莫讓網路成為洩密的公路

◎陳韋志

近期紐約時報大篇幅報導，美國網路安全公司 Mandiant 的最新研究指出，近年對美國公司、機構和政府單位大規模的網路攻擊行動，極可能源自中共位於上海的 61398 部隊。消息傳出後，中共方面當然拒不承認，並公開表示自己才是網路駭客活動中最大的受害者，其反應雖早在各國意料之內，但也對中共的圖謀有更深一層的認識。網路攻擊每次造成的損害皆視種類及規模而定，較嚴重時往往不下於一次傳統戰爭失利所帶來的損失，這鍵盤上廝殺的代價甚至非金錢所能衡量。在中共官方的扶植下，軍方與民間的駭客活動日益頻繁，且越發老練兇狠，並擅長以惡意程式或破解安全機制等方式，針對他國企業、科技、軍事、政治與經濟等重要資訊進行破壞或竊取，中共駭客甚至常利用臺灣及其他國家的伺服器作為中繼站執行所謂的「跳島戰術」，使受害者難以追蹤來源。所謂道高一尺、魔高一丈，即令美國作為網路的先驅亦是防不勝防，數十億美元及長期的研發結晶瞬間為他人所用，國際間亦合理懷疑中共近年來各項科技的突飛猛進多半是源於此道。

由於損害非同小可，美國政府除積極進行各項防堵作為外，更針對駭客入侵時所留下的網路足跡進行追查，如登入時慣用的英文拼音方式、獨特的簡體輸入法，以及駭客個人使用的社群網站 Facebook 和 Twitter 等，才得以反推追查真正的元兇就是中共。我們亦可以藉此了解一件事，亦即精明如駭客都因忽略資訊安全而洩漏行蹤，可見我們平日在使用網路時又豈能不謹慎小心，尤其在資訊媒體裝置不斷微型化、普及化及功能多元化的今天，各種資訊傳遞快速且便捷，在 Facebook 等社群網站或部落格內公開暢談生活瑣事已是現代人的家常便飯，但往往就在談天說地中洩密而不自覺。例如最近就有網路部落客貼出一則文章，內容係針對國軍飛彈指揮車偽裝成物流車輛的創意及技巧表示稱讚，接著更有其他網友回文，聲稱在何地、何時看過此等裝備，甚至有人連單位全銜也一併寫上。這些軍事迷看似交換心得的文章，無疑幫敵人情蒐單位一個大忙，有心者只要付網路費用再敲敲鍵盤就可以蒐集到我方的軍事部署與動態。然而，洩漏的軍情卻

會對國家造成難以估算的傷害。在平時，部隊就必須要另行調整部署或計畫，額外花費大量的人力物力來彌補；在戰時，國軍可能就要付出十倍百倍的代價及犧牲，卻因為那無知的隻字片語。

近幾年在馬總統的領導下，兩岸情勢雖趨於和緩，有部分國人亦因此鬆懈應有的保密警覺，其實只要多留心相關訊息，就會發現中共的各種情蒐與滲透仍是暗潮洶湧，不曾停歇；其中又屬網路攻擊最難防範。因此，凡我國民均需培養一個觀念，在網路上留下的各種訊息無遠弗屆，在電腦中存放的公務資料，只要連上網際網路，駭客就可以利用各種意想不到的方式對其進行存取，再藉由各種零碎的資訊，拼湊出「點」、「線」乃至於「面」的情報全貌；例如最近某大陸網民就利用 Google 衛星空照圖，標定了大量的臺灣防空部署位置並於網路發表，這些名稱與訊息都是藉由各種來源的資訊組合而成，姑且不論其可信度有多少，僅是圖上密密麻麻的陣地與裝備名稱已夠令人怵目驚心。希望能國人對於國防秘密能深切重視，明白「保密是國家安全的基礎」，切勿為了自己的一時大意而為國家帶來難以估計的危害，尤其國軍弟兄身為表率，更應恪遵「不公務家辦」與「不記述軍中事務於網路及個人電腦」等重要原則，牢記保密是國家的根本，唯有「樹根站得穩、才不怕樹梢颳颱風」。