從美國陸軍網路部隊之組建探討我陸軍通資部隊轉型

作者／王清安中校

提要

一、 為提升網路空間資訊優勢，2009年美國國防部整合各軍種網路部隊成立網路司令部。與此同時，各軍種又依各自任務需求，發展出所需的網路部隊。在此背景下，美國陸軍網路部隊是如何構建？編組、數量又為何？

二、2017年7月1日我國國防部為強化國軍通資電戰力，將原分散各軍種的通資部隊，整併為新軍種「資通電軍」。我陸軍通資部隊在移編至國防部「資通電軍」後，其通資電戰力是否將遭遇到衝擊？我陸軍又該如何因應？

三、研究發現，美國陸軍為奪佔未來網路空間的制高點，自 2011 年起，將原通信部隊、1 個情報旅及資訊作戰部隊整編為網路司令部。故借鏡該部隊之發展，以及前瞻我陸軍網路戰需求，提出我陸軍「擴建網路部隊能量」等 4 項建議，以肆應未來作戰需求。

關鍵詞：網軍、網路戰、資電優勢、網路威脅。

前言

2013 年，美國陸軍雜誌所刊《持續整建陸軍，以先期預防、型塑網路戰態勢並獲致勝利(Preparing the Army to Prevent, Shape and Win in Cyberspace)》指出，美國陸軍網路部隊若未能確保網路空間的資電優勢，將會影響整體作戰任務。同時，美國陸軍網路司令部(U.S. Army Cyber Command, ARCYBER)應在網路空間中做好充分準備，以便預防衝突、形塑有利戰略環境，繼而取得決定性的勝利。[1]2016 年美國陸軍網路司令部司令卡敦中將(Edward C. Cardon)表示：「隨著網路與作戰環境日漸重疊，未來陸軍的作戰優勢，很大程度上取決於陸軍在網路作戰中有多少把握。」[2]因此，影響未來美國陸軍作戰勝負的關鍵，將取決於網路部隊能否發揮其作用。

要贏得戰爭勝利，就必須要有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、防能力的部隊。2015年9月卡敦中將也曾表示：

---

[1] Rhett A.Hemandez，陳嘉容譯，〈美陸軍在網際空間的全方位策略(Preparing the Army to Prevent, Shape and win in cyberspace)〉《國防譯粹》(臺北)，第 41 卷第 1 期，國防部政務辦公室，2014 年 1 月，頁 5。

[2] Edward C.Cardon, David, P .McHenry and Christopher Cline，趙炳強譯，〈網際空間作戰中創新的重要性(The Relevance of Culture:Recognizing the Importance of Innovation in cyberspace operations)〉《國防譯粹》(臺北)，第 44 卷第 3 期，國防部政務辦公室，2017 年 3 月，頁 23。

「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。」[3]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。」[4]因此，網路人才的素質，對未來網路戰的影響，將是愈來愈重要。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。

2017 年，我國《四年期國防總檢討》報告(Quadrennial Defense Review, QDR)即指出：「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。」[5]同年 6 月 29 日蔡總統出席「通資電軍」指揮部時更表示：「成立資通電軍，就是資安視為國安的具體行動；同時，「資通電指揮部」將整合過去分散在資電作戰指揮部、電訊發展室及各軍種的資電部隊，成為國軍重層嚇阻戰略下的第一層嚇阻兵力。」[6]由此談話及國防部所出版的內容，凸顯出資電作戰將攸關未來我國臺澎防衛作戰勝敗關鍵。

綜合上述，網路部隊發展對未來戰爭是如此重要。然而，截至 2017 年 7 月底，探討我陸軍資電作戰能力能否滿足我陸軍作戰需求，只側重電子戰及網路戰防護作為之論述，而著眼於我陸軍通資部隊之轉型，則是寥寥無幾。這樣過於被動的網路戰思維，將無法在網路空間取得任何優勢。基此，透過研究美國陸軍網路部隊之發展，將有助於提升我陸軍資電戰力，這便是本文研究的動機。雖然，我陸軍與美國陸軍在作戰需求與面臨威脅不全然相同，但在網路部隊發展上，美國的網路戰力仍是全球軍事強國數一數二。故本文採「個案研究法」，首先探討美國陸軍網路部隊與網路戰之關係。其次，瞭解其網路部隊發展過程。接續探討編制、數量，進而評估作戰效能之特、弱點及面臨何種挑戰。最後，提出我陸軍資電部隊轉型建議事項。

網路部隊與網路戰之概述

網路空間是繼陸、海、空及太空的第五維戰場。誰擁有制網權，誰就擁有戰場優勢。要擁有制網權，就必須構建網路部隊，以確保網路空間安全無虞。

一、網路部隊與網路戰之定義

隨著網路科技的發展，網路部隊對未來取得網路戰爭的勝敗，將是愈來愈重要。

---

[3] Ferdinand H.Thomas，楊黎中譯，〈美陸軍網路部隊人才留用(Retaining Soldiers on a New Battlefield:An Army Plugged into Cyber Needs Talented Specialists)〉《國防譯粹》(臺北)，第 43 卷第 2 期，國防部政務辦公室，2016 年 2 月，頁 57。

[4] Bill Roche, “Summit brings leaders together to build ready Total Army cyber forces,” Arcbyer,https://www.army.mil/article/184339/summit_brings_leaders_together_to_build_ready_total_army_cyber_forces,(March 15, 2017), 2017/8/2.

[5] 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 1。

[6] 黃庭、劉程鈞，〈資通電軍指揮部編成 統帥親臨主持〉《青年日報》(臺北)，2017 年 6 月 30 日，版 2。

(一)網路部隊(俗稱網軍)

由於網路空間為資訊終端用戶、實體線路及網路協定所構成。誰能破壞、癱瘓其網路空間，即獲取網路空間之優勢。據「美國陸軍網路司令部」網站指出，美國陸軍網路部隊的任務，即為確保美國陸軍資訊、通訊等系統環境所需的網路空間中，可採取任何行動的自由。同時，拒絕敵方進入該領域。[7]2013 年 6 月司令卡敦中將表示：「網路部隊任務即負責蒐集、分析網路空間中的數位資料，以維護網路設備妥善，如路由器和防火牆等，並對網路空間的各種事件做出處理與回報。」[8]另外，2015 年美國國會一份報告更指出，網路戰士(Cyber Warriors)亦應具備網路戰能力，且支持國家戰略目標所進行的網路攻擊行為。故網路部隊應具備使己方網路空間不受威脅，並透過網路偵測、攻擊等手段，獲取戰場情報優勢，進而癱瘓敵方通資系統能力的網路部隊。

(二)網路戰

2001 年，美國阿爾吉拉(Arquilla)及朗斐德(Ronfeldt)等兩位學者認為，網路戰為非國家行為，是由無政府組織之電腦駭客發起，最終演變成「新層次戰爭」及認識論。[9]2004 年另一位美國阿米斯德(Leigh Armistead)表示，網路戰為擾亂、阻絕或摧毀電腦與網路中的資訊或電腦與網路本身。而資訊作戰則為影響敵方觀察、指導及認知，促使敵方決定採取有利於指揮官軍事目標。[10]不僅如此，2015 年美國國會一份報告亦指出，網路戰(Cyberwarfare)為在網路空間中武裝攻擊或使用武力的狀態相關的行動；其網路活動將導致人員死亡、受傷或關鍵基礎設施重大破壞，如引發核電廠的崩潰，開闢水壩，造成洪水災害，並引起飛機空中交通管制干擾而墜毀。[11]因此，網路戰為運用網路傳輸手段(有、無線電)，對敵人網路空間中的節點、網路協定及終端用戶內的資料實施網路攻擊，以獲取或竄改網路情報，同時保護己方網路空間，不受敵人影響，進而癱瘓敵國重要關鍵基礎設施，引發人民恐慌，影響政府運作機制。

二、美國陸軍網路部隊與網路戰之關係

戰力的發揮，取決於有生力量的整合。要獲取資電作戰優勢，就必須透過網路部隊遂行網路戰攻擊、防禦及支援任務，確保我方網路空間不遭敵方攻擊。

(一)確保通資系統暢通

---

[7] "Cyber officercareer," Acybe, 2010 .U.S.Army, https://www.army.mil/article/40195/cyber-command-to-unite-network-defense-efforts, 2017/8/2.

[8] Ferdinand H.Thomas，楊黎中譯，〈美陸軍網路部隊人才留用(Retaining Soldiers on a New Battlefield:An Army Plugged into Cyber Needs Talented Specialists)〉《國防譯粹》(臺北)，第 43 卷第 2 期，國防部政務辦公室，2016 年 2 月，頁 59。

[9] 約翰・阿爾吉拉(John Arquilla)、國防部史政編譯室，《網路及網路戰》(台北：五南文化廣場，2003 年 8 年)，頁 5-6。

[10] 李·阿米斯德(Leigh Armistead)，國防部史政編譯室，《資訊作戰以柔克剛的戰爭(Information Operations：Warfare and the Hard Reality of Soft Power)》(臺北：五南文化廣場，2008年8月)，頁146-147。

[11] Catherine A. Theohary, and John W. Rollins, "Cyberwarfare and Cyberterrorism:In Brief," Congressional Research Service,Washington D.C.: Congressional Research Service, March 27, 2015, pp.1-3.

「作戰靠指揮、指揮靠通信」。2010 年 6 月 2 日時任美國網軍司令部史密斯將軍(Gen. Steven W. Smith)表示：「美國陸軍網路部隊負責捍衛陸軍網路空間的通資系統網路安全；在網路空間中裡應包含網路終端的資訊設備、資訊協定的路由器，以及實體線路的通資系統。」[12]協助美國陸軍部隊在網路空間，更有效地準備作戰，以取得戰爭勝利；同時，加強與國防部網路司令部進行「動態電腦聯網防衛作戰(Dynamic Computer Network Defense Operations)」，以確保聯合作戰任務成功。[13]不僅如此，2017 年 7 月 31 日美國《國防新聞》報導亦指出，未來美國海軍希望在陸軍的協助下，贏得未來與中國的多領域戰鬥(Multi-Domain Battle)；其中一項關鍵需求即為確保網路空間內的通資系統連接。[14]因此，確保網路空間中的通資系統暢通，對美國陸軍將是極為重要；確保網路空間實體鏈路的安全，則需要由網路部隊負起責任。

(二)強化資電作戰優勢

隨著網路科技的發展，取得網路戰場的資電優勢愈來愈重要。運用電腦攻擊手段(如電腦病毒、特洛伊木馬程序)或遂行資訊阻絕與欺敵，將可創造戰爭決定性優勢。同時，獲取資電作戰優勢，意味著已真正做好聯合作戰之準備。[15]隨著網路威脅日益增加，獲取資電作戰優勢對網路戰是極為重要的部分；其中，確保網路空間行動自由，就需要美國陸軍網路部隊運用新的方法來管理、保護數據資訊。[16]2014 年，美國卡敦中將更明確表示：「網路空間對於連續作戰的各階段非常重要，尤其是在戰場初期(形塑戰場)時，網路部隊的運用，將可提供指揮官預防武裝衝突及支持其目標的靈活選項。同時，亦可增強美國陸軍在網路空間的總體戰力。」[17]因此，網路部隊將為美國陸軍提供網路空間中的資電作戰優勢，並創造聯合作戰勝利的契機。換句話說，搶佔網路空間的制高點，開創勝利有利條件。

總之，要贏得戰爭勝利，就必須在網路空間中確保通資系統的暢通，以及獲取資電作戰優勢。網路部隊不僅提供美軍聯合部隊指揮官所需的網路空間的控制權，亦可削弱敵方進入及使用網路空間的自由權。奪取網路空間的制高點，就是取得部隊運用的主動權。

---

[12] C. Todd Lopez, "Cyber command to unite network defense efforts," arcyber, https://www.army.mil/article/40195/cyber-command-to-unite-network-defense-efforts,(June 2,2010), 2017/8/2.

[13] Rhett A.Hemandez，陳嘉容譯，〈美陸軍在網際空間的全方位策略(Preparing the Army to Prevent, Shape and win in cyberspace)〉《國防譯粹》(臺北)，第 41 卷第 1 期，國防部政務辦公室，2014 年 1 月，頁 5-6。

[14] Sydney J. Freedberg Jr, "Build Bare-Bones Network & Small Satellites For Multi-Domain Battle," the breakning defense, http://breakingdefense.com/2017/07/build-bare-bones-network-small-satellites-for-multi-domain- battle/,(July 31,2017), 2017/8/2.

[15] David S.Albets，李育慈譯，〈資訊優勢的重要觀念(Key Concepts for Information Superiority)〉《國防譯粹》(臺北)，第 36 卷第 4 期，國防部政務辦公室，2009 年 4 月，頁 13-21。

[16] "U.S. Army Cyber Command," arcyber, http://www.arcyber.army.mil/Pages/ArmyCyber.aspx, 2017/8/2.

[17] Rhett A.Hemandez，陳嘉容譯，〈美陸軍在網際空間的全方位策略(Preparing the Army to Prevent, Shape and win in cyberspace)〉《國防譯粹》(臺北)，第 41 卷第 1 期，國防部政務辦公室，2014 年 1 月，頁 5。

美國網軍發展背景與經過

隨著網路科技的普及，網路安全的威脅也相對日益增加。網路安全已威脅到「數位化、立體化」的美國陸軍建軍戰備。故要捍衛網路空間的安全與利益，最重要的手段，即為構建網路部隊。

一、美國網軍發展背景

沒有網路安全，就無法獲取戰爭勝利；確保網路空間的利益與安全，即為美國國防部打贏下一場戰爭的戰略目標。

(一)網路安全威脅日益增加

沒有網路安全，就沒有戰場優勢；要提升作戰優勢，就必須確保網路空間我方數據資料可以自由傳遞。隨著網路科技的發展，數位化、資訊化的通資系統，已強化聯合作戰之效能。然而，愈倚賴網路的部隊，將提供敵人愈可能尋求利用的弱點。同時，敵人也可以運用網路技術，開創網路戰攻勢的機會。[18]2006 年時任美軍聯參「資訊首席(Chief Information Officer)」的通資處長陸軍准將勞倫斯(Susan Laurance)曾公開表示：「美軍在傳統戰場上可以輕鬆面對敵人，但是面對虛擬網路空間的網路攻擊，會是一項挑戰」；另外，時任聯參指管通資系統次長陸戰中將施亞(Robert Shea)更是強調：「網路是美軍作戰的重心，但是網路防禦的能力卻是美軍的致命弱點。」[19]另外，值得注意的是，2008，美國軍方遭敵方特攻人員，將隨身碟插進中東地區美軍基地的筆記型電腦，其結果使得外國控制的伺服器，可以輕易獲取美軍的數據資料。此舉已促使美國必須重視網路安全的重要性，故美國國防部即展開代號「洋基鹿彈行動(Operation Buckshot Yankee)」，著手思考網路攻擊的可能方案。2010 年時任國防部副部長林恩(William Lynn)亦指出：「2000 年至 2010 年間入侵美國軍事網路的頻率和複雜性日益增長。網路戰是不對稱作戰，敵國運用網路攻擊，已對美國軍事能力構成重大威脅。」[20]另外，據 2011 年美國研究表示，網際網路已成為恐怖分子的廉價全球網路；網路戰將會是一場無烟硝的戰場。[21]由此得知，美國國防部已意識網路安全威脅的重要性。因此，構建一個安全的網路空間，確保已身的資訊自由傳輸、不遭竊取，對美國國防部而言，將是至關重要。

(二)打贏下場戰爭(網路戰)

網路戰場要贏得勝利，就必須透過網路部隊在網路空間中佔領數位橋頭堡，破壞

---

[18] 曹雄源，《美國國防暨軍事戰略》(桃園：國防大學，2008 年)，頁 33。

[19] Stew Magnuson，宋家駒，〈網路戰:美國國防部憂心其網路漏洞(Cyber War:Network Vulnerabilities Worry Pentagon)〉《國防譯粹》(臺北)，第 33 卷第 12 期，國防部政務辦公室，2006 年 12 月，頁 25。

[20]Lynn, William J, III, "Defending a New Domain," Foreign Affairs, Sep/Oct 2010, http://search.proquest.com.ezproxy.ndu.edu.tw:2048/docview/749414296/fulltext/77EF5B9019CF4A3APQ/3?accountid=7983#center, 2017/8/2.

[21] 高一中譯，G.Stavridis and Elton C.Parker Ⅲ，〈航向網路之海(Sailing the Cyber Sea)〉《國防譯粹》(臺北)，第 39 卷第 8 期，國防部政務辦公室，2012 年 8 月，頁 8。

敵人通資系統，使敵人在網路空間中無法自由傳遞資訊。2002 年時任總統布希簽署「國家安全第 16 號總統令」，要求國防部制定「網路空間行動戰略(The National Strategy to Secure Cyberspace)」。[22]隨後至 2005 年 3 月，美國國防部正式發布《國防戰略報告(The National Defense Strategy)》即明確指出：「網路空間的戰略地位，與陸、海、空、天等物理空間將等同重要；第五維的網路空間由此而生。」[23]此外，2006 年，美國一篇〈網路戰:美國國防部憂心其網路漏洞(Cyber War:Network Vulnerabilities Worry Pentagon)〉更揭露出，北韓及中共等國家的網路部隊，已對美國國家安全造成重大威脅。同時，美國必須發展網路戰士，即為「資訊安全專業人員(Information Assurance, IA)」。以利戰爭發起後，部署「資訊安全專業人員」，確保作戰勝利。[24]不僅如此，2010 年美國國際事務雜誌刊登出一篇《網路空間制定條約(A Treaty for Cyberspace)》亦明確指出，網路空間已成為軍事戰略家和未來主義者稱之為下一個戰場，美國必須確保在網路空間中持續佔據首席地位。同時，電磁波譜雖然不是一個全新的衝突區域，但對低成本獲取勝利的國家則是愈來愈具有吸引力。此外，網路空間中準備打下一場戰爭的國家，美國不是唯一的國家，中國、俄羅斯、印度、英國和韓國等，已組建網路部隊以獲取網路空間的戰場優勢。[25]此舉意味著美國網路戰已納入軍事戰略目標，發展網路部隊取得戰場優勢，將是打贏未來戰爭重要因素。

因此，美國陸軍在面臨日益嚴重網路空間安全的威脅下，確保已身的資訊自由傳輸、不遭竊取，將是至關重要。同時，支持美軍國防部戰略目標，取得網路空間的利益與安全，並為打贏下一場戰爭做好準備。另外，組建網路部隊更是世界軍事強國奪取網路空間制高點的必要手段。

二、美國陸軍網路部隊發展經過

隨著網路攻擊型態的多樣化及網路戰場的重要性，美國陸軍網路部隊從配屬於各戰區的網路緊應處理應變中心，擴編為與步、砲、裝等兵種位階規模的部隊。其任務由網路被動防護，轉向網路偵察、攻擊與防護等。

(一)成立電腦緊急處理應變中心

2002 年美國陸軍先後成立了陸軍通信司令部(Army Signal Command)及網路科技指揮部(Network Enterprise Technology Command, NETCOM)。[26]隨後至 2005 年，美國

---

[22] The whit washington, “The National Strategy to secure cyberspace,” https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, (February, 2003), 2017/8/2 .

[23] The National Defense Strategy of The United States of America, (March 2005), p13.

[24] Stew Magnuson，宋家駒，〈網路戰:美國國防部憂心其網路漏洞(Cyber War: Network Vulnerabilities Worry Pentagon)〉《國防譯粹》(臺北)，第 33 卷第 12 期，國防部政務辦公室，2006 年 12 月，頁 26-28。

[25] Rex Hughes, “A treaty for cyberspace,” International Affairs, Vol.86, No.2, March 2010, pp.523-541.

[26] 武獲山，〈美國陸軍網路空間作戰部隊組織結構發展解析〉《軍事文摘》(北京)，軍事文摘雜誌社，2016 年 12 月，頁 53-56。

戰略司令部發布《全球資訊柵格網路作戰聯合作戰概念(Joint Concept of Operations for Global Information Grid NetOps)》指出，美國陸軍網路作戰由「太空和導彈防禦司令部/戰略司令部」負責；同時在各戰區成立「電腦緊急處理應變中心(Computer Emergency Response Team, CERT)」。[27]此時美國陸軍的網路部隊僅是確保網路空間的安全，網路防禦作為過於被動。

(二)擴編網路部隊

2008 年 7 月，因應美國防部於 2009 年成立「網路司令部(U.S. Cyber Command)」所需，美國陸軍成立一支營級編制的「網路部隊(Network Warfare Battalion)」。[28]與此同時，「陸軍太空和導彈防禦司令部/陸軍戰略司令部(U.S. Army Space and Missile Defense Command/Army Forces Strategic Command, or USASMDC/ARSTRAT)」的網路部隊仍保留存在。[29]2010 年，美國陸軍正式成立「陸軍網路司令部(Army Forces Cyber Command, ARCYBER)」以作為美國網路司令部(USCYBERCOM)下轄的網路部隊。[30]同時，從通信和情報兵種抽調 2 萬 1 千名士兵，以強化陸軍網路戰力，並於 2012 年具備全面作戰能力，總部設在維吉尼亞州貝爾瓦堡(Ft. Belvoir, Virginia)。[31]

2014 年為強化網路部隊訓練戰力，美國陸網軍司令部與美陸軍訓練暨準則司令部，共同成立新組織部門「陸軍網路訓練中心(Army Cyber Center of Excellence)」(喬治亞州)。該中心，將負責訓練美國陸軍在通信、網路、電子戰及軍事情報界的網路空間專業能力，以滿足網路空間作戰所需。[32]此外，2015 年 4 月 14 日美國卡敦中將(Lt. Gen. Edward C. Cardon)在軍事網路計畫和態勢(Military Cyber Programs and Posture)聽證會上指出：「為強化管理網路部隊人員，美國陸軍已設立新的網路兵種 17(Cyber Branch 17)；需要 3,806 名具備核心網路技能的軍事人員和文職人員。」此外，美國陸軍網路司令部，預劃將 2016 年 10.2 億美元(陸軍獲撥預算 1,265 億美元)，投資 9,000 萬美元投資「陸軍網路訓練中心」新的作戰總部。[33](如表一)

---

[27] Department of Defense United States Strategic command, "Joint Concept of Operations for Global Information Grid NetOps," (Washington D.C, 2005), pp.25.

[28] 理查.克拉克.羅伯特著，呂晶華、成高帥，《網路戰-國家安全的新威脅及應對之策(Cyber war:the next threat to national security and what to do about it)》(北京:軍事科學出版社，2011 年 11 月)，頁 33。

[29] "Organization History Establishment of U.S. Army Cyber Command," arcyber.army, http://www.arcyber.army.mil/Pages/ARCYBERHistory.aspx, 2017/8/2.

[30] Gen. Edward C. Cardo, "2014 Green Book:Army Cyber Command and Second Army," U.S.Arcyber, https://www.army.mil/article/134857,(September 30, 2014), 2017/8/2.

[31] "Information Warfare:More Cyber Warriors Created," Strategy Page, https://www.strategypage.com/htmw/htiw/20140914.aspx,(September 30, 2014), 2017/8/2.

[32] Rhett A. Hemandez，陳嘉容譯，〈美陸軍在網際空間的全方位策略(Preparing the Army to Prevent, Shape and win in cyberspace)〉《國防譯粹》(臺北)，第 41 卷第 1 期，國防部政務辦公室，2014 年 1 月，頁 7-8。

[33] David Vergun, Coming Soon:More Cyber Careers? science.dodlive, http://science.dodlive.mil/2015/05/19/coming-soon-more-cyber-careers/,(May 19, 2015), 2017/8/2.

表一 美陸網軍發展大事紀

項次	年份	大事紀
1	2002-4 年	2002 年，美國陸軍先後成立了陸軍通信司令部以及網路科技指揮部。
2	2005 年	美國戰略司令部發布《全球資訊柵格網路作戰聯合作戰概念》指出，美陸軍網路作戰由「太空和導彈防禦司令部/戰略司令部」負責；同時在各戰區成立「電腦緊急處理應變中心」。
3	2008 年	7 月，陸軍建立了第一個臨時網路戰營。該營的任務包括支持陸軍和國防部各種任務，從戰術支援到旅戰隊。
4	2009 年	5 月下旬，由於國防部備忘錄，指示各軍種建立一個適當的網路部隊，以支持美國網路司令部；陸軍由一名准將負責陸軍網路作戰小組。6 月 23 日，美國國防部通過發表備忘錄的形式宣布建立美國網路司令部。
5	2010 年	2 月 1 日，陸軍副部長批准建立網路司令部，司令部基地位於福爾沃特堡。10 月 1 日，陸軍發布第 2010-26 號總命令，核定陸軍網路司令部指揮官為三星中將，直接向陸軍總部負責。12 月批准 780 個軍事情報旅，納編網軍司令部。
6	2014	美國陸軍網路司令部及訓練暨準則司令部共同為新的「陸軍網路訓練中心(Army Cyber Center of Excellence)」。該中心，將負責訓練美國陸軍在通信、網路、電子戰及軍事情報界的網路空間專業能力，以供網路空間作戰所需。
7	2015 年	4 月 14 日，美國陸軍網路司令部司令卡登中將在軍事網路計畫和態勢聽證會上指出：「為強化管理網路部隊人員，已設立新的網路兵種。

資料來源：武獲山，〈美國陸軍網路空間作戰部隊組織結構發展解析〉《軍事文摘》，軍事文摘雜誌社，2016 年 12 月，頁 53-56；Department of Defense United States Strategic command, Joint Concept of Operations for Global Information Grid NetOps (Washington D.C, 2005), pp.25；“Organization History Establishment of U.S. Army Cyber Command,” U. S. Arcyber, http://www.arcyber.army.mil/Pages/ARCYBER History.aspx, 2017/8/2；David Vergun, “Coming Soon:More Cyber Careers?,” science.dodlive, http://science. dodlive.mil/ 2015/05/19/coming-soon-more-cyber-careers/,(May 19, 2015), 2017/8/2.

美國陸軍網路部隊編組與數量

發揮網路戰力，搶佔網路空間的制高點，必須要有良好的編組與妥善訓練。

一、美國陸軍網路部隊編組

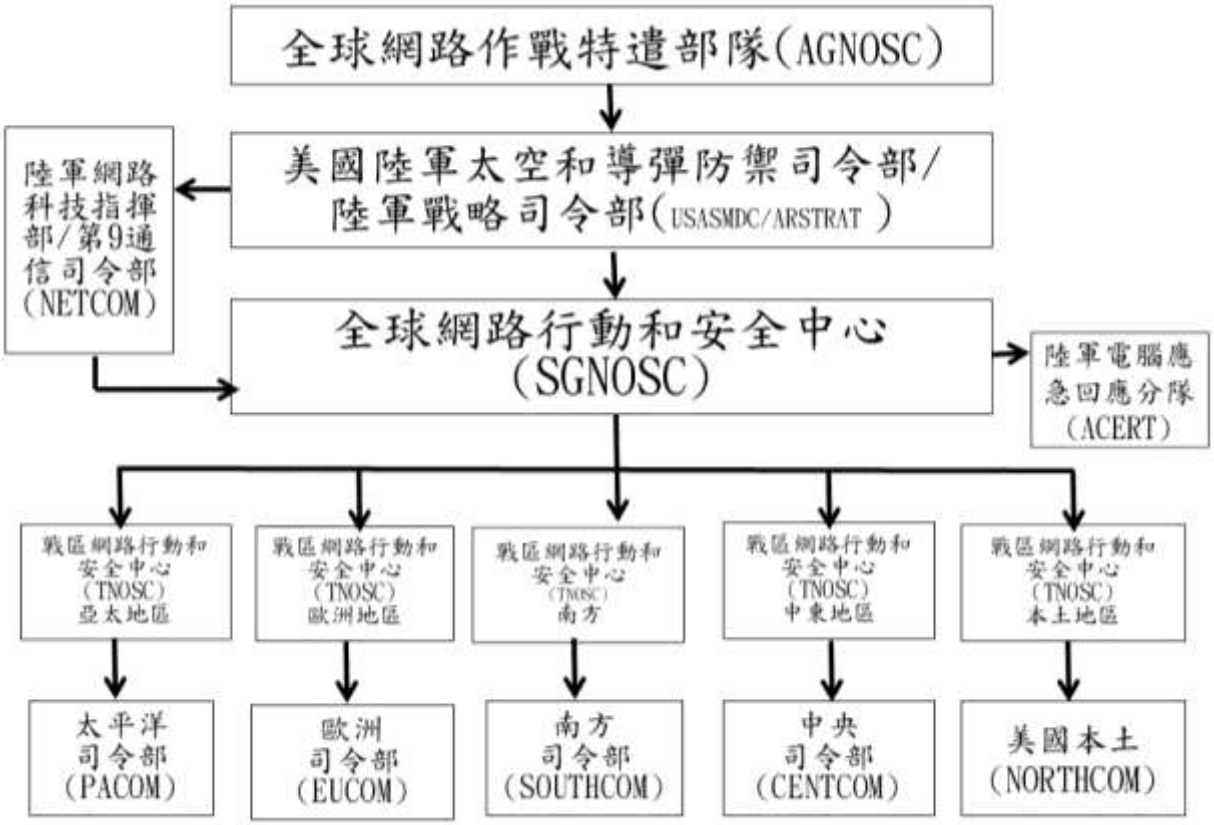
(一)組織架構

2005 年美國陸軍網路作戰體系組織架構劃分為三個層次：指揮層級，由「陸軍太空和導彈防禦司令部/戰略司令部」負責全般統籌指揮。執行、協調網路安全工作，由「陸軍全球網路行動和安全中心」負責。網路作戰行動，則由戰區「網路行動和安全中心(Theater Network Operations and Security Centers, TNOSC)」負責。此外，美陸軍成立「陸軍電腦應急回應分隊(Army Computer Emergency Response Team, ACERT)」，

以強化網路突發事件的處置力量，每個戰區網路行動和安全中心，都建立電腦應急回應分隊。[34](如圖一。)

美國陸軍為提升網路作戰能力，提供作戰指揮官更加全面的戰鬥支援能力，依照網路戰攻擊、防護與支援等任務，區分各種屬性的任務部隊。2011 年美國陸軍司令部，將「第 1 資訊作戰司令部(1st Information Operations Command)」及「情報和安全司令部(U.S. Army Intelligence & Security Command)」下屬的「780 軍事情報旅(780th Military Intelligence Brigade)」納入美國陸軍網路司令部。[35]併將原隸屬位於亞利桑納州瓦卡保(Arizona State)的「網路科技指揮部」(含分布於各戰區的通信人員)，以提供作戰行動所需要的支援。[36]據此，美國陸軍網路司令部已不再是負責網路空間網路安全，而是朝向支援陸軍作戰所需的網路攻擊、防護與偵察等能力發展。

圖一 2005 年美陸軍網路部隊組織架構圖



資料來源: Joint Concept of Operations for Global Information Grid NetOps, https://www.hsdl.org/?view&did=685398, 2017/8/2；Jeffrey L. Caton, "Army Support of Military Cyberspace Operations:Joint Contexts and Global Escalation Implications," The United States Army War College, https://www.hsdl.org/?view&did=761896, (2015/1), 2017/8/2.

[34] "Joint Concept of Operations for Global Information Grid NetOps," https://www.hsdl.org/?view&did=685398, 2016/8/5.

[35] Mr. Richard A David, DoD Training Day, "what's Cyber Hot," U.S Army, ttp://www.isaca-washdc.org/presentations/013/201402-session5.pdf,(February 11,2014), 2016/8/5, pp.4.

[36] 理查.克拉克.羅伯特著，呂晶華、成高帥譯《網路戰-國家安全的新威脅及應對之策(Cyber war:the next threat to national security and what to do about it)》(北京:軍事科學出版社，2011 年 11 月)，頁 33。

2012 年 12 月美國國防部批准了由軍種單位和國家安全局共同提供資源建立 133 支網路任務部隊(Cyber Mission Force)的計畫。其中陸軍的任務是建設其中 41 支網路部隊。另外，依據作戰目的與職能不同，網路部隊區分三種類型：網路戰鬥任務中隊(Combat Mission Team, CMT)，負責支援作戰司令部執行傳統軍事行動；國家任務中隊(National Mission Team, NMT)負責防禦國家關鍵基礎設施，防止惡意網路行動造成嚴重後果；網路防禦分隊(Cyber Protection Team, CPT)將與美國境內所轄電腦網路防禦分隊合作，防禦國防部聯合資訊網路。[37]

不僅如此，網路戰已為全民皆兵的戰爭型態。美國陸軍網路司令部已意識到，網路空間必須納編陸軍「國民警衛隊」和「後備役」網路部隊，才能符合未來作戰需求。[38]另外，美國「陸軍後備役」網路部隊，必要時能迅速提供增援力量。陸軍「國民警衛隊」網路部隊，則可以發揮各州與聯邦政府機構、民事與軍事組織、私營與公共部門之間的橋接作用，強化美國陸軍聯合網路空間作戰能力。[39]2015 年 4 月 14 日卡敦中將表示：「為強化美國國防部內部網路及美國國家關鍵基礎網路防護，美陸軍網路司令部已規劃將陸軍預備役和國民警衛隊共計 21 個網路中隊，供作戰指揮官使用聯合網路作戰，以保護盟友以及美國私營部門。」[40]根據 2017 年美國陸軍網路司令部網站報導證實，美陸網軍已完成 62 個網路部隊訓練(41 個為正規軍，10 個為預備役，11 個為陸軍國民警衛隊)，將可支持聯合作戰司令部、美國網路司令部和美國陸軍作戰。[41]由美陸軍網路部隊編組體系凸顯出，美國陸軍網路司令部為打贏網路戰爭，已完成軍、民網路力量的整合。

事實上，構建聯合網路空間的整體戰力，就必須考量電磁頻譜干擾與反干擾等重要問題。2014 年美國陸軍網路司令部下轄新成立「陸軍網路空間作戰與整合中心(Army Cyberspace Operations and Integration Center, ACOIC)」，其任務負責執行全譜網路空間作戰行動，並負責協調與陸軍其他司令部、其他軍種單位的網路作戰部門，共同執行聯合資訊作戰。[42]另外，美國陸軍為強化網路空間中的電磁頻譜管理能力，成立一個臨時網路電磁區隊(Cyber Electromagnetic, CEM)，負責追踪和管理陸軍網路空間中電

---

[37] Gen. Edward C. Cardo, "2014 Green Book:Army Cyber Command and Second Army," Arcyber, https://www.army.mil/article/134857,(September 30,2014), 2017/8/2.

[38] Rhett A.Hemandez，陳嘉容譯，〈美陸軍在網際空間的全方位策略(Preparing the Army to Prevent, Shape and win in cyberspace)〉《國防譯粹》(臺北)，第 41 卷第 1 期，國防部政務辦公室，2014 年 1 月，頁 7。

[39] "National Guard Bureau Cyber Mission Analysis, Assessment,"http://www.ngaus.org/sites/default/files/pdf/SASC_FY14NDAA%20Sec%20933e%20Assessment_29SEP14.pdf, (September 29,2014), 2017/8/2.

[40] David Vergun, "Coming Soon:More Cyber Careers?," science dodlive, http://science.dodlive.mil/2015/05/19/coming- soon-more-cyber-careers/,(May 19, 2015), 2017/8/2.

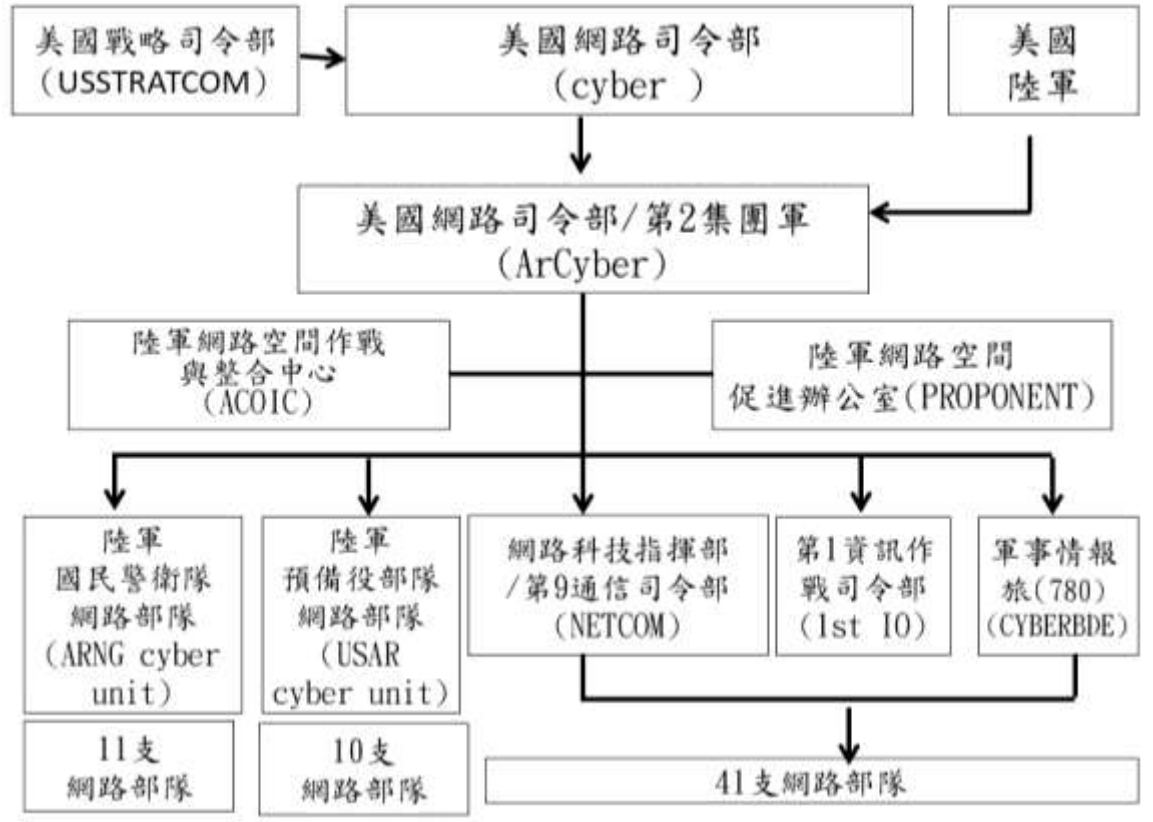
[41] Bill Roche, "Summit brings leaders together to build ready Total Army cyber forces," Arcbyer, https://www.army.mil/article/184339/summit_brings_leaders_together_to_build_ready_total_army_cyber_forces, 2017/3/19.

[42] Jeffrey L. Caton,"Army Support of Military Cyberspace Operations:Joint Contexts and Global Escalation Implications, The United States Army War College, https://www.hsdl.org/?view&did=761896,(January,2015), 2017/8/2, pp.24。

磁頻譜分配、干擾情形。[43]此外，為加強網路作戰訓練，同年 3 月在原通信訓練中心的基礎上，整合電子戰、網路戰等專業元素，成立「陸軍網路訓練中心(Army Cyber Center of Excellence, ACCE)」。2015 年 10 月該中心具網路、通信和電子戰部隊訓練的全面能力。[44](如圖二)

不可諱言，決定網路戰勝關鍵在於創新的網路科技優勢。為確保美國陸軍能繼續保持領先敵人的地位與科技發展的速度，美國陸軍網路司令部在夥伴關係上，擴及至政府、業界及學術界，以建構創新的「網路空間群(Cyberspace Constellation)」網路。同時，美陸軍司令部正與陸軍軍官學校網路研究中心、陸軍研究實驗室及其他單位密切合作，以形塑有利戰略環境。[45]因此，美國陸軍為打贏網路戰爭，獲取網路空間的資訊優勢，乃是將產、官、學、研等單位整合，以為美國陸軍開創網路戰的新契機。

圖二 美陸網軍組織架構圖



資料來源: Jeffrey L. Caton, “Army Support of Military Cyberspace Operations:Joint Contexts and Global Escalation Implications,” The United States Army War College, https://www.hsdl.org/?view&did=761896,(2015/1), 2017/3/19；Gen. Edward C. Cardo,” 2014 Green Book:Army Cyber Command and Second Army,” arcyber, https://www.army.mil/article/134857,(2014/9/30), 2017/3/19.

[43] Gen. Edward C. Cardo,” 2014 Green Book:Army Cyber Command and Second Army,” Arcyber, https://www.army.mil/article/134857,(September 30,201), 2017/8/2.

[44] 同註 43。

[45] Rhett A.Hemandez，陳嘉容譯，〈美陸軍在網際空間的全方位策略(Preparing the Army to Prevent, Shape and win in cyberspace)〉《國防譯粹》(臺北)，第 41 卷第 1 期，國防部政務辦公室，2014 年 1 月，頁 6。

另外值得一提的是，2017年初美陸網軍司令部副指揮官麥基准將表示，美國陸軍網路部隊除強化國家基礎建設防禦外，也逐漸將網路作戰能力整合至戰術環境之中。另外，美軍希望未來能在戰術行動指揮中心增加網路作戰諮詢專家，並為旅級以上的單位中配屬「前進網路管制官」，以提升美國陸軍在戰術環境中更有效地運用網路作戰能力。[46]

總之，美國陸軍網路部隊已於2016年完成整訓。其所編組為「網路科技指揮部」(軍、民網路戰力整合)、「第1資訊作戰司令部」(網路攻擊)及「780軍事情報旅」(網路情報蒐集)，以提供國防安全所需。另作戰管制「國民警衛隊」和「後備役」網路部隊，以確保美國國防部內部網路及美國國家關鍵基礎網路防護，適時供作戰指揮官使用聯合作戰網路空間使用。此外，為做好網路空間頻譜管理，由美國陸軍「網路空間作戰與整合中心」負責對上、下及友軍協調。同時，網路作戰訓練由美國陸軍「網路訓練中心」負責，以強化網路作戰能力。

二、美國陸軍網路部隊數量

由於網路空間為資訊終端用戶、網路協定及實體線路所構成。根據美國陸軍網路司令部網站指出，網路空間的安全防護，由陸軍網路司令部的正規軍、國民警衛隊、預備役等網路部隊，以直接維持戰術邊緣和擴大戰略邊界。[47]

(一)正規軍

2009 年 12 月 22 日美國陸軍網路司令部獲得陸軍副部長的批准，建立一個新的單獨指揮部(309 人)，其司令部位於「福爾沃特堡」。隔年 10 月，陸軍發布了第 2010-26 號總命令，指定三星命令作為美國陸軍網路司令部。該指揮部經授權的 561 人分配在貝爾沃堡和梅德堡。[48]並於 2012 年由 6,000 員發展至 2014 年的 1 萬 4 千員，到 2016 年底為 2 萬 1 千員。[49]

「網路科技指揮部」擁有駐在全球各地士兵、平民和工程師具有網路專業知識約近 16,000 員，將為聯合作戰環境的網路空間，提供保護和操作陸軍網路不受威脅。[50]另外，網路情報旅(780)位於馬里蘭州米德堡基地，編制為 1,200 員，其中 80%為軍人，餘 20%為文職聘雇人員；該旅下轄 2 個營分為 781 營(駐地：馬里蘭州米德堡)及 782

[46] 蘇尹崧，〈因應數位化時代戰爭─美網戰單位建置超前，搶占致勝優勢〉《青年日報》(臺北)，2017 年 2 月 12 日，版 5。
[47] "U.S. Army Cyber Command," arcyber, http://www.arcyber.army.mil/Pages/ArmyCyber.aspx, 2017/3/19.
[48] "Organization History Establishment of U.S. Army Cyber Command," Arcyber, http://www.arcyber.army.mil/Pages/ARCYBERHistory.aspx, 2017/3/18.
[49] 龔鈺哲、岳松堂，〈美國陸軍賽博戰力量建設綜述〉《現代軍事》(北京)，459 期，現代軍事出版社，2015 年 4 月，頁 82-83。
[50] "Network Enterprise Technology Command," arcyber, http://www.arcyber.army.mil/Pages/NETCOM.aspx, 2017/3/19.

營(喬治亞洲米德堡)。[51]

不僅如此，為能提供美國陸軍作戰需求，美國網路戰士已規劃擁有不同的軍職專長。有些是網路密碼戰專業人員(35Q)，執行數位密碼初步分析，建立目標識別和操作模式，並且利用各種參數來分析資訊。「網路防禦人員」(Cyber Network Defender)(25D)係維護基礎設施支援、分析網路防禦資料、對事故和網路損壞做出回應，以及負責網路防禦行動。有些網路戰士也擁有情報蒐集的背景和相當高程度的電腦網路技能。[52]2012-2014 年美國陸軍網路司令部成立 3 個團隊，網路加密分隊負責軍事情報機構的網路安全，計劃人員為 500 員，由 780 軍事情報旅指揮。網路防禦分隊負責網路監控、評估等網路戰任務，為 600 員。通信技術分隊(255S)部署於聯軍司令部，戰區通信司令部等，與網路防禦共同執行美國陸軍網路攻擊與防護，計劃 250 員。[53]故其主要成員，為具有網路專業背景的士兵、平民和工程師組成，其重點任務為網路防禦。

(二)國民警衛隊網路部隊

2014 年 6 月陸軍國民警衛隊與陸軍網路司令部簽署的一份備忘錄，將 2013 年美陸軍國民警衛隊(the Army National Guard, ARNG)網路防禦分隊，轉隸於陸軍網路司令部。[54]這支暫時被稱為第 1636 網路防禦中隊(1636th Cyber Protection Team)，由 39 名組成 (軍官 7 員、16 名士官和 17 位士兵)。其與陸軍網路司令部其他現役部隊共同接受同等標準的訓練。執行任務包括網路空間防禦行動、網路司令部戰備狀態檢查、漏洞評估、網路部隊作戰行動威脅模擬，關鍵基礎設施評估等。[55]因此，美國陸軍為強化網路戰能力，已將國民警衛隊網路部隊納入正規軍併同訓練，以提升網路戰防護能力。

(三)預備役網路部隊

陸軍後備部隊網路作戰小組(The Army Reserve Cyber Operations Group, USAR)是一個大規模網路部隊，於 2016 年 10 月由「陸軍後備役資訊作戰司令部(Army Reserve Information Operations Command)」創建。[56]此外，陸軍在網路作戰力量發展過程中也

---

[51] 龔鈺哲、岳松堂，〈美國陸軍賽博戰力量建設綜述〉《現代軍事》(北京)，459 期，現代軍事出版社，2015 年 4 月，頁 83。

[52] Erdinand H.Thomas，楊黎中譯，〈美陸軍網路部隊人才留用(Retaining Soldiers on a New Battlefield:An Army Plugged into Cyber Needs Talented Specialists)〉《國防譯粹》(臺北)，第 43 卷第 2 期，國防部政務辦公室，2016 年 2 月，頁 57-60。

[53] 龔鈺哲、岳松堂，〈美國陸軍賽博戰力量建設綜述〉《現代軍事》(北京)，459 期，現代軍事出版社，2015 年 4 月，頁 85。

[54] Mike Milord, "Army Cyber Command, Army Guard sign memorandum to integrate cyber protection team," https://www.army.mil/article/127442,(June 5,2014), 2017/3/24.

[55] 武獲山，〈美國國民警衛網路力量發展情況分析〉《軍事文摘》(北京)，第 10 期，軍事文摘雜誌社，2016 年 10 月，頁 50。

[56] Sgt. Erick Yates ,"Army Reserve cyber leaders brief congressional staff delegation," arcyber,https://www.army.mil/article/183907/army_reserve_cyber_leaders_brief_congressional_staff_delegation,(March 8,201), 2017/3/19.

注重相關預備役組織的建設。例如，第 1 資訊作戰司令部還包含 4 支「預備役部隊戰區資訊作戰大隊(Theater IO Groups)」，其都具備提供資訊作戰和網路空間計畫、分析、技術支援能力。[57]根據 2017 年報導指出，美陸軍為強化美陸軍網站上修復網路漏洞，已於 2016 年 12 月推出「陸軍數位役」，以強化網路防護。[58]

總之，美國陸軍網路部隊自 2010 年成立網路司令部，到 2016 底完成正規軍、國防警衛隊、預備役等網路中隊 61 支整訓，共計人員為 2 萬 1 千員；該部隊肩負著陸軍網路空間優勢，支援國防部網路司令部網路空間縱深防禦，以及協助國家關鍵基礎設施網路防禦。

美國陸軍網路部隊能力特、弱點分析

網路空間將是繼陸、海、空及太空後的第五維戰場。在網路部隊發展過程中，必然有達成目標的特點，亦有遇到困難的弱點。

一、特點

打贏下一場戰爭，是軍事戰略目標最高宗旨。建軍備戰是支援達成軍事戰爭目標的必要手段。美國陸軍網路部隊遵循軍事戰爭目標，打贏聯合作戰、做好戰備演訓、整合軍民網路力量，以建構符合其作戰需求的網路部隊。

(一)提升網路空間聯合防禦能力

2014 年美陸網軍司令部所出版的《2014 綠皮書(2014 Green Book:Army Cyber Command and Second Army)》指出，透過「網路科技指揮部」與國防部資訊局(CIO/G6)協調，以提高陸軍網路空間防護能力(Joint Information Environment, JIE)。另外，陸軍網路司令部通過聯合作戰模式，與空軍和國防部資訊系統局，建立一個新的網路防護架構[59]，以提升網路防護能力。此外，根據美國網軍訓練要求《Training for Cyber Soldier》指出，2015 年 10 月徵募的第一批陸軍網路作戰士兵，必須參加的高級個人訓練項目，並於 2016 年 2 月開始。高級個人訓練專案區分二階段，第一階段訓練內容為海軍聯合網路分析師課程 22 週訓練，第二階段訓練同樣持續 22 週，訓練場地也會從海軍設施轉移到陸軍網路訓練中心。[60]另外值得注意的是，陸軍網路司令部透過大數據能力，強化網路監控的持續性，以防止內部威脅和改進記錄程序，進而提高處理的時效性和

---

[57] "Concerning Digital Warriors:Improving Military Capabilities in the Cyber Domain," https://www.hsdl.org/?view&did=734237,(July 25, 2012), 2016/9/2.

[58] 〈美空軍募網路高手 專責武器軟體研發〉《青年日報》(臺北)，2017 月 1 月 8 日，版 5。

[59] 該網路架構旨在增加頻寬和網路安全，同時降低成本。將骨幹頻寬提高到每秒 100G 傳輸能力(每秒 100 千兆字節)，同時促進增強的企業服務，提供更高的容量需求。

[60] "Training For Cyber Soldiers," army cyber, http://www.arcyber.army.mil/Style%20Library/ARCYBER%20Custom%20Assets/factsheets/ARCYBER%20fact%20sheet%20-%20Cyber%20Training%20at%20CCOE%20(15March2016.pdf, 2017/8/2.

有效性，以確保美國陸軍網路空間的行動自由。[61]故美國陸軍網路部隊，為支持聯合作戰型態，在網路空間與國防部、友軍建構起聯合資訊網路環境，確保網路空間安全。另外，為確保聯合資訊網路空間安全，陸軍司令部網路部隊，自 2016 年初，網路戰士須分至海軍及陸軍完成網路高階訓練。

(二)加強網路戰課題演練

提升戰備最務實的手段，即是透過演習以強化部隊戰力。自 2010 年起美國陸軍網路部隊每年均派員至各戰區參與實兵演習及兵棋推演，以提供指揮官規劃網路空間所需的能量。美國陸軍網路部隊也扮演戰鬥訓練中心網路攻擊軍的角色，以提供美國陸軍戰鬥部隊更真實的網路實景，磨練網路空間作戰能力。[62]不僅如此，為能滿足陸軍網路部隊之訓練要求，2015 年美國陸軍通信電子司令部(U.S. Army Communications-Electronics Command, CECOM)更建立一個模擬的網路戰場(Cyber Battlefield)，提供一個現實的網路空間環境，以測試和應用網路戰士於課堂所學的網路技能。同時，該系統已透過 CECOM 的學習管理平台(CECOM's Learning Management Platform)提供線上操作環境和功能，以減少培訓時間和人力成本。[63]故要建構一支具有網路戰力的網軍，就必須透過訓練、演習以提升整體作戰效能。

(三)強化軍民網路整合力量

2015 年 4 月 14 日美國國防部首席網路顧問 Eric Rosenbach 在參議院武裝部隊委員會新威脅和能力分委員會作證詞時(U.S. Senate Committee on Armed Services, Subcommittee on Emerging-Threats and Capabilities)表示：「為強化現役部隊在網路空間的能力，各軍種已制定「預備役構成部隊整合戰略(Reserve Component Integration Strategies)」。該項戰略，將置重點於網路司令部中的現役部隊、文職人員等網路專長人員，與民間企業部門密切合作，以確保網路安全人才可以為國防部及國家服務。[64]此外，2016 年美國國防部已與美國矽谷高科技廠商，共同合作開發網路戰創新項目，以應付敵人利用網路攻擊對抗美國利益；該計畫規劃美國陸軍網路司令部將派遣 10 名網路專業人員(第 780 軍事情報旅、陸軍網路研究所及陸軍網路保護旅)，與 10 個矽谷高科技廠商合作，以提升網路作戰效能。同時，美國陸軍網路部隊將與史丹佛大學合作，以作為「國防駭客

[61] Gen. Edward C. Cardo, "2014 Green Book:Army Cyber Command and Second Army," arcyber, https://www.army.mil/article/134857,(September 30,2014), 2017/8/2.

[62] Rhett A.Hemandez，陳嘉容譯，〈美陸軍在網際空間的全方位策略(Preparing the Army to Prevent, Shape and win in cyberspace)〉《國防譯粹》(臺北)，第 41 卷第 1 期，國防部政務辦公室，2014 年 1 月，頁 6。

[63] Douglas A. Solivan Sr, "Army Launches Cyber Training Range," science.dodlive.mil, http://science.dodlive.mil/07/16/army-launches-cyber-training-range/,(July 16, 2015), 2017/8/2.

[64] Eric Rosenbach, "U.S. Senate Committee on Armed Services, Subcommittee on Emerging-Threats and Capabilities," armed-services, https://www.armed-services.senate.gov/imo/media/doc/Rosenbach_04-14-15.pdf, (April 14, 2015), 2017/8/2.

(Hacking4Defense)」計畫。[65]不僅如此，2017 年 8 月美陸軍更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)」。此特遣隊在完受訓後，將接手現有「第 169 網路防衛隊(169th Cyber Protection Team)」的任務，以強化與維持陸軍網路的基礎架構。[66]故美國陸軍網路部隊正透過軍、民間網路人才的整合，以打造出符合陸軍作戰需求的網路空間。

因此，美國陸軍網路部隊發展過程，其置重點於聯合資訊網路空間整合、建立網路部隊參與實兵演習及兵棋推演機制，以及整合民間產業、學界及研究機構等，強化其網路空間防護能力，確保己身網路空間資訊作戰優勢。這些發展的特點，正是我陸軍構建資電作戰能力借鏡的方向。

二、弱點

美國陸軍網路部隊，要支持各戰區戰演訓練，首當其衝，便是指揮權責不明的問題。其次，隨著網際網路安全日益嚴重，網路人才已成為軍、民間搶手對象。最後，隨著作戰節奏的增快，美陸軍所需要的通資系統之無線電，所遭遇的問題便是頻譜管理問題。

(一)指揮權責不明

網路空間是數個網路終端伺服器所構成。重重網路防護機制，是確保美軍網路防護成功的不二法門。然而，作戰指揮權責與戰鬥支援權責不清時，就會造成網路防護一個看不見的漏洞。2014 年 1 月 19 日美國戰爭學院所出版《網路空間：區域和全球視野(Cyberspace: Regional and Global Perspectives)》研究指出，美軍網路司令部與戰區作戰司令部之間的網路空間指揮與管制仍然是一個嚴峻挑戰。其因，為美軍戰區司令部負責各自戰區內的網路作戰，而美國網路司令部負責網路空間的全球性網路防禦和作戰行動，兩者在網路空間指揮與管制的任務、職責和權限方面的區分並不明確。[67]此外，美國網路司令部和國民警衛局共同舉辦「網路衛士 4-1」演習證實，美國國民警衛隊網路部隊也面臨支援權責未清楚釐清等問題。[68]因此，美國陸軍網路司令部如何整合國防警衛隊、預備役與戰區網路部隊，將是美陸網軍第一個所面臨的挑戰。

(二)網路人力不足

為強化網路安全防護，在軍、民間單位，均以提高待遇招攬網路科技人才。然而，高科技人才培訓不易，在僧多粥少的情況下，對美陸網軍必然造成嚴重的挑戰。2014 年，美國蘭德公司所出版的《駭客招聘:對網路安全工作人力市場調查(Hackers Wanted :

---

[65] KEVIN MCCANEY, “Army, Silicon Valley to tackle social media challenge,” Defense Systems website, https://DEFENSESYSTEMS.COM/ARTICLES/2016/03/10/ARMY-SILICON-VALLEY-SOCIAL-MEDIA-CHALLENGE.ASPX, (MAR 10, 201), 2017/8/2.

[66] 王光磊，〈美後備網軍動員 將列網路司令部〉《 青年日報》(臺北)，2017 年 8 月 22 日，版 8。

[67] Colonel Brett Reister, “Cyberspace Regional and Global Perspectives,” United States Army War College, 2017/8/2.

[68] 武獲山，〈美國國民警衛網路力量發展情況分析〉《軍事文摘》，第 10 期，2016 年 10 月，頁 50。

An Examination of The Cybersecurity Labor Market)》即透露出：「美國的網路安全專業人員嚴重短缺，尤其是在從事國家安全與情報工作，這種的網路安全專業人員的短缺，將使美國在網路空間遭遇到嚴重的衝擊」。同時，美國歐洲司令部(EUCOM)亦因網路人才短缺，已影響到美國參與北約網路防禦夥伴合作的關係。[69]另外，美國全國短缺約 3 萬名網路安全領域人員。在國防部大幅增加網路部隊編制的背景下，也使得各軍種招募網路安全專業人員的困難度增大。[70]另外值得注意的是，由於美國企業也非常欠缺網路科技專業人員，美國頂尖企業都願意提供比軍中薪餉高三倍的優渥薪資，以便做為吸引軍中優秀高科技人員到其公司服務。[71]因此，美軍陸網軍網路部隊在成軍發展過程中，將遭遇網路人才不足的問題。

(三)網電戰力尚未完成整合

由於網路傳輸的快速性及隱匿性，網路戰無法像傳統戰爭中，可以運用後備動員力量陸續投入兵力。美國「網路盾牌-2016 演習」中，即發掘到國防警衛隊網路部隊無法立即投入演習，其原因為無充足的時間做為臨戰轉換訓練，美國民警衛隊網路部隊必須利用一週時間，針對參演人員網路基本技能進行培訓和認證後，才能投入演訓。[72]另外，由於美軍近年來發展的網路戰傾向戰略層面，但在作戰與戰術層面，對各種針對無線電通信的電戰檢測、干擾與欺騙手段，卻較為不重視；該項問題已造成美國陸軍嚴重缺乏電戰專長人員。此外，由於網路安全是橫跨軍、民的共通領域，但電戰專長卻是軍事專長，迫使陸軍不得不派員至海空軍，乃至於陸戰隊，參與地面用電戰系統，甚至高階電戰系統的相關培訓課程。另外值得注意的是，美國陸軍為將網路作戰與電戰整合，已規劃讓擁有一方專長者，能夠獲得另一個專長的培訓，讓網路戰與電子戰，逐漸形成一體兩面的作戰單位。[73]由上述資料凸顯出，美國陸軍網路部隊正面臨著網路空間中的實體安全及網路戰力整合問題。

因此，美國陸軍網路部隊在發展過程中，所面臨著網路部隊指揮權責不明、網路人才不足，以及網電戰力尚未完成整合等問題。亦值得本軍通資部隊轉型過程中借鏡。

策進我陸軍通資部隊轉型發展之道

網路戰不比傳統戰爭，比的是高科技人才、網路實體防護，及軍民整合力量。我

---

[69] Martin C. Libicki David Senty Julia Pollak, “Hackers wanted : an examination of the cybersecurity labor market,” (WASHINGTON, DC: RAND OFFICES SANTA MONICA), 2014, p23.

[70] 同註 68。

[71] Ferdinand H.Thomas，楊黎中譯，〈美陸軍網路部隊人才留用(Retaining Soldiers on a New Battlefield:An Army Plugged into Cyber Needs Talented Specialists)〉《國防譯粹》(臺北)，第 43 卷第 2 期，國防部政務辦公室，2016 年 2 月，頁 59。

[72] 同註 68。

[73] 王光磊，〈媒體提醒：美軍電戰領域落後〉《青年日報》(臺北)，2017 年 2 月 12 日，版 5。

陸軍通資部隊在歷任長官指導、支持下，已朝向數位化通資系統發展，截至2017年已完成旅、營級以上數位化通資系統構連。藉由評估本軍資電部隊戰力，並參考美陸網軍發展之特、弱點，據以策進本軍資電部隊轉型之發展。

一、我國陸軍通資部隊戰力評估

在臺澎防衛作戰中，我陸軍負有國土防衛之重責。延伸至網路空間中，我陸軍資電部隊亦負有維護實體線路安全之重責。然而，2017年7月我陸軍通資部隊於移編國防部資通電軍後，首先極可能面臨指揮權責問題。其次，在徵、募併行的兵役制發展下，我陸軍通資部隊的編現比更是無法與友軍、國防部相比。最後，我陸軍網路戰力，亦因編制不足，無法有效整合軍、民網路戰力。

(一)指揮權責不明，影響構建聯合網路空間安全

我陸軍資電群負有整合作戰區通資系統職責，提供對上國防部聯合作戰指揮中心、對下聯兵旅語音、數據、視訊等功能。然而，隨著 2017 年 7 月國防部資通電軍成立後，原陸軍各作戰區各資電群，以及外(離)島防衛部通資連等單位即併入資通電軍，與各作戰區(防衛部)的作戰指揮鏈，也從原建制關係轉為配屬關係。在組織編裝調整後，其支援作戰區資通能量方面，是否會出現與美陸軍網路司令部與網路司令部，因任務分配上，而產生著指揮權責不明的問題，即待掌握與商確。以美國戰區為例，即希望運用網路部隊配合特種作戰向敵發起攻擊。然而，因網路攻擊是屬於國家安全問題，決定權在於國防部，而非戰區權責。故我陸軍資電群移編後，對我陸軍整體通資電戰力勢必造成影響。

此外，網路空間是透過實體線路與無線網路構成，倘若無法確保傳輸過程中的安全，將加大網路安全之威脅。根據我國前國防部副部長林中斌指出：「目前共諜潛伏在台估計至少有 5,000 位。」[74]雖然，我陸軍指管通資系統，已強化旅、營級資傳保密系統建設，但在我陸軍平時部署仍以有線電為主，在中共「組織戰役與整備階段」即可運用些許的特工、網路部隊，對我陸軍實施突然性網路攻擊，即可癱瘓我陸軍通資系統。此舉意味著我國境內的重要伺服器，亦可能遭到硬、軟殺攻擊，如此一來，我陸軍在網路空間將無任何優勢可為。

(二)網路部隊達編率過低

由於網路戰場是個無邊疆域的戰場，其資訊在網路戰場空間快速傳遞，致使網路空間是無法以地理疆域實施劃定。由於網路攻擊手段已將「偵察、攻擊」整合為一(發現即攻擊)。若加上通資系統的脆弱性，一旦網路空間出現突破點，其所造成的結果，將會是全面性的網路癱瘓。雖然，我陸軍網路空間為各作戰區資電群、聯兵旅/後備旅

[74] 周毓翔、郭建伸，〈5000 共諜在哪？林全也不知〉《中國時報》(臺北)，http://www.chinatimes.com/newspapers/20170315000354-260118，(2017 年 03 月 15 日)，2017 年 3 月 19 日下載。

通資連所構成的內部網路，與外部網際網路有所隔離。但承上述問題指揮與管制權責不明，未來在監控、處理網路空間時，是否會出現真空現象將是令人擔憂。

不僅如此，由於網路人才在現今軍、民市場是可極為搶手的熱門職業，雖然，在2017年我國已同意未來在志願加給－「網路戰勤務加給」方面，規劃將高達5千到5萬元。[75]但面臨選擇擔任網路戰士乙職時，仍不敵國防部、海、空軍等優勢。這項難題和美國陸軍網路部隊面臨同樣困境。另外，2015年，我陸軍備役少將曾祥穎研究表示，未來台、澎防衛作戰將是現實環境與虛擬世界並存的作戰；培養網路人才，將是至關重要。[76]由上述資料凸顯出，我陸軍缺乏網路人才，已是個根本的問題。該項的問題，無疑對我陸軍網路戰防護戰力，造成一個巨大的衝擊。

(三)軍、民網路戰力尚未完成整合

由於網路戰是全民戰爭型態，其網路戰場空間是虛擬、無邊疆化，無法區分戰時與平時階段。雖然，國防部已於2017年7月，邀請國立交通大學進行網路安全交流合作，強化國防部通資安全防護及網路戰士培育能量，以厚實國軍資安防護能量。[77]然而，在我陸軍資電群移編後，以及我陸軍旅級演訓任務頻繁與網路人力不足下，想比照美國陸軍網路司令部的編組人員，與民間學校共同研究網路攻、防能力，實為困難。

此外，由於網路戰攻擊性質，是不分日、夜24小時限制，在我軍資通電戰力值勤人力又不足情況下，運用軍、民網路戰力整合，更顯重要。未來「台、澎防衛作戰」所需資訊流量與通信需求，必將超出現有最大流量的經驗值，所需軍、公民營的資源，便面臨一項考驗。[78]另外，2017 年美國蘭德公司一份報告表示，台灣應該考慮將後備軍人的動員從救災轉化為作戰演訓，並加強與美國的交流，使後備軍人成為有戰力、可以嚇阻中共動武的部隊。該報告亦建議我國在後備軍人中，組成擅長電子與網路作戰的特殊單位，以阻絕敵人進入台灣的電磁領域。[79]故我陸軍網路戰力，在軍、民尚未有明確整合下，實難發揮戰力。

總而言之，我陸軍資電部隊與美國陸軍網路部隊差異，首先在於美國陸軍組織中，設有網軍司令部(三星中將)，編制計有負責網路偵蒐的網路情報780旅、網路安全防護的「網路科技指揮部」，以及專職網路攻擊的「第1資訊作戰司令部」所構建美國陸軍網路空間戰力，並與國防部網路司令部、國土安全部(國民警衛隊、預備役等網路部隊)

---

[75] 劉濰菘，〈5類勤務加給 報請政院核定〉《青年日報》(臺北)，2017年5月5日，版3。

[76] 曾祥穎，〈「大數據」對未來作戰之影響〉《陸軍學術雙月刊》(龍潭)，第51卷第542期，國防部陸軍司令部，2015年8月，頁21。

[77] 黃德潔，〈國防部、交大座談強化資安〉《青年日報》(臺北)，2017年7月27日，版3。

[78] 曾祥穎，〈美陸軍網狀化作戰之檢討與展望〉《陸軍學術雙月刊》(桃園)，第48卷第526期，2012年12月，國防部陸軍司令部，頁19-20。

[79] 曹郁芬，〈美蘭德報告建議：台灣後備軍人 應從救災變能打仗〉《自由時報》，http://news.ltn.com.tw/news/politics/paper/1080806，(2017年2月24日)，2016年8月5日下載。

合作，以確保國家關鍵基礎設施網路安全。其次，美國陸軍網路司令部，還設有「陸軍網路空間作戰與整合中心」，以作為頻譜管理、協調作業單位。第三，為強化網路戰訓練，美國陸軍司令部，亦設置網路訓練中心。此外，並規劃於旅級以上，增設「前進網路管制官」以做網路戰備工作。(如表二)

表二 美軍與本軍網路部隊之比較

區分 / 項目	美陸網軍	本軍
網路戰負責單位	美陸網軍司令部	司令部通資連；各作戰區資電群，聯兵旅/後備旅通信連。
任務	確保美陸軍可在網路空間和通資系統環境中採取任何行動的自由，並拒絕給我們的對手進入該領域。	負責通資系統建立作業與維護。
指揮架構	美國網軍司令部對下指揮第1通信團、780情報旅及企業指揮部，並整合國民警衛隊與預備役網路部隊。	由各作戰區統合運用通資能量。
教育訓練	卓越中心下轄通信兵學校。另透過陸軍官校實驗室。	本軍教準部下轄通資電學校。
人才招募	續服現役獎勵金每月最高領到500美元(約新臺幣：15,000元)；派任加給每月最高能領到300美元(約新臺幣：90,000元)。	新臺幣5千到5萬元。
軍民網路戰力整合	由企業指揮部負責第1通信群戰時納編4個。	由各戰區整合。配合每季軍、公民營會報。

資料來源：作者整理。

二、本軍資電部隊轉型策進建議

承上所述，我陸軍通資電戰力已面臨指揮權責不明等 3 項問題，且在國防總預算有限下，結合我陸軍作戰任務需求優先順先，構建網路空間防禦體系。

(一)擴建網路部隊能量，重新律定指管權責

網路空間安全，不僅要求防禦縱深，亦需要聯合防護。由於網路戰講求是「先發制人、快速應變」，網路節點一旦遭受到突破，就註定戰爭失敗的命運，因為網路安全無法承受任何戰術、意外等風險所造成的損失。此外，中共解放軍已在2015年底，配合軍改將天軍、網軍及電戰部隊，整併為戰略支援部隊，以獲取制太空權及制網權。我陸軍深負國土防衛重責大任，其所鞏固亦是網路空間中實體層傳輸之通信暢通。基

此，建議參照美國陸軍網路部隊發展經驗，成立一個我陸軍網路指揮部(層階為旅級)，以做為協調國防部資通電軍之窗口。此外，重新檢討軍職專長，建議參照美陸網軍在網路戰專長代碼，區分「網路密碼戰專業人員」及「網路防禦人員」等，以提升網路防護能力。

(二)成立網路訓練中心

訓練是確保戰力不二法門。我陸軍「通資電訓練暨測考中心」，負有培育通、資、電等人才之責。然而，該中心因受限教育資源、場地幅員，僅能實施通資電基礎訓練，無法提供最佳網路真實環境，磨練進訓學員網路空間處理能力。鑒此，我陸軍應建議國防部，儘速整合我陸軍通訓中心及通電軍指揮部訓練中心等教、測能量，成立「網路訓練中心」。透過訓練、演訓及學術交流，以提升整體網路空間資電作戰能量。

另外值得注意的是，我國正積極推動國防產業自主化，其中資安產業也是發展要項。另外，在地理位置上，我陸軍「通資電訓練暨測考中心」鄰接新竹科學園區、中科院、電展室，以及中原、交通國立大學及國防大學理工、管理學院。在長遠考量，建議我陸軍「通資電訓練暨測考中心」亦須要成立網路訓練中心部門。該部門，不僅可強化我陸軍網路空間訓練能量，亦可做為整合產、學、研等網路科技能量之窗口。另外，在實體鏈路骨幹銜測等班隊，建議遷回南部原通測中心舊址，藉由崗南地區以強化網路空間實體銜接測試，以達到為戰而訓之目標。

(三)增編網電員額，強化網路戰攻、防演練

沒有頂尖的網路防護人員，就無法捍衛網路空間的資訊節點。但受限於現實環境，目前本軍網路戰課目演練僅能以兵推方式實施，而無法以模擬網路作戰空間實施演練。鑒此，在未來我陸軍各項演習中，建議參照美陸軍網路部隊方式，納編資通電軍擔任假想敵，透過加強網路戰攻、防演練課目，以磨練我陸軍在網路戰攻、防能力的處置程序作為。另外，建議參照美國陸軍網路部隊，除旅級編制通信官(少校)、資訊官(上尉)外，並增設「前進網路管制官」，以落實平戰合一，提升網路空間作戰效能。

(四)打破舊有動員思維，突破傳統框架

網路戰已是繼陸、海、空、太空第五個戰場。以往傳統後備動員觀念，是將動員兵力投入第一線守備部隊，以我陸軍「通資電訓練暨測考中心」為例，動員兵力，為負責支援建立第一線守備部隊通資系統暢通。然而，臨戰轉換的時間是無法守住網路攻擊的快速性。此外，網路高科技人才，若投入第一線戰場實施系統維護，亦無法發揮效果。鑒此，我陸軍在網路戰後備役徵集方面，必須突破舊有框架，建議參照美國陸軍網路部隊，預備役納編民間網路高科技人才，成立為網路特遣隊，配合我國資通電軍指揮部或我陸軍網路部隊共同建構聯合資訊環境，以發揮網路戰力。

結論

曾任美國陸軍網路司令部司令卡敦中將表示:「未來無論陸軍所面臨的挑戰是什麼，都會有網路的成分在內，陸軍必須要對此做好準備。」[80]美國陸軍為提升網路戰力，自2010年起成立網路司令部，並於2016年底完成61支網路區隊整訓。其發展過程中，美陸軍網路部隊為強化其網路戰力，先後整併網路情報780旅、網路攻擊「第1資訊作戰司令部」，以及新成立「陸軍網路空間作戰與整合中心」與「網路訓練中心」。無論美國陸軍網路司令部所遭遇到困難及完成的成效，相信均值得我陸軍在未來構建資電作戰能力參考借鏡。此外，令人驚訝的事，美陸軍網路部隊為打贏網路戰，除擴編網軍現役戰力外，並未受國防部網路司令部影響，仍積極協調民間網路力量，整合產、學、研等機構，以強化其網路戰力，捍衛美國陸軍網路空間優勢。這點亦是我陸軍學習效仿之對象，我陸軍絕不能因資電群移編國防部資通電軍後，就抱以消極、被動的態度來面對未來網路戰的威脅。反之，我陸軍更應積極整合、擴編網路戰力，以確保網路空間之通資暢通，提升資電作戰優勢為發展願景。

參考文獻

一、 李·阿米斯德(Leigh Armistead)、國防部史政編譯室，《資訊作戰以柔克剛的戰爭(Information Operations:Warfare and the Hard Reality of Soft Power)》(臺北：五南文化廣場，2008年8月)。

二、 約翰·阿爾吉拉(John Arquilla)、國防部史政編譯室《網路及網路戰》（台北：五南文化廣場，2003年8年）。

三、 曹雄源，《美國國防暨軍事戰略》(桃園：國防大學，2008年)。

四、 理查.克拉克.羅伯特著、呂晶華、成高帥，《網路戰-國家安全的新威脅及應對之策》(Cyber war:the next threat to national security and what to do about it)(北京:軍事科學出版社，2011年11月)。

五、 龔鈺哲、岳松堂，〈美國陸軍賽博戰力量建設綜述〉《現代軍事》(北京)，459期，現代軍事出版社，2015年4月。

六、 David S. Albets，李育慈譯，〈資訊優勢的重要觀念(Key Concepts for Information Superiority)〉《國防譯粹》(臺北)，第36卷第4期，國防部政務辦公室，2009年4月。

七、 Edward C.Cardon, David, P .McHenry and Christopher Cline，趙炳強譯，〈網際空間作戰中創新的重要性(The Relevance of Culture:Recognizing the Importance of

[80] Ferdinand H.Thomas，楊黎中譯，〈美陸軍網路部隊人才留用(Retaining Soldiers on a New Battlefield:An Army Plugged into Cyber Needs Talented Specialists)〉《國防譯粹》(臺北)，第 43 卷第 2 期，國防部政務辦公室，2016 年 2 月，頁 57。

Innovation in cyberspace operations)〉《國防譯粹》(臺北)，第44卷第3期，國防部政務辦公室，2017年3月。

八、 Ferdinand H.Thomas，楊黎中譯，〈美陸軍網路部隊人才留用(Retaining Soldiers on a New Battlefield:An Army Plugged into Cyber Needs Talented Specialists)〉《國防譯粹》(臺北)，第43卷第2期，國防部政務辦公室，2016年2月。

九、 G. Stavridis and Elton C. Parker，高一中譯，〈航向網路之海(Sailing the Cyber Sea)〉《國防譯粹》(臺北)，第39卷第8期，國防部政務辦公室，2012年8月。

十、 Stew Magnuson，宋家駒譯，〈網路戰:美國國防部憂心其網路漏洞(Cyber War: Network Vulnerabilities Worry Pentagon)〉《國防譯粹》(臺北)，第33卷第12期，國防部政務辦公室，2006年12月。

十一、武獲山，〈美國國民警衛網路力量發展情況分析〉《軍事文摘》(北京)，第10期，軍事文摘雜誌社，2016年10月。

十二、武獲山，〈美國陸軍網路空間作戰部隊組織結構發展解析〉《軍事文摘》(北京)，軍事文摘雜誌社，2016年12月。

十三、曾祥穎，〈美陸軍網狀化作戰之檢討與展望〉《陸軍學術雙月刊》(桃園)，第48卷第526期，國防部陸軍司令部，2012年12月。

十四、Martin C. Libicki David Senty Julia Pollak, “Ackers wanted:an examination of the cybersecurity labor market, (WASHINGTON, DC:RAND OFFICES SANTA MONICA), 2014.

十五、Catherine A. Theohary, and John W. Rollins, “Cyberwarfare and Cyberterrorism:In Brief,” Congressional Research Service,Washington D.C.: Congressional Research Service, March 27, 2015.

十六、Colonel Brett Reister, “Cyberspace Regional and Global Perspectives,” United States Army War College, 2017/8/2.

作者簡介

王清安中校，中正理工學院88年班、陸軍通信電子資訊學校正規班175期、國防大學陸軍學院98年班、國防大學戰院暨戰研所107年班，曾任排長、連長、通參官、營長、主任教官，現任通資組組長。