指定題

DOI:10.6237/NPJ.202004_54(2).0004

淺談科技與網路安全防護趨勢發展

海軍士官長　蔡在昇

提　　要：

一、隨著網路的攻擊日新月異及當前新興科技演變而引起的風險，企業和組織針對資訊安全勢必將面臨更廣泛與多元的挑戰，不僅對於資訊安全團隊的需求將提高，多層式防護的資安政策也在企業經營及軍隊組織中扮演關鍵的角色。

二、近年來網路快速蓬勃發展，迅速且複雜的特性讓企業面臨嚴峻的網路威脅挑戰，網路罪犯能針對特定的組織、產業和客戶進行網路攻擊，我們應瞭解未來的網路威脅(如竊取個資、加重網路釣魚攻擊手段和物聯網風險(裝置漏洞攻擊及工業網路被駭風險提升)，及早加以應對。

三、隨著科技進步與發展，網路已成為關鍵的生活場域，就軍事作戰而言，網路作戰對於軍事嚇阻、戰力投射及戰略威脅，具有相當程度的影響力，顯示國軍資安防護措施工作確實不容懈怠，也唯有不斷精進資安防護工作，蓄積國軍「不對稱」網路作戰能力，才能確實阻斷中共網軍對我國不斷的網路攻擊，共同創造「勝兵先勝」之作戰契機。

關鍵詞：網路威脅、資安防護、物聯網風險、工業控制系統風險

壹、前言

隨著網路犯罪日新月異的全球攻擊態勢及當前新興科技的演變而引起的網路風險，著名資安防護業者「趨勢科技」(Trend Micro Inc.)2019年發布資安預測報告〈Trend Micro Security Predictions For 2019〉中，即針對新興科技、威脅情勢與使用者行為做分析[1]，而報告中更提出警示，他們預測對網路個人帳號密碼攻擊、網路釣魚案例與商業電子郵件詐騙會變得更多；此外還有企業員工在家辦公衍生的資安風險議題，以及工業控制系統(Industrial Control System，簡稱ICS)的攻擊入侵威脅提高，都將是未來應當注重的網路防護趨勢。

而鑑於在過去民間組織及企業不斷發生資安事件，尤以去年著名的「台積電」因遭病毒感染導致產線停擺，病毒從一部機臺蔓

註1：趨勢科技，〈2019年資安年度預測報告〉，https://documents.trendmicro.com/assets/rp，2018年12月19日，檢索日期：2020年1月5日。

延到全臺的台積電晶圓廠，造成新臺幣52億元損失[2]。此重大資訊安全事件的發生，凸顯企業公司對連網裝置普及，所面臨的資安問題應予重視；而駭客也將攻擊轉向工業自動化控制系統為代表的相關操作技術系統，藉由駭入系統將可蒐集如廠房設備配置圖、企業技術關鍵門檻值(Critical Thresholds)以及裝置設定等資料，進而從事後續攻擊，並從中獲取商業利益。面對科技時代發展的趨勢，企業和組織針對資訊安全勢必將面臨更廣泛與多元的挑戰。

綜上所述，不僅企業對於資訊安全團隊的需求將提高，多層式防護的資安政策，也將在企業經營及軍隊組織中扮演關鍵的角色，唯有順應科技情勢，提早掌握網路安全防護趨勢、不斷精進資安防護工作，才能有效建構防護能量，這也是撰文主要目的。

貳、網路威脅趨勢與特性

近年來網路快速蓬勃發展，迅速且複雜的特性讓企業面臨嚴峻的網路威脅挑戰，網路罪犯能針對特定的組織、產業和客戶進行網路攻擊。時至今日，資安攻防已是「不對稱戰力」之競爭，單一企業愈來愈難以對抗有組織、且專業分工的駭客集團。面對威脅來自於世界各地，企業應意識到若要面對全新的威脅，需要有強大威脅情資(Cyber Threat Intelligence)蒐集能力，企業決策者可利用網路威脅情資，做出符合目前外部威脅趨勢及最正確的資安決策指示；另外，產業間的威脅資訊分享機制，也能有效提供早期資安預警情資，至於聯防與資安防護改善的良性循環，降低資安事件發生衝擊，以及企業營運可能被迫中斷之風險。

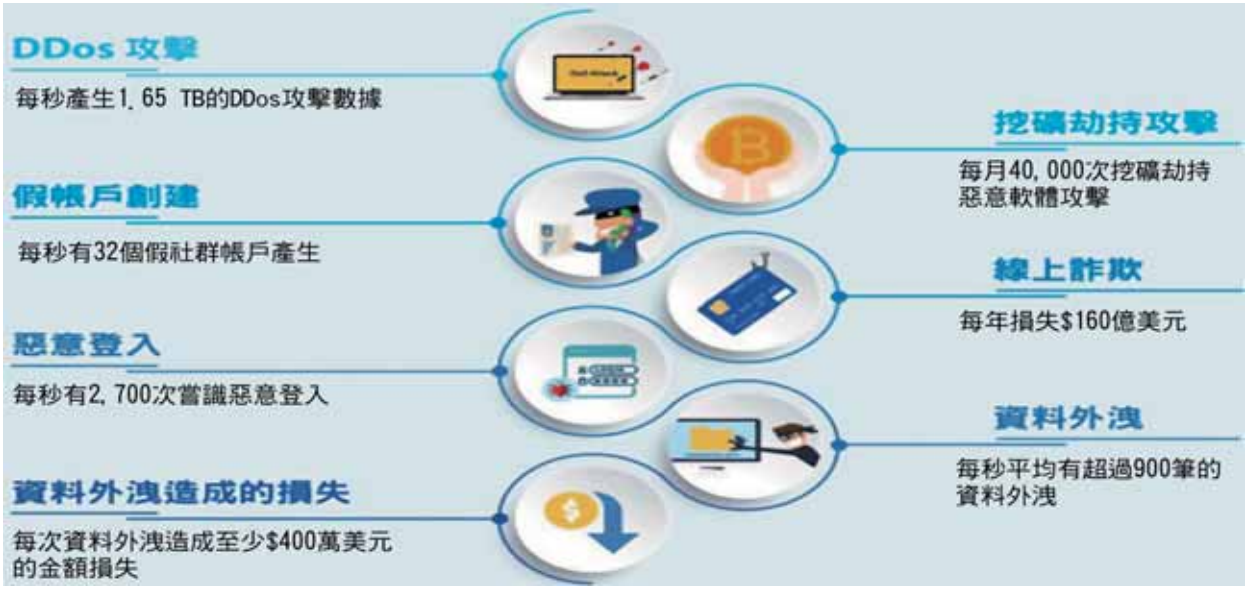
因應科技日新月異，「連網裝置普及」肯定會是未來趨勢，企業和組織為了產能效率，也將持續導入更多連網設備。從國際著名資安廠商「星盾科技」(Force Sheld)公布全球2018年網路威脅受害相關數據來看[3]，2018年全球網路每秒產生1.65兆位元組(Terabyte，縮寫為TB)大小的分散式阻斷服務攻擊(Distributed Denial-of-Service attack，簡稱DDos)攻擊[4]、創立32個假社群帳戶、2,700次嘗試破解帳戶惡意登入，而每次資料外洩造成至少400萬美元(約新臺幣1兆2,000萬元)的損失、每月有4萬次以上的挖礦劫持(Cryptojacking)[5]惡意軟體攻擊、線上詐欺每年損失160億美元、每秒平均超過900筆資料外洩(相關數據，如圖一)，顯見資訊安全已面臨更廣泛與多元的挑戰；另「趨勢科技」所發表《2019年資安年度預測報告》(Trend Micro Security Predic-

註2：王宏仁，〈台積電產線中毒大當機事件簿〉，iThome，2018年8月10日，https://www.ithome.com.tw/news/125118，檢索日期：2020年1月5日。

註3：〈2018 資安威脅報告〉，「星盾科技」(Force Sheld)，2018年12月4日，https://www.forceshield.com/papersreports/，檢索日期：2020年1月5日。

註4：分散式阻斷服務攻擊(Distributed Denial-of-Service attack，簡稱DDos)：DDos係指一種網路攻擊手法，目的在於使目標電腦網路或系統服務資源耗盡，導致服務中斷或停止，參照維基百科，檢索日期：2020年1月6日。

註5：挖礦劫持(Cryptojacking)：挖礦劫持是一種惡意行為，利用受感染的設備來計算挖掘加密貨幣。〈分類：Cryptojacking(挖礦劫持)〉，資安趨勢部落格，2018年6月25日，https://blog.trendmicro.com.tw/?cat=3602，檢索日期：2020年1月6日。



圖一：星盾科技公布全球2018年網路威脅受害相關數據

資料來源：〈2018 資安威脅報告〉，「星盾科技」(Force Sheld)，2018年12月4日，https://www.forceshield.com/papersreports/，檢索日期：2020年2月5日。

tions For 2019)[6]中，說明未來的網路威脅已朝向消費者、企業、政府機關、資安產業、工業控制系統、雲端基礎架構與智慧家庭等七大領域延伸，並聚焦在企業、消費者與工業控制系統，有關威脅說明如後：

一、鎖定機密個資竊取

(一)企業部分

近幾年資料外洩事件頻傳，從國際著名資安廠商「星盾科技」(Force Sheld)公布全球網路威脅受害相關數據[7]來看，截至2019年8月全球外洩個資已高達24億筆，而且前3大攻擊所洩露的資料數量，都在1億筆以上，比起過往都要來得多。許多遭竊事件的資料數量都非常龐大，而且觀察這種現象，發現駭客已轉移重點，著重在奪取企業重要機密資料，從中獲得有效利益最大化，且這個趨勢將會越見明顯。例如「萬豪國際集團」(Marriott International)旗下的子集團「喜達屋」酒店(Starwood Hotels)，2018下半年就驚傳5億筆房客資料被駭[8]，僅次於2013年「雅虎」(Yahoo)網路服務公司30億筆網路帳號資料外洩規模[9]，而這些遭駭事件，除了使企業界業務營運受到波及與商譽受損，甚至可能遭以獲利為目的之網路犯罪者竊取客戶個資，勒索高額贖金，賠上的不止是金錢，還有企業形象。

註6：同註1，頁1。

註7：同註3，頁6。

註8：張佑生，〈萬豪酒店集團宣布 5億房客個資遭駭〉，聯合新聞網，2018年11月30日，https://udn.com/news/story/6813/3511559，檢索日期：2020年1月5日。

註9：陳曉莉，〈糗大了！Yahoo的30億用戶資料全都外洩了〉，iThome，2017年10月4日，https://www.ithome.com.tw/news/117253，檢索日期：2020年1月5日。

(二)個人部分

面對消費者個人的攻擊方面，駭客抓住大眾對重大活動的好奇心，例如透過2020年我國總統大選的時事議題，來進行社交工程詐騙之外，更看上了網路紅人的傳播能力。駭客鎖定「網紅」的社群帳號，並嘗試入侵取得控制權，讓網紅帳號成為駭客進行網路攻擊的工具，利用植入惡意程式的連結或是訊息，騙取追踪粉絲點閱，使得粉絲遭牽連受駭，造成個人資料與財物損失。並且將各種網路釣魚的手法，轉移至手機簡訊以及通訊軟體APP訊息上，發展出結合社交工程手法的新興網路攻擊，例如SIM卡(電話號碼智慧卡)劫持手法(SIM-jacking)，犯罪者先取得個人電話號碼和資訊，再假冒手機用戶，向電信廠商技術服務人員申辦新的SIM卡(電話號碼智慧卡)，爾後透過簡訊存取用戶的帳號資料，甚至盜用電子錢包等等。觀察這種現象，發現駭客對社交工程更用心、更客製化，造成當事人失去戒心而遭竊。

二、加重網路釣魚攻擊手段

網路釣魚通常是指企圖透過電子郵件、通訊軟體來獲得個人資訊，或竊取你的身分認證，大多數網路釣魚會企圖讓自己看起來像是一般行為，實際上卻是用於犯罪活動。在現今多元裝置以及操作系統趨勢下，駭客將不再像以往採取單一軟體系統層面的漏洞攻擊套件模式，而是利用網路社交工程，廣布式地進行網路釣魚攻擊，或是歹徒假冒信譽良好的個人或企業機構，誘騙受害者提供個人敏感資訊等詐騙手法。以2018年統計資料為例，「趨勢科技」已阻擋超過2億多筆網路釣魚相關的網路連結，相較於2017年成長接近3倍，預期2020年會再創高點[10]。而有別於以往偽造企業往來信件格式的手法，駭客透過竊取員工社群網路上的資訊，提高網路釣魚詐騙信件的可信度，同樣達到入侵企業的目的，不可不防。

此外，近年相當猖獗的變臉詐騙攻擊或稱為商務電子郵件入侵(Business Email Compromise，BEC)，依然是歹徒向企業詐財非常強大且獲利豐厚的犯罪手法。駭客會建立類似目標公司的網域或偽造的電子郵件，來誘騙目標提供帳號資料。在監控受駭電子郵件帳號時，攻擊者又會試著找出進行轉帳及要求轉帳的對象。這些駭客通常會進行相當的研究，尋找財務高階主管變動的公司、高階主管正在旅行的公司，或是進行投資人電話會議，來製造機會進行騙局。不用懷疑，2018年BEC型式詐騙已經造成美國受害者將近7.5億美元(約新臺幣224.5億元)的損失，影響超過7,000人。

隨著時代的演進，駭客們的社交工程(Social Engineering)技巧越來越細膩，網路釣魚電子郵件已轉向假冒寄件人或加強隱藏惡意附檔，所以更應對各網路郵件小心謹慎；另外在科技發展下，現代有多樣化可連網裝置及系統，駭客將不再透過以往單一軟體系統層面的漏洞攻擊模式，轉而利用社交工程廣布式地進行網路釣魚攻擊。根據網路釣魚的威脅態勢統計，網路釣魚相關網址數量，不僅是逐年急速攀升，並從2018年的2

註10：同註1，頁18。

億1,000萬到了2019年9月的4億9,000萬，已成長2倍多，未來勢必持續攀高。

三、物聯網(Internet of Things，IoT)裝置漏洞攻擊

物聯網的概念相當簡單，期望透由廣域網路(Wan)或區域網路(Lan)將可連結網路設備串連在一起，但隨著各種設備資料上傳雲端管理控制的需求提升，市面上的物聯網設備也出現了爆炸性的成長。其中，透過不同設備所蒐集到的數據，都將進一步傳輸到後端分析，在此過程之中便出現許多資安弱點；例如針對路由器、網路監視器、印表機等，需要仰賴網路連線運作的物聯網設備。近年來的攻擊事件層出不窮，根據「卡巴斯基」(Kaspersky)防毒企業公布的資安分析報告，他們從物聯網裝置裡發現的惡意軟體共12萬1,500多種，比起前一年的3萬2,614種要多出將近3倍[11]。因此，即便是小至物聯網插座開關，也不能掉以輕心。又例如「邁克菲」(McAfee)防毒企業於8月時，揭露「貝爾金」(Belkin)全球電腦硬體生產商生產的其中一款智慧插座，就含有可遭受駭客攻擊的遠端程式漏洞，並表示這款插座一旦連接了家裡的無線網路，就能讓駭客對其他連線的裝置執行致命性的攻擊行為[12]。

相較於消費性物聯網，企業界的物聯網遭遇駭客攻擊的案例雖然相對少，但倘若產業物聯網安全失守，帶來的直接經濟損失卻是非常驚人的。例如2018年8月台積電爆出機台感染電腦病毒，造成產線機台停擺，製成品大量報廢，造成經濟損失超過新臺幣50億元[13]；另第一銀行自動提款機系統則因為被植入惡意程式，在2016年7月爆發盜領案，損失也超過新臺幣8,300萬，所幸後來大部分贓款成功追回[14]。對產業物聯網應用來說，資安政策跟標準作業流程固然是守護物聯網安全的重要關卡，但企業資安事件頻傳，也顯示光靠企業內部的資安政策跟標準作業程序(Standard Operating Procedures，簡稱SOP)是不夠的。科技產業必須設法用科技來解決人為因素問題。

目前物聯網設備常見的入侵方式分為：硬體入侵、韌體逆向工程以及應用介面入侵。其中，儘管透過硬體入侵的方式相對較為困難，但是在硬體開發過程中，多半會留下連線管道，以供後續工程人員除錯與監控之用，也勢必會留下安全漏洞。因此，為了提升物聯網應用的安全性，從最根本的晶片元件設計開始，到後續的硬體系統設計、韌體(Firmware)開發、應用軟體開發、通訊介面乃至系統上線後的日常維運，都必須做到滴水不漏。上述各環節之中，只要有一個環節存在漏洞，就會給駭客單點突破的機會。

四、工業網路被駭風險提升

註11：安全內參，〈卡巴斯基：中國大陸已成物聯網攻擊的最大來源地〉，2019年10月17日，https://www.secrss.com/articles/14382，檢索日期：2020年1月6日。

註12：陳曉莉，〈McAfee：Belkin智慧插頭含有遠端程式攻擊漏洞〉，iThome，2018年8月22日，https://www.ithome.com.tw/news/125413，檢索日期：2020年1月27日。

註13：王宏仁，〈台積電產線中毒大當機事件簿〉，iThome，2018年8月10日，https://www.ithome.com.tw/news/125118，檢索日期：2020年1月5日。

註14：黃彥棻，〈駭客入侵一銀ATM流程追追追〉，iThome，2016年7月25日，https://www.ithome.com.tw/news/107294，檢索日期：2020年1月6日。

現今企業營運比以往更需資訊數據即時運算，也因此工業控制系統網路必須與企業資訊網路連結，隨著物聯網、智慧製造概念的崛起，企業界推廣製造自動化，提高營運效率。無論是軟硬體的虛實整合，或機台與機台之間的相互串連，「智慧化」整合都已成為新世代工業自動化系統的必要機制。不過，既然工業自動化與智慧化引入資訊與通訊科技，資安威脅自然也隨之而來。工業生產設施、物聯網、以及關鍵的產業基礎設施，成為駭客新一波鎖定攻擊的目標。駭客會將不安全的企業資訊網路設備當成跳板，再移轉到最容易攻擊的工業控制系統設備和資料庫，造成交通網絡停擺，能源供應中斷，甚至影響人身安全。

根據「趨勢科技」公司(Trrnd Micro Inc.)的報告《Trend Micro Security Predictions For 2019》指出，目前案例顯示，關於工業控制系統中監控與資料擷取系統(Supervisory Control and Data Acquisition，SCADA)的漏洞，大部分出現在協助顯示資料與接受操作人員指令的人機介面(Human-Machine Interface，HMI)[15]，駭客對現代SCADA系統攻擊的途徑，首先可透過人工，或是讓SCADA控制主機感染病毒，去植入未經授權的控制程式，並且對該設備所在網段的通訊封包下手，因為SCADA使用的控制協議不具備加密機制，這可以讓攻擊者透過發送命令，以控制該設備並取得相關資料，例如：廠房的設備配置圖、企業技術關鍵門檻值以及裝置設定等資料，進而從事後續攻擊，除了可能造成相關營運中斷，更甚者可能利用製程中的易燃物質或是重要資產，以威脅生命和財產安全。

目前企業為了提升效率，努力朝向資訊自動化，隨著企業將越來越多生產工作透過軟體或線上應用程式來達成，若未在一開始就做好防範措施，歹徒將有更多機會可以駭入流程。自動化軟體很可能本身就含有漏洞，而且在與現有系統整合時，也可能形成資安缺口；不僅如此，甚至有心人士會試圖尋找企業的供應商、合作夥伴或外包廠商的弱點，從內部漏洞進行試探並攻擊來達成其目的，因此自動化已為其供應鏈帶來資安風險。我們應當應思考如何從源頭的產品設計、中間的生產環境、到後期產品實際應用情境，都將安全防禦思維融入其中，同時為攻擊造成損害之後，應採取的事件預作應變準備，才能從工業體系全局考慮整體的安全策略，並將可能發生的威脅損失降至最低。

綜合而言，顯示網路駭客攻擊對象聚焦於消費者、企業與工業控制系統，而國軍現行政策雖已將軍用網路與外部網路實體隔離，但仍可能透過有心人士從內部進行個資竊取及網路釣魚攻擊；而物聯網的普及也已是國軍推動資訊化的趨勢，物聯網所能肇生的風險不會因裝置置於軍中而有所消弭，例如監視器、網路印表機及網路交換器等，都可能因疏於檢查、或未關閉相關網路漏洞，導致資訊資料外洩。因此，我們更應瞭解當前網路攻擊趨勢，掌握防護先機，方可有效避免類案肇生。

註15：同註1，頁34。

參、資安防護作法與建議

資安防護是一個從實體文書時代及環境，一直到當前行動化、虛擬化與雲端化時代一直存在且不斷演繹更新的重大議題。隨著大環境的改變，加上各種推陳出新技術的推波助瀾，使得資訊安全不論「攻」與「防」都出現了極大的變動。其中「個人資料保護法」的全面實施更刺激了全新資安意識、資安策略、資安投資與資安產業的發展，也由於個資法加諸了各企業應對用戶資料保密的規範，讓企業在因應資料外洩上在觀念、作法及政策方面也有所改變，並注重最新資料外洩防護技術與方案在實際部署與成效上的狀況。

資料外洩對企業而言，是個從未消失的重大威脅；不僅如此，過去舊有的外洩手法與管道不僅不會消失，全新攻擊方式、來源及管道卻不斷推陳出新。再加上行動化與雲端運算的興起，不但讓攻擊端的管道變多，更使得擁有合法權限的組織內賊，獲得更多可趁之機。我們從前述所提到的網路威脅趨勢中，可以發現資料外洩防護機制，已不可侷限在靠著過去「主外」的防護策略，更不能限縮在靠著架設單一資安防護設備，即可完善資安防護的概念，而應朝向協同防禦及內外兼具的方向發展。為了因應今後來自內、外部的資料攻擊威脅，行政院「國家資通安全會報」技術服務中心並已公布《關鍵資訊基礎設施資安防護建議》[16]，重點內容摘要臚列，概述如后：

一、消弭漏洞風險，落實資安稽核

當前民間企業的外洩管道非常多元，除了實體隨身碟及外接式硬碟外，從傳統的電子郵件、即時通訊、網站，再到Line、行動App、雲端儲存與各類型手持裝置全都是資料外洩的可能管道。企業應該就自身環境與員工需求，來評估這些管道的風險程度，並在預算允許的狀況下，給予不同層級的安全控管及防護；此外，企業也必須加強員工所用隨身碟、網路及郵件等常見外洩管道的安全控管機制。另一方面，因應駭客與內賊的不斷覬覦，企業應具備郵件與Web雙向進出管道內容的檢測機制，才能杜絕竊賊等有心人士的任何不軌之舉。

國軍雖在資安管控政策上推行許多與時俱進的作法，並就任何可能外洩管道建立嚴密管控機制，例如資訊資料交換須逐級申請，並嚴格落實檢疫政策、資訊資產清點作為，及透過資安防護軟體24小時監控電腦，以防杜任何資料外洩。近幾年更推行國軍各營區專用的網路管理系統，以強化各單位對網路設備的監控管理，對降低各種管道外洩風險已見成效。然鑑於網路設備必須持續汰舊換新，及因應民用通信器材開放程度加大，因此必須持恆推動資安稽核政策，方能落實管控資安風險。唯有訂定完善的稽核政策，並且依週期落實執行；並透過相關業務承辦人及資訊人員有效管控及持恆推動，方可消弭資安管控疏漏等風險。

二、區分防護等級，嚴管人員權限

由於資料外洩防護的面向太廣，即使預

註16：《資訊基礎設施資安防護建議》，行政院國家資通安全會報技術服務中心，2019年1月30日，頁2-36。

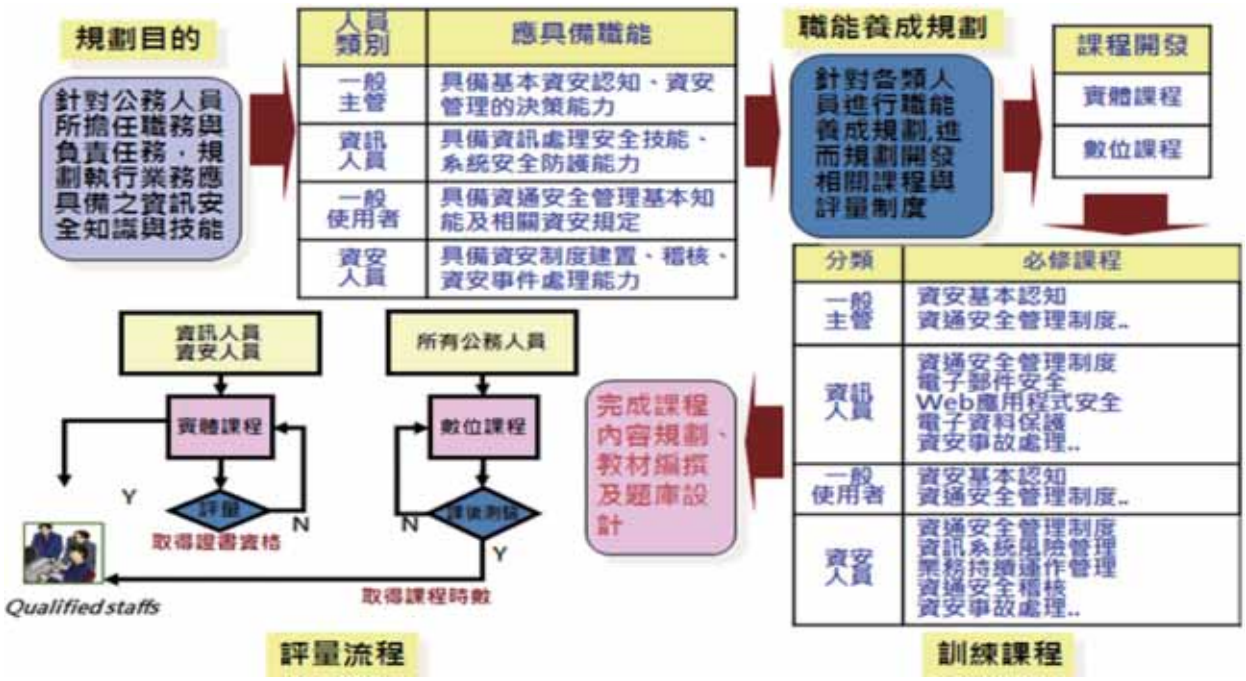
圖二：我國「資通安全管理法」規範對象、方法及目標示意圖

資料來源：〈108年5月份資訊安全宣導〉，行政院資通安全處，2019年5月2日，https://reurl.cc/72ajxd，檢索日期：2020年1月25日。

算再充足，硬體再強大，但畢竟牽扯到人員管理，難以做到百分之百的完善部署，更何況經費有限，自然必須先就自身的狀況與需求，將有限資源優先放在最急迫的安全防護點上，然後再循序漸近地進行其他防護面向的加強工作，以逐步完善整體資安防護的能力。因此，能收容多端點的閘道口便會是預算投資優先的目標，針對資料防護方案的部署策略，可先從各閘道端的防護開始部署，先行規劃具完善防護機制的「網路拓撲」[17]，再採購具認證合格的網路防護設備，當防護成效逐漸顯現同時，資安人員已具相關設備操作能量及防護知識，便可以逐步擴大到下游端點資料防護外洩方案的導入，並以「母雞帶小雞」方式，逐步將相關知識實施擴訓教學，使各層級一般使用者都能奠定良好的資料安全與隱私權意識後，即可漸次提升組織內的資安防護能量。

再者，針對所有資訊資料必須就人員管理、權限管理與資料外洩防護等議題通盤檢討，並訂定人員操作權限政策，針對機敏資料的管理，可以透過權限管理，在既有的流程面上得到更縝密的控管，例如對於被保護的機敏資料存取，必須提供嚴謹的管控流程，有效管理資訊資料，強化被保護資料的存取管理。資料標示分類可以提供資安人員清楚定義不同資料的安全等級，以提供相對應的存取管理機制，接著運用角色、欄位/列、以及時間存取的控制方式，結合內部稽核管理方式，確保被保護資料不會被任何非法

註17：「網路拓撲」係指網路節點(node)實際的或邏輯的連接形式。〈網路拓撲〉，維基百科， https://zh.m.wikipedia.org/wiki/網路拓撲，檢索日期：2020年1月6日。



圖三：現行政府推廣公務人員資安職能規劃藍圖

資料來源：〈資安職能規劃〉，行政院國家資通安全會報技術服務中心，2019年4月30日，https://www.nccst.nat.gov.tw/Capacity?lang=zh，檢索日期：2020年1月5日。

的管道取得。為了要達到「最少的資訊揭露原則」，就要一一審視每個人的工作需求為何？之後，又要再對應到可能會有什麼樣的存取權限；而在組織經常變動的環境中，可能就得定期審視個人業務職掌即時修訂，才能確保人員權限都能適得其所。我國目前所頒布〈資通安全管理法〉[18]就已明訂規範對象、方法及目標(相關示意，如圖二)，俾使公務機關及非公務機關可明瞭自身義務，並依方法及目標，執行相關資安政策。

三、擬定完善政策，重視人才培訓

面對資訊網路的各種威脅宛如作戰一般，部隊光有精良的武器，卻沒有整體戰略與中心思想是無法打贏戰爭的。所以，除了導入良好的資料外洩防護方案外，更重要的，莫過於防護政策的擬定、宣導，培訓與稽核；否則各種作為將亂無章法、流於形式，無法達到功效。「ISO 27001 ISMS」是當前國際推行的資訊安全管理系統認證，要求審視組織內部資訊技術、安全技術、資訊安全管理系統三者，透過控制方法導入完善流程，把資訊風險降低到可接受的程度內。因此，現行各資安政策或流程均必須參酌「ISO 27001」，以「風險已受到有效控制」之原則，達成「資訊安全」的目標；此外，現行政院所頒布的〈資通安全管理法〉，將資安

註18：《資通安全管理法》，行政院網站，2018年6月6日，https://nicst.ey.gov.tw/file/5E759C566290EA66?A=C，檢索日期：2020年1月6日。

防護提高為法令之位階，將公務機關及非公務機關一併納管，以要求一致化、標準化之規範，更凸顯資安防護的急迫性。

此外，資訊人員便是組織內部對網路威脅的第一道防線，資安工作本身有一個特質，由於威脅不斷在改變，因此資安人員必須隨時充實專業知識，以因應這些新的威脅，現行政府所頒布的〈資通安全管理法〉內已明確規範公務人員資安職能規劃(規劃藍圖，如圖三)及納管公家機關需有資安專職人員的人數配置，並對公務人員之資安作業區分為4類人員，並提供線上資安職能訓練，以防杜資安事件。由此可見，唯有針對資安人才妥善職涯規劃，依專才進行培訓，並力推人員考取相關領域國際認證資安認證，才能有效強化組織資安能量；另在人員資訊專長能量建立之後，除了可依組織特性提出適切建議供主官(管)參考，並且依人員區分授予專業知識，將資安能量普及化。唯有強大的資安專業，才可有效落實相關資安稽核及防護流程，強化組織資安防護能量。

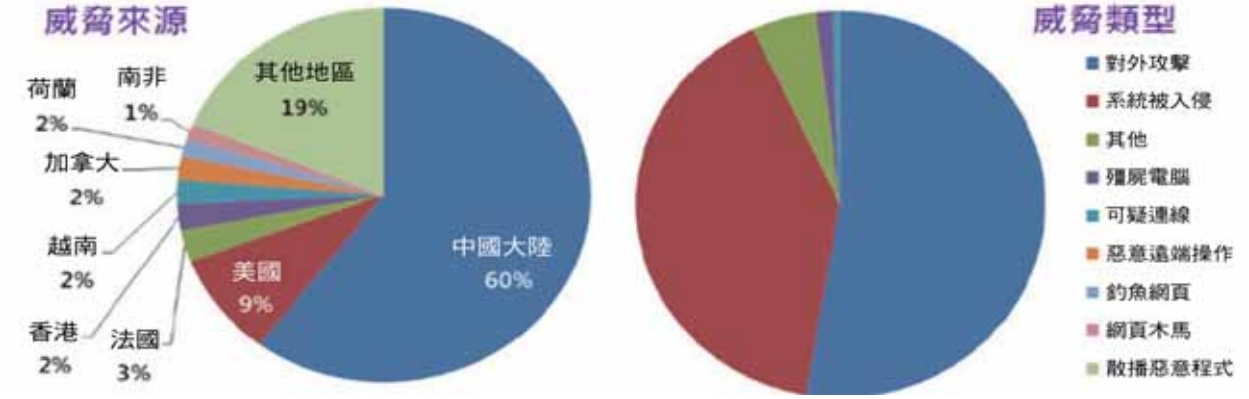
四、掌握威脅情資，健全資安架構

古語有云「知己知彼，百戰不殆」。於瞬息萬變的戰局中，如何事先瞭解自己，也瞭解敵人，才能做出最好的判斷達成任務。網路威脅情資即是指一種以情資為主導的對抗策略，如有效運用的話，可協助組織瞭解網路犯罪者入侵所使用之戰術、策略及程序。政府在2018年成立「國家資安資訊分享與分析中心」，透過情資格式標準化與系統自動化之分享機制，建立縱向與橫向跨領域之資安威脅與訊息交流；而組織則應善用相關情資來源管道，藉由即時迅速的預警機制，將所發生的資安事件，藉由標準化的通報訊息，快速地傳遞給主管機關，不僅可以防止事件擴散，更能經由即時地通報，讓其他相關人員可以有警覺，並能進行即時防禦。

網路攻擊日新月異，近幾年進階持續性滲透攻擊(Advanced Persistent Threat，APT)的出現，在資料外洩上的影響程度與破壞力更大；APT就是網路攻擊者特定組織先行蒐集情資，分析入侵手段，進而執行複雜且多方位的網路攻擊，此時完善的資安防護架構，也充分凸顯存在的價值，而如何自檢資安架構，可參酌國際標準架構做自我審視，例如美國國家標準與技術研究所(NIST)訂定的「資安框架」(Cybersecurity Framework，CSF)就明確條列出了資安組織架構，盤點組織的資安現況，找出需要優先著手改善的架構面向，評估現有能量，規劃相關資安防護架構，如此才能在不斷循環性地調整資安政策與管控措施下，達到完整有效的資安防護目標。

肆、國軍因應網路威脅的省思與建議

現今科技發展迅速，世人依賴電腦與網路執行各項工作日深；但伴隨而來的網路威脅及資安問題，長期以來亦困擾著各國政府、企業及人民。而現在的「網路戰」更可達到兵不血刃地破壞對方的指管通資中樞，達到「不戰而屈人之兵」的效果。依「臺灣電腦網路危機處理暨協調中心」(TWCERT/CC)公布〈2019年網路威脅來源及威脅類型〉，



圖四：我國2019年網路威脅來源及威脅類型

資料來源：周峻佑，〈TWNIC首度發表臺灣網路資安態勢分析，對外攻擊是頭號威脅〉，iThome，2019年3月8日，https://www.ithome.com.tw/news/129208，檢索日期：2020年2月17日。。

發現我國目前每月平均面對3億次的駭客掃描(攻擊前的探勘)、3,000萬次攻擊；其中六成攻擊來自於中國大陸[19](數據圖，如圖四)，這也顯示國軍對日新月異的網路威脅確實不容懈怠，因此重視資安防護工作，將資訊安全視為國軍達成作戰任務及遂行資訊作戰的重要作為，才能確實確保組織及國家的安全。以下就國軍「網路作戰」部分，除參考我國《108年國防報告書》所列內容外[20]，並提出個人相關建議，分述如後：

一、未來發展運用及省思

國軍「資訊戰」發展運用的三大戰略目標，其一、打造國家資安機制，確保數位國家安全，其二、建立國家資安體系，加速數位經濟發展，其三、推動國防資安自主研發，提升產業成長[21]，並應以「網路攻防為核心」、「通訊安全為基礎」、「電磁發展為前瞻」做為三大主要任務[22]。前兩個任務目標為建立有效資安防護體系，以確保政府體制的安全運行，並促使日漸數位化的民間經濟活動順利開展，而第三個任務目標則著重在我國自主資安技術能量的培養，以增強國防實力，並促進資安產業的建立。由於，資訊安全已成為現代資通訊系統應用不可或缺的要素；且就整體國家戰略而言「資安即國安」。簡言之，其具有兩層意涵，在消極面，我國民間與政府組織都必須建置精實完整、與時俱進的資安防衛機制，以有效抵擋平時和戰時的外部網路攻擊；至於在積極面上，因未來戰爭型態極有可能以資訊戰先行，透過資訊攻防癱瘓敵對國家指、管、通、情、監偵能力，塑造「勝兵先勝」的態勢。我國也應將「國艦國造」、「國機國造」的決心與氣魄，運用在發展軍、民兩用的自動資

註19：〈6成網路攻擊都是來自中國！59萬筆文官資料外洩只是一角 臺灣為何深陷資安危機〉，《今周刊》，2019年11月18日，https://www.businesstoday.com.tw/articele/category/80392/post/201907310017/，檢索日期：2020年1月6日。

註20：國防報告書編纂委員會，《中華民國108年國防報告書》(臺北：五南文化廣場，2019年9月)，頁69。

註21：同註20。

註22：闕志克，〈何謂資安即國安〉，http://talk.ltn.com.tw/article/paper/1249488，自由電子報，2018年11月26日，檢索日期：2020年1月6日。

安攻防技術，方得以確保在未來資訊網路戰爭中具備與敵抗衡的實力。

國軍強調「首戰即決戰」概念，並以「創新/不對稱」戰術因應中共武力威脅。因此，在建軍規劃上須跳脫建立對等武力的傳統觀念，將國防資源及科技能力集中在關鍵戰力，建立實質嚇阻力量有效反擊能力。而國防科技發展趨勢係為確保國防網路能在安全架構下正常運行，以支援軍事作戰任務，有效進行網路攻防為主軸，在遂行防衛作戰前提下，國軍應著重下列五項發展策略[23]：

(一)強化全方位資訊作戰組織

鑒於時代日新月異，現在的網路戰已將攻擊、防護及偵蒐納入全方位作戰機制，故面對新形態作戰，應將國軍各網路戰力整合，審視人力、編裝及任務，逐步辦理調整編裝，以提升組織運作全方位效能。

(二)發展新式資訊攻防戰具

在籌劃網路戰攻擊、防護及偵蒐應處能力中，應與民間產業、政府機關及學術單位多方合作，藉此瞭解國軍自身不足，尤以資安裝備及系統為重；另近幾年因應新型態網路攻擊，我應著重於智慧型弱點漏洞探測、偽冒、欺敵及誘捕系統等網路攻防系統，以協助戰場指揮官完成作戰指令下達；另運用多重攔截及網路阻斷方式，遲滯敵作戰節奏，為國軍爭取反制作為時間。

(三)創造優質資訊戰人力留用環境

鑒於資訊人才招募不易，國軍應逐步創新軍民網路人力招聘制度，建立網路戰穩固之戰力，並針對所需資訊專才，鼓勵人員考取國際證照，並依證照給與加給，俾提升人才素養，拓展國際視野。

(四)推動資訊安全跨域合作

如前所述，現行藉由民間產業、政府機關及學術單位多方合作，建立資安聯防與溝通機制，定期執行緊急應變演練及網安情資分享，才能建立軍民一體的聯合網路防護架構體系。

(五)研擬多元資訊作戰計畫

應針對中共指管網路、軍事武器系統等相關重要設施加強情蒐，針對前瞻網路科技及資訊關鍵技術，提供網路偵蒐、預警及阻絕等功能，掌握網路威脅趨勢，以制定多元作戰計畫，提早封鎖並瓦解中共網路之攻勢。

二、強化資訊戰之建議

分析當今戰爭型態，在空間上早已不打全面戰爭，而以殲擊目標的局部作戰為主；故全球各國紛紛成立網路作戰部隊。借重資訊網路的作戰能力，例如利用誤導、錯亂、阻絕、封鎖等手段，造成對手在開戰前即陷入「耳不聰、目不明」的狀態，無法正確決策。更可藉由網路技術，先期掌握情資，癱瘓敵方軍事系統，進而獲取戰場優勢。有鑑於此，國軍於2017年6月29日整合資訊網路戰、電子戰及資通平臺等三大區塊成立「資通電軍」，並以網路攻防為核心，通訊安全為基礎，電磁發展為前瞻做為資通電軍三大主要任務[24]，彰顯資訊戰早已成為「先戰之戰」。

註23：同註20。

註24：〈資通電軍指揮部編成典禮〉，總統府網站，2017年6月29日，https://www.president.gov.tw/NEWS/21451，檢索日期：2020年1月6日。

隨著科技進步與發展，網路已成為關鍵的生活場域，且其特性使網路資源爭奪成為有別於陸、海、空及太空之外的新型作戰型態；就軍事作戰而言，網路作戰對於軍事嚇阻、戰力投射及戰略威脅，具有相當程度的影響力，或進而左右他國之認知與決策，達到資訊、網路作戰預期規劃的作戰效益[25]。對我國而言，中共謀我之心未曾稍減，刻正積極藉由網路戰，發動前置攻擊及窺探我軍情資，企圖癱瘓我國家安全與軍事指揮系統，獲取戰場優勢，國人不可不防。畢竟網路作戰須於平時著手經營，戰時始可發揮戰力；再者，現代戰爭發展趨勢中，資訊戰不僅是前哨戰，更是臺澎防衛作戰致勝的關鍵因素，因應資訊戰已成為不可逆的趨勢，有效整合現有公民營資源，建立精實的國防通資電系統，滿足國軍聯合作戰需求，有效提升國軍整體資訊戰力[26]，至關重要。而如何在防衛作戰中，強化資訊作戰已成為當前重要課題，建議如後[27]：

(一)建立優勢資訊戰力

資訊作戰首重「安全」，故資訊戰的重點在於網路安全防護，故應發展安全防護機制與系統裝備，朝向構建自動化、系統化以及資訊化之安全防護系統目標邁進。在建構安全防護網後，進而發展主動式的網路戰監偵及反制作為，方可確保國軍在資訊戰場的優勢，遏制中共犯臺企圖。

(二)嚴密管控通資安全

在配合國家資通安全政策發展下，應著手朝向建置國軍資訊戰防護及通資訊緊急應變作業能量，並結合民間業界及學術單位資安防護能量，發展主動積極資訊防護及網路監偵能力，以確保通資安全，共同鞏固國軍通資安全。

(三)防護聯戰指管鏈路

數據資料鏈路為未來戰場掌握情資及遂行指揮管制之首要工具，國軍秉持聯合作戰需求與指導，應針對國軍指、管、通、情、資訊系統及三軍共通的自動化數據傳輸鏈路，建構資安防護牆，才能使專網作業安全無虞，有效保障聯戰指管鏈路安全。

(四)有效整合通信網路

通用網路平台建立為爭取「資訊優勢」之關鍵要素，主要以建置三軍通用戰術聯戰網路為目標，結合國軍現有資通電系統及民間通訊資源，形成軍民共用多重節點、複式網路的通聯手段，藉以充分發揮及運用整體國家資源，提升通資戰力、有效支援作戰。

伍、結語

現代化網路戰爭讓人防不勝防。從資訊保密的角度看，小從網路遊戲帳號密碼被盜，大到企業、國家的機密外洩，無不造成個人、團體與國家的傷害。從軍事的角度來看，則說明了兩軍對戰中，若要取得勝果，首

註25：〈中共政軍發展評估報告〉，國防安全研究院，2018年12月12日，https://indsr.org.tw/wp-content/uploads/2018/12/中共政軍發展評估報告，檢索日期：2020年1月6日。

註26：〈國家資通安全戰略報告-資安即國安〉，總統府網站，2018年10月，https://www.president.gov.tw/Page/ 317/969/，檢索日期：2020年1月6日。

註27：同註20。

先要落實情資管控，避免駭客入侵與資料外流，及早因應無所不在的網路作戰威脅。為此國防部已將通資安全視為國軍達成各項作戰任務、遂行資訊作戰的重要作為，並積極從事國軍資安整備工作，除建置嚴密的資安防護機制、頒布多項資安管控措施、主動查察違規事件外，另也要從政策面、管理面、技術面三管齊下，落實資安工作。

國人須知，資訊網路作戰是場沒有砲火的戰爭，也是不經宣戰就已全天候進行的戰鬥，唯有全軍上下一心，準確對資訊戰時代的要求做出預測研判，並依新型網路威脅預先做出整體的安全防護規劃與決策，達成精準打擊敵作戰節奏之任務目標，也才能蓄積國軍「不對稱」網路作戰能力，消弭當前任何資安威脅，也才能創造「勝兵先勝」之作戰契機，共同確保組織及國家的安全。 ⚓

作者簡介：

蔡在昇士官長，海軍技術學校常備士官班92年班、海軍技術學校士官長正規班98年班、海軍官校士官二專班101年班，曾任海軍通信系統指揮部訓練士、臺北通信隊有線電修護士、左營通信隊領班、士官督導長，現服務於海軍通信指揮部。

老軍艦的故事

永春軍艦 PF-52

永春軍艦為一海岸巡邏艦，係由美國American Shipbuilding公司所建造，1943年9月18日下水成軍，命名為「Gavia」，編號為AM-363。民國38年，海關緝私艇「榮星」號移交我海軍使用，由於與「永」字號掃佈雷艦同型，經命名為「永春」軍艦，編號為MSF-52，民國39年6月編入第三艦隊，民國41年9月改隸第四艦隊，民國45年改編號為PF-52，隸屬於巡邏艦隊，擔任海岸巡防及外島防務任務。該艦自成軍後曾參加過多次戰役，其中較重要戰役計有南日島戰役、東山島戰役及黃岐海戰。

民國50年7月1日該艦由於艦體老舊，內部機件不堪修復，隨即奉令除役。(取材自老軍艦的故事)