國軍網路戰部隊發展策略之研究

作者／李建鵬中校、蔣建軍少校

提要

一、肆應現階段複合式作戰環境及與日俱增之網路駭侵威脅，全球各國日益重視網軍之發展，本文以美、俄、日及中共等組建「網軍」之聯合國成員國家，做為本次發展策略研究參據。

二、我國網路戰部隊發展須同步與時俱進，並依據國家作戰需求，針對戰略思維、組織編裝、兵力結構、科研能量及教育訓練等面向逐步調整，以利國軍網路戰部隊兵力發揮不對稱戰力。

三、本文探討我國軍網路戰部隊策略發展現況，並統整網路戰領域專家意見，研擬提出精進作為芻議，期可提供國軍網路戰部隊發展之參據。

關鍵詞：網軍、網路攻擊、網路戰發展策略。

前言

美國著名未來學家托夫勒曾預言:「電腦網路的建立與普及將澈底地改變人類生存及生活的模式，而控制與掌握網路的人就是主宰。誰掌握了資訊，控制了網路，誰就將擁有整個世界。」在現今複雜的作戰環境中，網路多元性(無地域、全時域、隱匿等)及便利性之運用已佔有舉足輕重地位，這也使得破壞網路與保護網路的「網路戰」隨之誕生，未來戰爭的型態將以大規模網路攻擊取代傳統發射導彈的作戰方式。

網路戰為實體戰爭前哨戰，是沒有煙硝的戰爭，亦為陸、海、空、天以外的第五維空間。基此，美國於 2009 年成立「網路司令部(Cyber Command, CYBERCOM)」，負責進行網路作戰並加強防範網際空間之威脅；俄國於 2013 年成立專門打擊網路威脅的獨立部隊，對外界資訊進行監測，以打擊網路威脅；日本於 2015 年成立網路空間防衛隊，強化政府機構及重要基礎設施對網路攻擊之防禦能力；中國大陸近年軍改置重點於「質量建軍，科技強軍」，於 2016 年元旦成立「戰略支援部隊(Strategic Support Force, SSF)」，成為中共陸軍、海軍、空軍及火箭軍以外的第五支新型態「作戰力量」，而美國總統川普亦於 2017 年 8 月 18 日將「網路司令部」，升格為聯合作戰司令部的第 10 部。

要贏得戰爭勝利，就必須要編制具有戰鬥力的部隊；同理，要搶佔網路空間的制高點，就必須要有一支具備網路戰攻、防、蒐能力的部隊。2015 年 9 月美國國防部卡敦中將表示:「面對難以捉摸的網路空間威脅，美國陸軍必須培養更多優質的網路人才。」另外，2017 年 2 月 23 日美國陸軍網路司令部司令納卡索(Paul Nakasone)更明確指出:「具有網路專業知識的官兵，

對陸軍網路部隊來說，將是至關重要。」因此，網路人才的素質，對未來網路戰的影響，將是愈來愈顯著。換言之，網路部隊的整體戰力，將決定誰擁有網路戰場的制高點。[1]而我國於 2017 年「四年期國防總檢討」報告(Quadrennial Defense Review, QDR)亦指出：「國軍將強化資通電作戰能力，以創新不對稱作戰思維，使敵國陷入多重困境，以嚇阻其不輕啟戰端。」[2]

因應世界諸國對於網路戰威脅日益重視，我國網路戰發展亦須同步與時俱進，國防部於 2017 年 7 月 1 日整合各軍種通資部隊，編成「資通電軍指揮部」，成為現有陸、海、空三軍以外，獨立的第四軍種，其中最大亮點即為網路戰部隊，蔡英文總統自就任以來，對於數位國土的安全性就相當重視，並強調「資安等於國安」的國家政策，[3]意味著當全球世界進入全面網路作戰時代，敵情威脅不僅只來自於鄰近的國家，更多的威脅來自境外場域網路空間，而這樣網路威脅對於我國安全之影響何其嚴重，舉凡「分散式阻斷服務攻擊(Distributed Denial of Service, DDoS)」、病毒軟體、木馬程式、網路釣魚等駭客攻擊手法，均會造成國家關鍵基礎設施、國軍武器指管系統、商用物聯網、政府機關及企業公司與個人電腦等核心資料及機敏數據，遭到竊取及破壞，進而影響國家網路及國防戰備安全，此等危害絕對不亞於傳統武裝攻擊，甚至凌駕於戰機、船艦、導彈或任何陸地上高價值主戰裝備攻擊力之上。而為了於常規作戰(傳統武器)、視距外作戰(網路戰)及心理戰等整合性之複合式網路戰場中獲取資電優勢，以利後續軍事任務推展及確保國家安全無虞。我國除了打造一支具有早期預警、縱深防禦及處理網路威脅、作戰實力的軍隊外，未來更必須要朝向「以網路攻防為核心」之可恃戰力構建策略逐步發展。

本文藉由歸納國外網路戰部隊組織運作及策略發展之相關研究為基礎，探討我國網路戰部隊現行策略發展現況，並結合專家訪談，提出發展策略精進作為芻議，期可供國軍網路戰部隊於建軍備戰策略之參據。

各國網路戰部隊發展策略探討

現今各國逐步將主要武器數量和部隊數據公諸於世，但對於網路部隊的編制與運用卻多所保留，即是因為極其重要，故採必要隱密措施。任何國家都不敢輕易使用核彈，一旦使用必會導致兩敗俱傷的結果；而網路戰是當今除經濟戰之外，另一項兵不血刃即可征服他國的戰爭空間之作戰手段。欲獲取網路戰優勢至少需具備三方面的條件：健全的網路戰部隊、先進的網路戰攻防武器及縝密的網路戰作戰策略。根據聯合國統計，在聯合國的 193 個成員國

[1] 王清安，〈從美國陸軍網路部隊之組建探討我陸軍通資部隊轉型〉，《陸軍通資半年刊》(桃園)，第 130 期，陸軍通信電子資訊訓練中心，2018 年 9 月，頁 1-2。
[2] 涂俊緯，〈106 年 QDR 公布揭示軍事戰略「防衛固守、重層嚇阻」〉，《青年日報》(臺北)，2017 年 3 月 17 日，版 2。
[3] 黃庭、劉程鈞，〈資通電軍指揮部編成 總統親臨主持〉，《青年日報》(臺北)，2017 年 6 月 29 日，版 1。

裡，有 67 個國家宣布組建網路戰部隊(不含非公開秘密組織)，[4]顯見各國都已將網路戰視為未來的作戰整備重心，全球組建網路戰部隊之國家如表一。

表一 聯合國成員國組建網路戰部隊之國家

洲別	國家
美洲	美國、加拿大、巴西、古巴、阿根廷、哥倫比亞
歐洲	俄羅斯、英國、法國、德國、義大利、西班牙、波蘭、荷蘭、丹麥、挪威、芬蘭、奧地利、瑞士、烏克蘭、白俄羅斯、希臘、匈牙利、斯洛伐克、克羅地亞、立陶宛、愛沙尼亞、阿爾巴尼亞
亞洲	中國、印度、日本、朝鮮、韓國、伊朗、以色列、緬甸、越南、新加坡、印度尼西亞、馬來西亞、哈薩克斯坦、格魯吉亞、土耳其、斯里蘭卡
非洲	南非
大洋洲	澳大利亞、斐濟

資料來源：作者繪製。

綜觀全球組建「網軍」之聯合國成員國家，本文以美、俄、中共等亞洲及歐美國家做為網路戰部隊發展策略研究主軸，經審視各國多朝向「強化全方位網路戰組織」、「研發新式網路戰具」、「培育優質網戰人力」、「創新整合網路訓練平臺」及「推動多元網路策略聯盟」等構面持續逐步發展。而本文所探討網路戰部隊國家，以具備較完整之網路戰編制架構及兵力結構，且有網路戰實際戰功及競賽實力為考量，列舉以色列等網路強國成軍沿革及發展特色說明如後。

一、以色列

以色列的「網路防衛軍」於 2016 年成軍，人數約 5,000 員，以色列網路防衛軍是保衛國防軍軍隊資訊和通信的樞紐。[5]以色列網路防衛軍成員均由駭客和資安專家們組成，回擊來自世界各地虛擬跳動的攻擊網際網路通訊協定位址(Internet Protocol, IP)、各式不同的攻擊型態和惡意軟體，因應以色列航空系統、金融銀行、國防軍事等不同領域的襲擊，並統由「電腦應急應變小組(Computer Emergency Response Team, CERT)」資安動態即時顯示系統監控及管制。以色列培養網路人才作法，一是運用遊戲方式模擬網路攻防戰場，藉以提高受訓者之興趣，並從過程中培訓及篩選優秀人才；其二為挑選擅長撰寫程式語言之資優學生，於服兵役期間投入「網路防衛軍」專責網路戰工作，並役滿退伍後輔導創立資安公司，持續與國防軍建立合作機制。

以色列人口(約 900 萬人)雖然遠不及我國，惟於網路資安及高科技領域之網路防衛軍，卻是極盡所能網羅網路實戰經歷豐富之頂尖人才為其主要發展特色，且前瞻未來將是網路競

[4] 〈67 個國家組建網路戰部隊〉，《觀察者 APP》，https://m.guanvha.cn，2017 年 6 月 8 日，(檢索日期：2019 年 4 月 26 日)。

[5] 〈打贏網絡戰爭以色列在行動每月經歷幾十起網絡攻擊〉，《中國新聞網》，http://www.chinanews.com/mil/2017/07-06/8270208.shtml，2017 年 6 月 8 日，(檢索日期：2019 年 2 月 12 日)。

賽、資安防禦與資訊作戰之世代，擁有高科技資安人才，就等於擁有強大的網路作戰能力，藉由與產、官、學、研等策略聯盟單位合作，並導入高端網路人才，以整合軍民能量。

二、南韓

因應北朝鮮網路部隊之敵情威脅，南韓亦於 2014 年成立「國軍網路司令部」，人數約 2,000 員，復於 2018 年將其更名為「網路作戰司令部」，把網路戰從消極的「防護」為主模式轉變為積極的「應對作戰」模式，[6]利用敵方弱點先發制人、未雨綢繆，除規劃發展類似「震網(Stuxnet)」的網路虛擬武器外，並舉辦世界駭客大賽，南韓軍方長期構想是構建類似美軍網路司令部數萬人規模網路部隊。在全球駭客競賽(DEF CON CTF)獲得冠軍的 DEFKOR，是由南韓政府精心培養的駭客攻防團隊，其奪冠兩個關鍵在於挖掘漏洞的速度(如微軟 IE、蘋果 Safari、安卓 Chrome 等三大瀏覽器漏洞及零時差漏洞)和撰寫攻擊程式的速度，在開賽 4 小時內便寫出第一支攻擊程式打遍全場，大幅領先其他團隊。

韓國除具備優秀的技術人員外，同步研發高科技網路戰具，透過分析攻擊流量、先進反制手法及防禦技術，強化人員技術培訓及創新網路戰具戰法，為韓國建構「網路司令部」之模式。

三、俄羅斯

俄羅斯於 2008 年成立「科技旅」，大量招募開發軟體之電腦程式編寫及資訊技術人才，其主要任務為對外界資訊進行監測及打擊網路威脅，人數約有 12,000 員。[7]舉世聞名事件即為 2011 年對愛沙尼亞及喬治亞實施「分散式阻斷服務攻擊」，癱瘓愛沙尼亞與喬治亞政府及金融網路數十日。另於 2015 年透過釣魚郵件及社交工程等網路攻擊手法，竊取美國總統歐巴馬社群網路及日程安排等非公開訊息，復於 2015 年攻擊烏克蘭電力網路，導致烏克蘭國境內大範圍停電，並於 2016 年使用散布假消息手法干涉美國總統大選等事件，前述事件跡證皆指向俄羅斯科技旅所為，惟其隱蔽能力強，雖矛頭均直指俄羅斯，然以美國強大的網路追蹤偵查能力，卻仍無法抓住其破綻及罅隙。

俄羅斯網路部隊為應對網路空間領域實戰需求，各大軍事院校及研究院均開設多元化之網路課程，置重點於網路手法與傳統戰鬥方式結合，逐步提升未來的網路戰骨幹能量。另開發網路戰訓練平臺，用於模擬網路空間攻防作戰環境、測試網路武器裝備及檢驗網路攻防戰術戰法，俾使網路作戰能量持續提升。

四、中共

「戰略支援部隊」為中共於 2015 年編成之獨立軍種，人數約 10 萬餘員，是將「戰略性、基礎性、支撐性都很強的各類保障力量」進行功能整合後組建而成的高科技部隊，亦是中共

---

[6] 〈南韓重組國防網軍，更名為網路作戰司令部〉，《經濟日報》，https://money.udn.com/money/story/5641/3299704，2018 年 8 月 9 日，(檢索日期：2019 年 2 月 12 日)。

[7] 〈「普丁廚師」如何操縱美大選？揭發俄國網軍運作內幕〉，《鏡週刊》，https://www.mirrormedia.mg/story/putin-cook/，2018 年 2 月 17 日，(檢索日期：2019 年 2 月 12 日)。

軍改重大調整的一部分，[8]中共規劃運用該部隊於未來高科技戰爭中，利用網路戰擴大其能力和影響力，主要以不對稱的作戰能力建設軍隊，以期能擊敗美國等實力較強的對手，其重要戰功即為 2015 年以「進階持續性滲透攻擊(Advanced Persistent Threat, APT)」竊取美國聯邦人事管理署 2,100 萬筆機敏個資案件。

中共戰略支援部隊並非屬於陸軍、海軍、空軍或火箭軍之一部分，而是直接隸屬於中央軍事委員會，該部隊的兩個主要單位是空間系統部(負責航空作戰)及網路系統部(負責網路戰)，[9]確保在未來複合式威脅戰場環境中，遠程精確打擊、無人機偵察和戰略空中作戰皆於不同程度上運用戰略支援部隊，取得資電優勢。探討中共軍事武力發展，其中資電作戰整備以強化網路作戰專業能量為目標，並成立資訊網路作戰部隊(即戰略支援部隊)，藉由整合民間科研能量、建構網路訓練學校(院)、挹注軍事預算及演習對抗訓練，提升整體網路戰力，並順應世界資訊科技不斷發展的趨勢下，作戰方針亦同步調整「攻勢為主」，透過網路滲透等手法，發掘目標國網路系統弱點(漏洞)，進而獲取所望利益。

五、美國

美國「網路司令部」屬軍方機構，負責執行網路軍事行動及保護軍方電腦系統，為美國國防部之一體化作戰司令部，該部隊於 2009 年 6 月 23 日成立，人數約 12 萬餘員，由陸軍網路司令部(Army Forces Cyber Command)第 780 軍事情報旅、海軍網路司令部(Fleet Cyber Command/United States Tenth Fleet)第 10 艦隊、空軍第 24 航空隊(24th Air Force)以及海軍陸戰隊網路空間司令部(Marine Corps Cyberspace Command)等 4 支部隊整合而成。[10]2017 年 8 月 18 日，美國總統川普已將美軍網路司令部升級為聯合作戰司令部第 10 部，以強化美軍的網路空間作戰能力，並加強美國國家資安防禦，進一步確保美軍及其盟國在網路空間的行動自由，以及削弱與拘束敵方在網路空間的行動自由等。現下轄 133 支「國家網路任務部隊」，共區分 4 類型作戰任務：國家任務組共計 13 支部隊，主要負責透過發現敵人活動、阻止網路攻擊並反制敵人，為美國資訊網路系統提供保護；網路防護組計有 68 支部隊，主要負責保護美國國防部資訊網路，並為網路部隊實施作戰準備；戰鬥任務組有 27 支部隊，主要負責執行軍事網路行動以支援作戰司令部作戰部隊；網路支援組有 25 支部隊，主要負責提供分析與規劃，以支援國家任務部隊各小隊和作戰任務部隊各小隊，[11]前述部隊均已於 2018 年 9 月具備全面作戰能力(Full Operational Capability, FOC)，美軍網路司令部組織如圖一。

---

[8] 〈揭秘陸軍領導機構火箭軍戰略支援部隊〉，《中國青年報》，http://zqb.cyol.com/html/2016-01/02/nw.D110000zgqnb_20160102_2-01.htm，2016 年 1 月 2 日，(檢索日期：2019 年 2 月 12 日)。

[9] 〈中國火箭軍和戰略支援部隊，到底有多厲害？〉，《端傳媒》，https://theinitium.com/article/20160121-opinion-military-reform-china-muzhi/，2016 年 1 月 21 日，(檢索日期：2019 年 2 月 12 日)。

[10] 〈美國網路司令部官方簡史〉，《E 安全》，https://www.easyaq.com/news/33130322.shtml，2018 年 7 月 27 日，(檢索日期：2019 年 2 月 12 日)。

[11] 〈美軍網路司令部 133 支國家網路任務部隊全部具備作戰能力〉，《美國華裔教授專家網》，http://scholarsupdate.hi2net.com/news.asp?NewsID=20991，2016 年 10 月 25 日，(檢索日期：2019 年 2 月 12 日)。

圖一 美軍網路司令部組織圖

資料來源：作者繪製。

美國網路司令部改變以往的防禦戰略，「以防為主」之作戰策略轉為「攻防兼備」，歐巴馬政府時期「美國軍方在對外採取任何重大網路行動前都必須得到白宮的批准」的指令，現已遭川普廢除，意味無須在對手進入美國網路系統時才實施攔截，可以針對攻擊方採取先發制人行動，明顯從「防禦」姿態轉為「進攻」態勢。[12]該司令部有名的戰功是 2011 年透過網路監聽軟體程式及手法，成功發現恐怖組織首領賓拉登藏身點；2014 年攻擊朝鮮網際網路，造成朝鮮半島全區網路癱瘓；2016 年對伊斯蘭國恐怖組織發動網路攻擊，以該組織的通信網路、宣傳網站及社交網站帳號為主要目標，透過網路癱瘓及發布假指令等方式，成功削弱其傳遞情報、下達指示、招募新人和電子支付等能力。

為肆應現階段複合式作戰環境，美軍由「陸軍網路訓練中心(Army Cyber Center of Excellence, ACCE)」、矽谷高科技廠商及史丹佛大學等單位合作，並發展「國防駭客(Hacking4 Defense)」計畫，並召集橫跨全美百餘名具備網路系統或網路安全專業網路專家，組成「Echo 特遣隊(Task Force Echo)」，以強化美軍網路的基礎架構。故美軍已透過調整部隊定位、改變作戰思維、結合民間資源、強化教育訓練、建立攻防訓場、提增國防預算等構面運作，完成符合美軍作戰網路團隊建置，並發展為全戰備能力網路部隊。

[12] 〈美軍第十個聯合作戰司令部成立!川普宣告網路司令部升格〉，《風傳媒》，https://www.storm.mg/article/317918，2017 年 8 月 19 日，(檢索日期：2019 年 2 月 12 日)。

六、法國

法國的網路部隊雖然發聲不多，但卻實力強勁，這一點可以從其在科索沃及利比亞兩場戰爭中看出。於 1999 年科索沃戰爭中，該網路部隊藉由發動分散式阻斷服務攻擊，使敵方網路陷入癱瘓。尤其是在利比亞戰爭中，其網路部隊深度參與，且戰果豐碩。因此，法國政府於 2014 年為網路安全、防禦和研發投入 10 億歐元，主要用來聘請高水準研究人員和工程師，這支被命名為「Cybercom」的國家駭客軍隊能力已經不僅僅侷限於防禦，而是具有進攻其他國家資訊系統以及參與網路戰爭的實力，目前該部隊人數約為 2,600 人，[13]並計劃儲備一支民間網路安全與防禦力量，培養一批在私營企業工作之網路防禦專家，以便在必要時可以服務於政府軍隊。

法軍近年來著重於駭客軍隊和作戰部隊聯合展開演練，重點演練網路戰部隊在複雜多元環境下支援作戰單位的行動，規劃大面積停電、煉油廠漏油、港口關閉等網路襲擊場景，並認為「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」，唯有實施軍民聯合的網路總體戰，方能打贏未來網路戰爭。

七、德國

由於德國多數武器系統，均使用網路與資訊科技支援。因此，德國軍隊一直都是網路駭客和外國情報機關刺探的高價值目標，亟需一支專業化網軍，提供全方位網路防護。基此，德國政府建立「國家網路空間防禦中心」，由聯邦國防軍「網路空間作戰司令部」主導，聯邦憲法保衛局、聯邦民眾保護與災害救助局、聯邦刑事犯罪調查局、聯邦警察、聯邦情報局及各州代表均參與其中工作，一旦發生網路空間攻擊，該中心可迅速評估形勢，並向政府提出應對措施建議。

德軍於 2017 年打造攻防兼備的「網路空間作戰司令部」，人數約 3,000 員，[14]該部隊同時具備攻擊及防禦能力，主要任務包括確保聯邦國防軍情報系統在國內外的安全運作、加強在網路情報空間的偵察和影響力、支援國防軍其他部門完成任務、資訊化背景下與其他機構合作維護國家安全、確保政府網路關鍵基礎設施不受破壞、加強網路安全設施建設等。「網路空間作戰司令部」與聯邦國防軍其他軍種平起平坐，成為陸軍、海軍、空軍、聯合支援軍及聯合醫療軍之外的第六軍種，規劃於 2021 年擴編至 1 萬 3,500 人，除了將聯邦國防軍戰略偵察、情報技術和地理情報等部門人員整編到網路軍，亦對外招攬業界網路駭客，提升國防軍原有的網路攻防力量。

網路戰部隊發展策略分析

[13] 〈法國成立首支網路部隊，稱其重要性超過軍隊〉，《雷鋒網》，https://www.leiphone.com/news/201612/31vXdG3pacHzZbdK.html，2016 年 12 月 15 日，(檢索日期：2019 年 2 月 12 日)。

[14] 〈德國打造攻防兼備的網路軍〉，《新華網》，http://www.xinhuanet.com/world/2017-04/12/c_1120796671.htm，2017 年 4 月 12 日，(檢索日期：2019 年 2 月 12 日)。

本段歸納學者專家對網路戰部隊發展提出之重點策略，俾作為探討國軍網路戰部隊發展策略之參據，策略分析重點如後：

一、調整組織型態、網軍擴編升格

美國即使已是世界最強網路國家，具備全球最完整網路部隊，然而面對各國不斷的網路威脅，仍需持續建構網路嚇阻能力，以捍衛網路空間安全，同時加強美國政府資產及關鍵基礎設施之網路安全防護能力，並保護數據和情報之完整性，將美軍網路司令部升級為最高級別的聯合作戰司令部後，除可顯示美國強化對付網路威脅之決心外，亦更能堅定盟友與夥伴信心，對敵產生嚇阻力量。[15]網路司令部將進一步強化美國的網路安全，也將加強與盟邦的合作，對全球網路安全威脅做出快速反應，在網路司令部層級升格後，即與上級單位戰略司令部同級，成為美軍最高級別的聯合作戰司令部之一，美軍原有 9 個聯合作戰司令部(Unified Combatant Command)，其中 6 個依「戰區」劃分，分別為北方司令部、南方司令部、中央司令部、非洲司令部、歐洲司令部、太平洋司令部；三個以「職能」劃分，分別為戰略司令部、特種作戰司令部、運輸司令部，而網路司令部將成為第四個按照職能劃分的聯合作戰司令部，也是美軍第十個聯合作戰司令部。將網路司令部升級成為聯合作戰司令部層級，意味著網路空間正式與陸、海、空、天(太空)並列成為美軍的第五維戰場，亦成為與美軍陸、海、空三個軍種一樣的一級司令部，雖然網路是一個虛擬空間，但實際有其運作，而將之視為美軍新增的一個軍種「網軍」也無不可。

二、改變戰略思維、攻防能力兼備

未來網路戰戰法，勢必將先聲奪人，以現今「防衛固守、重層嚇阻」軍事戰略構想，將無法適應於未來網路作戰進程，須知網路空間戰略高地，乃是兵家必爭之地，誰先佔領，誰就有機會獲取最後勝利。[16]借鏡 2013 年，俄羅斯出兵佔領克里米亞，能順利獲得軍事勝利，即為俄羅斯巧妙運用網路戰先發制人。

中共領導人在軍隊現代化建設過程中發現，短時間內其軍事力量無法提升至美國軍事水準，卻可利用網路空間特性與跨空間領域及延伸效應之戰略價值，將敵驅逐至相對不利的狀況。面對 21 世紀的挑戰，解放軍任務已將國家利益的概念由確保傳統疆域安全與主權，進一步擴張到遠海、外太空與電磁空間，並主張必須發展確保這些利益的必要戰力。[17]中共解放軍的網路威懾戰，不僅僅是針對電腦及網路以病毒手段實施攻擊，其威懾手段主要體現有二：其一為將國家實力轉化為威懾資訊，以遏制侵略者的戰略，是當今世界各國競爭抗衡的一種

---

[15] 高清華，〈美軍「第三次抵銷戰略」與美中網路資訊作戰之研究－兼論對兩岸軍事對峙之影響〉，國防大學政治作戰學院政治學系政治研究碩士班碩士論文，2018 年 5 月，頁 49-50。

[16] 王清安，〈中共網軍發展對本軍威脅評估之研究〉，《陸軍通資半年刊》(桃園)，第 127 期，陸軍通信電子資訊訓練中心，2017 年 4 月，頁 23。

[17] 金登富，〈中共網路戰略思維之概念性探討(The Conceptual Analysis of PLA's Cyber Strategy)〉，國防大學戰略研究所戰略與國際事務碩士班碩士學位論文，2014 年 3 月，頁 96-121。

形式，也是網路威懾的戰略的威力；其二為軍事上的積極防禦，強調以積極攻擊削弱對手的進攻，改變被動的局面，必須把握時機以突發性攻擊作為反制手段，以抵銷和遏制強國的軍事威懾。意即戰時將透過網路竊取、病毒攻擊等軟殺傷，結合火力硬摧毀，破壞敵民生基礎設施、關鍵節點，迫使敵屈服。

三、研發攻防戰具、獲取作戰優勢

網路社會中，各種軟硬體、技術與運用等將實現高度的整合。儘管美國官方表示美國絕不容許軍方從事網路攻擊行為，但經中共民間相關業者研析，美軍為了網路進攻能力，已大力開發電腦網路戰武器，據其評估目前美軍至少已經研製出 2,000 多種電腦病毒武器，[18]加上訓練有素的網路戰攻擊部隊，只要符合美國戰略需要，隨時可發起資訊網路攻擊，侵入別國網路，進行破壞、癱瘓，甚至控制資訊系統。

美軍第三次抵銷戰略，即是運用不對稱作戰與技術創新反制對手反介入與區域拒止能力，意謂在網路作戰空間及人工智慧領域投資與研發。[19]美軍在執行第三次抵銷戰略期間，國防預算為 10 年來新高，使其可以獲得所需的資源與經費，執行相關軍事科技的研發與網路戰具的創新。再者，由網路作戰技術角度言之，網路戰攻防主要是對相應網路軟體運用，而網路軟體使用的過程又往往十分簡單，故開發及研製網路攻防軟體武器，是最直接、最重要的網路戰基礎，亦是網路戰之核心。網路軟體武器研發人員，同時為典型的網路戰戰士，可見在網路戰力的規劃中，要將研發、建設與運用一體籌劃，才能創造最大效益，俾藉以獲取作戰優勢。

「工欲善其事、必先利其器」，此乃千古不變之真理，想要在全球虛擬環境打贏網路戰爭，就必須研發高端的網路戰具，不僅需握有尖銳的矛，也需具備堅硬的盾，再輔以綿密之情蒐武器及創新戰術戰法，方能制敵機先、克敵制勝，俾臻「無堅不摧、無攻可破」之終極目標。

四、挹注專案預算、強化教育訓練

為了反制駭客攻擊，美國在 2015 年成立 40 支網路部隊，其中 13 支部隊是要在美國遭受網路攻擊時回擊，歐巴馬強調該隊伍並非防禦性的隊伍，而是攻擊性的網路部隊。[20]美國國防部在 5 年內投入 260 億美元發展網路科技，主要用於保衛軍方的網路，並投入數十億美元來發展網攻武器，在國防部預算全面縮減情況下，網路攻擊武器是少數增加投資的項目。

美國在國家整體網路安全的專案預算部分，分別在 2013 年投入 103 億美元、在 2015 年投入 125 億美元，乃至歐巴馬總統提議在 2016 年撥款 140 億美元用於加強美國網路安全，以保護聯邦政府和私有企業的網路免遭駭客威脅，其預算數皆呈現穩定成長趨勢，而國防部

---

[18] 莊凱婷，〈網路戰與國家安全—以美國網際空間策略為例〉，國立政治大學外交學系戰略與國際事務碩士在職專班論文，2018 年 7 月，頁 92。

[19] 同註 18，頁 39-59。

[20] 吳孟軒，〈網路權力之爭—美「中」網路攻擊與戰爭初探(The Cyberspace Power Struggles and Cyber Wars Between US and China)〉，《展望與探索》(桃園)，第 12 卷第 7 期，法務部調查局，2014 年 7 月，頁 69。

網路司令部分配到的經費，也將用來支援防禦性和進攻性網路空間作戰能力，持續加強培訓和建設網路任務部隊；[21]另美陸軍網路指揮部在 2013 年已達成網路空間訓練制度化的關鍵目標，並計劃成立「卓越網路中心(學校)」，增加網路制度面與作戰面的整合，以打造制度性網路能量，支援鞏固陸軍在信號、網路、電子戰，以及軍事情報界的網路空間專業能力，俾達成執行有效網路空間作戰之制度面與作戰面的整合。

五、結合產學資源、建立攻防訓場

美軍認為定期展開軍民聯合網路演習甚為重要且事關重大，要完成軍方肩負之確保美國軍事網路安全、支援聯合作戰及保護境內關鍵基礎設施正常運作等三大網路核心任務，必須與其他聯邦政府機構、州和地方政府，特別是民間企業進行合作。基於恐怖分子與網路空間結合等趨勢，除了上述國土安全部被賦予執行網路安全等工作外，也主導結合各民間產學資源，來強化對於資訊交換與合作的管道，主動管理網路相關威脅，以及協調網路資訊共享，目的是能夠在複雜電磁環境中，迅速處理網路安全問題，[22]其中重要的合作夥伴即是私人企業、學術界、聯邦機構以及國內外重要組織機關，甚至後來國土安全部每兩年舉行一次的網路風暴演習(Cyber Storm)，也是強調在政府與私人企業進行合作，提升對於網路安全威脅的因應能力。

六、小結

本文就前述國外網路戰部隊發展現況及綜合學者文獻探討內容，摘要彙整分析矩陣表如表二，由表可看出各國網路戰部隊發展策略之趨勢，是以組織型態之調整(提升)為必然、具攻防兼備之能力為根本，並結合產學教訓孕育專業部隊能量為基礎，再挹注國防專案預算全面提升戰力。

表二 網路戰部隊發展策略分析矩陣表

策略／國家	組織型態	攻防兼備	戰具研發	教育訓練	結合產學
以色列	網路防衛軍(2016)	回擊作戰模式	未公開	遊戲模擬攻防戰場	國防工業融入民用網路
南韓	網路作戰司令部(2018)	應對作戰模式	自主研發網路戰戰具	政府菁英計畫	駭客攻防團隊DEFKOR
俄羅斯	科技旅(2008)	監測及攻擊	自主研發網路戰戰具	開設多元化之網路課程	多元化之網路課程
中共	戰略支援部隊(2015)	攻勢為主	自主研發網路戰戰具	建構網路訓練學校	整合民間科研能量

[21] 黃志軒，〈國土安全脈絡下美國網路安全戰略發展(The Development of U.S. Cybersecurity Strategy Under The Concept of Homeland Security)〉，國防大學政治作戰學院政治學系政治研究碩士班碩士論文，2015 年 6 月，頁 92-101。

[22] 邱陳慶，〈美國網路部隊發展之研究兼論稜鏡事件的影響〉，淡江大學國際事務與戰略研究所碩士在職專班碩士論文，2017 年 1 月，頁 33-34。

美國	網路司令部(2009)	先發制人、進攻態勢	自主研發網路戰戰具	專案計畫	國防駭客計畫、Echo特遣隊
法國	Cybercom(2014)	網路安全防禦優先	未公開	儲備民防力量	軍民聯合網路總體戰
德國	網路空間作戰司令部(2017)	攻擊及防禦能力兼具	未公開	聯邦國防軍大學	招攬業界網路駭客

資料來源：作者繪製。

我國網路戰部隊發展策略探討

一、發展策略現況探討

我國網路戰部隊在 2005 年以前全銜為「統一通信指揮部」，主要負責纜線搶修、骨幹傳輸平臺維護、電子監察及資訊戰作業等任務，其中專責資訊作戰任務的資訊戰中隊，編制人數約 50 員；復於 2005 年組織調整為「資電作戰指揮部」，並成立網路戰大隊，負責執行網路情蒐和網路防護等任務，編制人數約 200 餘員。依據國家安全戰略指導，為確保國軍指管及資訊系統有效運作，並具國家層級資安事件應處能力及協助關鍵基礎設施防護，國防部於 2017 年 7 月 1 日以資電作戰指揮部編制為基礎，整合陸軍資電群等單位，編成「資通電軍指揮部(Information Communication Electronic Force, ICEF)」，並將網路戰部隊層級從大隊層級提升為聯隊層級，編制總人數約為 1,000 餘人，專責網路戰任務人數僅約 500 人。其核心任務調整為假新聞情蒐與反制、網路心理攻防、國家資安事件應處、協防關鍵基礎設施及確保國軍指管傳輸暢通等，並藉由中科院和產、官、學、研等機構技術支援合作，打造一支具備處理網路威脅、不對稱作戰實力的軍隊，並以「網路攻防為核心」戰力發展主軸。發展策略摘重如下：

(一)整合軍民人才，維繫網戰戰力

為鞏固部隊戰力，滿足網路戰快速應變需求及加強國軍網際網路攻防能量，依國軍後備戰士志願短期在營服役實施計畫，招選具資訊專長之後備軍人轉服「網路戰士」，並已與民間公司及財團法人等單位完成合作意向書簽署，藉由汲取民間技術，化民力為我力，融我力為戰力，達到「平時養兵少、戰時用兵多」之建軍目標。資通電軍現採導入全時軍職人員、兼職民間網路戰士等方式，其中軍職人員可透過不同等級資訊證照考取結合戰功，申領高額之網路戰加給；而網路戰士亦可依原退役階級或經由評審委員完成能力評鑑後，除給予行政院核定之日薪外，可再依戰功加發獎金。藉由前述作法，提高專業人才薪資及加給，強化民間資訊人才加入之誘因，可整合軍民網路戰領域之人才，提升網路戰部隊戰力。

(二)委外教育訓練，建構進階技能

藉由完整委外網路教育訓練，培訓所屬人員考取駭客技術專家認證(Certificated Ethical Hacker, CEH)等專業證照，且與專業教育訓練機構密切交流，可協助網路戰部隊人員完成各級證照考取，持續強化人員本職學能，戮力建構足以和世界強國匹敵之網路戰部隊。資通電軍官兵成軍迄今已考取駭客技術專家認證、資安危機處理師(EC-Council Certified Incident Handler,

ECIH)、微軟系統專家(Microsoft Certified Systems Engineer, MCSE)及資安分析專家認證(EC-Council Certified Security Analyst, ECSA)等類多張國際資訊證照，持恆培育所屬人員考取國際專業證照，俾提升整體專業技能。

(三)挹注國防預算，強化科研能量

在年度獲賦國防總預算內挹注網路戰各項預算，用以協助網路操作人員取得相關網路戰技能及進階認證，並投資網路攻、防、蒐各式戰具籌建，提升整體軟硬體效能。資通電軍現有網路戰戰具可區分為數位鑑識、網路反制、網路情蒐及網路防護等類型，主要以自主研發、軍投建案及商購軟體等 3 種方式籌獲，現況以委中科院研發為主，同時基於「寓兵於民」理念推動技術研究學合案，與中科院、交通大學共同成立「國防資電科技中心」，藉以達成資電科技智能化與自動化目標，提升人員素質並強化科研能量，朝自主研發目標努力，俾符未來作戰實需。

(四)資安分析共享，全面策略聯盟

結合現行對國軍各單位實施不定期網路滲透測試任務，以及定期配合行政院編組分赴各部會辦理資安健檢時機，將所查獲弱點及漏洞交由網路戰攻防實驗室，分析偵獲各項網路攻擊滲透手法，再將系統弱點(漏洞)修補措施回饋國軍各單位、政府各部會以及產學策略聯盟，提升我國整體網路全面防護能量；另可將網路戰攻防實驗環境驗證成果，提供中科院科研案及國防資電科技中心學合案納為研發參據，確保研改戰具符合部隊作戰實需。資通電軍依令執行「國家關鍵資訊基礎設施防護(Critical Information Infrastructure, CII)」協防任務，成軍迄今對中央院會及各縣市政府執行滲透測試，檢測風險及資訊系統弱點戰果豐碩，且均回饋單位並提供修復建議。

(五)建構攻防平臺，實戰累積經驗

資通電軍網路戰部隊現已完成第一代網路戰攻防平臺建置，建構網路攻防實驗室及訓場，俾與 IT 業界網路技術同步並提供網路戰部隊攻防訓練之練兵場，持續透過網路攻防實驗室或委託研發單位開發新一代網路戰攻防環境，並朝現今複合式作戰方向發展專業技術網路戰具，並搭配網路反制、防護及情蒐戰術戰法，不斷提升整體網路攻防技術能量。另資通電軍每年均專案編組積極參加全球駭客競賽(DEF CON CTF)及美國黑帽駭客年會(Black Hat USA)等國際級網路攻防活動競賽，一則可驗證網路戰部隊人員攻防技術及能力，二則可藉由參加此類國際競賽，獲取新知且厚植實戰經驗。將持續爭取參加各式實戰演練機會，以驗證平時訓練成效。

二、敵我態勢分析

(一)國軍網路戰部隊雖已於 106 年 7 月整合提升為資通電軍網路戰聯隊，然組織變革及任務調整未盡周延，現階段僅能有限度執行網路戰偵蒐及攻防作業，反制能量仍需持續籌建。況且全軍各單位現有資訊安全各項設備，尚未完全建立整合運用、集中控管之機制，一旦遭受

敵方網路戰攻擊後，恐難以即時有效控管及應變制變，資訊安全防禦強度有待提升。另網路戰反制任務未能依中共網路環境實況仿真，僅能靠持續投資建案、自主研發，方能逐步提升網路戰攻擊能量，尚需通資電整體規劃且整合時程實緩不濟急。

(二)在未來複合式威脅戰場環境中，中共「戰略支援部隊」可提供遠程精確打擊、無人機偵察和戰略空中作戰之戰力支持，其軍事武力發展策略中，網電作戰整備即以強化網路作戰專業能量為目標，並順應世界資訊科技不斷發展的趨勢下，作戰方針亦同步調整「攻勢」為主。反觀我國國軍作戰指導為「防衛固守、重層嚇阻」，我國網路作戰策略即以「守勢」為主，且礙於國際輿論壓力，致網路作戰仍以防護及情蒐為主、反制為輔，相較於中共積極對外網路活動(滲透竊密及癱瘓攻擊等手段)，我國軍網路戰部隊各項戰術戰法偏重守勢，面對威脅難以遽然予以反制還擊，恐喪失制敵先機。

(三)由於中共積極發展超限戰、信息戰、不對稱戰法及新式戰具等，其武力犯臺模式已非一成不變，而是更具多元化，使我軍對此反制、防護等作為更加繁重。國軍目前網路戰攻防、網路管理、系統支援、資訊網路及時監控等機制，雖已透過資安防護管理系統、網管系統之建置、精進與整合而漸臻完備。惟面對未來數位化主導之戰場，中共將採取諸般先制手段，如癱瘓我資訊網路系統、植入後門程式、滲透截取我方資料流，進而延緩指管通情決策作為，降低部隊運作效率。

(四)中共信息戰之威脅包括網路戰、心理戰及情報戰等面向，依過去敏感時機中共所發動之駭客編組、運用方式及攻擊能量判斷，國軍資通網路系統環境在平時雖未遭受直接攻擊，但於戰時若採行軍、公、民營通資網路整合運用，勢必會面臨因民間通資體系安全防範作業未臻完善，進而阻滯國軍指管/通資電網路之正常運作。

(五)資訊科技進展神速，網路攻防戰具必須不斷更新研改，亟需持續透過技術研改及專才延攬，方能不斷籌建新式裝備及戰具，惟就國軍網路戰部隊人員通過證照考取，順利申領網路戰加給後，總薪資最多不過約為 7-8 萬元，仍遠遠落後業界待遇(薪資均高達 10 萬元以上)，[23] 再加以軍事部隊嚴謹之生活管理及訓練，對人才招募誘因相對薄弱，將面臨網路技術專業人才缺口之嚴重問題；中共亦面臨相同的狀況，目前中共每年可培育網路技術專業人才僅 3 萬餘人，但與實際總需求數落差過大，缺口比例高達 95%，而各行業資訊系統和資訊基礎設施需要各類網路技術人才需求到 2020 年將增長到 140 萬，[24]專業人力不足已是世界各國政府、民間企業共同面臨之頭痛問題。

三、專家訪談指導

所謂「專家」指的是對某一專業領域具有優異表現、天賦異稟或經驗豐富、技術熟稔之

[23] 〈資訊網路工程師薪水待遇最新情報查詢〉，《1111 人力銀行》，https://www.jobsaiary.com.tw/salarysummary.aspx?codeNo=140402，2018 年 4 月 2 日，(檢索日期：2019 年 2 月 12 日)。

[24] 〈2017 年上半年互聯網安全報告〉，《國家信息中心》，https://www.sic.gov.cn/archiver/SIC/UpFile/.../20170807115920801889.pdf，2017 年 8 月 8 日，(檢索日期：2019 年 12 月 14 日)。

專業人士，本研究邀請網路戰部隊編成相關單位(國安會資通安全辦公室、國防部通次室發展規劃處、資通電軍指揮部網戰整備處、資通電軍指揮部網路戰聯隊及中科院資通所等)，決策管理及實務工作人員為專家訪談對象，俾依訪談結果作為精進之參據。以下茲摘錄專家訪談指導：

(一)中共於 2016 年元旦成立「戰略支援部隊」，已成為陸海空軍及火箭軍以外的第五支新型態「作戰力量」，直接隸屬於中國共產黨中央軍事委員會；而美國總統川普亦於 2017 年 8 月，將美軍網路司令部由原戰略司令部下的二級司令部升級為美軍第 10 個聯合作戰司令部。反觀我國資通電軍雖已於 2017 年 7 月成軍，惟編制層級及人數仍遠不及三軍司令部，為有效網路戰戰力發揚及前瞻境外勝負決戰，建議未來可師法美軍等全球網路強國，將資通電軍指揮部戰略層級向上提升，並下轄網路戰指揮部，編制網路作戰聯隊、網路防護聯隊及網路情蒐聯隊等單位，主責網路反制(網攻)、網路防禦(網防)及網路偵蒐(網蒐)等三大核心任務，方可發揮我軍不對稱之網電作戰實力。

(二)遵國家政策指導，國軍網路戰部隊主要任務為防禦我國數位疆土之安全，除了平時戮力於資訊網路技術訓練外，並依演訓期程驗證國軍網路防護強度及人員本職學能。另可配合政府各部會執行資安環境稽查，如行政院攻防演練、外交部資安健診、主計總處網路體檢及金管會滲透測試等。期藉多元任務代替訓練方式，積極落實戰訓本務，完善資通電軍網路戰各方面之戰力。

(三)國軍應主動在網路戰方面協調軍民合作、建立策略聯盟。以國內某 IT 教育訓練業者為例，其與國內七所大學(政治大學、健行科技大學、樹德科技大學、聖約翰科技大學、長庚大學、正修科技大學與靜宜大學)產學合作成立「大專院校專業認證訓練中心(Academia Accredited Training Center, AATC)」，共同推廣國際電子商務顧問局(The International Council of Electronic Commerce Consultants, EC-Council)全系列資安認證課程，協助學生在校即可取得資安專業證照與技術能力，提升就業競爭力，截至 2018 年已經培訓 1,300 位學員取得資訊安全駭客攻防系列如 ENSA 網路安全管理師、CEH 駭客技術專家、ECSA 資安分析專家等認證證照。是故，建議資通電軍應主動與國內外具資訊網路權威之大專院校及民間業界教育機構建立策略聯盟，以培訓網路戰部隊人員資安技術能量。

(四)要全面提升部隊人員技術能力，除了持續精進我國網路戰戰具研發及攻防訓場建構外，亦須國防預算的投資及參加國際間舉辦的賽事，以韓國政府資安菁英計畫(Best of the Best, BOB)為例，自 2012 年開始每年以充足的經費和資源，持續培養年輕資安攻防選手。在第 23 屆全球駭客競賽的南韓參賽隊伍，以驚人的快速挖掘漏洞和撰寫攻擊程式的實力，在首度參加 CTF 決賽便奪得冠軍寶座，可見其計畫執行有成的戰果展現。我國應汲取韓國培訓經驗，挹注國防預算投入資通電軍網路戰部隊，並積極不斷參與網路競賽，藉由參與國際競賽獲取實際戰功及網戰經驗，俾肆應敵方網路威脅。

精進作為芻議

參酌前述網路戰部隊發展策略探討、敵我態勢分析及專家訪談指導，本段針對網路戰部隊發展各面向提出三項精進作為芻議，分述如後：

一、攻防策略調整

(一)提升各式網攻手法

經參與歷年全球駭客競賽等國際網路競賽活動，回顧手機、網路設備、物聯網及工控系統等相關新式網攻手法主題中，可發現重大資安事件或漏洞，已由單一弱點式攻擊轉化成複合式網攻手法；攻擊者使用坊間免費工具已轉化成自行開發針對性之弱點攻擊工具；而單一駭客行為已轉化成團隊組織作戰。建議網路戰部隊參酌以上網攻手法進化趨勢，調整現行任務編組及網攻策略，全面提升各式網攻手法。

(二)結合心戰戰術戰法

國軍網路戰部隊近幾年積極投入美國黑帽駭客年會等網路交流派對，年會中所提「深偽(Deepfake)」技術(藉由仿冒具高知名或影響性人物聲音、臉部表情及影像等，散播不實消息，藉此擾亂人心意圖)，因投入成本小，其產生效益大，可作為對敵之不對稱作戰之手段。孫子兵法曰：「上兵伐謀」，而凡謀之所成，攻心為上，讓敵軍喪失戰鬥能力，從而使己方達到完勝目的。建議網路戰部隊可將深偽技術納入研究範疇，適時結合心戰部門，製作影片偽冒敵軍重要人物誌影像，透過網路社群平臺散布有利我方之假消息，打擊敵軍心士氣。

(三)強化網路情資獲得

網路戰攻防技術世界各國均列為高度機密作為，國軍對中共相關攻防技術發展情資來源有限。鑒於國外已有地理定位情資販售管道，建議可納入產官學研合作機制或委由中科院增列採購需求，自第三方管道購置中國大陸電信商之重要人物地理情資，作為監控與精準打擊目標。

二、系統戰具籌獲

(一)零時差漏洞戰具採購

現階段國內尚無相關購買零時差漏洞戰具管道與機制，建議國防部協請國安會運用特別預算採購，並積極與產官學研單位及中科院共同合作是項戰具開發及研製，以確保我國關鍵基礎設施正常運作及全軍指管網路安全無虞。

(二)各類網攻戰具研改

目前國軍網路戰具開源能量仍未臻周延，建議聘請坊間資安公司講師及高專技駭客，針對國軍現行網路戰具持續進行研改，包含滲透測試虛擬機、內網匿蹤、逆向工程及惡意注入等戰具。另藉由各式交流管道，索取新式駭客工具包，俾利與中共戰略支援部隊之網軍相互抗衡。

(三)建立工控系統攻防能力

因應網路安全威脅逐年增加，國軍網路戰部隊應具備防護多樣性系統類型之能力，包含工業控制系統(Industrial Control Systems, ICS)、資訊與通信科技(Information and Communication Technology, ICT)、資訊科技(Information Technology, IT)等系統。其中業界針對「工業控制系統」主題已有相關論文研究，建議網路戰部隊可納入戰具研發標的及教育訓練規劃課程，以有效掌握「數據採集與監視控制系統(Supervisory Control And Data Acquisition, SCADA)」架構，藉由熟稔相關系統弱點，與國際網路攻防技術接軌。

三、健全教育訓練

(一)培養網路高專技人才

各國駭客及資安高手，不乏具備紮實資訊網路進階學理，如逆向工程、資料結構、演算法、密碼學及程式語言等專業技能，而國際級講師所發表論文及研究心得，更囊括理論闡述、技術說明及攻擊策略等複合式網路作戰思維。反觀國軍網路戰部隊，大多數人因基本學養不足，僅擅長操作戰具執行滲透測試等初階網路任務，惟少部分師資及幹部擁有程式開發或漏洞撰寫能力。建議資通電軍應運用各式(類)建案專業領域課程，強化網路戰人員本職學能及提升獨立自主系統漏洞發掘及程式(Mobile Application, APP)開發能力。

(二)了解物聯網技術運用

物聯網技術可結合軍事通信平臺暨聯合作戰指管系統、火力控制系統與精準打擊武器成為戰鬥物聯網路，需從感知層、網路層與應用層強化防護機制，包含資料格式一致性、資料加密、標準化通信協定及無線感測網路(Wireless Sensor Network, WSN)資安防護等項目。現今社會正處於資訊網路蓬勃發展的時代，需同時瞭解物聯網裝置設施特性及相關通信協定，並透過組合語言與逆向工程技術，針對裝備程式碼進行剖析後，始可運用弱點執行網路駭侵。惟熟悉物聯網裝置特性、通信協定及語言程式，非一朝一夕即能培養速成；建議利用委外教育訓練實施物聯網機電工程授課，俾使網路戰人員了解物聯網硬體與軟體之基本觀念及其周邊模組基礎運用。

(三)規劃網路軍售培訓案

全球網路強國不外乎美國、俄國、法國、日本、韓國等，前述國家於近幾年皆有運用網路戰部隊從事網攻實戰經驗，我國網路戰部隊要能與中共匹敵，除與國內產官學研單位合作交流外，亦應極力爭取網路攻防軍售培訓案，藉由人員至網路強國深度學習及技術實作，將國際間網路威脅及攻、防、蒐手法全數吸收，方能確實壯大網路戰能量。

結論

因應國際網路威脅，我國政府除了成立行政院資通安全處，亦積極推動資通安全管理法的立法，同時正式成立資通電軍，作為「資安就是國安」的具體行動。惟面對越來越複雜的網路空間作戰，必須具有更卓越的組織層級與戰略高度，才能夠真正有效因應這些來自網路

對於數位疆土安全的威脅。所以，藉由政府各部會、國防部、中科院及民間產學技術等產、官、學、研等單位支援合作，確保國家關鍵基礎設施的安全，資通電軍也必須要有整合國軍作戰及民間技術之能力，持續精進整體網路能量。另外，亦須加強培育資通電人才。資安人才短缺與不足一直是國家在發展資通安全政策一項致命的缺點，有優秀的人才，才能創造最佳戰力，故應該要提高優秀人才從軍網路戰部隊的誘因，俾以持續壯大網路攻防能量。

資通電軍編成之主要宗旨，除捍衛「數位國土」的責任，最終目標是建立世界級網路攻防能量，使國防相關的資產與基礎設施免於組織性駭客與恐怖分子的網路侵襲；在武器裝備部分，需更積極創新資安動態防護系統、網路滲透攻擊系統、對阻斷服務式攻擊及先進式持續性威脅攻擊偵測反制系統，與惡意程式分析鑑識系統等；在國防預算部分，應持續投資充足預算，提升國軍網路戰部隊能力；在教育訓練部分，藉由完整的網路訓練課程、健全的證照考取制度與高度的對外連結，吸引民間優秀資安科技人物力資源為國防所用，回饋於國家整體數位國土的防護。資通電軍編成係為國軍第四軍種，除強化我國網路空間作戰能力，亦進一步加強國家整體資安防禦，並對敵人形成威懾。此次成軍使我軍網路空間作戰由單一指揮官負責統一指揮，有助於簡化時效性要求高的網路作戰指揮控制。惟因應全球網際網路威脅及順應各國政策發展方向，我國資通電軍亦應參考其組織編制，提升網路戰部隊作戰層級，以適應國軍網路空間長期作戰及鞏固我國國家數位疆土安全。

參考文獻

一、《中華民國 106 年國防報告書》(臺北：國防部，2017 年 12 月)。

二、王清安，〈從美國陸軍網路部隊之組建探討我陸軍通資部隊轉型〉，《陸軍通資半年刊》(桃園)，第 130 期，陸軍通信電子資訊訓練中心，2018 年 9 月。

三、王清安，〈中共網軍發展對本軍威脅評估之研究〉，《陸軍通資半年刊》(桃園)，第 127 期，陸軍通信電子資訊訓練中心，2017 年 4 月。

四、吳孟軒，〈網路權力之爭-美「中」網路攻擊與戰爭初探(The Cyberspace Power Struggles and Cyber Wars Between US and China)〉，《展望與探索》(桃園)，第 12 卷第 7 期，法務部調查局，2014 年 7 月。

五、王清安，〈中共網路空間主權概念建構之研究〉，國防大學戰略研究所戰略與國際事務碩士班碩士論文，2018 年 5 月。

六、江威霖，〈構建國軍網路戰情蒐、防護與攻擊之訓練與評鑑模式〉，國防大學資訊管理學系碩士論文，2013 年 12 月。

七、金登富，〈中共網路戰略思維之概念性探討(The Conceptual Analysis of PLA’s Cyber Strategy)〉，國防大學戰略研究所戰略與國際事務碩士班碩士學位論文，2014 年 3 月。

八、邱陳慶，〈美國網路部隊發展之研究兼論稜鏡事件的影響〉，淡江大學國際事務與戰略研

究所碩士在職專班碩士論文，2017 年 1 月。

九、高清華，〈美軍「第三次抵銷戰略」與美中網路資訊作戰之研究－兼論對兩岸軍事對峙之影響〉，國防大學政治作戰學院政治學系政治研究碩士班碩士論文，2018 年 5 月。

十、莊凱婷，〈網路戰與國家安全—以美國網際空間策略為例〉，國立政治大學外交學系戰略與國際事務碩士在職專班論文，2018 年 7 月。

十一、黃志軒，〈國土安全脈絡下美國網路安全戰略發展(The Development of U.S. Cybersecurity Strategy Under The Concept of Homeland Security)〉，國防大學政治作戰學院政治學系政治研究碩士班碩士論文，2015 年 6 月。

十二、涂俊緯，〈106 年 QDR 公布揭示軍事戰略「防衛固守、重層嚇阻」〉，《青年日報》(臺北)，2017 年 3 月 17 日。

十三、黃庭、劉程鈞，〈資通電軍指揮部編成 總統親臨主持〉，《青年日報》(臺北)，2017 年 6 月 29 日。

十四、〈資訊網路工程師薪水待遇最新情報查詢〉，《1111 人力銀行》，https://www.jobsaiary.com.tw/salarysummary.aspx?codeNo=140402，2018 年 4 月 2 日，(檢索日期：2019 年 2 月 12 日)。

十五、〈67 個國家組建網路戰部隊〉，《觀察者 APP》，https://m.guanvha.cn，2017 年 6 月 8 日，(檢索日期：2019 年 4 月 26 日)。

十六、〈打贏網絡戰爭以色列在行動每月經歷幾十起網絡攻擊〉，《中國新聞網》，http://www.chinanews.com/mil/2017/07-06/8270208.shtml，2017 年 7 月 6 日，(檢索日期：2019 年 2 月 12 日)。

十七、〈南韓重組國防網軍，更名為網路作戰司令部〉，《經濟日報》，https://money.udn.com/money/story/5641/3299704，2018 年 8 月 9 日，(檢索日期：2019 年 2 月 12 日)。

十八、〈受威脅可協助「摧毀敵國軍事系統」，日本防衛省擴編「網路防衛隊」〉，《The News Lens 關鍵評論》，https://www.thenewslens.com/article/73730，2017 年 7 月 17 日，(檢索日期：2019 年 2 月 12 日)。

十九、〈「普丁廚師」如何操縱美大選？揭發俄國網軍運作內幕〉，《鏡週刊》，https://www.mirrormedia.mg/story/putin-cook/，2018 年 2 月 17 日，(檢索日期：2019 年 2 月 12 日)。

二十、〈全球各國駭客部隊戰力總覽〉，《不及格網管之資訊安全暨網通筆記》，http://mis.bankshung.net/，2016 年 6 月 7 日，(檢索日期：2019 年 2 月 12 日)。

二十一、〈魚叉式網路釣魚〉，《資安趨勢部落格》，https://blog.trendmicro.com.tw/，2018 年 10 月 8 日，(檢索日期：2019 年 5 月 3 日)。

二十二、〈揭秘陸軍領導機構火箭軍戰略支援部隊〉，《中國青年報》，http://zqb.cyol.com/html/2016-01/02/nw.D110000zgqnb_20160102_2-01.htm，2016 年 1 月 2 日，(檢索日

期：2019 年 2 月 12 日)。
二十三、〈中國火箭軍和戰略支援部隊，到底有多厲害？〉，《端傳媒》，https://theinitium.com/article/20160121-opinion-military-reform-china-muzhi/，2016 年 1 月 21 日，(檢索日期：2019 年 2 月 12 日)。
二十四、〈美國網路司令部官方簡史〉，《E 安全》，https://www.easyaq.com/news/33130322.shtml，2018 年 7 月 27 日，(檢索日期：2019 年 2 月 12 日)。

作者簡介

李建鵬中校，中正理工學院電機系87年班、國防管理學院指參班101年班。曾任電子官、修護組長、通參官、資參官、電戰官、教官。現任國防大學教官。

蔣建軍少校，中正理工學院電子科94年班、空軍航校國軍電子戰參謀正規班100年班、國防大學空軍指揮參謀學院108年班。曾任資網官、分隊長、訓練官、編裝官。現任資通電軍指揮部計畫官。