指定題

DOI:10.6237/NPJ.202204_56(2).0005

淺談新型態「資訊戰」及網路攻防結合運用

On the New Type of Information Warfare and the Combination of Network Attack and Defense

海軍少校　余政倫

提　　要：

一、「資訊安全，人人有責」，隨著國防部開放智慧型行動裝置進入營區，各單位資安防護工作就已落實到每位官兵弟兄身上，智慧型裝置除可加速業務聯繫與協調外，亦可快速得知社會與國際之間各種事件；然中共亦可透過社交工程手段監控持有者，如稍不留意可能讓其獲取軍中資訊或利用假訊息來誤導視聽，官兵應予正視。

二、隨著科技普及，民生電氣用品及商用設備，亦漸漸冠上「智能」或「智慧」二個字，這些設備多具有「物聯網」功能，未來幾年國軍需面臨這類商用物聯網設備大量進入營區，因此有必要及早思考應對之道，以確保資訊網路環境安全。

三、近年來，「資訊戰」已從攻擊「軍事重要設施」，轉變為攻擊「關鍵基礎設施」等民用設備；所以，必須思考面對新型態資訊安全威脅，並持續加強資訊安全防護機制，以減少資訊戰造成的損失。而國軍從資安防護的建置、維持及專業人員培訓，都是必要的手段；畢竟，唯有受過良好訓練的資安攻防人才與觀念，才能將網路惡意入侵的可能性降到最低，確保國軍資訊網路安全。

關鍵詞：物聯網、資訊安全、資訊戰

Abstract

1.With the start of the Ministry of National Defense's policy of opening smart mobile devices into the camp, unit security protection has been implemented for every officer and soldier, but the CCP can also monitor every movement of its holders through social engineering methods, and even obtain military affairs or provide false information to mislead the audience.

2.In the next few years, we will have to face these large numbers of com-

mercial IoT devices entering the military, and we will have to think about how to deal with it to ensure the security of the unit's information network environment.
3. Information warfare has gradually shifted from attacking "critical military facilities" to "critical infrastructure" and other people's livelihood facilities. Therefore, it is necessary to think about what information security protection mechanisms should be used in the face of new information security threats to reduce future information war losses.
Keywords: Internet of Thing、Information security、Information warfare

壹、前言

英國戰略思想家勞倫斯・佛里德曼(Lawrence Freedman)在《戰略大歷史》(Strategy:A History)中提到隨著資訊的日益數位化，即時通信技術應運而生，資訊爆炸也取代了以往的資訊匱乏，成為各國新的挑戰，尤其大量數據資料可以通過公開或非法手段輕易獲得；[1]而網路上各種活動，包括消費、娛樂、人際交流時，這些提供服務的公司，也開始記錄使用者的喜好和習慣。至於國軍人員使用智慧型手機時，部分手機APP軟體如「谷歌地圖」(Google Map)、「臉書」(Facebook)及「推特」(Twitter)等平台，為提供服務也會蒐集人員所在位置等相關資訊，並匯集到伺服器當中；然當這些資料一旦外洩，透過資料的相互交叉比對，就能推測手機使用者身分(如軍、文職)、交友狀況、工作與住家地點或活動位置、型態(如參加軍種年度例行演習等任務)等數據。這些網路公司可利用社交工程手段，進行更多資訊蒐集，並藉由使用者使用之APP軟體，影響其認知、態度與行為。[2]凡此種種對國軍官兵而言，自當謹慎應對、小心防範。

我國《110年四年期國防總檢討》中談到：「隨著資訊科技發展與網路運用普及，網路駭客及惡意程式技術不斷精進，整體資安環境面臨的挑戰不斷提升。敵可運用資訊戰手段，對我國重要資訊網路系統進行滲透及破壞，影響國家正常運作與社會秩序」，[3]顯見國軍早已意識到「資訊戰」手段逐漸趨於多元與新穎，從攻擊「軍事重要設施」，轉變成攻擊政府機關、「企業物聯網」(Internet of Thing，以下簡稱IoT，或「物聯網」)、「雲端運算」(Cloud Computing，CC)、「社群網路服務平台」、「關鍵基礎設施」(Critical Infrastructure，以下簡稱CI)等設施(設備)，凸顯資安攻擊確實令人「防不勝防」。

我國海軍近期積極執行「新一代飛彈巡防艦」、「多功能人員運輸艦」、「潛艦國造」、「高效能艦後續量產」、「快速布雷

註1：Lawrence Freedman著，王堅、馬娟娟譯，《戰略大歷史》(臺北市，商業周刊出版社)，2020年4月，頁251-255。
註2：林雨蒼，〈臺灣面臨新型態資訊戰，不僅是「網軍」那麼簡單〉，端傳媒，2019年4月29日，https://theinitium.com/article/20190429-opinion-taiwan-information-warfare，檢索日期：2022年1月3日。
註3：國防總檢討編纂委員會，《中華民國110年四年期國防總檢討》(臺北市，國防部)，2021年3月，頁40。

艇」等造艦計畫，[4]及持續部署「雄風二、三型」、「魚叉Ⅱ型」攻船飛彈等武器，[5]這些都是中共極欲獲取的重要資訊；另一方面，除人員滲透等實體手段外，網路駭客的攻擊亦從未間斷。因此，國軍需要謹慎思考如何面對新型態資訊安全威脅、需要建立哪些資訊安全防護機制，以減少未來資訊戰造成的損失，這些面向值得國軍幹部確實審慎思考應對。期望透過研究內容，提供官兵面對「資訊戰」不同的思考方向，包含資安防護機制的建置與維持、增加「資安專業」人員及培訓等手段；畢竟，唯有受過良好訓練的資安攻防人才與觀念，才能將惡意入侵的可能性降到最低，確保國軍資訊網路安全，同時有助戰場勝利，這也是撰寫本文主要目的。

貳、資訊戰定義與特性

1991年的「波灣戰爭」，造成國際間對戰爭型態、戰爭原則與作戰準則的轉變，此戰役亦開創以網絡為中心的戰法及軍事事務革新，亦代表著「資訊戰」此一戰爭新型態已經來臨。因此，有必要就「資訊戰」（或稱「網路戰」）定義與特性，做進一步說明，並探討資訊科技對未來戰場影響與作戰模式改變。逐項分析如後：

一、資訊戰定義

（一）「資訊戰」可定義為「對立雙方為爭奪對於資訊的取得權、控制權及使用權，而展開的一種爭戰形式，其目的在於利用這些資訊優勢使對方屈服，或是使對方喪失這類優勢，而達到干擾對方之作用」[6]。美國陸軍對「資訊戰」定義為：「藉由採取影響敵人資訊、資訊相關程序、資訊系統和電腦網路等行動，以奪取資訊優勢；同時，亦須對己方資訊系統採取防護措施[7]；而我國防部則定義為：「運用各種手段影響敵方決策與資訊系統之行動以創造優勢」、「運用資訊科技影響敵方並防護我方指管程序與資訊系統之行動以獲取戰場優勢」[8]。

（二）狹義的「資訊戰」亦可定義為「網路戰」，其內容包括針對敵對國家政府機關、軍事單位、金融機構、私人企業和社群等團體，利用開放性的網絡平台與資訊技術，進行資料竊取、癱瘓系統服務與竄改他人資料等方式，獲得戰場優勢，範圍含括使用資訊技術向對方進行的試探、偵測，以及對上述活動所進行的偵察、干擾、破壞和反利用等反制行動；另為對抗敵方的偵察、引導、指揮、控制、通信、資訊分析、偽裝欺騙和

註4：〈國艦國造願景與商機〉，國防部海軍司令部，2016年6月22日，http://www.taia.org.tw/doc/201606221644403747.pdf，檢索日期：2022年1月5日。

註5：陳宇陽、謝志淵，〈從美軍「多領域作戰」發展探討國軍源頭打擊能力建構與運用〉，《海軍學術雙月刊》(臺北市)，第55卷，第3期，2021年6月1日，頁96。

註6：程文理，〈資訊戰概論〉，國防新聞網，2016年6月26日，http://www.ewmib.com/news.php?news_id=124&cate_id=9，檢索日期：2022年1月5日。

註7：U.S. Army Headquarters, “Information Operations”,2014.12.20, p.18。

註8：袁翌祥，〈資訊戰型態運用於日常生活手段之探究〉，痞客邦，2017年8月11日，https://airwolf1700.pixnet.net/blog/post/343465774-%E8%B3%87%E8%A8%8A%E6%88%B0%E5%9E%8B%E6%85%8B%E9%81%8B%E7%94%A8%E6%96%BC%E6%97%A5%E5%B8%B8%E7%94%9F%E6%B4%BB%E6%89%8B%E6%AE%B5%E4%B9%8B%E6%8E%A2%E7%A9%B6%EF%BC%88%E5%AE%8C%E6%95%B4，檢索日期：2022年1月3日

打擊殺傷等採取的作戰行動，以及對敵方之干擾、破壞和反利用而採取的防範措施等均屬之[9]。

二、資訊戰特性

綜整國內、外有關「資訊戰」之內容論述，有關「資訊戰」特性分析如下：[10]

(一)未來資訊時代的戰爭，不復存在前線與後方的分野、平時與戰時的區別；凡是與電腦網路連線之處，都將暴露在敵方攻擊的威脅下。而資訊在戰爭中扮演的角色，也就是將資訊運用於作戰之中，進而轉變為「資訊戰」的觀念。

(二)在高科技推動下的戰爭型態詭變萬千，為掌握資訊優勢，未來的戰爭運作將可能是：軍隊的行動自由取決於「制資訊權」、作戰目標以破壞敵人資訊優勢打亂敵方決策程序為主、火力運用從面的打擊轉為「點穴作戰」、指揮體系趨於扁平化、整合軍民電子資訊作戰系統及作戰人員的謀略運用與決策角色，將更加多元與重要。

(三)資訊科技在非致命性的作戰中，將扮演極為重要的角色，而資訊戰的直接攻擊屬於非致命性質，其副作用可能不屬於非致命性質，但造成的傷害或經濟損失，並不亞於致命性作戰。例如戰時軍隊通信指管網路若遭到破壞，將可能造成人員傷亡或迫使任務中止；如果是破壞國家經濟運作、公共資訊、電力網、供水系統或國家基礎設施等，其影響層面將更寬廣及嚴重。

(四)資訊時代戰爭的另一特性是與大眾傳播媒體的關係越來越密切，新聞媒體已不再是被動報導一般軍事活動，而是直接參與其中；如2014年俄羅斯併吞烏克蘭克里米亞半島事件，俄羅斯即是利用新聞媒體並結合資訊網路攻勢，並採取非武力方式達成占領克里米亞之目的，網路威力可見一般。[11]

參、新型態資安威脅與網路攻擊事件探討

「世界經濟論壇」(World Economic Forum，WEF)在2021年1月所做的《全球風險報告》(Global Risk Report 2020)中，列出2020年全球風險排名，其中「失敗的網路安全措施」(Failure of cybersecurity measures)位於前10名內，顯見日益複雜和頻繁的網路犯罪或攻擊，將導致經濟中斷、財務損失、地緣政治緊張和社會不穩定，影響範圍小至個人生活，大至國家安全層級。[12]我國政府亦綜整出近年全球重大網路攻擊事件，歸結出包含「個人資料與憑證外洩攻擊白熱化」、「勒索軟體攻擊風險激增」、「IoT與行動式設備資安弱點威脅升高」、「運用進階持續性威脅攻擊竊取資料」、「資安(訊)供應商遭駭將破壞供應鏈安全」及「關鍵資訊基礎設施漏洞造成風險倍增」等6項資安威脅趨勢(如圖一)，[13]均值得國人及

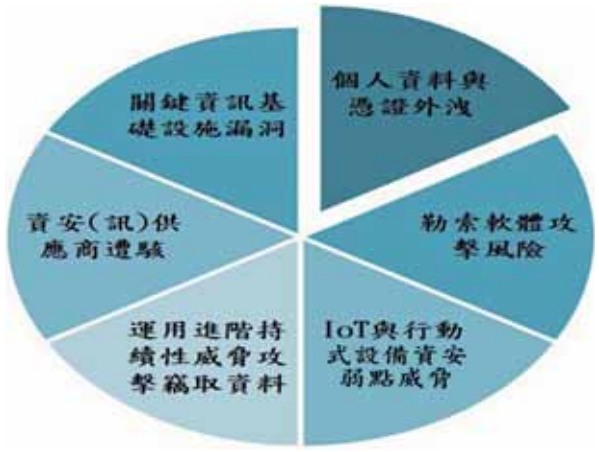
註9：陳志誠，〈資訊戰及其對國家社會安全之影響〉，《資通安全分析專論》(臺北市)，2015年12月，頁4。

註10：楊順利，〈從美國戰略性資訊戰概念論資訊作戰對國家安全之影響〉，《國防雜誌》(桃園市)，第20卷，第11期，2005年11月1日，頁119。

註11：倪一峯，〈俄國對克里米亞混合戰的運用：兼論對我之啟示〉，《國防雜誌》(桃園市)，第33卷，第4期，2018年12月1日，頁45。

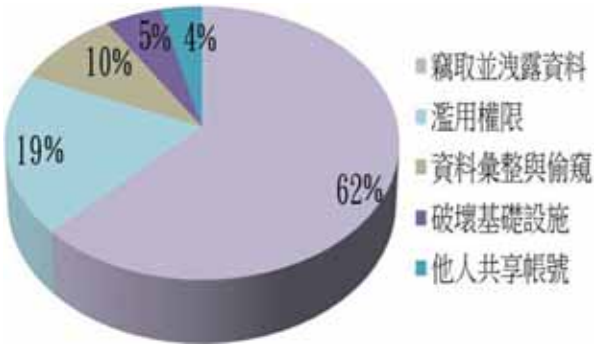
註12：World Economic Forum,“Global Risk Report 2020”, 2021.1.19, P.11、89。

註13：〈國家資通安全發展方案〉，行政院國家資通安全會報，2021年2月，https://nicst.ey.gov.tw/，檢索日期：2022年1月5日。



圖一：近年全球資安威脅趨勢圖

資料來源：參考〈國家資通安全發展方案〉，行政院國家資通安全會報，2021年2月，頁3，由作者彙整製圖。



圖二：Securonix公布109年內部威脅報告圖

資料來源:參考Securonix, " 2020 Securonix Insider Threat Report ", 2020.5, p.4，由作者彙整製圖。

官兵重視，逐項說明如後：

一、個人資料與憑證外洩攻擊白熱化

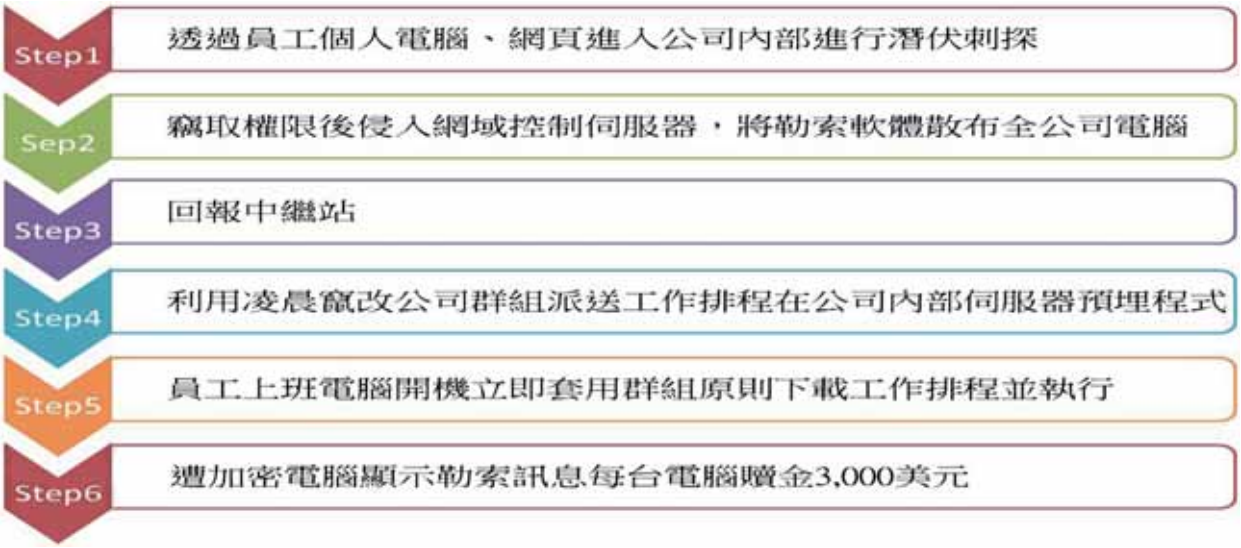
(一)2020年5月資安分析業者「Securonix」公布一份《內部威脅報告》(Insider Threat Report)，說明有關企業內部網路安全及資料外洩的事件中，有六成是由即將離職的員工或約聘人員所造成；其中以竊取並洩露機密資料占百分之六十二最高(如圖二)。從手法上來分析，最常見的是把公司的電子郵件轉寄到個人郵件帳號、濫用雲端權限、彙整資料與下載、使用未經許可的隨身碟等，都是可能的原因。[14]2016年美國民主黨總統參選人希拉蕊・柯林頓(Hillary Clinton)在擔任國務卿期間，因違反要求政府官員之間的通信應做為機構檔案加以保留的規定，使用非聯邦伺服器上維護的官方國務院電子郵件帳戶，而部分郵件被認定屬國家機密並斲傷競選形象，間接造成敗選；[15]此案例殊值國軍官兵同仁借鏡。國軍各單位也常有官兵職務調整或退伍，資訊部門也應特別注意與加強管制，尤其針對即將卸(離)職(或退伍)人員之內部電子郵件、或網路硬碟使用期限與權限查核等程序，才能防止資料外洩情事。

(二)現今許多公司企業允許員工使用雲端工具工作，這也讓員工容易與非企業帳號共享文件，再加上公司各部門之間的政策及工作程序不同，也提高了單位「資訊科技」(Information Technology，簡稱IT)安全團隊處理內部威脅事件的難度。[16]以2019年國內防毒軟體科技大廠「趨勢科技」(Trend Micro)發生員工竊取客服資料庫事件，此資料庫內含有客服工單編號、用戶姓名、電子郵件信箱及部分客戶電話號碼等；這名員工

註14：Securonix , " 2020 Securonix Insider Threat Report ", 2020.5, p.4。

註15：劉致廷，〈希拉蕊電郵門美國國務院列22封郵件為最高機密恐衝擊民主黨初選選情〉，風傳媒，2016年1月30日，https://www.storm.mg/article/80633，檢索日期：2022年1月5日。

註16：郜敏，〈內神通外鬼！資安業者：公司資料外洩六成為內部員工所為〉，Newtalk新聞網，2020年5月27日，https://newtalk.tw/news/view/2020-05-27/412863，檢索日期：2022年1月6日。



圖三：2020年我國重要企業遭勒索軟體攻擊事件流程示意圖

說明：經法務部調查局研判為海外的Winnti Group或與該組織有關聯的駭客，先透過員工個人電腦、網頁進到公司內部竊取特權帳號後，將勒索的加密軟體散布到全公司的電腦，並勒索每台電腦贖金約3,000美元(折合新臺幣83萬元)。

資料來源：參考吳雅瑜、王興中，〈中油、台塑遇勒索軟體 研判海外組織所為〉，公視新聞網，2020年5月15日，https://news.pts.org.tw/article/478979，檢索日期：2022年1月4日，由作者彙整製圖。

將竊得資料賣給外部犯罪組織，而犯罪組織得手相關資料後，便用來撥打詐騙電話牟利，影響近12萬名用戶。[17]因此個人資料與憑證外洩來源不僅可能來自於外部駭客惡意攻擊，更可能源自於內部意外或刻意洩露。

(三)國軍網路雖屬實體隔離網路，可有效遏止外部資訊網路攻擊威脅，[18]但隨著近年部分非機敏服務委民間廠商辦理(如服裝供應系統APP)，因此廠商的系統伺服器將存放國軍人員部分個資，方便提供相關服務並與人員資料核對；若遭惡意人士利用網路入侵或內部員工刻意竊取變賣，將造成國軍人員身分或職務遭揭露，讓有心人士藉機接近或利誘相關業管，進而探取軍中機敏資訊，其影響同樣不容小覷。

二、勒索軟體攻擊風險激增

2020年，國內多間重要能源及科技公司如「中油」、「台塑」及記憶體封測廠「力成」，接連傳出遭勒索病毒攻擊，經研判攻擊行為來自中國大陸駭客組織「Winnti Group」，該組織也預謀對國內企業再度發動勒索軟體攻擊。勒索病毒入侵的途徑相當繁雜，如員工不小心點選釣魚郵件、或遭感染的USB隨身碟被接上公司電腦、或是駭客透過軟體漏洞植入惡意程式等都是可能途徑；而駭客順利進入企業內部網路並竊取電腦

註17：周峻佑，〈內賊難防！趨勢科技驚傳家庭用戶個資外洩，已遭人濫用於撥打詐騙電話〉，iThome電子報，2019年11月6日，https://www.ithome.com.tw/news/134050，檢索日期：2022年1月5日。

註18：李建鵬、陳保佑，〈淺談國軍網路安全防護作為之研究〉，《海軍學術雙月刊》(臺北市)，第55卷，第1期，2021年2月1日，頁128。

帳號權限後，會將病毒擴散至各台電腦，待員工上班開機時，即顯示電腦內存放檔案均遭加密，並藉機勒索現金或加密貨幣(如圖三)。單位要防範勒索病毒肆虐，在事前就必須做好資料備份及異地備援，並將備份資料做加密處理；另在發現病毒的當下，為防止感染擴大，應儘快關機斷網，並保留證據方便讓鑑識單位分析，據以找出來源或做適當損害管控，避免造成內部更多損失。[19]

三、IoT與行動式設備弱點，升高資安威脅

(一)「企業物聯網」(IoT)是現今社會應用最廣泛的技術之一。由於網際網路的無所不在、網路頻寬的不斷成長、連網裝置的多元化，都讓IoT充滿擴充性和多樣性。目前IoT已澈底改變的產業包括生產、製造、金融、醫療及能源；不僅如此，也催生智慧家庭、智慧建築、甚至智慧城市(如圖四)。然而隨著IoT系統及裝置普及在我們生活周遭，亦成為駭客欲從中獲得不法利益之標的，也將衍生更複雜、更大的資安風險。關鍵原因如后：[20]

1. 可蒐集豐富大量的資料：

「物聯網」感應器和裝置會蒐集非常詳細的環境與使用者資料，這些資料對於IoT環境的正常運作來說是必要的；若缺乏妥善保護，一旦遭竊或外洩，將引發連續的不良反應。

2. 虛擬與實體環境密切關連：

圖四：物聯網的應用範疇

資料來源：〈從經濟發展角度來看物聯網〉，每日頭條，2016年10月30日，https://kknews.cc/tech/p444nv2.html，檢索日期：2022年1月4日。

許多IoT裝置都會根據其接收到的環境資訊來做出反應，讓虛擬與實體之間的連結更加緊密。這或許能為使用者帶來便利，但也讓網路威脅更容易造成實體傷害，同時擴大其衝擊層面。

3. 創造複雜的環境：

在IoT環境當中有著相當數量的裝置(如智慧手錶等穿戴裝置)，彼此即時、同步交互作用，雖然可以讓IoT的功能變得多采多姿，但其代價就是造成更大的攻擊面，一旦資料外洩，就成為資安破口。

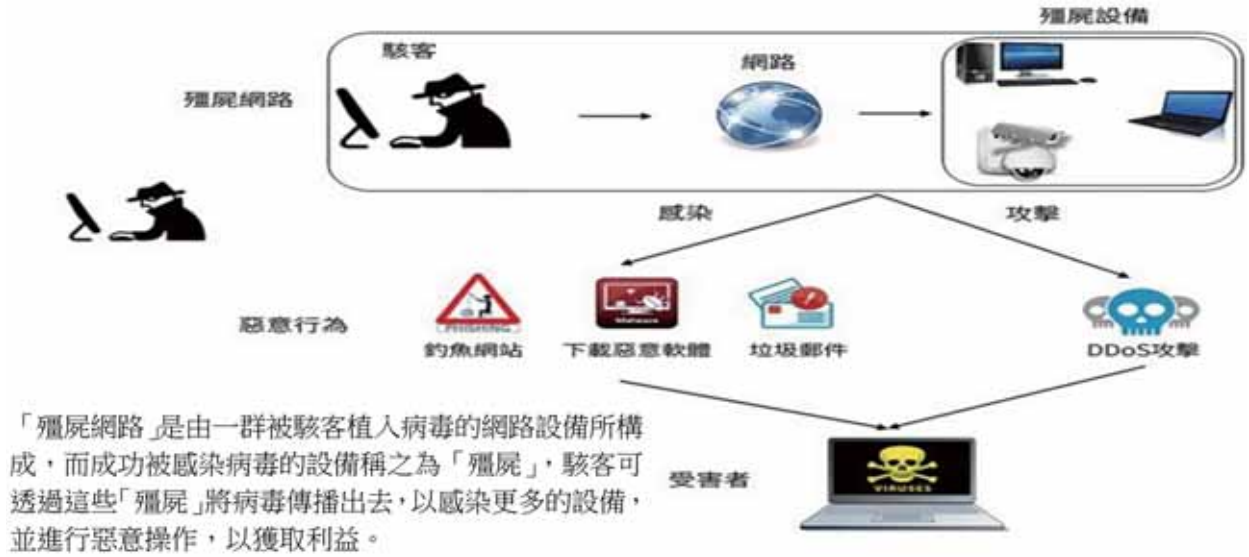
4. 架構集中化：

若將IoT裝置蒐集到的資料都彙整集中到某個工作站或伺服器資料庫上，或許會比建置分開的資料庫更節省成本；但卻會因所有IoT裝置都連回同一源頭，而使得遭到攻擊時影響的層面擴大。

(二)2018年時，就曾發生國外駭客利用

註19：〈勒索病毒如何防範？認識傳播途徑、預防方法，保衛資訊安全！〉，聚碩科技，2020年10月26日，https://www.sysage.com.tw/News/TechnicalDetail/695，檢索日期：2021年11月8日。

註20：〈IoT 物聯網裝置的四個資安風險〉，趨勢科技部落格，2019年6月24日，https://blog.trendmicro.com.tw/?p=60834，檢索日期：2022年1月5日。



圖五：殭屍網路運作結構圖

資料來源：參考〈知己知彼方能因應看清殭屍網路肆虐真相〉，網管人，2019年11月12日，https://www.netadmin.com.tw/netadmin/zh-tw/technology/5F56F8CC54014484878C1F84414C8A9D，檢索日期：2022年1月5日，由作者彙整製圖。

「Mirai」殭屍網路病毒挾持50萬台網路攝影機，並發動「分散式阻斷服務攻擊」(Distributed Denial-of-Service Attack，DDoS)攻陷美國學校的伺服器，造成該校師生繳交作業及評量等網站伺服器長時間中斷服務事件，引發全球譁然(如圖五)。[21]此外，2019年11月在東京舉辦的全球知名「白帽駭客大賽」(簡稱PWN2OWN)，參賽的選手展現破解多項「物聯網」裝置之技術(如手機、路由器及家用智慧裝置等產品)，並揭露其資安漏洞，可見便利的IoT，也會帶來重大的資安危機。[22]

四、運用「進階持續性威脅」攻擊竊取資料

(一)駭客從事「進階持續性威脅」攻擊(Advanced Persistent Threat，簡稱APT)時，可分為下列幾個步驟：[23]

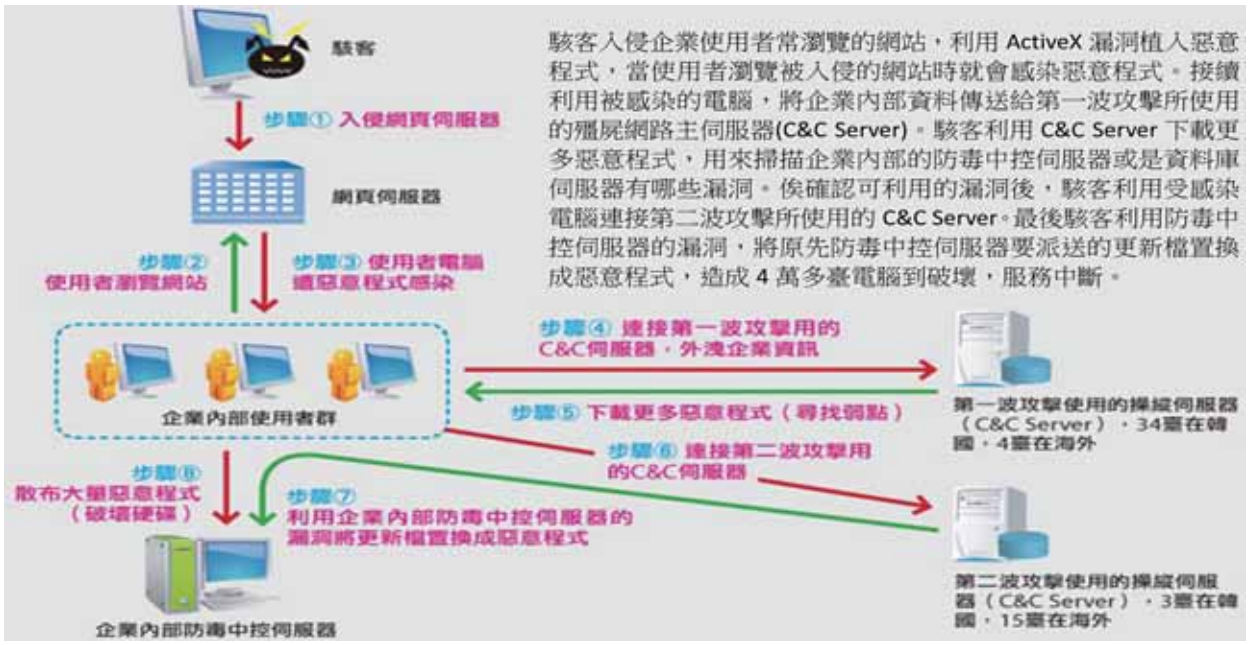
1. 入侵前的資訊蒐集：

蒐集攻擊標的伺服器的弱點或目標人員不良之使用習慣，在APT攻擊過程中占了相當大的比重。例如入侵網站服務，首先查看目標「伺服器回應客戶端數據」(Server

註21：「阻斷服務攻擊(DOS)」攻擊者藉由不當方式占用系統資源(例如CPU)，達到干擾正常系統運作的進行；「分散式阻斷服務攻擊(DDOS)」則利用網路上被惡意程式控制的電腦做為跳板，集中向某一特定的目標電腦送出大量的網路訊息，藉以把目標電腦的網路資源及系統資源耗盡。林妍溱，〈惡名昭彰的殭屍網路病毒Mirai作者之一被判賠償860萬美元〉，iThome電子報，2018年10月30日，https://www.ithome.com.tw/news/126699，檢索日期：2022年1月5日。

註22：陳曉莉，〈Pwn2Own Tokyo 2019：Amazon Echo、三星與Sony電視，以及路由器都被成功入侵〉，iThome電子報，2019年11月11日，https://www.ithome.com.tw/news/134125，檢索日期：2022年1月5日。

註23：「進階持續性攻擊(APT)」是針對特定組織所作出複雜且多方位的攻擊，APT可能會採取多種手段，像是惡意軟體，弱點掃描，針對性入侵和利用惡意內部人員去破壞安全措施。劉家維、李美雯，〈進化中的APT進階持續性威脅〉，國立臺灣大學計算機網路中心電子報，2019年12月20日，http://www.cc.ntu.edu.tw/chinese/epaper/0051/20191220_5104.html，檢索日期：2022年1月4日。



圖六：韓國著名的「320駭客攻擊」事件圖

資料來源：參考〈320韓國黑暗日駭客攻擊手法大剖析〉，iThome電子報，2013年4月30日，https://www.ithome.com.tw/tech/80030，檢索日期：2022年1月7日，由作者彙整製圖。

Response Headers)、「網站瀏覽資訊」(Cookie)內所包含的訊息，確認網頁伺服器的類型與版本，或利用瀏覽器擴充套件、網路安全掃描工具(如Nmap、Shodan)等，以取得攻擊目標伺服器訊息；若攻擊目標為人員，則可利用社群軟體觀察人員的網路活動及習慣，訂製出客製化的社交工程攻擊手法。

2. 滲透防線與對外通訊：

在掌握攻擊目標人員的使用習慣後，利用網路上免費的攻擊工具，製作偽裝過的後門程式放在公開網站上，誘使目標人員下載並執行。例如將惡意執行檔案(EXE)偽裝成其他的檔案格式，如簡報檔案(PPT)、圖像檔案(JPG)或壓縮檔案(ZIP)等，以降低目標人員的資安警覺。

3. 於內部網路進行橫向擴散：

攻擊者利用遭入侵的主機做為跳板，以獲取更高的主機使用權限；甚至針對內部網路防護不足的問題，將後門程式安裝在企業內部網路，擴散後將進一步掌控更多的資訊設施與裝備。

4. 外傳加密資料與清除入侵痕跡：

駭客最後會挑選適當的時機，將重要的資料打包外傳，並清除入侵痕跡，屆時將造成組織的重大損失及事後調查的困難。

(二)2013年3月，南韓遭遇史上最大規模「320駭客攻擊」事件，當日從電視台、銀行、超市到政府機關，累計有4萬8,700台電腦遇駭，造成銀行大量「自動櫃員機」(即ATM)故障、商店營運中斷、政府單位網頁無法瀏覽。經過調查是由北韓主導的有預謀攻擊，且至少是在1年以前就不斷入侵或滲

透目標機關的電腦，並植入各種惡意程式，同時設定在3月20日下午14時一起發動攻擊(如圖六)。該事件為韓國史上最大規模的駭客攻擊，甚至有不少韓國資安業者將這次事件稱為「韓國黑暗日」(Dark Korea)，可見當時網路攻擊影響層面之大，無與倫比。[24]

五、資安(訊)供應商遭駭將破壞供應鏈安全

各種軟體、硬體、網站應用程式、IT服務，部分會採用或搭配第三方供應的技術與服務，由於用戶端無法有效掌握技術或服務資安防護是否足夠，於是也成為駭客突破主要目標防線的一種手段。「供應鏈攻擊」即是駭客設法滲透與攻擊目標相關的軟體開發社群、委外廠商、合作夥伴，如果提供部分服務與元件的第三方資安防禦程度較低，相關人員也無資安防護與威脅意識，就會破壞整體供應鏈安全。[25]近年來供應鏈攻擊事件趨於多元，對軟體類型之攻擊仍為最大宗，其攻擊模式略述如下：[26]

(一)軟體供應商可能本身就是攻擊者。例如買下一家擁有成千上萬企業客戶的軟體公司，便可以利用它的軟體產品做為運送惡意程式的「特洛伊木馬」(Trojan Horse)[27]，並對客戶的電腦系統產生破壞或竊取資料，甚至控制電腦系統。

(二)軟體供應商被攻擊者所駭致軟體產品遭埋入惡意程式。如2020年12月13日爆發的「太陽風(SolarWinds)駭客攻擊」事件，對美國政府機構(財政部、能源部、國土安全部、司法部、國家安全局等)造成有史以來範圍最廣、程度最深的傷害。[28]

(三)軟體供應商的產品使用含「惡意程式」或「具有漏洞」的第三方軟體(如「開源軟體【Open Source Software】」，簡稱OSS，又稱「開放原始碼軟體」)，這種軟體允許使用者修改，故駭客常將該類型軟體植入惡意程式後，提供軟體供應商客製化販售。此外，OSS版本管理與維護機制相對鬆散，所以常存在大量漏洞，易使駭客利用漏洞，將OSS植入惡意程式，造成網路資安風險。

六、關鍵資訊基礎設施漏洞造成風險倍增

(一)「關鍵基礎設施」(CI)範圍相當廣泛，且與民眾生活密不可分，包含能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學園區與工業區等8大領域，而支持CI所需之資通系統稱為「關鍵資訊基礎設施」(Critical Information Infrastructure，CII)，其特色在於需要很長的時間才能夠建構完成；然一旦發生事故

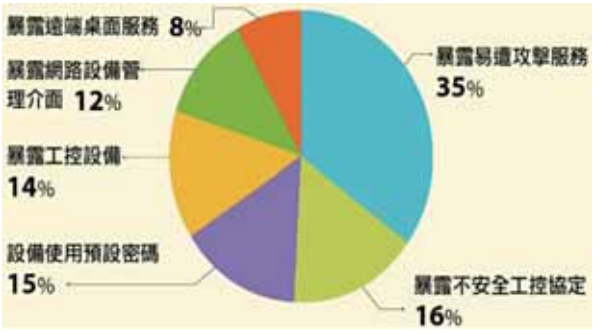
註24：王宏仁，〈韓國史上最大APT駭客事件始末〉，iThome電子報，2013年4月30日，https://www.ithome.com.tw/node/80029，檢索日期：2022年1月5日。

註25：李宗翰，〈攻擊型態趨於多元，供應鏈防護需涵蓋VPN網路與外部服務〉，iThome電子報，2020年1月9日，https://www.ithome.com.tw/news/135178，檢索日期：2022年1月6日。

註26：闕志克，〈供應鏈資安問題的對策〉，自由時報評論網，2021年1月18日，https://talk.ltn.com.tw/article/paper/1426232，檢索日期：2022年1月7日。

註27：「特洛伊木馬」(Trojan Horse)簡稱「木馬」，係在電腦領域中指的是一種後門程式，具有很強的隱秘性，駭客常用該程式來遠端控制或盜取其他使用者的個人訊息或密碼等資料。

註28：闕志克，〈太陽風駭客攻擊事件的啟示〉，i創科技，2021年1月4日，https://itritech.itri.org.tw/blog/hacking_enlightement/，檢索日期：2022年1月8日。



圖七：2020年我國CI資安檢測風險圖

說明：2020年經濟部「國營事業委員會」委託資安公司針對我國多個重要關鍵基礎設施廠站的操作技術(Operation Technology，OT)進行資安檢測，其中暴露易遭攻擊服務的比例高達35%，其次為暴露不安全工控協定和設備使用預設密碼。

資料來源：黃彥棻，〈2020年最大OT風險出爐：35%的關鍵基礎設施曾暴露易遭攻擊的服務〉，iThome電子報，2021年1月12日，https://www.ithome.com.tw/news/142181，檢索日期：2022年1月6日。

，很容易帶來重大影響，包含國家安全、生命健康與環境污染等。[29]

(二)2019年美國一家位於猶他州的「再生能源」(Renewable Energy)電力生產商遭駭客利用防火牆已知漏洞，觸發「阻斷服務攻擊」(Denial of Service，DoS)指令，雖然遭受攻擊後未影響電力供應，但卻造成該公司控制中心與其他各個站點設備之間通訊斷線，無法即時監控與聯繫其他站點情事。[30]此類事件與2020年5月我國「中油公司」爆發遭駭客勒索病毒的攻擊等案件，都再再證明提供關鍵基礎設施服務的廠區資訊系統安全非常重要，任意的中斷服務，造成的影響都十分巨大(資安檢測風險，如圖七)。[31]

肆、因應新型態資訊戰網路攻防建議

我國《110年四年期國防總檢討》中提到：「近年中共已完成軍隊組織調整，並積極提升網路作戰能力，現階段以網軍情蒐集竊取軍、工、商業等資料，並意圖掌握我國關鍵節點，建立攻擊清單，做為後續作戰階段之網路攻擊目標」、「戰時對我國關鍵資訊基礎設施及軍事相關資訊系統發動攻擊，破壞政府運作及造成軍警應變失能，嚴重影響國家安全與社會安定」[32]；由此可知，中共對我國的網路攻擊，已非僅針對軍事或政府機關做為攻擊目標，而是只要能透過網路連結相關設備或裝置使用者，均可成為被攻擊對象，這更凸顯資安防護的重要性。然而國軍中除了「資通電軍指揮部」下轄的「國軍資安防護中心」具備全時監控全軍網路、端點防護及資安稽核等資安防護能量外，[33]對國軍各級同仁而言，亦須認真思考各單位面對新型態資訊作戰方式，仍須加強哪些資安防護手段，才能防止與降低惡意的網路攻擊風險。以下列舉數項精進建議，俾做為強化人員資安意識之參考，期能有助提升資訊安全防護。

一、落實人員資訊安全防護作業與警覺

註29：黃彥棻，〈2020年最大OT風險出爐：35%的關鍵基礎設施曾暴露易遭攻擊的服務〉，iThome電子報，2021年1月12日，https://www.ithome.com.tw/news/142181，檢索日期：2022年1月5日。

註30：〈美國能源公司系統遭遇DDoS攻擊〉，每日頭條電子報，2019年5月7日，https://kknews.cc/zh-tw/world/5nnx463.htm，檢索日期2022年1月16日。

註31：同註29。

註32：國防總檢討編纂委員會，《中華民國110年四年期國防總檢討》，國防部，2021年3月，頁40。

註33：劉嘉偉、張家瑛，〈面對中共網軍威脅國軍資訊網路安全之探討〉，《海軍學術雙月刊》(臺北市)，第55卷，第3期，2021年6月1日，頁126。

表一：資安攻防人才核心知識領域十項課程

資安攻防課程	攻擊手法	防護對策
資安管理常規工作	社交工程	資安政策
資訊安全系統架構	系統漏洞	系統更新漏洞修補
密碼學	網路監看仿冒攻擊	資料加密數位簽章
網路通訊安全	網路掃描阻絕服務	封包加密防火牆
認證、授權與存取控制	奪取權限密碼的竊取	身份認證存取控制
入侵偵測與防護	網路掃描暴力攻擊	入侵偵測
攻擊技術分析	緩衝區溢位阻絕服務	緩衝區處理阻絕服務防範
電腦病毒與惡意程式	特洛伊木馬病毒攻擊	木馬防護病毒防治
弱點掃瞄技術	系統漏洞	弱點掃描分析
資訊法律及道德	—	—

資料來源：林宜隆、花俊傑，〈資安攻防人才核心知識領域之探討〉，《電腦稽核期刊》(臺北市)，第22期，2010年7月20日，頁79-87。

「人」是造成資安事件發生的最主要因素。人員安全威脅的來源對象，分別為不當操作或缺乏警覺心的使用者、違反規定的使用者、惡意意圖的內部(離職)人員等三類，其防範方式如下[34]：

(一)任職前的背景調查

對於單位新進人員應完成適當的身家背景調查，若任職屬處理敏感性、機密性資料的職務，更應謹慎地篩選過濾，妥善完成調查與考核；另外對是否有竊盜前科、是否有財務困難，以及有不良的調(離)職原因等，均須納入任職考核選項，確保參與資安有關人員的資格純淨。

(二)管理與教育訓練

1. 人員在職期間應依國軍相關保密工作規範，賦予機密維護責任，例如簽署保密切結書，並妥善完成職責劃分和職務輪調，俾能相互制衡、防範不良意圖的作用，並由業管有關部門(如政戰、監察、保防等)定期考核與更新人員負責之任務機密屬性。

2. 並非所有的安全事件都是單位人員蓄意造成的，部分是人為錯誤或疏失所導致，包括像資料輸入錯誤、或對資安認知不足而遭社交工程攻擊等。所以要給予操作人員正確的資安觀念與教育訓練(如資安政策、法令規定、作業程序，及如何正確使用系統等)，讓渠等瞭解不但要有責任謹慎操作資訊系統，還要小心防範入侵者，才能降低安全風險。

(三)離(調)職處理

舉凡單位資安或一般人員離(調)職的蓄意報復均屬於惡意威脅，所以各單位對人員離職其安全處置應注意友善的結束工作關係、檢核離職流程、刪除或停止使用帳號、取回單位資產(如個人電腦及網路磁碟資料)及修改伺服器密碼等；儘管手續繁瑣，但卻是防堵惡意資安威脅的基本工作，不容輕忽。

二、持續培育與招募單位資安攻防人才

(一)無論在軍中或民間企業組織，資訊安全工作多交由系統或網路管理等資訊人員

註34：邱瑩青，〈資訊安全的最大威脅-人員安全〉，資安人電子報，2009年8月31日，https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=672，檢索日期：2022年1月4日。

來兼任，但是面對重要資訊安全工作如建置防火牆、入侵偵測系統、防毒軟體的安全設備與產品，若沒有專業的資安人員來負責維護與調整，只依照當初在安裝時所做的預先設定，其防護效果與運作效能都會「大打折扣」；尤其，若缺乏即時的識別、回報與防護能力，到頭來甚至「一無是處」。為強化資安工作，各單位可參考國內學者所綜整的資安攻防人才核心知識領域十項課程(如表一)，依單位特性及人力現況篩選合適課程做訓練，不足部分可透過外聘專講教師或學術研討方式補強，俾奠定單位資安人才養成與進階之基礎。[35]

(二)國軍「資通電軍指揮部」於2017年7月正式編成，目的為建構國軍資訊、通信、電子、資安人力能量，強化國家關鍵基礎設施防護，提升整體網路戰力。[36]該指揮部也負責承辦國軍各單位資安人員資安專業教育訓練流路規劃，並派遣單位人員參加民間資訊(安)教育訓練機構課程充實資安技能，及不定期參與國際資安競賽驗證與發揚國軍資安軟實力。[37]換言之，為吸引民間具備資安專業人員加入資通電軍行列，並讓此類具高技術性資安專長人員能「長留久用」，適時檢討提高其職務加給，應有助增加民間資安人才加入軍旅之誘因與提高專業人員留營意願。

三、提升資訊安全防護設備基礎建設

單位發生資安事件，除了依循「國軍電腦緊急應變計畫」通報外，亦須探討該事件對單位與個人會造成什麼影響？損失有多大？系統服務停擺的時間有多久？分析上述的問題就可以瞭解單位可承受的最大損失範圍，並按照基礎、標準及進階三個階段來設計與建置單位資訊安全防護設備(如表二)：[38]

(一)基礎防護

單位個人電腦均應安裝基本的防毒軟體與資安管控系統(如國軍Kerberos軟體)，方可上線使用；另外個人持有經核可攜入營區智慧型手機亦須安裝與啟用國軍「自動化管理系統」(Mobile Device Management，簡稱MDM)，除禁絕攜帶型裝備於營內不當使用外，亦應加強查察，以降低資安外洩風險。此外負責網站營運或基地(營區)網路單位(如各基地通信隊)，均應建立「防火牆」(Firewall)或「網站應用程式防火牆」(Web Application Firewall，以下簡稱WAF)等網管設備，落實過濾與阻擋不明來源網路位址(Internet Protocol Address，簡稱IP)可能帶來的資安風險。

(二)標準防護

各單位網路管理部門(如資訊室或相關科、組)均有建置自動化入侵偵測與「即時防禦系統」(Intrusion Detection and

註35：林宜隆、花俊傑，〈資安攻防人才核心知識領域之探討〉，《電腦稽核期刊》(臺北市)，第22期，2010年7月20日，頁79~87。

註36：〈國防消息常見問答集〉，國防部，https://www.mnd.gov.tw/PublishTabs.aspx?parentId=10021&NodeId=169006&title=%u570b%u9632%u6d88%u606f&SelectStyle=%u5e38%u898b%u554f%u7b54%u96c6，檢索日期：2022年1月16日。

註37：吳書緯，〈戰力強！國軍代表勇奪美國網安競賽第一嚴德發部長勉「資安即國安」〉，《自由時報》，2021年2月5日，https://news.ltn.com.tw/news/politics/breakingnews/3433513，檢索日期：2022年1月18日。

註38：Scott Wu，〈資安防護設計面面觀〉，Cloudmax部落格，2019年8月28日，https://blog.cloudmax.com.tw/security-protection/，檢索日期：2022年1月6日。

表二：資訊安全防護設備基礎建設計階段一覽表

階段	防護內容	防　護　說　明
基礎防護	防毒軟體	安裝基本的防毒軟體，對於系統的檔案進行即時的防護。
	行動裝置管制	安裝與啟用智慧型手機自動化管理系統，遏止攜帶型裝備遭不當使用。
	防火牆	只允許開放的服務可以在外部進行存取。
	標準WAF	對一般的網頁資料輸入與存取進行過濾。
標準防護	IDP系統	自動將某些已知的威脅擋掉。
	社交攻擊	避免駭客在公司內部植入木馬並直接透過內部網路進行存取。
	防護安全設計檢視	確認所有可以存取的雲端或內部系統，並限制沒被允許狀態下進行存取。
進階防護	進階WAF設定	偵測惡意登入行為或辨識SQL Injection等特殊針對應用程式弱點的攻擊。
	DDoS 防護	透過不同機房、不同設備以及團隊針對不同的攻擊行為做過濾與判斷，已確保網站遭受攻擊時仍能對外營運。
	資料庫防火牆	針對資料庫的存取與寫入進行監控，並過濾掉惡意或可疑的行為。
	加強安全設計	針對現有系統的架構與資料儲存進行檢視。

資料來源：參考Scott Wu，〈資安防護設計面面觀〉，Cloudmax部落格，2019年8月28日，https://blog.cloudmax.com.tw/security-protection/，檢索日期：2022年1月6日，由作者彙整製表。

Prevention，IDP)，自動將某些已知的威脅阻擋過濾，以減低網管人員因人工作業上的疏漏，衍生資安事件。此外，配合國軍「資通電軍」不定期「社交工程電子郵件」(亦稱「釣魚郵件」)派送，以驗證單位人員資安警覺性，這些例行的檢查防護機制，都有其重要性，執行人員均應提高警覺，切實執行相關作業，以維資訊網路安全。

(三)進階防護

藉由司令部等高司單位對下轄所屬單位網站實施弱點掃描，以發掘單位未察覺系統或網站漏洞，進而實施修補與強化。單位伺服器均應建置有異地備援機制，以降低系統受損或攻擊後復原時間，並確保網站遭受攻擊時仍能啟用備援系統來持續提供服務。

四、確保物聯網(IoT)設備安全

國防部近年委託「中山科學研究院」研發「國軍雲」，將具備智慧型營區監偵、車輛管制、進出識別、環境監控、警示等安全管理功能，[39]此即是比照民間單位將相關物聯網設備或系統，逐漸建置到國軍各單位，藉由系統智能化管理，降低人工操作與管理上的疏失。國軍面對這些大量商用物聯網(IoT)設備未來將進入軍隊，必須思考如何積極應對，以確保單位資訊網路環境安全。有鑑於此，國軍建制IoT的資安基本原則(如表三)，建議如下：[40]

(一)蒐集與儲存的資訊都必須詳細規劃

國軍單位在導入物聯網(IoT)之前應須詳細規劃其資料「用途為何？」與「哪些人員可以使用？」；另外儲存的伺服器亦需訂定標準儲存格式，並藉由「資料共享」機制，以減少後續其他單位重複建置IoT系統的成本與時程。

註39：張弘昌，〈國家中山科學院自主研發智慧監偵與管理平台〉，聯合新聞網，2019年7月10日，https://udn.com/news/story/6885/392128，檢索日期：2022年1月6日。

註40：同註20。

表三：物聯網(IoT)設備資安原則一覽表

原則	內　　容
一	所有蒐集的資料和儲存的資訊都必須清楚規劃。
二	每個連上網路的裝置在設定時都確實達到安全。
三	單位的資安策略應建立在駭客已入侵的假設上。
四	每一個裝置都必須受到妥善的實體防護。

資料來源：參考〈IoT 物聯網裝置的四個資安風險〉，趨勢科技部落格，2019年6月24日，https://blog.trendmicro.com.tw/?p=60834，檢索日期：2022年1月7日，作者彙整製表。

(二)網路的裝置操作應符合安全規範

一般物聯網(IoT)裝備會提供預設帳號與密碼，提供使用者對該設備進行一定程度的操作設定，但單位往往設定後未立即更換帳號與密碼，容易成為駭客攻擊目標或變為「殭屍」設備。所以各單位採購建置完成可連網設備後，應立即與定期重新設定帳密；此外應不定期更新設備系統版本漏洞，以防止駭客利用漏洞入侵設備，進行資料竊取或系統破壞。

(三)資安策略應建立在「已遭駭」的前提上

沒有任何防禦作為能百分之百防堵不斷演進的資安威脅，因此單位的資訊部門應將所有物聯網(IoT)系統或裝備，都假設為易遭駭客入侵或攻擊目標，優先管制納入「資訊安全管理制度」(Information Security Management System，簡稱ISMS)，[41]以發掘系統或設備資安風險，進而實施風險管控等防護措施，以消弭資安事件肇生。

(四)裝置均應受到妥善的實體防護

物聯網(IoT)資料伺服器，應建置於單位機房，以提供設備在穩定溫、濕度及供電環境下運作，並方便管理特定人員接觸設備之機會；資料蒐集端設備可依需要加裝具上鎖外盒或者架設在不易接觸之高處，以防非相關或惡意人員可輕易進行破壞或是盜取機敏資料。

五、建立資安(訊)供應商資訊安全管理機制

(一)我國政府為有效管制委外辦理資通系統之建置、維運或提供資通服務時，須要求委外廠商依政府相關資安規定完成自家產品資安防護[42]，其中包含委外廠商查核項目表，以提供政府機關與企業在對供應鏈或委外廠商管理時參考，並列入合約要求及專案的稽核項目。

(二)國際雲端服務供應商如「亞馬遜」(Amazon)、「微軟」(Microsoft)、「谷歌」(Google)、「甲骨文」(Oracle)等大廠，已採用「資安責任共同承擔模型」(Shared Security Responsibility Model，SSRM)，來劃分出雲端服務供應商與客戶間權力與責任。所謂SSRM指可以適用於多元而專案複雜的供應鏈活動或資訊作業委外，透過這些架構客製化每項作業的活動，涵蓋實體環境、系統、帳戶、權限存取、資料、傳輸、日誌、維運及作業(遠程操作)，並提出合宜的資

註41：「資訊安全管理制度(ISMS)」是國際資訊安全標準之一。訂定企業應當如何管理資訊以達到安全的標準，優點在於企業將擁有一套安全且具系統性的方法來保護資訊安全，現今國軍單位均已配合國防部資安政策定期對單位資訊設備或系統實施ISMS管理。

註42：〈資通安全管理法施行細則〉，行政院國家資通安全會報，2018月11月21日，頁1-2。

安規範要求供應商依循，對提出服務需求的企業(甲方)而言，亦可透過SSRM訂出資安自評表與查核底稿，讓供應商(乙方)自評或委請第三方進行資安確信稽核，如此在整個供應鏈中，無論是資訊實施、應用，還是管理和記錄都可以透過SSRM來客製化並落地執行。[43]

伍、結語

「資訊安全，人人有責」。隨著國防部開放智慧型行動裝置入營政策開始，資安防護已落實到每位官兵弟兄身上，智慧型裝置除可加速業務聯繫與協調外，亦可快速得知社會與國際之間各種事件來降低營內與營外資訊不對稱；但對中共而言，極可能透過社交工程手段監控持有者一舉一動，更甚者獲取軍中事務或提供假訊息來誤導視聽，國軍官兵在使用方便的前提下，仍應保持高度警覺，避免個資遭竊，畢竟「影響個人事小、傷害國軍事大」。[44]

新興或新型資訊科技及技術的發展，往往會衍生資訊網路安全問題與風險，此外中共也無時無刻不在利用網路與系統漏洞竊取國軍各種機敏資訊，所以各單位除遵守政國防部所訂定的資安政策外，亦需強化單位內部人員資安觀念、持續培育資安專業人員，及落實資訊安全防護設施更新，唯有將資安防護概念落實官兵行動當中，時時保持資安警覺，並透過完善的資安政策，才能有效提升國軍資安防護能量，才能真正阻絕惡意入侵的機會，確保國軍整體資訊網路安全。⚓

作者簡介：

余政倫少校，國防大學管理學院93年班，國防大學國防管理學院資訊管理碩士101年班，國防大學海軍指揮參謀學院105年班。曾任海軍教育訓練暨準則發展指揮部資訊官、通信官、海軍艦隊指揮部資訊官，現服務於海軍軍官學校。

註43：柯志賢、陳志明、周哲賢，〈從SolarWinds事件看供應鏈資安責任共擔〉，《勤業眾信通訊》(臺北市)，3月號，2021年3月，頁25。

註44：呂兆祥，〈網路空間的新形態作戰模式 虛假訊息攻擊〉，《海軍學術雙月刊》(臺北市)，第54卷，第5期，2020年10月1日，頁143-144。