國防大學政治作戰學院政治學系研究所

碩士學位論文

國軍資訊與心理作戰整合之研究

A Study on the Integration of Information Operations and Psychological Operations in the R.O.C. Armed Forces

研究生：蔡沛辰 撰

指導教授：曾維國 博士

中華民國一〇九年五月

國防大學政治作戰學院政治學系碩士學位論文

口試委員會審定書

國軍資訊與心理作戰整合之研究

A Study On The Integration Of Information Operations and Psychological Operations In The R.O.C. Armed Forces

本論文係蔡沛辰君（學號：1090720102）在國防大學政治作戰學院政治學系完成之碩士學位論文，於民國109年5月12日承下列考試委員審查通過及口試及格，特此證明。

指導教授 曾維國

委　　員 郭雪真

委　　員 袁烏

學系主任 莫大華

中華民國109年05月12日

國防大學政治系碩士生論文文責自負聲明書

本人瞭解並保證所撰寫之論文完全遵守著作權法及學術倫理規範，指導教授已善盡告知、審查、監督之義務。論文倘有抄襲、捏造、改作、妨礙他人著作權，或其他一切有違著作權及學術倫理規範之情事，以及衍生相關民、刑事責任者，概由本人負責，與指導教授、論文口試委員及政治學系所有師長無關。

論文題目：國軍資訊與心理作戰整合之研究

研究生：[redacted]（簽章）

學號：10907201O2

指導教授：曾維國

我已閱讀下方說明，並同時繳交原創性檢測報告。：

☑論文原創性檢測報告

☑學位論文口試作業規定第肆(六)條

經遭檢舉論文抄襲，且調查屬實者，雖已授予學位，專案報請國防部予以撤銷，並註銷其已發給之結業證書與學位證書。

中　　華　　民　　國 109 年 5 月 12 日

謝詞

經過長時間的奮鬥，終於完成這一份論文的撰寫。首先感謝指導老師曾維國博士耐心在論文撰寫的全程協助我檢視並修正每一個細節讓這份論文更加完美。再來必須感謝系主任莫大華博士以及曾經在課堂上給予我學術指導的每一位老師，讓我快速地累積必要的知識，使已經放下書本十數年的我具備足夠的能力與信心進行學術文章寫作。另外，也要感謝同學年的各位研究所同學們，與各位一同度過的歡樂時光已成為我心中畢生難忘的寶貴記憶。最後，感謝我的家人讓我在北上就讀研究所期間無後顧之憂，能夠致力於學業，終能完成我在此一階段中所設定的目標，繼續往人生的下一個階段邁進。


國防大學
National Defense University

摘要

近年國內外多有學者指出中華民國正陷入烏克蘭式危機，指出中共正試圖複製俄羅斯併吞克里米亞之經驗，運用其信息戰手法，侵略我國於無形。此外，我國前參謀總長李喜明上將於民國108年漢光35號演習中增設（任務編組的）「資訊作戰中心」，用以整合情報、網路、電子、謀略、欺敵、輿論、心理、保防、特種作戰以及戰略溝通等功能；而此能力整合之方式，神似於美軍資訊作戰機制，以上，遂成為筆者之研究動機。進而，本文試圖探究：一、美軍資訊作戰能力安排與機制設計，及其資訊作戰乙詞之完整概念意涵。二、探討中共解放軍信息戰之本質及其戰略支援部隊的信息戰職能。三、國軍現行資訊作戰機制以及相關部隊能力是否足以應對中共對我信息戰。

本研究基於探討我國資訊作戰機制之發展，試圖參考美軍及解放軍資訊作戰機制，以知己知彼，甚至以敵為師，蒐整相關文獻，分析美軍及解放軍資訊作戰制度的演變及其現況，再檢視我國當前聯合作戰機制下之資訊作戰有關能力，最後透過SWOT競爭策略分析架構進行策略發展，尋求我國資訊作戰機制發展之整合走向。本研究顯示：一、心理作戰於資訊作戰中之重要性受到低估，建立完善之資訊作戰機制必須適當將資通電能力與心理作戰相互結合；二、我國尚無美軍「資訊環境(information environment)」之概念，而此概念對於當代之國防安全至關重要，且有賴於平時之經營；三、我國資訊作戰之機制尚未發展完備，若不改善恐難解決當前所面臨之本位主義弊病。

關鍵字：資訊作戰、心理作戰、整合。

Abstract

Researchers from different nations indicate that the R.O.C. is falling into the Ukrainian style crisis, and CCP is trying to duplicate the Russian experience in the successful annexation of Crimea, an invisible invasion by its information operations(IO). In addition, Adm. LI, HSI-MING, the former chief of staffs had set up a wartime organization, “IO center”, during the Han Kuang 35th Exercise, integrating intelligence, electronic warfare, strategy, military deception, public affairs, psychological operations, military security, special operations, and strategic communication; and this kind of capability integration seemed like the IO mechanism of the United States military. All above forming the author’s motivations for this research. This research investigates three critical issues: 1.The arrangement and mechanism design of the U.S. military IO and the thorough conecpts. 2. Looking into the heart zone of the PLA IO, and the capabilities for the Strategic Support Force operating it. 3. To evaluate whether our current IO mechanism and unit capabilities enough for countering the threats from PLA IO.

For better development of IO mechanism in R.O.C., this research takes U.S. armed forces and PLA IO as a reference, knowing our enemy, or even learning from them. By analyzing U.S. and PLA IO institutuonal evolutions and their current status, this paper exams the R.O.C. armed force IO capabilities under current joint operations mechanism and adopts SWOT analysis to develop proper strategies for the development and integration of the IO mechanism of the R.O.C. armed forces. There are three important findings in this research: 1. The importance of the psychological operations in the IO mechanism is heavily underestimated, it requires full integration among information, communication, electronics, and psychological operations for a complete IO mechanism. 2. The R.O.C. armed forces are lacking the concept of “information environment” which is critical for national security and relies on constant managing during peacetime. 3. The IO mechanism in the R.O.C. armed forces remain to be developed and improvements must be made to refrain the negative influence from parochialism.

Key Words: Information Operations, Psychological Operations, Integration.

目錄

圖目錄

表目錄

第一章、緒論

自從 2014 年俄羅斯以資訊作戰手段兼併克里米亞之後，資訊作戰帶來的新型威脅受到全球矚目，然而當時國內研究者似乎未能多加關注此一新形態威脅之發展。直至 2018 年英國衛報以〈中共是否會將臺灣變成下一個克里米亞〉的標題刊登之報導，[1]方才喚醒國內研究者，並開始將烏克蘭以及克里米亞當時面臨之資訊作戰威脅與我國所面臨之威脅進行對比，[2]而中共解放軍戰略支援部隊這支被歐美研究者稱為「中國的資訊作戰部隊」在 2016 年初成軍，我們除了可以從其中嗅出解放軍依照美軍資訊作戰能力整合輔以軍隊改組，積極發展解放軍資訊作戰能量之意圖外，亦可從其將人稱「三戰基地」之三一一基地納入戰略支援部隊轄下，感受到「克里米亞模式」之資訊作戰威脅似將成真。

有鑒於此，我國國防部為了應對中共信息戰相關威脅，近年除了成立資通電軍之外，亦在前參謀總長李喜明上將之規劃下，於民國 108 年漢光演習中新增了「資訊作戰中心」這個戰時編組，[3]其能力整合之模式似與美軍資訊作戰之概念相似。

---

[1] Simon Tisdall, "Will China turn Taiwan into the next Crimea," *The Guardian*, April 3, 2018, <https://www.theguardian.com/world/2018/apr/03/how-safe-is-taiwan-from-becoming-the-next-crimea-us-china>.(Accessed:6/4/2020)

[2] 將克里米亞與臺灣現況類比之國內研究者諸如臺北大學犯罪研究所助理教授沈伯洋以及臺灣教授協會等組織，詳見: https://www.tahr.org.tw/news/2325。克里米亞與臺灣在歷史背景上有許多近似之處可作為對比，在俄國反共內戰中，擁護沙皇並企圖恢復羅曼諾夫王朝的白軍，最後被迫退守至克里米亞島作為其「復興基地」，然而仍因缺乏天險而被俄共殲滅。因此，當代之俄國文學家如阿克薛諾夫在其作品《克里米亞島》中，產生了如果克里米亞如臺灣一般有海峽天險阻隔，是否也能如同中華民國偏安一隅的嗟嘆；詳見: 賴盈銓，〈阿克薛諾夫小說《克里米亞島》中的「臺灣主題」〉，《俄國語文學報》，第五期，2002 年 6 月，頁 245-262。另外，俄國文學家索忍尼辛於 1982 年 10 月 23 日受邀於臺北中山堂演講之時也說道：「富蘭哥爾將軍在俄國內戰據守的克里米亞很可能成為俄國的這麼一塊土地.....而在中國，由於海峽遼闊，臺灣就成了中華民國所留下的一塊復興基地」。編譯者不詳，《索忍尼辛的聲音與迴響》(臺北:黎明文化事業股份有限公司，1982 年 11 月)，頁 150。

[3] 洪哲政，2019/3/22。〈年度漢光兵推今展開首次推演假新聞攻擊與反制〉，《聯合新聞網》，<https://udn.com/news/story/10930/3769841>。(瀏覽日期：2020 年 3 月 18 日)

然而，我國針對資訊作戰及中共信息戰相關之研究，多係針對資安方面，忽略了資訊作戰抑或中共信息戰中能力整合之取向，尤以忽略心理、認知層面之議題，未能多加探討。在此情勢下，闡明究竟何謂資訊作戰並探討我國當前資訊作戰能力是否足以應付中共之信息戰威脅極為重要，是故，本文將針對美軍資訊作戰機制、中共戰略支援部隊之組織架構與職能內涵以及我國當前資訊作戰相關部隊之能力進行綜合性探討，並以 SWOT 競爭策略分析架構分析之，藉以提出我國資訊作戰機制發展之建議，以利應對來自中共解放軍戰略支援部隊之信息戰威脅。

第一節、研究動機與目的

壹、研究動機

我國前參謀總長李喜明上將於國軍民國108年精神戰力專案教育總長總結教育中談到：「我們藉由網路與傳媒，將所望的訊息，傳遞給敵方軍民，去影響他們的心理，進而達到策應軍事作戰的目標，也是非常重要的，所以今年我們新增加了一個資訊作戰中心，藉由這個組織來整合情報、網路、電子、謀略、欺敵、輿論、心理、保防、特種作戰以及戰略溝通等功能」[4]，李上將此一說法別有新意，具有政策宣示作用，甚至已是實驗性運作或驗證某些新構想，似可以「軍事轉型」(military transformation)[5]視之；若然，國軍資電作戰與心理作戰之整合值得探究，

[4] 華視，〈國軍 108 年精神戰力專案教育-總長教育總結〉，《國軍 108 年精神戰力專案教育》，國防部，2019 年 5 月 22 日，<https://www.youtube.com/watch?v=gTb_4RPU4E0&feature=youtu.be>。

[5] 軍事轉型(military transformation)一詞，依據美國國防部部長室部隊轉型辦公室 2003 年秋季出版的報告，軍事轉型是指「軍事競爭與合作之變動本質的形塑過程，藉由國家優勢的運用以及保護自身的不對稱脆弱性，將各種概念、能力、人員、組織賦予新的結合，以維持有助於支撐世界和平與穩定的戰略地位。」Office of Force Transformation, *Military Transformation: A Strategic Approach*, (Washington: Department of Defense, Fall 2003), P. 2. 此外，美國蘭德(RAND)智庫設有"military transformation"的主題網頁，該網頁對軍事轉型的簡要定義是：國家為達成某一特定目的所採取的軍事調整(the adjustment of a nation's military to achieve a specified objective)；相關資訊可參閱：http://www.rand.org/topics/military-transformation.html(Accessed 20/09/2019)

此為研究動機之一。

美軍聯合作戰資訊作戰準則JP3-13中對資訊作戰(Information Operations, IO)之定義為：「在軍事行動中，整合運用資訊相關能力並配合其他作戰行動來影響、干擾、破壞或竄改敵人或潛在敵人的決策，同時也對我方決策進行防護。」[6]其中所謂資訊相關能力(Information Related Capabilities, IRC)，計有：戰略溝通(Strategic Communication, SC)、聯合跨部會協調組(Joint Interagency Coordination Group)、公共事務(Public Affairs)、軍民作戰(Civil-Military Operations, CMO)、網路作戰(Cyberspace Operations, CO)、資訊確保(Information Assurance, IA)、太空作戰(Space Operations)、軍事資訊支援作戰(Military Information Support Operations, MISO)、情報(Intelligence)、軍事欺敵(Military Deception, MILDEC)、作戰安全(Operations Security, OPSEC)、特殊技術作戰(Special Technical Operations, STO)、聯合電磁頻譜作戰(Joint Electromagnetic Spectrum Operations, JEMSO)及關鍵領導人交涉(Key Leader Engagement, KLE)等14項能力，透過上述14項能力之整合來創造有利於美國政府及其軍事目標之資訊環境。[7]以上是美軍資訊作戰轉型的概況，可作為我國資訊作戰相關能力整合及資訊作戰機制建立之參考，此為動機二。

事實上，資訊作戰得到全球注目之起點始於1991年之波斯灣戰爭，當時美軍在伊拉克地區運用資訊作戰配合正規武力戰席捲伊軍之後引發各國關注；而俄羅斯在2014年未發一兵一卒侵吞克里米亞(Crimea)，更使全世界對於資訊作戰有了新的認識，誠如美國蘭德公司(RAND Corporation)指出，俄羅斯侵吞克里米亞的手段即包含「資訊作戰」，[8] 另外，薩宗諾夫(Vladimir Sazonov)等學者之研究更直指俄羅斯係透過長時間的資訊作戰來達成併吞克里米亞之目的[9]。在各國熱議之際，國內

---

[6] Joint Chiefs of Staff, "*Joint Publication 3-13: Information Operations*," November 20, 2014, p. ix.

[7] Ibid., pp. II-5 - II-13.

[8] Michael Kofman, et al. *Lessons from Russia's Operations in Crimea and Eastern Ukraine*(Santa Monica, CA: RAND Corporation, 2017), pp. 64-75.

[9] Vladimir Sazonov et al. "Methods and tools of Russian Information Operations used against Ukranian Armed Forces: The Assessments of Ukranian Experts," *ENDC Occasional Papers*, Vol 6, 2017.pp. 52-66.

亦有諸多聲浪指出「臺灣正面臨烏克蘭式危機」[10]、「臺灣正克里米亞化」[11]之憂慮−中共試圖複製俄國侵吞克里米亞的經驗，對我國實施無形的侵略，而此威脅一開始看似漫無邊際，但隨著人民解放軍戰略支援部隊在2016年成軍，並從2018年起循美軍資訊作戰模式陸續整合了「情報」、「電子對抗」、「太空」、「偵察」、「網路」以及「心理戰」等軍事能力後，[12]解放軍發展資訊作戰對我國可能造成之威脅愈發明顯，不可輕忽，此為動機三。

以上顯示，資訊作戰已與傳統概念有異，其發展似有朝向功能擴充甚至軍文整合的現象，實有進一步研究的必要。其中，美軍業已推行心理作戰(Psychological Operatinos, PSYOP)與資訊作戰整合為所謂「軍事資訊支援作戰」(MISO)的軍事轉型數年，[13]因此，筆者認為國軍亦應從軍事轉型的方向進行建軍備戰的思考，才能維持可恃戰力，確保國家安全無虞。

綜上所述，解放軍戰略支援部隊顯然是中共當代軍事轉型及資訊相關能力整合之結果，而我國相對應於戰略支援部隊相關能力之軍事單位為通資電軍及心理作戰大隊等兩個部隊單位，而此兩單位當前之運作機制是否足以因應人民解放軍戰略支援部隊帶給我國之資訊作戰威脅，抑或應「師夷長技以制夷」，進而推動我國資訊作戰機制發展及相關能力之整合，當是國軍應該優先探討研究並預擬應對做為之優先事項。

---

[10] 洪博學，〈台灣正面對「烏克蘭式危機」〉，《民報》，2019 年 1 月 31 日，< https://www.peoplenews.tw/news/795e8505-7b42-4c4f-a931-5f414a2671a3 >。

[11] 蔡志弘，〈台灣正克里米亞化〉，《中時電子報》，2019 年 3 月 4 日，< https://www.peoplenews.tw/news/795e8505-7b42-4c4f-a931-5f414a2671a3 >。

[12] 國防部，《國防報告書》(台北：國防部，2017 年)，頁 33。

[13] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. iii.

貳、研究目的

一、 我國目前似有意參考美軍經驗發展我國之資訊作戰機制，鑒此，本研究希望能解析美軍資訊作戰機制之完整概念及其能力組建，凸顯資訊作戰「能力整合」之特性與心理作戰之核心地位。

二、 認識解放軍信息戰與三戰之發展，以及戰略支援部隊之能力組建可能對我國帶來之資訊作戰威脅。

三、 檢視國軍相關單位之能力、限制，探索國軍此一領域（資訊、心理及其他相關作戰能力發展）整合必要及其可能取向，並參考美軍經驗對國軍未來在資訊作戰與心理作戰之發展上有何借鑒?

第二節、文獻回顧

壹、資訊作戰（Information Operations）

資訊戰（Information Warfare）與資訊作戰（Information Operations）兩個相近的名詞常造成研究者的混淆，而美國國會研究處的資訊戰學者希歐海莉(Catherine A. Theohary)認為，美國政府各部門現行準則中雖未賦予資訊戰明確之定義，但通常將其以「為追求相對優勢所進行的資訊運用與管理」，其中包含了攻勢及守勢作為，而「warfare」一詞通常與武裝衝突或其他軍事相關活動劃上等號，但政治作戰（political warfare）則被理解為一運用政治手段使敵人服從於其意志，[14]在此觀點下，資訊戰其實就是政治作戰的其中一種形式。然而，筆者於1998年版的美軍聯合作戰資訊作戰準則中發現，當時美軍賦予資訊戰（IW）的定義為：「在危機、衝突及戰爭時期對單一或多個敵對勢力(adversaries)進行的資訊作戰(IO)，以達成或推展特定目標」，[15]然而在後續的2006年版資訊作戰準則中，即將資訊戰乙詞移除。[16]

從拿破崙時代開始，作戰就可以區分為三個階層：戰略階層（strategic level）、作戰階層（operational level）與戰術階層（tacticle level），資訊戰發生在戰略層面，而資訊作戰屬於作戰階層，旨在運用各種與資訊有關的能力及戰術來實現其所支持之戰略目標，在作戰階層中必須透過計畫、執行來確保戰役與主要作戰行動以達成戰區或作戰地區內之戰略目標，作戰行動為達成這些戰略目標而將特定的戰術、技術與程序與之相互鏈結。戰術階層的作戰所考量的則是透過將各戰鬥單位在敵我之間進行秩序井然的安排與調動來實現作戰目標。[17]簡言之，相對於資訊戰，資訊作戰是較低層次的作戰行動，而此行動整合了各種資訊相關能力與戰術戰法來

---

[14] Catherine A. Theohary, "*Defense Primer: Information Operations*," December 18, 2018, p. 2.

[15] Joint Chiefs of Staff, "*Joint Publication 3-13: Information Operations*," October 9, 1998, p. I-1.

[16] Joint Chiefs of Staff, "*Joint Publication 3-13: Information Operations*," January 13, 2006, p. iii.

[17] Catherine A. Theohary, *Defense Primer: Information Operations*, op. cit., p. 2.

使資訊戰所欲達成之戰略目標完美實現。

另外，她也提到，資訊作戰可能是公開進行的，例如政府刻意製作與傳散民主價值的訊息，在此情況下，政府對這種活動的參與便是廣為人知的，祕密的資訊作戰行動是指那些如果被察覺有政府參與便將遭拒的行動，網路空間所提供之匿名性可為這種秘密的資訊作戰提供理想的戰場，但她也認為資訊作戰的戰場並非單純只有網路空間。[18]

從其觀點我們可以將資訊戰與資訊作戰的關係理解為資訊戰包含但不等於資訊作戰，資訊作戰可能只是資訊戰的戰場中其中一個工具，但她未詳細戰略、作戰、戰術三個階層之差異，若以美軍聯合作戰資訊作戰準則JP3-13中，針對各種不同階層作戰所列述之評估要點（assessesment criteria）解析之：戰略階層的評估要點在於是否能達成戰區或國家之目標、戰術階層之評估要點在於是否能完成一項計畫或戰役、戰術階層則專注於特定的、地方性的軍事活動評估。[19]此解釋應較能區別各階層作戰之分野。

美國蘭德公司的資訊作戰專家保羅(Christopher Paul)則將資訊作戰之各項能力區分為三個部分，分別為「資訊內容」、「資訊系統」、「其他相關之資訊能力」，資訊內容包含了心理作戰、軍事欺敵以及作戰安全，資訊系統則囊括電子戰與電腦網路作戰(現為網路作戰)，其他相關軍事能力則有公共事務、軍民作戰等。[20]由於其著作早在2008年出版，故其分類未能完全與現況相連結，但為各項資訊相關能力作出清楚的屬性劃分。在其2018年的研究中則強調了資訊環境（Information Enviroment, IE）的重要性，而在資訊環境中，可區分為三個場域，第一為認知域（cognitive dimension），以人為中心（human centric）；第二為資訊域（information dimension），以資料為中心（data centric）；第三為實體域（physical dimension），以

---

[18] Catherine A. Theohary, *Defense Primer: Information Operations*, op. cit., p. 6.

[19] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. VI-13.

[20] Christopher Paul,"Information Operations: Doctrine and Practice," *Journal of Strategic Security*, Vol. 2, No. 4, November/December 2009, pp. 75-77.

有形的、實際發生的事件為中心（tangible, real world），而資訊作戰應專注於爭取認知域中的優勢。[21]此觀點與《國軍政治作戰要綱》中所述政治作戰「以人為中心」之特性一致，[22]而透過此一觀點，也呼應了希歐海莉(Catherine A. Theohary)認為「資訊戰其實就是政治作戰的其中一種形式」之觀點。

另外值得一提的是，在其研究中提出認知域是資訊環境中最重要的場域，他們引用美軍資訊作戰準則內之敘述：「這個領域(認知域)構成了資訊環境中最重要的組成部分」，[23]筆者完全能夠同意這個觀點，如同孫子兵法有云：「謀定而後動」，而認知域恰恰就是提供了謀劃的功能，此領域的功能在於對於受眾（target audience）要有清楚的認識並瞭解，才能知道如何影響他們的情感、認知並擴展至其決策（行為）上，倘若未能善加謀畫，就算在實體域或者資訊域中有著強大的能力，也無法對其產生影響，更甚者，可能產生反效果。如同筆者在美國參加心戰軍官班訓練時常聽到教官的提醒：「做差勁的心戰還不如不做的好（no PSYOP is better than bad PSYOP）」，但相對的，認知域雖然有如人類大腦一般重要，但並不是否認其他場域中之軍事能力的重要性，畢竟有發達的大腦卻無健康完整的軀幹，大腦所想之事仍無法付諸實現。

美國陸軍上校波依德(Curtis D. Boyd)撰文評析美國陸軍資訊作戰之內涵時特別強調了心理作戰（PSYOP）與公共事務（PA）在資訊作戰中的重要性，此文章標題直指「Army IO is PSYOP（陸軍資訊作戰即是心理作戰）」，[24]他認為資訊作戰，無論在平時或戰時，即是進行一場人心的爭奪戰，能否成功主要取決於能否適應人文地貌（human terrain），[25]在這種人類情感交錯的競爭環境中，能否影響對手和當

---

[21] Christopher Paul et al., *Improving C2 and Situational Awareness for Operations in and Through the Information Environment* (Santa Monica, CA: Rand, 2018), pp. 30-39.

[22] 中華民國國防部，《國軍政治作戰要綱》，(臺北：國防部，2016 年)，頁 1-4。

[23] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. I-3.

[24] Curtis D. Boyd, "Army IO is PSYOP: Influencing More with Less," *Military Review*, Vol. 87, No. 3, May/June 2007, p. 74.

[25] 人文地貌(human terrain)是一個被廣泛運用於美國陸軍及海軍陸戰隊的詞彙，相對於地貌是針對地理環境的認識，人文地貌著重的部分在於對於作戰區域內除卻地理相關資訊後，針對社會、種

地居民的心理取決於資訊內容和資訊傳遞者的可信度，是故，波依德認為資訊作戰應在良好的戰略溝通（strategic communication）框架之下，由心理作戰之「影響」能力與公共事務之「告知」能力來領導，才能確實的完成資訊作戰的任務與目標。然而，筆者認為，他的觀點局限於戰術或作戰階層之資訊作戰，但值得一提的原因仍在於，藉由此文獻可呈現出心理作戰於資訊作戰架構中扮演的核心角色。

回顧國內對於資訊作戰之研究，在博碩士論文方面，研究著實為數不多，且尚未有針對我國資訊作戰與心理作戰整合之相關議題所進行之研究，製表整理論文概要如表1-1。

族、經濟與政治等元素。詳見：Jacob Kipp, Lester Grau, Karl Prinslow, Don Smith, “The Human Terrain System: A CORDS for the 21st Century,” *Military Review*, Vol. 86, No. 5, September/October 2006, p. 9.

表1-1 我國以資訊作戰為主題之博碩士論文概要整理表

作　　者	論　　文　　題　　目	內　　容　　概　　要	出 版 年
洪霽廷	俄羅斯資訊作戰之研究，2000-2016	俄羅斯資訊作戰手段之研究，與本文所欲探討之美國、中共及我國資訊作戰內容低度相關。	2019
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	探討主體與本文雷同，然而該論文雖以資訊作戰為題，探討內容主要係針對網路作戰層面之探討進行論述，缺乏資訊作戰能力整合之論述。	2018
吳來益	資訊作戰對我國武獲政策的影響	綜合以探討美國及中共資訊作戰相關發展，並兼論對我國武獲有何影響，然而，卻在探討美軍資訊作戰時出現誤用中共「空天一體」概念於美軍資訊作戰上之重大謬誤，且探討內容限於電子戰及網路作戰。	2015
邵楷崴	運用孫子兵法於雲端資訊作戰策略之研究	運用孫子兵法之謀略觀進行整體之資安攻防探討。	2014
方士源	以正規化概念分析建構資訊作戰知識本體之研究	以2006之美軍資訊作戰準則為基礎，定義資訊作戰，並據以建立模組對於中共資訊作戰進行探討。	2011
黃明楷	從中共資訊作戰的觀點論我國之資訊安全	主要針對中共網路作戰與我國資安應對作為進行探討，其參考文獻多為2000年之前之著作及研究。	2007
唐汝達	資訊作戰之法政層面探討	整體以國內學者之觀點探討美軍資訊作戰之定義，但缺乏美軍準則之探討。研究重點在於透過波灣戰爭、科索沃戰爭以及阿富汗戰爭中之美軍資訊作戰所可能衍生之法律問題。	2006
林恩杰	資訊作戰理論與應用之研究	整體針對資訊作戰於後勤、情報以及作戰行動之實戰應用進行研究探討。	2001

資料來源：作者自行整理於臺灣博碩士論文知識加值系統中以「資訊作戰」單詞針對論文名稱進行精準查詢所獲取之結果。<https://ndltd.ncl.edu.tw/cgi-bin/gs32/gsweb.cgi/ccd=RRehHY/search#result>

而在學術期刊論文之研討方面，葉志偉在其研究中，探討了美軍聯合作戰資訊作戰準則JP3-13之演進，詳盡地將1998年至2012年間不同之準則版本進行比對，在「資訊相關能力」一詞上，他認為在詞彙運用上，從2006年區分「核心能力（core capabilities）」和「支援與相關能力（supporting and related capabilities）」，到2012年版融合為「資訊相關能力（information related capabilities）」，用資訊相關能力這種界線模糊之詞句，更能反映在資訊作戰中軍、民、政府部門都在某種程度上涉入其中的本質，他也指出美軍在資訊作戰準則的演進期間，逐漸優化其作業流程並發展作業框架。[26]另外，2012年版的準則運用更大的篇幅來說明，如何在資訊作戰過程中，在各資訊相關能力間進行協調，使其能保持資訊的一致性，發揮最大的效果。最後，葉志偉也提出與筆者一致之見解，認為資訊作戰常被誤認為「資訊化作戰」，亦即美軍之網路作戰（Cyberspace Operations），他認為資訊作戰乃是從作戰發起前、中、後對於資訊相關能力之整體協調運用，而且也指出《國軍資訊戰要綱》久未實施修訂之情況以及未重視資訊作戰人員之培養等缺失，[27]也在其論述中強調了「影響」的重要性，深具參考價值；然而筆者仍要指出，指揮官之決策固然是資訊作戰意圖影響之重點，但受眾的選定上應更廣泛的包含政府或非政府組織、團體乃至個人、政治領袖、軍隊指揮官、乃至市井小民，都應被考量在資訊作戰的受眾選定及影響範圍內。

而吳奇英則是將資訊作戰與心理作戰兩個概念相結合，來解釋我國之「資訊心理戰」概念，他的指出一般人對於資訊一詞理解上的謬誤，網際網路是用來傳遞資訊之途徑，是故，網路作戰不能與資訊作戰畫上等號。[28]因為，資訊作戰或除了透過網路來傳遞訊息之外，還包括其他各式各樣之傳媒（例如社群媒體、廣播、電視、

---

[26] 葉志偉，〈美軍資訊作戰聯戰準則之演進〉，《海軍學術雙月刊》，第 51 卷第 2 期，2017 年 5 月，頁 123。

[27] 同前註，頁 114-126。

[28] 吳奇英，〈資訊時代政治作戰中心理戰的運用與發展—以美伊戰爭及兩岸資訊心理戰為例〉，《復興崗學報》，第 85 期，2005 年 12 月，頁 71-94。

報紙等）、人與人的交流、軍事威懾（如演習、兵力調動）等手法進行。但隨著智慧型手機與網路使用的日漸普及，網際網路理所當然的成為了資訊作戰的捷徑，也因此使得當代研究者誤將網路作戰與資訊作戰畫上等號。

呂爾浩及魏澤民的研究中，廣泛涉獵了美國諸多學者對於資訊作戰相關概念之探討，並以此為基礎，綜合檢視中共信息戰之發展，並以類型學之觀點，對中共信息戰做出「攻擊常規資訊作戰」、「攻擊非常規資訊作戰」、「防禦常規資訊作戰」、「防禦非常規資訊作戰」等四種分類。然而，未能針對中共資訊作戰相關能力及限制進行深入研究，實為可惜。[29]

我國前國防部副部長林中斌在其2005年出版之「以智取勝」一書中，即提到中共「信息戰」之發展，並且對於中共資訊戰與其心理戰之關聯性加以闡述，[30]另外，書中亦且引用美方觀點，指出「北京雖然希望能避免戰爭.....信息戰將成為其戰爭手段中不可或缺的部分」，[31]其以敵為師之篇目中，亦提出我國應正視解放軍信息戰發展之趨勢，並發展相對能力以為因應之看法，[32]其觀點與本研究相關，本研究擬延伸其洞見，聚焦於資訊作戰能力的整合面向。

綜合以上各種觀點，我們可以瞭解到，資訊作戰的目標，並非僅僅運用單一的軍事或非軍事手段，如駭客攻擊或心理作戰所能達成，必須透過各種資訊相關能力共同參與謀畫及執行，方能發揮最大功效，這也是為何美軍2012年後的版本，要運用極大篇幅來強調各資訊相關能力間的調和運作，以求使各資訊相關能力在對目標受眾傳遞訊息時不相牴觸，以達成效果之最大化，完美扮演其戰力倍化器（force multiplier）之角色。[33]所以，國軍在積極發展國防武力的同時，是否也應投入資源發展資訊作戰機制及相關能力，不失為一廉價而有效之國防投資方向。

---

[29] 呂爾浩、魏澤民，〈中國“資訊作戰”的類型分析〉，《遠景基金會季刊》，第 7 卷第 3 期，2006 年 7 月，頁 190-208。

[30] 林中斌，《以智取勝》(臺北:全球防衛雜誌，2005 年)，頁 253。

[31] 同前註，頁 264。

[32] 同前註，頁 122。

[33] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. I-1.

貳、心理作戰（美軍軍事資訊支援作戰）

回顧美軍心理作戰之發展簡史，美軍心理作戰早於第一次世界大戰期間，就曾讓德國的戰場元帥興登堡(Paul von Hindenburg)相當頭疼，他曾說：「敵人不只在我們的前線投下如雨般的砲火，也投下大量精美印刷紙張；其空軍投下的不只是殺傷身體的炸彈，同時也投下企圖摧毀靈魂的傳單」，[34]德軍統帥的一席話，成為美國成功遂行心理作戰的鐵證。至波斯灣戰爭時，美軍以資訊作戰為首，整合心理作戰、電子作戰(Electronic Warfare, EW)、軍事欺敵、作戰安全等軍事能力之計畫作為，避免在資訊傳播層面上的不協調。[35]

在911事件後，美國開始在中東地區進行反恐戰爭，由於敵人不同於以往的正規部隊，相較於一、二次世界大戰時著重於敵方正規軍意志的摧毀的心理作戰與海灣戰爭期間著重於打亂敵人指管系統的資訊作戰，在反恐戰爭中的資訊作戰更著重於對作戰地區內的民眾做出影響，進而美軍藉由阿富汗地區10年來的資訊作戰及心理作戰經驗，進行美軍心理作戰部隊之軍事轉型，在2010年1月7日先將心理作戰準則由原本獨立之編目JP3-53變更為JP3-13.2，原本之準則編碼JP3-53在參謀總長聯席會議(Joint Chiefs of Staff)的編目中被移除，[36]納入資訊作戰JP3-13之子目，更在2011年的12月20日將該準則名稱變更為軍事資訊支援作戰，並將其定義為「透過計畫做為向外國政府、組織、個人進行政治、經濟、軍事及意識型態之活動，以創造對美國政府及其軍事目標有利之情感、態度、理解、信仰與行為」。[37]順帶一提，一封從五角大廈流出的內部電子郵件中指出，本次的名稱變更是為了讓心理作

---

[34] Joint Chiefs of Staff, " *Joint Publication 3-53: Psychological Operations*," September 5, 2003, p.VII-1.

[35] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(1998), op.cit., p. I-20.

[36] Joint Chiefs of Staff, "*Joint Publications Operations Series*" Joint Publications Operations Series, < https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/>.(Accessed：17/1/2019)

[37] Joint Chiefs of Staff, "*Joint Publication 3-13.2: Military Information Support Operations*,"December 20, 2011, p. vii.

戰的名稱聽起來不那麼邪惡，[38]但在2011版的軍事資訊支援作戰（Military Information Support Operations）準則中則敘明轉型之原因在於：「根據國防部長的備忘錄，將此刊物中的心理作戰乙詞適當更換為軍事資訊支援作戰，能更精確的傳達在平、戰時計畫性作為之本質」，[39]雖然美軍在2017年10月，為提振其心戰部隊成員的士氣，又將其部隊名稱改回心理作戰，任務名稱及準則方面則維持軍事資訊支援作戰之名稱，[40]仍列屬資訊作戰中14項資訊相關能力之一，而且居於領銜地位，在希歐海莉的研究即指出「心理作戰乃是資訊作戰的核心」[41]。另外，其準則中也指出：「當我們將飛機、船艦、部隊和軍事裝備用於或作為軍事資訊支援作戰行動來創造認知層面的效應時，會對受眾產生特定的心理效果。」[42]，是故美軍軍事資訊支援作戰，旨在從認知域影響受眾，從而造成心理效果（psychological effect），與資訊作戰之核心概念十分類似，可見軍事資訊支援作戰（心理作戰）在美軍資訊作戰機制內之重要性。

另外，洪陸訓與莫大華主編《廿一世紀歐美主要國家心戰部隊的發展》亦探討了美軍的轉型，有助於本研究了解2011年之前美軍心戰部隊轉型時的初期發展概況，該文發現美軍「能力整合、總體思維」之觀點，與本文欲探討之美軍資訊作戰與軍事資訊支援作戰之整合若合符節。[43]

回顧國軍對於心理作戰的定義，必須先探討政治作戰六戰中的心理戰。[44]《國

---

38 Marc Ambinder, “Original Document: Making PSYOPS Less Sinister”, *The Atlantic*, January 30, 2010. <https://www.theatlantic.com/politics/archive/2010/06/original-document-making-psyops-less-sinister/58947/>.(Accessed：17/1/2019)

39 Joint Chiefs of Staff, *Joint Publication 3-13.2: Military Information Support Operations*, op. cit.,p. iii.

40 Meghann Myers, “The Army's psychological operations community is getting its name back”, *Army Times*, November 6, 2017. <https://www.armytimes.com/news/your-army/2017/11/06/the-armys-psychological-operations-community-is-getting-its-name-back/>.(Accessed：17/1/2019)

41 Catherine A. Theohary, *Defense Primer: Information Operations*, op. cit.,p. 1.

42 Joint Chiefs of Staff, *Joint Publication 3-13.2:Military Information Support Operations*, op. cit., p. A-1.

43 曾維國，〈廿一世紀美國心戰部隊的發展研究〉，輯於洪陸訓、莫大華主編，《廿一世紀歐美主要國家心戰部隊的發展》（臺北：國防大學政治作戰學院，2011 年），頁 36-40。

44 依照《國軍政治作戰要綱》，我國政治作戰之六戰可區分為思想戰、組織戰、情報戰、謀略戰、心理戰以及群眾戰。

軍政治作戰要綱》中載明心理戰之目標為：「心理戰是攻心作為，以目標對象的心理為戰場，以情報為依據，以傳播為手段，從精神上去主導、轉化或鞏固目標對象的心理與行為，使有利於我之作戰」[45]。而心理作戰之目標則更加明確，其目標為：「依據國家安全政策與軍事戰略指導，運用心理作戰、戰略溝通手段，影響敵對國家及國際社會等目標地區軍民心理，改變其認知與態度，導引其行為，進而有利於國家政策與軍事任務之達成」，[46]除了準則的定義之外，吳奇英以「資訊心理戰」之概念來進行探討，他認為資訊心理戰是「資訊戰與心理戰之相互配合運用的作戰型態，是利用『資訊』進行宣傳，以求鞏固我國軍民之心理防線，並爭取群眾支持，在此同時亦可打擊敵對一方軍民士氣。」，[47] 他也試圖將「資訊」之概念予以澄清，認為：「資訊是通過文字、數據和各種信號來傳遞、處理和表現客觀事物特性的知識流……是人類感受到的客觀存在和差異。」，[48]在其敘述中，人類的「感受」得到了強調，而感受即是屬於認知域之層次。此研究雖然早在10數年前發表，卻能早於美國研究者之前，指出人類因素在資訊作戰中扮演的重要角色，從而將資訊作戰與心理作戰兩個概念相結合，可惜未有後續研究進行深入探討。

在方鵬程的研究中，完整呈現美軍在波斯灣戰爭期間，心理作戰產品如何透過傳統媒體或網際網路等途徑進行傳散，方式包括廣播、電視節目、海報、傳單、電子郵件等管道，將美軍心戰計畫者所謀畫之心理作戰訊息，傳遞給伊拉克官員、軍隊指揮官、基層士兵與市井小民等各階層，進而協助其他路線的作戰順利進行。[49] 波斯灣戰爭距今已有 20 餘年之遙，然而卻是美國向世界展示，非武力作戰（nonkinetic operations）結合武力作戰（kinetic operations）之創新思維之舞台，也廣泛被認為是當代資訊作戰的初登板。

---

[45] 同註 27，頁 3-10。

[46] 同註 27，頁 4-9。

[47] 同註 33，頁 83。

[48] 同註 33，頁 79。

[49] 方鵬程，〈美軍戰略性傳播的媒體運用分析：以 2003 年波斯灣戰爭為例〉，《復興崗學報》，第 97 期，2010 年 3 月，頁 23-45。

美國前國防部長馬蒂斯（James Mattis）在擔任北約的盟軍最高指揮官時，曾在公開演說中指出:「掌握看法是當代衝突的嶄新制高點(capturing perceptions is the new “high ground” in today’s conflicts)」[50]，所謂掌握看法即是攻心，要如何攻心，要透過用何種途徑、手段攻心，是心理作戰計畫者需要思考的，而將計畫付諸實現，則是網路、電子、媒體等相關單位要努力的範圍，能否如馬蒂斯所言，能否成功搶佔「看法（perception）」這個制高點，端看我國能否統合運用各項軍事、政府甚至民間資訊相關能力，來發揮最大的心理作戰效能。

綜合以上觀點，國防部所規劃之資訊作戰核心為美軍之軍事資訊支援作戰，而美軍之軍事資訊支援作戰之前身，即是心理作戰(Psychological Operations, PSYOP)。

參、中共解放軍戰略支援部隊

中共建政以來，「積極防禦（active defense）」一直為其戰略構想之核心，而其積極防禦戰略構想的內涵，亦從1993年江澤民的「打贏高技術條件下局部戰爭」、到2004年胡錦濤的「打贏信息化條件下的局部戰爭」，[51]至今演變為2015年習近平的「打贏信息化局部戰爭」戰略構想。也因此，中共人民解放軍的戰略支援部隊在2015年12月31日成立之初，即被多數研究者將其視為中國的資訊戰（information warfare）部隊，同時也被視為中共「積極防禦（active defense）」戰略構想的核心單位，[52]並處於習近平推動強軍軍事轉型政策的其中一個重要環節，習近平在2017年19大中宣示，要在2020年實現「機械化，信息化建設之重大進展」， 2035年實現「國防和軍隊現代化」，並配合其「軍民融合」政策，使強國、強軍雙軌並進，最終在

[50] James Mattis, “*Launching NATO’s New Strategic Concept*,” speeches & transcripts, July 7, 2009, NATO.< https://www.nato.int/cps/en/natolive/opinions_56392.htm>(Accessed:20/1/2019)

[51] 同註 12，頁 30。

[52] John Costello, “The Strategic Support Force: China’s Information Warfare Service,” *China Brief*, Vol. 16, No. 3, February 8, 2016, pp. 15-19.

本世紀中葉，將解放軍打造為「世界一流軍隊」。[53]

戰略支援部隊雖名為部隊，但其規模卻相當於一個獨立軍種等級，統整了與資訊領域相關的能力，包括空間和網路作戰、電子戰、心理戰能力。[54]在林穎佑的研究指出，戰略支援部隊之成立宗旨，在為解放軍提供可靠的資訊能力和戰略支援之保障，為陸海空和火箭軍撐起一把「資訊傘」並與各軍種之行動融為一體，成為戰爭制勝的關鍵力量。[55]換言之，戰略支援部隊將過去分立的航天、情報、電戰、指管戰、網路作戰、通信系統以及心理作戰等軍事能力，透過讓其直屬中央軍委會及提高位階並整合於單一框架中，使資訊作戰地位不致在傳統軍事領導幹部之軍種或兵科本位主義遭到忽視。

在解放軍戰略支援部隊成立之事件中，許多人將目光焦點放在其對於「網」、「電」、「天」能力之組建與統合，然而筆者認為，吾人觀察之重點應在於，原本負責對臺「三戰」工作的「三一一基地」以及負責心理戰等工作的總政治局轄下單位被移入戰略支援部隊內，也因此強化了其心理戰傳播能力，[56]對此，王清安即在其研究中指出，中共在對於網路空間之界定上，包含了藉由網路、媒體所發動、針對個人意識型態進行影響的宣傳戰及心理戰，而中共將原總政治部編制之聯絡部（原名為對敵工作部）情蒐人員納入戰略支援部隊之「網路空間作戰部隊」中，[57]可見其藉由統合心理作戰與網路作戰機構，來強化心理戰傳播能力之意圖。

另外，美國學者倪凌超(Adam Ni)以及季北慈(Bates Gill)的研究中，指出戰略支援部隊的網路系統部之下，整合了信號情報（signals intelligence）、網路間諜（cyber

---

53 同註 12，頁 30。

54 同註 12。

55 林穎佑，〈中共戰略支援部隊的任務與規模〉，《展望與探索》，第 15 卷第 10 期，2016 年 10 月，頁 104。

56 John Costello, Joe McReynolds, “China’s Strategic Support Force: A Force for a New Era,” in Phillip C. Saunders et al., eds., *Chairman Xi Remakes the PLA*(Washington, D.C.: National Defense University Press, 2018), p. 452.

57 王清安，〈中共解放軍「戰略支援部隊」之發展對我陸軍威脅評估－以網路作戰部隊為例〉，《陸軍通資半年刊》，第 131 期，2017 年 4 月，頁 8。

espionage）、電腦攻擊（computer attack）、電磁頻譜戰（electromagnetic warfare）以及心理作戰（psychological operations）等各式各樣的軍事能力[58]。其研究中對於筆者最大之貢獻在於提供完整的組織架構分析，有助於瞭解戰略支援部隊之全般組織架構與指揮關係，進而推測戰略支援部隊之能力與限制，從而能與我國之相關能力進行對照。

柯斯特羅(John Costello)與麥瑞諾德(Joe McReynolds)則認為，解放軍戰略支援部隊的建立，除了在組織上整合了太空、網路、電子以及心理戰等等不同的作戰能力及原屬總參謀部之單位以外，戰略支援部隊的創設也在不同的軍事能力間構築了一種創新的調和方式，並增進了在未來戰爭中扮演決勝因素的「戰略性資訊作戰（strategic information operations）」的效率[59]。此篇專書論文被收錄於美國國防大學出版的「Chairman Xi Remakes the PLA」一書中，足可顯示戰略支援部隊的重要性，不亞於火箭軍的創設以及各種解放軍中推動的變革，我們若以「達成戰區或國家目標」來定義「戰略」一詞，那麼戰略支援部隊的設立，就可視為是達成中共「中華民族偉大復興」國家方針的一顆重要棋子，因此筆者相信，中共未來將持續透過戰略支援部隊的能力，加強對臺「法律戰」、「心理戰」以及「輿論戰」之力道，吾人應及早設法因應，方能維持我中華民國之長治久安。

綜合以上文獻所得，「資訊作戰」一詞的概念與運作已轉型為相關能力的整合運用，另結合前參謀總長李上將的說法，可彙整為美「中」臺三方對資訊作戰相關能力組合比較表（如表1-2）。

[58] Adam Ni, Bates Gill, “The People’s Liberation Army Strategic Support Force: Update 2019,” *China Brief*, Vol. 19, No. 10, May 29, 2019, p. 16.

[59] John Costello, op. cit., p. 479.

表 1-2 美「中」臺「資訊作戰相關能力組合」比較表

	認知域	資訊域	實體域
美軍	● 戰略溝通 ● 軍事資訊支援作戰 ● 軍事欺敵	● 網路作戰 ● 資訊確保	● 跨部會協調組 ● 公共事務 ● 軍民作戰 ● 太空作戰 ● 情報 ● 作戰安全 ● 特殊技術作戰 ● 關鍵領導者交涉 ● 聯合電磁頻譜作戰
解放軍戰略支援部隊	● 三一一基地（對臺心理戰、法律戰、輿論戰）	● 61398 部隊 ● 61419 部隊 ● 61786 部隊	● 航天系統部(太空、核試) ● 原屬總參謀部電子作戰雷達部及其所屬電子戰單位
國軍	● 心理作戰大隊	● 資通電軍網路戰大隊	● 資通電軍電子作戰中心 ● 資通電軍指管防護大隊 ● 電訊發展室
備註	61398、61419、61786 部隊為中共網軍部隊，原屬總參謀部技術偵查部。		

資料來源：筆者自製(參考：美軍資訊作戰準則 JP3-13；國防部人才招募中心網頁；The People’ s Liberation Army Strategic Support Force: Update 2019)。

第三節、研究方法與結構

壹、研究途徑與研究方法

在研究途徑方面，本研究試圖透過歷史制度主義的理論視角，探索美軍與中共解放軍的資訊作戰制度發展，並以渠等制度現況為重點，檢視各自制度演進之不同路徑以及現況發展結果（尤其是共同或雷同的部分），據以發掘相似、共同或可能較佳的制度走向，做為國軍資訊作戰制度建構、調整或轉型的參考。歷史制度主義之基本概念為「路徑依賴」，意即當政府之政策、制度形成時，除非遭受相當大之阻力或趨勢改變，否則不會變更其所選定之路徑，[60]所以歷史制度主義研究途徑著重於捕捉制度發展之歷史脈絡與時間序列，並依循此脈絡找出路徑依賴與制度改變之關鍵時刻，藉以對現行制度產生之因果做出詮釋。[61]繼之，再以SWOT的競爭策略分析架構，試圖探討國軍在解放軍當前信息戰威脅下的資訊作戰制度發展策略選擇。透過歷史制度主義之研究途徑與SWOT競爭策略分析架構之運用，期能呈現資訊作戰能力整合在美「中」臺三方各自的發展態勢，釐清相關概念之異同並探討對我資訊作戰與心理作戰制度發展與能力整合之重要性、必要性或可行性的相關意涵。

在研究方法方面，本研究以文獻分析法進行研究，文獻研究法係指利用既存的官方文件或史料，輔以系統性及客觀的檢證，如此認證既存事實之真偽，並藉以驗證對該事實之觀點、看法是否合宜[62]。本文主要將以官方出版之文件或書籍為研究骨幹，輔以學者專家觀點，藉以捕捉美國、中共以及我國資訊作戰相關能力及制度發展之歷史脈絡及現有能力，以求做出最合理之分析與解釋。

---

[60] Guy Peters 著，王向民、段紅偉譯，《政治科學中的制度理論:"新制度主義》(Institutional Theory In Political Science: "The New Institutionalism") (上海：上海人民出版社，2011 年)，頁 69。

[61] 蔡相廷，〈歷史制度主義的興起與研究取向－政治學研究途徑的探討〉，《臺北市立教育大學學報》，第 41 卷第 2 期，2010 年 11 月，頁 59-60。

[62] 瞿海源等著，《社會及行為科學研究方法：質性研究法》(臺北：東華書局，2015 年)，頁 51。

貳、研究架構

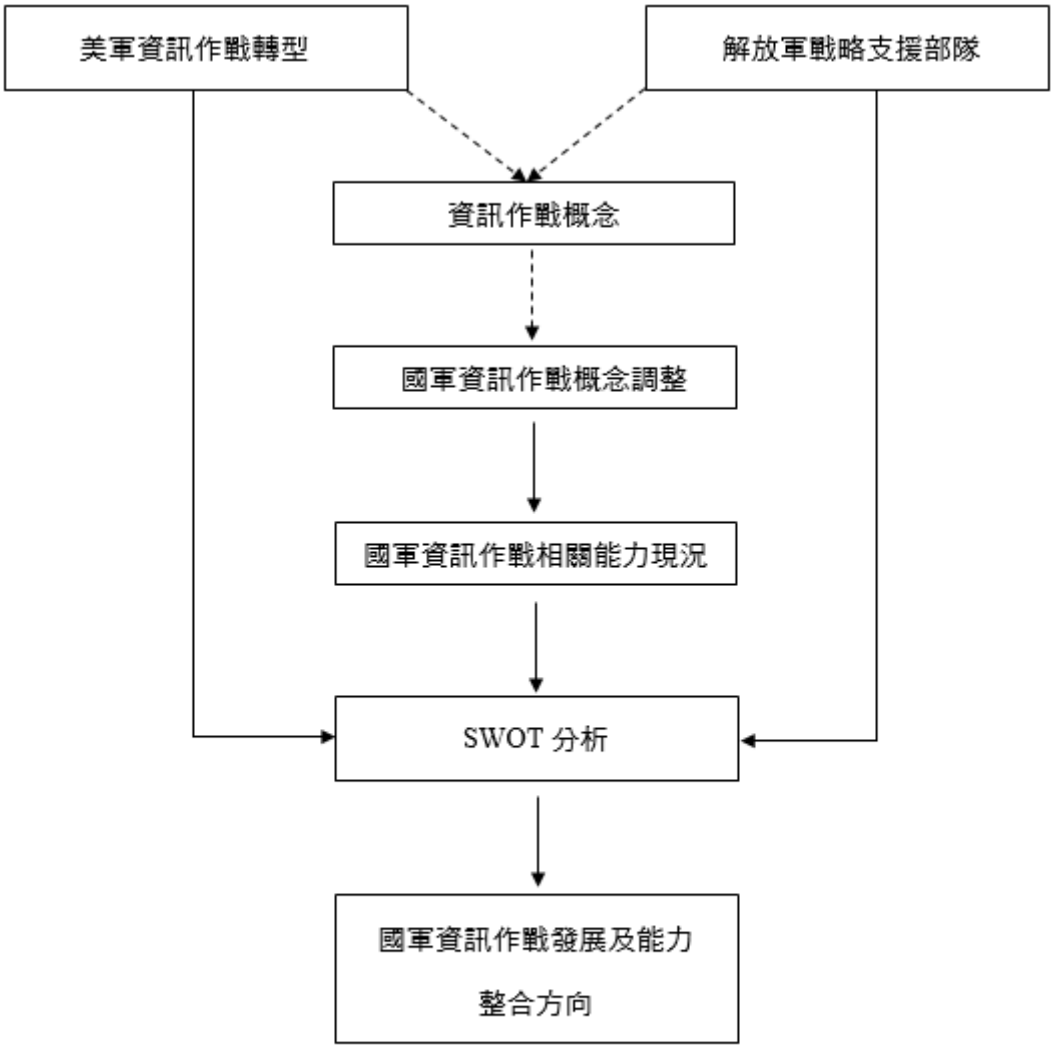

圖1-1 研究架構圖

資料來源：作者自製

第四節、研究範圍與研究限制

壹、研究範圍

一、 美軍資訊作戰概念係指各種資訊相關能力之整合與運用，然國內相關研究均將其誤認為「電腦網路能力」之軍事運用，是故，為釐清資訊作戰之全般概念，本研究將聚焦於心理作戰（美軍為軍事資訊支援作戰）與資訊作戰之關聯性探討，以提供後續研究者不同之思維途徑。

二、 從中共解放軍之信息戰與三戰之關聯性來擴大探討，中共解放軍戰略支援部隊集結了太空作戰、電子戰、網路作戰、三戰等不同資訊相關能力之意涵及對我國可能之威脅。

三、 從美軍資訊作戰之角度，探討我國整體現行制度，包含負責資電作戰之「資通電軍」與負責心理作戰之「心理作戰大隊」之優點及不足之處，並研提改進方案。

貳、研究限制

一、 資訊作戰範圍既深且廣，本研究僅針對我國現行資電作戰與心理作戰制度之優劣進行分析與研討並提出改進策略，其他如通信、電子戰乃至C4ISR系統方面之發展則以及細部執行層面之議題不多加探討。

二、 中共因政府體制較不公開透明，許多軍事準則或典籍未能取得或並費最新版本，不足之部分將引用美國官方或民間智庫機構之研究成果佐證之。

第二章、美軍資訊作戰能力組成與運作機制

美軍聯合作戰準則 JP1 中，原訂有 6 項聯合作戰功能(joint functions)，依序為指揮與管制(command and control, C2)、情報(intelligence)、火力(fire)、運動與機動(movement and maneuver)、防護(protection)、持續力(sustainment)，而在 2017 年進行準則修訂時，正式將資訊(information)新增為第 7 項聯合作戰功能，在對資訊這項聯合作戰能力的說明中將其定義為「涵蓋了資訊的處理與運用，並與其他聯合作戰能力相互整合，用以影響相關行為者的觀感、行為、行動或不行動、人類或自動化產生的決策」，[63]這項準則上的重大變更，凸顯了美國對於資訊作戰的重視程度。

而我國在李前總長的大力推動下，首次在演習中成立「資訊作戰中心」，將國軍情報、網路、電子、謀略、欺敵、輿論、心理、保防、特種作戰及戰略溝通等 10 項能力進行整合，即是試圖依循美軍的制度來發展我國國軍資訊作戰之能力，然而其談話內容中「將所望訊息傳遞給敵方軍民，來影響他們的心理」之「目標」，[64]則與美軍軍事資訊支援作戰(MISO)，也就是心理作戰之定義中「向外國受眾傳達經篩選的資訊與指標…」之敘述不謀而合。讀者在此可能產生疑惑，李前總長是否已將美軍資訊作戰與軍事資訊支援作戰的概念混淆?答案是否定的，因為心理作戰從 1998 年版的美軍聯合作戰資訊作戰準則出版以來，就一直在資訊作戰之中扮演「核心能力」的角色。[65]而引述美國國會研究處研究員希歐海莉(Catherine Theohary)的說法「心理作戰是資訊作戰的核心」。[66]

美軍心理作戰於 2011 年(psychological operations, PSYOP)轉型成為軍事資訊支援作戰(military information support operations, MISO)，並由原準則編目 JP3-53 移

---

[63] Joint Chiefs of Staff, "*Joint Publication 1:Doctrine for the Armed Forces of the United States*," July 12, 2017, I-19.

[64] 同註 4。

[65] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(1998), op.cit., p. IV-3.

[66] Catherine A. Theohary, "*Information Warfare: issue for congress*," March 5, 2018, p. 2.

至JP3-13.2，正式成為美軍資訊作戰架構中14項「資訊相關能力」(information related capabilities)之一，[67]在這 14 項能力的調和運作下，美軍得以創造並爭取「資訊環境」(information environment)中的優勢。然而，和一般人所認識的「資訊作戰」不同，美軍聯合作戰資訊作戰準則 JP3-13 中，運用大篇幅內容強調認知層面影響以及資訊環境的操作等內容，而美軍亦有研究者提出「資訊作戰即是心理作戰」的觀點，[68]因此，本章節將從美軍資訊作戰中各項資訊相關能力的介紹出發，介紹美軍軍事資訊支援作戰於資訊作戰架構下所扮演之角色，並針對我國鮮少有人探討的「資訊環境」之概念進行探討，俾能對於美軍資訊作戰之內涵能有更深入的認識。

第一節、美軍資訊相關能力之簡介

根據美軍2014年版的資訊作戰準則所更動之內容，美軍當前的資訊作戰在於如何對於當前的「資訊相關能力(information related capabilities, IRC)」進行評估，並將資訊相關能力加以整合運用(如圖2-1)，圖中左側9項為聯合作戰資訊作戰準則內訂定之資訊相關能力(IRC)，右側為其他未列入資訊相關能力之各部門代表，美軍聯戰部隊資訊作戰小組進行會議時，即是透過這種各能力整合之方式，支持聯合作戰部隊指揮官乃至國家目標。[69]以下即介紹美軍各項資訊相關能力之內涵，未顯示於圖中的戰略溝通(SC)、資訊確保(IA)、太空作戰(SO)、聯合電磁頻譜作戰(JEMSO) 、關鍵領導人交涉(KLE)等5項能力也將一併說明原因。

---

[67] Joint Chiefs of Staff, *Joint Publication 3-13.2: Military Information Support Operations*, op.cit., p. iii.

[68] Curtis D. Boyd, Army IO is PSYOP: Influencing More with Less, op.cit., p. 74.

[69] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. iii.

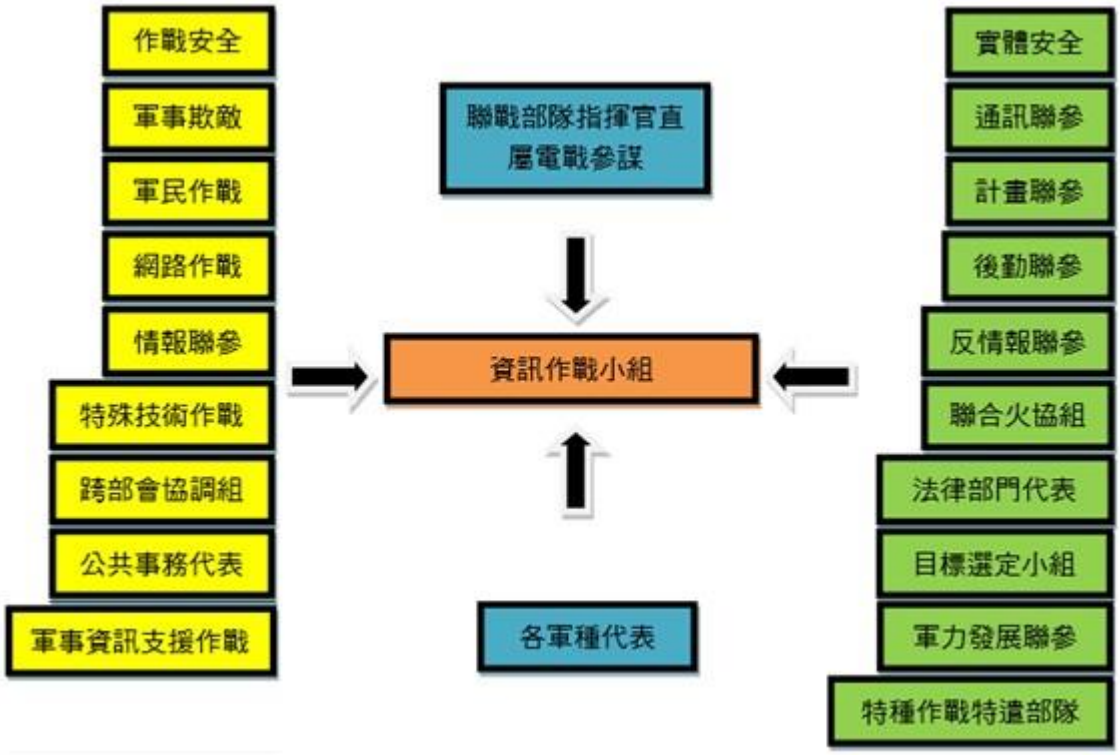

圖2-1 美軍聯合作戰資訊作戰小組成員示意圖

資料來源: Joint Chiefs of Staff, *Joint Publication 3-13:Information Operations*, November 20, 2014, p. II-6

壹、美軍資訊相關能力簡介

資訊相關能力(IRC)是影響資訊環境中任何一個場域的工具、技術或是活動，他們能影響受眾在決策進行之前、後的資訊蒐集、處理及傳遞，而藉此影響其決策，並支持美國政府或聯戰部隊指揮官目標之達成，[70]美軍聯戰準則內列述之資訊相關能力，以下將依序介紹之。

一、 戰略溝通(Strategic Communication, SC)

依據美國參謀總長聯席會議於2009年出版的「戰略溝通聯合整合構想」（Strategic Communication Joint Integrating Concept）中所述，戰略溝通是一項「持恆運作的功能」，範圍涵括所有軍事行動，聯戰部隊會與盟

[70] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. I-3.

友、敵人或其他對象間有策略的持續進行溝通。聯戰部隊之戰略溝通具有「增進美國的可信度與正當性」、「削弱對手的可信度與正當性」、「使選定之受眾採取特定行為以支持美國或國際目標」、「使競爭對手採取特定行動」等四個基本的戰略溝通目標，而戰略溝通的步驟包含了美國政府如何透過協調一致的計畫作為，來接觸關鍵受眾並相互理解，而這些作為是以國家整體力量來進行的，其中會牽涉到跨部會協商的過程與整合，以期符合國家整體戰略。[71]而戰略溝通未出現於資訊作戰小組示意圖係因在聯合作戰資訊作戰準則之敘述中，將戰略溝通說明為一溝通傳遞美國政府之戰略指導(strategic guidance)至政府內、外部各組織、機構之流程(process)，而跨部會協調組會在資訊作戰小組中代表美國政府實施戰略溝通流程，以使訊息同步化。

二、 跨部會協調組(Joint Interagency Coordination Group, JIACG)

跨部會協調組是在軍、文部門(計畫人員)間經常性建立協同關係之參謀組織，而跨部會協調不只運用於公部門之間，除了國防部與其他政府部門間的協調聯繫之外，美軍與私人單位、非政府組織也同樣會為了國家目標的達成而進行相互的協調，為了達成上述國家目標，通常需要多方面運用外交、軍事、經濟等各種各樣的手段方能順遂。[72]同樣的，資訊作戰的計畫過程乃至進行中，也需要透過跨部會協調組來與其他公、私部門保持密切聯繫，以求訊息之一致性。

三、 公共事務(Public Affairs, PA)

美軍公共事務聯合作戰準則JP3-61裡面引用了美國前總統歐巴馬(Barack Obama)的一席話，內容說道：「當我們無法清楚並公開的解釋我們所做出的努力時，我們將面臨的是恐怖分子的宣傳(proapganda)與

---

[71] Joint Chiefs of Staff, "*Strategic Communication Joint Integrating Concept*," October 7, 2009, p. iii.

[72] Joint Chiefs of Staff, "*Interorganizational Cooperation*," October 18, 2017, p. GL-8.

國際間的猜疑，我們降低了在夥伴與人民前的正當性，同時也降低了美國政府的可信賴度」，[73]從歐巴馬的發言中，我們可以發現公共事務的重要職能，即在於作為部隊之喉舌。另外，在該準則中亦將公共事務軍官定位為指揮官的發言人，公共事務軍官必須要具備足夠的知識、技能、資源及權限來提供即時、真實且精確的資訊。而在資訊作戰中，公共事務必須與資訊作戰的各種活動間做出充分的協調，以避免衝突(deconflict)。[74]

四、 軍民作戰(Civil-Military Operations, CMO)

依據美軍聯合作戰準則JP3-57所描述，軍民作戰的功能在於軍隊如何藉由直接支持當地重建秩序的軍事行動來建立、維持、影響或破壞與當地居民或組織(indigenous popupations and institutions)的關係，而這些行動的終極目的在於建立、恢復或維持穩定的作戰環境(operational enviroment)。[75]而在資訊作戰準則中，則進一步說明軍民作戰因為在作戰地區有良好的經營，所以可以提供資訊作戰良好的資訊傳遞管道，並且協助資訊作戰計畫者辨識當地的目標受眾(target audience)。[76]

五、 網路作戰(Cyberspace Operations, CO)

網路作戰前身為電腦網路作戰(Computer Network Operations, CNO)，在美軍聯合作戰準則JP3-12定義中，網路作戰即包含了美國國防部在軍事層級、國家層級或事務層級進行的網路行為，[77]而資訊作戰準則中則指出，網路作戰包含了資訊科技基礎設施與其中包含之資料、網路與通訊網絡、電腦系統與其中的控制器及處理器。當網路作戰協助資訊作戰時，

---

[73] Joint Chiefs of Staff, "*Joint Publication 3-61: Public Affairs*," August 19, 2016, p. I-1.

[74] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. II-7.

[75] Joint Chiefs of Staff, "*Joint Publication 3-57: Civil-Military Operations*," July 9, 2018, p. viii.

[76] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. II-7.

[77] Joint Chiefs of Staff, "*Joint Publication 3-12: Cyberspace Operations*," June 8, 2018, p. II-7.

即是運用其網路通訊能力來針對實體域(例如:無線網點)、資訊域(例如:加密的信文)與認知域(例如:在網路上影響受眾的認知)三個領域進行活動，來影響敵人或潛在敵人的決策。[78]

六、 資訊確保(Information Assurance, IA)

此項能力並無聯合作戰準則，但在2015年6月9日頒布的參謀總長聯席會議針對資訊確保的指示事項中，可以發現內容諸如網路安全督察計畫(Cyber Security Inspection Program)、資訊作戰狀況(Information Operation conditions)、個別事件處理計畫(Incident Handling Program)、網路停權(Network Suspensions)等等的內容，都是與資訊安全防護作為有關。[79]另外，在資訊作戰準則中提到，資訊確保對於爭取資訊優勢(Information Superiority)是必要的，聯合作戰部隊指揮官需要資訊安全能力來進行基礎設施防護以確保資訊的流通無阻，更甚者，才能進行影響敵對方的攻勢作為，[80]而在該文件中也指出，資訊確保主要由通訊聯參(J6)負責與其他單位間進行資訊確保任務之協調，故未特別要求資訊確保人員出席資訊作戰小組會議，僅由通訊聯參代表參加。

七、 太空作戰(Space Operations, SO)

美國於2019年12月20日成立了第六軍種，太空軍(USS Space Force)，顯示美國對於爭奪太空領域主導權的決心。在美軍聯合作戰準則JP3-14中指出，太空支持著資訊流通與決策進行，[81]在JP3-13中也指出，將太空能力整合進入聯合作戰中能夠成為顯著的增強戰力，太空作戰透過太空部隊對於情報、監視、偵查、飛彈預警、環境監控、衛星通訊以及以

---

[78] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. II-9.

[79] Joint Chiefs of Staff, "*Chiarman of the joint chiefs of staff instruction: Information Assurance (IA) and support to computer network defense (CND)*," Jun 9, 2015, p. ii.

[80] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. II-9.

[81] Joint Chiefs of Staff, "*Joint Publication 3-14: Space Operations*," April 10, 2018, p. II-9.

太空為基礎的定位、導航與計時等強化功能來支援資訊作戰，由此可見，掌握太空領域就等於掌握了資訊的流通性並使自己處於先制的地位，對於資訊作戰十分重要。[82]而太空作戰所掌握的情、監、偵、通訊等能力的支援與強化，在資訊作戰小組會議的各部門代表(如情報、指揮官直屬電子作戰參謀等)掌握，故未列於圖示中。

八、 軍事資訊支援作戰(Military Information Support Operations, MISO)

如前述軍事資訊支援作戰之前身為心理作戰(Psychological Operations, PSYOP)，在美軍聯合作戰準則JP3-13中指出，軍事資訊支援作戰是透過完善的計畫作為來對國外受眾傳遞篩選過的訊息或方針來影響他們的情感、動機、主觀認知並最終達到外國政府、組織、團體乃至個人在行為上產生改變。在資訊環境中軍事資訊支援作戰針對認知域進行影響行動，對象從敵對方、友方乃至中立群眾都是影響的對象。[83]美國國會研究處的研究員，同時也是資訊戰、網路安全專家的希歐海莉(Catherine A. Theohary)，在其提供給國會的報告中直指「軍事資訊支援作戰是資訊作戰的核心」，更凸顯了軍事資訊支援作戰與資訊作戰間緊密的關係。[84]

九、 情報(Intelligence)

情報是軍隊作戰成功的要素，孫子云：「知己知彼，百戰不殆」，情報便是讓軍隊指揮官能夠「知彼」的重要軍事能力，在美軍聯合作戰準則JP3-13中指出，情報對資訊相關能力的計畫者與資訊作戰「整合者」提供當地人口為中心的社會文化情報以及資訊的流通程度(例如:網路覆蓋率等資訊)，使他們能夠運用適當的手法引導受眾做出所望之行為。[85]

---

[82] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. II-9.

[83] Ibid., p. II-9.

[84] Catherine Theohary, op. cit., p. 1.

[85] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. II-10.

十、 軍事欺敵(Military Deception, MILDEC)

從字面上來解釋，軍事欺敵就是釋放錯誤的資訊欺騙敵人，而使敵人做出錯誤的決策。而在美軍聯合作戰準則JP3.13.4中寫到，軍事欺敵作為資訊作戰的其中一項能力，必須和其他相關能力密切協調並整合，以達支持指揮官的作戰任務之目的，而總體上來說，即是影響敵方決策者的資訊系統與決策。[86]

十一、 作戰安全(Operations Security)

美軍作戰安全的概念類似於我國國軍的保防安全，在美軍聯合作戰準則JP3-13.3中敘明，作戰安全用於識別、控制與保護關鍵資訊，辨識可能被敵方情報系統所掌握或觀察的行動，那些特定的資訊可能被敵人蒐集、分析與解譯後會對其產生助益。[87]簡言之，就是審定有哪些資訊是需要保密，哪些可以公開。

十二、 特殊技術作戰(Special Technical Operations, STO)

這項能力相當特殊且神祕，在美軍可供線上獲取的準則內之記述均為「若要詳細瞭解特殊記述作戰的資訊以及其對資訊作戰做出的貢獻，請洽作戰指揮部或軍種司令部內的特殊技術作戰計畫人員」，[88]然而一篇1999年的華盛頓郵報報導透露了，特殊技術作戰相關部門在冷戰時期成立，是一種攻擊性的資訊戰(offensive information warfare)。[89]

十三、 聯合電磁頻譜作戰(Joint Electromagnetic Spectrum Operations, JEMSO)

---

[86] Joint Chiefs of Staff, "*Joint Publication 3-13.4: Military Deception*," January 26, 2012, p. ix.

[87] Joint Chiefs of Staff, "*Joint Publication 3-13.3: Operations Security*," January 6, 2016, p. ix.

[88] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. II-12.

[89] William M. Arkin, "Phreaking Hacktivists," *washintonpost.com*, Janunary 18, 1999, < https://www.washingtonpost.com/wp-srv/national/dotmil/arkin011899.htm>.(Accessed:11/2/2020)

聯合電磁頻譜作戰區分電子戰(Electronic Warfare, EW)與電磁頻譜管理作戰(Electromagnetic Spectrum Management Operations, JESMO)兩個部分，根據美軍聯合作戰準則JP6-01的敘述，聯合電磁頻譜作戰旨在爭取電磁作戰環境中(Electromagnetic Operational Environment, EMOE)的資源與優勢，並解決電磁干擾(electromagnetic interference)之問題。[90]而聯合作戰資訊作戰準則JP3-13則指出，所有資訊相關的任務都仰賴電磁頻譜(Electromagnetic Spectrum, EMS)來進行，而聯合電磁頻譜作戰則提供了在作戰或任務地區內電磁頻譜攻防的能力；另外，聯合電磁頻譜作戰在資訊作戰中的任務將由指揮官直屬電子作戰參謀進行協調與計畫。[91]

十四、 關鍵領導人交涉(Key Leader Engagement, KLE)

關鍵領導人交涉在參謀總長聯席會議的電子圖書館中，亦無獨立之準則編目。依據美軍聯合作戰準則JP3-13，關鍵領導人交涉是美軍指揮官在經過完善謀劃後與外國受眾間產生的交流互動，而目的在於透過影響對於當地居民具有影響力的人物，間接對大眾產生影響，以支持聯合作戰部隊指揮官的目標，如此的交涉可能由軍事資訊支援作戰幕僚、民事幕僚(civil affairs)或是由資訊作戰幕僚來進行策畫，奉核定後再由各部隊指揮官執行，故未列於圖2-1席次中。[92]

貳、從核心能力到相關能力

美軍雖於2014年版的聯合作戰資訊作戰準則訂定14項資訊相關能力，但並非

---

[90] Joint Chiefs of Staff, "*Joint Publication 6-01: Joint Electromagnetic Spectrum Management Operations*," March 20, 2012, p. vii.

[91] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. II-12.

[92] Ibid., p. II-14.

一開始就是如此，事實上，在2012年準則修訂之前，各能力被區分為「核心能力」(core capabilities)與「相關能力」(related capabilities)，[93]直至2012年準則修訂後，方才將現有之14項資訊相關能力納入準則中，將「核心能力」的用詞一併轉變為「相關能力」，其原因並未敘明，但可從準則內介紹資訊作戰與資訊相關能力的關係與整合之前言中推敲端倪：「資訊作戰無關各能力間的主導權(ownership)，而是將各能力視為戰力的增幅器來創造所望效果」。[94]由此敘述可推知，美軍會如此強調資訊作戰並非關乎各能力間的「主導權」，應是在推行資訊作戰制度期間，因為強調「核心能力」，使得聯戰指揮官或其參謀誤認為策畫資訊作戰行動時「核心能力」為「主要」考量，因此美軍才特別於準則內強調資訊作戰之「整合者」的角色，強調「只要是能夠用來創造所望成效之能力，都應在計畫流程中被納入考量」。[95]此項敘述也說明了圖2-1中，參與資訊作戰小組會議之成員，不僅止於資訊相關能力所派遣之代表與會。

另外，美國陸軍上校西卡雷斯(Carmine Cicalese)在其文章中，也解釋了這個名詞更動帶來的益處。他認為這樣的改動能讓「指揮官與其幕僚不受限的將更多可能影響敵方決策的選項納入考量，同時又能讓各種能力在資訊作戰的準則的框架下，更加自由自在的發展及改變」。[96]他強調了「將更多可能影響敵方決策的選項納入考量」，也印證了前述之觀點，也就是原本的「核心能力」乙詞在某種程度上造成聯戰部隊指揮官或其參謀之混淆，致使美軍在檢討後決定做出名詞上的修訂。

---

[93] 在 2006 年版準則中，資訊作戰核心能力(core capabilities)為心理作戰(PSYOP)、軍事欺敵(MILDEC)、作戰安全(OPSEC)、電子戰(EW)以及電腦網路作戰(CNO)；而相關能力(related capabilities)僅有公共事務(PA)、軍民作戰(CMO)以及國防支持公共外交(defense support to public diplomacy)等 3 項。

[94] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. II-5. (原文為:IO is not about ownership of individual capabilities but rather the use of those capabilities as force multipliers to create a desired effect. There are many military capabilities that contribute to IO and should be taken into consideration during the planning process.)

[95] Ibid., p. II-5.

[96] Carmine Cicalese, "Redefining Information Operations", *Joint Forces Quaterly*, Vol. 69, 2nd quarter, 2013, pp. 109-112.

參、資訊相關能力有賴整合運用

在美軍聯合作戰準則中敘明，整合資訊相關能力之目的在於「影響受眾」[97]，另外，美國國防部在2017年修正的《國防部3600.01號指導》(Department of Defense Directive 3600.01)文件中表明「資訊相關能力應該要整合運用，來影響、擾亂、破壞或竄改受眾的決策」，[98]另外，上述兩份文件也強調了各項能力間必須持續協調(coordinate)以達到去衝突化(deconfliction)之目的，以發揮戰力倍化器(force multiplier)的效果，[99]美軍之所以在這些資訊作戰的規範性文件中不斷強調，資訊相關能力必須要整合運用能從蘭德公司所撰擬《美軍於阿富汗地區之資訊作戰–2001至2010年間之心理作戰成效》乙書中看出端倪，該報告於2012年4月30日發布，在其報告第六章〈影響資訊作戰與心理作戰的組織性問題〉內的7項檢討中，就有「資訊作戰與各單位作戰行動缺乏整合」、「過長的反應時間與協調上的拖延」、「資訊作戰與心理作戰之間之介面效能不彰」、「資訊作戰軍官遭到孤立」、「資訊作戰與公共事務之間缺乏協調」等5項檢討屬於能力間的整合失當，[100]也因此可以推知，美軍為何會在2012年11月大修自從2006年以來未曾修訂資訊作戰準則，並處處強調「協調」與「整合」的重要性。綜合以上所述，資訊相關能力的運用關係著資訊作戰之成敗，而如何調和運用各資訊相關能力及其他軍事、政府部門以及民間之能力，並且避免在資訊環境(information enviroment)中產生訊息之不協調(inconsistant messaging)，更甚者能夠互相加乘，協助指揮官乃至國家目標之達成，才是資訊作戰的最終極目標。[101]

---

[97] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. I-5.

[98] Department of Defense, "*Department of Defense Directive 3600.01*," May 4, 2017, p. 12.

[99] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. I-1.

[100] Arturo Munoz, *U.S. Military Information Operations in Afghanistan: Effectiveness of Psychological Operations 2001-2010* (Santa Monica, CA: RAND Corporation, 2012), pp. 119-132.

[101] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. II-14.

第二節、資訊環境

在前一節談論美軍資訊作戰相關能力時，可以發現資訊作戰旨在統合運用各項軍事能力來爭取軍隊甚至國家整體在資訊環境(information environment)中的能動性與優勢，但是資訊環境這個名詞在我國國軍卻沒有人探討與重視，所以將進一步介紹他們極力想營造優勢的「資訊環境」究竟是什麼，以便進行後續研究及探討。

壹、資訊環境的構成

美軍聯合作戰準則JP3-13賦予資訊環境的定義為：「收集、處理、發送或是依據資訊行事的個人、組織、系統之聚合體」[102]，而此環境由實體域(physical dimention)資訊域(informational dimention)與認知域(cognitive dimention)這三個時時刻刻與每個個人、組織或是整個社會系統交流互動的場域所構築而成(如圖2-2)，資訊相關能力可能橫跨複數個場域中進行活動，聯戰部隊指揮官透過資訊相關能力之運用來向處在物理域及資訊域中的受眾提供或傳遞訊息，並衝擊其認知域，最終影響其決策。[103]以下列述各場域之特性與內涵。

圖 2-2 資訊環境示意圖

資料來源：Joint Chiefs of Staff, "*Joint Publication 3-13: Information Operations*," November 20, 2014, p. I-2

[102] Ibid., p. I-1

[103] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. I-3.

一、 實體域(physical dimension)

實體域在美軍的定義中由指揮與管制(command and control, C2)、關鍵決策者以及個人或機構遂行影響作戰(influence operations)時所仰賴的基礎設施所組成[104]；進言之，此場域中包含個人、指管設施、報章刊物、無線基地台、手機、電腦等等之類的實體物件。

二、 資訊域(informational dimension)

資訊域是以資料為中心的場域，在美軍聯合作戰準則中將資訊域描述為「資訊被收集、處理、儲存、傳散的場域」[105]，在此場域中的行動將會影響資訊的內容及流動。而作者認為，在資訊域中的核心在於透過實體域而連結、傳遞的資訊，諸如聲音、影像、文字等電磁紀錄等等，而透過在資訊域中進行的行動，傳遞各式各樣的資訊。

三、 認知域(cognitive dimension)

認知域乃是以人類為中心的特殊場域，所謂的以人類為中心是指「傳遞、接收以及依照訊息做出反應或行動的個人或團體」，[106]而各種資訊相關能力在認知域中的操作會影響其對所獲得資訊的處理流程及看法、價值判斷等，最終影響他們的決策，有許多因子能夠造成這些影響，諸如文化、信仰、規範、動機、情感、經驗、道德、教育、身分認同、意識形態等等諸多樣貌，均能在認知域的操弄上獲致成果，[107]而藉由操弄這些因子，才是影響受眾決策及其後續行為之最佳途徑，這也是認知域在美軍的資訊作戰準則中被認定為「資訊環境中最重要的部分」。[108]

除了美軍聯合作戰準則之外，在美國陸軍技術手冊ATP3-13.1中也將資訊環境

---

104 Ibid., p. I-2

105 Ibid., p. I-3

106 Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. I-3

107 Mazarr, Michael et al. *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment*(Santa Monica, CA: RAND Corporation, 2019), pp. 16-20.

108 Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. I-4

中的三個場域做出清楚的定義與舉例，其中實體域影響的是內容(content)，例如實體網路、人際網絡等等；資訊域影響的則是密碼(code)，例如蒐集、編碼、處理、儲存、傳散、撥放與保護的資訊、社群媒體的應用軟體等；認知域影響的是情境(context)，例如觀點與輿論、資訊帶給人如何的衝擊(詳如表2-1)。

表2-1 資訊環境內部各場域區分表

種類	影響	範例
實體域	內容(content)	現實世界與其內容、尤其是能夠支持意見、資訊與訊息交換的物件 ・ 資訊系統與實體網路 ・ 通訊系統與網路 ・ 人與人際網絡 ・ 個人裝置、個人數位助理、手持裝置與社群媒體、圖像式使用者介面
資訊域	密碼(code)	・ 被蒐集、編碼、處理、儲存、傳散、撥放與保護的資訊 ・ 資訊的後設資料、資訊流與其品質 ・ 社群媒體應用軟體、資訊交換與搜尋引擎 ・ 密碼本身 ・ 任何自動化產生的決策
認知域	情境(context)	・資訊對人類意志造成的衝擊 ・情境化的資訊與人類決策 ・無形資產，例如道德、價值、世界觀、狀況覺察 ・觀點與輿論 ・對刺激而產生的心理計算，例如喜歡社群媒體應用程式中的某樣物品

資料來源：Department of the Army, "*Army Techniques Publication 3-13.1: The Conduct of Information Operations*," October 4, 2018, p. 2-2

貳、資訊環境中之資訊流動及變化

以上針對資訊環境中三個場域之內涵進行探討，但三個場域中的資訊流動及

如何形成影響決策仍未明朗，對此，西卡雷斯上校提出了資訊域是鏈結實體域及認知域的重要環節，而將其建構成一個決策程序中行動與反應的循環(action-reaction cycle)，他認為所有資訊的傳散(dissemination)、處理(prcess)與蒐集(collect)都在資訊域中進行，而透過資訊域中的努力，能夠影響認知域中的狀況覺察與決策，最終造成不同的行動與反應，而聯合作戰部隊指揮官與其幕僚應該依據變動中的認知域及實體域狀況，不斷重複進行這個循環 (如圖2-3)。[109]

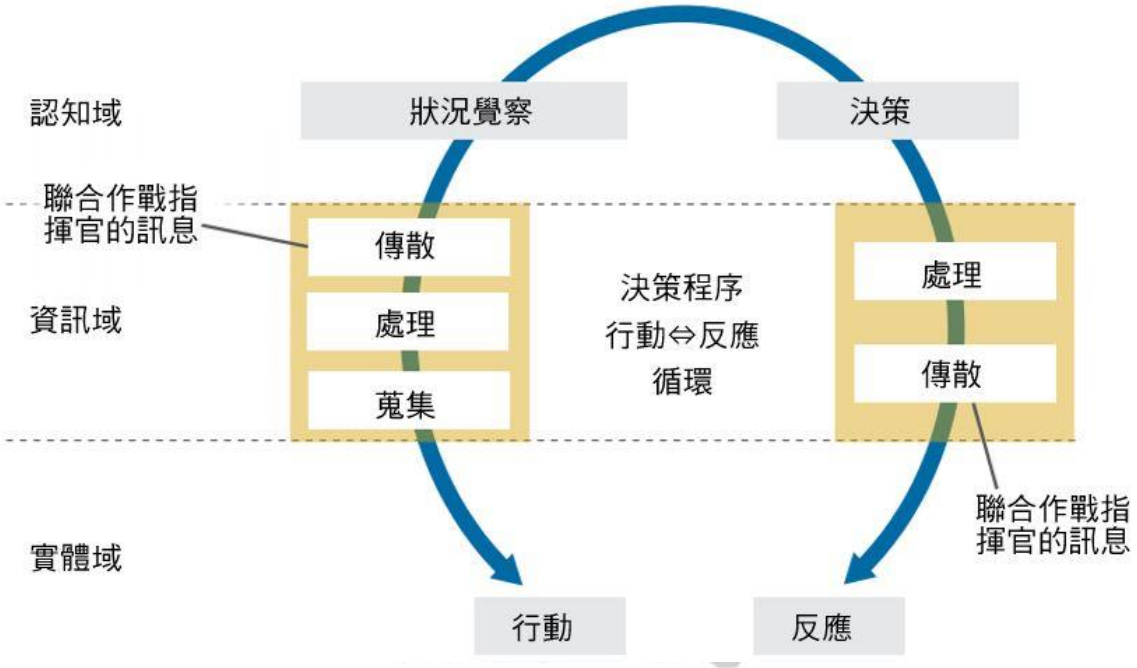

圖2-3 行動-反應決策程序循環示意圖

資料來源:Carmine Cicalese, “Redefining Information Operations”, *Joint Forces Quaterly*, 2nd quarter, 2013, vol. 69, pp. 109-112. <https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-69/JFQ-69_109-112_Cicalese.pdf>.

然而，西卡雷斯的行動-反應決策程序循環僅說明了實體域、資訊域以及認知域間的連結以及美軍如何在資訊域中透過資訊蒐集、處理以及傳散的各步驟來影響受眾的決策，未能進一步說明資訊如何流動、改變並影響受眾的決策，對此，蘭德公司的資訊作戰專家保羅(Christopher Paul)，在其2018年的著作中，則以5個層次，

[109] Carmine Cicalese, op. cit., pp. 109-112.

劃分出資訊的流動及變化以及受眾接收資訊後產生行動之循環(如圖2-4)。[110]

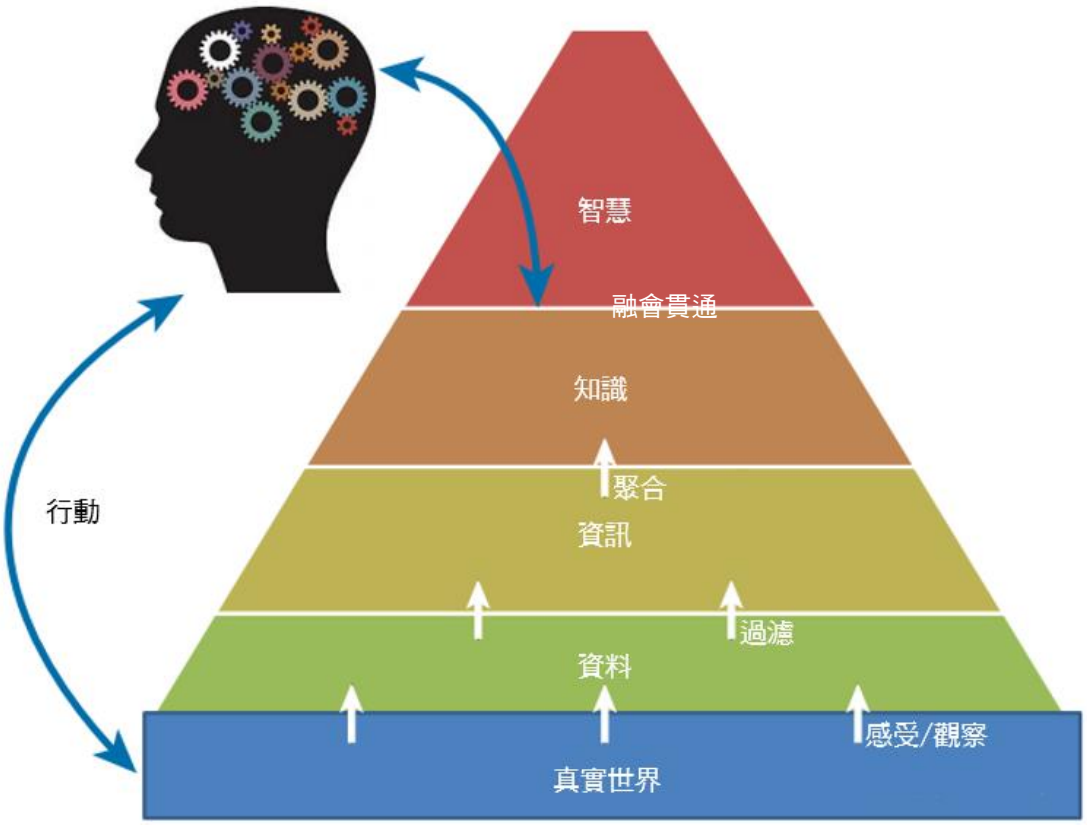

圖 2-4 資訊環境與行動循環示意圖

資料來源：修改自：Christopher Paul et. al, *Improving C2 and Situational Awareness for Operations in and Through the Information Environment*. (Santa Monica, CA: RAND Corporation, 2018). p. 8.

如上圖所示，真實世界(Physical World)係指受眾生活的真實世界即屬於物理域之範疇，而受眾在日常生活中透過感受(Sensor)與觀察(Observation)接收資料(Data)，資料再經過過濾後成為資訊(Information)，而資訊再經聚合之後，內化成為受眾本身的知識(Knowledge)，知識經過融會貫通(Synthesis)之後則進入認知域成為個人之智慧(Wisdom)，個人行動則基於本身的智慧所產生，而行動後又會在受眾的生活中創造出新的資料，如此進行重複之循環。[111]而此種循環正是美軍資訊作戰所專注之

[110] Christopher Paul et al., *Improving C2 and Situational Awareness for Operations in and Through the Information Environment*, op. cit., p. 8.

[111] Ibid.

著力點。

透過上述的探討，我們可以發現，美軍整合運用各個資訊相關能力，在資訊環境中進行活動，並達成資訊作戰計畫者所欲達成之效果。另外，美軍資訊作戰與其他作戰類型的計畫流程中，針對作戰評估(operation assessment)較為不同，因為資訊作戰在的評估要項及作戰效能評量上通常仰賴認知域的測量。[112]所以，各種資訊相關能力在實體域及資訊域中的所進行的活動，都是為了在認知域中造成衝擊與影響，因此本文在此歸納出二種類型之資訊能力，第一、於實體域及資訊域中創造、蒐集或傳遞資訊(資料)或妨礙敵方、保護我方進行以上行為之資訊相關能力，例如：軍民作戰、關鍵領導人交涉、網路作戰、情報、聯合電磁頻譜作戰、特殊技術作戰、跨部會協調組、資訊確保、太空作戰、軍事欺敵。第二、計畫如何運用其他能力對認知域產生衝擊的資訊相關能力例如：戰略溝通、公共事務、軍事資訊支援作戰(心理作戰)。[113]透過這兩種類型之能力間之密切合作，美軍資訊作戰方能達成聯合作戰部隊指揮官乃至於美國政府所望之成效。

參、資訊環境中之運作情形

在認識構成美軍資訊作戰中至關重要的兩個元素−資訊相關能力以及資訊環境後，我們將進一步探討，美軍資訊作戰到底如何將資訊相關能力整合並投入資訊環境。對此我們依然必須回到美軍資訊作戰準則中進行探討，美軍聯合作戰資訊作戰準則內，在針對資訊作戰與個別資訊相關能力間的關係進行介紹時，不斷強調整合(integrate)、同步(synchronize)與去除衝突(deconflict)，如同美國波依德上校發表之文章中，要大家不妨將資訊作戰看作是各種資訊相關能力的整合者(integrator)。

---

112 Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. VI-2

113 分類係參考 Eric V. Larson 等人之著作中對於影響作戰(Influence Operations)之分類，詳見：Eric V. Larson et al., *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities*(Santa Monica, CA: RAND Corporation, 2009), p. 3-4.

[114]在美軍聯合作戰準則中，將資訊作戰作為一個整合者，要如何將資訊相關能力整合後投入資訊環境中運作，繪製了完整的示意圖(如圖2-5)。

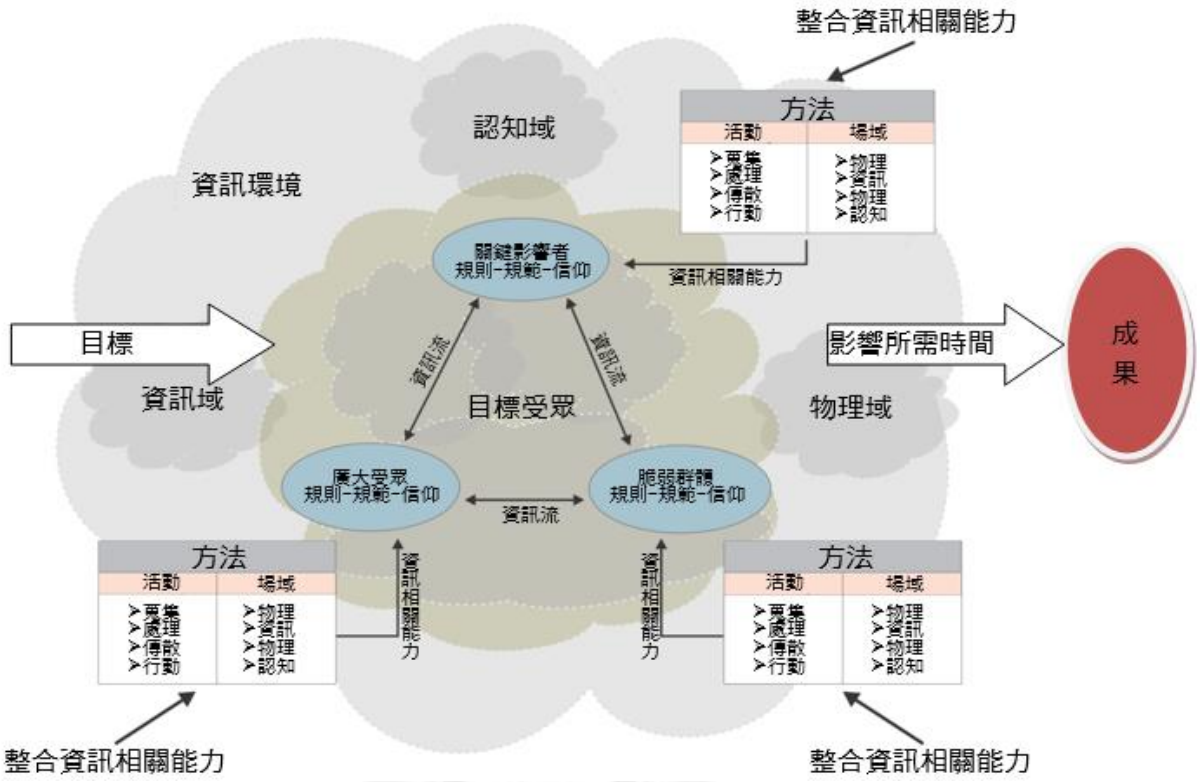

圖2-5 資訊相關能力運用示意圖

資料來源:Joint Chiefs of Staff, "*Joint Publication 3-13:Information Operations*," November 20, 2014, p. I-8

在上圖中，說明了美軍資訊作戰為了達成其資訊作戰目標，將各種資訊相關能力整合後(指涉完成計畫作為後)，投入資訊環境中，分別針對各場域進行資訊的蒐集、處理及傳散，其順序分別是在實體域中進行資訊的蒐集，接著在資訊域中處理所蒐集之資訊，然後回到實體域中進行處理完的資訊成品傳散(product dissemination)，最後在認知域中進行行動，在進行一定時間的資訊投放後，產生所望成效，也就是對受眾產生認知上的影響，進而影響他們的決策(行為)。

---

[114] Curtis D. Boyd, "The Future of MISO", *Special Warfare*, Vol. 24, Issue 1, January-February 2011, pp. 22-28.

第三節、美軍資訊作戰的運作

上個節次中，我們已然瞭解資訊相關能力如何被投放於資訊環境之各場域中運作，本節次將著眼於美軍如何資訊作戰的計畫流程、執行流程與成效評估，希望透過如此探討能夠深刻瞭解美軍資訊作戰之目的，並對於本文後續之研析有所助益。

壹、美軍聯合作戰資訊作戰計畫流程

美軍資訊作戰的計畫流程分為七個步驟，依序為計畫啟動、任務分析、發展行動方案、分析行動方案與兵棋推演、比較行動方案、核定行動方案、發展計畫或命令，以下依序列述之。[115]

一、計畫啟動(planning initiation)：各種資訊相關能力應於此階段即整合進入計畫流程，而資訊作戰業參在此階在受領命令及初步計畫指導後，即開始召集資訊作戰小組、並審視戰略指導文件、辨識計畫所需等級、提出資訊需求、持續觀察狀況等作業。

二、任務分析(mission anaysis)：任務分析的目的在於瞭解本次的作戰行動有何問題，並擬定出適當的指導以利後續計畫流程順遂，完成任務分析後，各業參應對任務具有充分之瞭解。在此階段除了與作戰、情報等部門將有密切之聯繫協調及工作事項外，在資訊作戰本身的項目就是要分析出各別資訊作戰能力對於本次任務能有何種幫助。

三、發展行動方案(COA development)：在此階段資訊作戰人員必需再次聲明資訊作戰任務，並訂定出資訊作戰的工作事項、資訊作戰的基礎假設、限制、找出當前資訊作戰缺乏之項目、識別資訊作戰風險等工作。

---

[115] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., pp. IV-7 -IV-8.

四、分析行動方案與兵棋推演(COA analysis and war gaming)：相對應於聯合作戰計畫的任務分析階段，在本階段中資訊作戰業參必需提出資訊作戰支援構想並充分瞭解聯合作戰指揮官所望之影響成效，並找出最適合完成本次任務的資訊相關能力或相關活動，其後必需提出效能評量方法與其指標，剩餘如檢視交戰規則(rule of engagement, ROE)、識別作戰風險等細項在此省略。

五、比較行動方案(COA comparism)：此階段將基於任務為出發點來比較各別行動方案之優劣，並將資訊作戰任務的需求與可運用的資訊相關能力做出關聯性對照，最後從資訊作戰的觀點將行動方案作出排序。

六、核定行動方案(COA approval)：在此階段資訊作戰業參將向聯合作戰指揮官進行個行動方案之簡報，最後由指揮官下達決心採取何種行動方案。

七、發展計畫或命令(plan or order development)：依據聯合作戰指揮官的決心及其核定之行動方案來完成資訊作戰計畫及命令。

以上為美軍聯合作戰資訊作戰計畫流程之簡要敘述，實際上此種七步驟的計畫模式不僅是資訊作戰如此，軍事資訊支援作戰(心理作戰)之計畫流程亦區分七步驟，這些流程都是依據美軍聯合作戰計畫準則JP5-0中的聯合作戰計畫流程中發展所得，[116]另外，在2012年的準則修正中，特別強調了「資訊作戰必需整合於聯合作戰計畫流程內」之改動，[117]也說明了美軍企圖透過標準化的作業流程，使資訊作戰與其他資訊相關能力乃至其他作戰途徑軍能配合無間。

貳、美軍聯合作戰資訊作戰執行流程與應用

[116] Joint Chiefs of Staff, "*Joint Publication 5-0: JJoint Planning*," June 16, 2017, pp. V-2 -V-49.

[117] Joint Chiefs of Staff, "*Joint Publication 3-13: Information Operations*," November 27, 2012, p. iii.

關於美軍聯合作戰資訊作戰之執行流程，美軍帕拉羅中校(Hans F. Palaoro)先將資訊相關能力(在當時為核心能力與相關能力)區分為軟性與硬性工具，然後分別針對敵人之心智(mind)遂行影響、另一端針對C4ISR系統進行破壞，最終達成敵方行為上的改變或喪失抵抗能力之目的。[118]然而，因美軍聯合作戰準則JP3-13修正後在資訊相關能力方面已有所不同，作者試依照美軍現行準則改繪如下圖(如圖2-6)。

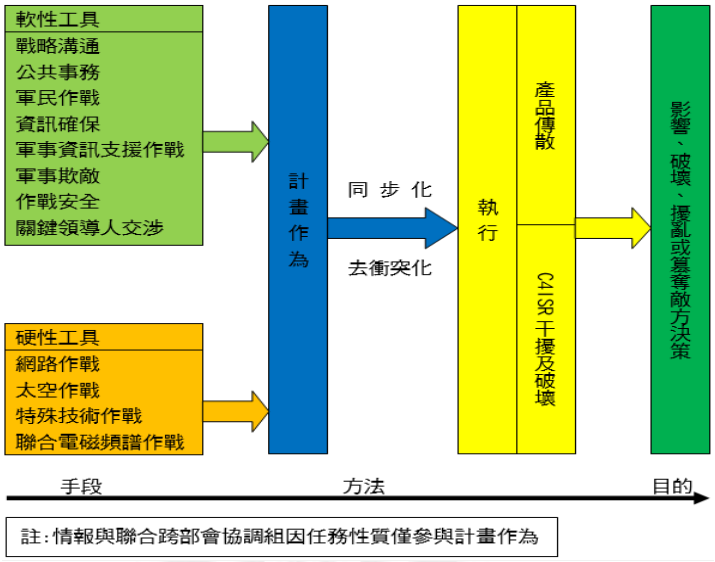

圖2-6 資訊作戰流程圖

資料來源：修正自：Hans Palaoro, "*Information Strategy: The Missing Link*", Joint Forces Quaterly, 4th quarter, 2010, vol. 59, No. 4, p. 85.

從帕拉羅的論述，結合目前美軍聯合作戰準則，資訊作戰的流程就是將各種手段(資訊相關能力)透過計畫流程整合後，再分別運用軟性及硬性的方法達成目的，然而，僅透過圖示可能仍難以瞭解美軍資訊作戰到底可以如何運用，故在此援引美軍聯合作戰準則JP3-13中的簡略範例(如表2-2)。

[118] Hans Palaoro, "Information Strategy: The Missing Link", *Joint Forces Quaterly*, Vol. 59, No. 4, 4th quarter, 2010, pp. 83-85.

表2-2 美軍資訊相關能力運用範例

狀　　況	敵對方正試圖推翻甲國的政府，並運用致命與非致命手段來向民眾展示甲國政府無法支持與保護其人民。
聯戰指揮官目標	保護甲國政府不被推翻
所望效果	1.民眾對甲國政府保護人民的能力產生信心 2.敵對方無法推翻甲國政府
潛在受眾	1.敵對方領導人(敵對方) 2.甲國人民(友善、中立、潛在敵人)
達成聯戰指揮官目標的潛在手　　段	1.外交行動(例如:外交照會或公共外交) 2.資訊手段(例如:戰略溝通、媒體) 3.軍事武力(例如:派遣安全部隊、作戰行動、軍事資訊支援作戰、公共事務、軍事欺敵) 4.經濟資源(例如:制裁、對甲國國家建設挹注資金) 5.商業、文化、或其他私部門手段
潛在方法	1.針對性的無線電及電視廣播 2.封鎖敵對方港口 3.政府或商業經營的網站宣傳 4.關鍵領導人交涉

資料來源: Joint Chiefs of Staff, "*Joint Publication 3-13: Information Operations*," November 20, 2014, pp. II-3 – II-4.

範例雖然簡略，但我們可以清楚從內容得知，美軍資訊作戰在每個不同的狀況下，會選定適當的手段(資訊相關能力)，然後再細部決定在實體域及資訊域中採取哪些方法，來影響敵方的決策，最終造成行為上的改變。例如在範例中，敵對方領導人可能因為港口遭到制裁，進而造成資源、經濟上的影響，所以改變其決策，不再染指甲國，意即產生行為上的改變；抑或是因為敵對方人民接受到網路的宣傳後，產生反戰輿論，進而造成敵對方內部壓力，影響其決策，進而停止對甲國政府的顛覆行動。當然，美軍資訊作戰能運用的能力不僅止於範例內的描述，根據聯合作戰準則所述，資訊作戰即是動用舉國之力，包含外交、資訊、軍事、經濟(diplomatic, informational, military, economic, DIME)，使美國領導人能解決世界各角落發生的問題。[119]因此，美軍的資訊作戰往往不僅止於國防部參與，視情況可動員各部會乃至私部門資源進行資訊作戰。

[119] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. ix.

參、美軍資訊作戰之運作本質

綜合以上對於美軍資訊作戰的探討，可以發現美軍資訊作戰歷經長久的發展，時至今日成為各項軍事能力，乃至整體國力的整合與運用，與國內目前多數單從網路科技進行探討的論述完全不同，作者認為，美軍資訊作戰應可用機制(mechanism)來定位，而美軍在2017年修正的《國防部3600.01號指導》中也將資訊作戰描述為「原則性機制(principle mechanism)」，透過此一原則性機制的運用，在作戰過程中整合、同步化、運用即評估各種各樣的資訊相關能力，並與其他作戰進程相配合，以影響敵人或潛在對手的決策程序並保護己方決策程序。而在此機制中，軍事資訊支援作戰(心理作戰)就應如希歐海莉所言：「是為資訊作戰的核心」(are central to IO)，[120] 或者，如其所言，資訊作戰是某種形式的政治作戰(political warfare) 。[121]

除了希歐海莉的論述以外，蘭德公司資訊作戰專家保羅(Christopher Paul)在其2017年的著作「主宰愚人的國度」(Dominating Duffer's Domain)中，運用說故事的手法，講述一個資訊作戰軍官和虛擬大陸阿托匹亞(Atropia)上的住民進行合作的故事。[122]然而主角雖然是資訊作戰軍官，但在短短3頁的故事中，除了資訊作戰(IO)之外，幾乎只有提及軍事資訊支援作戰(MISO)，而且故事中的資訊作戰軍官「協助修改」了軍事資訊支援作戰的系列計畫，來達成他的任務的描述，更是緊緊的把資訊作戰與軍事資訊支援作戰扣在一起，也可見軍事資訊支援作戰在資訊作戰中的重要性。另外從美國蘭德公司將資訊作戰賦予影響作戰(influence operations)的別名上可以得知，美軍雖有強大的武力與科技能力，仍然十分注重不戰而屈人之兵的伐謀手段。[123]而我們也再次證明，資訊作戰之乃是一種整合、協調各種資訊相關能力，

---

120 Catherine Theohary, op. cit., p. 1.

121 Catherine A. Theohary, Information Warfare: issue for congress, op. cit., p. 2.

122 Christopher Paul and William Marcellino, *Dominating Duffer's Domain: Lessons for the U.S. Army Information Operations Practitioner*(Santa Monica, CA: RAND Corporation, 2017), pp. 33-35.

123 蘭德公司資訊作戰專題首頁賦予資訊戰之定義原文為：「Information operations and warfare, also known as influence operations, includes the collection of tactical information about an adversary as

透過這謝能力之和諧運作產生綜合性的效果，進而在認知域中影響受眾之「機制」。

小結

「資訊」一詞，雖然包含電腦、網路等科技裝置及技術，但這些在美軍的資訊作戰中並不是主角，真正的重點在於抽象的「影響」。所謂的資訊不僅僅是運用報章雜誌、媒體、口耳相傳等和平方式才能傳遞，例如，美國海軍將航母打擊群調動到北韓外海，美國陸軍或海軍陸戰隊在俄羅斯邊境進行軍演，都會創造並傳遞大量資訊。[124]但是在運用任何手段向外傳遞訊息時，都要注意不可以互相衝突或牴觸，以免造成訊息的不協調甚至衝突，而降低我方訊息的可信度。最後，綜合本章內各節之討論，作者認為，美軍資訊作戰是一種整合運用所有可能之手段，來進行認知域中的影響及操弄之機制(mechanism)，而我國若能學習此機制來對抗中共對我國之文攻武嚇，就如同美軍1998年版的聯合作戰資訊作戰準則中所陳述，資訊作戰極具效率且成本效益的特性(efficient and cost effective)，[125]我國如能研究效法之，也不失為國防上一項廉價且有效之投資。

well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent」，詳見<https://www.rand.org/topics/information-operations.html>.(Accessed：14/9/2019)

[124] Scott K. Thomson and Christopher E. Paul, “Paradigm Change: Operational Art and the Information Joint Function”, *Joint Forces Quaterly*, vol. 89, 2nd quarter, 2018, pp. 8-14. <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1490645/paradigm-change-operational-art-and-the-information-joint-function/>. (Accessed:10/6/2019)

[125] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(1998), op.cit., p. I-11

第三章、解放軍信息戰及其戰略支援部隊

在美國網路作戰指揮部(USS CYBERCOM)組建之後，解放軍意識到國家戰略利益不斷向資訊空間拓展，迅速增強資訊攻防能力並確保資訊安全已成為國力增長的關鍵，在其2019年國防白皮書的敘述中，網路空間是經濟、社會與國家安全的關鍵領域，網路安全是所其面臨最嚴峻的安全威脅。因此，解放軍必需加快網路空間力量建設，專注發展網路安全，提升國家網路防禦能力，建設與「網絡強國」之名相稱之網路防護力量，保障資訊網路安全，並捍衛國家「網路主權」。[126]

而解放軍在其強軍系列叢書《戰略邊疆》內，將資訊作戰能力區分為資訊進攻能力與資訊防禦能力，其中，資訊進攻能力係指利用各種資訊攻擊手段，採取資訊威懾、資訊滲透、資訊遮斷、資訊擾亂、資訊削弱、資訊封鎖、資訊欺騙和資訊摧毀等方式，癱瘓、中斷、削弱、利用、欺騙乃至摧毀敵方資訊系統及其功能，使其喪失資訊優勢和資訊能力的能力。而資訊防禦能力則是透過採取資訊防護、探測攻擊和資訊恢復等形式，保護己方的資訊系統不被敵方干擾、破壞和利用，以保持資訊系統工作的穩定的能力。[127]

解放軍為了確保在其「資訊邊疆」中的優勢，並配合習近平的強軍軍改，解放軍戰略支援部隊於2015年12月31日成軍，而該部隊的組建將成為中共資訊作戰部隊的主力，同時也建構了中共「積極防禦」戰略構想之核心。[128]這支部隊將會為解放軍撐起「資訊傘」，意即為解放軍落實資訊防護工作，並且會整合各軍種與系統，提供「準確高效可靠的資訊支撐和戰略支援保障」。[129]由此敘述看來，這支部隊將會以資訊、通訊的防禦為主。另外，中共在其2019年國防白皮書中將戰略支援部隊

---

126 中華人民共和國國防部，〈新時代的中國國防〉，《中華人民共和國國 防白皮書》，2019 年 7 月 24 日，頁 6。<http://www.mod.gov.cn/big5/regulatory/2019-07/24/content_4846424.htm>。(瀏覽日期:2019 年 8 月 12 日)

127 周碧松，〈戰略邊疆〉，《軍報記者》，2016 年 8 月 15 日，< http://zlzy.81.cn/tb/2016-08/15/content_7231775.htm >。(瀏覽日期:2019 年 6 月 12 日)

128 John Costello, op.cit., p. 15.

129 Ibid.

描述為「維護國家安全的新型作戰力量」，主要能力包括資訊通信保障、戰場環境保障、新技術試驗、資訊安全防護等守勢的防護力量。[130]然而戰略支援部隊中，卻加入了號稱解放軍「三戰」基地之「三一一基地」，[131]另外也編入了原本的總參謀部技術偵查部負責網路攻擊的網軍部隊，其將原本在地理位置上分散的各個電子作戰、網路作戰及心理作戰部隊集合在同一個部隊指揮體系下，[132]展現了解放軍試圖整合這些能力來進行網路化宣傳戰的意圖，可謂是中共所發展的、或可謂有些許模仿美軍資訊作戰進行能力整合之端倪，[133]而這些攻勢軍事能力之整合也證明了中共在其國防白皮書內宣稱之守勢防護力量皆為虛言。是故，本章將著眼探討要點有兩點，其一為三戰與美軍資訊作戰之關聯性，其二為中共戰略支援部隊之組織架構與能力，透過本章節之探討，期望能對我國面對中共所帶來之非傳統型態威脅有所助益。

第一節、中共三戰、信息戰與美軍資訊作戰

我國對於三戰之討論與研究，多侷限於探討三戰之本質與策略，如我國國防大學出版之《三戰策略大解析》即是從三戰之發展背景及策略意涵等面向展開，而後逐一剖析「法律戰」、「心理戰」、「輿論戰」，最後對三戰之策略、應用及我國之因應作為進行論述。[134]然而，澳門理工學院朱顯龍教授在《全球政治評論》期刊發表之文章，罕見的納入資訊戰之概念一併討論，並提出三戰乃是中共歸納學習美軍波灣戰爭及其後之數場戰爭所得之論點。[135]本節將更進一步找出中共三戰、信息戰及美軍資訊作戰間之關聯，並試圖歸納出中共三戰於戰略支援部隊內可能扮演之角

130 同註 126，頁 9。

131 John Costello, Joe McReynolds, op. cit., p. 17.

132 Ibid., p. 452.

133 Ibid., p. 23.

134 張文廣主編，《中共「三戰」策略大解析》（桃園：國防大學，2008 年），頁 1-20。

135 朱顯龍，〈中國「三戰」內涵與戰略建構〉，《全球政治評論》，第 23 期，2008 年 7 月，頁 31。

色，期能使更多國內研究者注意戰略支援部隊具有「太空作戰」、「電子作戰」、「網路作戰」及「三戰」之整合性功能，並能夠提出更多應對策略與建議。

壹、中共三戰、信息戰與美軍資訊作戰之關聯性

美軍資訊作戰在中共稱之為信息戰，美軍首次使用資訊戰爭(information war)之概念始於1976年一篇名為《武器系統與資訊戰爭》的研究報告中，此研究被視為是美軍資訊作戰之開端，[136]而中共隨後自80年代中期開始就開始關注信息戰的發展，最早關於信息戰之著作出現於1990年，由浙江大學出版社出版的《信息戰》乙書。[137]根據人民網關於信息戰之專欄報導，中共將信息戰定位於「對思想與精神的攻擊」，並指出如果只單從軍事面或技術面了解信息戰是錯誤的，[138]另外在2010年版的《軍隊政治工作學》中也指出，作戰方式無論軟硬都朝信息化的方向發展，所以制信息權不能僅限於C4ISR、電子戰、網路戰等數位化武器裝備的制信息權，[139]也應將奪取政治、心理、宣傳信息的制信息權也納入其中。[140]由上所述，我們可以得知，中共對於資訊作戰，也就是其信息戰之定位與前章所述之美軍資訊作戰係屬雷同，均以爭取實體域、資訊域內之優勢為基礎，認知域之

136 Thomas Rona, "*Weapon Systems and Information War*", Office of the Secretary of Defense, July 1, 1976, p. 1. <https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf>.(Accessed:8/3/2020)

137 陳勇、姚有志主編，《面向信息化戰爭的軍事理論創新》(北京：解放軍出版社，2004 年)，頁 5-6。

138 沈偉光，〈信息戰：對思想和精神的攻擊〉，《人民網》，2004 年 6 月 1 日，< http://people.com.cn/BIG5/junshi/1078/2536549.html>。(瀏覽日期：2020 年 3 月 8 日)

139 制信息權，美軍稱為 information dominance，依據中國大百科全書網站之定義，制信息權之定義為：「奪取並保持己方使用信息的自由權和主動權，剝奪敵方使用信息的自由權和主動權。基本目標是控制戰場信息空間，最高目標是控制敵方的認知和信念系統。」< https://poe.zgbk.com/ecph/words?SiteID=1&Name=%E5%88%B6%E4%BF%A1%E6%81%AF%E6%9D%83 >。(瀏覽日期:2020 年 3 月 8 日)

140 王幸生主編，《軍隊政治工作學》（北京：軍事科學出版社，2010 年），頁 281。

主導為目標。

中共於2003年頒布的《中國人民解放軍政治工作條例》中首次提出運用心理戰、法律戰以及輿論戰，此後即被稱為三戰，在解放軍《軍隊政治工作學教程》內，也成為「政治工作」代名詞。[141]然而，中共突然提出三戰之構想著實引發各界聯想，就中共於21世紀初期論及信息戰的相關著作或報導文件中，解放軍大量關注之美軍作戰行動分別為1991年的海灣戰爭、1999年的科索沃戰爭、2001年的阿富汗戰爭以及2003年的伊拉克戰爭。[142]此觀點從以負責培養解放軍政工幹部之南京政治學院副教授孫建祥發表之論文可見端倪，該論文旨在倡議三戰人才之培養，其中引述伊拉克戰爭中美軍第四心理作戰群之表現，指出該單位運用多達400餘名的語言翻譯、電腦網路、通信技術、輿論宣傳、心理諮詢與法律顧問等專業人員，使美軍能夠迅速瓦解了伊拉克部隊的抵抗，依據該研究之說法，美軍在伊拉克戰場上演了一場以「三戰致勝」的好戲。[143]另外，無論在2004年解放軍出版社出版之《面向信息化戰爭的軍事理論創新》，[144]或是2010年軍事科學出版社出版的《軍隊政治工作學》等三戰相關著作中，[145]都可以看到中共所研究之對象不外乎上述自1991年至2003年間美軍之境外作戰行動及軍事轉型，無獨有偶，解放軍國防大學教授張召忠在其著作《怎樣才能打贏信息化戰爭》中，亦論及海灣戰爭立下機械化戰爭走向信息化戰爭之里程碑、展開全球信息化戰爭先河者則為科索沃戰爭，其後依序為阿富汗戰爭之實踐，直至伊拉克戰爭才完整勾勒出信息化戰爭之輪廓。[146]從以上中共對於信息戰之研究可得知，解放軍在信息化之革新歷程上緊跟著美國的腳步前進，而三戰

---

141 中華人民共和國國防部，《中國人民解放軍政治工作條例》，2003 年 12 月 5 日，頁 2。<http://dysw.cnki.net/jd/djzs/《中國人民解放軍政治工作條例》.pdf>。(瀏覽日期:2020 年 2 月 26 日)

142 同註 135，頁 31。

143 孫建祥，〈論三類新型軍事人才的培養〉，《武漢工程大學學報》，第 31 卷第 8 期，2009 年 8 月，頁 11。

144 同註 137，頁 4。

145 同註 140，頁 254-292。

146 張召忠，《怎樣才能打贏信息化戰爭》（北京：世界知識出版社，2004 年 6 月），頁 130。

之開展與中共對於美軍之研究息息相關。

從美軍資訊作戰與中共三戰之屬性上進行對比 ，兩者均屬於非致命性的作戰方式。美軍資訊作戰，如前章所論述，是以鞏固實體域及資訊域之力量為基礎，達成認知域中之優勢之爭取，進而支持國家或軍事目標之達成；而中共三戰則是其「政治工作」之核心，亦是針對認知域進行鬥爭的作戰態樣，而資訊即是作為攻擊敵人認知域的主要手段，中共認為認知系統是由個體或群體的認知、意志、情感、信念等內容所構築，要破壞此系統，不僅需要武力震懾，更需要心理的直接攻擊，而伴隨著爭奪認知域的戰爭來臨，三戰也愈發重要。[147]綜理上述論點，我們可以發現：三戰乃是中共長期針對美軍軍事行動觀察及研究後，所歸納出之「新形態政治工作」，而其內涵與美軍心理作戰相近，而其「整合資源」與組織展開行動的部分，[148]又與美軍資訊作戰之能力整合概念相契合。

貳、三戰與美軍心理作戰之比較

從三戰的層次面上來看，比較中共三戰與美軍心理作戰同時期準則之層次界定，[149]都分為戰略層次(strategic level)、戰役層次(operational level)與戰術層次(tactical level)。在中共三戰方面，從2007年的《軍隊政治工作學》中整理得知，戰略層次三戰係由中國共產黨中央及中央軍委會之決策所領導，內容係針對國際間之輿論、中立國或敵國之官方或民間使用各種宣傳媒介，並透過政治及外交等手段，來達成震懾敵人心理、爭取官方支持、贏得民眾信賴；在戰役層次的三戰則是由戰區或戰役軍團組織實施之，並由相關專業部隊執行，主要實行對象為敵方軍民，手段則為廣播、電視、空投、海漂等方式和手段；戰術層級的三戰由作戰部隊自行組

147 同註 143，頁 11。

148 同註 140，頁 273。

149 美軍 2000 年後之聯合作戰心理作戰準則版本為 2003 年(PSYOP)、2010 年(PSYOP)、2011 年(MISO)；解放軍《軍隊政治工作學》作者可得之版本則為 2006 年及 2010 年版。故文中以美軍 2003 年版《聯合作戰心理作戰準則》與解放軍 2006 年版《軍隊政治工作學》之內容進行對比。

織實施，對象則是現正交戰中之敵軍部隊，可能配合專業部隊作業進行，主要作為有防止敵人心戰策反、執行俘虜政策和喊話、廣播、宣傳彈等。[150]對比同期的美軍心理作戰聯合作戰準則JP3-53內之層次界定，戰略層級心理作戰乃是由美國政府各部門來執行全球性的資訊活動(information activities)，藉以影響外國受眾的態度、感受與行為以利美國之目標與意圖，這些活動主要在軍事領域外進行，但可動用國防部的資源並接受心戰部隊的協助；戰役層級的心理作戰是由聯合作戰部隊指揮官組織及運用，用以強化美國及聯軍部隊在作戰地區中的軍事任務執行能力，在作戰地區內，心理作戰可獨自作業或參與其他作戰行動之進行；戰術層級之心理作戰是由戰術層級部隊指揮官(tactical commander;意即旅級以下作戰部隊)運用，主要用途是對抗敵方部隊，獲取相對性的軍事優勢、達成戰術目標。[151]以上為中共2007年版軍隊政治工作學及美軍2003年版內之層次敘述內容比較(如表3-1)。

然而，上述的分層於2010年的美軍聯合作戰心理作戰準則以及中共《軍隊政治工作學》中內，都作了篇幅上的刪減，均只提及各層次之目的。在美軍聯合作戰心理作戰準則方面，戰略層次的目標在於達成美國政府、地區作戰指揮官(geographic combatant commander)或是跨國伙伴(multinational partners)之目標；戰役層級的心理作戰則是協助區域政策(regional policies)與軍事計畫(military plans) 之遂行；戰術層級的心理作戰則是協助地方上之軍民決策層級(local military and civil authorities)，創造地方性、立即性的效果，以支持戰役性目標之達成。[152]

---

[150] 岳忠強，《軍隊政治工作學》（北京：國防大學出版社，2007 年），頁 364。

[151] Joint Chiefs of Staff, "*Joint Publication 3-53: Psychological Operations*," op.cit., p. I-5.

[152] Joint Chiefs of Staff, *Joint Publication 3-13.2: Psychological Operations*, op. cit., p. I-4 - I-5.

表3-1 中共三戰與美軍心理作戰各層次比較表

	中共三戰		美軍心理作戰	
層次區分	運用層級	內涵	運用層級	內涵
戰略層次	黨中央、中央軍委會	對象:國際間之輿論、中立國或敵國之官方或民間。 手段:各種宣傳媒介、政治及外交等手段。 目的:震懾敵人心理、爭取官方支持、贏得民眾信賴。	美國政府	對象:外國受眾。 手段:全球性的資訊活動。 目的:影響態度、感受與行為以利美國之目標與意圖。
戰役層次	戰區、各戰役軍團	對象:敵方軍民。 手段:廣播、電視、空投、海漂等。 目的:支援戰局或大型戰役,為軍隊創造最有利的形勢。	聯合作戰部隊	對象:作戰地區內外國受眾。 手段:無線電、印刷品或其他媒體型式。 目的:強化美國及聯軍部隊在作戰地區中的軍事任務執行能力。
戰術層次	作戰部隊	對象:交戰中之敵軍部隊。 手段:防止敵人心戰策反、執行俘虜政策和喊話、廣播、宣傳彈等。 目的:削弱或動搖敵軍作戰決心,引誘敵方犯錯。	作戰部隊	對象:作戰當面之敵方、中立軍民。 手段:喊話、傳單、廣播或其他媒體型式。 目的:獲取相對性的軍事優勢、達成戰術目標。

資料來源:一、岳忠強,《軍隊政治工作學》(北京:國防大學出版社,2007年),頁364。

二、Joint Chiefs of Staff, "*Joint Publication 3-53: Psychological Operations*," September 5, 2003, p. I-5.

在中共2010年版的《軍隊政治工作學》中則將三戰中之輿論戰及法律戰描述為「主要於戰略層級發揮影響力」,心理戰則描述於戰略、戰役及戰術層級「教育訓練要求」之部分。[153]然而,無論是美軍的心理作戰準則或是中共的《軍隊政治工作學》,都共同強調了資訊化的重要性,尤其在中共2010年版的《軍隊政治工作學》中特別強調了應該要強化「資訊技術」、「電子技術」、「網路技術」以及「電腦軟體

[153] 同註 140,頁 266-279。

技術」的運用，[154]由此可知「政治工作資訊化」已列為解放軍政工之發展重點。

參、三戰「信息化」

解放軍在其《軍隊政治工作學》中講述輿論戰、法律戰、心理戰之篇章中雖不斷提及政治作戰「信息化」之概念，但對於為何要信息化以及如何信息化未有深刻論述，故以下將就「為何」及「如何」進行探討。

在2016年6月16日，解放軍軍事雜誌《國防參考》的微信帳號貼出了一篇由南京政治學院副教授逯記選撰寫，題為「專家：如何在現代戰爭中融合心理戰」的文章，該文章論及當代戰爭空間已由陸、海、空戰場擴展到資訊空間和心理空間，綜合於物理域、資訊域和認知域中共同產生作用，並指出：「只有將資訊優勢有效地轉化為認知優勢，才能給聯合部隊帶來競爭優勢，甚至達到不戰而屈人之兵之效果」。[155]獲取資訊優勢對於獲取認知優勢之重要性可由美軍聯合作戰軍事資訊支援作戰準則中對於電腦網路作戰(Computer Network Operations;現為網路作戰Cyberspace Operations)與軍事資訊支援作戰之關聯性敘述中得到解答：

> 電腦網路作戰提供軍事資訊支援作戰部隊傳播能力（包括互動性的網路活動）與拒止或降低敵對方存取、報導、處理或傳遞資訊的能力。這些能力以提供資訊環境中數位媒體之通行權之方式來支援軍事資訊支援作戰，使其能觸及更多所望接觸之受眾並阻絕受眾方面不利於作戰目標達成之資訊。[156]

---

154 同註 140，頁 274。

155 逯記選，〈專家：如何在現代戰爭中融合心理戰〉，《國防參考》，2016 年 6 月 16 日，<http://www.81.cn/jmywyl/2016-06/16/content_7105198_3.htm>。(瀏覽日期：2020 年 3 月 13 日)

156 Joint Chiefs of Staff, *Joint Publication 3-13.2: Military Information Support Operations*, op. cit., p. II-11.

從美軍軍事資訊支援作戰準則內之敘述中能發現，美軍以網軍力量結合心理作戰，實際上是為了強化心理作戰的產品傳遞能力。另外，文中更進一步提出：「受資訊化及全球化條件的影響，心理打擊由過去戰場上的戰術手段，一躍成為影響戰爭全域的戰略措施」，[157]也提供了一部分解釋，以往戰術性心理作戰手段諸如傳單、海報、廣播、喊話等等；然而隨著心理戰的層級提升置戰略層級，所施行心理戰之對象不同，而傳播媒介也不同，在戰略層級的心理作戰中，尤以現代我國智慧型手機使用率高達70.4%，[158]解放軍若能夠將其心理作戰、抑或三戰組織賦予堅強之網路能力，那麼其「三戰」之影響、滲透能力定能獲得一定程度之提升，也方能夠達到其《軍隊政治工作學》中所強調之「奪取政治、心理、宣傳信息之制信息權」。[159]以上為解放軍三戰工作信息化之「為何」。

在如何方面，解放軍在於針對美軍聯合作戰行動之研究中，特別關注美國前參謀總長聯席會議副主席歐文斯(Bill Owens)所提出之「系統集成」理論。中共認為隨著現代科學技術、特別是信息技術的迅速發展並廣泛運用於軍事領域，現代軍隊從而發展成為眾多武器、裝備系統構成的複雜而龐大之體系，想要駕馭這樣的龐然大物，必需使各種武器裝備「一體化」。[160]簡言之，系統集成就是運用大系統來統合其他次級系統間的相互作用，致使各次級系統能發揮更大之功效，美軍也得以從系統集成論發展出其聯合作戰機制及C4ISR系統。[161]而在系統集成之範疇下，「信息化」之政治工作、或稱三戰，即是將信息化戰爭中的「軟作戰系統」，以信息攻擊為核心，進行「政治性信息對抗」，[162]戰略支援部隊也就是這種「軟殺傷」能力之集成(如圖3-1)。

---

157 同註 155。

158 維基百科，〈各國智慧型手機普及率列表〉，《維基百科》，<https://zh.wikipedia.org/wiki/各國智慧型手機普及率列表>。(瀏覽日期：2020 年 3 月 13 日)

159 同註 140，頁 281。

160 同註 137，頁 196。

161 同註 137，頁 199。

162 同註 140，頁 281。

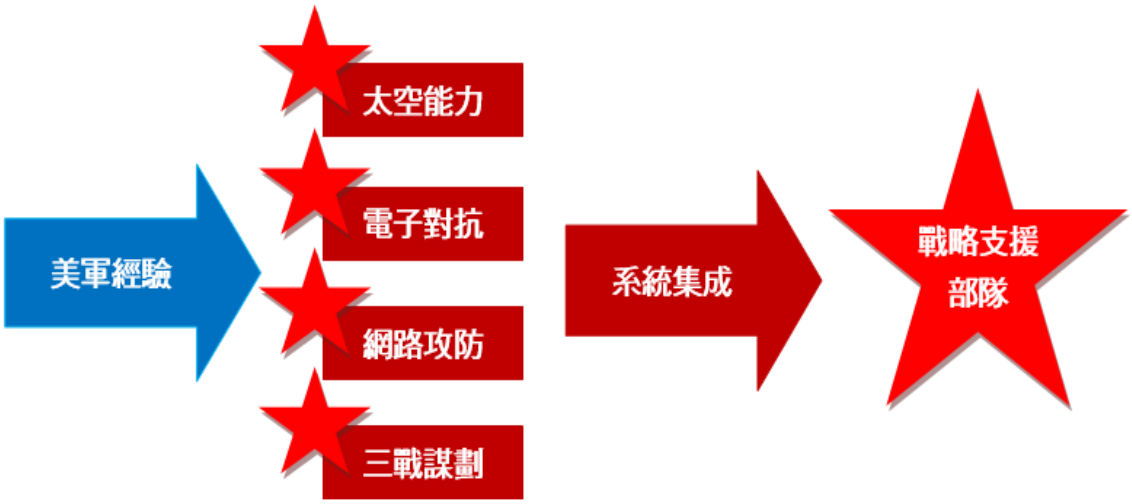

圖 3-1 解放軍戰略支援部隊能力集成示意圖

資料來源：作者自製。

綜合以上探討，可推測中共三戰發展自美軍心理作戰，而中共信息戰學習自美軍資訊作戰，那麼我們也不難依照美軍心理作戰與資訊作戰之關聯性，推演出「三戰是中共信息戰之核心」的結論。另外，中共依照「系統集成」之原則，將各式「軟殺傷」能力整編至解放軍戰略支援部隊內而成為中共之「信息戰部隊」，那麼專司「政治性信息對抗」的「三戰基地」將會是戰略支援部隊之核心無誤。

最後，如若三戰最重要的功能是針對認知域進行「政治性對抗」，那麼足以在信息化條件下的局部戰爭中爭取足夠「資訊優勢」之資訊能力即成為中共在認知域中鬥爭成功之關鍵因素。是故在戰略支援部隊集合了「太空部隊」、「電子戰部隊」、「網軍部隊」及「三戰基地」等軟殺傷能力之集成下，其透過統合並強化太空指管通信、電磁領域、網路能力等實體及資訊域能力，來強化其政治工作、抑或三戰工作在認知域中鬥爭之效能。是故，在下兩個節次將透過探討目前已知之戰略支援部隊組織架構，幫助我們更加瞭解解放軍將如何描繪出其資訊作戰藍圖。

第二節、戰略支援部隊航天系統部

戰略支援部隊為戰區級部隊，下轄參謀部、政治工作部、紀律檢查委員會、航天系統部、網路系統部等5個副戰區級單位及後勤部、裝備部等2個正軍級單位。其中掌管太空作戰的航天系統部，與掌管信息戰的網路系統部乃是主要的任務執行單位，其餘單位均為行政功能。 在習近平的推動的軍改中，總參謀部、總裝備部、總政治部中的行政功能大多被移編至中央軍委會直屬之聯合參謀部、裝備發展部以及政治工作部中，而原屬的任務與部隊則大量由戰略支援部隊接手，其中航天系統部主要的任務以及部隊是來自原總裝備部的部隊，另外也包含數個總參謀部中負責太空C4ISR任務的單位；而網路系統部則接收了總參謀部第三處及第四處負責技術偵蒐及攻擊性的網路作戰行動的人員及任務，此外，也接收了原屬總政治部的單位，也就是號稱為三戰基地的三一一基地(如圖3-2)。[163]以下首先針對戰略支援部隊航天系統部進行解析。

[163] Adam Ni, Bates Gill, op.cit., p. 14-17.

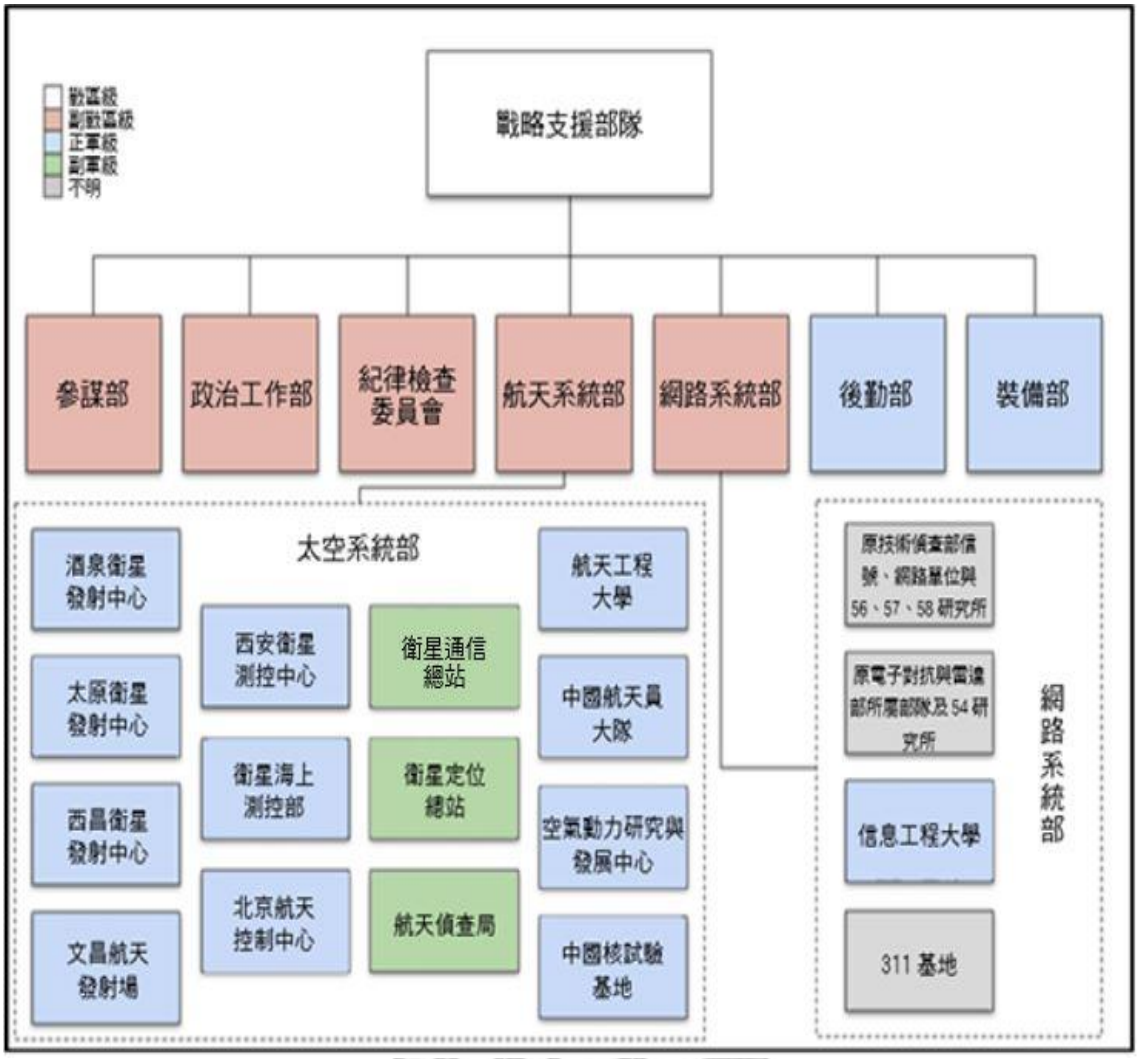

圖3-2 戰略支援部隊組織架構圖

資料來源: Adam Ni, Bates Gill, “The People’s Liberation Army Strategic Support Force: Update 2019,” *China Brief*, Vol. 19, No. 10, May 29, 2019, p. 12.

壹、航天系統部之組織

首先論及航天系統部，航天系統部接受了大部分原屬總裝備部以及分散於解放軍內各處之太空能力相關單位，有效整合成為一支新的太空部隊，下轄單位可區分為負責太空發射任務的酒泉、太原、西昌等三個衛星發射中心及文昌航天發射場，

負責太空遙測追蹤與控制的西安衛星測控中心、衛星海上測控部、北京航天控制中心，負責太空C4ISR任務的衛星通信總站、衛星定位總站及航天偵查局，負責研究發展與支援任務的航天工程大學、中國航天員大隊、空氣動力研究與發展中心、中國核試驗基地等單位，以下列述之。[164]

一、太空發射設施：[165]

(一) 酒泉衛星發射中心：第二十試驗訓練基地，部隊番號：63600，正軍級。

(二) 太原衛星發射中心：第二十五試驗訓練基地，部隊番號：63710，正軍級。

(三) 西昌衛星發射中心：第二十七試驗訓練基地，部隊番號：63790，正軍級。

(四) 文昌航天發射場：所屬基地以及部隊番號尚未明朗，正軍級。

二、遙測、追蹤與控制：[166]

(一) 西安衛星測控中心：第二十六試驗訓練基地，部隊番號：63750，正軍級。

(二) 中國衛星海上測控部：第二十三試驗訓練基地，部隊番號：63680，正軍級。

(三) 北京航天控制中心：所屬基地及部隊番號尚未明朗，正軍級。

三、天基通訊與情、監、偵：[167]

(一) 衛星通信總站：部隊番號：61096，副軍級。

(二) 衛星定位總站：第三十五基地，部隊番號：尚未明朗，副軍級。

(三) 航天偵查局：部隊番號：61646，副軍級。

---

164 Adam Ni, Bates Gill, op.cit., p. 15.

165 Ibid., p. 13.

166 Ibid., p. 14.

167 Ibid., p. 15.

四、研發與支援：[168]

(一) 航天工程大學：解放軍針對航天指揮、管理與航天工程之主要教育訓練機構。

(二) 中國航天員大隊：管理中共太空人部隊之專責單位。

(三) 北京追蹤與通信技術研究所：天基資訊、通信、導航及控制技術之研發單位。

(四) 空氣動力研究與發展中心：中共最大的空氣動力學研究機構，第二十九試驗與訓練基地，部隊番號：63820。

(五) 中國核試驗訓練基地：負責核能科學與科技，輻射、雷射科技與定向能源武器研發。[169]

貳、航天系統部之職能及任務

中共於2015年發表之〈中國的軍事戰略〉一文中指出，太空領域是國際戰略競爭的制高點，太空已經開始「武器化」，此外也強調了其和平利用太空，反對太空武器化和太空軍備競賽之一貫主張，[170]直至2019年發表之〈新時代的中國國防〉白皮書中均抱持同一論述，[171]中共在其對外發布之官方文件中，不斷強調其「防禦」性質之國防武力，然而在《解放軍報》一篇針對美國太空軍的報導中，卻將與戰略支援部隊航天系統部擁有「航天發射」、「航天測量」、「跟蹤管理」、「航天監視作戰」

---

168 Adam Ni, Bates Gill, op.cit., p. 15.

169 定向能源武器(direct energy weapon, DEW)，聚合高功率之能量束進行攻擊之遠距離武器，區分高能雷射、強力微波、粒子束等三種類。詳見：<https://www.mjib.gov.tw/FileUploads/eBooks/d15121fc09b342d682d71d3054e7cd3b/Section_file/22c9b59f61184a2fbe1bbc4bd7421abb.pdf>。(瀏覽日期：2020 年 3 月 12 日)

170 中華人民共和國國防部，〈中國的軍事戰略〉，《中華人民共和國國防白皮書》，2015 年 5 月 26 日，頁 5。< http://www.mod.gov.cn/big5/regulatory/2015-05/26/content_4617812_5.htm >。(瀏覽日期:2019 年 8 月 12 日)

171 同註 126，頁 3。

和「軍事航天員」等五項相同軍事職能之太空軍，描述為「憑優勢謀求霸權」的野心工具，已難自圓其和平利用太空之說法。[172]

除了上述5項航天系統部所擁有之軍事職能之外，由解放軍出版之《戰略學》一書中，則將解放軍航天能力之建構方向訂出四大目標，分別為「航天資訊支援能力」、「航天控制能力」、「航天攻防能力」以及「航天軍事活動保障能力」等4項能力，航天資訊支援即是著眼於以太空為基礎之通信能力；航天控制能力係指航天領域內之主宰能力；航天攻防能力指涉彈道飛彈攻擊及反制彈道飛彈之能力；航天軍事活動保障能力則廣泛的包含了航天裝置、載具之回收、維護、指揮控制等工作項目。[173]

另外，在另一本著作《空間作戰學教程》中，將其太空任務區分為，進入航天、利用航天、及控制航天等三個面向，以下分就其內容概述之。[174]

一、 進入航天

區分為「航天發射」、「航天操控」、「航天器在軌服務及回收」等三個部分。航天發射除基礎發射能力之具備外，亦需要具備在作戰時期迅速發射航天設備以補充戰損之能力；航天操控則是牽涉了航天器進入軌道後的正常運作及功能發揮，包括了軌道調整、數據分析、任務資料輸入等能力；而航天器在軌服務及回收，則是指涉後勤支援服務，包括了軌道運行中添加燃料、航天器之回收等工作，對於中共航天兵力運作有一定程度之貢獻。

二、 利用航天

在航天領域的利用方面，則牽涉到太空C4ISR的能力建構與使用，概分為「偵蒐監視」、「導彈預警」、「通信中繼」、「導航定位」、「氣象觀測」以及

---

[172] 方瀟澎，〈太空軍到底是個什麼軍?〉，《解放軍報》，2020 年 2 月 3 日，<http://www.mod.gov.cn/education/2020-02/03/content_4859465.htm>。(瀏覽日期:2020 年 3 月 2 日)

[173] 肖天亮，《戰略學》（北京：國防大學出版社，2017 年修訂版），頁 33-88。

[174] 姜連舉，《空間作戰學教程》（北京：軍事科學出版社，2013 年），頁 63-67。

「大地測繪」等任務。透過地形地貌、天文氣候、海洋資料、敵軍動態等資料之獲取，與「天基」通信指管鏈路之確保，來協助解放軍先期掌握敵軍動態、發揮武器最佳效能，並從而獲取相對之戰場優勢，提升解放軍「打贏信息化條件下的局部戰爭」之能力。

三、控制航天

所謂控制航天，所指涉乃是「進攻」、「防禦」以及「封鎖」之能力。所謂航天進攻即是使用衛星武器或電子戰等軟、硬性軍事能力對敵人之軍隊或航天設施造成損害，降低敵人航天或戰鬥能力；而航天防禦則是相對於航天進攻，對於敵人可能運用航天能力對解放軍部隊或航天設備造成損害之手段加以防禦或進而反制；而航天封鎖則係指涉運用攻擊型武器在航天領域與地面之間構築屏障，防止敵對方之航天裝備、載具進入航天領域運作。

參、中共成立「天軍」之意義

在中共所定義之信息化戰爭中，戰場空間分層為陸、海、空、天、電等5層次領域密切結合，[175]傳統之陸、海、空暫且不談，「天」及「電」兩個作戰領域即是「航天領域」及「電磁領域」。在2015年5月26日《中國的軍事戰略》白皮書發表記者會上，中共國防部發言人對於環球時報記者所提問：「中國是否將成立一支天軍」之答覆中，只含糊其辭表示「中國政府一貫主張和平利用太空，反對太空武器化和太空軍備競賽」，[176]然而，半年後中共戰略支援部隊成軍，而「天軍」即包含在其中。

中共國防部於2015年發布之《中國的軍事戰略》白皮書中表示中共將「密切跟

[175] 同註 137，頁 202。

[176] 婁楊宣、黃子娟，〈國防部：中國空軍將向空天一體化發展〉，《人民網》，2015 年 5 月 26 日，<http://military.people.com.cn/n/2015/0526/c1011-27058165.html>。(瀏覽日期:2020 年 3 月 16 日)

蹤掌握太空態勢，應對太空安全威脅與挑戰，保衛太空資產安全，服務國家經濟建設和社會發展，維護太空安全」。[177]另外，2019年發布之《新時代的中國國防》白皮書中，亦提及「中國積極參與國際太空合作，加快發展相應的技術和力量，統籌管理天基信息資源，跟蹤掌握太空態勢，保衛太空資產安全，提高安全進出、開放利用太空能力」。[178]先後兩份白皮書中，同樣陳述了太空領域對於中共國防安全的重要性，不同之處在於，2019年發布之白皮書中，對於太空領域的運用上，明確整理出「統籌天基信息資源，跟蹤掌握太空態勢」以及「保衛太空資產安全，提高安全進出、開放利用太空」等兩大主軸。

如將上述兩大主軸對應至前段敘述之「航天能力建構四大目標」，「統籌天基信息資源，跟蹤掌握太空態勢」即對應至「航天資訊支援能力」，而相關單位則包括負責遙測、追蹤及控制的西安衛星監控中心、中國衛星海上測控部、北京航天控制中心另外還包括負責天基通訊與情、監、偵之衛星通信總站、衛星定位總站及航天偵查局等單位。「保衛太空資產安全，提高安全進出、開放利用太空」則對應至「航天控制能力」、「航天攻防能力」以及「航天軍事活動保障能力」，相關單位有酒泉衛星發射中心、太原衛星發射中心、西昌衛星發射中心、文昌航天發射場等單位負責航天軍事活動保障，而中國核試驗基地等研發與支援單位則為航天控制及攻防能力的建構做出貢獻。其中，就在戰略支援部隊成軍不滿一年之際，獨步全球之量子科學實驗衛星「墨子號」由酒泉衛星發射中心成功發射升空，也象徵了未來量子通信技術於軍用領域之運用上，中共已領先美國一步，若解放軍未來成功將量子通信運用於軍事上，便能提供解放軍更快速、安全、無法被干擾的通信鏈路，也將能大大的提升了解放軍的聯合作戰效能。[179]

除此之外，解放軍報報導引述美國國防部研究和工程部副部長格里芬(Michael

---

177 同註 170，頁 5。

178 同註 126，頁 3。

179 nippon.com 編輯部，〈中國最尖端的「墨子」號量子通信衛星〉，《nippon.com》，2019 年 9 月 4 日，<https://www.nippon.com/hk/japan-topics/c06501/?pnum=1>。(瀏覽日期:2020 年 2 月 26 日)

Griffin)向媒體之談話內容：「摧毀導彈的最佳時機是導彈發射初期，定向雷射武器具備完成這項任務的能力」，[180]而其中描述之定向雷射武器即是前述「中國核試驗中心」所負責之研發項目，也代表了太空系統部除了試圖透過發展天基的通信及情、監、偵系統外，著力進行太空攻防能力之建構。關於此點，美國軍事情報局(Defense Intelligence Agency)於2019年發表之中共軍力報告書中也表示：「中共正積極發展各式各樣的反太空能力，例如反衛星飛彈或定向能源武器」，[181]「空中骨幹柵格網」，以及「雲計算」、「軟體定義網路」等先進技術，達成空中、地面、海上各類武器平臺、感測器等資訊節點的自主網路聯結和高速寬頻通信，且為聯合作戰指揮提供網路支援之目的，[182]都需要局部之太空優勢才能達成，也可見太空系統部於解放軍乃至於中共之戰略價值及重要性。

第三節、戰略支援部隊網路系統部

中共2015年發布之《中國的軍事戰略》白皮書中指出，網路空間是經濟社會發展新支柱和國家安全新領域，且各國於其間之戰略競爭日趨激烈，網路空間對軍事安全影響逐步上升，所以解放軍應加快網路空間力量建設，保障國家網絡與信息安

---

[180] 謝嘯天，〈上升段導彈獵手：天基雷射武器〉，《解放軍報》，2019 年 4 月 12 日，<http://photo.81.cn/bqtk/2019-04/12/content_9475543.htm>。(瀏覽日期：2020 年 3 月 12 日)

[181] Defense Intelligence Agency, *China Military Power: Modernizing a Force to Fight and Win* (Washington, D.C.: Defense Intelligence Agency, 2019), p. 43.

[182] 宋長江，〈進一步強化資訊主導的作用〉，《解放軍報》，2019 年 7 月 23 日，<http://www.mod.gov.cn/jmsd/2019-07/23/content_4846327.htm>。(瀏覽日期:2019 年 12 月 14 日)；柵格網即為美軍之 Global information grid 於我國國防部頒印之《新編國軍簡明美華軍語辭典》中，譯為「全球資訊網格」，係指橫跨全球相互連接之點對點資訊能力，此資訊能力用於收集、處理、儲存、傳遞、與管理戰鬥人員、政策規畫者及相關支援人員所需資訊，非相關之企業、單位、人員無法連線至此網路。(以上詳見: https://csrc.nist.gov/glossary/term/Global-Information-Grid)；軟體定義網路(software-defined networking)係指以軟體功能取代路由器中之控制平臺，使網路管理者能在不更動硬體的前提下重新規劃網路並控制流量。(以上詳見：https://zh.wikipedia.org/wiki/軟體定義網路)

全，維護國家安全和社會穩定，[183]隨後，戰略支援部隊便在年底成軍。在美國國防大學2018年出版之《Chairman-Xi Remakes the PLA》中將之定位為中國的資訊作戰部隊，[184]目前公布於該專書中，由前總參謀部技術偵查部移編入戰略支援部隊，負責網路間諜與偵查工作之部隊計有第二局(61398部隊)，第四局(61419部隊)，第八局(61786部隊)與第十二局(61486部隊)，另外還有負責提供研究發展及人才培育的第五十六、五十七、五十八研究所。除了情報工作能力之外，在網路與電子戰的部分，則併入了負責戰略性電子戰及電腦網路攻擊的電子對抗與雷達部所屬之電子對抗旅，第五十四研究所與信息工程大學。另外，網路安全基地、洛陽電子裝備試驗中心、以及負責解放軍三戰工作的三一一基地也被併入戰略支援部隊網路系統部之指揮鏈中，[185]以下就網絡系統部所屬各單位職能進行探討。

壹、網路情報單位

一、第二局：該局已知部隊番號為61398，駐地為上海市浦東新區，主要負責美國與加拿大地區之網路情蒐，專司北美地區之政治、軍事、經濟等情報進行蒐集，早於2006年就遭北美資安公司Mandiant所揭露。[186]

二、第四局：該局已知部隊番號為61419，本部設於山東省青島市，因其大量聘用韓語專業人員，被視為負責兩韓情資蒐集之機構。

三、第八局：該局已知番號為61786部隊，專司俄羅斯及中亞地區的電子訊號截聽工作。[187]

---

183 同註 170，頁 5。

184 John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era* (Washington, D.C.: National Defense University Press, 2018), p. 450.

185 Adam Ni, Bates Gill, op.cit., p. 16.

186 宋兆理、劉濯銨，〈中共戰略支援部隊-網路系統部序列介紹〉，《陸軍通資半年刊》，第 131 期，2019 年 4 月，頁 25。

187 孫嘉業，〈習近平通令透露的軍事機密〉，《明報》，2016 年 8 月 25 日，<https://news.mingpao.com/ins/%E6%96%87%E6%91%98/article/20160825/s00022/147209151581

四、 第十二局：該局已知番號為61486部隊，該部隊被美國政府指控為駭客部隊，專司歐洲、日本、美國之政府部門、太空及衛星產業以及國防承包商進行網路攻擊，[188]然而亦有研究指出該單位係負責太空信號情報蒐集與衛星通訊截聽，同時也可能負責地面衛星接收站之控制。[189]

貳、研發及支援單位

一、 第五十四研究所:該研究所隸屬前總參謀部第四部「電子對抗與雷達部」，該部主要負責電子戰、雷達干擾、軍用通信系統以及 C4ISR 系統管理，然而美國在2020年2月10日起訴該研究所四名軍官，指控渠等對美國易速傳真公司資料庫從事駭客活動。[190]然而從該中共採購「激光探測定位系統」之公告文件中表示，該裝具之採購只能由五四研究所來進行，然其採購目的應非文件表面所述之「反監視」、「反狙擊」，而是進行「激光雷達」之採購。[191]因此，從此採購文件可合理研判該研究所為負責電子及雷達對抗等任務無誤。

二、 第五十六研究所：該所為中共最早建立的電腦科學與工程相結合的大型綜合計算技術研究所，位於江蘇省無錫市。該所主要負責高性能電腦系統工程、電腦與通信工程、資訊網路工程、資訊安全、電腦應用程式與資

9/習近平通令透露的軍事機密（文-孫嘉業）>。(瀏覽日期:2020 年 3 月 3 日)

188 Perlroth, Nicole, " 2nd China Army Unit Implicated in Online Spying", *The New York Times*, June 10, 2014,<https://www.nytimes.com/2014/06/10/technology/private-report-further-details-chinese-cyberattacks.html>. (Accessed:3/3/2019).

189 John Costello, Joe McReynolds, op. cit., pp. 494-495.

190 林穎佑，〈從美國起訴中國網軍看戰略支援部隊〉，《Yahoo 論壇》，2020 年 2 月 28 日，<https://www.ccu.edu.tw/new_content_demo.php?type=newspaper&id=21621>。(瀏覽日期:2020 年 3 月 3 日)

191 北京國泰建中管理諮詢有限公司，〈鐳射探測定位系統專案單一來源採購公示公告〉，《招標公告》，2016 年 10 月 31 日。<http://www.bjgtjz.com/newsview.asp?nid=11478>。(瀏覽日期:2020 年 3 月 3 日)

訊保密等的研究與開發。[192]號稱「太湖之光」並曾是世界運算速度最快的神威超級電腦即是由該所研製。[193]

三、第五十七研究所：該所四川省成都市，依據其招生訊息所示，該院為戰略支援部隊培養通信與資訊系統、電磁場與微波技術等兩個專業領域之碩、博士人才。近三十年內共培養博士近40位，碩士240餘位。[194]

四、第五十八研究所：該所目前僅被辨識為從前總參謀部技術偵查部移入戰略支援部隊之單位，其餘資訊均未明朗。[195]

五、信息工程大學：該校為基礎軍事院校教育機構，畢業任官為中尉，所培養人才之專長計有資訊工程、通信工程、偵測工程、人工智慧、水聲工程、測繪工程、遙感科學與技術、測繪工程、地理科學、軍事地理資訊工程、導航工程、密碼學、管理科學與工程、保密管理、微電子科學與工程、電子科學與技術、資訊安全、資訊對抗技術、電腦科學與技術、網路工程、網路空間安全、密碼工程、軍事大數據工程、預警探測、電子資訊工程、作戰目標工程、軍事外語類、偵察情報、國際事務與國際關係等29項。[196]

六、網路安全基地：目前僅由中共新聞頁面辨識出該單位屬於戰略支援部隊直屬單位，由新聞內容顯示，該單位於全國級之網路安全競賽中負責出題，顯示其網路安全能力確為翹楚。[197]

---

192 卓博人才網，〈無錫江南計算技術研究所〉，《企業首頁》，2014 年 2 月，<http://big5.jobcn.com/position/company.xhtml?comId=112263432>。(瀏覽日期:2020 年 3 月 3 日)

193 林庭瑤，〈5G 爭霸未落幕…陸超級電腦模擬核爆？老美心驚狠打壓〉，《聯合新聞網》，2019 年 6 月 28 日，<https://udn.com/news/story/7332/3897005>。(瀏覽日期:2020 年 3 月 3 日)

194 FREE 考研研招網，〈中國人民解放軍總參第五十七研究所簡介〉，2016 年 1 月 19 日，<http://school.freekaoyan.com/sc/zc57s/2016/01-19/1453191374448059.shtml>。(瀏覽日期:2020 年 3 月 3 日)

195 John Costello, Joe McReynolds, op. cit., p. 461.

196 中國軍網，〈2019 軍校招生簡章第二十四站：資訊工程大學〉，《中國軍網》，2019 年 6 月 21 日，<http://www.chinamil.com.cn/201311jxjjh/2019-06/21/content_9535184.htm>。(瀏覽日期:2020 年 3 月 3 日)

197 南方電網，〈公司在多項網路安全競賽中斬獲大獎〉，《大雲網》，2018 年 10 月 23 日，<http://www.sgcio.com/yqxxh/itcsg/100351.html>。(瀏覽日期:2020 年 3 月 3 日)

七、洛陽電子裝備試驗中心：目前之資料指出其為「解放軍進行『複雜電磁環境』下進行電子資訊系統測試的國家級基地」，[198]然經《中國軍網》報導解放軍某基地領導曾指出：「我軍的信息作戰部隊發展很快，但始終缺少對手，也缺少對抗訓練需要真實的『複雜電磁環境』，建設一支專業的電子對抗訓練大隊勢在必行」，而該基地在2005年起開始肩負解放軍電子對抗部隊實兵對抗任務。[199]也就是目前解放軍所稱之「電子藍軍」，而電子藍軍在2018年的「淬火·洛陽-2018A演練」影片中，可比對出藍軍人員臂章為戰略支援部隊(如圖3-3)，是故，可推測該中心除進行電子裝備測試任務外，尚轄有電子對抗大隊，負責解放軍全軍之電子對抗演練事宜。另外，從央視新聞的報導也可以顯示，該中心尚負有「保障導彈發射」、「衛星測控」、「保障載人航太」、「深空探測」等測繪任務，而任務執行手段包括「單一大地測量」、「天文測量」、「工程測量」、「精密工業測量」、「衛星導航定位」等多個方式。[200]

198 Adam Ni, Bates Gill, op.cit., p. 17.

199 鄒維榮，〈军报刊文介绍我军信息战尖刀部队：2009 年正式组建〉，《解放軍報》，2017 年 8 月 29 日，< http://www.81.cn/big5/jwgz/2017-08/29/content_7734539.htm>。(瀏覽日期:2020 年 3 月 3 日)

200 王薇，〈中國洛陽電子裝備試驗中心：經天緯地標校中國精度〉，《央視新聞》<http://news.sina.com.cn/o/2016-09-16/doc-ifxvyrit2646084.shtml>。(瀏覽日期:2020 年 3 月 3 日)

	
戰略支援部隊臂章	電子藍軍人員臂章

圖3-3 電子藍軍人員臂章對照圖

資料來源：

一、中國軍網，〈揭秘解放軍“15式”系列臂章胸標〉，2016年4月15日，<http://military.people.com.cn/BIG5/n1/2016/0415/c1011-28279463-5.html>。(瀏覽日期:2019年12月15日)

二、新華社，〈「淬火·洛陽-2018A」演練：電磁空間 紅藍雙方激烈對抗〉，《新華視頻》，2018年5月16日，<http://www.xinhuanet.com/video/2018-05/16/c_129873557.htm>。(瀏覽日期:2019年12月15日)

參、三戰單位

三一一基地：駐地福建省，該基地能獲取之資料極少，最關鍵之資料在於《The Diplomat》雜誌披露中共「高新七號」心理戰飛機之報導，報導內指出，隨著當時隸屬解放軍總政治部的三一一基地在福建成立，中國大陸已為對臺心理戰打下了堅實的基礎。2011年，該基地被指定為所有對台心理戰工作的焦點，包括幫助轉播中國大陸的“海峽之聲”廣播電臺的節目；另外，該基地也配合南京軍區實施攻臺軍演。[201]

以上為戰略支援部隊網路系統部所屬單位之簡介，我們可以從中發現，網路系統部統合了解放軍全軍電子作戰、網路作戰以及三戰等「軟殺傷」手段，未來中共如欲學習俄羅斯侵吞克里米亞(Crimea)般「不戰而屈人之兵」的手段腐蝕臺灣軍民

[201] Aaron Jensen, “China Prepares for Psychological Warfare,” *The Diplomat*, August 14, 2013. <http://mil.cankaoxiaoxi.com/2013/0817/257086.shtml>.(Accessed:18/6/2019)

士氣，瓦解團結向心，那麼戰略支援部隊中之天軍、網軍及電子戰部隊如何與三一一基地協調運作，將成為中共打贏臺海「信息化局部戰爭」之成敗重點。

小結

透過本章探討發現，中共三戰極可能為依循美軍心理作戰發展而來；同理推測，隨著美軍心理作戰與資訊作戰關係愈發緊密，中共亦極可能參考(仿效)美軍資訊作戰之模式組建戰略支援部隊，建構其「軟殺傷」之能力；而「軟殺傷」目的之一，亦可應用於包括「透由政治瓦解、輿論造勢、心理鬥爭、法理鬥爭、宗教影響，而解除對方的思想武裝」，[202]也就是政治工作的作戰功能。在資訊技術、傳播技術高度發達的今天，解放軍發揮政治工作作戰功能的手段也已超越過去，除了傳統的傳單、廣播、報刊雜誌、電視節目等手段外，內容農場、[203]網路水軍、[204]電子媒體、網路直播、社群媒體平台甚至是網軍等新型態工具與手段更可增添其政治工作之靈活應用，傳播手段與能力獲得充分的提升，有效擴展了輿論戰、心理戰、法律戰的涵蓋面，增強了其三戰工作之潛在效能。因此，我們必須思考，在解放軍戰略支援部隊充分整合了太空通信、電子對抗、網路攻防、三戰謀畫能力等資訊化「三戰」新組織架構及能力日漸完備之際，我國勢必成為首當其衝的目標，在此新而無形的安全威脅下，我國應當建立相應之能力與機制謹慎應對之。

---

[202] 同註 140，頁 256-260。

[203] 內容農場係指為取得網路流量，大量發布網路文章及之網站或企業，而其發布之文章內容通常為剽竊、造假而來。(詳見:https://zh.wikipedia.org/wiki/%E5%85%A7%E5%AE%B9%E8%BE%B2%E5%A0%B4)

[204] 網路水軍為大陸地區用語，係指受雇於網路討論串或留言區中留下正、負評之公關公司及其工作人員，意即協助「帶風向」。(詳見: https://www.cmoney.tw/follow/channel/article-9385797)

第四章、國軍聯合作戰體制下資訊作戰能力發展現況

認識了美軍資訊作戰機制與解放軍戰略支援部隊之後，本章將著眼於我國資訊作戰能力之現況之探討，我們將從聯戰機制切入，探討李前總長倡議之「資訊作戰中心」如何透過整合傳統六大中心中之「資訊相關能力」,[205]在演習中進行運作，進而定義出屬於國軍之「資訊相關能力」對國防部參謀本部資通電軍以及國防部心理作戰大隊進行介紹，俾利後續進行美國資訊作戰機制、中共戰略支援部隊以及我國資訊作戰機制之比較。

第一節、我國聯合作戰機制與資訊作戰相關能力

我國聯合作戰機制之核心組織架構，戰時於聯合作戰中心中設有人事、情報、作戰、後勤、通資電以及政治作戰等六大中心所構成，前總長李上將於108年度漢光演習中實驗性新增之「資訊作戰中心」中所納入之「情報」、「網路」、「電子」、「謀略」、「欺敵」、「輿論」、「心理」、「保防」、「特種作戰」以及「戰略溝通」等功能，[206]本文將之稱為國軍之「資訊相關能力」。此等資訊相關能力之建構，或為模仿美軍資訊作戰機制而來；是故，本文將試從我國資訊作戰相關準則中對於資訊作戰之定義進行探討，再針對我國當前聯合作戰機制，試圖將各相關組織之功能與國軍資訊相關能力予以釐清，方能瞭解我國資訊作戰機制如何於聯合作戰框架下運作。

壹、國軍聯合作戰基本組織架構與指揮管制關係

---

[205] 六大中心係指《國軍聯合作戰要綱(第三版草案)》中所訂定之人事、情報、作戰、後勤、通資電以及政戰等六個中心。

[206] 同註 4。

依據我國《國軍聯合作戰要綱(第三版草案)》，我國聯合作戰組織架構，概分為平時的「軍政」、「軍令」、「軍備」三大體系，以及戰時的「聯合作戰中心」與「戰爭支援中心」。平時軍政、軍令、軍備系統分別依照業務屬性向各部會協調戰爭資源之調配，戰時則編成「聯合作戰中心」與「戰爭支援中心」，由聯合作戰中心向戰爭支援中心提出作戰需求，而戰爭支援中心負責聯絡政府各相關部會，統合整體國力，支援作戰任務之需求。[207]聯合作戰中心由「軍令」體系之聯參及政治作戰局轉換編成人事、情報、作戰、後勤、通資電以及政戰中心，然108年度漢光演習於李總長規劃下增加「資訊作戰中心」而成為七大中心之戰時編組。[208]「聯合作戰中心」負責各作戰區、聯合空軍作戰中心、海軍特遣部隊、外島防衛指揮部以及直屬部隊之指揮，而「戰爭支援中心」則是透過靈活運用平時所進行之協調、規劃與整備，掌握國家總體資源，支援軍事作戰任務之達成。[209]綜合以上所述，繪製我國聯合作戰組織架構圖如圖4-1。

[207] 國防部，《國軍聯合作戰要綱(第三版草案)》，國防部，2016 年 5 月 1 日，頁 1-1-2。

[208] 張晏彰，〈【國軍 108 年「精神戰力專案教育」】李總長：仿真戰場演練 務實檢討改進〉，《青年日報》，2019 年 5 月 23 日，<https://www.ydn.com.tw/News/337312?fontSize=S>。(瀏覽日期:2019 年 6 月 30 日)

[209] 同註 207，頁 1-1-3。

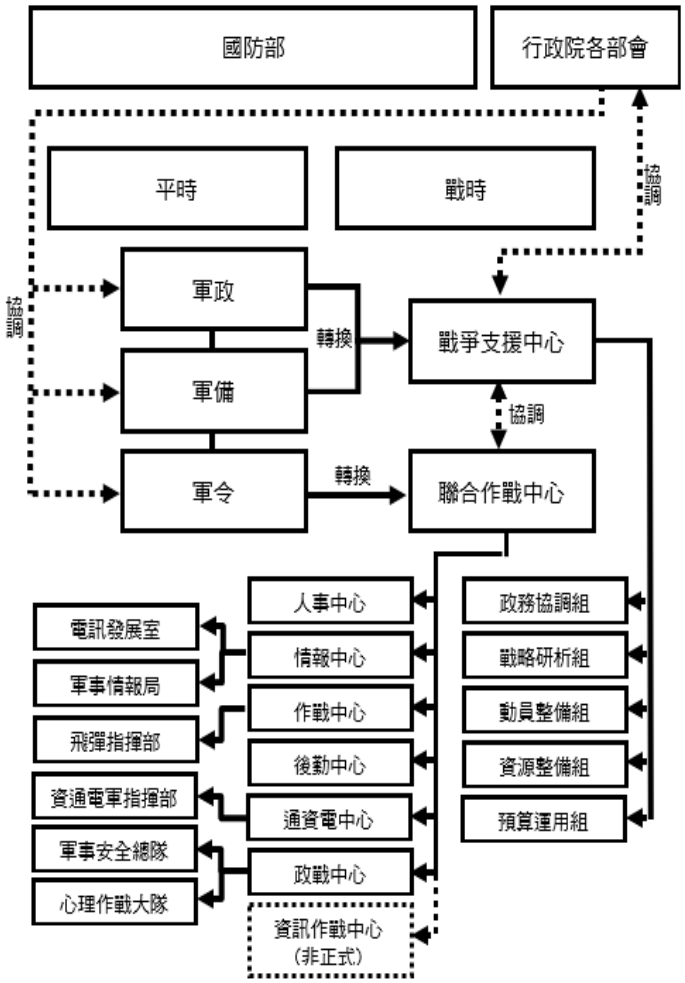

圖 4-1 國軍平、戰時組織架構圖

資料來源：整理自：國防部，《國軍聯合作戰要綱(第三版草案)》，國防部，105 年 5 月 1 日，頁 1-1-2 – 1-1-3。

如圖所示，國防部平時之軍令系統於戰時轉換為聯合作戰中心，聯合作戰中心負責所屬之人事、情報、作戰、後勤、通資電、政戰中心負責各所轄及相關部隊之指揮與管制；而軍政、軍備體系戰時則轉換為戰爭支援中心，負責協調需政府支援事項。另外，從《聯合資電作戰教則(試行本)》中訂定之資電作戰戰時指管流程顯示，我國聯合作戰機制已經有透過通資電中心內部之資電作戰小組整合網路戰、電子戰、心理作戰、軍事欺敵、民事與公共事務等能力，並執行全般資電作為之架構，

[210]是故，資訊作戰中心應非新設，可推斷是將舊有之「資電作戰小組」提昇為「資訊作戰中心」，藉由位階之提昇來增強其整合能力，而其整合方式或為依照美軍聯合作戰資訊作戰小組召集各資訊相關能力及其他軍事能力代表共同研商之方式，來遂行國軍的資訊作戰計畫作為。

貳、聯合作戰中心職能與資訊相關能力

介紹國軍聯合作戰組織架構後，即當著手解析各中心之職能，並與李前總長倡議整合於「資訊作戰中心」中的10項能力相結合，方能對於國軍當前資訊相關能力之建構及運用有更進一步之認識，以下依照各中心職能列述之：

一、人事中心：依據準則中規定，人事中心負責統一制定員額管制、戰場晉任、兵員補充、戰場晉任、軍職派代、軍法、軍紀與獎懲等工作。人事中心無論於美軍資訊作戰機制或是李前總長所整合至資訊作戰中心中之10項能力均未涉及人事中心負責事項。[211]

二、情報中心：情報中心於平時負責情報政策制定與情報整備工作，戰時則為軍事情報工作的「指導」、「蒐集」、「處理」與「運用」，其中包括軍事情報之蒐集、彙整與情報產出，以及反情報與相關計畫之制定，國防部直屬部隊有「軍事情報局」及「電訊發展室」受其節制。[212]另外，欺敵亦屬通資電中心情報支援官兼任。[213]對應美軍之資訊相關能力，則包含「情報」、「軍事欺敵」、「作戰安全(反情報)」等三項。[214]

---

[210] 國防部，《聯合資電作戰教則(試行本)》，國防部，2009 年 9 月 28 日，頁 5-3。

[211] 同註 207，頁 1-2-9 – 1-2-12。

[212] 同前註，頁 1-2-12 – 1-2-15。

[213] 同註 210，頁 5-2。

[214] 美軍作戰安全之定義為「運用系統性的方式來辨識、控制與保護關鍵資訊。其目的有二，一者為識別可能被敵方情報系統所辨識之行動；二為找出可能產生出敵方可能蒐集、分析以及解譯

三、作戰中心：協調並統合運用各單位能力，負責制定行動方案、產製作戰計畫、下達兵力運用與各部隊任務分配、作戰指揮與行動要領、狀況意外時之應變措施、作戰終止及指揮責任移轉等工作。於制定整體作戰計畫之同時，將資通電作戰計畫以及政治作戰計畫以作戰計畫之附件方式呈現之，適時運用電子戰、網路戰及政治作戰及欺敵作戰等作為創造作戰優勢，[215]「特種作戰」之計畫與運用均屬作戰中心負責。

四、後勤中心：後勤工作範圍包括戰時物資需求預判、物資獲得與輸送分配、裝備保修與後送、人員運輸與保健醫療等工作，[216]非關乎資訊相關能力之範疇。

五、通資電中心：以聯合指揮、管制、通信、資訊、情報、監視、偵查系統(C4ISR)為核心，完成通資電戰力整備並支援聯合作戰任務之達成。通資電中心整體負責通信、資訊、電子戰等功能。通資電中心成立資電作戰小組，並由情報、政治作戰部門支援情報官(兼任欺敵計畫官)以及心理戰計畫官等兩個席位，負責通資電中心整體資電作戰行動及修訂作戰計畫之建議。[217]李前總長所述之「網路」與「電子」兩項能力屬於通資電中心所負責。另外，美軍資訊相關能力中，計有「網路作戰」、「資訊確保」、「特殊技術作戰」、「聯合電磁頻譜作戰」等4項屬於該中心之領域屬性範圍。

六、政戰中心：下轄「政戰綜合」、「文宣心戰」、「保防安全」及「新聞傳播」

並產生有用資訊之特定指標」。另外，我國《國軍聯合作戰要綱(第三版草案)》內所述，情報中心之反情報重點在於「隱匿我軍企圖」。詳見 Joint Publication 3-13.3: Operations Security, p. vii. 以及《國軍聯合作戰要綱(第三版草案)》，頁 1-2-13。

[215] 同註 207，頁 1-2-15 － 1-2-17。

[216] 同前註，頁 1-2-17 － 1-2-20。

[217] 同註 210，頁 5-2。

等四個小組，並依令成立「戰時新聞中心」以利新聞傳播工作之遂行。另外，政戰中心亦透過整合「情報」、「作戰」、「通資電」、「戰爭支援中心」功能，成立「戰略溝通」任務編組，負責國軍戰略溝通行動方案之研擬與策劃，「心理作戰大隊」與「軍事安全總隊」均由政戰中心統一指揮運用。[218]在李前總長談話中，「謀略」、「輿論」、「心理」、「保防」以及「戰略溝通」等5項能力均屬政戰中心業管。[219]如若對應美軍資訊相關能力，則包含「戰略溝通」、「公共事務」、「軍民作戰」、「軍事資訊支援作戰(心理作戰)」、「軍事欺敵」、「關鍵領導人交涉」以及「作戰安全」等6項，其中作戰安全(反情報)部分工作牽涉軍事安全總隊之任務，[220]故與情報中心有所重疊。

七、戰爭支援中心：戰爭支援中心下轄政務協調組、戰略研析組、動員整備組、員整備組、預算應用組等5個小組，由軍政、軍備單位轉換編成、負責協調政府各部會，動員總體國力，支援軍事作戰任務之達成。[221]對應於美軍資訊相關能力為「聯合跨部會協調組」。

八、資訊作戰中心：資訊作戰中心之組織與運作機制尚未納入國軍聯合作戰要綱內，相關組織細節以及運作模式未能獲取，只能從新聞媒體之報導中分析之。據報導，在漢光35號演習中首次以資訊作戰中心垂直整合情報等十個功能，反制假想紅軍所

---

[218] 同註 207，頁 1-2-24 － 1-2-27。

[219] 「謀略」係屬政治作戰六大戰之「謀略戰」範疇；「輿論」係指新聞處理、公共事務相關工作；「保防」則為政治作戰局保防安全處及軍事安全總隊所負責；「心理」係指政治作戰局文宣心戰處及其所轄心理作戰大隊負責；「戰略溝通」於國防部亦係由政治作戰局領銜負責。

[220] 軍事安全總隊之任務為「依據國軍保防工作之政策與指導，對足以影響國家、國軍安全或利益之資訊，進行蒐集、研析、處理及運用；並應用保防、調查、檢管等措施，確保國家、國軍安全」，詳見《國軍政治作戰專業部隊(單位)指導與運用教則》，頁 3-1。

[221] 同註 207，頁 1-1-3。

發布之「假新聞」，並由美軍網路作戰司令部(USCYBERCOM)之現役軍官到場，協助驗證國軍對於假新聞之反制能力。[222]

以上為我國聯合作戰機制組織與資訊相關能力之概述，但綜合對比各中心之任務與李前總長談話所述之10項能力以及美軍資訊相關能力可發現，限於國力因素，其中尚缺乏美軍「太空作戰」能力乙項，而其中政戰中心肩負5項我國、6項美軍資訊相關能力為最多(綜整如表4-1)，由此可見，美軍、解放軍以及國軍之資訊作戰，皆是以「認知域」之爭奪作為核心目標，資訊作戰中心之設置，無疑是效法美國聯合作戰資訊作戰機制中召集資訊作戰小組進行能力整合之方式而實施。另外，由於資訊作戰中心尚未納入正式之戰時編制，僅透過演習進行成效驗證，如後續能依照演習中獲致之成果，將資訊作戰中心以及其運作機制進行完善之準則發展，必能對我國平、戰時之友我資訊環境建構作出貢獻。

[222] 同註 3。

表4-1 我國聯合作戰機制與臺、美資訊相關能力關係對照表

	國軍資訊相關能力	美軍資訊相關能力
人事中心	無	無
情報中心	情報、欺敵	情報、作戰安全、軍事欺敵
作戰中心	特種作戰	無
後勤中心	無	無
通資電中心	電子、網路	網路作戰、資訊確保、特殊技術作戰、聯合電磁頻譜作戰
政戰中心	謀略、輿論、心理、保防、戰略溝通	戰略溝通、公共事務、軍民作戰、作戰安全、關鍵領導人交涉、軍事資訊支援作戰
戰爭支援中心	無	聯合跨部會協調組

資料來源：作者自製，參考自：

1、國防部，《國軍聯合作戰要綱(第三版草案)》，國防部，2016年5月1日，頁1-2-9 － 1-2-27。

2、Joint Chiefs of Staff, "*Joint publication 3-13: Information Operations*," November 20, 2014, p. ix.

參、國軍資訊作戰發展與美軍資訊作戰制度之關聯性

透過上述的探討，資訊作戰中心確實與美軍聯合作戰資訊作戰機制中之「資訊作戰小組」相似，也意圖藉由透過國軍內部能力與外部之民力、乃至國家整體之力量之整合，來應對中共之信息戰作為。另外，實際針對我國現行之通資電以及心理作戰準則進行研討後可發現，我國之資訊作戰相關準則都是跟隨美軍之腳步逐步進行發展，相關事例如下。

首先，在通資電方面。2011年修訂之《國軍通資電要綱(草案)》例言中即說明：「本要綱係通盤檢討『國軍通信電子要綱』、『國軍電子戰要綱』以及『國軍資訊戰要綱』等三本要綱，並參考美軍聯合作戰資訊作戰準則JP3-13所編纂而成」[223]，也

[223] 國防部，《國軍通資電要綱(草案)》，國防部，2011 年 1 月 11 日，頁 1。

因為如此，該要綱中針對「資電作戰」之定義為：「係積極或消極的綜合運用電腦網路戰(CNO)、電子戰(EW)、心理戰(PSYOP)、軍事欺敵(MILDEC、作戰安全(OPSEC)及實體攻擊(Physical Attack)等能力，攻擊敵方並防護我方資通電之作戰運用，以有效遂行資電作戰」，[224]而上述要綱內訂定之資電作戰「六大核心能力」，[225]即為美軍1998年版聯合作戰資訊作戰準則中之六大「主要能力(major capabilities)」。[226]從其附錄之中英文對照及專有名詞解釋中，都可比對出，其內容均係源自美軍資訊作戰準則之內容，例如針對公共事務(Public Affairs)的解釋為「公共訊息和社區關係的活動，直接針對國防部各不同單位之公開性事務」，[227]與1998年版之美軍資訊作戰聯合作戰準則中針對公共事務的簡短解釋相符合。[228]

其次，在心理作戰方面，2012年修訂之〈聯合作戰-心理作戰教則(試行本)〉，可為例證之亮點有三。首先，該教則內將聯合作戰心理作戰區分為戰略、戰役、戰術三個層級，而各層次之目的與美軍分層相同，依序為國家利益、聯合作戰目標最後為戰術目標；[229]然而，雖然在層次區分上類似，但在其餘內容方面無太多相似之處。另外，在教則中數次提及心理作戰與資電作戰之整合，「心理作戰是資電作戰核心能力之一」之敘述，[230]內容符合了《國軍通資電要綱(草案)》中對於核心能力之定義；[231]最後，教則內提出「資訊心理戰」之概念，並定義為「運用資訊傳播技術與手段，向目標對象傳達經選定訊息之作戰方式，以影響其感情、動機、推理邏

---

224 同註 223，頁 1-02。

225 同前註，頁 3-02。

226 Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(1998), op.cit., p. I-9.

227 同註 223，頁 附錄 2-01。

228 Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(1998), op.cit., p. GL-10. 原文為：「Those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense. Also called PA.」

229 國防部，《聯合作戰-心理作戰教則(試行本)》，國防部，2012 年 11 月 22 日，頁 1-1。

230 同前註，頁 1-2 – 1-3。

231 同註 223，頁 3-02。

輯、行為與認同，達成心理戰之目標」，[232]內容似與美軍軍事資訊支援作戰(MISO)之定義神似。[233]

經過上述探討，可以歸結出國軍與美軍資訊作戰機制關聯性最深之兩個作戰型態–「資電作戰」以及「心理作戰」與解放軍戰略支援部隊相同，發展重點似為追尋美軍資訊作戰機制之路徑逐步前行，也支持了前述李前總長在演習中所設立之資訊作戰中心為效法美軍資訊作戰制度之假設。

第二節、國防部資通電軍指揮部組織與任務

國防部資通電軍指揮部於2017年7月1日編成，直接隸屬於國防部參謀本部，負責國軍資訊、資安、通信、電子能量之建構，並且具有強化國家關鍵基礎設施防護之能力，厚植全方位網路防禦能力，[234]平時負責國軍資通電系統之維護並協助國家級關鍵基礎設施防禦；戰時確保國軍指、管、通、資、情、監、偵(C4ISR)系統暢通及有效運作，捍衛國家安全。[235]而資通電軍作為我國「重層嚇阻、防衛固守」戰略指導下之第一層防衛兵力。[236]惟限於該單位之機敏屬性，部分資料無法獲取或呈現，僅能以現行通資電準則以及可從公開資料中可推斷之資料架構推斷其組織之概略功能。以下就其緣起、組織架構與職能最後為其聯合作戰中之運用分別論述之。

---

232 同註 223，頁 附錄 1-4。

233 美軍對於軍事資訊支援作戰(MISO)之定義原文為：「MISO are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals in a manner favorable to the originator's objectives.」

234 國防部，〈常見問答集〉，《國防消息》，2020 年 3 月 18 日，<https://www.mnd.gov.tw/PublishTabs.aspx?parentId=10021&NodeId=169013&title=%u570b%u9632%u6d88%u606f&SelectStyle=%u5e38%u898b%u554f%u7b54%u96c6>。(瀏覽日期：2020 年 3 月 18 日)

235 同註 12，頁 61。

236 王炯華，〈重層嚇阻戰略第一層國防部首證實：通資電兵力〉，《蘋果電子報》，2017 年 12 月 4 日，< https://tw.appledaily.com/new/realtime/20171204/1252876/>。(瀏覽日期：2020 年 3 月 23 日)

壹、資通電軍之緣起

資通電軍指揮部係由原屬資電作戰指揮部改制升格而成，而其改制之早於2003年國防部一場以「中共軍備信息化對2010年對臺海安全影響」為題之會議中，即提出「成立資電司令部」之相關討論，且國防部亦認為確有必要改制，惟礙於當時無所屬部隊可支撐此組織調整，故此提案暫遭擱置。[237]其後，民進黨智庫「新境界文教基金會」於2015年5月所提出之《國防政策藍皮書第九號報告：2025年台灣軍事防衛能量》，該藍皮書中認為應「即刻補強國軍資訊作戰能力」，而其中之具體措施即為「在現有的陸、海、空軍軍種外，整合現有國軍資訊、通訊與電子相關之單位與能量，成立獨立的第四軍種」，也據信為資通電軍成立之推手之一。[238]我國政府之所以會愈發重視網路安全，應與中共網軍在全世界之網路竊資及駭客行為已受到全世界之關注有關，2013年美國資安公司Mandiant即揭露中共網軍「61398部隊」在全世界之攻擊行為，並指出其攻擊不僅是為了竊取情報，更為了關鍵基礎設施的「控制權」，[239]也因為如此，才進一步促使當時之政府迫切的要求國軍建立相應的網路安全防護能力，也促成了資通電軍之誕生。

在資通電軍成軍後，許多人都會將資通電軍與解放軍戰略支援部隊進行對比，國防部網頁上亦於常見問答集中提供了「中共戰略支援組織與本軍的異同」之資訊，其內容將解放軍戰略支援部隊描述為肩負「情報偵查」、「網路偵蒐」、「電子監聽」、「衛星情報」「網路攻擊」、「病毒研製」之攻勢性質資訊作戰部隊，而我國之資通電軍則為守勢任務導向。[240]另外，從〈民國106年國防報告書〉也能發現，國防部將資通電軍之任務定位於「平時負責國軍資通電系統之維護並協助國家級關鍵基礎設施防禦；戰時確保國軍指、管、通、資、情、監、偵(C4ISR)系統暢通及有效

---

237 同註 30，頁 201。

238 新境界文教基金會國防政策諮詢小組，〈國防政策藍皮書第九號報告：2025 年台灣軍事防衛能量〉，《新境界文教基金會》，2015 年 5 月，<http://www.dppnff.tw/uploads/20150525205515_6229.pdf>。(瀏覽日期：2020 年 3 月 18 日)

239 David E. Sanger，〈揭秘中國網絡戰部隊〉，《紐約時報中文網》，<https://cn.nytimes.com/china/20130219/c19hack/zh-hant/>，2013 年 2 月 19 日。(瀏覽日期：2020 年 3 月 23 日)

240 同註 234。

運作，捍衛國家安全」[241]，就此定義上也可以看出資通電軍係為應對網路之新型態威脅而組建之相應戰力。

貳、資通電軍之組織架構與職能

資通電軍下轄有「資訊通信聯隊」、「網路戰聯隊」以及「電子作戰中心」等單位，[242]以下分述之。

一、資訊通信聯隊：所屬單位遍布於外、離島地區如金門、東引、馬祖、澎湖，以及本島地區之桃園(龍崗，龍游營區)、台中(新社，中興嶺營區)、高雄(旗山，泰山營區)、花蓮(美崙)等地。[243]由2017年7月9日漢聲廣播電臺臉書專頁有關「資通電軍指揮部資訊通信聯隊資通支援第一大隊成軍」之新聞消息以及其討論串內容顯示，該大隊駐地「龍游營區」原係陸軍73資電群之駐地，[244]由此推知，本島之第六、八、十軍團資電群及金、馬、東、花等地防衛基地指揮部通資作業連均被併入該聯隊中。由原資電群及通資作業連之任務及能力推知，該聯隊及所屬各大隊負責有、無線電通信及資訊系統建立與維護並確保通信系統網路暢通之職能。[245]

---

241 同註 12，頁 61。

242 維基百科，〈國防部參謀本部資通電軍指揮部〉，《維基百科》，2019 年 10 月 28 日，<https://zh.wikipedia.org/wiki/國防部參謀本部資通電軍指揮部>。(瀏覽日期：2020 年 3 月 18 日)

243 屏東縣崁頂鄉公所民政科，〈國軍資訊通信聯隊人才招募〉，《屏東縣崁頂鄉公所網站》，2018 年 5 月 29 日，<https://www.pthg.gov.tw/TownKto/News_Content.aspx?n=FF5357F5BDA5E114&sms=E54FF8470F4AF507&s=34200CCA9980FE00>。(瀏覽日期：2020 年 3 月 18 日)

244 資通支援第一大隊，〈資通支援第一大隊成編〉，《漢聲廣播電臺臉書專頁》，2017 年 7 月 9 日，<https://www.facebook.com/voiceofhan/posts/1782558188426396/>。(瀏覽日期：2020 年 3 月 18 日)

245 靖天電視臺 GoldenTV，〈義勇軍風 2—認識陸軍 74 資電群〉，《靖天電視臺 Youtube 頻道》，2015 年 7 月 15 日，<https://www.youtube.com/watch?v=hJdJTzYrNlI>。(瀏覽日期：2020 年 3 月 18 日)

二、網路戰聯隊：隸屬單位由資電作戰指揮部所屬之網路相關單位推估，區分網路作戰中隊以及網路防護中隊兩個單位，[246]網路戰聯隊主要負責「資訊網路」、「資訊系統」、「衛星」、「電話」外，亦負責「資安健診」、「網路研析」與「技術支援等作業」，[247]為國軍網路戰之骨幹部隊，另肩負有協助國家級國家關鍵資訊基礎設施防護 (Critical Information Infrastructure Protection, CIIP)之重要資訊安全維護任務，[248]在人力資源方面，106年下半年度發放網路戰加給72人次，平均每月僅12人次，共發放新台幣158萬元，意謂可能有12人具備領取網路戰加給之資格。[249]另外，在人員專業程度方面，其專業程度認證依照資通電軍網路戰專業加給區分，由高至低依序為「專家級」、「菁英一級」、「菁英二級」、「專精一級」以及「專精二級」等五個等級，其中尚未有專家級人員，菁英級13%，專精級87%，人才專業度培育方面尚待努力。[250]

三、電子作戰中心：目前已知轄有5個中隊級單位，負責電子戰系統建立以及維護作業、保修補給以及電子戰協調、資料蒐整等任務，

246 同註 210，頁 2-5。

247 國立臺灣師範大學職涯發展中心，〈國防部參謀本部資通電軍指揮部網路戰聯隊簡介〉，《國立台灣師範大學職涯發展中心 Youtube 頻道》，2019 年 1 月 22 日，<https://www.youtube.com/watch?v=TeI1X-_NyYM>。(瀏覽日期：2020 年 3 月 18 日)

248 楊欣燕，〈國防部資通電軍指揮部網路戰聯隊招募〉，《國立嘉義大學官網》，2018 年 9 月 26 日，<http://www1.ncyu.edu.tw/csie/itemize.aspx?itemize_sn=144721>。(瀏覽日期：2020 年 3 月 18 日)；CII(Critical Information Infrastructure)關鍵資訊基礎設施係指支持八大類關鍵基礎設施運作所需之重要資訊系統或監控、調度與數據擷取系統，如資通系統(Information and Communication Technology, ICT)、工業控制系統(Industrial Control Systems, ICS)及資訊系統(Informational Technology, IT)等都在此列。詳見<https://nicst.ey.gov.tw/File/6DE01F9D9F70C0C8?A=C>，頁 2。

249 國防部，〈國防部主管 107 年度單位預算評估報告〉，《立法院網站》，2018 年 2 月 9 日，<https://www.ly.gov.tw/Pages/Detail.aspx?nodeid=5249&pid=166473>。(瀏覽日期：2020 年 3 月 19 日)

250 洪哲政，〈國軍資通電軍尖端網戰人才缺〉，《聯合新聞網》，2019 年 4 月 17 日，<https://udn.com/news/story/10930/3760674 >。(瀏覽日期：2020 年 3 月 19 日)

並同時確保電子戰系統運作正常。實際執行手段則有電子戰偵蒐、測向、定位以及干擾等手段。[251]

目前可蒐集之資通電軍有關資訊如前所述，綜整如圖4-2。先不論資訊通信聯隊以及電子作戰中心，以網路戰聯隊對比美國網際作戰指揮部之任務部隊而言，美軍網路作戰指揮部之任務部隊區分網際國家任務小隊(Cyber National Mission Teams, NMT)，負責國家層級的網路攻防活動；網際作戰任務小隊(Cyber Combat Mission Teams, CMT)，負責軍事有關之網路作戰行動，支援作戰指揮官之目標與任務達成；網際防護小隊(Cyber Protection Teams, CPT)，負責防禦項目為國防部之資訊網路以及依照任務之優先順序給與防護支援；網際支援小隊(Cyber Support Teams , CST)提供網際國家任務小隊與網際作戰任務小隊分析與計畫之支援。[252]相對於美軍網路作戰指揮部之任務組織，資通電軍之網路戰聯隊雖然似乎僅接收原資電作戰指揮部所轄之資訊戰大隊網路作戰以及網路防護等兩個中隊。

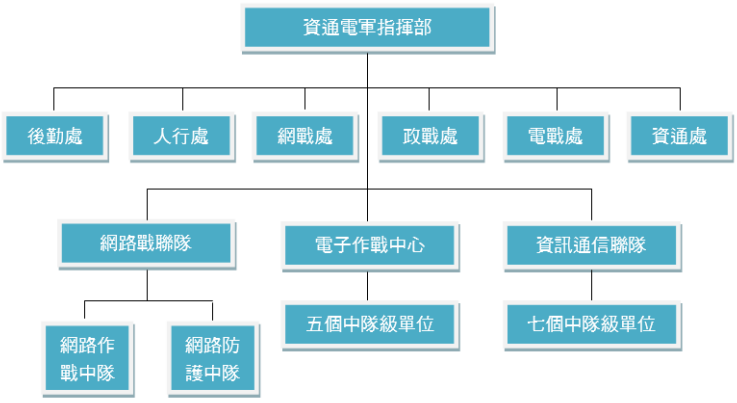

圖 4-2 資通電軍指揮部組織架構圖

資料來源：作者自行繪製。

[251] 國防部，〈資通電軍指揮部的任務〉，《國軍人才招募中心網頁》，2018 年 9 月 7 日，<https://rdrc.mnd.gov.tw/EditPage/?PageID=8c8b7d44-68dc-45f4-9c49-813fce5c4bb9>。(瀏覽日期：2020 年 3 月 18 日)

[252] Cyber Command Public Affairs, “Cyber Mission Force achieves Full Operational Capability,” *United States Cyber Command Website*, May 17, 2018, <https://www.cybercom.mil/Media/News/News-Display/Article/1524492/cyber-mission-force-achieves-full-operational-capability/>.(Accessed : 23/3/2020)

參、聯合作戰中資通電軍之運用

以上探究資通電軍之由來與組織架構後，本文將繼續探究資通電軍指揮部之運用，由於當前尚未能獲取資通電軍指揮部相關之準則，本文將企圖透過〈國防報告書〉等公開資料中，對於資通電軍任務之敘述以及現有準則對於「資電作戰」之運用原則進行歸納，期能瞭解資通電軍將如何於平、戰時為國軍、乃至國家所用。

一、平時之運用：國防部民國106年度國防報告書將資通電軍平時之任務訂為：「維護國軍各式資通電系統及防衛國防資訊網路，支援國家層級網際防禦」，[253]資通電軍人才招募訊息也提到其肩負「協助國家級國家關鍵資訊基礎設施防護之重要資訊安全維護任務」，[254]此外，民國108年頒布之「資安即國安-國家資通安全戰略報告」中也將國防部納入「行政院資通安全會報產業發展組」，並與外交部及國家安全局共同組成「國家資通安全指導小組」，分別負責網際網路防護、駐外使館網路防護、以及網際網路偵蒐。[255]然而，依據行政院資通安全會報組織架構圖所示(如圖4-3)，國防部並未列在關鍵基礎設施安全管理組之相關部會內，[256]而在〈行政院國家資通安全會報設置要點〉中，亦未見國防部於其間之角色，[257]資通電軍是否與資安業管機關確實連結仍待進一步探究。

---

253 同註 12，頁 61。

254 同註 247。

255 國家資通安全辦公室，《資安即國安-國家資通安全戰略報告》(臺北：國家安全會議，2018 年 9 月)，頁 19-42。

256 行政院國家資通安全會報，〈行政院國家資通安全會報組織架構圖〉，《行政院國家資通安全會報網站》，2019 年 2 月 14 日，<https://nicst.ey.gov.tw/Page/1AD9DA2B470FD4C0>。(瀏覽日期：2020 年 3 月 23 日)

257 資通安全處，〈行政院國家資通安全會報設置要點〉，《行政院國家資通安全會報網站》，2019 年 2 月 14 日，<https://nicst.ey.gov.tw/Page/1308C3D16D271378>。(瀏覽日期：2020 年 3 月 23 日)

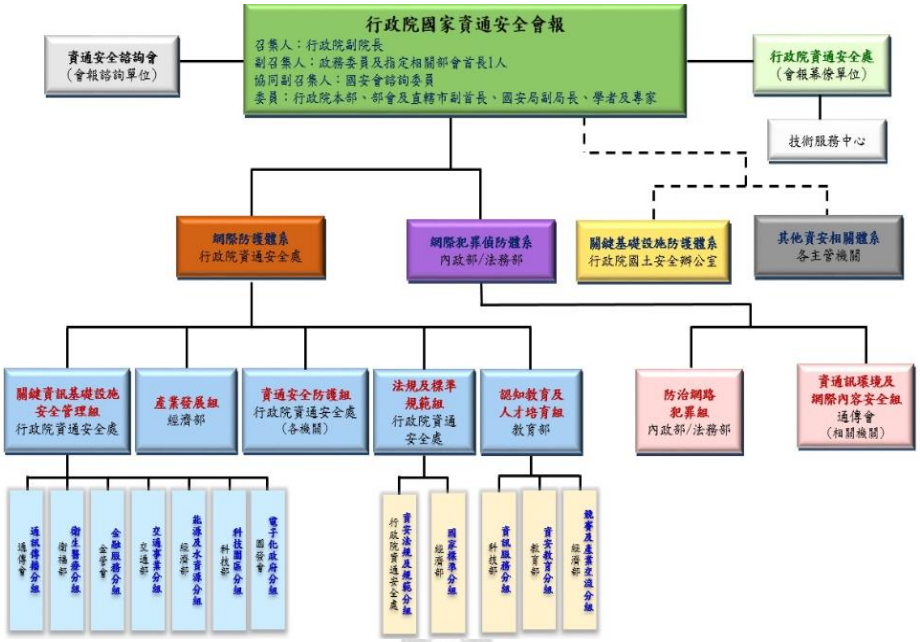

圖 4-3 行政院資通安全會報組織架構圖

資料來源：行政院國家資通安全會報，〈行政院國家資通安全會報組織架構圖〉《行政院國家資通安全會報網站》，2019 年 2 月 14 日，<https://nicst.ey.gov.tw/Page/1AD9DA2B470FD4C0>。

二、戰時之運用：國軍資電作戰戰力之運用依據《聯合資電作戰教則(試行本)》之記述，區分攻勢作為及守勢作為，以下列述之。[258]

(一)攻勢作為：主要運用手法有網路戰、電子戰與實體攻擊、心理戰與軍事欺敵等三項。網路戰旨在應用國軍網路能力，對敵人資訊系統與裝備資訊流的運作進行破壞、阻絕、衰退、擾亂或欺騙等作為；電子戰與實體攻擊係綜合應用電磁與指向性能量等電子戰手段或特戰武力、精準導引武器、高功率微波攻擊武器等實體攻擊手段來削弱或摧毀敵人使用之電戰系統；心理戰與軍事欺敵則是透過系統性的謀劃，將杜撰之情資傳遞給特定對象，使其產生我方所望之行為，導致其在軍事決策上產生誤判或錯置其重點與時機。[259]

[258] 同註 210，頁 3-1 – 3-37。

[259] 同註 210，頁 3-3 – 3-18。

(二)守勢作為：守勢作為方面則在於網路安全防護、電子戰與實體防護以及心理與軍事欺敵之防護等三大面向。網路安全防護重點在於透過各種主、被動防禦作為之運用，增加網路安全防禦縱深，並協調各網路及情、監、偵系統早期獲得敵之動態，並提供聯合作戰中心運用；電子戰及實體防護則是透過採取地形運用、掩體構築、發射管制、部隊警衛等方式確保資電系統之安全，最優先防護之重點為中樞指揮機構以及C4ISR系統；心理與軍事欺敵之防護之重點在於鞏固我國軍民心防，並配合網路戰與欺敵作為釋放虛假訊息，以達到誤導敵人決策之目的。[260]

第三節、國防部心理作戰大隊組織與任務

國防部心理作戰大隊下轄五個心戰中隊及一個戰時編組之第六中隊，受國防部政治作戰局之管制，負責戰略溝通、對敵心理作戰、國軍文宣及政治教育、部隊宣慰等工作。[261]以下將逐一介紹心理作戰大隊之組織架構、運用方式以及相關能力及限制。

壹、國軍邁向資訊心理戰

心理戰為我國政治作戰制度中之一環，政治作戰之特性即為「以人為中心」、「以智慧取勝」、「無時空限制」，[262]心理戰之目標毫無疑問即是對人，而能否策畫出良好、有效之心理戰作為，有賴策畫者之智慧，然而在早期我國試圖對大陸地區

[260] 同前註，頁 3-18 – 3-35。

[261] 國防部，《國軍政治作戰專業部隊(單位)指揮與運用教則》，國防部，2016 年 11 月 15 日，頁 2-1。

[262] 同註 22，頁 1-4。

進行的心戰行為中，僅能侷限於「空飄氣球」或對陸區之「心戰廣播」等模式進行，[263]即是受到疆界之「空間限制」。隨著時空推移至高度資訊化之現代社會中，「資訊化」帶動了全球化，漸漸突破了傳統國家疆界之限制，[264]中共看到了這點，所以在其「資訊邊疆」上構築了「網路長城」，[265]用來防堵境外勢力透過網路空間竊取其國內資料，甚至利用網路之匿名性及自由性來操弄其國內輿論，影響其統治基礎。[266]由此看來，網路長城之目的即是在資訊科技層面上保護中共國內政、經、軍、心，其中「心」的部分即是處於認知域之防禦，亦可說是對於「心理戰」之防禦。

回到國軍資訊心理戰之探討，依據《聯合作戰-心理作戰教則(試行本)》所賦予之定義為：「運用資訊傳播技術與手段，向目標對象傳達經選定訊息之作戰方式，已影響其感情、動機、推理邏輯、行為與認同，達成心理戰之目標」，[267]然而在於準則內，並無明確說明「資訊心理戰」應該如何進行。對此，吳奇英將我國資訊心理戰之執行方式可分為「廣播心戰」、「電視心戰」以及「網路心戰」等三個面向。[268]廣播心戰即是國軍利用無線電電臺製播廣播節目之能力，對大陸地區發送信號，期影響大陸地區軍民之認知與態度；電視心戰主要指涉對於本國軍民之心防鞏固措施，例如莒光日電視教學及軍事發言人室透過媒體舉辦記者會等；而網路心戰則包含電子郵件、網站留言、電信傳真、簡訊發送、網站設置以及網站廣播等6個項目。[269]網路心戰之手段在現階段已然有所變革，隨著資訊技術的應用，無論是社群網站或是即時通訊軟體已成為民眾生活中不可或缺的一部分，其快速、即時傳播資

---

263 許峰源，〈50 年代台海心戰「空飄氣球」瓦解敵方士氣的歷史，您知道嗎?〉，《國立教育廣播電臺》，2018 年 5 月 25 日，<https://www.ner.gov.tw/programExpress/5b0517cb4e091300058748d8>。(瀏覽日期：2020 年 3 月 25 日)

264 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》，第 20 卷第 11 期，2005 年 11 月 1 日，頁 116。

265 同註 126。

266 林穎佑，〈中國近期網路作為探討：從控制到攻擊〉，《臺灣國際研究季刊》，第 12 卷第 3 期，2016 年 9 月 1 日，頁 52。

267 同註 229，頁 附錄 1-4。

268 同註 28，頁 88。

269 同前註，頁 88-89。

訊的效率打破媒體時空界限、無遠弗屆，[270]根據「臺灣傳播調查資料庫」針對台灣民眾2012年至2016年間之媒體使用習慣調查顯示，台灣民眾在科技資訊發達、網路普及化之現況下，利用網路獲取資訊的人口比例逐漸提昇，民眾使用網路瀏覽及蒐集資訊的比例從2014年的24.2%提昇至2016年的78.9%，顯示出網路已成為及作為民眾獲取知識與資訊最普及之管道，[271]影響力不言可喻。若以美國心戰計畫程序中對於可及性(accessibility)的評估上來看的話，[272]在現今的心戰計畫者選定影響受眾所欲使用之媒介(mideum)時必定成為首選。綜上所述，我國心理作戰制度必當朝向「資訊化」發展，擺脫傳統心戰限於「傳單」、「喊話」等戰術性心戰作為之刻板印象。

目前從準則層面檢視，心理作戰大隊除了延續傳統戰術性心戰作為之作業能力外，更擁有執行戰略至戰術層級心理戰之能力，其能力從基本之文宣品製作、多媒體產品製作、戰術性廣播及喊話、乃至戰略層級之情報蒐集、研析以及戰略性廣播、網路心戰訊息傳遞之能力，[273]可見國軍遂行資訊心理戰之能力已逐漸成熟。

貳、心理作戰大隊之組織架構及其能力與限制

認識我國資訊心理戰概念後，接著將繼續介紹我國心理作戰大隊之組織、能力與限制。國防部心理作戰大隊下轄五個心戰中隊以及一個戰編中隊，為我國執行心理作戰任務之專業部隊，更是一支於2014年與美軍第七心戰群簽署合作協議書之

---

[270] 漢聲廣播電臺，〈透過科技整合反制中共心戰〉，《漢聲廣播電臺網站》，2019 年 11 月 28 日，< https://www.voh.com.tw/TW//News/ugC_News_Detail.aspx?NewsCatID=2&NewsID=382>。(瀏覽日期：2020 年 3 月 25 日)

[271] 臺灣傳播調查資料庫，〈台灣民眾媒體使用行為變遷初探-2012 年至 2016 年〉，《TCS 電子報》，2017 年 7 月 17 日，<http://www.crctaiwan.nctu.edu.tw/ResultsShow_detail.asp?RS_ID=67 >。(瀏覽日期：2020 年 3 月 25 日)

[272] Joint Chiefs of Staff, "*Joint Publications 3-53: Psychological Operations*," op.cit., p. VI-6.

[273] 同註 261，頁 2-1 – 2-2。

部隊，協議書訂定平時雙方交流互訪，戰時則視需求相互支援，[274]以下就其組織架構進行解析。

一、心戰一中隊：下轄三個分隊，均具有多媒體產品製作及網路傳散能力，負責網路心理戰及反敵心戰任務之遂行，另負責作戰區內政戰兵要之調查，應急作戰生效後依令協同資通電軍部隊遂行國軍心戰文宣及資電心戰作為，於防衛作戰期間協同資通電軍電子戰以及網路戰單位遂行資電心戰任務。限制因素為「欠缺對敵以電子戰干擾及破壞時之防護能力」。[275]

二、心戰二中隊：下轄三個分隊，負責國內、國際及中共敵情蒐研工作，每日透過網路媒體、電視媒體、報刊雜誌、學術著作及外國軍事報導等媒平臺蒐集敵情，並進行分析研判，提供高層決策正確且即時之參考資料，除此之外亦具有多媒體影像製作之能力。限制因素為「欠缺對敵電磁脈衝攻擊之防護能力，固定陣地與設施、裝備容易使資訊設備及訊號接收能力遭敵軍干擾、破壞」。[276]該中隊另建構有大數據輿情(民情)蒐研系統，用於掌握中共內部政情發展及內部矛盾，並提供我軍心戰計畫者運用。[277]

三、心戰三中隊：下轄三個戰術心戰分隊，配屬各作戰區執行戰術性心戰作為，具備文宣品印製、戰場喊話及播音之能力。限制因素為「欠缺對敵電磁脈衝攻擊之防護能力」。[278]

四、心戰四中隊：前身為漢聲廣播電臺，於民國103年11月1日併入心戰大隊

---

[274] 羅添斌，〈國軍心戰大隊本月赴美深度參訪〉，《自由時報》，2016 年 3 月 2 日，<https://news.ltn.com.tw/news/politics/paper/963567>。(瀏覽日期：2020 年 3 月 24 日)

[275] 同註 261，頁 2-6。

[276] 同前註，頁 2-10。

[277] 黃德潔，〈網路輿情蒐研系統 掌握大陸民情〉，《青年日報網站》，2017 年 9 月 21 日，<https://www.ydn.com.tw/News/256133>。(瀏覽日期:2020 年 3 月 20 日)

[278] 同註 261，頁 2-14。

成為第四中隊，[279]下轄四個分隊以及十五個轉播中繼臺，可透過國內網、大陸網及網路等三種系統平臺進行24小時節目製播。限制為「廣播站臺地點固定，容易受敵攻擊」。[280]

五、心戰五中隊：下轄四個分隊，不分平、戰時執行國軍文宣政教節目製播、戲劇策畫編審、美術設計、軍中音樂推廣及部隊巡演工作，藉以激勵官兵士氣，支援軍事作戰。[281]

六、心戰六中隊：下轄七個戰術心戰分隊，其中六個分隊之能力及限制與心戰三中隊相同，配屬至各作戰區負責戰術心戰任務之執行，另有一資訊心戰分隊，具備資訊心戰傳輸及網路攻防能力，可執行心戰訊息、心戰網頁傳散、置換及網路攻防等任務。[282]

綜整前述心理作戰大隊之組織如圖4-4，未列於圖中者尚有心戰作業車、心戰喊話車以及機動廣播車等戰術心戰裝備，惟心理作戰大隊之「網路」能力如何判定(如：資通電軍採取證照分級)，尚未能獲得相關資訊，僅能從準則內賦予之任務判定其具備一定程度之網路能力。

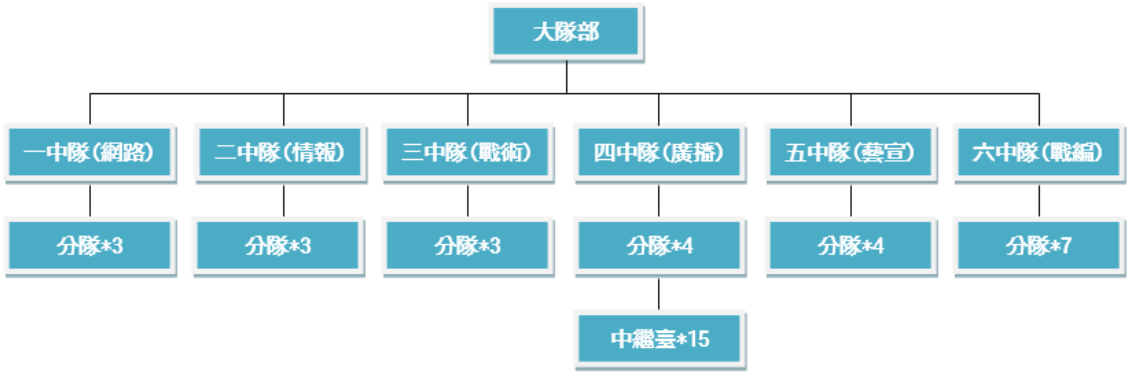

圖 4-4 國防部心理作戰大隊組織架構圖

資料來源：作者重繪自：國防部，《國軍政治作戰專業部隊(單位)指揮與運用教則》，國防部，2016 年 11 月 15 日，頁 2-1－2-31。

---

279 漢聲廣播電臺，〈五心匯聚鍛鑄心戰戰力〉，《青年日報網站》，2016 年 2 月 1 日，<https://www.ydn.com.tw/News/100404>。(瀏覽日期：2020 年 3 月 24 日)

280 同註 261，頁 2-18 – 2-19。

281 同前註，頁 2-24 – 2-25。

282 同前註，頁 2-26。

參、心理作戰大隊與資訊作戰之統合運用

心理作戰已於〈國軍通資電要綱(草案)〉內納為資訊作戰核心能力之一，[283]接著將對比〈聯合作戰－資電作戰教則(試行本)〉與〈聯合作戰－心理作戰教則(試行本)〉之內容，統合出我國現行準則中對於心理作戰大隊於資電作戰之中將如何被應用。

首先，《國軍通資電要綱(草案)》在其訓練想定中，將各種核心能力之運用要點區分為「經常戰備時期戰備整備階段」、「防衛作戰時期應急作戰階段」、「防衛作戰時期全面作戰階段」等三個階段作出區別，以下列述之。

一、經常戰備時期戰備整備階段：

於此階段心理作戰專業部隊應持續針對中共動態之情蒐，研判其對臺心理戰之特、弱點，提出反制之構想，並強化各項戰備整備作為；另外心理戰應配合網路戰及電子戰遂行軍事欺敵之任務，以求影響敵方作出錯誤的決策。[284]

二、防衛作戰時期應急作戰階段：

心理作戰於此階段應運用網路及廣播等宣傳途徑，並配合軍事欺敵作為，於對敵實施心理作戰攻勢之同時，爭取國際輿論支持。[285]

三、防衛作戰時期全面作戰階段：

進入此階段，也就是最後之國土防衛作戰，此時心理作戰大隊配屬至各作戰區之心戰分隊，結合作戰區防衛作戰要點，靈活運用心戰文宣、傳單與心戰喊話等戰術性心戰作為，協助軍事作戰任務之達成。另外，心戰四中隊應結合防衛作戰實況，適時報導有利戰訊，激勵官兵士氣。[286]

---

[283] 同註 223，頁 3-02。

[284] 國防部，《聯合作戰–資電作戰要綱(試行本)》，國防部，2009 年 9 月 28 日，頁 6-3。

[285] 同前註。

[286] 同前註。

至於《聯合作戰－心理作戰教則(試行本)》，中特別以「心理作戰專業部隊與資電作戰部隊指導與運用」之章節，介紹心理作戰與資電作戰部隊之統合運用。首先，準則指出，心理作戰專業部隊與資電作戰部隊之關係為互相支援、協調之平行關係，心理作戰專業部隊完成之心戰訊息可藉由網路戰、電子戰等資電作戰部隊能力傳散，共同協助軍事作戰任務之達成。[287]

另外、心理作戰與資電作戰應於「明訂核心任務」、「集中規劃管理」、「作戰安全管理」以及「整合評估作為」等四項原則性指導下協力運作，以下分述之。

一、明訂核心任務：係指心理作戰與軍事欺敵之成功，將對我方軍事任務產生關鍵性之影響，所以心戰計畫者必須完全瞭解指揮官之決心及意圖，妥慎配合軍事行動規劃心戰作為，方能對聯合作戰產生正面之影響。[288]

二、集中規劃管理：心理作戰與軍事欺敵作業由統一之單位指導管制，有利於整體規劃，確保各方行動目標一致，避免衝突而產生負面影響。[289]此處所謂統一之單位指導管制，應係指《聯合資電作戰教則(試行本)》中之「資電作戰小組」，[290]現或為李前總長所倡議下成立之「資訊作戰中心」。

三、作戰安全管理：心理作戰與軍事欺敵作為應依照敵我作戰能力，目標強弱點分析而決定之，並落實保密作為，以免敵方竊知我軍意圖而遭敵反心理戰及反欺敵戰影響，危害部隊安全。[291]

四、整合評估作為：心理作戰與軍事欺敵作為應結合整體作戰構想，並與軍事作戰計畫一同進行評估，以分析利弊及強化戰果。[292]

---

[287] 國防部，《聯合作戰-心理作戰要綱(試行本)》，國防部，2012 年 11 月 22 日，頁 5-4。

[288] 同前註，頁 5-4。

[289] 同前註。

[290] 同註 210，頁 5-2。

[291] 同註 287，頁 5-5。

[292] 同註 287，頁 5-6。

最後，心理作戰與資電作戰之運用在《聯合作戰−心理作戰要綱(試行本) 》訂有六項共同之任務，以下列述之。[293]

一、運用網路及廣播等能量宣傳我軍之正當性，爭取國際輿論支持。

二、積極宣揚國防政策，落實全民防衛動員。

三、鼓舞軍民士氣，堅定抗敵意志。

四、透過資電作戰媒介執行心理作戰、軍事欺敵等謀略性作為。

五、掌握敵主要指揮者訊息，打擊敵領導威信，弱化敵軍作戰意志。

六、干擾或破壞敵作戰意志。

綜合以上所述，國軍資電作戰與心理作戰在於準則及部分組織之面向上早已有整合之作為，但通資電方面對心理作戰之陳述限縮於「心理作戰結合軍事欺敵」，心理作戰方面提出配合通資電作戰部隊執行資電作戰任務，卻未明確規劃配合與協調之作法。是故，通資電中心資電作戰小組提升為資訊作戰中心之原因應係為了將各能力集合，於聯合作戰之過程中進行更完善之整合及評估規劃，以支持軍事作戰之優勢。

小結

綜合以上之探討可以發現我國聯合作戰資訊作戰之發展，均是依照對於美軍制度之研究得來，從早期之政戰、通資電兩大中心雙軌並行，逐步由通資電中心成立資電作戰小組，整合情報、心理作戰等能力，構成我國資訊作戰之雛形；現在，在李前總長之倡議下，更進一步成立與通資電中心以及政戰中心平行之「資訊作戰中心」，並效法美軍資訊作戰小組會議之模式，整合「情報」、「網路」、「電子」、「謀略」、「欺敵」、「輿論」、「心理」、「保防」、「特種作戰」以及「戰略溝通」等功能，

[293] 同前註。

期能對中共之「假訊息」進行反制，更企圖達成「以彼之道還施彼身」之功效，[294]可謂是在資訊作戰之發展進程上邁進了相當大的一步，然而，除卻聯合作戰之指管體系外，「資通電軍指揮部」以及「心理作戰大隊」等實際進行資訊作戰之部隊，渠等能力能否足堪重任，諸如資通電軍網路戰人力專業證照取得，或者是心理作戰大隊之網路作業人員專業能力是否充足，與資通電軍之合作管道是否暢通等問題，礙於現有準則內容無法呈現以及單位保密措施，在此尚難進行分析對照。

最後，資訊作戰之重要，在於無論平、戰時均在進行，尤以中共而言，更是不分平、戰時均不斷運用其整體國力，遂行其以三戰為核心之信息戰，以求創造政治面上之優勢並引導國內、外之輿論趨勢。[295]國軍在戰時聯合作戰資訊作戰機制以及相應之能力發展完備後，當考慮如何像美軍扣或解放軍一般，於平時將資訊作戰能力應用於國家(戰略)層級之「資訊攻防」上，領頭為我國在資訊環境中獲取部分之優勢，而不要在國家整體資訊安全體系(行政院資通安全會報)中缺席。

294 同註 3。

295 Christopher Paul et al., *Lessons from Others for Future U.S. Army Operations in and Through the Information Environment: Case Studies*(Santa Monica, CA: RAND Corporation, 2018), p.109-110.


國防大學
National Defense University

第五章、中共信息戰威脅下我國發展資訊作戰機制 SWOT 分析

我國當前所面臨最大之安全威脅主要即來自中共，部分軍事研究者運用混合戰爭(Hybrid War)的觀點來形容我國當前所面臨之威脅，[296]然而本文中認為混合性戰爭並不適用於臺海現況。美國蘭德公司認為：「混合性戰爭這個名詞沒有一貫的定義，通常指涉隱密的行動並以傳統武力或核武力支援之，藉以達成對國內政治或外國目標之影響」，[297]而美國國家情報總監(Office of the Director of National Intelligence, ODNI)副主席吉布森中將(Karen H. Gibson)則認為，混合性戰爭是「一種前所未見的能力，此能力是以資訊作為戰爭的要素，並將戰爭的容量、速度、範圍、縱深以及精確度都予以提升，因為全球的資訊科技產業讓人們更加緊密的連結在一起並且能更加自動化且精確地傳遞訊息」，[298]綜合蘭德公司的研究與吉布森中將的說法，我們可以發現，混合性戰爭的運用即是運用資訊的力量來影響目標，並在減少武力使用與武裝衝突的情況下達到目的，所以混合性戰爭中的大部分乃是由資訊作戰構成。然而，其餘資訊作戰無法達成的部分就要由實際武裝部隊來執行，例如在克里米亞的例子中，俄羅斯的各種作為都被歸類為資訊作戰，但惟有最後必要且無法由資訊作戰完成的武力占領，係透過傳統武力之運用來達成，而其過程未發一彈，也看出了資訊作戰對整體混合性戰爭的貢獻程度。是故，本文認為中共當前對我國之「武嚇」，如軍機、軍艦繞臺長航等作為，尚未能稱作「混合戰」，因為如同本文第二章所述，當美軍將航母打擊群調動到北韓外海，也會創造大量資訊，同理可證，共機、共艦繞臺也是意圖對我國軍民、對周邊國家、對歐美各國傳達特定訊息，係屬其「信息戰」抑或是「三戰」之一環。然而，要論及完整之中共信息

---

296 許閔政，〈敵政工部隊(人員)現況及威脅評估報告〉，發表於「第四屆國軍政治作戰戰術戰法」研討會（臺北：國防部政治作戰局等，2019 年 12 月 11 日），頁 27。

297 Andrew Radin, "*Hybrid Warfare in the Baltics*," RAND Corporation Website, Feb 23, 2017 , <https://www.rand.org/pubs/research_reports/RR1577.html>.(Accessed:9/4/2020)

298 Jim Garamone, "*Military Must Be Ready to Confront Hybrid Threats, Intel Official Says*," DoD Website, September 4, 2019, <https://www.defense.gov/Explore/News/Article/Article/1952023/military-must-be-ready-to-confront-hybrid-threats-intelligence-official-says/>.(Accessed:9/4/2020)

戰，其範疇包含甚廣，除了解放軍的太空、通信、電子戰、網路作戰以及三戰能力對於平、戰時之運用之外，其「非常規信息戰」，也就是大家所熟知之「超限戰」，範圍即更廣泛的包含了在政治、經濟、外交等各種範疇上運用中共總體國力進行干擾及破壞，[299]因此，本文在後續分析中將在各內、外因素之分析中，就「實體域」、「資訊域」、「認知域」針對從事資訊作戰(信息戰)之人員(質、量)、科技(軟、硬體研發)、武力(軍力水準及預算)、以及認知層面(抵抗意志、敵我意識，此方向限於內部因素分析)等方向進行分析，並希望藉由如此之分析，得以運用我國資訊作戰之優勢(Strength)開發機會(Opportunity)，並針對弱勢(Weakness)採取保護與改進措施來應對威脅(Threat)，[300]最後依據SWOT分析架構所發展之策略提出建議為我國資訊作戰發展提出建議。以下將依照SWOT分析架構之6個步驟，依序為：描述產業環境、確認影響產業外部之因素、預測與評估未來的外部因素、檢視產業內部的優勢與弱勢、利用SWOT分析架構研擬可行策略、進行策略選擇依序進行之。[301]描述產業環境的部分在本文二至四章已然闡明，本章將就內、外部之因素進行盤點，綜合發展出因應中共解放軍戰略支援部隊威脅之策略。

第一節、外部因素帶來之威脅與機會

外部因素主要即指涉本文主要之探討對象—中共戰略支援部隊。於此節次內，將綜合探討戰略支援部隊之長、短處，而其長處在後續的SWOT分析中即為威脅、而短處即為我國之機會所在。

壹、解放軍戰略支援部隊之優勢

---

299 同註 29，頁 210。

300 Craig S. Fisher and Babette E. Bensoussan 著，陳苑欽等譯，《企業策略與競爭分析：工具與應用》(Strategic and Competitive Analysis)(臺北：台灣培生教育出版股份有限公司，2007 年)，頁 112。

301 同前註。

解放軍戰略支援部隊所擁有之優勢，即成為國軍之「威脅」所在，本文在此總出「科技能力快速成長，研究發展已奏其功」、「軍民融合政策推展，人才培育質量並重」、「中共持續國防投資，網戰預算大幅增加」以及「中共網軍惡名昭彰，征戰各國經驗豐富」等4項，以作為SWOT分析中之「威脅」因素。

一、科技能力快速成長，研究發展已奏其功：解放軍戰略支援部隊所屬教育及研發單位眾多，現已知有第五十四、五十六、五十七、五十八研究所、信息工程大學、網路安全基地、洛陽電子裝備試驗中心等單位。單看第五十四研究所，即具有5,400餘名科技人員以及博、碩士研究生1,800餘員。[302]近年重大研發成果計有曾是世界運算速度最快的神威超級電腦、北斗導航系統、墨子號量子科學衛星等項目。中共成功於2016年底成功於酒泉衛星發射中心發射墨子號量子科學衛星，在量子通信研究上領先全球，[303]而美國國防情報局出版的的2019年中共軍力報告書也說明，中共正積極進行高超音速武器、奈米科技、高效能運算、量子通信、太空系統、人工智慧、機器人系統、高效能渦輪引擎等軍事科技之研發。[304]

二、軍民融合政策推展，人才培育質量並重：在中共大力推動「軍民融合」政策下，解放軍戰略支援部隊開始與中國科技大學、上海交通大學、西安交通大學、北京理工大學、南京大學、哈爾濱工業大學等知名大專院校以及航太科技集團公司、航太科工集團公司、電子科技集團公司等軍工企業簽署「培養新型作戰力量人才戰略合作框架協議」，透過此項框架協議的落實，催生創新團隊進行尖端科技研究，為解放軍培養「新型作戰力量」專業人才。[305]

---

302 百度百科，〈中國電子科技集團公司第五十四研究所〉，《百度百科》，2020 年 4 月 13 日，<https://baike.baidu.com/item/中国电子科技集团公司第五十四研究所>。(瀏覽日期：2020 年 4 月 19 日)

303 同註 179。

304 Defense Intelligence Agency, op. cit., p.49

305 鄒維榮，〈戰略支援部隊與地方 9 單位簽訂人才培養戰略合作框架協議〉，《新華網》，2017 年 7

三、中共持續國防投資，網戰預算大幅增加：兩岸除了國防預算的不對等，在2018年的國防預算為我國國防預算之13倍，且中共之資訊不透明，可能實際之軍事預算遠超過檯面所公布之11070億人民幣之數額。[306]另外，根據美國華盛頓自由燈塔報(The Washington Free Beacon)的報導，戰略支援部隊在成立之初，就大幅增加了網路作戰部門的預算，其增幅高達30%，而其預算的大量增加可能係因從事網路作戰之人員增加所致。[307]如此龐大的預算差距，在未來可能逐步使兩岸在網路作戰之能力上日漸失衡。

四、中共網軍惡名昭彰，征戰各國經驗豐富：在戰略支援部隊成立之前，其總參謀部技術偵查局所屬之網路戰部隊已是惡名昭彰，早於2006年美國資安公司即披露，了一個駭客組織使用937個C&C伺服器(709個位於中國，109個位於美國)，該組織發起的攻擊中有97%源自中國，該團體即為編入戰略支援部隊網路系統部之「61398部隊」，而此部隊只是其眾多網軍中之一支。[308]另外，英國金融時報(Financial Times)報導，每每拿下全球駭客大賽「Pwn2Own」以及「Black Hat」等賽事冠軍的中國駭客在官方的旨意下「缺席」比賽，原因是因為官方要求駭客必須將漏洞先上繳給官方。[309]換句話說，中國駭客參加國際駭客賽事，亦是在幫西方國家找到安全漏洞，而歷年來每每拿下優秀戰績的中國駭客們，也直接的為西方國家的資訊安全作出貢獻。

月 12 日，<http://www.xinhuanet.com/mil/2017-07/12/c_129653088.htm>。(瀏覽日期：2020 年 3 月 16 日)

306 國防部，《國防報告書》(台北：國防部，2019)，頁 31-114。

307 Bill Gertz, “Chinese Military Revamps Cyber Warfare, Intelligence Forces: Changes meant to improve PLA high-tech warfighting,” *The Washington Free Beacon*, January 27, 2016, <https://freebeacon.com/national-security/chinese-military-revamps-cyber-warfare-intelligence-forces/>. (Accessed：15/1/2020)

308 同註 186，頁 23-26。

309 Louise Lucas, “China hackers ordered to report software holes to spy agency,” *Financial Times*, March 28, 2018, <https://www.ft.com/content/eaf7f080-3186-11e8-b5bf-23cb17fd1498>. (Accessed：6/3/2020)

貳、解放軍戰略支援部隊可能之缺陷

解放軍戰略支援部隊所擁有之缺陷，對於國軍而言即為勝機，本文在此總出「人才培訓供不應求，網路安全人才匱乏」、「中共政工素質低落，軍隊政治工作弱化」等2項，以作為SWOT分析中之「機會」因素運用之。

一、人才培訓供不應求，網路安全人才匱乏：騰訊公佈之《騰訊安全2017年度互聯網安全報告》中指出，截至2017年上半年為止，網路安全人才需求量高達70萬人，而且每年需求量將以1.5萬人遞增，[310]雖然中共積極推動軍民融合，並大量培養相關從業人才，短期間內勢必無法填補其人才缺口，而在最終造成軍隊與民間企業爭搶網路安全人才之窘境。另外，戰略支援部隊在2018、2019兩年連續招考文職人員3,760員(2018年招考1037員；[311]2019年招考2723員。[312])，亦凸顯中共解放軍戰略支援部隊內部專業人員缺乏之情形。

二、中共政工素質低落，軍隊政治工作弱化：解放軍領導為雙首長制，政工在部隊中之地位舉足輕重，負責部隊之政治工作及思想工作，近期《解放軍報》中一篇名為「戰時政工集訓助推人才培養」之報導中指出：「所屬政治工作幹部隊伍能力高低不一、素質參差不齊等問題，聚焦備戰打仗這個鮮明導向，本著缺什麼補什麼、戰時需要什麼就考什麼的原則，著眼提升政治工作幹部備戰打仗和崗位履職能力素質」，[313]顯示出中共中央對於解放軍政工幹部素質低落之隱憂。另外，在一篇題為「合成政工群，僅僅負

---

310 騰訊安全，《騰訊安全 2017 年度互聯網安全報告》，騰訊電腦管家網站，2018 年 1 月 17 日，<https://guanjia.qq.com/news/n1/2258.html>。(瀏覽日期：2020 年 2 月 22 日)

311 奇創公考，〈2018 軍隊文職招聘戰略支援部隊職位表下載〉，《奇創公考網站》，2018 年 7 月 11 日，<https://www.xuezi.net/jzg/bkzn/zwb/2018-07-11/1165.html>。(瀏覽日期:2020 年 4 月 18 日)

312 華圖教育，〈戰略支援部隊-2019 軍隊文職招聘職位表〉，《華圖教育網站》，2019 年 3 月 13 日，<https://www.xuezi.net/jzg/bkzn/zwb/2018-07-11/1165.html>。(瀏覽日期:2020 年 4 月 18 日)

313 賴瑜鴻，〈戰時政工集訓助推人才培養〉，《後勤保障新聞》，2018 年 11 月 27 日，<http://hq.81.cn/content/2018-11/27/content_9475512.htm>。(瀏覽日期：2020 年 4 月 19 日)

責政治工作嗎?」的報導中指出：「在演習中負責接替營長、副營長指揮的指導員表示：『原本打算利用合成政工群破解戰時政治工作瓶頸問題，卻因為缺乏戰技、戰術手段，既不能第一時間掌握從旅到營的指揮鏈路上的資訊，各成員之間也不能建立通暢的通信聯絡，合成政工群幾乎成了名存實亡的僵屍群』」，[314]諸如此類的報導顯現出中共政工面臨之人力素質低落與組織弱化之迫切問題，如不解決此等問題，解放軍政治工作以及三戰能力將慢慢地被邊緣化。

參、外部因素之未來可能發展

至於解放軍戰略支援部隊未來可能之發展方面，如預判可能為良好的發展即對我國造成威脅，相對的，如果判斷發展不佳，則可能成為我國未來相對發展之機會，本文在此總出「中共持恆研究發展，打造一流信息勁旅」以及「全力投資信息教育，大量培育專業人才」等2項，分別納入「威脅」與「機會」因素中。

一、中共持恆研究發展，打造一流信息勁旅：在中共中央辦公廳與國務院辦公廳共同發布之《國家信息化發展戰略綱要》中提出「加快資訊強軍，構建現代軍事力量體系」之指導原則，而其中「加強體系化建設」、「提高實戰化訓練水準」、「深化軍事鬥爭準備」之要點均顯示出中共中央堅定把信息化作為軍隊現代化建設之發展方向。[315]未來中共勢必將持續投入人力及經費，造成兩岸除了軍力之不對等之外，在資訊能力上也呈現不對等之狀態。

---

[314] 李兵正，〈“合成政工群”，僅僅負責政治工作嗎？〉，《中國軍網》，2017 年 8 月 14 日，<http://www.81.cn/2017jj90/2017-08/14/content_7720160.htm>。(瀏覽日期：2020 年 1 月 10 日)；文中所指合成政工群係指為執行戰時政治工作所進行的「實驗性」編組，然而依照文中的描述，合成政工群因其政治工作普遍未能與作戰任務相結合，且所展現之「亮點」普遍是為了「搶風頭」，而在最終遭致失敗。而後續的中共媒體報導也未再提及合成政工群。

[315] 中共中央辦公廳、國務院辦公廳，《國家資訊化發展戰略綱要》，2016 年 7 月，頁 13-14。

二、全力投資信息教育，大量培育專業人才：在前述之《國家信息化發展戰略綱要》中針對人才培育也提出了「人才資源是第一資源，人才競爭是最終的競爭。要完善人才培養、選拔、使用、評價、激勵機制，破除壁壘，聚天下英才而用之，為網信事業發展提供有力人才支撐」的論點，[316]顯示中共體認到人才對於其信息化發展之重要性，未來將以「造就一批領軍人才」開始，先培養一批師資人才，接著將這些師資人才投入高等教育體系，達成其「壯大專業人才隊伍」之目的，補足當前之人才缺口。[317]

第二節、內部因素呈現之優勢與弱勢

我國現行準則內所訂定之資訊作戰制度，主要區分「資通電作戰」與「心理作戰」兩大骨幹，以資通電作戰為主、心理作戰為輔，透過兩者的結合來達到各階層之資電(訊)作戰目標。以下試將就個別之優、缺點臚列之，以作為SWOT分析中「優勢」(Strength)以及弱勢(Weakness)之分析因素。

壹、國軍當前資訊作戰制度之優勢

防護能力」、「資訊心戰創新發展，結合科技創造優勢」以及「持恆跨國交流合作，吸收美軍實戰經驗」等3項次，並可作為SWOT分析中之「優勢」因素進行分析，以下分別列述之。

一、聯合作戰資通電作戰

配合國家資安體系，強化網路防護能力：資通電軍網路戰聯隊除了負責「資訊網路」、「資訊系統」、「衛星」、「電話」外，亦負責「資安健診」、

316 同註 315，頁 7。

317 同前註。

「網路研析」與「技術支援等作業」之外，[318]亦肩負有協助國家級國家關鍵資訊基礎設施防護(Critical Information Infrastructure Protection, CIIP)之重要資訊安全維護任務，[319]隸屬單位由資電作戰指揮部所屬之網路相關單位推估，區分網路作戰中隊以及網路防護中隊兩個執行單位。[320]依照「國家資通安全發展方案(106年至109年)」之規劃，目前配合「資安即國安」政策，於行政院資安會報產業發展組中特設「國防需求分組」，意圖透過國防部資訊安全相關需求，帶動我國資訊安全產業整體發展，提高我國資訊安全產業相對於全球市場之技術優勢以及競爭力。[321]

二、聯合作戰心理作戰

(一)資訊心戰創新發展，結合科技創造優勢：國軍從波斯灣戰爭開始，即試圖透過針對美軍在戰場上遂行之心理戰戰術、戰法進行研究，試圖將我國之心理作戰從傳統的傳單、喊話等戰術性心理戰作為，帶往結合新科技之資訊心理戰。[322]而近年隨著資料科學在各領域的應用逐漸普及，國軍也開始探討大數據在心理作戰上的應用，並實際將其運用於中國大陸輿情分析上，[323]這是在中共政工的相關文獻、新聞報導中均未發現之創新應用，也成為我國在心戰議題之掌握上能領先解放軍政工之優勢所在。

(二)持恆跨國交流合作，吸收美軍實戰經驗：解放軍與美軍長期以來亦有軍事交流活動，然而此等交流合作之大前提，仍係美國開始將中共視為對手，因此美軍之意圖多在建立軍事互信機制避免擦槍走火，[324]或者宣揚

---

318 同註 247

319 同註 248。

320 同註 210。

321 行政院資通安全會報，《國家資通安全發展方案(106 年至 109 年)》，2019 年 4 月 11 日，頁 33。

322 同註 28，頁 72。

323 黃德潔，〈網路輿情蒐研系統 掌握大陸民情〉，《青年日報網站》，2017 年 9 月 21 日，<https://www.ydn.com.tw/News/256133>。(瀏覽日期:2020 年 3 月 20 日)

324 蔡明彥，〈美國與中國軍事交流之發展與限制 (二〇〇四～二〇〇七年)〉，《歐美研究》，第 39 卷第 3 期，2009 年 9 月，頁 540。

美軍軍威以嚇阻中共擴張野心等目的，[325]且從美軍在環太平洋演習中限制解放軍不得參加作戰有關訓練，[326]即可看出美中軍事交流仍屬政治性的表面形式，並無軍事層面的實質交流互動。相對於解放軍與美軍之表面互動，我國長期派員至美軍接受心戰軍官班、公共事務軍官班、民事軍官班等相關班隊之訓練，培養專業人才眾多，[327]且在政治作戰局的努力推動下，心理作戰大隊與美軍第七心戰群簽訂合作協議定期交流互訪，[328]透過各種訓練及交流活動，都能有助於我國心理作戰專業人員吸收美軍實戰中獲得之心得及經驗，強化我國心理作戰之理論及實務基礎。另外，我國自2015年起獲邀參加美軍主辦之「國家戰略溝通峰會」[329]及「太平洋戰區資訊作戰會議」[330]等交流活動，也得以參與各國當前對於戰略溝通、資訊作戰等重要課題之尖端研討，避免淪為「筆上談兵」或「閉門造車」之流。

---

325 馬振坤，〈近期中美與外軍舉行聯合軍演情形〉，《ws.mac.gov.tw》，2019 年 9 月，<https://ws.mac.gov.tw/Download.ashx?u=LzAwMS9VcGxvYWQvMjk1L2NrZmlsZS8wMTc4OGVkMC1jYzc0LTRmYzUtYTY2Ni1mNDc4MjQ3YjI3M2UucGRm&n=5LiJ44CB6L%2BR5pyf5Lit576O6IiH5aSW6LuN6IiJ6KGM6IGv5ZCI6LuN5ryU5oOF5b2iLnBkZg%3D%3D>。(瀏覽日期：2020 年 4 月 27 日)

326 荊元宙等，〈政策報告：中共近期與外軍聯合軍演之觀察〉，《亞太和平研究基金》，108 年 7 月，<https://www.faps.org.tw/files/5926/5A3B3344-C7D9-4FBD-8364-0DA59AC5EC0B>。(瀏覽日期：2020 年 4 月 27 日)

327 沈煒比，〈美軍心戰軍官班受訓出國報告〉，《公務出國報告資訊網》，2017 年 11 月 9 日，<https://report.nat.gov.tw/ReportFront/PageSystem/reportFileDownload/C10601338/001>。(瀏覽日期：2020 年 4 月 20 日)

328 同註 274。

329 徐凱琳，〈第九屆國家戰略溝通峰會觀察紀要〉，《公務出國報告資訊網》，2018 年 7 月 20 日，<https://report.nat.gov.tw/ReportFront/ReportDetail/detail?sysId=C10700664>。(瀏覽日期：2020 年 4 月 20 日)

330 傅文成、余宗基，〈Using big data approaches to explore how people evaluated armed forced in disaster relief mission〉，《公務出國報告資訊網》，2016 年 12 月 08 日，<https://report.nat.gov.tw/ReportFront/ReportDetail/detail?sysId=C10700664>。(瀏覽日期：2020 年 4 月 20 日)

貳、國軍當前資訊作戰制度之弱勢

國軍當前資訊作戰制度之弱勢，可概略歸結出「資通電軍人才缺乏，專業培養有待加強」、「資電心戰雙頭馬車，觀念分歧各自為政」以及「準則失修內容陳舊，未能跟上趨勢潮流」等3項，以下分別列述之。

一、資通電軍人才缺乏，專業培養有待加強：依據「國防部主管107年度單位預算評估報告」之內容所示，資通電軍網路戰聯隊於106年下半年度共計發給網路戰加給72人次，平均每月僅12人次，共發放新台幣158萬元，此數據意謂可能僅有12人具備領取網路戰加給之資格，雖然資通電軍於107年度樂觀以320發放人次進行預算編列，仍被立法院視為「過於樂觀」而凍結部分預算，顯示資通電網路戰聯隊內部專業人員不足之問題。[331]另外，在人員專業程度方面，資通電軍以專業程度認證之獲取來配發網路戰專業加給，由高至低依序為「專家級」、「菁英一級」、「菁英二級」、「專精一級」以及「專精二級」等五個等級，其中尚未有專家級人員，菁英級13%，專精級87%，[332]相對於每每拿下全球駭客大賽「Pwn2Own」以及「Black Hat」等賽事冠軍且遭到全球多國資安公司示警的中國駭客，[333]資通電軍在人才專業度培育方面尚待努力。

二、資電心戰雙頭馬車，觀念分歧各自為政：本位主義係指「以己方為中心而不顧整體的利益，或是以偏私的意見強調某方的重要性」，[334]社會上亦不乏國軍內部的各軍種、兵科間充滿了本位主義對立的觀感。[335]對此，中華

---

331 同註 249。

332 同註 250。

333 Louise Lucas, “China hackers ordered to report software holes to spy agency,” *Financial Times*, March 28, 2018, <https://www.ft.com/content/eaf7f080-3186-11e8-b5bf-23cb17fd1498>. (Accessed：6/3/2020)

334 EZ TALK 編輯部，〈本位主義 parochialism〉，經理人月刊網站，2017 年 3 月 1 日，<https://www.managertoday.com.tw/english/vocabulary/view/486>。(瀏覽日期:2020 年 4 月 20 日)

335 余一鳴，〈我國軍種文化差異之研究—以 Hofstede 的文化測量為架構〉，《復興崗學報》，2007 年

人事主管協會資深講師吳昭德也於網路媒體以退伍軍人的身分撰文指出「隨著國防預算的刪減各個部門所獲的資源相對減少，使原本就存在於國軍內部的本位主義更加擴大，各部門皆以鞏固自己部門利益為優先考量，對於整體國軍發展事務則置於後項」。[336]所以，在當前國軍內部之「資訊作戰制度」分由國防部通信電子資訊參謀次長室以及國防部政治作戰局兩大兵監單位間共同操刀之際，難免對於資訊作戰效能造成不良之影響，回顧前述，美軍資訊作戰準則中因為不想使大家誤認為能力間有主從之分，故不斷強調「相關能力」的用詞，想必也是深怕本位主義作祟而影響資訊作戰效能。[337]

三、準則失修內容陳舊，未能跟上趨勢潮流：綜觀本文內引用之國軍準則，2016年修訂者計有《國軍聯合作戰要綱(第三版草案)》、《國軍政治作戰要綱》2冊，其餘分別為2012年修訂之《聯合作戰-心理作戰教則(試行本)》、2011年修訂之《國軍通資電要綱(草案)》以及2009年修訂之《聯合資電作戰教則(試行本)》，經比對發現2011年修訂之《國軍通資電要綱(草案)》係參考美軍1998年之資訊作戰準則內容撰寫，更凸顯國軍準則之編修普遍未受重視。

參、國內之其他因素

綜合以上解放軍戰略支援部隊與我國目前資訊作戰制度之優勢與弱勢之處，以下接續提出數點於我國資訊環境中可能產生影響之因素。

一、中共內容農場侵腦、網路言論難以阻擋：「2019台灣網路報告」中臚列出

12 月 1 日，第 90 期，頁 3。(瀏覽日期：2020 年 4 月 20 日)

336 吳昭德，〈觀點投書：看見這樣的國軍，我很擔憂〉，《風傳媒》，2016 年 7 月 30 日，<https://www.storm.mg/article/147185>。(瀏覽日期：2020 年 4 月 24 日)

337 Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. II-5.

我國前15個流量最多的網站或品牌之代表公司，依序為Yahoo、Google、Msn、Facebook、痞客幫、LINE、聯合新聞網、東森新聞網、自由電子報、旺旺中時所屬媒體、維基百科、三立新聞網、每日頭條(KKNEWS.CC)、中華電信、富邦媒體(MoMo購物台網站)。[338]其中流量第13名的「每日頭條」網站(KKNEWS.CC)以其其他數個網站，在2019年遭臺灣事實查核中心及臉書認定為具有中共背景之內容農場而禁止分享其貼文。[339]雖然事實查核中心已設法降低這些內容農場網站對我國國民的影響，然而流量仍能夠與其他新聞媒體並駕齊驅，可見中共平時信息戰。

二、國民抗敵意志低落、對我國防不抱信心：由美國杜克大學委託我國政治大學選舉研究中心實施之2019年《台灣國家安全調查》報告指出，調查對象在回答「如果臺灣與大陸發生戰爭，請問您會採取什麼行動？」之題項中，等直接或間接參與抵抗之回應僅有23.1%(依序為從軍9.2%、抵抗6.4%、保衛國家0.5%、支持政府的決定6.5%、參加抗議0.1%、後勤補給0.4%)，[340]在此題項之回答中顯示，國人之抗敵意志實屬低落，而其原因有可能是因為在同調查中，「如果大陸攻打過來的話，請問您覺得我們國軍有沒有足夠能力保衛臺灣？」之題項中，高達69.6%的民眾認為國軍沒有足夠的能力保衛國家。[341]綜觀箇中原因，臺灣人心目中素有「好男不當兵」的刻板印象，而2013年的洪仲丘事件更引發民眾普遍對於國軍的不信任感，雖然國軍近年頻以全民國防營區開放參觀活動以及暑期戰鬥營等活動企圖扭轉民眾對於部隊的刻板印象，但從此調查之數據看來，成效明顯不彰。然

---

338 創市際市場研究顧問，〈台灣網路安全報告〉，《財團法人台灣網路資訊中心》，2019 年 12 月 22 日，<https://report.twnic.tw/2019/>。(瀏覽日期：2020 年 4 月 13 日)

339 即時新聞，〈開鍘！臉書打擊假消息 傳中資「內容農場」遭禁止分享〉，《自由時報電子報》，2019 年 10 月 15 日，<https://news.ltn.com.tw/news/politics/breakingnews/2947171>。(瀏覽日期:2020 年 4 月 10 日)

340 政治大學選舉研究中心，《台灣國家安全調查》，Program in Asian Pacific Security Studies，2019 年 1 月 7 日，<http://bit.ly/2HiK5vw>。(瀏覽日期：2020 年 4 月 9 日)

341 同前註。

而相對於中共平時運用駭客攻擊竊資、內容農場及網路水軍擾亂人心，頻繁出動戰機、航艦繞臺威逼，乃至經濟收買、外交壓迫等國家層級信息戰手段，不斷對我國軍民進行威逼、利誘以及示好等等作為對我國資訊環境之實體域以及資訊域產生影響並在最終對於認知域造成衝擊，而使我國國民之抗敵意志愈顯低落。

三、雖有零星資安事件、整體網安狀況良好：而在公部門(含國防部)的電磁資料保護部分，綜觀我國行政院資通安全處自2018年第2季至2019年第4季每季所發布之《資通安全技術報告》，中，將資安事件由輕微至嚴重區分1至4級統計之，我國公部門在期間內均未發生4級資安事件，而3級資安事件發生率每季則為4%至6%不等。[342]行政院資通安全處簡宏偉處長在接受媒體訪問時表示，我國公部門在民國107年平均一個月受到3000萬次攻擊，然而只有262件成功，其中3級資安事件只有6件。[343]反觀中共互聯網信息辦公室所發布之2019年7月《CNCERT互聯網安全威脅報告》顯示，中共單月即有52件政府機構網頁遭惡意置換攻擊，並有116個政府網站遭植入後門程式，另有了 1,809 起涉及政府部門以及銀行、民航等重要資訊系統部門以及電信、傳媒、公共衛生、教育等相關行業的漏洞事件，[344]與我國全年資安情況兩相對照之下，我國當前資安防護情況堪稱良好。

---

342 行政院資通安全處，〈108 年第 4 季資通安全技術報告〉，《資通安全技術報告》，2019 年 1 月，<https://www.nccst.nat.gov.tw/TechnicalReport>。(瀏覽日期：2020 年 4 月 12 日)

343 中央社，〈台美首次網攻演練，資安處：台每月遭攻擊 3,000 萬次〉，《科技新報》，2019 年 11 月 4 日，<https://technews.tw/2019/11/04/taiwan-and-ait-first-network-attack-drill/>。(瀏覽日期：2020 年 4 月 13 日)

344 中華人民共合國互聯網信息辦公室，《CNCERT 互聯網安全威脅報告》，2019 年 9 月 19 日，<http://www.cac.gov.cn/2019-09/19/c_1570421786756209.htm>。(瀏覽日期：2020 年 2 月 20 日)

以上為解放軍戰略支援部隊以及我國資訊作戰之優勢及弱勢所在，彙整各項因素如表5-1，以及以下將藉由表列之各項因素，發展勢當之策略。

表5-1 SWOT因素彙整表

S：優勢	W：弱勢
一、網路整體安全狀況佳(S1) 二、資訊心戰發展領先解放軍(S2) 三、跨國交流合作利於我國人才培養(S3)	一、網軍攻擊能力弱(W1) 二、本位主義合作不佳(W2) 三、準則教範陳舊(W3) 四、資訊作戰缺乏平時作為(W4)
O：機會	T：威脅
一、中共當前面臨網路安全人才缺口(O1) 二、中共當前面臨軍隊政工弱化難題(O2)	一、解放軍科研能力高於我國(T1) 二、中共國防支出多於我國(T2) 三、網軍攻擊能力優(T3) 四、中共透過內容農場、網路水軍等方式持續對我國實施平時之信息戰(T4)

資料來源：作者自製。

第三節、SWOT策略發展與策略選擇

前二節內容中完成了內外因素之篩選後，即可運用SWOT分析架構開始進行策略發展，將優勢、弱勢、機會、威脅在策略發展矩陣內適配後，可以得到最大限度使用優勢與機會的SO(Maxi-Maxi)策略、利用機會克服弱勢之處之WO(Mini-Maxi)策略、運用優勢並迴避威脅的ST(Maxi-Mini)策略以及降低弱勢之處並躲避威脅的WT(Mini-Mini)策略 (如表5-2)。

表5-2 SWOT策略配對表

內部因素 / 外部因素	優勢(Strength)	弱勢(Weakness)
機會(Opportunity)	SO：Maxi-Maxi策略	WO:Mini-Maxi策略
威脅(Threat)	ST：Maxi-Mini策略	WT：Mini-Mini策略

資料來源：Craig S. Fisher and Babette E. Bensoussan著，陳苑欽等譯，《企業策略與競爭分析：工具與應用》(Strategic and Competitive Analysis)(臺北：台灣培生教育出版股份有限公司，2007 年)，頁112。

總體而言 SWOT 分析架構之策略發展，著重於如何以優勢(Strength)開發機會(Opportunity)增強競爭能力，並針對弱勢(Weakness)之處採取保護與改進措施來應對外來之威脅(Threat)。[345]以下將運用表 5-1 之分析因素導入表 5-2 之策略配對，並形成表 5-3 之策略發展表。

表 5-3 SWOT 策略發展表

內部因素 / 外部因素	● 網路安全能力佳(S1) ● 資訊心戰發展領先解放軍(S2) ● 跨國交流合作利於我國人才培養(S3)	● 網軍攻擊能力差(W1) ● 本位主義合作不佳(W2) ● 準則教範陳舊(W3) ● 資訊作戰缺乏平時作為(W4)
● 中共當前面臨網路安全人才缺口(O1) ● 中共當前面臨軍隊政工弱化難題(O2)	一、吸取美軍實戰經驗，發展資訊作戰能力(S2、S3、O2) 二、綜合運用內外資源，培養資訊攻防能力(S1、S3、O1)	一、結合國內優質學府，培養資電專業人才(W1、O1) 二、完善資訊作戰機制、落實準則編修工作(W2、W4、O2)
● 解放軍科研能力高(T1) ● 中共國防支出多(T2) ● 網軍攻擊能力優(T3) ● 中共透過內容農場、網路水軍等方式持續對我國實施平時之信息戰(T4)	一、運用跨國合作機會，發展完善防護能力(S3、T3、T4) 二、開展臺美網戰交流，強化我國網戰人力(S3、T1、T2、T3)	一、善用戰略溝通作為，鞏固國內軍民向心(W4、T3、T4) 二、重視國軍準則編修，鼓勵國防軍事研究(W3、T1)

資料來源：作者自製。

[345] 同註 300。

以上內、外部因素交叉適配後，SO、WO、ST、WT 策略發展策略如下。

壹、S0策略發展

整體而言，SO策略之發展 係利用優勢之處，針對機會所在進行突破，是故我國應強化我國已統整之資通電軍組織並針對當前對岸資安人員缺乏之破口善加利用。另外由於資電心戰發展較中共為佳，且中共政工失能之跡象未見改善，我國認知域爭奪之能力應優於中共，應賡續運用現有組織及人才、甚至擴充之，持續擴大兩岸認知域爭奪能力之差距。綜合以上要點，SO策略發展如下。

一、吸取美軍實戰經驗，發展資訊作戰能力(S2、S3、O2)

美軍為全球少數擁有充足實戰經驗之部隊，其資訊作戰機制經過歷次戰爭之淬鍊，發展已臻完善，我國持續運用雙方交流之機會，吸取其寶貴經驗，並據以發展適合我國之資訊作戰機制，並及早鞏固我國實體域、資訊域及認知域等各面向共同著手，鞏固我國資訊環境，對抗中共從政、軍、經、宗教、文化、輿論等各方面不斷對我國進行之國家層級信息戰。

二、綜合運用內外資源，培養資訊攻防能力(S1、S3、O1)

資訊作戰在平時之執行主要係由網路作戰及資訊心理戰組成，目前我國網路安全態勢良好，國軍應配合政府「資安即國安」政策，向政府爭取資源，通盤發展我國資訊作戰之攻防能力。首先，應綜合運用國內政策資源及美軍交流訓練機會，強化資通電軍網路戰人員教育訓練，輔導取得專業證照以提升其專業能力，其中當然同實包括了網路安全防禦與網電情蒐等攻、防能力。在資訊心理戰方面，我國現今資訊心理戰侷限於對於對岸輿情的大數據情蒐，而如同我國知悉海峽之聲廣播電臺係屬中央軍委政治工作部所轄之對臺統戰工作電臺一般，中共亦深知我國漢聲廣播電臺長期以來試圖對大陸地區民眾傳達民主思想及自由之訊息，必然會從網站禁訪、無線電波覆蓋等方式進行訊息阻隔之行動，我國心理作戰大隊可試圖計畫性運用類似於中共內容農場及網路水軍對我國進行之信息戰行為，運用經營非

官方色彩之微博、微信、推特、QQ等在大陸地區受眾觸及較深、較廣之社群媒體帳號，並配合我國對大陸地區進行之大數據輿情蒐集成果，妥慎設定議題，向大陸地區民眾持續傳達民主自由的可貴。由於資訊戰手段既多且廣，在此舉此例，後續可待其他研究者或實務執行者繼續執行層面之探討。

貳、WO策略發展

在WO策略之發展上，應運用中共解決資安及政工兩方面人才質、量問題之隙，加速審視我國資通電軍網路戰人員之專業程度，以及資通電、心理作戰兩大能力間所存在之本位主義難題，另外也應儘速進行準則研修，以符合實況並將我國資訊作戰機制內通資電及心理作戰如何合作之問題徹底解決。

一、結合國內優質學府，培養資電專業人才(W1、O1)

除了配合政府政策爭取資源以及吸收友邦實戰經驗之外，資通電軍亦應運用國內一流大專院校之教學資源進行人才培育之工作。目前，資通電軍已與交通大學達成策略聯盟協議，攜手培養資安專業人才，應賡續尋求國內資訊相關頂尖學府進行合作交流，並配合政府政策，與資安產業界進行交流合作，以提升人員培訓之質與量，未來期能與更多優秀學府進行產學合作，提升資通電軍人員整體專業能力。

二、完善資訊作戰機制、落實準則編修工作(W2、W4、O2)

我國當前資訊作戰及心理作戰相關官方文件內，對於平時之作為著墨甚少，例如資通電僅在國防報告書中提及「平時負責國軍資通電系統之維護並協助國家級關鍵基礎設施防禦」，而如何協助、如何執行各項作為均未有律定。另外，心理作戰大隊亦除了大數據輿情蒐集及漢聲廣播電臺之廣播節目外，對應中共之信息戰威脅並無積極作為。最後，完整的資訊作戰需要各種能力之相互配合，而擔綱主要角色的資通電軍以及心戰大隊能否擺脫本位主義之拖累至關重要。因此，訂定完善、明確之資訊作戰機制，並將

之詳訂於準則內，以供執行單位作為依循，並透過每年演習驗證準則是否合宜，並逐次修訂之，方能搶在解放軍政工之前站穩腳步，迎戰中共解放軍戰略支援部隊所帶來之信息戰威脅。

參、ST策略發展

對於運用優勢及迴避威脅之策略發展方面，應認識到兩岸最大之鴻溝在於人員數量、以及經費之差距上，面對已將網路戰視為大國間角力之正規力量的中共，我們應避其鋒芒，並運用我國政治作戰之優勢，於資訊環境中開展勝機。

一、運用跨國合作機會，完善資訊防護能力(S3、T3、T4)

我國當前資安防護狀況雖屬良好，然而亦並非零資安事件產生，且中共網軍經驗豐富，駭客足跡遍及世界各地，我國仍應當謹慎應對。另外，資訊防護的另一方面應屬資訊「內容」之防護，主要係指對於中共企圖藉由網路之開放空間，以內容農場、網路水軍等方式危害我國軍民認知域之安全。對此，我國於2019年獲邀參加美國主辦之「大規模網路攻防演練（CODE）—實兵演練活動」，[346]該演練是由美國、日本、澳洲等10數國網軍模擬北韓對我國金融機構關鍵基礎設施發起攻擊，透過此活動我國資安團隊亦從參予國之攻擊中發現資安漏洞並予以修補，透過此類跨國合作活動，可有效提升我國關鍵資訊基礎設施之防禦能力。另外，臉書與我國事實查核中心合作，限制中共背景之內容農場散布資訊，目前成效雖不顯著，然而往後亦可依照此種模式，持續強化我國對於中共假訊息、錯訊息之威脅與影響之防護能力。

二、開展臺美網戰交流，強化我國網戰人力(S3、T1、T2、T3)

我國之弱點之一即為網路戰人員專業不足，雖然目前資安狀況良好，但應係軍網採取實體隔離之資安維護方式所致，我國如欲針對中共當前網路安

346 彭琬馨、李欣芳，〈網攻演習落幕 美盼深化與我合作〉，《自由電子報》，2019 年 11 月 9 日，<https://news.ltn.com.tw/news/life/paper/1330641>。(瀏覽日期：2020 年 4 月 24 日)

全人才短缺之情形獲得優勢，即應運用國軍與美軍常態性交流之優勢，提出網路戰人員訓練需求，藉美軍資源提升我國網路戰人員之專業程度與素質。

肆、WT策略發展：

WT策略的發展上在於體認我們很弱，要作什麼能改變很弱的體質同時也能對應外來的威脅，在此策略發展中主要發展項目針對內容未提及人才培育之弱點原因有二，首先。

一、善用戰略溝通作為，鞏固國內軍民向心(W4、T3、T4)

戰略溝通亦屬於美軍資訊作戰之相關能力之一，戰略溝通聯戰部隊之戰略溝通具有「增進美國的可信度與正當性」、「削弱對手的可信度與正當性」、「使選定之受眾採取特定行為以支持美國或國際目標」、「使競爭對手採取特定行動」等四個基本的戰略溝通目標的角度上來看。[347]國防部應於平時即依美軍資訊作戰機制，並運用此機制協調戰略溝通相關作為，透過良好的議題設定與溝通作為，期望達成「增進政府的可信度與正當性」、「削弱中共的可信度與正當性」、「使國人支持政府方針」、「使中共不敢輕越臺海防線」之目的。

二、重視國軍準則編修，鼓勵國防軍事研究(W3、T1)

美軍之所以強大，除了投入高額國防預算之外，也實事求是地進行準則編修，而其對於國防軍事研究之重視，也反映在某些事件上。如蘭德公司針對阿富汗地區2001至2010年的資訊作戰作為的研究發表後，美國即修訂了聯合作戰資訊作戰準則，而修訂的內容都恰似針對蘭德公司提出之檢討事項進行改進，諸如「資訊作戰與各單位作戰行動缺乏整合」、「過長的反應時間與協調上的拖延」、「資訊作戰與心理作戰之間之介面效能不彰」、「資訊作戰軍官遭到孤立」、「資訊作戰與公共事務之間缺乏協調」等。

---

[347] Joint Chiefs of Staff, "*Strategic Communication Joint Integrating Concept*," op. cit., p. iii.

[348]所以，在我國無法如美國一般投入高額的國防預算與對岸進行軍備競賽之同時，我們更應注重基本面上的軍事理論發展與準則教範編修等工作，才能以最有限之資源發揮最大的國防實力。

小結

孫子兵法有云：「上兵伐謀，其次伐交，其次伐兵，其下攻城」，我國當前面臨之威脅主要來自於中共，雖然中共之「攻城」、「伐兵」、「伐交」上都遠勝於我國，然而在「伐謀」的領域中依靠的則是人智而非軍事武力。所以，國防部除了在軍事武力上建構不對稱之嚇阻戰力外，也應在伐謀之資訊作戰上著力研究，並於平時即應開展資訊作戰作為，而非僅於戰時開展相關作為。另外，中共當前固然有其缺陷之處，然而，其作為一個足以稱為區域霸權之大國，在其經費挹注與政策導向之下，改進這些缺陷只是時間問題，我國如若在研究研發上停滯不前，定不利於我國之長治久安。

[348] Arturo Munoz, op. cit., pp. 119-132.


國防大學
National Defense University

第六章、結論

中華民國自 1949 年政府播遷來臺以來，即不斷面對中共在軍事、外交、經濟等各方面之威脅，2019 年 1 月 2 日中共領導人習近平於《告臺灣同胞書》發表 40 周年紀念會上的提及：「中國人不打中國人。我們願意以最大誠意、盡最大努力爭取和平統一的前景.....我們不承諾放棄使用武力，保留採取一切必要措施的選項」，此發言內充分顯示中共領導人不曾、也不可能放棄武力侵臺之選項，雖然如此，和平統一，不耗費一槍一彈拿下臺灣才是他們的最優先考量。因此，在俄國成功以資訊作戰手段拿下克里米亞後，信息戰更成為了中共對臺攻略的首選利器，進而建立了戰略支援部隊並逐步於資訊環境中入侵我國之「資訊邊疆」。而這也是延續中共前國家主席胡錦濤於 2004 年所提出之「入島」、「入戶」、「入腦」、「入心」對臺戰略方針，在此「入腦」、「入心」之認知域威脅下，中共將循「克里米亞模式」對我國發動資訊作戰攻勢之假設愈發真切。

經過本文之研究可以發現，無論美軍或解放軍所定義之資訊作戰，均不是單指網路能力之發揮與應用，而是廣泛包含了通信、電子、資訊、認知等不同領域軍事能力，針對不同狀況與目的，將各種軍事能力於資訊環境中進行整合與運用，有必要時甚至不惜動用舉國之力進行之。從俄羅斯兼併克里米亞的案例，我們更可以發現掌握認知域的重要性愈發重要，儼然成為了新時代戰略衝突的制高點，然而，我國當前資訊作戰相關機制的能力分散以及缺乏有效的整合，似乎將使我國無法應對中共戰略支援部隊所帶來之信息戰威脅，而李前總長所領銜規劃之「資訊作戰中心」，意圖效法美軍資訊作戰之能力整合，似乎就是解決目前問題之最佳途徑。

本文以新制度主義之歷史研究途徑，試圖探詢美、「中」、臺三方之資訊作戰相關能力及制度發展脈絡，透過發展歷程之探討，發現美軍之資訊作戰發展歷程，確實為中共所關注，並在某種程度上依循美軍資訊作戰發展之歷史脈絡不斷發展至今，而我國雖亦因長期與美軍合作交流，在某種程度上亦跟隨美軍之腳步，然而發

展之腳步稍嫌遲緩，李前總長成立「資訊作戰中心」這一大步，是國軍在發展新型態作戰能力上之一大進展，然而仍有準則及理論發展、人才培育及固有觀念破除等問題待解決。

第一節、研究發現

壹、資訊作戰涵涉認知領域，心理作戰能力不可或缺

美軍對於資訊作戰定義：「在軍事行動中，整合運用資訊相關能力並配合其他作戰行動來影響、干擾、破壞或竄改敵人或潛在敵人的決策，同時也對我方決策進行防護」[349]，這個定義看似十分明確，但是又異常的廣泛，畢竟每個人的生活中，時時刻刻都在做出決策。個人決策上，指揮官下達作戰命令是一種決策，影響這個決策是資訊作戰的目標，從他國的元首的政策決定或民眾的投票意向，都是資訊作戰可以影響之決策；更甚者，現在的人工智慧技術發達，而程式所產生的自動化決策(automated decision-making)也成為了資訊作戰的目標。[350]眾人對於資訊作戰之認識常止於「網路作戰」、「電子作戰」等範疇，多數人忽略了「資訊」這個名詞的廣泛含意。當我們對於資訊環境中的三個領域「實體域」、「資訊域」、「認知域」進行充分理解之後，即可以發現，資訊作戰的的範疇無遠弗屆，可以是電子信號干擾、可以是網路系統癱瘓、也可以是軍力展示與威嚇，更甚者，也可能是每日在社群媒體中隨手可得之圖像、影片、文字等。是故，資訊作戰除了網路作戰與電子作戰之範疇外，亦包含非常大的「心理作戰」成分於其中，這也是美軍從 1998 年的第一版資訊作戰聯戰準則即將「軍事資訊支援作戰」列為其「核心能力」之緣故。

---

[349] Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*(2014), op. cit., p. ix.

[350] Joint Chiefs of Staff, *Joint Publication 1:Doctrine for the Armed Forces of the United States*, op.cit., p. I-19.

貳、資訊環境攸關國家安全，資訊作戰有賴平時經營

俄羅斯於 2014 年佔領克里米亞，其以資訊作戰貫穿全程，最後以軍事占領收尾的混合性戰爭手法，成功在不發生正規軍事衝突及造成傷亡的情形下，擴增了近 27,000 平方公里的國土，並確保了其黑海艦隊之基地賽瓦斯托波爾(Sevastopol)的安全，而俄羅斯總統普丁也公開讚揚俄羅斯軍隊在接管克里米亞的任務中展現了俄羅斯軍隊的「新能力」[351]此次事件使得各國對於資訊作戰的運用上有了更深一層的警覺與認識。以往軍隊強調「戰場環境(operational environment)」中對於武裝衝突的準備與經營，然而在新型態戰爭之威脅下，資訊環境(information environment)中的衝突日益升溫，而資訊作戰之重心也從以往針對作戰環境進行影響的指管戰(command and control warfare, C2W)轉向進行資訊環境內部針對網路安全進行經營與鞏固的網路作戰，隨著媒體、新媒體以及網路的發展，各國發現了認知域中進行影響效益龐大且廉價，故使得資訊作戰的重點又回到了心理作戰、戰略溝通等等針對認知域之影響活動。

在此潮流之下，中共軍改中成立了被美國稱為資訊作戰部隊的「戰略支援部隊」，而其改組之方式即是透過將各種信息戰的教育訓練、研究發展、實兵執行單位等相關能力，以「組織集成」之方式進行整合，透過統一、扁平化的指揮鏈來改善戰術、戰役、戰略層級之信息戰效能，雖然其劍指方向未必朝向我國，但從我國與中共之緊張關係來看，我國實應重視中共戰略支援部隊所帶來之「信息戰」威脅。也因此，國軍除了重視平時的戰場環境經營之外，「資訊環境」之經營應成為國軍當前重要之課題。

---

[351] 新華社，〈普京首次承認俄羅斯軍隊直接參與接管克里米亞〉，《新華網》，2014 年 3 月 28 日，<http://www.xinhuanet.com//world/2014-03/28/c_126329844.htm>。(瀏覽日期：2020 年 4 月 2 日)

參、國軍資訊作戰機制未全，資訊心戰尚待兼容整合

本研究可發現，除了美國之資訊作戰單純以「機制」的建立來進行各資訊相關能力之整合外，中共則是在軍事改革中，並將原本分散各處，執行太空作戰、電子戰、網路作戰、三戰之「組織」統整於解放軍戰略支援部隊的方式來進行資訊相關能力之整合，並同時除去總參謀部，使得指揮鏈中減少一個層級，並使指揮系統扁平化，透過對於中、美兩強之資訊作戰發展進行研究，可以發現如欲進行高效之資訊作戰確有進行能力整合之必要性。

我國現行之「資訊作戰」能力整合在李前總長的擘劃之下已然開展，而其中之主體即為通信電子資訊參謀次長室下轄之「資通電軍」以及政治作戰局所屬之「心理作戰大隊」兩大專業單位擔綱。然而當前制度可能面臨之難題有三，其一為構成通信電子資訊參謀次長室負責之「資電作戰」與政治作戰局負責的「心理作戰」間蒙受本位主義之困擾，有礙齊心完成資訊作戰任務；其二為資通電軍網路作戰專業人力不足，尚難確實發揮網路作戰之能力；其三為我國軍事準則資料過於老舊，尚未架構出明確的運作架構與執行規範，或如美軍資訊作戰準則一般提供資訊作戰執行相關人員統一概念與執行依據，將使國軍之資訊作戰在執行上無所依歸。

第二節、研究建議

壹、重視國軍準則編修工作、研發資訊作戰能力機制

國軍部分準則過於老舊不合時宜，如本文內所引用之《聯合作戰-心理作戰教則(試行本)》、《聯合資電作戰教則(試行本)》以及《國軍通資電要綱(草案)》等準則，且內容多為原則性的綱要說明，缺乏如美軍準則一般具有理論說明及框架描繪甚至執行流程之律定，惟有完善準則的編修以及詳述其中的理論架

構並訂定可行之作業流程，方能使執行者與任務相關人士有所依循，使我國資訊作戰相關部隊能以統一之思維協力達成資訊作戰之目標，塑造有利之資訊環境。建議國防部應令國防大學以及各資訊相關能力業參共同組成資訊作戰理論發展暨準則編修委員會，區分「資訊作戰理論發展」、「資訊作戰準則編訂」、「資訊相關能力準則編修」、「常態性資訊作戰組織與機制建立」等四階段，逐步完善符合我國國防需求之資訊作戰能力，俾使我國資訊作戰臻於完善。

貳、把握內外資源優勢機會，加速資訊作戰人才培育

資訊作戰也是一門需要「科際整合」的專業，除了通信、電子、電腦軟硬體等專業外，也需要傳播、心理、政治、甚至藝術等學科綜合而成。應多方培養資訊作戰相關能力之專業人才，建議人才培養管道如次。

一、基礎人才培育：

我國中正理工學院以及政治作戰學院為國軍資訊作戰相關專業主要之培育院所，應由國防部統一檢討人才培育所需專業，並要求相關院校開設相應之專業課程，例如於政治作戰學院心理研究所及新聞研究所開設心理作戰或資訊作戰之專業課程，以滿足資訊作戰人員培育所需。另外，國防部可與國內優秀大專院校合作，以 ROTC 或文職人員招聘模式爭取優秀畢業生進入資通電軍或心理作戰大隊等相關單位服務，提升資訊作戰相關單位之人力質量。

二、進階人才培育：

在人員進入專業單位服務一段時間取得實務經驗後，可鼓勵人員報考國內外碩、博士取得學位，並鼓勵針對資訊作戰或心理作戰理論進行操作化運用之研究。另外，也應鼓勵考取相關證照，增進本職有關理論基礎以及實務執行能力，並評估特定專業類別以專業認證比照軍事學歷(指參學院、戰爭學院)之相關作法。

三、國內產業合作：

資訊作戰結合相關產業合作，派遣相關專業人員如資安、大眾傳播等專業類別人員至民間產業工作交流，孰悉產業脈絡及相關資源，並獲取軍事以外之實務經驗。

四、海外軍事交流：

向美方爭取相關專業訓練之訓額，如資訊作戰專長班(Information Operations Qualification Course)或網路上尉軍官職涯班(Cyber Captains Career Course)等專業訓練班隊訓額，以求吸取美軍從歷年實戰中獲致之寶貴經驗，轉化為我國所用。另外亦可循當前心理作戰大隊與美軍第七心戰群簽署合作協議之例，簽訂資通電軍與美軍相對應機關或部隊之合作協議，深化實質軍事交流。

參、借鑒美軍實戰經驗教訓，強化平戰結合資訊作戰

美軍資訊作戰制度雖然也曾被指出有「資訊作戰與各單位作戰行動缺乏整合」、「過長的反應時間與協調上的拖延」、「資訊作戰與心理作戰之間之介面效能不彰」、「資訊作戰軍官遭到孤立」、「資訊作戰與公共事務之間缺乏協調」等缺點，然而美軍在獲悉此報告內容後，立即做出準則上的修訂及資訊作戰機制上的改良，獲致當前可稱完備之資訊作戰制度，我國當借鑒美國豐富之實戰經驗，參考其資訊作戰機制做為我國資訊作戰機制發展之基礎。

前總長李上將在年度漢光演習中引入美軍資訊作戰機制，意圖應對敵戰時可能對我國軍民發布假訊息等信息戰攻勢，雖從新聞報導無法窺得完整演習想定內容及聯合作戰中心內部之資訊作戰機制全貌，但此針對資訊環境的鞏固作為實為一大創舉，亦是我國面對中共信息戰威脅迫切所需之作為，國防部應將此機制納入正式戰時組織編制中，並著手修訂相關準則，訂定明確之職能、編組與作業程序。另外，考量信息戰之威脅平戰時均存在，應設立常態性

之資訊作戰編組，專責平時之資訊作戰計畫、執行與效能評估事宜。於此同時，中央部會應由國安會統籌，設立國家層級資訊作戰機制，方能運用整體國家資源，打贏信息環境中之無煙硝戰爭。


國防大學
National Defense University

參考文獻

一、中文部分

（一）專書

王幸生主編，2010。《軍隊政治工作學》。北京：軍事科學出版社。

朱成，2015。《那些年一直錯用的SWOT分析》。新北：創見文化。

岳忠強，2007。《軍隊政治工作學》。北京：國防大學出版社。

林中斌，2005。《以智取勝》。臺北:全球防衛雜誌。

姜連舉，2013。《空間作戰學教程》。北京：軍事科學出版社。

國防部，2009。《聯合資電作戰教則(試行本)》。臺北：國防部。

國防部，2011。《國軍通資電要綱(草案)》。臺北：國防部。

國防部，2012。《聯合作戰-心理作戰教則(試行本)》。臺北：國防部。

國防部，2015。《國防報告書》。臺北：國防部。

國防部，2016。《國軍政治作戰要綱》。臺北：國防部。

國防部，2016。《國軍聯合作戰要綱(第三版草案)》。臺北：國防部。

國防部，2017。《國防報告書》。臺北：國防部。

國防部，2019。《國防報告書》。臺北：國防部。

國家資通安全辦公室，2018。《資安即國安-國家資通安全報告》。臺北：國家安全會議。

張召忠，2004。《怎樣才能打贏信息化戰爭》。北京：世界知識出版社。

陳勇、姚有志主編，2004年。《面向信息化戰爭的軍事理論創新》。北京：解放軍出版社。

編譯者不詳，1992。《索忍尼辛的聲音與迴響》。臺北：黎明文化。

瞿海源、畢恆達、劉長萱、楊國書，2015。《社會及行為科學研究方法：質性研究法》。臺北：東華書局。

（二）專書譯著

Fisher, Craig S. and Babette E. Bensoussan著，陳苑欽等譯，2007。《企業策略與競爭分析：工具與應用》(Strategic and Competitive Analysis)。臺北：臺灣培生教育出版股份有限公司。

Peters, Guy著，王向民、段紅偉譯，2011。《政治科學中的制度理論:"新制度主義》(Institutional Theory In Political Science: "The New Institutionalism")。上海：人民出版社。

（三）專書論文

張五岳，2004。〈中共政局變遷對我國家安全之影響〉，丁渝洲主編，《臺灣安全戰略評估2003-2004》。臺北：遠景基金會。頁25-40。

曾維國，2011。〈廿一世紀美國心戰部隊的發展研究〉，洪陸訓、莫大華主編，《廿一世紀歐美主要國家心戰部隊的發展》。臺北：國防大學政治作戰學院。頁1-56。

（四）期刊論文

朱顯龍，2008。〈中國「三戰」內涵與戰略建構〉，《全球政治評論》，第23期，頁29-49。

余一鳴，2007。〈我國軍種文化差異之研究—以Hofstede的文化測量為架構〉，《復興崗學報》，第90 期，頁1-36。

吳奇英，2005。〈資訊時代政治作戰中心理戰的運用與發展——以美伊戰爭及兩岸資訊心理戰為例〉，《復興崗學報》，第85期，頁71-93。

呂爾浩、魏澤民，2006。〈中國"資訊作戰"的類型分析〉，《遠景基金會季刊》，第7卷第3期，頁187-229。

宋兆理、劉濯銨，2019。〈中共戰略支援部隊-網路系統部序列介紹〉，《陸軍通資半年刊》，第131期，頁23-46。

林穎佑，2016。〈中國近期網路作為探討：從控制到攻擊〉，《臺灣國際研究季刊》，第12卷第3期，頁51-68。

孫建祥，2009。〈論三類新型軍事人才的培養〉，《武漢工程大學學報》，第31卷第8期，頁10-13。

楊順利，2005。〈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》，第20卷第11期，頁116-126。

蔡明彥，2009。〈美國與中國軍事交流之發展與限制 (二〇〇四～二〇〇七年)〉，《歐美研究》，第39卷第3期，頁533-566。

蔡相廷，2010。〈歷史制度主義的興起與研究取向－政治學研究途徑的探討〉，《臺北市立教育大學學報》，第41卷第2期，頁39-76。

賴盈銓，2002。〈阿克薛諾夫小說《克里米亞島》中的「臺灣主題」〉，《俄國語文學報》，第5期，頁245-262。

（五）研討會論文

許閔政，2019。〈敵政工部隊(人員)現況及威脅評估報告〉，「第四屆國軍政治作戰戰術戰法」研討會。臺北：國防部政治作戰局等，頁27-37。

（六）官方文件

中共中央辦公廳、國務院辦公廳，2016/7。《國家資訊化發展戰略綱要》。

中華人民共和國國防部，2015/5/26〈中國的軍事戰略〉，《中華人民共和國國防白皮書》。

中華人民共和國國防部，2019/7/24。〈新時代的中國國防〉，《中華人民共和國國防白皮書》。

行政院資通安全處，2019/1。〈108年第4季資通安全技術報告〉,《資通安全技術報告》。

行政院資通安全會報，2019/4/11。《國家資通安全發展方案(106年至109年)》。

國家資通安全辦公室，2018/9。《資安即國安-國家資通安全戰略報告》。

（七）網路資料

中央社，2019/11/4。〈台美首次網攻演練，資安處：台每月遭攻擊 3,000 萬次〉，《科技新報》，<https://technews.tw/2019/11/04/taiwan-and-ait-first-network-attack-drill/>。(瀏覽日期：2020年4月13日)

中國軍網，2000/10/31。〈某摩步旅提高部隊政工網的使用效益〉,《中國軍網》，<http://search.chinamil.com.cn/search/milsearch/stouch.jsp?keyword=%E6%94%BF%E5%B7%A5&searchfield=TITLE&indexsearch=1#>。(瀏覽日期：2020年1月15日)

中華人民共合國互聯網信息辦公室，2019/9/19。《CNCERT互聯網安全威脅報告》，<http://www.cac.gov.cn/2019-09/19/c_1570421786756209.htm>。(瀏覽日期：2020年2月20日)

方瀟澎，2020/2/3。〈太空軍到底是個什麼軍?〉,《解放軍報》，< http://www.mod.gov.cn/education/2020-02/03/content_4859465.htm>。(瀏覽日期:2020年3月2日)

北京國泰建中管理諮詢有限公司，2016/10/31。〈鐳射探測定位系統專案單一來源採購公示公告〉,《招標公告》， <http://www.bjgtjz.com/newsview.asp?nid=11478>。(瀏覽日期:2020年3月3日)

台灣民意基金會，2018/6/17。《2018台灣人最喜愛的國家》，台灣民意基金會網站，<https://www.tpof.org/圖表分析/2018台灣人最喜愛的國家（2018年6月17日）/>。(瀏覽日期：2020年4月12日)

百度百科，2020/4/13。〈中國電子科技集團公司第五十四研究所〉，《百度百科》，<https://baike.baidu.com/item/中国电子科技集团公司第五十四研究所>。(瀏覽日期：2020年4月19日)

行政院國家資通安全會報，2019/2/14。〈行政院國家資通安全會報組織架構圖〉，《行政院國家資通安全會報網站》，<https://nicst.ey.gov.tw/Page/1AD9DA2B470FD4C0>。(瀏覽日期：2020年3月23日)

宋長江，2019/7/23。〈進一步強化資訊主導的作用〉，《解放軍報》， < http://www.mod.gov.cn/jmsd/2019-07/23/content_4846327.htm>。(瀏覽日期:2019年12月14日)

沈煒比，2017/11/9。〈美軍心戰軍官班受訓出國報告〉，《公務出國報告資訊網》，<https://report.nat.gov.tw/ReportFront/PageSystem/reportFileDownload/C10601338/001>。(瀏覽日期：2020年4月20日)

卓博人才網，2014/2。〈無錫江南計算技術研究所〉，《企業首頁》，<http://big5.jobcn.com/position/company.xhtml?comId=112263432>。(瀏覽日期:2020年3月3日)

周佑政，2019/10/10。〈台灣雙十節：蔡英文稱拒絕「一國兩制」成台灣最大共識〉，《聯合新聞網》，<https://udn.com/news/story/120766/4096991>。(瀏覽日期：2020年3月20日。

周碧松，2016/8/15。〈戰略邊疆〉，《軍報記者》，< http://zlzy.81.cn/tb/2016-08/15/content_7231775.htm >。(瀏覽日期:2019年6月12日)

奇創公考，2018/7/11。〈2018軍隊文職招聘戰略支援部隊職位表下載〉，《奇創公考網站》，<https://www.xuezi.net/jzg/bkzn/zwb/2018-07-11/1165.html>。(瀏覽日期:2020年4月18日)

林倖妃，2019/12/30。〈天下2020獨家國情調查：台灣vs.中華民國　世代衝突，更勝南北〉，《天下雜誌網站》，<https://www.cw.com.tw/article/article.action?id=5098353>。(瀏覽日期：2020年4月18日)

林庭瑤，2019/6/28。〈5G爭霸未落幕…陸超級電腦模擬核爆？老美心驚狠打壓〉，《聯合新聞網》，<https://udn.com/news/story/7332/3897005>。(瀏覽日期:2020年3月3日)

林穎佑，2020/2/28。〈從美國起訴中國網軍看戰略支援部隊〉，《Yahoo論壇》，<https://www.ccu.edu.tw/new_content_demo.php?type=newspaper&id=21621>。(瀏覽日期:2020年3月3日)

青木節子，2019/9/4。〈中國最尖端的「墨子」號量子通信衛星〉，《nippon.com》，<https://www.nippon.com/hk/japan-topics/c06501/?pnum=1>。(瀏覽日期:2020年2月26日)

南方電網，2018/10/23。〈公司在多項網路安全競賽中斬獲大獎〉，《大雲網》，< http://www.sgcio.com/yqxxh/itcsg/100351.html>。(瀏覽日期:2020年3月3日)

屏東縣崁頂鄉公所民政科，2018/5/29。〈國軍資訊通信聯隊人才招募〉，《屏東縣崁頂鄉公所網站》，<https://www.pthg.gov.tw/TownKto/News_Content.aspx?n=FF5357F5BDA5E114&sms=E54FF8470F4AF507&s=34200CCA9980FE00>。(瀏覽日期：2020年3月18日)

政治大學選舉研究中心，2019/1/7。《台灣國家安全調查》，Program in Asian Pacific Security Studies，<http://bit.ly/2HiK5vw>。(瀏覽日期：2020年4月9日)

洪哲政，2019/3/22。〈年度漢光兵推今展開首次推演假新聞攻擊與反制〉，《聯合新聞網》，<https://udn.com/news/story/10930/3769841>。(瀏覽日期：2020年3月18日)

洪哲政，2019/4/17。〈國軍資通電軍尖端網戰人才缺〉，《聯合新聞網》，<https://udn.com/news/story/10930/3760674 >。(瀏覽日期：2020年3月19日)

胡瑞玲，2019/6/12。〈香港「反送中」 郭台銘：香港一國兩制是失敗的〉，《聯合新聞網》，<https://udn.com/news/story/6656/3867319>。(瀏覽日期：2020年2月23日)

孫嘉業，2016/8/25。〈習近平通令透露的軍事機密〉，《明報》，<https://news.mingpao.com/ins/文摘/article/20160825/s00022/1472091515819/習近平通令透露的軍事機密（文-孫嘉業）>。(瀏覽日期:2020年3月3日)

徐凱琳，2018/7/20。〈第九屆國家戰略溝通峰會觀察紀要〉，《公務出國報告資訊網》，< https://report.nat.gov.tw/ReportFront/ReportDetail/detail?sysId=C10700664>。(瀏覽日期：2020年4月20日)

涂鉅旻，2016/8/20。〈電腦遭中國駭客入侵 國防大學：無機密資料〉，《自由時報》，<https://news.ltn.com.tw/news/politics/breakingnews/1801199>。(瀏覽日期:2020年4月10日)

馬振坤，2019/9。〈近期中美與外軍舉行聯合軍演情形〉，《ws.mac.gov.tw》，<https://ws.mac.gov.tw/Download.ashx?u=LzAwMS9VcGxvYWQvMjk1L2NrZmlsZS8wMTc4OGVkMC1jYzc0LTRmYzUtYTY2Ni1mNDc4MjQ3YjI3M2UucGRm&n=5LiJ44CB6L%2BR5pyf5Lit576O6IiH5aSW6LuN6IiJ6KGM6IGv5ZCI6LuN5ryU5oOF5b2iLnBkZg%3D%3D>。(瀏覽日期：2020年4月27日)

國立臺灣師範大學職涯發展中心，2019/1/22。〈國防部參謀本部資通電軍指揮部網路戰聯隊簡介〉，《國立台灣師範大學職涯發展中心Youtube頻道》，<https://www.youtube.com/watch?v=TeI1X-_NyYM>。(瀏覽日期：2020年3月18日)

國防部，〈國防部主管107年度單位預算評估報告〉，《立法院網站》，<https://www.ly.gov.tw/Pages/ashx/File.ashx?FilePath=~/File/Attach/166473/File_150060.pdf>. (瀏覽日期：2020年3月19日)

國防部，2018/9/7。〈資通電軍指揮部的任務〉,《國軍人才招募中心網頁》，<https://rdrc.mnd.gov.tw/EditPage/?PageID=8c8b7d44-68dc-45f4-9c49-813fce5c4bb9>。(瀏覽日期：2019年8月15日)

婁楊宣、黃子娟，2015/05/26。〈國防部：中國空軍將向空天一體化發展〉,《人民網》， <http://military.people.com.cn/n/2015/0526/c1011-27058165.html>。(瀏覽日期:2020年3月16日)

張晏彰，2019/5/23。〈【國軍108年「精神戰力專案教育」】李總長：仿真戰場演練務實檢討改進〉,《青年日報》，<https://www.ydn.com.tw/News/337312?fontSize=S>。(瀏覽日期:2019年6月30日)

許峰源，2018/5/25。〈50年代台海心戰「空飄氣球」瓦解敵方士氣的歷史，您知道嗎?〉,《國立教育廣播電臺》， <https://www.ner.gov.tw/programExpress/5b0517cb4e091300058748d8>。(瀏覽日期：2020年3月25日)

傅文成、余宗基，2016/12/8。〈Using big data approaches to explore how people evaluated armed forced in disaster relief mission〉,《公務出國報告資訊網》，<https://report.nat.gov.tw/ReportFront/ReportDetail/detail?sysId=C10700664>。(瀏覽日期：2020年4月20日)

創市際市場研究顧問，2019/12/22。〈台灣網路安全報告〉,《財團法人台灣網路資訊中心》，<https://report.twnic.tw/2019/>。(瀏覽日期：2020年4月13日)

彭琬馨、李欣芳，2019/11/9。〈網攻演習落幕 美盼深化與我合作〉,《自由電子報》，<https://news.ltn.com.tw/news/life/paper/1330641>。(瀏覽日期：2020年4月24日)

華圖教育，2019/3/13。〈戰略支援部隊-2019軍隊文職招聘職位表〉,《華圖教育網站》，<https://www.xuezi.net/jzg/bkzn/zwb/2018-07-11/1165.html>。(瀏覽日期:2020年4月18日)

逄記選，2016/6/16。〈專家：如何在現代戰爭中融合心理戰〉，《國防參考》，<http://www.81.cn/jmywyl/2016-06/16/content_7105198_3.htm>。(瀏覽日期：2020年3月13日)

黃德潔，2017/9/21。〈網路輿情蒐研系統 掌握大陸民情〉，《青年日報網站》，<https://www.ydn.com.tw/News/256133>。(瀏覽日期:2020年3月20日)

新境界文教基金會國防政策諮詢小組，2015年5月。〈國防政策藍皮書第九號報告：2025 年台灣軍事防衛能量〉，《新境界文教基金會》，<http://www.dppnff.tw/uploads/20150525205515_6229.pdf>。(瀏覽日期：2020年3月18日)

楊欣燕。〈國防部資通電軍指揮部網路戰聯隊招募資訊〉，《國立嘉義大學官網》，<https://en.mcut.edu.tw/p/404-1051-34244.php?Lang=zh-tw>。(瀏覽日期：2020年3月18日)

漢聲廣播電臺，2019/11/28。〈透過科技整合反制中共心戰〉，《漢聲廣播電臺網站》， < https://www.voh.com.tw/TW//News/ugC_News_Detail.aspx?NewsCatID=2&NewsID=382>。(瀏覽日期：2020年3月25日)

維基百科，2019/10/28。〈國防部參謀本部資通電軍指揮部〉，《維基百科》，< https://zh.wikipedia.org/wiki/國防部參謀本部資通電軍指揮部>。(瀏覽日期：2020年3月18日)

臺灣事實查核中心，2019/6/20。〈打擊假消息台灣事實查核中心與臉書合作〉，《研究與動態》，<https://tfc-taiwan.org.tw/articles/591>。(瀏覽日期：2020年4月13日)

劉禹伸，2019/6/17。〈俄國電網資安遭駭客攻擊事件對我國能源供應穩定帶來的啟示〉，《能源知識庫》，<https://km.twenergy.org.tw/Data/db_more?id=3668>。(瀏覽日期：2020年4月13日)

劉興、林文斌，2016/3/28。〈加強政工網遠程編輯隊伍建設〉，《中國軍網》，<http://www.81.cn/jsjz/2016-03/28/content_6980042.htm>。(瀏覽日期：2020年1月15日)

賴于榛，2019/10/16。〈禁購清單遲未出爐 政院：評估影響產業界或有貿易糾紛〉，《聯合新聞網》，<https://udn.com/news/story/6656/4106921>。(瀏覽日期: 2020年3月11日)

謝嘯天，2019/4/12。〈上升段導彈獵手：天基雷射武器〉，《解放軍報》，<http://photo.81.cn/bqtk/2019-04/12/content_9475543.htm>。(瀏覽日期：2020年3月12日)

羅添斌，2016/3/2。〈國軍心戰大隊 本月赴美深度參訪〉，《自由時報》，<https://news.ltn.com.tw/news/politics/paper/963567>。(瀏覽日期：2020年3月24日)

二、英文部分

（一）專書

Costello, John and Joe McReynolds, 2018. *China's Strategic Support Force: A Force for a New Era.* Washington, D.C.: National Defense University Press.

Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer, 2017. *Lessons from Russia's Operations in Crimea and Eastern Ukraine*, Santa Monica, CA: RAND Corporation.

Larson, Eric V., Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell H. Schwartz, and Cathryn Quantic Thurston, 2009. *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities*. Santa Monica, CA: RAND Corporation.

Munoz, Arturo, *U.S. Military Information Operations in Afghanistan: Effectiveness of Psychological Operations 2001-2010, 2012.* Santa Monica, CA: RAND Corporation.

Paul, Christopher and William Marcellino, *Dominating Duffer's Domain: Lessons for the U.S. Army Information Operations Practitioner*, 2017. Santa Monica, CA: RAND Corporation.

Paul, Christopher, Colin P. Clarke, Bonnie L. Triezenberg, David Manheim, and Bradley Wilson, 2018. *Improving C2 and Situational Awareness for Operations in and Through the Information Environment.* Santa Monica, CA: RAND Corporation.

Paul, Christopher, Colin P. Clarke, Michael Schwille, Jakub P. Hlavka, Michael A. Brown, Steven Davenport, Isaac R. Porche III, and Joel Harding, 2018. *Lessons from Others for Future U.S. Army Operations in and Through the Information Environment: Case Studies.* Santa Monica, CA: RAND Corporation.

Sazonov, Vladimir, Holger Mölder, Kristiina Müür, Pille Pruulmann-Vengerfeldt, Igor Kopõtin, Aarne Ermus, Karl Salum, Andrei Šlabovitš, Viljar Veebel and René Värk, 2016. *Russian Information Campaign Against the Ukrainian State and Defense Forces*, Tartu: Estonian National Defence College.

（二）專書論文

Costello, John, and Joe McReynolds, 2018, “China’s Strategic Support Force: A Force for a New Era,” in Phillip C. Saunders et al., eds., *Chairman Xi Remakes the PLA, Washington*, D.C.: National Defense University Press, pp. 437-518.

（三）期刊論文

Boyd, Curtis D., May-June, 2007.“Army IO is PSYOP: Influencing More with Less,” *Military Review*, Vol. 87, No. 3, pp. 67-75.

John Costello, “The Strategic Support Force: China’s Information Warfare Service”, *China Brief*, Vol. 16, No. 3, February 8, 2016, pp. 15-19.

（四）官方文件

Defense Intelligence Agency, 2019. *China Military Power: Modernizing a Force to Fight and Win*, Washington, D.C.: Defense Intelligence Agency.

Department of Defense, 2017. *Department of Defense Directive 3600.01*, Washington, D.C.: Department of Defense.

Department of the Army, 2018.*Army Techniques Publication 3-13.1: The Conduct of Information Operations*, Washington, D.C.: Joint Chiefs of Staff.

Joint Chiefs of Staff, 1998. *Joint Publication 3-13: Information Operations*. Washington, D.C.: Joint Chiefs of Staff.

Joint Chiefs of Staff, 2003. *Joint Publication 3-53: Psychological Operations*. Washington, D.C.: Joint Chiefs of Staff.

Joint Chiefs of Staff, 2006. *Joint Publication 3-13: Information Operations*. Washington, D.C.: Joint Chiefs of Staff.

Joint Chiefs of Staff, 2009. *Strategic Communication Joint Integrating Concept.* Washington, D.C.: Joint Chiefs of Staff.

Joint Chiefs of Staff, 2011. *Joint Publication 3-13.2: Military Information Support Operations*. Washington, D.C.: Joint Chiefs of Staff.

Joint Chiefs of Staff, 2012a. *Joint Publication 3-13.4: Military Deception.* Washington, D.C.: Joint Chiefs of Staff.

Joint Chiefs of Staff, 2012b. *Joint Publication 6-01: Joint Electromagnetic Spectrum Management Operations*, Washington, D.C.: Joint Chiefs of Staff.

Joint Chiefs of Staff, 2012c. *Joint Publication 3-13: Information Operations*. Washington, D.C.: Joint Chiefs of Staff.

Joint Chiefs of Staff, 2014. *Joint Publication 3-13: Information Operations*. Washington, D.C.: Joint Chiefs of Staff.

Joint Chiefs of Staff, 2015. *Chiarman of the joint chiefs of staff instruction: Information Assurance (IA) and support to computer network defense (CND)*, Washington, D.C.: Joint Chiefs of Staff.

Joint Chiefs of Staff, 2016a. *Joint Publication 3-13.3: Operations Security*, Washington, D.C.: Joint Chiefs of Staff.

Joint Chiefs of Staff, 2016b. *Joint Publication 3-61: Public Affairs*, Washington, D.C.: Joint Chiefs of Staff.

Joint Chiefs of Staff, 2017. *Interorganizational Cooperation.* Washington, D.C.: Joint Chiefs of Staff.

Joint Chiefs of Staff, 2018a. *Joint Publication 3-12: Cyberspace Operations*, Washington, D.C.: Joint Chiefs of Staff.

Joint Chiefs of Staff, 2018b. *Joint Publication 3-57: Civil-Military Operations*, Washington, D.C.: Joint Chiefs of Staff.

（五）網路資料

Agrawal, Nina, 2017/1/17. “There’ s more than the CIA and FBI: The 17 agencies that make up the U.S. intelligence community”， *Los Angels Times*,

<https://www.latimes.com/nation/la-na-17-intelligence-agencies-20170112-story.html>.(Accessed：19/3/2020)

Arkin, William M., Janunary 18, 1999.“Phreaking Hacktivists,” *washintonpost.com*, < https://www.washingtonpost.com/wp-srv/national/dotmil/arkin011899.htm>.(Accessed:15/10/2019)

Boyd, Curtis, January-February 2011. “The Future of MISO”, *Special Warfare*, (Fort Bragg, N.C.: the United States Army John F. Kennedy Special Warfare Center and School), vol. 24, Issue 1, pp.22-28. <http://www.soc.mil/SWCS/SWmag/Archive/SW2401/SW2401TheFutureOfMISO.html>.(Accessed:7/10/2019)

Cicalese, Carmine, 2013.“Redefining Information Operations”, *Joint Forces Quaterly*, (Fort Lesley, Washington, D.C.:National Defense University Press), vol. 69, pp. 109-112. <https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-69/JFQ-69_109-112_Cicalese.pdf>.(Accessed:25/8/2019)

Cyber Command Public Affairs, 2018/5/17. “Cyber Mission Force achieves Full Operational Capability,” *United States Cyber Command Website*, <https://www.cybercom.mil/Media/News/News-Display/Article/1524492/cyber-mission-force-achieves-full-operational-capability/>.(Accessed：23/3/2020)

Garamone, Jim, 2019/9/4. “Military Must Be Ready to Confront Hybrid Threats, Intel Official Says,” DoD Website, <https://www.defense.gov/Explore/News/Article/Article/1952023/military-must-be-ready-to-confront-hybrid-threats-intelligence-official-says/>.(Accessed:9/4/2020)

Gertz, Bill, 2016/1/27. “Chinese Military Revamps Cyber Warfare, Intelligence Forces: Changes meant to improve PLA high-tech warfighting,” The Washington Free

Beacon, <https://freebeacon.com/national-security/chinese-military-revamps-cyber-warfare-intelligence-forces/>.(Accessed：15/1/2020)

Jensen, Aaron, 2013.“China Prepares for Psychological Warfare”, *The Diplomat*.<http://mil.cankaoxiaoxi.com/2013/0817/257086.shtml>.(Accessed:18/6/2019)

Lucas, Louise, 2018/3/28.“China Hackers Ordered to Report Software Holes to Spy Agency,” *Financial Times*, <https://www.ft.com/content/eaf7f080-3186-11e8-b5bf-23cb17fd1498>.(Accessed：6/3/2020)

Mazarr, Michael J., Ryan Michael Bauer, Abigail Casey, Sarah Heintz, and Luke J. Matthews, 2019. *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment*. Santa Monica, CA: RAND Corporation, <https://www.rand.org/pubs/research_reports/RR2714.html>.(Accessed：10/11/2019)

Ni, Adam, and Bates Gill, 2019. “The People’s Liberation Army Strategic Support Force: Update 2019,” *China Brief*, Washington, D.C.:James Town Foundation. <https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/>. (Accessed:14/7/2019)

Perlroth, Nicole, 2014/6/10.” 2nd China Army Unit Implicated in Online Spying”, *The New York Times*, <https://www.nytimes.com/2014/06/10/technology/private-report-further-details-chinese-cyberattacks.html>. (Accessed:3/3/2019)

Radin, Andrew, 2017/2/23.“Hybrid Warfare in the Baltics,” RAND Corporation Website,<https://www.rand.org/pubs/research_reports/RR1577.html>. (Accessed:9/4/2020)

Reed, John, 2013/3/8. “How many cyber troops does the U.S. have?”, Foreign Policy, <https://foreignpolicy.com/2013/03/08/how-many-cyber-troops-does-the-u-s-have/>.(Accessed：19/3/2020)

Rona, Thomas, 1976/7/1. “*Weapon Systems and Information War*”, Office of the Secretary of Defense, <https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf>.(Accessed:8/3/2020)

Theohary, Catherine, 2018/12/18. *Defense Primer: Information Operations*, Washington, D.C.: CRS, Congressional Research Service, <https://fas.org/sgp/crs/natsec/IF10771.pdf>.(Accessed：4/9/2019)

Theohary, Catherine, 2018/3/5. *Information Warfare: Issues for Congress*, Washington, D.C.: CRS, Congressional Research Service, <https://fas.org/sgp/crs/natsec/R45142.pdf>.(Accessed：4/9/2019)

Thomson, Scott and Christopher E. Paul, 2018. “*Paradigm Change: Operational Art and the Information Joint Function*”, Joint Forces Quaterly, Fort Lesley, Washington, D.C.:National Defense University Press. <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1490645/paradigm-change-operational-art-and-the-information-joint-function/>. (Accessed:10/6/2019)

Tisdall, Simon, 2018/4/3. “Will China turn Taiwan into the next Crimea,” *The Guardian*, <https://www.theguardian.com/world/2018/apr/03/how-safe-is-taiwan-from-becoming-the-next-crimea-us-china>.(6/4/2020)

Treisman, Daniel, 2016. “Why Putin Took Crimea: The Gambler in the Kremlin,” *Foreign Affairs*, <https://www.foreignaffairs.com/articles/ukraine/2016-04-18/why-russian-president-putin-took-crimea-from-ukraine>.(Accessed:6/4/2020)