從駭客網路攻擊探討國防供應鏈資安防護趨勢之研究

空軍上校　林于令　空軍少校　莊玉雯

提　要

一、隨著資安威脅發展趨於多元，駭客攻擊目標從隨機式轉變成鎖定式攻擊， 逐漸從單純的組織轉移到供應鏈上，近年常見多起政府機構、企業的供應鏈攻擊事件，突顯承包商或第三方分(轉)包商的資安防護完整性極為重要，尤其是面對必要的供應服務，更是防不勝防。

二、在國防產業時代下委外工項逐年增加，應省思國防廠商透由供應鏈所帶來的威脅，倘若在國防供應鏈上未建立完善的資安稽核及資安成熟評鑑機制，恐怕成為國軍資安防護的灰色地帶，存在未知的資安威脅。

三、本文參酌美國國防部推行網路安全模型認證機制，與我國國防產業條例之廠商級別評鑑及資安法等規範相較差異性，進而探討國防供應鏈未來資安防護趨勢走向，俾作為國防產業契約訂定的資安機制之參考。

關鍵詞：供應鏈攻擊、國防廠商、資安成熟評鑑

前　　言

在面對網路數位環境下，人工智慧(Artificial Intelligence, AI)、雲端服務、物聯網(Internet of Things, IoT)裝置等新興技術應用已逐漸普及化，加上5G世代帶來快速行動網路優勢，有助企業管理更為方便，相對衍生更多潛在資安風險，從近年來不論是政府機關、半導體產業或是金融機構等等發生的網路攻擊事件中，可看出網路駭客已開始鎖定管理服務供應商或第三方分(轉)包商作為攻擊目標，再透由供應鏈體系進而滲透擴大攻擊範圍，也就是所謂的「供應鏈攻擊」，尤其是面對必要的供應服務，更是防不勝防。

國軍未來與國防廠商合作的機會越來越頻繁，對於國防供應鏈不論是廠商級別認證、資通安全稽核及交付資安檢測等程序，若疏於完善的資安防護機制而形成破口，恐怕會對國軍帶來極大的資安威脅。

資訊供應鏈威脅之探討

網路攻擊從最早期利用社交工程郵件散播病毒的攻擊方式，在資訊科技創新與網路快速發展下，攻擊目標和手法持續轉變，已進化到針對系統、應用程式等漏洞進行攻擊，從被動式轉化為主動式，所面臨的是難以察覺的網路威脅，已是個人認知、組織安全及國家政策等各階層不可輕忽的問題。

一、資訊供應鏈網路攻擊型態

供應鏈攻擊係駭客針對特定目標的上、下游供應廠商反覆偵查，從資安防護弱點入侵，竊取權限後利用受信任的管道散撥惡意程式，間接入侵特定目標[1]，因此，本節以「社交工程」、「水坑式攻擊」、「APT攻擊」及「表單劫持」等相似攻擊手法做進一步分析，探討供應鏈上潛在的資安威脅：

(一)社交工程(Social engineering)攻擊

現今的網路攻擊都會結合社交工程手法，尤其以目標式攻擊居多，通常會以新興事件為誘餌，用以操控使用者心理產生興趣而疏於防範，利用人性弱點、溝通建立信任、假冒身分或將惡意程式隱藏於軟體等方式，引誘使用者下載並安裝該軟體或要求資訊輸入，藉機竊取遂行非法的存取、破壞行為，其常見應用在社交工程的攻擊方法如下：[2]

1.電子郵件夾帶病毒：將惡意程式隱藏於電子郵件中藉機散播病毒。

2.網路釣魚：利用偽冒熟人、知名的企業或以誘餌主旨寄送電子郵件，要求收件人疏於求證逕而點擊郵件中的超連結，進行惡意程式下載或輸入個人資料(包含帳號密碼、信用卡資訊等)。

3.圖片植入惡意程式：利用色情、美女圖片觸發使用者的好奇心點擊來散布惡意程式。

4.偽裝修補程式：為社交工程欺騙手法，偽裝成微軟的漏洞修補程式，藉由使用者對合法軟體的信任疏於防範。

(二)水坑式攻擊

首先會運用「零時差(Zero-Day)漏洞」攻擊概念，針對已公開含有漏洞的軟體程式、系統，在廠商釋出修補更新前，駭客先長期潛伏發掘漏洞，利用已知漏洞進行攻擊，是場廠商與駭客之間的攻防競賽。

最後以人員使用習慣與信任的弱點建立橋樑持續橫向攻擊，通常使用者對於經常瀏覽且信賴的合法網站認定為安全的環境，所以當攻擊者想要攻擊特定目標時，會運用網站程式的漏洞，在後端植入惡意程式，當用戶端瀏覽時會點擊觸發自動下載程式，遭受感染成殭屍電腦後，通常會自動連線至外部中繼站，下載最新的惡意程式，看似為使用者合法連線行為，躲避防毒軟體的偵測不易被發現，可提高存活率，水坑式攻擊的流程分成三個階段進行如圖1：

1.透過觀察或推測特定目標族群可能會使用的網站。

2.利用各種方式滲透入侵目標網站，潛伏發掘漏洞，並植入惡意程式。

3.當特定目標的人員來存取連結遭駭的網站時，就有機會遭受到惡意程式感染，成為傀儡電腦，達到擴散攻擊成效。[3]

1 「供應鏈攻擊」(iThome電子報)，https://www.ithome.com.tw/news/144212，(檢索日期：2021年5月3日)。
2 「社交工程突破人性防火牆」(資安人科技網)，https://www.informationsecurity.com.tw/article/article_detail.aspx?t2id=4&aid=5707，(檢索日期：2021年5月3日)。
3 張一善，「建構端點設備上APT攻擊防禦機制之研究」，臺北：國立臺北教育大學理學院資訊科學系碩士論文，2014年，頁9-10。

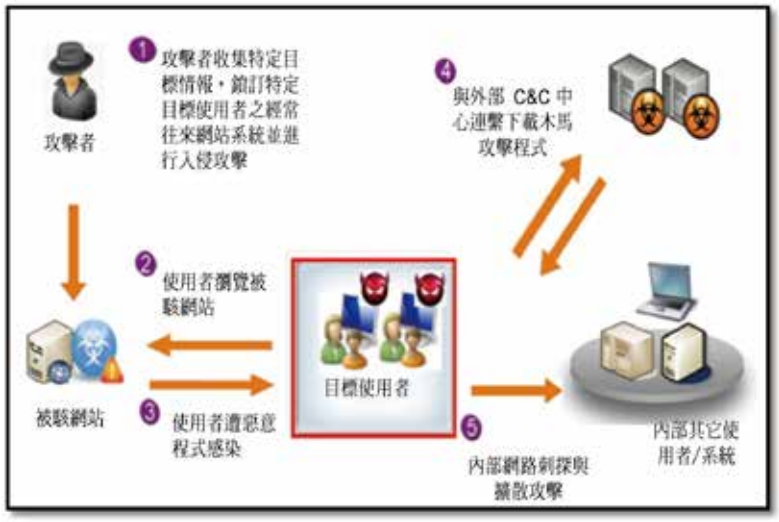

圖1　水坑式攻擊示意圖

資料來源：張一善，建構端點設備上APT攻擊防禦機制之研究，頁9-10。

(三)進階持續性滲透(Advanced Persistent Threat,APT)攻擊

APT攻擊行為具有長期、持續性的潛伏，專門鎖定特定的政府機關、企業組織或是個人等，透過長期蒐集資訊並針對攻擊目標的環境、特性等屬性策畫攻擊工具，且單一倚靠防火牆、入侵偵測系統及防毒軟體等系統是無法完全防禦，屬於規模性的滲透攻擊活動，APT攻擊行為區分七個階段如圖2：

1.選定攻擊目標後，會針對目標進行情報蒐集及環境背景探測。

2.依目標屬性客製化之攻擊程式，以引誘被害目標觸發工具，通常為較小、不易發現的惡意程式，避免遭防護系統偵測蹤跡。

3.透過社交工程誘導或欺騙目標使用者點擊已被入侵的網站，待其他手法進行攻擊工具傳遞及觸發。

4.瞭解攻擊目標所屬的環境、操作的系統及防護設備潛在漏洞，透過此威脅點進一步滲透搜索。

5.藉由目標內部已滲透成功之攻擊工具，主動與外部中繼站構連，下載植入其它攻擊能力較強化之後門程式，以利更深入攻擊。

6.取得目標系統管理權限、帳密及資料、程式等機敏資訊，並傳送至外部中繼站，建立控制管道。

7.開始進行竊取資料、破壞、橫向系統滲透等行為。[4]

(四)網頁表單內容劫持(Formjacking)

「表單劫持」為近年駭客竊取機密資料新興攻擊手法，可稱之為「虛擬ATM掃描」，駭客將惡意程式碼植入零售商網站，

圖2　APT攻擊流程示意圖

資料來源：張一善，建構端點設備上APT攻擊防禦機制之研究，頁7。

4 張一善，建構端點設備上APT攻擊防禦機制之研究，頁6-7。

藉此竊取購物者的信用卡資訊，取得消費者機密資訊後販售獲利，為網路罪犯牟取暴利的最新途徑，舉例來說，2018年英國航空公司(British Airways)官方網站與APP軟體遭到表單劫持的攻擊，約有38萬名搭機乘客的支付資訊與個人資料遭竊，對企業和消費者之間構成嚴重威脅，因此，資安業界認定此攻擊手法屬供應鏈攻擊之一。[5]

(五)小結

綜析供應鏈常見攻擊手法共通點均為鎖定特定企業組織、某網站或軟體服務，將有害文件、程式植入某網站、合法軟(硬)體及資訊服務，透過大企業與上、下游供應商之間的人員、系統認證信任關係，以社交工程進而滲透企業內部網路，伺機竊取機密資訊。

二、資訊供應鏈攻擊案例探討

在《2020臺灣資安大會的供應鏈安全論壇》中指出，近來國內臺灣企業組織多起APT攻擊案例都是從供應鏈下手，突顯駭客相當擅長突破保護機制，[6]因此，藉由供應鏈網路攻擊案例分析，深入探討駭客鎖定目標族群及其攻擊動機：

(一)歐州飛機製造商空中巴士遭駭客竊取文件

2019年9月，全球第9大軍火供應商-歐州飛機製造商空中巴士(Airbus)發生「資料遭未經授權存取」資安事件，其駭客入侵目的想竊取飛機組件的認證流程技術文件，甚至是軍事運輸機A400M的引擎資料，駭客的攻擊目標鎖定英國的引擎製造商勞斯萊斯、法國技術諮詢公司與供應商Expleo公司，以及兩家法國承包商等都是空中巴士供應鏈上的公司，透過這些公司與空中巴士之間的虛擬專用網路(Virtual Private Network, VPN)加密連線，試圖攻擊空中巴士的系統。[7]

許多企業、政府機關為求方便，常提供遠端連線桌面、VPN登入等機制，讓委外廠商進行遠端操作與維運，致使VPN網路的漏洞成為駭客主要入侵管道之一；以中國駭客組織Blacktech為例，利用尚未修補之漏洞取得設備控制權作為惡意程式中繼站，另一途徑攻擊國內供應商或政府機關之對外服務網站，破解員工VPN網路帳號密碼成功滲透內部網路竊取資訊，甚至以多途徑方式取得控制權，藉以向其他單位進行攻擊。[8]

(二)開放原始碼軟體遭植入後門，成為滲透企業的新利器

5 「表單點擊劫持超越勒索軟高、挖礦劫持成2018年首要威脅」(iThome資訊電子報)，https://www.ithome.com.tw/news/128887，(檢索日期：2020年12月3日)。

6 「2020臺灣資安大會的供應鏈安全論壇」(iThome資訊電子報)，https://www.ithome.com.tw/news/139448，(檢索日期：2020年11月11日)

7 「2020年10大資安趨勢6：供應鏈安全」(iThome電子報)，https://www.ithome.com.tw/news/135178(檢索日期：2020年9月27日)。

8 「調查局首度揭露國內政府委外廠商成資安破口的現況，近期至少10個公家單位與4家資訊服務供應商遇害」(iThome電子報)，https://www.ithome.com.tw/news/139504，(檢索日期：2020年11月10日)。

2017年9月，系統清理軟體(CCleaner)是許多資訊科技人喜好使用的免費工具軟體，駭客設定IT人員常使用工具軟體為目標，竄改該軟體並利用供應鏈管道，將攻擊程式散播到許多企業，導致227萬臺電腦受到影響。[9]

2018年7月，德國的巴代利亞廣播公司和北德廣播公司聯合發布了Winnti駭客集團的研究報告，解析駭客鎖定TeamViewer軟體公司、科技公司西門子、Vlve遊戲公司等企業為攻擊目標，以線上遊戲產業為主，設法混入生產環境當中竊取程式原始碼，將惡意程式碼注入廣泛使用的合法檔案，以便後續散播到其他受害者環境。[10]

2020年5月29日《行政院國家資通安全會報技術服務中心》資安新聞發布：駭客鎖定利用NetBeans整合開發環境之電腦為主要攻擊目標，將Octopus Scanner惡意程式植入至開發電腦中，修改編譯程式檔案，讓開發者將惡意程式會一併載入編譯好之檔案，再上傳至GitHub軟體共享平台持續散播。[11]

(三)台積電生產線新機臺遭病毒感染，產線停擺3天痛失26億元

2018年8月台積電新竹一座晶圓廠內，生產線的天車系統(AMHS)部分新接收的機臺遭受勒索病毒(Wanna Cry)感染，因工程師個人疏失面對新接收機臺與導入自動搬運系統，未依標準作業程序先執行隔離掃毒作業再連線，導致病毒利用台積電的全台晶圓連線管理能力，快速感染所有機臺，影響7奈米產線暫時關機停擺，產能受影響3天，損失近26億元。[12]

因此，台積電於2019年7月成立供應商資訊安全協會及在國際半導體產業設備與材料協會(SEMI)成立相關小組，訂定機臺資安標準，除了做好自己的資安工作外，也建構上、下游供應鏈資安環境，使得合作供應商也必須重視資安問題。[13]

(四)小結

透由實例可見供應鏈裡中小企業、製造業及研發人員，都是駭客主要攻擊目標，尤以中小企業居多，原因是中小企業的資安意識及防禦能力較為薄弱，大多都是信任之軟體程式、硬體裝置及與上下游供應商間使用VPN網路、雲端服務等等，成為駭客進行滲透的利器，因此必須要先瞭解當前資安威脅，才可有效防範。[14]

9 「2020年10大資安趨勢6：供應鏈安全」(iThome電子報)，https://www.ithome.com.tw/news/135178(檢索日期：2020年9月27日)。

10 「2020年10大資安趨勢6：供應鏈安全」(iThome電子報)，https://www.ithome.com.tw/news/135178，(檢索日期：2020年9月27日)。

11 「資安新聞」(行政院國家資通安全會報技術服務中心)，https://www.nccst.nat.gov.tw/NewsRSSDetail?lang=zh&RSSType=news&seq=164018，(檢索日期：2020年11月16日)

12 「生產線驚傳遭病毒攻擊停擺 台積電：1天內可以復工」(自由時報-證券產業)，https://ec.ltn.com.tw/article/breakingnews/2509102，(檢索日期：2020年12月10日)

13 「【臺灣資安大會直擊】面對供應鏈資安風險，半導體龍頭台積電設立供應商資訊安全協會」(iThome電子報)，https://www.ithome.com.tw/news/139644，(檢索日期：2020年12月10日)

三、資訊供應鏈攻擊面向剖析

新型態的網路攻擊主流以「供應鏈」及「就地取材(LOTL)」等戰術模式進行，所謂「知彼知已，百戰不殆」，透由文獻探討瞭解其攻擊手法及特定攻擊目標族群，以駭客組織視角去探討資訊供應鏈的潛在資安漏洞：

(一)資訊供應鏈架構

駭客的攻擊不會只針對單一企業進行攻擊，大多會從關係企業作為滲透起點，以資訊產業體系區分為上、中、下游廠商，上游通常為各類資訊設備零組件製造商、軟體程式開發商及資安公司原廠等，中游為經銷商，下游則為直接提供終端用戶各類資訊終端應用產品、資訊服務、維護等供應商如圖3。

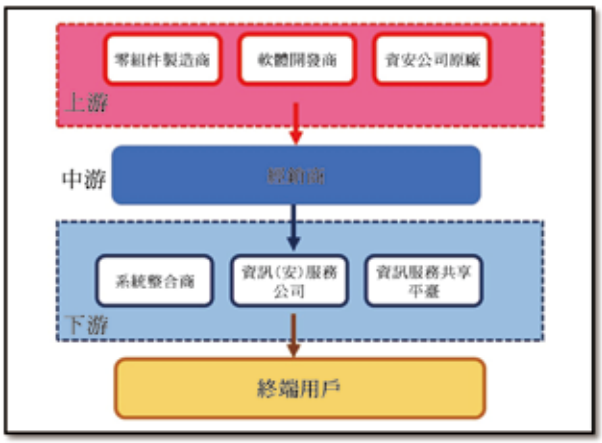

圖3　資訊供應鏈架構圖

資料來源：本研究自行整理。

在國防產業體系下，許多委外軍事應用系統、資訊設備並不是由合約的主承包商獨力研發製造，而是層層轉包其他廠商負責供應某一部分，就像是美國武器製造大廠洛克希德馬丁(LockheedMartin)公司約與1萬6,000家供應商合作，美國國防部約有30萬家供應商，[15]每個廠商規模有大有小，若這些供應商不重視網路安全，也沒有財力投入建立完善資訊安全系統，恐怕遭駭客鎖定滲透，進而成為竊取軍事科技之管道。

(二)潛在資安漏洞剖析

1.不安全的網路共享基礎結構

常見上游製造商、開發人員使用網域名稱服務(Domain Name Service,DNS)、公開金鑰基礎建設(Public Key Infrastructure,PKI)、雲端服務及VPN服務，甚至是員工的私人聯絡方式與下游廠商建立資料交換的橋樑，在不安全的共享基礎結構下，駭客容易藉機駭入暗中進行惡意程式植入、竄改開源軟體程式碼等破解行為。

2.通過企業間信任安全憑證、身分識別

利用廠商彼此間合作信任關係，偽冒、竊取開發人員身分及控制權限，依照使用者習性設計釣魚郵件或網站，獲取中、下游廠商的信任，直接通過安全認證許可，已受感染的合法軟體程式可任意透由供應鏈傳播至其他關係企業。

3.公開發行及提供受感染的軟(硬)體元件

因下游廠商過度信任的錯誤觀念，進而認定上游供應商所製造的合法軟(硬)體元件是安全的，缺乏資安檢測、漏洞修補等機

14 「與其假造不如入侵合法網站，水坑式攻擊成APT最新手法」(資安人科技網)，https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=7413，(檢索日期：2020年12月3日)

15 財團法人國防安全研究院，「2019評估報告國防科技趨勢」，2019/12，頁60。

制，不假思索於網路上公開發行共享，公開網路環境使得惡意程式可快速擴散，作為駭客網路攻擊跳板。

4.測試中或未公開的系統構連

以系統開發商來說，測試中或未公開的系統常為了方便測試及確切掌握使用者需求，且在無完備的防禦機制下，與其他正式系統的線上服務構連建立網路通道，很有可能成為駭客的首要攻擊目標。[16]

(三)小結

在關聯式的資訊供應鏈中，許多軟、硬體的供應商都成為駭客覬覦之目標，以最快速、不易被發現的方式直接滲透，甚至輕而易舉到下游終端使用者，經分析供應鏈裡各企業會以內、外部來定義安全性，網路駭客則是利用兩者之間的信任機制作為滲透管道，尤其是面對必要式的供應服務，更是難以偵測與防禦駭客的攻擊，舉例來說，近期一家網路監控軟體公司(SolarWinds)產品遭駭客滲透，導致美國數個重要政府機構及大型企業淪為駭客供應鏈攻擊目標，該公司軟體產品也列於我國近年的共同供應契約中的政府採購清單，[17]因此，我們必須要認清網路威脅無所不在，信任不代表於一切安全，除了提高對內網端點活動的監測能力外，也必須具備料敵機先、主動察覺與應處各種潛在威脅的能力，才可降低網路攻擊的發生。

國軍資安防護機制現況

為確保國防資訊安全，國軍管控各資訊系統落實「專網專用、實體隔離」之資安要求，由於近年國軍委外研發資訊軟(硬)體、資訊系統工項增加，必須跳脫「國軍網路」是封閉安全的傳統認知，瞭解當前國防供應鏈資安威脅，以供應鏈網路攻擊事件及美國國防部國防廠商網路安全認證等作為借鏡，與我軍現行資安政策相較探討差異性，作為國軍未來資安管控對策參考。

一、現行網路基礎架構

「國軍網路」為全軍共用的資訊交換平台，一旦單位或個人疏於防範而損及軍網安全，將可能危及國軍網路資訊傳遞之安全性，甚至造成軍事機敏資訊外洩之風險，為確保國軍網路安全的情況下，國軍網路以虛擬區域網路(Virtual Locail Area, VlAN)劃分區隔「對外部公開區域」、「隔離網路」及「內部網路」等多個網路環境，使其免於內部網路直接遭受外部之威脅危害如圖4。

(一)對外部公開區域：可稱之為「非軍事區(Demilitarized Zone,DMZ)」，處於網際網路與內部網路中間的區域，通常會設置網頁、電子郵件及DNS等對外公開的的伺服器，扮演著緩衝地帶的角色，與內部網路做切割分離。[18]

16 李善新，「從國際推動趨勢談我國資安治理之挑戰與政策整備」，國土及公共治理季刊，第7卷，第4期(2019/12)，頁12-13。

17 「Solar Winds Orion供應鏈攻擊事件震驚全美，臺灣是否受影響？行政院資安處表示公部門採購皆非受影響產品」(iThome電子報)，https://www.ithome.com.tw/news/141829，(檢索日期：2020年12月29日)。

18 增井敏克，圖解資訊安全與個資保護/網路時代人人要懂的自保術(臺北：碁峰資訊股份有限公司，2019)，頁66-67。

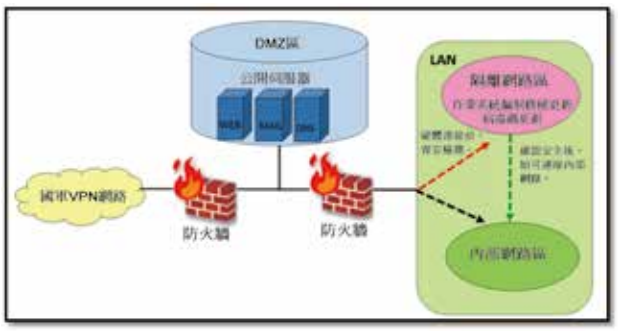

圖4　網路基礎架構圖

資料來源：本研究自行整理。

(二)隔離網路：若純粹以防火牆切割外、內部網路，是無法完全防範內部網路遭受病毒感染之風險，因此，對於新接收資訊系統、軟(硬)體元件在連接內部網路前，需先透過暫時連線的隔離網路環境下進行資安檢測工作，確認安全再連接到內部網路。

(三)內部網路：為國軍各單位內部行政電腦、資訊服務系統等設備使用之區域網路環境，透由單位入口端防火牆防護機制與國軍VPN網路作為區隔。

二、多層防禦資安機制

依網路攻擊模式從外到內部網部環境訂定防禦對策，部署多層式資安管控設備，於各端即時監測及阻擋異常入侵行為，除了可提高防禦效果外，也可爭取受到攻擊所需的應處時間，本節將探討國軍如何部署多層資安防護系統，提升國軍內部網路安全。

(一)出、入口資安對策

1.偵測、防止外部的入侵

區分為「入侵偵測系統(Intrusion Detection System,IDS)」及「入侵防止系統(Intrusion Prevention System,IPS)」等2道防護機制，主要透由IDS偵測判斷來自外部惡意連線，再由IPS阻擋不當連線行為。

(1)IDS：屬防禦型防護機制，於入口端負責對網路與系統監聽網路封包，可偵測惡意及異常行為，如發現異常行為，將自動發出警訊通報，並記錄各種攻擊企圖、行為及結果。

(2)IPS：屬主動型防護機制，當發現網路異常封包、或惡意行為時，會立即阻斷來源IP位址連線。[19]

2.資安區域聯防

結合各區域資安聯防，建立資訊安全防護網，如監控疑似網路攻擊行為可即時通知各區域進行預防，並增設阻擋規則，提升資安事件之預警與應處能力。

3.阻擋不當存取行為

於外、內部網路交界處設置防火牆，扮演著內部網路守門員角色的資安設備，負責監控IP位址連線起迄端、通訊埠進行規則過濾。

(二)內部端點資安管控

1.電腦病毒及惡意軟體之防範

各端電腦系統須安裝防毒軟體，透由檔案特徵與病毒碼比對，偵測病毒、發出警告並予以隔離，除了保持病毒碼更新外，使用者必須正確認知並提高個人資安警覺，跨網資料交換依程序先完成檢疫工作，確認安全始可傳送至國軍內部網路。

2.權限管理

19 增井敏克，圖解資訊安全與個資保護/網路時代人人要懂的自保術，頁62-63。

各電腦設備除須安裝部頒資安管控軟體外，須依使用者權限律定資訊系統及設備的存取授權，防止惡意偽冒、非經授權之不當存取，藉以攻擊國軍內部網路。

3.網路存取管控

各資訊設備網卡須合法註冊使用，透由動態主機組態協定(Dynamic Host Configuraton Protocol,DHCP)服務管控派送IP位址，強制綁定IP與MAC，防範使用者私自竄改IP或未經核准逕自連網，即時掌握區域網路的網路存取情況，如遇非法存取可阻斷連網能力及應變處置回報。

(三)小結

建構資安防護縱深機制，可降低零時差威脅，但現今駭客不會直接從外部做正面攻擊，可藉以委外資訊服務之供應鏈滲透至內部網路，所以國軍資安防護面向不再只是著重於縱向防護，內部端點防護才是最終資安防線，須建構主動偵測能量，才可有效降低網路攻擊之威脅。

三、國防廠商資安管控機制

國軍面臨層層轉包的機制下，必須重新思考對於委外服務的依賴，不能過度信任外部合作資源，須建立評核標準評估資安成熟度，各企業組織已逐漸導入供應鏈的資安評鑑，為提升我國資安防護能力，藉由本節探討美國國防部的國防供應鏈資安稽核機制，與國軍國防廠商安全管控機制相較分析，作為未來訂定國防供應鏈資安稽核機制之參考。

(一)我國各級機關資訊安全等級評鑑

資訊安全是企業應盡的責任與道德的展現，一旦出現資訊安全問題，影響不只是企業本身，連帶的客戶、廠商也會受到影響，導致不可預知的後果；因此，我國為推動國家資通安全政策，建構各機關資通安全環境，將探討我國現行法規範國防廠商資訊安全政策，俾利後續分析窒礙問題。

1.資通安全責任等級分級

依《我國資通安全管理法》目的為推動各機關強化資訊安全管理，其子法提到公務機關及特定非公務機關所涉及業務範疇之資通安全責任等級，由高至低，分為A級、B級、C級、D級及E級[20]，國軍單位依照分級原則按任務及重要性劃分等級及應辦事項如下(如表1)[21]：

(1)國防部本部、各軍種司令部、軍團指揮部及三軍總醫院、國家中山科學研究院等，業務涉及國防安全事項及屬公立醫學中心，列為A級。

(2)軍事院校、軍醫局及各地區國軍醫院，其資通系統服務涉及區域性、地區性與共用性，及屬公立區域醫院或地區醫院，列為B級。

(3)特定非公務機關之國防安全研究院自行辦理資通業務，惟資通系統由國防部代

20 行政院，「資通安全責任等級分級辦法」，資通安全管理法，2019/8/26，第1080184606號，頁2-3。

21 國防部，「國防部及所屬單位暨所管機關資通安全責任等級分級表」，國軍資通安全責任等級分級作業指導，2019/10/8，國通資安字第1080002272號令，頁6-7。

表1　國軍資通安全責任等級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	資安責任等級應辦事項 A	B	C	D	E
管理面	資通系統分級及防護基準		★	★	★		
	資訊安全管理系統之導入及通過公正第三方之驗證		★	★	★		
	資通安全專責人員		★	★	★		
	內部資通安全稽核		★	★	★		
	業務持續運作演練		★	★	★		
	資安治理成熟度評估		★	★			
	限制使用危害國家資通安全產品		★	★	★	★	★
技術面	安全性檢測	網站安全弱點檢測	★	★	★		
		系統滲透測試	★	★	★		
	資通安全健診	網路架構檢視	★	★	★		
		網路惡意活動檢視	★	★	★		
		使用者端電腦惡意活動檢視	★	★	★		
		伺服器主意惡意活動檢視	★	★	★		
		目錄伺服器設定及防火牆連線設定檢視	★	★	★		
	資通安全威脅偵測管理機制		★	★			
	政府組態基準		★	★			
	資安弱點通報機制		★	★	★		
	端點偵測及回應機制		★	★			
	資通安全防護	防毒軟體	★	★	★	★	
		網路防火牆	★	★	★	★	
		具有郵件伺服器者，應備電子郵件過濾機制	★	★	★		
		入侵偵測及防禦機制	★	★			
		具有對外服務之核心資通系統者，應備應用程式防火牆	★	★			
		進階持續性威脅攻擊防禦措施	★	★			
認知與訓練	資通安全教育訓練	資通安全專職人員	★	★	★		
		資通安全專職人員以外之資訊人員	★	★	★		
		一般使用者及主管	★	★	★	★	★
	資通安全專業證照及職能訓練證書	資通安全專業證照	★	★	★		
		資通安全職能評量證書	★	★	★		

資料來源：行政院，「資通安全責任等級分級辦法」，頁5-6。

管，列為D級；另國防工業發展基金會全部資通業務及系統維運均由國防部兼辦，列為E級。

2.資安治理成熟度(Maturity Level)

依《我國資通安全管理法》其子法「資通安全責任等級分級辦法」A、B級特定公務機關之管理面每年須辦理1次資安治理成熟度評估，資安治理成熟度須達第3級以上[22]，以掌握企業資安防護情形，降低資安風險；資安治理成熟度架構包含「策略面」、「管理面」及「技術面」3大面向之11個流程構面為基礎(如圖5)，依流程構面評分能力度，最終評定整體資安治理成熟度等級(如表2)，其等級區分0至5級，共計6級：[23]

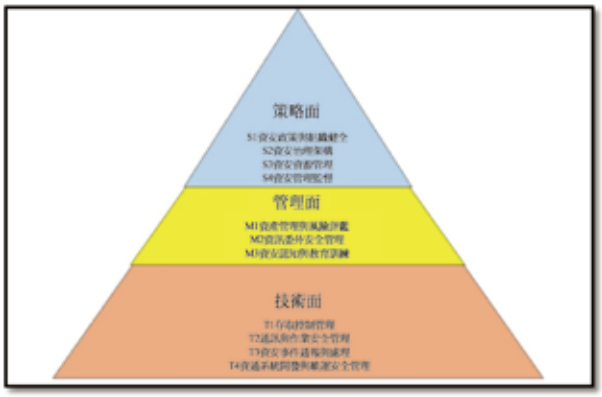

圖 5　資安治理成熟度架構圖

資料來源：本研究自行整理

22 行政院，「國家資通訊安全發展方案-民國106-109年」，行政院國家資通安全會報，2017。

23 林晶瑩，「政府機關資安治理成熟度評估機制」，國土及公共治理季刊，第7卷，第4期(2019/12)，頁80-87。

表2　資安治理成熟度之流程構面分級評估

等級	定義	資安治理三大面向		
		策略	管理	技術
Level 5	創新型(Innovating) 透過識別創新應用、技術、新的機會，來優化資安治理各流程構面	S2資安治理架構		
Level 4	可預測型(Predictable)開始運用歷史資料蒐集與分析建立可預測的流程，持續改善治理流程	S4資安管理監督		
Level 3	制度化型(Established)定義與部署治理流程作業標準化	S3資安資源管理		T3資安事件通報與處理 T4資通系統開發與維護安全管理
Level 2	管理級(Managed) 流程構面已進行管理，包含規劃、執行與監督的過程		M1資產管理與風險評鑑 M2資訊委外安全管理	T1存取控制管理
Level 1	基礎型(Basic) 開始具備基本資安治理執行能力		M3資安認知與教育訓練	T2通訊與作業安全管理
Level 0	未成熟型(Immature) 代表未成熟，不具資安治理能力。	Level 1之任一流程構面能力度為0		

資料來源：林晶瑩，2019/12。〈政府機關資安治理成熟度評估機制〉，《國土及公共治理季刊》，第7卷第4期，頁88。

依《國防產業發展條例》第4條，為了確保廠商服務與供應品質，我國法律設立之國內法人、機構或團體得向國防部申請列管軍品商資格級別認證，須依國防產業專長領域項目、及由公正第三方針對廠商進行級別認證，建立甲、乙、丙級廠商評鑑基準，據以評估廠商參與各等列管軍品研發、產製、維修之總體能量，達到評鑑基準級別，始由國防部實施安全查核並加入國防產業，其級別評鑑事項計7項因素[24]：

(1)科技水準

(2)經營規模及軍品研發、產製、維修經驗

(3)創造國內產值及國內就業機會

(4)產業、學術、研究機構合作及與外國廠商工業合作績效

(5)與外國廠商從事研發、產製、維修合作績效及產品獲原廠認證之證明

(6)誠信履行政府機關(構)契約紀錄

(7)資通安全管理維護紀錄或稽核結果(如表3)

3.列管軍品廠商資通安全維護稽核

表3　國防廠商資格級別「資通安全管理維護紀錄或稽核結果報告」評鑑事項表

評鑑事項	評鑑要點
資通安全管理維護紀錄或稽核結果報告	內部資通安全防護規定及制度。 資通安全維護設施建置及運用。 資通安全維護實際執行情形及成效。 歷史資通安全防護不良紀錄及後續維護紀錄，或政府機關(構)稽核報告結果。 其他與資通安全管理維護紀錄或稽核結果報告有關之重要事項。

資料來源：國防部，「第2章第5條列管軍品廠商資格級別認證辦法」。

24 國防部，「第2章第5條列管軍品廠商資格級別認證辦法」，國防產業發展條例，2020/9/10，第1090191481號。

依《國防產業發展條例》第5條第2項及第4條第3款規定　訂定「資訊安全管理系統之導入」、「資通安全專業證照」、「限制使用危害國家資通安全產品」、「資訊資產管理」、「實體與環境安全」、「資訊作業安全管理」、「存取控制」、「危機處理」等類別資通安全維護稽核檢核項目，鑑別廠商之資通安全管理狀況，為確保列管軍品研製生產維護期間的安全，要求凡申請級別認證之廠商及下游供應廠商須通過資通安全稽核檢核項目為符合條件，查核結果若單一項列為「未符合」時，稽核結果為「未符合」，若稽核項目均列為「符合」或「不適用」時，稽核結果為「符合」。

(二)美國國防部(Department of Defense,DoD)國防供應鏈資安管理

網路安全風險威脅了美國政府及國防工業承包商與國家安全，每年全球因遭駭所損失金額可高達6千億美元[25]，美國DoD為保護國防工業的機敏資訊和智慧財產權，要求競標國防部IT承包商必須具備網路安全成熟度模型認證(Cybersecrity Maturity Model Certification,CMMC)，主要強化國防供應鏈中非機密資訊的保護，此認證須由DOD受權之第三方評估單位，依照承包商的規模大小、專案之機密性，取得相應等級的網路安全能力認證，其認證區分為5等級[26]：

1.Level1基本網路防護(Basic)：能保護好聯邦政府的合約資訊(Federal Contract Information,FCI)，屬於最基本的資安機制。

2.Level2中等網路防護(Intermediate)：有能力保護受管制的非機密資訊，著重於承包商之網路安全程序，確定承包商有效地記錄、管理、審查及最佳化網路安全部署。

3.Level3良好網路防護(Good)：證明有能力保護受控未分類的資訊(Controlled Unclassified Information, CUI)，大致對應於美國國家標準技術研究院(National Institute of Standards and Technology, NIST)發布NIST SP 800-171標準。

4.Level4-5主動防護(Proactive)：證明有能力保護CUI，並能降低進階持續性威脅(APT)的風險

(三)我國與美國之國防產業供應鏈資安管控機制差異分析

綜析前段探討我國及美國的國防廠商資安級別評鑑機制後，將歸納以「廠商資格審查」、「資安級別認證」、「執行技術面」、「資安事件通報機制」及「定期稽核」等5層面相較資安管控機制(如表4)，進一步探討我國國防供應鏈資安防護不足之處。

對於網路駭客而言，攻擊國防供應鏈中的第二線分包商比攻擊第一線承包商更有吸

25 「美國國防部將開始要求承包商必須具備網路安全認證」(iThome電子報)，https://www.ithome.com.tw/news/135658，(檢索日期：2021年1月12日)。

26 「CMMC模型認證」，OUSD A&S網站，https://www.acq.osd.mil/cmmc/draft.html，(檢索日期：2021年1月12日)。

表4　我國與美國國防部對國防產業資安管控機制比較表

國別 / 比較層面	我國國防部	美國國防部(DoD)
廠商資格審查	國防廠商須由公正第三方依專長領域完成資格級別評鑑，達到基準級別及保密、資通安全維護查核始可投入國防產業合作。	廠商承接國防部合約前，除了自身要符合NIST SP 800-171規範，也必須要負責其下所有分包商符合規範，只有一家分包商不符合安全標準，該承包商則無法承接國防合約。
資安級別認證	A、B級公務機關每年須辦理一次資安治理成熟度評估；另各級特定非公務機關應辦事項未要求辦理資安治理成熟度評估。	要求所有主承包商及分包商須由第三方依據專案的機密性，而取得不同等級的CMMC安全認證。 承(分)包商可依企業規模大小選擇評定認證級別，要獲得國防部的合約承包商至少須達到Level3級，分包商至少達到Level1級。
執行技術面	要求凡申請級別認證之廠商及下游供應廠商須通過資通安全稽核檢核項目為符合條件。	DoD將CMMC各級別控制項納入新合約，CMMC1級17項、2級72項、3級130項(涵蓋第1、2級控制項)、4級有156項及5級有171項，可作為審核企業是否符合NIST 800-171標準第三方認證。
資安事件通報應處機制	要求國防廠商加入TWCERT/CC資安通報機制；另針對機密專案辦公室發生資訊安全事件時，應立即通報甲方應處。	美國DoD要求所有承(分)包商建立資安事件通報流程，如有任何資安事件，都必須在72小時內通報。[27]
定期稽核	每年須辦理一次資安治理成熟度及企業內部資安健檢評估。 對承(分)包商須定期執行同等之安全查核工作，並依「列管軍品廠商資通安全維護稽核作業要點」鑑別廠商之資通安全管理狀況。	DoD承(分)包商每三年須接受由經核准第三方進行獨立安全評定，並獲得CMMC特定成熟度級別的認證。

資料來源：本研究自行整理

引力，美國DoD推行CMMC模組認證可同時規範第一、二線供應商的網路安全準備度，相較於國軍現行規範參與國防事務之廠商及分包商管控機制，我國未依主承包商、分(轉)包商所負責領域分級評鑑，其所見問題如下：

1.資安責任A級應辦事項適用問題

國軍單位大多列為A級資安責任等級，假設未來若以相對等級要求合作承包商，恐會出現應辦事項適用問題，一般企業若須實踐A級應辦事項必須先投入龐大成本建構，但國防產業分包商多為中、小企業恐怕有窒礙問題；相較於美國DoD以CMMC認證供應鏈上所有國防分包商，只要符合至少第1級即可通過，較適用小規模企業。

2.年度評鑑未依領域分級實施

不論是何種產業領域資安檢核工項均相同，屬於維持性評鑑，對於負責具有機敏性(或一般)事務之廠商無法區分級別差異，相較於美國DoD係屬於進階型評鑑，廠商可依照每年所負責領域不同及經營改革而評估獲取更高級別認證。

3.招標條件未納入資安標準

美國DoD要求競標國防部IT合約之承包商、分包商必須通過CMMC認證符合NIST SP 800-171工業標準規範始可加入國防產業，惟我國國軍針對國防產業IT商招標資格未將企業導入CNS27001或ISO27001國家資安標準認證列為必要條件，無法確認廠商資訊安全基礎完整性。

27 財團法人國防安全研究院，「2019評估報告國防科技趨勢」，頁62。

4.資安通報應變機制未一致

美國DoD要求所有承包商成立資安應變小組，並與其分(轉)包商之間建立資安事件通報流程，如有任何資安事件，都必須在72小時內通報，[28]國軍雖已明訂定國防廠商應建立管理責任與程序，惟僅要求機敏辦公室如發生資安事件時應立即通報甲方應處，針對一般性國防廠商未明確律定，國防供應鏈不論廠商列管性質為何，均應將所有的主承包商及分包商納入規範，俾全面掌握國防供應鏈資安狀況。

(四)小結

由於國防供應鏈裡涉及不計其數的上下游承包商，而每個企業內部網路基礎架構、資安管理政策會因為組織規模大小而有所差異，因此，未來我國必須將整個供應鏈上所有廠商都納為資安規範對象，並於合約訂定廠商的資安成熟評鑑相關作為，方可精進國防供應鏈資安防護機制，確保供應鏈安全。

國防供應鏈資安防護趨勢芻議

隨著全球網路攻擊型態轉變，我國已開始重視供應鏈安全問題，國內部分大型企業也陸續開始導入美國國家標準與技術研究所(National Institute of Standards and Technology,NIST)推行網路安全框架(Cybersecurity Framework,CSF)，前章已歸納出我國國防供應鏈潛在問題，顯見廠商受限於專業技術、財力多寡及認證方資格等因素，導致實行成效不甚理想，亦突顯我國國防供應鏈資安認證機制仍未周延，對國軍未來資訊安全將是一大威脅。

為了確保國防供應鏈資訊安全，首先訂定國防廠商資安審核基準，嚴格把關每一家廠商加入資格，促使廠商在還沒競標前就有資安防護概念，相對也能夠規範自己的分包商；再來訂定我國與主承包商之間交付資安稽核機制，建立零信任架構，確保產品安全交付；最後，於國軍內部網部建構主動偵測能量，可有效察覺APT攻擊潛在風險。

一、國防廠商資安政策審核基準

顧名思義就是必須要先取得門票才可進入會場之概念，針對列管軍品商(含分包商)訂定審核基準，凡從事與資訊相關領域之廠商，須具備資安國際標準認證及達到資安成熟度評鑑標準，始可投入國防產業合作。

(一)奠定資訊安全基礎，成為招標首要條件

現在許多企業組織均以ISO 27001為資訊安全管理標準為基礎核心，依資安法要求資通安全責任等級A、B、C級之公務機關全部核心資通系統須導入CNS27001或ISO27001等資訊安全管理系統標準，[29]惟現行我國針對國防產業IT商招標資格未將企業導入CNS27001或ISO27001認證列為必要條件，主承包商是第一線與國軍合作交流甚密之企業，因此，承包商在競標前必須要先通過資安國際標準認證，始可確保供應鏈品質及安全。

28 財團法人國防安全研究院，「2019評估報告國防科技趨勢」，頁62。

29 行政院，「資通安全責任等級分級辦法」。

(二)訂定資安成熟度評鑑，依領域分類分級規範

資安成熟度評鑑基準項目訂定可參考NIST提出的CSF網路安全框架控制項，像是美國DoD推行的CMMC認證模型各級別評估指標是以NIST SP 800-171標準為核心訂定，可輔助驗證承包商導入NIST SP 800-171程度。[30]

雖然我國資安責任A級政府機關早已推動資安治理成熟度評估模式，成熟度可達到第3級以上，但始終未將國防產業納入評估範圍，導致不易掌握承(分)包商資安治理能力，建議國軍可依《國軍資通安全責任等級分級作業指導》規定，針對國防IT廠商列管資訊系統假定發生資安事件時影響情況結合「資通系統防護需求分級原則」，以「機密性、完整性、可用性、法律遵循性」等構面，對應「高、中、普」防護需求等級作為承包商分類基準[31]，以承(分)包商防護需求等級律定適用成熟度標準評鑑(如表5)，可提供國防部每年對國防供應鏈所有IT廠商辦理資安治理成熟度評估之參考；另針對分包商資安成熟度評估標準，因機密性影響構面嚴重涉及國防安全，不論等級為何必須比照相同標準評估，其餘普級因影響程度輕微屬可容許範圍，因此分包商僅須達到第1級具備基本資安防護能力即可通過。

表5　國防廠商適用資安治理成熟度對照表

防護需求等級 / 影響構面	高	中	普	影響說明
機密性	Level 5	Level 5	Level4	資訊系統發生資安事件時，可能造成系統資料外洩或遭竄改等情事，導致資料機密性受到損害。
完整性	Level4	Level3	Level2	資訊系統委外開發與營運時，若未有效執行資安防護作為，可能會造成系統完整性遭受破壞。
可用性	Level4	Level3	Level2	考量資訊系統故障可容許業務中斷時間及影響業務執行效能降低程度。
法律遵循性	Level3	Level2	Level2	基於機關負有遵守法律規章之責任與義務下，如發生違法情事時，面臨衝擊後果之嚴重程度。

資料來源：本研究自行整理

(三)建構多層網路架構，落實存取權限管控

主承包商所供應之產品及軟體元件多數是由分包商研製，再交由主承包商組成最終件交付，面對多方企業合作關係，必須要求主承包商將網路區分外、內部及核心(重要資料庫、系統)，員工透過外部網路與其他企業聯繫，工控環境(OT)部署在內部網路，其重要資料庫、文件存放於具備存取控制之環境，建構多層式網路架構，每層律定使用者的存取權限，降低遭滲透風險。

30 「2021資安大預測 趨勢6：資安成熟度｜資安成熟度升格為產業落實資安重要議題」(iThome資訊電子報)，https://www.ithome.com.tw/news/142117，(檢索日期：2020年2月2日)。

31 國防部，「資通系統防護需求分級原則」，國軍資通安全責任等級分級作業指導，2019/10/8，國通資安字第1080002272號令。

(四)建立資安通報機制，即時應變降低損害

企業的資安事件處置機制極為重要，主承包商須擔負起監督其分包商OT環境安全外，應與分包商間建立資安事件通報流程，由主承包商成立資安應變團隊，同時納入國軍電腦緊急應變中心通報，只要國防供應鏈中某一廠商發生資安事件，立即雙向通報及緊急應處，防止攻擊範圍擴散及降低災損，其概念如同我國區域聯防機制，可有效掌握各單位資通安全事件。

二、供應鏈交付資安稽核機制

供應鏈網路攻擊事件常見主承包商(以下簡稱甲方)未能監督整體供應鏈安全情況，最終將已遭植入後門程式的設備提供給業主(以下簡稱乙方)，乙方對於新接收設備無相關資安檢測標準程序，未能及早偵測資安潛在風險。

為確保我國國軍網路安全，甲乙方之間必須從預設信任走向零信任交易模式，當甲方依約履行新設備架裝、維修更新等工項，建構安全交付機制是國軍未來資安防護重視的一環。

(一)建立零信任(Zero Trust)架構

許多企業、政府機關以「堡壘式」的網路安全概念，著重於保衛邊境，預設內部網路環境及所有使用者都是安全無虞[32]，但駭客以「人」的慣性作為滲透橋梁，入侵取得企業內部存取權限，在無防備的情況下成功竊取資訊，甚至再跨企業持續攻擊，演變成內外雙向攻擊，因此很多的企業專家都在提倡資安零信任的概念，其核心精神是「Never Trust, Always Verify」。[33]

我國必須先建立零信任架構，從外部國防廠商、駐點維護商至內部使用者，以「角色」做為核心概念，集中控管內、外部網路流量，對每位使用者的存取行為分析、應用存取賦予必須的權限，以最小權限原則管理，活化整體防禦。

(二)建立資安檢測程序

甲乙方最終交付的階段是國防供應鏈最後一道防線，在設備上線前的資安檢測工作是不可忽略的，所以甲方必須建立資安檢測程序，並納入合約附加條件要求乙方通過安全檢測才算是完成履約，讓乙方更重視資安的必要性，層層稽核確保供應鏈安全交付。

資安檢測工作必須在具有獨立、實體隔離的網路環境下執行，因此，在國軍內部網路切割獨立網段作為資安檢測環境，與其他線上設備實體隔離，凡是從乙方交付的軟、硬體(包含修復件)均須先於資安檢測環境中執行病毒碼偵掃、源碼檢測及弱點檢測等基本程序，最後執行漏洞修補工作。

(三)資安健檢結合滲透測試

32 「什麼是零信任？它如何保護特權存取？」(CYBERARK資安網站)，https://www.cyberark.com/zh-hant/what-is/zero-trust/，(檢索日期：2020年2月3日)。

33 「零信任模式勢在必行」(iThome資訊電子報)，https://www.ithome.com.tw/voice/132062，(檢索日期：2020年2月3日)。

國軍資安檢測工作大多藉由已知駭客行為、病毒特徵的定義檔下執行比對，相較滲透測試不同的是，滲透測試如同執行深層的資安健檢，會以駭客的攻擊思維找出潛在的安全漏洞，驗證資訊系統及硬體設備的安全強度，及早發掘弱項予以改善加強防禦能力，相對所需花費的成本、時間會比弱點檢測來的多[34]，對於中小企業的財力較不容易做到，A級非公務政府機關每年須執行資安健檢乙次，建議乙方於合約規範訂定資安健檢必要性，要求甲方每年導入滲透測試，提供測試報告及改善結果作為交付稽核的佐證文件。

三、國軍內部資安防護精進建議

藉由第三章文獻探討瞭解國軍資安防護部署著重於縱深面向，從外到內部建構多層次防禦系統，可提早預警及有效阻擋不明入侵者，但資安防護的部署是朝可阻擋哪些攻擊來規劃，卻忽略本身無法防禦攻擊的弱點在哪，內部端點防護及資安威脅情資整合是國軍目前所缺乏的能量，也是未來資安防護精進地方，成功的資安防護不只是具備對外的防禦能力，必須建構內部主動偵測能量及威脅情資共享機制，並強化單位資安人才培育，才可有效降低各種網路攻擊之威脅。

(一)部署端點防護機制

以現行防毒軟體偵掃模式是單靠病毒特徵碼及惡意行為分析比對，對於像是APT攻擊手法較難以偵測、防禦，構成國軍內部網路潛在風險；《資通安全管理法》於2020年11月增修訂資通責任等級A級之公務機關須部署端點偵測及回應(Endpoint Detection and Response,EDR)機制[35]，EDR可尋找網路中存在可疑的活動，也就是所謂的「灰色地帶」，將相關佐證資料提供人員深入分析、判定行為，輔助國軍資安監控人員執行分析鑑識工作；另一方面對於潛在事件的回應很快，如遇到端點觸發資安事件可即對該端點採網路中斷方式應處，降低攻擊擴散的風險[36]，EDR所扮演的是輔助國軍資安威脅管控機制，可彌補人員專業不足的缺角。

(二)資安威脅情資分享機制

如今資安攻防已是不對稱戰力之網路戰場，除了強化自身資安防禦及主動偵測能量外，必須要意識到平時威脅情資蒐整及共享的重要性，民國107年我國政府正式成立「國家資安資訊分享與分析中心(National Information Sharing and Analysis Center, N-ISAC)」，透過縱、橫向跨領域情資分享機制，可即時得知某產業特有的惡意攻擊行為及程式，甚至可快速識別自身內、外部網路安全現況，於最短時間內加強防護及下達

34 「弱點掃描VS滲透測試，你知道差別是什麼嗎？」(iThome資訊電子報)，https://www.ithome.com.tw/pr/137286，(檢索日期：2020年2月7日)。

35 行政院，「資通安全責任等級分級辦法」，頁5-6。

36 「【面臨層出不窮的持續性進階威脅，端點防護是臺灣資安廠商立足全球市場的新機會】國產EDR展現臺灣資安研發能量」(iThome資訊電子報)，https://www.ithome.com.tw/tech/129245，(檢索日期：2021年2月7日)。

決策，使傳統防禦能力轉變為主動威脅情資運用，提升國家資訊安全整體應變與防護能力。[37]

以N-ISAC作為借鏡，精進國軍現行「安全資訊事件管理平台(Security Information and Event Management, SIEM)為資安威脅情資共享平臺，建立格式標準化與系統自動化之分享機制，其共享對象區分為內、外部單位，內部除既有資通電軍網路環境研析單位外，建議可增納國軍各軍種電腦緊急應變中心，外部建議與技服中心、國網中心及國內、外資安公司等合作，有效取得即時的威脅情資(例如：惡意程式、系統安全漏洞攻擊手法、惡意偵測行為及資安情報等)進行分析，提升情資的完整性及正確性，使國軍有效達到制敵機先之目標。

(三)強化資安專業培訓

如何在最短時間內防止攻擊擴散、恢復資訊服務運作，一直都是國軍部隊訓練的目標，然而現實上常受限於人員專業技術不足、人力及設備短缺等因素致使單位資安維護能量下滑，國軍招募資訊人才不如一般企業來得容易，因此，資安的專業培訓是國軍必須要重視的一環，礙於人員經管制度即便是培育的資安人才，恐怕未來也會接觸非資訊專業的工作，導致人員對職場產生倦怠感，因此，除了藉由委外資訊證照考取課程、資安相關研討會交流及安排定期資訊能力鑑定等培育機會外，必須正視資訊專業人員經管問題，建議各軍種編制資訊專業小組，針對專業人員採目標式的強化訓練，經管調整以專才專用原則規劃，才可維持國軍資安專業能量，提升培育成效。

另現行資訊委外訓練課程都是以輔導證照獲取為優先，建議可增加委外資安危機處理認證相關課程，培育專業的危機處理人員，提升部隊初步處理資安危機能量。

結　　論

近期俄羅斯對外情報局透由美國軟體供應商(SolarWinds)供應政府與各大公司的軟體與服務這條管道，將已植入惡意程式的更新軟體提供給客戶下載並進行駭客攻擊，成功滲透到美國國務院、國土安全部、商務部、財政部及美國著名500大企業，造成美國史上最大的國家級資安威脅[38]，就是「供應鏈攻擊」，利用受信任的供應商當作跳板擴大攻擊範圍，即便是受信任的資訊系統及合作商都有可能會帶來資安威脅，網路駭客恐怕將鎖定國防供應鏈這條管道嘗試透由承辦人員、交付資訊軟(硬)體入侵國軍內部網路，我們應認清供應鏈資安潛在風險及脆弱點，才可有效防禦攻擊提升存活率。

曾任麥道航太駐台代表廖宏祥表示：

37 「國家資安資訊分享與分析中心(N-ISAC)」(行政院國家資通安全會報技術服務中心)，https://www.nccst.nat.gov.tw/NISAC，(檢索日期：2021年5月3日)

38 「SolarWinds Orion供應鏈攻擊事件震驚全美，臺灣是否受影響？行政院資安處表示公部門採購皆非受影響產品」(iThome電子報)，https://www.ithome.com.tw/news/141829，(檢索日期：2020年12月29日)。

「國安威脅不限於實體，網路攻擊對經濟與國安議題皆造成嚴重威脅」[39]，我國在貫徹「資安即國安」的目標下，未來的資安防護趨勢已不單只侷限在外部資安防護，國軍未來整體資安政策必須導入零信任機制，建立甲乙方供應交付的資安檢測程序及部署內部網路主動偵測威脅、資安威脅情資共享及強化資訊專業等能量，透由層層稽核應變機制，確保整體國防供應鏈資訊安全，讓國軍資安防護做到無邊界、無漏洞之目標。

作者簡介

林于令上校，國防管理學院資管系88年班、空軍航空技術學院電戰參謀班96年班、國防管理學院資管系研究所98年班。曾任財務官、資處官、預算官、資訊督導官，現任職國防大學管理學院國管中心財力管理組指參教官。

莊玉雯少校，航院通信電子參謀班102年班。曾任通信官、資參官、網工官、分隊長。現為國防大學空軍指參學院少校學員。

經國號戰鬥機 (照片提供：張家維)

39 「每月對台網攻逾3千萬次 廖宏祥：台灣有權在網路戰行使自衛權」(自由時報電子報)，https://news.ltn.com.tw/news/politics/breakingnews/3388343，(檢索日期：2020年2月8日)。