軍事教育

惡意程式攻擊演進與資訊安全防護分析探討

空軍備役上校　吳嘉龍

提要

國家實驗研究院科技政策研究與資訊中心於第201410004期資通安全電子報報導美國科技公司阿卡邁(Akamai)發表「網路攻擊」排行榜，公布網攻來源地比率，研究顯示，全球有43%的網路攻擊來自中國，排行第一，比率遠超第二名的印尼；美國則以13%排名第三，台灣也以3.7%位居第四名。芬蘭上市資安公司芬安全(F-Secure)指出，從2011年迄今不到3年間，行動裝置惡意程式家族成長高達3倍，在Android平台上共有294個，在各地資安事件不斷發生的刺激衝擊下，政府機關與企業遠比過去更注重資安防護，但是觀察相關因應與作為，似乎仍然無法完全阻擋惡意駭客的入侵，根據Gemalto公布2015年的資料外洩水準指數(Breach Level Index)顯示，2015年全球總計發生1673次資料外洩事件，共約有超過7億筆的資料外洩，然而其中也有多達47%資安事件無法掌握資料外洩程度。而在前述資料外洩事件中，與個資外洩事件相關事件約達53%，且有多達46次重大資料外洩事件的資料遺失量達百萬筆以上，顯見竊取個資依然是駭客獲取龐大經濟的主要來源，顯見面對資訊安全與惡意程式威脅不可不慎。

關鍵字：資訊安全技術、網路威脅分析、惡意程式攻擊、網路管理、資安防護。

壹、前言

隨著人們在網路上進行愈來愈多的學習、分享、聯繫、購物與銀行交易，網路惡意攻擊也迅雷不及掩耳地跟著搭上了這股風潮。全球每年受到網路詐騙的受害者高達數百萬人。事實上，觀察現代戰爭發展趨勢，資訊戰不僅是前哨戰，更成為作戰致勝的關鍵因素。當前恐怖組織、跨國犯罪組織及有心人士都明白運用網路空間的脆弱性，由網路攻擊各國金融、醫療或救災等重要資訊網路系統，乃至依賴這些網路作為神經的重大關鍵基礎設施，不僅更容易且頗具破壞力。此外，極端團體亦可利用網路空間宣傳，招募新成員、募款、提供武器與戰術指導，達致有效組織行動、實施攻擊和擴散其意識形態。此種外部環境的變動，為人們帶來新一波的威脅，對生活與安全造成潛在風險；各國也都意識到網路空間安全的重要性，力圖發展攻防能量。據FBI統計，光美國2012一年發生的網路詐騙案件就有30萬起，金額達5億美金之譜，受害者平均每人的損失金額將近4千美金。手機資安公司「檢查哨」與「小心張望」日前公布最新安卓手機病毒「疫情」，稱有多達1000萬支安裝舊版安卓作業系統的手機，已遭透過產生釣魚網站連結的惡意軟體感染，當中以中國大陸、印度、菲律賓及印尼使用者居多。賽門鐵克安全團隊發現，移動惡意軟體開發者對威脅攻擊進行更新，現可攻擊安卓最新運行系統Marshmallow中的授權模式。在安裝移動應用時，安卓系統的授權模式會向所安裝的應用授予權限，經國內165反詐騙諮詢專線大數據統計分析，目前國內詐騙最多之解除分期付款詐騙案件型態，相關研究指出，這類惡意軟體每月為不肖開發商賺進約30萬美元。近期發現詐騙集團已鎖定資訊安全管理機制較差之網站竊取民眾交易個資，以進行電話詐騙或假拍賣詐騙，而該等網站也因自身安全機制薄弱產生許多虛擬交易糾紛，為能強力監督網站業者改善資安，內政部警政署刑事警察局主動與臺北市政府法務局消保官合作，首次對於發生最多詐騙與糾紛事件網路平臺業者提出要求，分別針對「加強身分驗證機制」、「會員密碼更換機制」、「全面禁止會員私下交易」、「推動賣場巡邏機制」及「全面實施第三方支付制度」等五大面向提出改善作法，如逾期未改善，不排除依據消費者保護法第58條規定處以罰鍰，希望推動第三方警政概念與其他行政機關或民間團體建構有效聯防機制，提升國內網路交易安全及防杜詐騙發生[1]。

貳、中共網軍威脅與日俱增

中國從波灣戰爭及1996年台海危機後，積極發展資訊戰攻防能量，首次資訊

戰演練正式於1997年10月進行，作戰想定是以某軍區集團軍遭電腦病毒(computer virus)攻擊，該集團軍使用防毒軟體進行防護，以避免戰情系統癱瘓。共軍積極發展「電腦網絡作戰」(Computer Network Operations)能力，是建立「非對稱性戰略優勢」的重要環節，其中包括「制資訊權」和「制電磁權」，並以「電子對抗」、「通信對抗」，以及「網絡對抗」為主要內涵之作戰形式。1999年中共網軍一詞首見於解放軍報，網軍初期規模大概為營級，之後網軍規模不斷擴充，包括有攻擊、防衛與維護三大部門，對外國進行資訊滲透、改造與破壞等工作。不同於傳統中共網軍，由以往支援部隊軍事行動為主，已經為了因應中國大陸崛起所必須之政、經、軍、心等需求，逐漸由戰時等特殊時間角色，轉為承平時期不斷對涉及中共相關利益或可利用資源進行技術、專利、乃至於重大政策等情報蒐集，2002年「中國國防白皮書」提到，近年來共軍加快實現由傳統練兵方式向科技練兵的轉變，充分運用現代科學技術組織實施軍事訓練。2002年1月1日組成「科研實驗部隊」，其中將共軍全軍規範為七大類，即陸軍、海軍、空軍、第二砲兵、科研實驗部隊、預備役部隊、武警部隊等，分別研擬訓練大綱體系。中共組建「網軍」部隊新兵種，並且重點培訓具高科技作業能力的優秀人才，列為「863專案」的培植人才。中共在2005年開始將「電腦網路作戰」的攻勢作為列為演習的項目，二砲部隊於2006年還成立電子戰藍軍部隊，以攻防演練的方式大幅增進共軍網路攻擊能力。共軍於2010年7月19日正式成立總參謀部資訊保障基地，該基地為推進共軍資訊化建設科學發展的重要步驟，是深化軍隊改革、加強軍隊資訊化建設集中統管的重大舉措，亦為共軍建制序列中一支戰略資訊支援保障力量[2]。

戰場網路戰是利用網路技術把上至高級指揮所，下至單兵以及各種武器系統的所有軍用電腦聯成一個整體，實現軍隊作戰資訊，網路戰也是把敵方的戰略目標作為首要攻擊對象，如軍隊的C4ISR系統，國家的交通樞紐、通信中樞等等。通過對這些戰略目標的攻擊，直接地影響敵方的戰略決策和戰略全局，以便迅速地達成戰略企圖。網路戰可以導致通信阻塞、交通混亂、經濟崩潰，使作戰指揮不暢、武器失靈等。就國家安全方面而言，資訊網路攻擊可以成為一種強大的軍事武器，它是屬於資訊戰的一環(資訊戰武器包括了電腦病毒、蠕蟲、木馬程式及高能電磁脈衝武器、奈米機器人、邏輯炸彈等)，電腦病毒等的惡意程式將成為新的攻擊手段，在未來戰爭中使用的資訊武器將扮演重要角色。在中共不放棄武力犯臺的前提下，臺灣資訊安全近年開始面臨越來越嚴峻的挑戰，依據大紀元電子報2014年5月20日報導指出，2014年5月19日美國司法部以「網路間諜」罪名起訴5名共軍軍官，指控他們透過網際網路竊取美國高科技產業機密，聯邦調查局追查這5名共軍軍官，發

現都是來自共軍所屬代號為「61398」網路戰部隊成員。在技術不斷翻新，手法越來越多元的情況下，威脅可謂與日俱增。中共自1997年起即積極策劃網路戰力，外界估計其總體戰力約達18萬人。國內政府機關(構)近3年發現、並通報資安事件平均每年約300餘件，可知中共網軍攻擊呈現增加趨勢。為滿足資訊化時代的要求，共軍致力開展信息化建設，政治工作為共軍生命線，為將生命線結合數據鏈，共軍統一建立組織、幹部、宣傳文化等數據庫，並相繼開發涵蓋戰略、戰役、戰術層次，且能適用主戰部隊、預備役部隊、民兵等多種對象需求的政工指揮資訊系統。習近平曾於2015年「全面實施改革強軍戰略」的講話中強調，要構建能夠打贏信息化戰爭、有效履行使命任務的具中國特色現代軍事力量[3]。

在未來資訊化戰場上，計算機網路進攻和計算機網路防禦是計算機網路戰中不可分割的兩個部分，單純的網路進攻和網路防禦都不能達成計算機網路戰的目的。為確保科技進步給人類社會帶來的是便捷而非災害，提出適切的國家網路安全戰略，清楚說明我國在網路空間的安全政策與指導方向，採取更積極有效的行動應對網路威脅，成為政府、企業與民間共同努力當務之急。隨著網路技術與通訊科技不斷地推陳出新，無論是公營機關或企業組織，均有可能面臨資訊安全的衝擊，不僅是機關單位的正常運作、企業的永續經營受到影響，甚或國家的安全亦受到威脅，如何加強資訊安全工作，尤其是網路安全管理，為當前重要課題。網路戰指的是透過網路化的指揮管制將分散配置的力量投入交戰；攻擊節點戰則是要求在作戰目標的選擇上，要著眼於對方作戰體系、作戰網路上的關節點，以造成系統的破壞，即戰爭發起時以破壞對方的通訊網路為首要目標。然而國家網路產業發展，首重資訊安全，工業4.0架構包括物聯網(IOT)及其他許多可在網路上進行的商業活動，因此，如何促進網路安全，以保障這些商業活動不受外來侵擾，儼然成為成功的關鍵。空間技術快速發展，為“網電一體戰”提供了更為廣闊的戰場，現代網電技術裝備日益廣泛地滲透到戰場各個領域，使得各種網路資訊被當作攻擊目標時，其對抗行動的空間範圍將波及整個資訊領域，只要是網路和電磁可及的地方都將成為資訊作戰空間。根據我國交通部統計，台灣是駭客攻擊活動最頻繁的國家，勝過美國、香港和中國大陸，主因是「多數駭客攻擊行為來自對岸」，由於中共可能的犯臺模式以「損小、效高、快打、速決」為戰略指導原則進行資訊攻擊，因此許多活躍的駭客來自大陸網軍，長年滲透台灣的國防、外交、民生(油、水、電)、航管、通信等關鍵系統，入侵規模及深度已構成「準戰爭程度」。目前解放軍已設置了若干資訊兵團，如各軍團組建資訊戰營，還設立了資訊戰武器及戰略之專責研究機構，如解放軍電子科技學院、總參謀部第三分部與資訊戰模擬中心等。而且，還全面規劃相

關訓練課程，使指揮層級軍官了解資訊戰發展，課程內容包括：資訊戰理論、通訊網路技術、電子反制、數位化部隊、資訊戰略戰術及電腦病毒攻擊等[4-5]。

網路戰是指敵對雙方針對戰爭可利用的資訊和網路環境，進行制資訊權的爭奪。資訊作戰由作戰保密、軍事欺騙、心理戰、電子戰、計算機網絡戰、實體摧毀等六大要素構成。通過電腦網路確保己方資訊和網路系統的安全，並蓄意擾亂、破壞與威脅對方的資訊和網路系統。中國在1980年代中期開始發展下一代戰爭的能力，而對資訊戰(或稱信息戰)的研究更是不遺餘力，自1983年起即已對資訊管理及電腦對抗技術方面積極研究發展，並陸續建立了與資訊高速公路聯網的校園資訊網路、作戰模擬系統及初級戰鬥實驗室。自波灣戰爭後中共高層重新體認到高科技戰爭的重要性，除需武器現代化外，一切當以資訊化為基礎，相對的經濟發展亦需現代化，早自1988年起，中國科學院推行三階段為期13年的國家知識創新工程試點工作，希冀提高在科技領域中各種學科的專業能力。美國國防部一份研究報告指出，中共正加緊進行電腦作戰研究，一方面防止其軍事通訊系統遭到干擾，另一方面希望能侵入敵方的資訊系統；這份報告中提出，中共正在研究各種方法，企圖在國

表一、中共網軍竊密作為情蒐方式與手段(自行整理)

網攻竊密作為	中共網攻竊密情蒐方式與手段內容
網路攻擊演練研發網管系統	中共在1997年於北京、南京及蘭州軍區演習，演習中試圖利用電腦病毒干擾、癱瘓、或破壞敵軍廣播及軍事通訊系統。人民解放軍報紙報導，中國大陸必須全力發展高素質的網路鬥士。為防禦其網站遭受來自外部的破壞，中共訊息產業部已成立中國網路安全管理中心，積極研發網路安全管理系統，並開發自主研製作業系統紅旗Linux。
運用正規網軍駭取商業機密	中共網軍自2004年起陸續竊取115家美國大型企業的商業資料，行業涵蓋資訊、電信、航空、能源等。美國資安公司曼迪安特(Mandiant)曾發表報告指出，經長期針對數百次發動「進階持續滲透攻擊」(APT)的追蹤調查，終於掌握共軍進行網路攻擊的證據，並確認其「61398部隊」是最主要的幕後黑手，這支編制可能達數千人的網軍部隊，精通英語及軟體程式編寫，而最近的發展是，他們已將竊密重點轉向高科技產品，尤其是精密無人機技術。
透過資訊分析伺機滲透蒐情	藉由電子郵件、網路社群等途徑詐取資訊或尋找攻堅目標，為中共網軍與情報單位慣用的滲透手法。其常見路徑係透過分析網路上各種公開資料，找尋並鎖定特定的目標，一方面潛伏伺機竊密，另方面則試圖吸收利用。如過去曾發生運用社群網路平台，掌握蒐集個人交友網絡、作息狀況、情緒起伏，甚或工作動態等訊息，進一步分析其任職單位、職務及經手業務，找尋重要目標與弱點，伺機接觸竊密。
攻堅手段多元技術利誘併用	據資料顯示，網軍不僅運用技術強攻，也兼採誘取方法，可以說是軟硬兼施，運用大量投餌方式，針對特定族群散布。例如於個人民網電子郵件接獲不明郵件，要求提供部隊資訊，並承諾給予豐厚報酬。經追查網路其IP均來自中國大陸、香港等境外地區。顯見中共網軍情蒐竊密工作所採取的手段「軟硬兼施」，不放棄任何滲透的機會。

外電腦網路中植入電腦病毒，作為其整體資訊戰戰略的一部份，中共希望具備足夠的電腦作戰能力，以干擾敵軍的指揮系統。美國智庫蘭德研究所的中共國防問題專家穆文能指出，中共軍方最終會發展出電腦網路攻擊的能力。觀察中共黨建思想平台的訊息化發展，其於2003年頒發〈關於進一步推進國家黨委辦公廳系統資訊化建設的意見〉，強調要推進黨建訊息化建設，並在2006年7月推出首個「全國性」黨建網站「中國共產黨新聞網」，後於2010年1月，習近平在「全國」基層黨建工作手機資訊系統正式開通儀式上強調，要將黨建工作透過手機技術推廣應用，「中國共產黨新聞網」另於2013年建置「全國黨建雲平台」，截至2015年3月底已有1070家各類黨組織入駐該平台，微信同名帳號亦同步上線，中共致力於發展「網電一體戰」能量，迄今已建成龐大且實際人數不明的網路戰部隊，中共網軍網路攻擊、竊密的實際作為、情蒐方式與手段說明參考研究整理如表一[6-8]。

參、網路攻防資訊科技發展分析

隨著資訊科技日新月異，資訊化愈發深入公司組織與民間，資訊安全與風險管理儼然成為不容忽視的重要議題。在享受資訊化便利性的同時，必須注意相關資訊資產是否受到妥善保護，並深思背後可能引發的風險問題。如何善用有限資源與有效落實資訊安全管理，是現代科技的重大挑戰。美國以保障資訊安全為重點，確立新世紀軍隊建設的指導構想，制定新的戰略。從總統、國防科學委員會、國防部到各軍種都頒布了有關資訊戰的命令、準則或發表研究報告，以期用新的戰略指導軍隊建設(如建設數位化部隊)和協調國家軍民資訊安全建設。從1993年起，美國相繼建立國家級、國防部級、軍種集合部隊級資訊戰機構21個，僅國防部資訊系統局(Defense Information Systems Agency，DISA)就有44個電腦緊急應變小組(Computer Emergency Response Team，CERT)散佈在世界各地。守勢資訊戰的加固與防範，主要是反干擾、損害管制、反情報、保密與查核。資通管理工作包括有：資通安全政策訂定、資通安全權責分工、人員管理及資通安全教育訓練、電腦系統安全管理、網路安全管理、系統存取控制管理、系統發展及維護安全管理、資訊資產分類及控管、實體及環境安全管理以及業務永續運作計畫管理。資訊安全威脅發展迅速如P2P分享軟體、IM(Instant Message)即時通訊軟體、無線網路風險、社交工程(Social Engineering)攻擊手法寄發惡意電子郵件、網頁掛馬(網頁插入惡意連結內容，使用者不自覺下載惡意程式)、網站釣魚(Phishing)、隨身碟風險(如外接式儲存裝置安全問題)、社群網路與網路勒索[9]。

資訊系統之定義為負責蒐集、處理、傳送、儲存及流通資訊的一組資產，其內

容包括硬體、軟體、網路、員工、實體環境及組織架構，特別強調資產間之關連，並加以群組，以獲得一致的防護水準，用以協助政府機關決策、協調、控制、分析及執行。資訊安全包含有可用性、機密性與完整性三項特性，其中可用性在確保所有經授權的使用者，在需要時，均可以獲得相關資訊或服務；機密性必須確保資料受到妥善保護，只有經授權的人，方能允許存取資訊；完整性在於確保資料之正確性，不會被意外或蓄意改變。資訊安全目的在保護單位的資訊資產，避免遭受各種威脅及降低可能危害，確保單位永續運作，以資訊安全風險定義來說明，風險(Risk)是特定威脅事件發生的可能性與後果的結合，風險管理(Risk Management)是以可接受的費用識別、控制、降低或消除可能影響資訊系統的安全風險的過程。安全控制(Security Control)是指降低安全風險的慣例、程序或機制。資訊防護要確保所有的資訊蒐集、處理與傳輸作業，都必須安全可靠，保護資訊系統與設施，以避免損壞、竊取和濫用。資料應避免招致竊取、破壞或更改。軟體則應實施病毒檢查與其他安全措施。資訊反制是指己方故意提供敵方不正確的資訊，使其造成錯誤的作戰決策；其中利用敵方資訊系統，在其毫無覺察的情況下，使用敵方資訊系統的數據或通信設備。通信必須安全可靠，以防止招致干擾、截聽、中斷或妨害。實施資訊防護，首先須分析己方易受攻擊之弱點，然後計畫性地採取防護措施。依據趨勢科技2013年調查，台灣高科技企業一年365天中，有346天受到駭客入侵，是全球平均220天的1.5倍；而被駭客入侵後，政府長達8.5個月才發現被駭，油、水、電企業8個月、其他高科技企業則要11個月後才知。面對中國18萬網軍部隊威脅，行政院資通安全辦公室在2015年1月12日報告指出，「台灣已成為中國駭客試驗場域、資安環境相當嚴峻」，駭客組織推陳出新的攻擊手法，是造成全球資安事件不斷發生的原因之一，尤其近來興起進階持續性威脅APT(Advanced Persistent Threat)網路攻擊手法，更是難以利用單一資安設備完成防禦阻擋[9]。

趨勢科技報告指出，2016年上半年，勒索病毒已成長172%，而變臉詐騙攻擊造成30億美元損失。依據行政院數據研究顯示，我政府機構每週受到1990多次的駭客網路攻擊，每個月透過電子郵件攻擊的有440次，事實上，軍事目標、電子通訊、電力及能源供應、金融業務及航空管制，均是駭客入侵的目標。故政府除應重視軍事指、管、通、情等系統之安全外，另應有所認知的是民間資訊系統與網路安全如果遭到破壞，後果實不亞於敵方大規模的空襲。因此，如何建構一套完整的安全措施及拓展我國資訊戰略縱深，有效嚇阻中共解放軍的犯台野心，實為重要且值得深思的議題。思科在2016年中的網路安全報告中指出，勒索軟體已成為最賺錢的惡意程式類型，而近期的攻擊案例來看，勒索軟體可能從個人轉向攻擊大型企業，

預期鎖定大型企業進行攻擊的勒索軟體感染能力增加，具備自我散布能力，並要求更高的贖金，企業應做好資料備份以快速回復正常營運。操作勒索軟體Mischa的犯罪集團透過Pastebin公布了競爭對手Chimera的解密金鑰。去年現身的Chimera勒索軟體主要透過電子郵件散布，鎖定小型企業進行攻擊，它除了會加密受害者的檔案並要求贖金之外，也威脅受害者一若不支付贖金將會公布所加密的檔案內容，以提高受害者的付款意願。勒索軟體Mischa犯罪集團入侵了競爭對手Chimera勒索軟體的開發系統，除了偷走程式碼，現在還公布Chimera的3500個解密金鑰，供資安公司開發解密工具，圖一為Chimera勒索軟體主要透過e-mail散布鎖定小型企業進行攻擊示意畫面說明，圖片來源取自Malwarebytes，圖二為No More Ransom提供免費服務說明勒贖軟體畫面示意圖[10]。

圖一、Chimera勒索軟體主要透過e-mail散布鎖定小型企業攻擊(來源Malwarebytes[10])

圖二、No More Ransom提供免費服務說明什麼是勒索軟體(來源No More Ransom [11])

資通安全資訊網(國家資通安全會報)在8月18日第201608003期資通安全電子報報導，資安廠商賽門鐵克研究指出，加密勒索軟體已成為駭客最有效的犯罪獲利模式，以去年來說，全球相關損失就高達新台幣百億元。根據2016年9月3日iThome電週文化報導，2016年臺灣第一季的資安威脅當中，賽門鐵克揭露勒索軟體名列前10大的排名，針對2015年度分析，臺灣面臨垃圾郵件問題的嚴重性位居全球第3名，傀儡網路惡意程式威脅也是名冊全球第3名；臺灣面對勒索軟體威脅，依嚴重程度而言，全球排名第45名，但在亞洲排名為第10名，今年度平均每17名個人或企業當中，就有一個遭到勒索軟體的威脅，較去年同期暴增35%。受到Locky勒索軟體攻擊的產業中，醫療照顧高居第一名，超過7成的受害比例，其次是電信及運輸

業；從國家統計來看，美國是受害最重的國家，日本、南韓分居二、三名，台灣則為第九大受害國家。勒索軟體主要散布的方式是惡意郵件和網頁掛馬，面對勒索軟體威脅的方式，除了有基本的防護軟體、定期更新應用程式安全性外，也要落實完整的備份政策。根據iThome電週文化報導，No More Ransom為一免費服務，包括說明什麼是勒索軟體、運作方式並提供如何防護如Cryptolocker、Teslacrypt、CTB-Locker、Cryptwall等勒索軟體相關資訊，受害者亦可透過該服務作通報，並使用Intel Security、卡巴斯基提供的破解工具。勒索軟體對臺灣帶來的威脅，在受駭嚴重的排名上，亞洲第十名、全球第四十五名，雖然比其他網路威脅受駭程度的排名較為落後，但勒索軟體對企業帶來的損害，卻是更直接且顯著的傷害。根據《路透社》報導，全球金融電訊協會SWIFT透露，駭客正針對使用SWIFT系統的銀行醞釀新一輪網路攻擊。蒐集威脅情資不只僅僅是國家或情報單位才會用到的手法，今日包括企業也開始需要更快掌握更多關鍵的資安情報。雖然安全軟體界及網路高手不斷釋出破解工具，然而勒贖軟體加密及感染手法日新月異，因此專家呼籲定時修補軟體漏洞可大幅降低資安風險，最安全的作法則是養成良好電腦使用習慣，不隨便開啟來路不明檔案或連結，並且要做好資料備份儲存[11]。

資通安全資訊網在8月25日第201608004期資通安全電子報報導，SecureWorks公司報告指出，惡意程式攻擊開始使用新型戰術，即在目標設備上安裝並運行虛擬機器，旨在隱藏自己的蹤跡。這些虛擬機器負責類比檔案系統，且大多數情況下運行在現有作業系統之內。根據電週文化IThome在2016年8月1日研究分析，在此針對美軍以潛水艇作為網路攻擊武器研究探討，Snowden在2013年針對維基百科解密公佈的文件中曾揭露駭客潛水艇USS Annapolis，該潛艇在一周內平均可執行數百次網路攔截行動。華盛頓郵報報導美國海軍打造潛水母艦，能從遠方遙控小型潛水艇以執行阻撓或進行駭客行動。用來偵查、掩飾或攻擊的潛水艇近來也成為美國執行網路攻擊的平台，美國海軍高層已向華盛頓郵報證實了此事。前美國中情局技術人員Edward Snowden在2013年公布的文件中，便有駭客潛水艇USS Annapolis的相關描述，USS Annapolis在一周內平均可執行數百次的網路開採行動。報導指出，美國海軍正著手打造潛水母艦，可於遠方遙控小型潛水艇執行阻撓或駭客行動。負責潛水艇專案的美國海軍少將Michael Jabaley表示，前線潛水艇的參與程度很高，而且具備最高等級的技術，能夠執行任何想要的任務。美國國家安全局的法律顧問Stewart Baker則說，要發動一場網路攻擊行動比防禦它還要容易許多，最安全的作法就是完全與網路隔離。圖三為美軍以潛水艇作為網路攻擊武器，圖片來源：America´s Navy[12]。

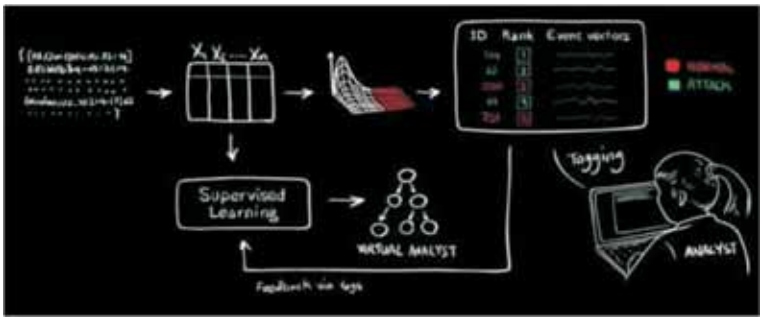
針對無人機與網路相互結合發展研究，美國資安顧問業者Bishop Fox在美國黑帽駭客年會展示利用無人機加上Raspberry Pi打造的網路攻擊無人機，鎖定企業資安防護較脆弱的無線通訊，例如藍牙、訪客Wi-Fi、RFID，只要以無人機遙控停妥於企業辦公大樓頂，就能竊取資料。美國黑帽駭客年會7月30日在拉斯維加斯登場，美國資安顧問業者Bishop Fox的兩位研究人員，利用Raspberry Pi迷你電腦與市售的無人飛機，以500美元的成本，加上自行研發的軟體，研發出被命名為危險無人機(Danger Drone)的概念驗證成品，用來攻擊企業較少投注資安資源的藍芽、訪客WiFi通訊、RFID、Zigbee，以及其他短距離無線通訊裝置。由於這類產品採用的通訊規格多半僅可在短距離內使用，要透過網路傳輸來入侵，則入侵的裝置也必須距離被駭裝置很近，在企業多半有門禁防護下，這類裝置往往在資安防護上仍有漏洞，但透過可遙控飛行的無人機，則可解決此一問題，進而攔截藍芽無線鍵盤或其他裝置傳輸的資料，甚至是取得這些裝置的控制權。該公司研發此無人網路攻擊機的主要目的，在於其業務範圍中的一大項目，便是協助客戶找出其資安防護布局配置的可能弱點，圖四為網路攻擊無人機[13]。

圖三、美軍以潛水艇作為網路攻擊武器(圖片來源：America's Navy[12])

圖四、網路攻擊無人機(圖片來源：電周文化翻攝自Popular Science[13])

軍事學家亞當斯(James Adams)在其《下一場世界戰爭》中強調：在未來的戰爭中，電腦本身就是一種武器，前線無所不在，奪取作戰空間控制權，不是砲彈或子彈，而是電腦網路系統中流動的位元組。網路攻擊適用範圍極為廣泛，網路入侵被廣泛視為係一種對於國家安全、公眾安全和經濟最嚴重的潛在挑戰。針對於人工智慧應用在網路攻擊的預測發展探討，麻省理工學院(MIT)電腦科學暨人工智慧實驗室(CSAIL)及專精於機器學習的新創公司PatternEx近日共同發表一份研究報告，展示了一個新的人工智慧系統AI2(原意為AI的平方，下面均以AI2表示)，其預測

網路攻擊行動的準確度高達85%，為先前系統的3倍。AI2使用非監督式機器學習(unsupervised machine-learning)將資料轉化成有意義的模式，以用來檢查可疑的事件，之後將這些事件交由人類分析師來判斷哪些事件屬於真正的攻擊，再將成果回饋到系統上。該團隊指出，AI2每天所掃描的日誌可拓展至數十億行，將眾多的資料轉換成各種不同的行為類別，再藉以判斷是正常或異常，圖五為MIT電腦科學暨人工智慧實驗室研發人工智慧平台AI2示意圖[14]。



圖五、MIT研發人工智慧平台AI2可準確預測85%網路攻擊行動(圖片來源：電周文化)[14]

肆、面臨資安威脅落實安全防護

美國國土安全部在2010年提出之四年期國土安全檢討報告(Quadrennial Defense Review，QDR)中提到，今日賴以生存之安全環境，已受到4大驅力衝擊。其中一個重要的驅力，就是政府部門與官員不當的網路管理與使用，增加了安全上的風險、侵害個人隱私。同時，惡意行為者也持續利用網路空間弱點，增加重大關鍵基礎設施的風險。這些行為者偷竊了政府的國防與外交等機密資訊、企業的金融資訊、智慧財產、商業機密及其他敏感資訊，也尋求攫取個人資訊與金融資訊。造成安全與執法部門調查與制止作為的實質新挑戰，實極具啟發性。美國聯邦調查局犯罪投訴中心(Internet Crime Complaint Center，IC3)於2016年5月27日公布了2015年的網路犯罪報告，指出2015年總計收到了逾28萬筆的網路犯罪投訴案件，損失金額約為10.7億美元，其中有7838件與商業郵件詐騙(Business Email Compromise，BEC)有關，導致企業損失了2.63億美元，不論是筆數或金額都佔了整體的1/4。歐盟自2001年制定《網路犯罪公約》；聯合國在2015年通過《網路行為準則》。目前國際間對打擊網路犯罪和網路恐怖主義已有高度共識，應透由雙邊、多邊或區域性協議共同應對。我國亦應積極參與加入，善盡國際義務，深化合作交流，以掌握攻擊來源、控制遭駭範圍及反覘個案事例，建立多面向、多維度網路危安預警情蒐能量，致力維護安全和平之網路空間。近年來，實體資產與網路空間結合的「網路—實體聚合」科技發展一日千里，虛擬空間具豐富、多樣化產製及更加便利生活運用的特性；安全維護上國家與非國家行為者可必要結合，例如政府與私部門合作，

以有效應對科技進步而來之實體與網路風險；但亦有治理不良的政府，基於政治、宗教等理由，與恐怖主義組織若有似無地互動。國家必須處理來源多樣化、更加複雜、糾結而不易區隔之混合性威脅，因此，不僅改變了以往軍事上所應對之戰爭形態；亦將戰場上的傳統軍事作戰、游擊戰、反暴動等及必須介入市民社會中運作的維和行動、制止恐怖主義攻擊、打擊組織犯罪等全部結合在一起，且均涉及了影響行動有效與最終決策之廣範圍的「資訊行動」(information operation)。多面向與多空間的防衛與攻擊設計儼然成為發展趨勢，但是此等面向與空間亦是可以被利用的弱點，不僅可影響個人思想，更可激發潛在支持者更大破壞行動，影響不能小覷[15-19]。

美國聯邦調查局(Federal Bureau of Investigation，FBI)犯罪投訴中心(Internet Crime Complaint Center，IC3)於2015年5月27日公布了2015年的網路犯罪報告，指出2015年總計收到了逾28萬筆的網路犯罪投訴案件，損失金額約為10.7億美元，其中有7838件與商業郵件詐騙(Business Email Compromise，BEC)有關，導致企業損失了2.63億美元。從ITRC(Identity Theft Resource Center)公布2016年全球資料外洩報告中，前五個月已共爆發454起重大資料外洩事件，整體資料洩漏數多達12,669,555筆，華盛頓郵報(The Washington Post)於2016年6月15日引述美國民主黨官員報導指出，俄國駭客滲透了民主黨全國委員會(Democratic National Committee，DNC)電腦網路，竊取了該黨對於共和黨總統候選人川普的所有研究資料。協助調查此一駭客事件的CrowdStrike在DNC的同意下揭露了部份事實。CrowdStrike表示，COZY BEAR與FANCY BEAR是全球兩大間諜情報駭客組織，他們有能力繞過許多安全解決方案，能夠不斷變更於目標系統上所植入的惡意程式、切換滲透方法，以及改用其他的命令與控制頻道，以避免遭到偵測。高科技犯罪者無論用何種手段、透過何種管道、入侵何種系統，最終的目的還是在於竊取有利可圖的資料，這些網路犯罪無論是政治、經濟、商業包含資訊行動的混合性威脅，攻擊手法不斷翻新，已經無法依傳統政府各部門的不同職別來應對，防禦措施也應隨時精進，且各個層級的政府官員、涉及國家生產力而影響綜合國力估算的私部門，若警覺不足，將不自覺陷入此等威脅，而造成難以彌補與無法估計的國家利益損失。美國政府將資安攻擊嚴重程度區分為5級，並責成FBI、國家網路調查聯合行動小組為重大資安事件的主要執法、調查單位。白宮發布美國針對重大資安攻擊的緊急應變指導準則，以因應威脅日益升高的網路攻擊。這項由美國總統歐巴馬發出的指導準則確立了美國聯邦政府回應相關資安事件時應依循的規範，明確定義在發生重大資安事件時，政府機構的責任歸屬，同時將重大資安事件定義為可能對國家安全

利益、外交關係、美國經濟、公眾信心、民眾自由或大眾健康與安全發生危害的有關攻擊。新指導原則將美國聯邦調查局、國家網路調查聯合行動小組指派為發生重大資安事件時負責威脅回應活動，如執法、國安調查的負責單位，而國土安全部則負責資產回應相關行動，如提供受影響單位相關必要技術援助以保護其資產不致受損或控制其損害[20-21]。

為了因應網路戰的興起，美國國防部2005年3月所公佈的「國防戰略報告」即明確的把網路空間和陸、海、空、天等定義為同等重要的戰爭場域；美國空軍新近所制訂的「國家網路戰軍事戰略」，也首度將網路空間界定為可以採取軍事行動的一個領域。2006年7月，美國空軍成立了第一支網路戰大隊，其任務是保證美國空軍在戰時和平時都能夠實施網路戰。解放軍的理論家們創造了“網電一體戰”一詞，以描繪把電子戰、電腦網路作戰和動能打擊用於切斷為敵手的作戰和力量投送能力提供支援的戰場網路資訊系統。中國認 ，攻擊信息系統比攻擊傳統的作戰系統更能削弱美國的戰鬥力。一旦台海爆發衝突，破壞美國的衛星可有效癱瘓美軍的作戰能力。美國國防情報局2016年2月警告，要擔心先進的國家行為者，如中國大陸與俄國透過網路空間之介面，不當取得所鎖定之人員、系統與網絡上的知識；且北韓與伊朗也是需要關注的網路攻擊與非對稱性回應之重要威脅者。我國政府團隊對資安工作的推動向來不遺餘力，資安防護策略係採深度、廣度及速度的三維度，包括協助機敏機關強化資安防禦縱深以降低損害，掌握網路威脅情報的目的不只在攻防層次，在攻擊發動前做到預防，讓攻擊者無法發動攻擊；建立資安聯防擴大整體防護網絡，共同防範駭客攻擊；以演練及預警提升機關應變速度，充分落實資安防禦措施[22]。

在最新的戰略競爭演變下，電腦網路本身就是一種武器與戰場。中共現階段軍事戰略核心概念，已調整成為攻防兼備與攻防一體，注重遏制危機和戰爭，中共主要攻擊模式發展趨勢是利用衛星、通資網路偵搜系統來竊取政治、經濟、軍事戰略，並透過電腦病毒、電磁脈衝炸彈攻勢作為，來干擾武器、戰情系統。自2005年起，共軍在演訓中已納入電腦

圖六、行政院國家資通安全會報入前瞻創新作法推升國家資安能量示意圖[23]

網路作戰，並將敵國網路列為打擊目標；而在攻台可能軍事行動選項之「不對稱作戰」方式中，將併用網路戰與資訊戰等手段，對我政、經、軍重要基礎設施及資訊系統實施破壞，癱瘓我指、管、通、資、情、監、偵體系，使國軍無法有效實施反擊。為了建構足夠的網路作戰能量，全球至少已有46個國家成立網路作戰部隊。以美國為例，即在2014會計年度投入數億美元擴大既有的網軍規模並安置所需設備；另外北約組織亦針對如何提高盟國應對現代網路戰爭的能力，以及北約集體的網路安全，召開首次的28國國防部長會議，充分說明資訊戰與網路戰已為當前各國重視的國防議題。資訊戰的攻防中，防衛技術是植基於攻擊的手法而發展，因此教育國軍官兵及一般民眾資訊安全的觀念及建全網路的正確使用方式，才是保障我國資安的最重要工作及目標，圖六為行政院國家資通安全會報入前瞻創新作法推升國家資安能量示意圖[21-22]。

把網路威脅情報依據網路戰爭的角度做分析，可將攻擊者意圖分成三類，可以得到三種不同類型的網路威脅情資；第一類是網路犯罪者(Cyber Crime)，第二類是駭客主義(Hacktivism)，第三類就是網路間諜(Cyber Espionage)攻擊。美國與歐洲充分瞭解建構資安環境與網路戰的重要性，美國國土安全部於2010年9月28日與十二個國家聯合舉行一場代號「網路風暴三號」的大規模網路安全演習，模擬駭客大舉入侵重要網路基建設施，同時也對2009年10月新成立的美國「國家網路安全暨通訊整合中心」進行首次測試，藉以強化美國聯邦、各州、國際和民間部門的資訊共用；在為期三至四天的演習當中，共模擬1500種網路攻擊模式，包括駭客入侵供電、水利系統和銀行等重要基礎建設設施，以測試電腦網路面臨攻擊時的應變能力。歐洲為提高各國應對網路攻擊的能力，歐盟27個成員國和冰島、挪威、瑞士3個非成員國於2010年11月4日聯合舉行名為“歐洲2010網路”的網路戰演練，並由為歐洲網路與資訊安全署和歐盟聯合研究中心規劃。為提升國家資通安全防護能量，我國行政院自2013年起推動技服中心行政法人化，並於2014年5月22日指定科技部為資通安全主管機關，國家資通安全辦公室於2015年8月報導行政院國家資通安全會報推動第四期「國家資通訊安全發展方案」，期透過強化國家資安政策、完備資安管理法規、健全資安防護網、推升資安產業能量、掌握資安防護自主技術及加強國際資安交流合作等，逐步實現「以建構安全資安環境，邁向優質網路社會」之願景[23]。

伍、資訊安全防護管理與結論

網路恐怖主義已是必須防範的重點，而且需要整個社會的參與，從政府到執法

單位到私營部門及全體國民投入，且國際間要擴大合作才可能有效的防範。「九一一事件」後，各國均關心來自恐怖主義組織將會發動網路攻擊之威脅。其原因是當全球強化反恐並較能協同一致作法時，例如控制常規金融體系而使恐怖主義組織不易傳輸經費；且當恐怖分子發現使用傳統對實體攻擊之方式更趨困難且風險更高時，網際網路就可能成為新戰場，或可以當成攻擊的新工具。國家安全戰略之實踐，除有賴強大的軍事實力外，尚須憑藉厚實之綜合國力(指標包含經濟力、軍事力、科技力、區域影響力及國家意志力)做後盾，牽涉範圍廣泛而全面。現代戰爭發展趨勢，資訊戰不僅是前哨戰，更成為作戰致勝的關鍵因素。資訊戰可做到兵不血刃地破壞敵方的指管通資中樞，導致無法動用武器、指揮鏈癱瘓，達到不戰而屈人之兵的效果；若網路一旦遭到癱瘓，不僅政經建設受到影響，可能導致社會動盪，後果相當嚴重。網路空間安全的確保，以及重要關鍵基礎設施的資訊安全防護，成了高難度的戰略挑戰。事實上，人類近20年來面對各式非傳統安全威脅，對於關鍵基礎設施防護的要求，已超過傳統災害風險管理的範疇。尤其是邁入物聯網時代，因其網網相連、相互依賴的特性，可謂沒有網安就沒有國安，尤其值得注意的是，中共對我們的威脅未曾稍減，其軍事整備、部署、竊密、蒐情，亦未因兩岸交流頻繁而有顯著改變。因此，只要兩岸情勢一旦發生變化，中共必將積極藉由網路和通信技術，發動前置攻擊，先期掌握情資，並癱瘓我方軍事系統，獲取戰場優勢。針對國軍資安防護作為探討，面對一場看不見的資訊作戰的戰爭型態，各級部隊要持續強化與深植官兵保密觀念及安全警覺，主動查察、反映問題，以杜絕機密外洩，維護國軍戰力與鞏固國家安全。當前我國家資訊通信安全政策，係依據《國家資通安全會報設置要點》，區分網安、網蒐及網攻三區塊推動。網安體系由行政院國家資通安全會報(資通安全辦公室)指導科技部、法務部及內政部，分別執行網際防護體系及網際犯罪偵防；網蒐及網攻體系，則由國家安全會議指導國安局統合、協調各情報機關執行網際情蒐，由國防部資電作戰指揮部，執行網際防禦(作戰)任務。為期建構完備的國家網路安全法制，相關部門應可參考美國、日本及歐盟等國，制定保護網路空間專法，以確保網路空間的安全。根據中華國土安全研究協會理事長汪毓瑋在民間國安會議專欄研究分析指出，反恐怖與網路安全全面性的網路安全立法內容建議包括以下方向：規定政府與私營部門分享有關網路空間威脅與弱點的重要資訊；鼓勵所有政府部門與相關企業針對所有全國性的關鍵基礎設施採取最佳的實踐與標準化；建立嚇阻恐怖分子與敵對國家進行可能造成重大關鍵基礎設施潛在傷害的網路攻擊戰略；建立可以引導政府採購之標準化與功能性指標，因而可以鼓勵製造商必須更佳的安全標準併入到其產品之中，並可以同時有利於政府與私營

部門維護網路安全[24-26]。

現代戰爭的發展趨勢，資訊戰不僅是前哨戰，更可藉由網路和通信技術，先期掌握情資，癱瘓敵方軍事系統，進而獲取戰場優勢。美國國防部的重要智庫-蘭德公司認為，工業時代的戰略戰是核戰爭，資訊時代的戰略戰主要是網路戰，而這種戰略戰是一種破壞性極大作戰形式，它實施的成敗關係到國家的安危與存亡。面對中共網軍，臺灣現行網路攻防力量由行政院帶領，設有行政院資安小組負責網路安全與防護工作；警政署刑事警察局、法務部調查局負責整合產、官、學、民間專業人士，建構「民間網路攻擊力量」；國安局與國軍相關單位負責攻擊與情報作為。從網路調查發現，確實已有更多恐怖分子使用眾多的網站來支持其發動心理作戰、籌募資金及協調攻擊行動。越是發達及資訊化程度越高的國家，對資訊設施的依賴性就越重，所以在個人方面，首先必須加強對資訊安全的重視及包括APT進階式持續性威脅與DDoS分散式阻斷攻擊等惡意程式的專業認知，才能有效防止這些惡意程式的氾濫；在國家安全方面，應積極研究資訊網路攻擊、防護及反制的方法，以確保國家的安全。網路攻防戰是一場無聲無息的戰爭型態，而且網際網路與電腦的弱點是持續存在，隨著網路科技不斷快速演進，電腦系統連結性與系統漏洞，實存有受到更快速與複雜之網路攻擊工具可以利用的弱點。總而言之，在21世紀網路空間普遍使用的今日，網路攻防也許正無聲無息的進行，因此新一代戰爭形態已儼然形成。當一個國家網路空間及資訊系統遭受入侵或破壞，重則導致系統癱瘓，輕者遭受經濟損失，故擁有網路空間技術的優勢，有助於達成維護國家網路安全的戰略任務。我們必須瞭解資訊戰的攻防中，防衛技術是植基於攻擊的手法而發展，故防衛技術通常是落後於攻擊手法的翻新，因此教育國軍官兵及一般民眾資訊安全的觀念及建全網路的正確使用程式不斷提醒與要求強化防範作為，才是保障我國資安的最重要工作及目標。因應高科技帶來的便利性，國軍逐漸有條件開放智慧型手機，相對資安保密作為更顯得重要。面對資訊安全防護的風險，國軍除持續落實軍、民網「實體隔離」與「專網專用」政策，建置嚴密的資安防護機制，並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，避免透過社群媒體、通訊軟體談論敏感公務或傳輸公文資料，養成高度資安警覺與良好的保密習性，嚴格遵守機密文件保管、傳送、存檔等請遵守加密動作，才能確保國軍整體安全與國家長治久安。面對網路惡意攻擊威脅，政府除藉由「專責機構、專法管理」，統整事權外，亦應投入更多資源，培養專業人才，並有效運用廣儲民間的資安人力，結合產官學研專業能量，建構完善之國家網路安全聯防機制，定期做滲透測試與內稽內控加強了解網站漏洞，並完成漏洞修補，加強資安存取控管，預防對重大關鍵基礎設

施之網路攻擊，完善落實緊急應變作為，重要軍政中心與民生設施尤應建立備援系統適時接替癱瘓系統運作，即時並充分掌握網路威脅情資以面對最新網路威脅，以有效達成捍衛數位疆土，確保網路空間安全的目標[27-30]。

陸、參考文獻

〔1〕國家資通安全科技中心，“2016年第一季全球DDoS攻擊年增125%”，2016年6月26日，http://www.nccst.nat.gov.tw/NewsRSSDetail?seq=15633。

〔2〕國防部政治作戰局保防安全處，“強化資安保密、杜絕機密外洩”，2016年7月25日，取自國防部青年日報社Youth Daily News。

〔3〕陳映禔，“共軍強化幹部政治工作資訊化能力之企圖”，2016年7月24日，取自國防部青年日報社Youth Daily News。

〔4〕楊菁菁，“中共「互聯網+」對黨建工作資訊化的影響”，2016年6月5日，取自國防部青年日報社Youth Daily News。

〔5〕美國國防部，《2010四年期國防總檢報告》(Quadrennial Defense Review Report，QDR)，2010年2月1日。

〔6〕資通安全資訊網，“國家資通安全會報”，2014年1月3日，取自第201401002期資通安全資訊網電子報。

〔7〕國防部青年日報社社論，“完善國家網路安全機制、捍衛數位疆土”，2016年6月15日，取自國防部青年日報社Youth Daily News。

〔8〕蔡輝榮、吳宗　，“面對資訊作戰之準備、發展與　實”，T1：資通安全政策，資通安全專　T96019，2007年。

〔9〕陳曉莉，“駭客過招！公布對手勒索軟體的解密金鑰”，2016年7月29日，取自iThome電週文化。

〔10〕陳曉莉，“思科：勒索軟體轉向攻擊大型企業用戶”，2016年8月1日，取自iThome電週文化。

〔11〕林妍溱，“英特爾、卡巴斯基與歐洲警方聯手推出免費服務對抗勒贖軟體”，2016年7月26日，取自iThome電週文化。

〔12〕陳曉莉，“美軍以潛水艇作爲網路攻擊武器”，2016年8月1日，取自iThome電週文化。

〔13〕陳文義，“美黑帽駭客年會：無人機加上Raspberry Pi打造500美元「網路攻擊飛機」”，2016年8月1日，取自iThome電週文化。

〔14〕陳曉莉，“MIT研發人工智慧平台AI2，可準確預測85%網路攻擊行動”，2016年4月19日，取自iThome電週文化。

〔15〕林盈達，“媒體被駭政府怎能置身事外－資安危機就是國安危機系列之一”，2014年7月22日，取自蘋果日報。

〔16〕編譯崔敬熙／綜合外電報導，“加強防駭、美軍網路特遣隊成立”，2014年10月28日，取自青年日報網。

〔17〕C4ISR Go South著，陳克仁譯，擴大籌建指管通資情監偵戰力(C4ISR Go South)，國防譯粹，40卷5期，35-46頁，2013年5月。

〔18〕Benson，“資安危機就是國安危機系列之三台灣可以成爲資安強國”，2014年7月24日，取自蘋果日報。

〔19〕Robert A. Miller and Daniel T. Kuehl.著，李育慈譯，二十一世紀之網域與「第一戰」(Cyberspace and the “First Battle” in 21st - century War)，國防譯粹，37卷，5期，21-31頁，2010年5月。

〔20〕樊國楨、黃健誠，“資訊安全管理系統要求事項之應然與實然初探「技不如人」還是「要求事項不如人」?”，第二十三屆全國資訊安全會議，2013年5月23-24日。

〔21〕國家資通安全科技中心，“俄國駭客組織入侵美國民主黨全國委員會”，2016年6月16，參考網址：http://www.nccst.nat.gov.tw/NewsRSSDetail?seq=15632。

〔22〕國防部青年日報社社論，“反制多樣化資訊攻擊、肆應混合威脅”，2016年5月25日，取自國防部青年日報社Youth Daily News。

〔23〕國家資通安全辦公室，“入前瞻創新作法，推升國家資安能量”，2015年8月31日，取自行政院國家資通安全會報。

〔24〕汪毓瑋，“【民間國安會議專欄】反恐怖與網路安全”，2015年4月21日，取自民報，http://www.peoplenews.tw/news/bcde0968-c68d-4e69-b4ae-46866a5eb074。

〔25〕戴雅真，“行政院資安處掛牌，強化資安應變效率”，2016年8月1日，取自中央通訊社。

〔26〕國防部史政編譯局譯，蓋瑞・哈特(Gary Hart)，“第四種國力：美國廿一世紀的大戰略”，2008年10月，臺北：國防部史政編譯局。

〔27〕林宗達，“全民皆兵-中共資訊戰之人民戰爭”，2005年5月，臺北：晶典文化事業出版社。

〔28〕楊民青，“新一代戰爭形態正在加快形成”，2016年4月3日，取自新華社世界問題研究中心。
〔29〕黎兆煒，“共軍發展「網電一體戰」之能力虛實研究”，淡江大學國際事務與戰略研究所碩士在職專班碩士論文研究計畫書，2012年1月。
〔30〕黃彥棻，“網路威脅情報正流行”，2016年9月16日，取自iThome電週文化。

作者簡介

空軍備役上校教授　吳嘉龍

學歷：中正理工學院48期電機系電子組，美國空軍理工學院電腦工程研究所碩士，國防大學理工學院國防科學研究所電子工程組博士。經　歷：電子官、區隊長，教官、講師、助理教授、科主任、校教評秘書、副教授、教授、系主任、圖書館館長、資圖中心主任。現職：空軍航空技術學院一般學科部航空電子工程科兼任教授。專長領域：資訊戰、通資安全、無線通訊、網路通訊協定、危機管理。