，恃吾有以待之」觀念，建立資訊安全防範機制，透過層層綿密控管，確保機密安全無虞。爰提下列認知與作為供參：

一、正視網路威脅，建立防護觀念

美國前司法部長埃里克·霍爾德（Eric Holder）曾表示：「中共網軍坐在電腦前，就能竊取維吉尼亞一家軟體公司的程式碼；國防承包商員工只要敲幾下鍵盤，便能盜取價值數十億美元的設計或程式。」面對中共網軍的滲透蒐情手段，國軍官兵應了解敵情威脅與敵諜手法，並依據「國軍保密工作教則」等規範，落實檢管作為。

二、具備資安警覺，養成保密習性

臺灣商業管理協會於 2018 年時研究商業機密持有者洩密案例中發現，其中 39%的工作者，都曾將客戶商業機密資料，在未採取任何防護的情況下寄出；52%的員工在離職時，都曾將工作內的資料帶走；86%的員工習慣將不明來源的郵件，再轉寄他人；26%的員工在工作任內，從來不曾更改過信箱密碼。上述說明，資安事件通常都來自於內部人員缺乏良好的保密習性所造成。因此，全體官兵都應引以為鑑，落實個人保密工作，才能確保單位機密安全。

三、慎選資訊產品，妥善操作運用

日前美國政府要求美軍禁用「中國大陸製造」的資訊設備，並透過公開聲明，表示陸製資訊設備，可能帶來資訊外洩風險。我國國家通訊傳播委員會在年初時審議通過國安條款，規定電信業者未來將不得再購買大陸製的設備。而國軍也已禁止營內使用及攜帶大陸品牌手機。因此我們在享用資訊帶來的便利同時，一定要慎選安全的通訊器材，並遵守資安規範，才能防範未知的風險。

肆、結語

國軍係維護國家安全的第一道防線，尤其面對中共網軍無孔不入的網路攻擊及竊密蒐情，全體官兵在營內應貫徹網路實體隔離的觀念及落實個人保密作為；幹部則依資訊安全檢管要項，加強保密檢查強度及密度，防範洩密違規情事。然而保密工作的成敗，取決於全體官兵對保密工作的重視程度，大家都應發揮保防警覺及危安預警功能，遇可疑立即回報反映，防杜敵人滲透蒐情，建立堅固的安全防線，方能確保國家安全無虞。