其他論述

DOI:10.6237/NPJ.202102_55(1).0008

淺談國軍網路安全防護作為之研究

海軍中校 李建鵬、海軍少校 陳保佑

提　　要：

一、依全球風險報告指出「網路攻擊」之科技風險，是僅次於天災環境風險外，對世界各國危害最大之風險，凸顯人們享受資訊交換便利之餘，伴隨著是資訊暴露的風險與威脅；各國刻正面臨網路安全威脅之嚴峻挑戰，國軍仍在中共網路攻擊威脅下，尤應警惕。

二、從近年網路攻擊事件觀察可知，網路攻擊已由單一手法衍生成複合式攻擊，其中「進階持續性滲透攻擊」具長期潛伏且不易偵測的特性，已成為駭客竊取各國機敏資料的主要手段，國軍應瞭解其特點及威脅，並儘早研擬防護因應作為。

三、因為網路世界沒有百分之百的防禦，資安更沒有絕對的安全。國軍在面臨嚴峻的網路攻擊威脅下，應持續完善資安管理標準、強化人員資安素養、厚植資安防護能量，俾確保國防機密不致洩露。

關鍵詞：網路攻擊、APT攻擊、網路安全防護

壹、前言

自1960年代發展電腦網路以來，隨著科技的不斷進步，網際網路在社會的各個層面已為全人類提供便利自在，並成為現代人類生活不可或缺的一部分，使用網路的人口也越來越多。截至2020年7月，全球約有48億的網路使用人口，網際網路普及率約為百分之六十二[1]。根據財團法人「臺灣網路資訊中心」(Taiwan Network Information Center，TWNIC)所做《2020臺灣網路報告》內容顯示，臺灣地區上網人口約為1,761萬人，上網率約為百分之八十三[2]。

在現今網路隨手可得及資訊爆炸的時代，人類溝通的管道更加多元化，透過網路可以快速地取得資料，享受資訊交換的便利性，但伴隨著是資訊暴露的風險與威脅。依據世界經濟論壇(World Economic Forum，

註1：Internet World Stats, “Internet Growth Statistics”，https://www.internetworldstats.com/emarketing.htm, accessed 28 October 2020。

註2：〈2020臺灣網路報告〉，財團法人臺灣網路資訊中心，2020年12月11日，https://report.twnic.tw/2020/assets/download/TWNIC_TaiwanInternetReport_2020_CH.pdf，檢索日期：2020年12月21日。

圖一：2015-2019全球風險矩陣圖

資料來源：參考WORLD ECONOMIC FORUM, "The Global Risks Report 2019" ，http://www3.weforum.org/docs/, 27 February 2018, accessed 25 October 2020，由作者彙整製圖。

WEF)《2019年全球風險報告》(The Global Risks Report 2019)顯示，在2018年全球可能風險排名中，「網路攻擊」名列第3、「資料詐欺或竊盜」名列第4；而在2019年全球可能風險排名中，「資料欺詐或竊盜」排名維持第4、「網路攻擊」排名則略降至第5[3]。該份報告指出在2018及2019年全球五大可能風險排名中(如圖一)，「資料詐欺或竊盜」及「網路攻擊」等2項科技風險，是僅次於「極端氣候事件」、「緩解氣候變化與適應失敗」及「自然災害」等環境風險外，對全球危害最大的可能風險，由此可知網路安全風險已影響人類的日常生活甚鉅。

在網際網路蓬勃發展的時代，網路攻擊手法不斷的更新，網路安全沒有百分之百的防禦，更沒有所謂絕對的安全；而國軍在臨嚴峻的網路攻擊威脅下，尤應有所警惕。撰寫本文主要目的，即希望透過蒐集並分析網路攻擊案例，結合美軍網路安全防護作為，提出國軍網路安全防護精進建議，期能進一步做為國軍提升整體資通安全防護規劃與決策參據，強化官兵的資安防護意識，以防護國軍網路安全。

貳、網路攻擊威脅探討

根據2018年國防部送交立法院的《國軍資安防護機制》書面報告指出，我國每月遭受數千萬次的網路攻擊，光是國防部所屬單位每月就承受近2,000萬次的網路攻擊。在2013年國防部所屬單位遭受網路攻擊計868

註3：WORLD ECONOMIC FORUM, "The Global Risks Report 2019" ，http://www3.weforum.org/docs/, 27 February 2018, accessed 25 October 2020.

表一：國防部所屬民網遭異常偵測、掃描及疑遭攻擊次數統計表

年度／單位	2013年	2014年	2015年	2016年	2017年
國防部網站	717, 788	1, 001, 142	1, 153, 275	4, 120, 552	9, 552, 884
國防大學	9, 405	877, 450	995, 312	219, 522	198, 469
人才招募中心	804, 092	4, 309, 186	4, 931, 321	28, 522, 275	31, 968, 975
軍醫局	4, 557, 186	720, 542, 371	561, 312, 118	276, 271, 708	162, 453, 979
政戰局	2, 597, 760	133, 587	856, 889	194, 621	492, 549
總計次數	8, 682, 221	726, 863, 736	569, 248, 915	309, 328, 678	204, 666, 856

資料來源：《國軍資安防護機制書面報告》(臺北)，國防部，2018年2月6日，頁4。

萬次，於2014年急遽增加到7億2,686萬次為最高紀錄，而後逐年下降，於2017年遭攻擊次數降至2億466萬次(如表一)[4]。由前述數據可研判，近年來國防部遭網路攻擊次數有下降之趨勢，主因係為國軍在網路安全防護上有顯著的進步，但亦有可能是網路攻擊的手法轉變為更精準、更有效之攻擊，故國軍在資安防護作為上，萬萬不可以掉以輕心。

雖然大部分的網路攻擊事件都難以確認其發動來源，但仍可經由資安鑑識與行為模式辨認。根據臺灣網路資訊中心(TWNIC)指出，從網路威脅情資分析攻擊來源，自中國大陸發動攻擊者約占了六成[5]。然不只我國飽受中共網路攻擊威脅，全世界都面臨這種高度風險，近期更有報導指出，「中國駭取海事軍用機密、鎖定全球超過27所大學攻擊」[6]，顯見中共持續對全球發動網路滲透攻擊，藉以獲取相關機敏資料及科技。

隨著網際網路的普及、雲端科技的運用，使網路攻擊事件也呈現擴大化及多樣化的趨勢，以往大部分的網路攻擊為單一手法，演變至今已是結合了社交工程、木馬程式及弱點攻擊等手法的複合式攻擊手段。我們必須先行瞭解網路攻擊的特性及各項攻擊手段，才能加以防制並避免遭受駭客攻擊。以下將針對網路攻擊定義及手段、網路安全威脅之趨勢，及進階持續性滲透攻擊案例，逐項分析說明。

一、網路攻擊定義及手段

(一)網路攻擊的定義

網路攻擊係指透過惡意軟體，蓄意使用電腦系統或網路，對目標資訊系統、基礎設施、網路系統及個人電腦裝置等，實施破壞、摧毀或使其無法運作之各式作為[7]。

(二)網路攻擊手段

一般包含電腦病毒、變種病毒、木馬程式、邏輯炸彈、飽和攻擊、弱點攻擊與社交工程等手段，攻擊方式各異。不論那種類型

註4：《國軍資安防護機制書面報告》(臺北)，國防部，2018年2月6日，頁4。

註5：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18日，https://www.ithome.com.tw/news/129208，檢索日期：2020年10月30日。

註6：尹俊傑，〈中國駭取海事軍用機密 鎖定全球超過 27 所大學攻擊〉，中央社，2019年3月6日，https://www.cna.com.tw/news/firstnews/201903060014.aspx，檢索日期：2020年10月29日。

註7：〈瞭解網路攻擊，學習防禦之道〉，IBM，https://www.ibm.com/tw-zh/services/business-continuity/cyber-attack，檢索日期：2020年11月18日。

表二：網路攻擊手段統計表

攻擊手段	攻擊作法說明
電腦病毒	一種小型程式，具有潛伏、發作、感染、破壞等典型的行為特色，有如生物病毒一般。電腦病毒一旦於對方的資訊系統內感染發作，經常會在極短時間內造成及顯著的破壞與大量的傳染散播。
變種病毒	一種程式工具，可依策略參數而產生大量的變種病毒。
木馬程式	一種任務導向的間諜程式，經常具有潛伏、窺探、匿跡、遙控等特色，一旦對方資訊系統被植入木馬，可對其進行長時間秘密入侵而不被發現。
邏輯炸彈	一種任務導向的惡意程式，可被設計成獨立運作而不需要與原攻擊方聯繫。一旦對方的資訊系統被植入邏輯炸彈，可於特定的時間或條件下，自動發作而破壞對方的資訊系統。
飽和攻擊	對被攻擊目標產生大量的垃圾資訊，以消耗其網路頻寬或系統資訊，使其減低或喪失功能。
弱點攻擊	利用被攻擊目標的系統弱點對其攻擊，使其系統發生錯誤、被入侵或當機。
社交工程	利用人性弱點，應用簡單的溝通和欺騙技倆，以獲取系統帳號、身分證號碼或其他機敏資料，來突破目標的資通安全防護，遂行其非法的存取、破壞行為。

資料來源：作者研究整理。

表三：網路攻擊手法差異比較

區　分	進階持續性滲透攻擊	一般網路攻擊
時　間	長期潛伏，隱匿行踪。	攻擊時間長短不一。
動　機	竊取所需要的特定機密，包含國家安全、各種組織情報和商業機密等等，常具有政治動機。	竊取金融與個人資料換取實質利益，不見得具有特定動機。
攻擊者	有資源、有組織、有計畫性的團體。	一般的個人或駭客組織。
攻擊對象	有針對性、範圍小，多以政府、軍事國防機構、大型能源產業、高科技產業等。	無針對性、大範圍，一般以金融業、線上交易業者、具有大量個資企業為主。
攻擊標的	挑選過的、高價值的機敏資料、各種組織的重要情資或智慧財產權等。	一般信用卡、銀行帳戶檔，或個人資料為主。
攻擊武器	客製化，常用單一的漏洞，經常是零時差漏洞的攻擊。	非客製化，複合多種常見漏洞在單一檔案攻擊，攻擊範圍大。
攻擊手法	為了確定攻擊一定成功，或同時用多種攻擊手法入侵。	速戰速決，通常以大量快速有效的單一手法入侵。
防毒軟體偵測率	1個月內新樣本偵測率約30%以下。	1個月內新樣本偵測率約90%。

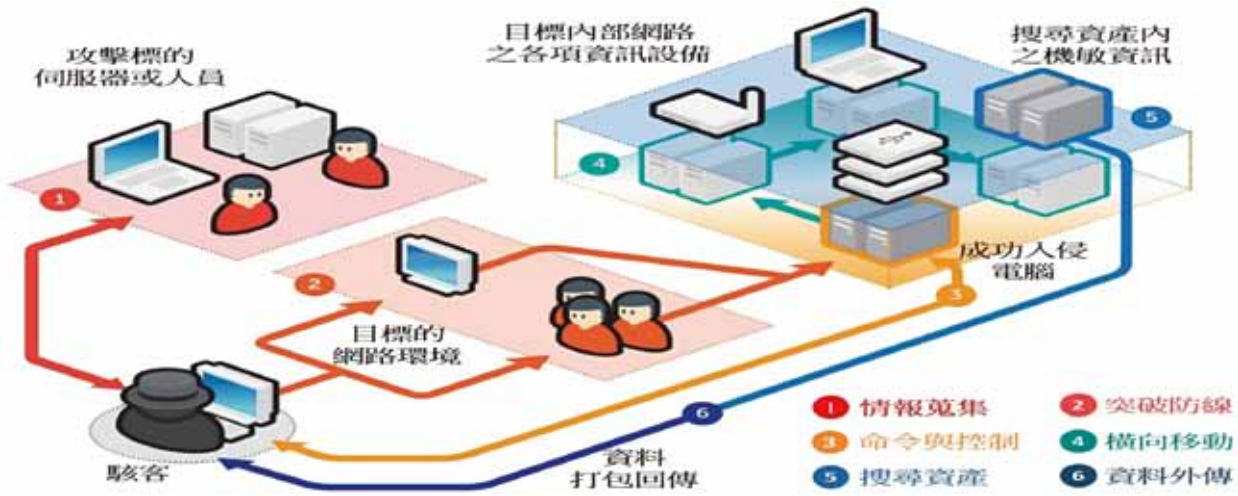
資料來源：黃彥棻，〈鎖定對象、長期滲透的攻擊手法：APT改寫資安威脅〉，iThome，2012年6月16日，https://www.ithome.com.tw/article/91044，檢索日期：2020年10月24日。

的攻擊都是駭客實現入侵目的所可能採取的方法，我們只有瞭解這些手段，才能有效的抵禦駭客攻擊(手段及作法，如表二)。

二、網路安全威脅趨勢及案例分析

隨著科技進步，電腦、智慧型手機、平板電腦，以及越來越普及的物聯網(Internet of Things，IoT)[8]裝置已大幅應用你我在日常生活中，引發的網路犯罪及個資保護等課題，也逐漸成為影響國家安全、社會安定之隱憂，使全球正面臨嚴峻的資安威脅。根據行政院「資通安全處」於2019年6月發表的《107年國家資通安全情勢報告》中指

註8：張菀庭，〈什麼是物聯網 IoT？〉，服務創新電子報，2016年4月19日，https://innoservice.org/9802/主題週專題報導-什麼是物聯網-iot/，檢索日期：2020年10月26日。



圖二：APT攻擊各階段示意圖

資料來源：參考趨勢科技，《進階持續性滲透攻擊(APT)發展趨勢2014年度報告》(臺北)，2015年4月30日，頁29，由作者彙整製圖。

出，近期資安威脅態樣計有進階持續性滲透攻擊、分散式阻斷服務攻擊、物聯網設備資安弱點威脅、關鍵資訊基礎設施資安風險、網路與經濟罪犯影響及資安(訊)供應鏈安全等6種，其中「進階持續性滲透攻擊」是近年來最熱門的資安議題[9]。其以多變的技術及不易防禦的特性，成為駭客最喜愛的一種網路攻擊手法(差異比較，如表三)。

經美國火眼(Fire Eye)公司長期的追踪調查發現，進階持續性滲透攻擊通常是由政府組織援助的特定駭客團體發起，且不同的團體會針對不同類型的目標，如：軍工、醫療、太空科技、海洋科技等不同的領域實施滲透攻擊，導致近年來美軍軍方及其國防工業承包商一再肇生網路駭客攻擊情事[10]。當前我國正執行「國機國造」、「國艦國造」及飛彈科技研發等專案，其必然成為中共駭客組織具有高度興趣竊取之項目，故以下將對進階持續性滲透攻擊做進一步探討及案例分析。

(一)進階持續性滲透攻擊(Advanced Persistent Threat，簡稱「APT」攻擊)

「APT」攻擊包含進階、長期、威脅等三個要素，是指組織(特別是政府)或者具組織性的團體精心策劃，並運用當時最先進的攻擊手法，長時間潛伏在網路或是系統內對特定目標執行持續性的網路監控及攻擊，以達到攻擊者之目的(通常是竊取機敏資料)，而且難以被偵測[11]。「APT」攻擊主要可區分為六個階段(如圖二)，簡要說明如下：

1. 情報蒐集：針對特定目標開始觀察特定組織或團體，並蒐集目標資訊環境和組織

註9：《107年國家資通安全情勢報告》(臺北)，行政院，2019年8月21日，頁4-8。

註10：吳其勳，〈中國網軍重現江湖，8個駭客組織回歸運作〉，iThome，2018年10月15日，https://www.ithome.com.tw/news/126295，檢索日期：2020年10月25日。

註11：〈什麼是APT進階持續性威脅〉，趨勢科技，2011年9月13日，https://blog.trendmicro.com.tw/?p=123，檢索日期：2020年10月24日。

架構等相關資訊，以制訂客製化的社交工程攻擊手法。

2.突破防線：利用電子郵件、通訊軟體、社群網路或應用程式弱點等方式，嘗試入侵特定目標的網路環境。

3.命令與控制：在入侵電腦安裝遠端控制通訊工具時，確認遭入侵成功的電腦和駭客伺服器間保持通訊。

4.橫向移動：利用遭入侵電腦做為跳板機器進行提權動作，並以後門程式在目標網路感染且掌控更多的設備。

5.搜尋資產：駭客透過掌控之設備、使用者帳號及權限，持續不斷地蒐集並過濾目標網路內各種重要資料或機敏資訊。

6.資料外傳：為避免遭組織偵知，駭客會挑選適當時機，低調且緩慢地將重要資料及機敏資訊打包回傳，並清除入侵痕跡，造成組織的重大損失及調查的困難。

(二)APT攻擊案例

隨著駭客攻擊的動機與目的轉變，我們面臨到的是一個不斷演變的網路攻擊手法及資安威脅環境。在這樣的環境中，因為APT攻擊具長期潛伏及不易偵測的特性，遭受攻擊的單位資料外洩的數量都不少，同時被竊取的也必定是重要的機密資料。經統計近年與美國軍方相關成功的APT攻擊案例，摘要臚列如后：

1.根據美國「參議院軍事委員會」(Senate Armed Services Committee)2014年的調查報告指出，與中共有關的駭客在一年內(2012年6月至2013年6月)至少20次成功入侵美國運輸司令部(U.S. Transportation Command，TRANSCOM)承包商的電腦系統，致使美軍部隊部署及動態有洩漏之虞。在這20次的滲透攻擊中，美國國防部僅掌握偵知9次入侵行為，而運輸司令部更少(僅2次)，顯示各部門缺乏資訊分享及回報能力[12]。

2.2017年澳洲情報局(Australian Signals Directorate，ASD)主管在一場安全會議上表示，澳洲國防部的一家承包商遭駭客入侵，大約有30GB(約1.5萬張800萬畫素的照片)的資料被竊取，包括美國最新的F-35戰鬥機及P-8偵察機、C-130運輸機等相關資料。駭客透過一個已知的漏洞入侵該公司[13]，其中令人難以置信的是，該公司資訊技術人員僅有一名，且經驗不足[14]。

3.美國太空總署(National Aeronautics and Space Administration，NASA)旗下的噴氣推進實驗室(Jet Propulsion Laboratory，JPL)於2018年4月遭駭客滲透入侵，導致如「火星計畫」等專案約500MB的檔案被竊取，且攻擊活動已潛伏超過十個月之久，駭客係利用樹莓派(Raspberry Pi)[15]微型電腦做為跳板，進入該實驗室的內部網路[16]。根

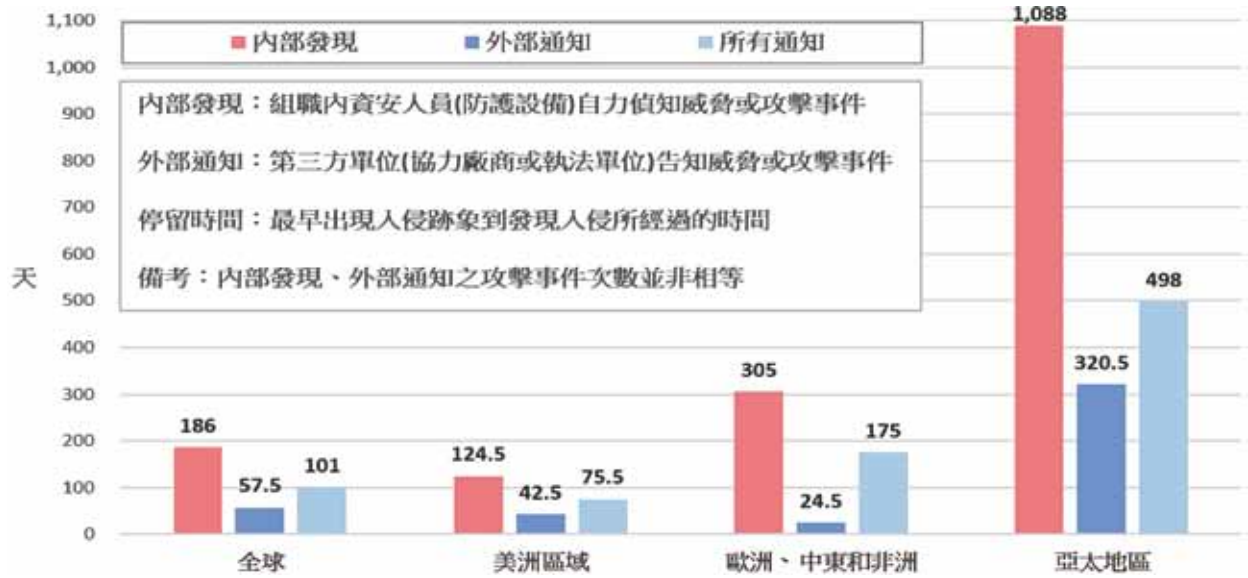
註12：陳曉莉，〈美國國防運輸機密難保，中國網軍一年成功入侵外包商電腦系統至少20次〉，iThome，2014年9月22日，https://www.ithome.com.tw/news/90998，檢索日期：2020年10月26日。

註13：陳曉莉，〈澳洲國防外包商遭駭，F35戰機資料外洩〉，iThome，2017年10月16日，https://www.ithome.com.tw/news/117492，檢索日期：2020年10月26日。

註14：王光磊，〈澳洲國防包商機敏資訊遭駭〉，《青年日報》，2017年10月13日，https://www.ydn.com.tw/news/newsInsidePage?chapterID=1015309，檢索日期：2020年10月26日。

註15：〈什麼是樹莓派〉，國立臺灣科技大學樹莓派實驗室，https://sites.google.com/site/rasberrypintust/home/shen-me-shi-shu-mei-pai，檢索日期：2020年10月24日。

註16：洪羿漣，〈落實辨識與可視化、新興IoT裝置安全看得見〉，新通訊元件，2020年1月2日，https://www.2cm.com.tw/2cm/zh-tw/market/58259D453CB14804B6347F7FFC3D01ED，檢索日期：2020年10月26日。



圖三：全球及各地區遭APT攻擊偵知天數統計圖

資料來源：參考FireEye Taiwan, “m-TRENDS2018”, Taipei, 21 June 2018, p.7，由作者彙整製圖。

據其中調查報告顯示，內部人員未依程序執行新增裝置管控，且網路閘道器未發揮隔離效果[17]。另NASA曾在2011年和2016年分別發生安全漏洞事件，2018年10月又遭駭客入侵所屬員工資訊伺服器[18]，顯見資安防護漏洞無所不在。

4. 2018年6月9日《華爾街日報》報導，中國大陸駭客於2018年1月及2月入侵一家名為「海軍水下戰中心」(Naval Undersea Warfare Center，NUWC)進行研發的承包商，竊取了614GB的資料，包括由潛艦發射的超音速反艦飛彈、感測器及訊號資料、潛艦無線電室密碼系統、以及海軍潛艦發展單位的電子戰資料庫[19]。

(三)APT攻擊綜合分析

前述各國歷年遭網路攻擊之實例，均為成功運用APT攻擊，以下分析其攻擊之特點如下：

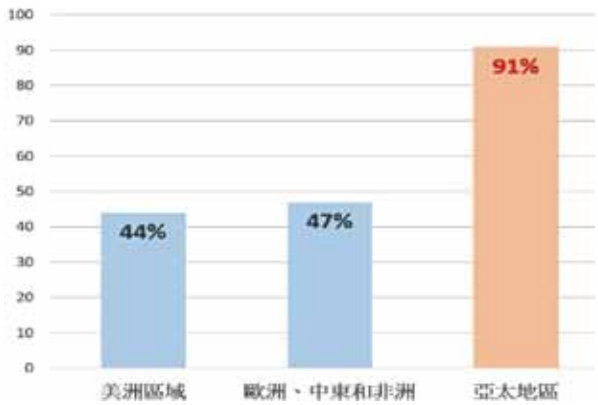
1. 潛伏期長，不易偵知：

駭客組織入侵後，長期潛伏於系統內，遭駭單位通常不具偵知能力，大多數是由第三方組織通知遭駭單位執行處置及查察作為。依火眼(Fire Eye)公司發布的《2018年資訊安全報告》指出，亞太地區的組織在偵測到入侵行為前，該威脅在系統內平均停留時間約為498天，而全球平均偵獲攻擊時間僅

註17：陳曉莉，〈美國太空總署遭駭調查：駭客以Raspberry Pi作為跳板滲透NASA網路〉，iThome，2019年6月24日，https://www.ithome.com.tw/news/131423，檢索日期：2020年10月23日。

註18：陳曉莉，〈NASA驚爆伺服器遭駭客入侵，過去12年員工個資恐遭外流〉，iThome，2018年12月20日，https://www.ithome.com.tw/news/127788，檢索日期：2020年10月26日。

註19：Ellen Nakashima and Paul Sonne, “China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare”, Washington Post, https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html, June 8 2018, accessed 28 October 2020.



圖四：各地區遭APT多次攻擊統計圖

資料來源：參考FireEye Taiwan, “m-TRENDS2018”, Taipei, 21 June 2018, p.22，由作者彙整製圖。

需101天(如圖三)，可見亞太地區組織的網路安全意識及因應網路安全攻擊事件的表現，相對較差[20]。

2. 複合式攻擊，不易防禦：

駭客已鎖定攻擊的對象，客製化的利用各項系統弱點、漏洞等複合式手法執行網路攻擊，而非單一手法攻擊，且不易遭防毒系統偵測，例如社交工程攻擊、零時差漏洞攻擊[21]、後門程式及惡意軟體等。「火眼公司」在2018年發布的同份報告中亦指出，曾遭受攻擊的組織有可能再次遭到攻擊；其中亞太地區有超過九成以上的組織被駭客再次鎖定及攻擊(如圖四)。

3. 攻擊目標轉向：

因應網路攻擊日益猖獗，世界各國均紛紛制訂相關資訊安全措施，並持續強化網路防禦能力，以有效降低公部門成功遭網路攻擊次數；而國防工業承包商因沒有迫在眉梢的危機感，加上內部員工資安素養參差不齊，導致資安防護投資不足，更容易造成網路安全突破點。這也是駭客組織轉而攻擊較易得手的國防工業承包商、科學研究室等，以獲取機密資訊之主因。

綜上所述，網際網路及雲端技術的發展，確實提供駭客一個滲透的媒介；而國防機密資訊更是駭客最想執行滲透及攻擊的目標。從層出不窮的駭客入侵事件及各國國防工業承包商、科學研究室遭攻擊的案例來看，國軍在國防自主的發展進程上，更應積極研擬有效之網路安全防護作為，以為因應。

參、美國網路安全因應作為

網際網路技術創始於美國，而其亦是第一個將網路安全納入國家安全戰略規劃之國家；即便如此，美國仍面臨從不間歇的駭客攻擊事件。以下探討美國網路安全戰略之發展及因應作為，期望能做為國軍網路安全防護作為之借鏡。

一、美國網路安全戰略及部隊之發展

自1960年代由美國國防部出資發明網際網路，其在網路的軍事運用上一直保有領導地位，而隨著網際網路及科技的蓬勃發展，美國為了應對可能發生的網路戰爭，進一步制定國家網路安全政策的需求，同時組建網路戰部隊。

(一)網路安全戰略發展

柯林頓(Bill Clinton)總統在任時期，認為人類所面臨的威脅將由實體世界轉向虛擬空間，戰略發展著重於資訊的完整性、保

註20：FireEye Taiwan, “m-TRENDS2018”, Taipei, 21 June 2018, p.7。

註21：〈什麼是零時差漏洞？有哪些漏洞攻擊手法？〉，趨勢科技，2019年12月26日，https://blog.trendmicro.com.tw/?p=62238，檢索日期：2020年10月28日。

表四：美國網路戰部隊發展大事紀

時　間	事　件	發　展　要　點
2009/6/23	設立網路司令部	前國防部長蓋茲(Robert M. Gates)下令成立網路司令部，做為美國網路戰最高指揮機構(隸屬戰略司令部下的二級司令部)。
2009/8/19	空軍網路戰司令部成立	整合網路、空中及太空行動以支持軍事行動。
2010/1/29	海軍艦隊網路戰司令部成立	整合海防作戰司令部、海軍網路戰司令部、海軍資訊作戰司令部等單位。
2010/10/1	陸軍網路戰司令部成立	負責主管陸軍網路任務、行動及功能。
2012/3/24	向各戰區派駐網路戰分隊	美軍網路司令部於6個戰區司令部(歐洲、印太、南方、中央、北方與非洲司令部)成立網路戰小組。
2013/1/29	網路司令部擴編	員額預計擴增五倍，並成立國家任務部隊、網路防禦部隊及作戰任務部隊等。
2014/3/4	規劃設立133支網路部隊	2014年《四年期國防總檢討》(Quadrennial Defense Review，QDR)提出美國規劃設立133支網路部隊的戰略目標。
2016/4/5	成立133支網路部隊	網路司令部司令於參議院軍事委員會聽證會表示，美軍迄今已建成133支網路部隊，總人數4,990人，分別為執行進攻任務的作戰部隊(27支)、保護國防部內部網路的網路防護部隊(68支)、保護美國國內電網等重要基礎設施(13支)以及支援部隊(25支)。
2018/5/4	網路司令部升級	成為特種作戰司令部、運輸司令部、戰略司令部外，第4個依職能劃分的聯合作戰司令部。

資料來源：參考朱志平、梁德昭，〈習近平時期美中網路安全競逐〉，《遠景基金會季刊》(臺北市)，第17卷，第2期，2016年4月，頁29-30，由作者彙整製表。

密性，並提升關鍵基礎設施的安全；小布希(George Walker Bush)總統任內，因發生「九一一事件」，戰略方向調整為提升網路威脅的預警、監控、防範，並加強反情報能力，阻止敵對和惡意的網路空間行動，建立快速反應機制以回應網路威脅，進而鞏固美國網路空間生態環境之安全。到了歐巴馬(Barack Obama)總統則進一步將網路安全升格至國家安全戰略層次，強調網路空間的和平穩定，聯合網路軍事演習，提升網路威脅對抗能力，並促進國際間網路合作。到了川普(Donald Trump)總統時期，則因美國面臨大量網路威脅，戰略發展主軸則以強化網路攻防能力、放寬網路軍事行動管制等作為，目的即在維護其網路空間中的國家安全與利益[22]。

(二)網路戰部隊之發展

美國國防部在2005年公布的《國防戰略報告》顯示，網路空間已和陸、海、空、天並列，成為同等重要且需要維持的第5大空間，也促使美國於2010年成立網路安全部隊，並組建「網路司令部」(美國網路戰部隊發展，如表四)。美軍網路司令部負責「保護美國國防部網路及資料安全」、「支援各作戰司令部及聯合軍事指揮官」及「根據命令保護美國的關鍵基礎設施」3項主要核心

註22：黃志軒，〈國土安全脈絡下的美國網路安全戰略發展〉，國防大學政治研究所碩士論文，2005年，頁47-64。

任務，所屬網路部隊依任務可區分為4種類型[23]：

1.國家任務部隊(National Mission Teams，NMTs)：負責偵測敵人活動、防制網路攻擊，確保國家安全。

2.作戰任務部隊(Combat Mission Teams，CMTs)：負責執行軍事網路行動，以支援作戰司令部。

3.網路防禦部隊(Cyber Protection Teams，CPTs)：負責保護美國國防部資訊網路，並實施網路作戰準備。

4.支援部隊(Support Teams，STs)：負責提供分析與規劃，以支援各任務部隊。

二、網路安全防護作為

儘管美國大力的發展網路戰部隊及網路攻擊技術，並訂定網路安全戰略，仍肇生層出不窮的網路攻擊事件；且因美軍各類國防工業承包商的網路安全防禦措施相較軍事組織更顯薄弱，故容易成為駭客攻擊對象。有關美軍因應網路安全防制作為[24]，分述如后：

(一)建立安全認證

美國國防部在2020年1月公布「網路安全成熟度模型認證」(Cybersecurity Maturity Model Certification，CMMC)，要求承包商及轉包商依據專案的機密性，取得相對應的網路安全認證。美國國防部將廠商網路安全防護能力分為5等級，以第1級防護等級最低、第5級為最高級，要成為國防部的合格承包商，網路安全防護等級至少要達到第3級；要成為CCMC第3級以上的廠商，必須具備包含建立與維持由專職人員運作的安全行動中心、24小時待命的網路安全應變小組、使用自動化機制偵測電腦系統中是否有未授權軟體、硬體或是檔案，以及當資訊跨系統移轉時，須以資料加密或其他安全的方式控制資訊流等4項重要安全措施，以維資訊安全。

(二)建立資安事件通報機制

美國國防部認為缺乏網路安全防護計畫的承包商將無法有效識別、預防、檢測和報告供應鏈所遭受之網路攻擊，其中以通報機制尤為重要。因此要求所有國防工業承包商與轉包商建立資安事件通報機制，如有發現任何網路入侵事件，必須在發現後的72小時內通報。

(三)調整網路架構為零信任

現行的網路架構是傳統邊界安全架構的方法，通過對網路上所有入口和出口點的存取進行控制，以保證網路安全。當使用者進入網路後，即便這些內容與其工作無關，仍然可以瀏覽網路上大部分的內容；然「零信任架構」把系統本身當成是不安全的，對系統上的每位使用者都不信任。因此，只賦予每位使用者及其終端裝置「最低限度存取權限」(Least-Privilege Access)，並依各使用者的任務賦予相對應的權限，以確保資料及系統服務安全。

(四)要求廠商揭露原始碼是否提供他國

註23：施欣妤，〈美133支網路任務部隊小組蓄勢待發〉，《青年日報》，2018年5月22日，https://www.ydn.com.tw/news/newsInsidePage?chapterID=1071534，檢索日期：2020年11月3日。

註24：吳俊德、蔡榮峰，〈國防產業安全〉，《2019國防科技趨勢評估報告》(臺北市：財團法人國防安全研究院，2019年12月6日)，頁51-69。

檢視

美國媒體曾經報導，某些軟體製造商曾經允許俄羅斯國防部門，檢視他們賣給美國政府機構的產品中軟體原始碼，將使得俄羅斯尋找到美國政府機構使用軟體的弱點，也可以更輕易的發動網路攻擊[25]。美國聯邦政府依《國防授權法》要求供應商須呈報/揭露其商業用途或內部用途的產品、系統、服務項目之原始碼，是否曾被「中」、俄等勁敵審視，做為是否建立合作的依據[26]。

(五)禁止採購中國大陸及俄羅斯之軟、硬體

基於資訊安全考量，美國防部禁止美軍與其合約廠商採用中國大陸及俄羅斯來源之硬體，並列出具有「中」、俄資金背景的軟體公司產品，避免該等兩國藉由相關產品將手伸入國防體系，以進行滲透破壞或竊取資訊等行為，威脅國家安全。

(六)執行網路安全演練

美國國土安全部自2006年開始每兩年舉辦一次名為「網路風暴」(Cyber Storm)的國際網路安全模擬演練[27]，提供大規模政府供應商網路安全演練的框架，用以評估國家抵抗數位間諜活動的防禦能力，並強化公共與私人部門的網路防護。

綜上所述，即便美國一直很重視資訊科技及網路空間的發展，制訂了國家網路安全戰略及網路部隊，建構強大的資訊戰力；然

圖五：國艦國造各階段作業流程示意圖

資料來源：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92。

因網路環境具複雜度及不易偵知威脅之特性，仍不時有遭受攻擊的事件發生。因此，美國對網路威脅深感憂慮，極力反制及防禦未知的網路威脅，且在面對網路攻擊及惡意軟體的威脅下，無論是相對於全球或是亞洲地區來說，臺灣都是特別嚴重的國家之一，所以我們更應特別重視網路安全防護各項作為。

肆、國軍網路安全防護精進作為

國軍現行網路實體隔離政策是避免資料外洩、阻絕來自外部資安風險之有效方式；惟當遂行任務而需要與外界互動時，即須面對承擔網路安全威脅之風險。以本軍「國艦國造」任務為例，即可看出各階段作業均需與設計承商及造船廠執行資料交換及審查，而此一過程，又極易造成防護破口(如圖五)。依據美國的案例分析及美軍網路安全防護作為，對國軍網路安全防護作為，提出幾項

註25：〈原始碼洩美軍弱點 美國新國防授權法案約束科技業〉，《青年日報》，2018年8月2日，https://www.ydn.com.tw/news/newsInsidePage?chapterID=1087690，檢索日期：2020年11月3日。

註26：CONGRESS, "NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2019 CONFERENCE REPORT", https://www.congress.gov/115/crpt/hrpt874/CRPT-115hrpt874.pdf, 25 July 2018, accessed 29 October 2020.

註27：谷威涵，〈Cyber Storm簡介〉，行政院國家資通安全會報技術服務中心，2014年7月2日，https://www.nccst.nat.gov.tw/ArticlesDetail?lang=zh&seq=1339，檢索日期：2020年11月3日。

建議，分述如后。

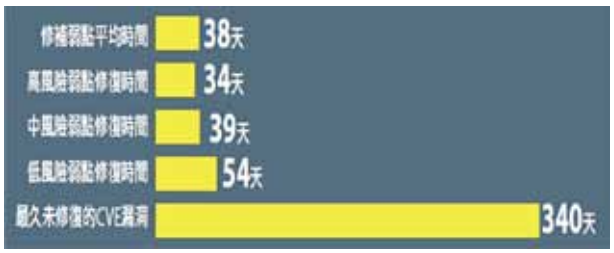
一、導入資安管理標準，強化資安稽核機制

依我國「資通安全管理法」子法「資通安全責任等級分級辦法」，明訂政府機關及特定非公務機關其資通安全責任等級，資通安全等級責任等級C級以上機關，其核心資通系統應導入「CNS27001」或「ISO27001」等資訊安全管理標準。本軍資通安全責任等級屬A級機關，資安業管單位應協助及輔導各單位導入ISO27001標準，以提升資安防護等級。

國外部分國防廠商遭駭客攻擊成功案例，多係因未落實資安相關作為，如作業網路使用非經核定之資訊設備、未落實網路實體隔離等情形，都是造成駭客有機可乘的主因。因此，為避免類案肇生，應由承辦(簽約)單位及軍種司令部成立專責編組(納編資訊及保防部門業管人員)，定期及不定期由編組人員稽核專案辦公室廠商資安及網路防護作為，透過雙重的稽核機制提升廠商網路安全防護等級，並降低遭有心人士滲透入侵風險。

二、建立資安管控小組，配置資安專責人員

根據調查，企業修補弱點平均需要38天，其中列為高風險應優先處理者也要34天，至於尚未處理的漏洞，甚致延遲將近一年才處置[28]。駭客常利用韌體[29]及軟體還沒有修補程式的安全漏洞進行攻擊；若單位無專責資安人員即時執行作業系統及程式的漏洞修補作業，從漏洞被發現到修補更新的空窗期，將大大提高遭滲透攻擊的機率(如圖六)。



圖六：弱點修復時間示意圖

資料來源：周峻佑，〈面臨不斷出現的變種攻擊亂象，企業的弱點管理處境日益艱難〉，iThome，2018年10月7日，https://www.ithome.com.tw/tech/126146，檢索日期：2020年11月5日。

我國「資通安全管理法」雖明確律定機關依其業務屬性應設置相關資通安全專責(職)人員，惟國軍部分單位受限於編制或人力運用，兼任人員難以落實執行相關資通安全業務；然因應現今嚴峻之網路安全威脅，實應建立資安管控小組，編制具備數位鑑識、分析、應變處置能力之資安專責人員，方可有效保障國防軍事機密之安全。

三、建構國防領域IASC，情資共享即時回報

近年來，日本政府單位、企業及國防工業承包商都遭到駭客攻擊，日本知名資安顧問在調查政府單位被駭的案件時，發現該單位的5個資安承包商雖都查覺到駭客入侵事件，卻都沒有對外通報，也沒有分享相關資訊，導致其他單位無法修復或阻絕該風險，致使特定組織可持續利用相同手法實施滲透攻擊[30]。

註28：周峻佑，〈面臨不斷出現的變種攻擊亂象，企業的弱點管理處境日益艱難〉，iThome，2018年10月7日，https://www.ithome.com.tw/tech/126146，檢索日期：2020年11月5日。

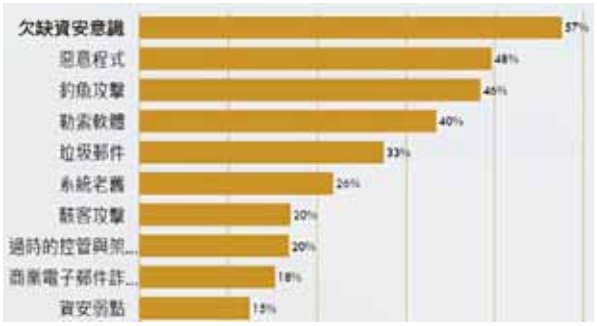
註29：〈韌體〉，維基百科，https://zh.wikipedia.org/wiki/韌體，檢索日期：2020年11月5日。

註30：〈日企業以通報攻擊為恥，使駭客有機可趁〉，臺灣電腦網路危機處理暨協調中心，2015年11月13日，https://www.twcert.org.tw/newepaper/cp-65-262-795af-3.html，檢索日期：2020年11月6日。

國防領域「資訊分享與分析中心」(Information Sharing and Analysis Center，ISAC)的建立，能增加國軍的資安威脅情資獲得管道，國軍業管人員及其承商得以橫向聯繫，並當偵知遭受攻擊時可情資共享、即時回報，保存資訊系統的電磁紀錄，以利鑑識人員進行事件分析、查察並進行應變處置、降低損害，以強化資安防護機制，防範類似事件再次發生。而這些舉措除可提升網路安全防護作為外，更能結合支援國防的非官方組織與企業，確保我國國防產業供應鏈的資訊安全。

四、強化資安職能訓練，協同執行資安演練

依據網路週刊「iThome」2019年企業資安大調查資料顯示，「員工疏忽、欠缺資安意識」是企業最大宗的資安風險(如圖七)[31]。「中央通訊社」報導指出，某科研機構人員因個人疏失，將研發中的機密文件遺留在公共自行車上，險些洩密[32]；另「中時電子報」報導指出，現役軍人違規攜帶隨身碟，因私自下載國際情勢等相關資料，違反資安規定遭汰除[33]。可見肇生資安風險及洩密事件大多是人為因素造成，故國軍各單位資通安全及資訊人員應定期接受資通安全專業課程(職能訓練)，以因應不斷演變及進化的攻擊手法及技術；另國軍人員配合行政院及國防部規劃，均會定期實施社交工程及網路攻



圖七：2019年TOP 10企業資安風險示意圖

資料來源：〈為何企業資安防護擋不住攻擊？〉，iThome，2019年4月4日，https://www.ithome.com.tw/article/129627，檢索日期：2020年11月5日。

擊演練，藉以提高所屬人員資安意識。而本軍現行資安演練並未將國防工業承包廠商納入協同演練，因此建議將其納入，並協請資通電軍定期對其實施資安健檢/弱點掃瞄，以提升國防供應鏈之資安應變能量。

五、強化資料交換流程，保障資料傳遞安全

本軍人員與部外單位及國防廠商等執行資料交換時，現行以將檔案燒錄至光碟交換為主，使用網際網路電子郵件傳遞為輔，資料於運送或傳遞過程中具高度風險有外洩之虞。故進行公務郵件交換時，雙方均應確實使用國防部專門建置與部外單位執行電子郵件傳遞之「國軍民網電子郵件系統」，以利有效掌握及管控郵件流向；另建議可研製與部外單位及國防廠商專用之加密式隨身碟，結合多因子加密機制，於使用隨身碟交換資料時，可透過系統自動加解密，並綁定電腦

註31：〈為何企業資安防護擋不住攻擊?〉，iThome，2019年4月4日，https://www.ithome.com.tw/article/129627，檢索日期：2020年11月5日。

註32：侯姿瑩，〈傳機密資料忘在YouBike車籃 中科院：違規者將究責〉，中央通訊社，2019年2月26日，https://www.cna.com.tw/news/firstnews/201902260263.aspx，檢索日期：2020年10月28日。

註33：周思宇，〈Usb下載資料 違反資安規定 入侵軍網 女中尉遭汰除〉，中時電子報，2016年8月17日，https://www.chinatimes.com/newspapers/20160817000429-260102?chdtv，檢索日期：2020年10月28日。

編號(網路卡位址等)，除授權之電腦及合法使用者可正常讀取檔案外，餘未經授權之電腦及使用者均無法開啟檔案，俾確保資料傳遞安全。

伍、結語

軍事學家亞當斯(James Adams)在其《下一次世界大戰》(The Next World War)書中曾提及：「在未來的戰爭中，電腦本身就是一種武器，前線無所不在。」[34]網路沒有實體界線，且不受空間及時間的限制，加上其具隱密且無法及時發現的特性，網路攻擊已經成為全球國家安全最嚴重的挑戰。行政院曾指出，境外對我國攻擊次數，在2018年每個月平均有2億次的掃瞄、3千萬次的攻擊[35]，由此可知有心人士對我國試探攻擊不曾停歇。我們正面臨著十分嚴峻的網路攻擊威脅，面對攻擊手法不斷的更新，系統漏洞一再的被發現且利用，顯見網路安全沒有百分之百的防禦，自然沒有絕對的資訊安全。

資訊安全的概念最基本的是「短桶理論」，也就是在木桶子裡能夠盛多少水，不是取決於最長的那一塊，而是最短的那一塊，因此，系統最弱的地方就是整個系統能力之弱點[36]。環顧國軍正於「國防自主」的政策指導下遂行「國艦國造」與「國機國造」任務，當此之際，防護自主產能與研發關鍵文件的資訊安全更顯重要，尤重打造「內外兼具」的網路安全防護能量，以確保國軍機敏資訊獲得完整之防護；況且「網路戰」是不分平、戰時，且完全未有煙硝的戰爭。換言之，國軍每一位電腦使用者都應隨時警覺，自己已經身處戰場，且面臨嚴峻之網路攻擊威脅，除了持續落實軍、民網「實體隔離」與「專網專用」政策，建置嚴密資安防護機制外，亦應針對資訊科技快速發展所衍生的新形態威脅，發展適切之防護措施，提升官兵的資安防護意識，以防護國軍網路安全，確維部隊戰力。

作者簡介：
李建鵬中校，中正理工學院87年班、國防大學管理學院指參班101年班、國防大學理工學院資工所碩士108年班。曾任中正艦電子官、建陽艦修護組長、臺北通信隊區隊長、通信系統指揮部科長、海軍司令部戰系處電戰官、資參官，現服務於國防大學管理學院。
陳保佑少校，海軍軍官學校專業軍官94年班、國防大學海軍指揮參謀學院109年班。曾任馬公軍艦修護組長、海洋監偵指揮部資管官、海軍司令部計畫處資參官、教育暨訓練準則發展指揮部通信官，現就讀國防大學聯合作戰參謀研究班。

註34：詹姆斯亞當斯(James Adams)著、張志誠譯，《下一次世界大戰》(新北市：新新聞文化出版，1999年)，頁1-2。
註35：黃彥棻，〈臺每首度聯手舉辦大規模網路攻防演練，臺銀行組藍隊聯隊對抗紅隊攻擊〉，iThome，2019年11月4日，https://www.ithome.com.tw/news/134003，檢索日期：2020年11月6日。
註36：李忠憲，〈資訊安全威脅與防護〉，《科學發展》(臺北市：科技部)，第553期，2019年1月，頁6-13。