以網電作戰淺談作戰區網電作戰小組

作者/温宗毅

提要

一、在現今高科技戰場中已是「大軍未動，網電先行」，藉由歷代戰爭及「俄烏戰爭」中網路戰及電子戰，不但可以熟知各種網電作戰手段，掌握網電優勢、創造戰場致勝先機，更能主導戰場。

二、國軍網電作戰小組負責各作戰階段網路戰、電子戰和心理戰等計畫策頒、兵力運用並提供指揮官網電作戰參謀建議，可參考美軍網電組織編組方式適當調整我軍編組方式。

三、國軍防衛作戰中，網電作戰已成為極具重要的一環，除強化網電作戰小組學能、落實實戰化訓練、培育專業網電人才，並納入軍事戰略思維，才能面對複合式的網電作戰。

關鍵詞：網路戰、電子戰、電磁頻譜作戰、網電小組

前言

隨著科技蓬勃發展，現代戰爭不像以往軍事作戰中只採用殺傷力大的兵器，各類型作戰型態逐漸改變，2014年俄羅斯以網路戰手段併吞了克里米亞，稱為當代網路戰戰役範例，而網路戰所帶來的新型態威脅也受到各國矚目；美陸軍於2016年提出多領域作戰(Multi-Domain Battle, MDB)之概念，也就是多維空間作戰概念，包含了陸、海、空、太空、網路及電磁頻譜等作戰環境，據以因應未來複合式威脅及其戰場環境挑戰，就可以知道現代戰爭脫離不了網路及電磁頻譜。

有別於傳統作戰空間，網路空間隨著科技發展已逐步另闢戰場，複雜且多元，穿梭不同空間與層級，在複雜電磁環境下，網路空間作戰、電子作戰、電磁頻譜作戰三者合流已是趨勢，誰能掌握並確保網路空間及資電優勢，即掌握先機也掌握了戰場。

自共軍軍改後，戰略支援部隊網路系統部整合過去總參三部（技術偵查部）、四部（電子對抗與雷達部）攻勢網路作戰與電戰能量，進行「網電一體戰」

的具體落實，[1]另以「網電一體戰」手法，對我政經軍重要機關實施網路資訊攻擊，並伺機散播不實消息，以達癱瘓我重要目標及擾亂民心之目的。[2]

本研究由探討共軍網電威脅及美、國軍網電部隊組織編組運作及任務分析為基礎，提出精進作為芻議，期可供國軍於建軍備戰策略之參據。

網電作戰名詞定義及戰役

一、定義

(一)美軍：

1.網路空間作戰：網路空間作戰是對網路空間能力的運用，其主要目的是在網路空間內或通過網路空間實現作戰目標。[3]

2.電子戰：美軍於 2020 年宣布廢止電子戰一詞，取而代之的是電磁戰，係指涉及使用電磁和定向能量來控制電磁頻譜或攻擊敵人。[4]

3.電磁頻譜作戰：包含軍事通信、偵測和電子戰等領域，以確保電磁頻譜在軍事行動之利用、攻擊、防護與管理電磁環境，支援指揮官作戰企圖。[5]

(二)國軍：

1.網路空間作戰：又稱網路戰，係運用電腦系統、網際網路或通信網路之網路空間，藉網路情蒐等手段，獲取軍事所需情報，並掌握敵系統弱點，適時對敵實施破壞、阻絕、衰退或摧毀存在於電腦與網路空間上之資訊，或是電腦及網路空間本身的相關作為，以達成軍事目的。[6]

2.電子戰：電子戰係運用電磁與指向性能量，以削弱或摧毀敵使用電戰系列，同時確保我軍有效運用電磁頻譜所採取之軍事行動。[7]

3.電磁頻譜作戰：電磁頻譜作戰一詞相較於電子戰，其電磁頻譜涵蓋範圍更廣，電子戰專注於雷達與無線電波之攻擊與防護，電磁頻譜作戰則擴展至整體電磁頻譜範圍（例：紅外線、雷射、微波、衛星通信及網路空間通信），電磁頻譜作戰係指為確保戰場軍事武器與其他實體，能經由電磁頻譜獲得戰場狀況覺知與通信能力所進行之利用、攻擊、防護與管理電磁環境，以達成指揮官

1 財團法人國防安全研究院，《2020國防科技趨勢評估報告》（臺北市：五南圖書出版股份有限公司，民國109年12月），頁111。
2 國防部，《中華民國108年國防報告書》(臺北：國防報告書編纂委員會，民國108年9月)，頁40~42。
3 Joint Chief of Staff, Joint Publication 3-85: Joint Electromagnetic Spectrum Operations,May20,2020,p.vi。
4 同註3，p.GL-9。
5 同註3，p.GL-8。
6 林予令，《國軍聯合作戰網電教則》（臺北：國防部，民國111年12月8日），頁1-2。
7 張雪光，《陸軍作戰要綱》（桃園：陸軍司令部，民國112年1月7日），頁1-5-58。

企圖之所有軍事行動，進而掌握「制電磁權」。[8]

二、著名戰役(事件)

(一)網路戰

資訊戰（Information Operations）係指在軍事行動中，運用戰略溝通、聯合跨部會協調、公共事務、軍民作業、網路戰、資訊確保、電子戰、心理戰、情報、軍事欺敵、作戰安全及關鍵領導幹部接觸等手段，影響、干擾、阻絕或竄改敵決策，以達自我防護之目的，而「網路戰」為資訊戰之一環，在歷史上不難發現有許多網路戰案例(如表 1)。

表 1 歷史上的網路戰事件

年份	網路戰事件
2007年	美國國防部長未加密的電子信箱帳號遭未知外部人士駭入，目的是得到五角大廈內部網路存取權限並加以利用。
2008年	喬治亞與俄羅斯衝突期間，網路數據交換中心遭到未知的境外人士駭入，政府網站遭到塗鴉。雖未造成政府網站終止服務，但駭客明顯是配合俄羅斯軍事行動對喬治亞施壓。
2009年	以色列於 1 月對加薩走廊的軍事行動，導致以色列網路基礎設施遭駭客攻擊，該攻擊針對政府部門至少 50 萬台電腦。
2012年	卡巴斯基防毒軟體公司發現了一個全球性的網路攻擊，是藉由微軟公司 Word 與 Excel 程式漏洞，主要攻擊目標在東歐及中亞等國家，該病毒收集了來自政府研究機構、軍事設施、核能等關鍵基礎設施資訊，此事件被稱為「紅色十月(Red October)」。
2015年	網路駭客於 2015 年間對烏克蘭電力公司（Oblenergos）進行高度複雜之網路攻擊，切斷約 25 萬居民電力，即便莫斯科始終否認對烏克蘭從事網路攻擊，烏國政府仍堅稱該事件幕後指使者為俄國。
2018年	美國聖地牙哥港於 2018 年 9 月，遭伊朗駭客惡意軟體攻擊，使得港口數日間的進入許可及公共文件使用受到限制，港口警察處理行政功能之電腦亦受到影響。依據港口發表之聲明，雖然該次網路攻擊事件並未對使用港口之船隻運行造成停擺或使公眾處於危險當中，但惡意軟體已滲透電腦網路並破壞港務管理系統。
2020年	網路駭客透過入侵軟體 Sunburst，成功入侵美國 Solar Winds Orion 平台，繞過防火牆，竊取機密事件，造成國防部、國務院等多家機構的機密文件及資訊遭竊。

資料來源：作者整理。

8同註6，頁1-2。

而近期的俄烏戰爭中，亦不難發現網路戰之手段，包含大規模的 DDos[9]攻擊及惡意軟體和發放假文件等(如表 2)。

表 2 俄烏戰爭的網路戰事件

日期	攻擊型態	目標	影響
2021 年 2 月	大規模 DDos 攻擊	烏克蘭安全和國防網站、其他國家機構及企業	網站遭破壞、攻擊結束後仍無法登入
2021 年 7 月	惡意軟體發布假文件	烏克蘭海軍網站	表達對黑海國家和北約盟國及合作夥伴參與「海風 2021」軍事演習不滿，並傳播有關軍事演習假資訊。
2022 年 2 月	DDos 攻擊	烏克蘭國防部及武裝部隊網站	網站無法連線，服務中斷。
2022 年 2 月	DDos 及 Wiper 攻擊	烏克蘭外交、內政、國防部、國家安全局等多部門網站	基輔、哈爾克夫等城市網路陸續斷線、網站無法登入、服務中斷。
2022 年 2 月	DDos 攻擊	烏克蘭首都基輔、哈爾克夫及烏克蘭部隊	1.基輔的網路流量下降六成；包括哈爾克夫的居民遭停電或斷網，約 70 個政府網站癱瘓。 2.烏軍個人手機接收到假訊息。

資料來源：黃郁文，<淺析俄羅斯「網路戰」-以2022年「烏俄戰爭」運用為例 >《海軍學術雙月刊》(臺北)，第56卷第4期，民國111年8月1日，頁97。

(二)電子戰

1904 年日俄戰爭與 1905 年日俄「對馬海峽」戰爭中，第一次運用現代通信電子技術，進行通信對抗，它詮釋一種全新的作戰形式「電子戰誕生」。

第二次世界大戰初期，電子戰仍僅限於通信對抗，只運用了電子偵察與電子欺騙等簡單手段。第二次世界大戰中期，雷達、導航與武器控制系統相繼問世，由單一的通信對抗發展到導航、雷達對抗等諸多種類，各國也相繼組建專業電子戰部隊。

9 阻斷服務攻擊(Denial of Service Attack,Dos)是近年來常見的一種網路攻擊模式，其目的在使被攻擊的目標網路或資訊系統的資源耗盡，使服務暫時中斷或停止，導致其正常用戶無法存取網路及資訊系統的服務。當惡意攻擊者運用網路上大量被攻陷的電腦作為殭屍(Bot)向特定的目標發動Dos攻擊，稱為分散式阻斷服務攻擊(Distributed Denial of Service Attack,DDos)。〈分散式阻斷服務攻擊防護策略探討〉，臺灣網路資訊中心，https://www.twnic.tw/NEWS4/165.php，檢索日期：2023年4月12日。

在「以敘貝卡山谷戰役」及「英阿福島戰爭」戰役中，電子戰發展迅速，尤以「美利雪特拉灣」戰役中，美國將「偵察–誘騙–干擾–導引–突擊」等諸般電子戰作為連成一體，而從波灣及科索沃戰爭更驗證了高科技與不接觸的時代來臨，電子戰更是由局部影響戰爭到貫穿作戰全程，開創了電磁頻譜的「第五維空間」，使得許多先進國家再次瞭解電子戰之重要性，並一致認為電子戰是未來致勝之最佳武力，如能在戰爭初期以極短時間內摧毀或癱瘓敵人運用電磁權的能力，便能奪取戰場主控權(歷史上著名的電子戰戰役如表 3)。

表 3 歷史上著名的電子戰戰役

年份	戰役名稱	電子戰運用作為
1904年	日俄戰爭	通信監聽與干擾獲致退敵。
1965年	越南戰爭	在這場戰役中，首次出現了電子偵察與反偵察、電子干擾與反干擾以及電子摧毀及反摧毀，美軍由此次戰役才正式有了電子戰支援、電子反制與反反制之定義與概念。
1982年	以敘貝卡山谷戰役	運用無人機誘敵發射雷達訊號，並藉電偵機實施偵蒐、定位作業後，實施精準打擊
1982年	英阿福島戰爭	運用電子情報偵蒐系統，接收衛星所提供之敵情資料，藉以獲知兵力部署、艦隊活動等情報；另利用地球曲度及海平面所造成之雷達死角，避開雷達偵測，使其無預警時間。
1986年	美利雪特拉灣戰爭	空陸一體化電子偵測，並對敵防空雷達及陣地飛彈實施電子干擾，將「偵察–誘騙–干擾–導引–突擊」等諸般電戰作為連成一體。
1991年	波灣戰爭	運用衛星對伊拉克軍事目標及電磁訊號進行不間斷偵察監視，並藉由各式電偵機針對雷達及無線電通信網路實施偵察及監聽，
2001年	阿富汗戰爭	藉由各項電子偵測，對敵通信系統實施干擾使其無法運作，並利用反輻射武器及GPS導航定位系統，對敵實施精準打擊。
2014年	入侵克里米亞事件	俄羅斯利用多項電子干擾、雷達反制及GPS干擾，破壞部隊間通信、壓制雷達系統及GPS信號，使烏克蘭喪失對部隊掌握和情報掌控的能力。
2020年	雙亞衝突	亞賽拜然運用大量的無人機對戰場目標區域實施全時段監控、破壞與摧毀；亞美尼亞未能將電戰與防空結合，遭受大量人員、裝備損傷。

資料來源：作者整理，參考錢高陞，<歷代戰爭中電子戰史實與評析>，https://top81.ws/show.php?f=6&t=107956&m=403606，2003年4月30日，(檢索日期 ： 2023年1月4日)。

而在 2014 年俄羅斯入侵克里米亞事件後，於 2022 年 2 月 24 日，俄羅斯以「非軍事化、去納粹化」為主要目的對烏克蘭發動戰爭，其中電子戰的手段更是層出不窮(電子戰相關運用如表 4)。

表 4 俄烏戰爭的電子戰運用

戰術運用	說明
商用衛星對俄軍事行動的偵察	烏克蘭於衝突爆發前，商業衛星公司的監測網路即注意到俄軍活動已經有所增加。許多商業衛星圖像公司提供的高解析度衛星照片，攝得大量俄軍活動照片，對亟需情報的政府部門非常有益。
電戰多重攻擊與壓制	俄羅斯運用Krasukha-4電戰裝備，用於干擾烏克蘭衛星信號及雷達導引武器，有效對敵低軌道偵察(通訊)衛星進行帶狀干擾，發揮屏蔽效果。而Borisoglebsk-2電戰裝備，則干擾烏克蘭無人機導引系統和無線電控制的地雷，使烏克蘭軍隊無人機，平均使用壽命僅約7日。
電子訊號軌跡輔以人工智慧進行精準打擊	俄羅斯運用電子戰系統偵蒐敵電子訊號軌跡同時，輔以人工智慧技術加持，除對目標偵蒐定位有系統紀錄外，更可對敵電子設備進行有效目標識別(相應武器載台)，搭配優勢兵火力實施精準打擊。
建置偽冒基地台，竊取俄軍各項資訊	俄軍使用 Era 加密軍用通話系統，雖為高端加密技術，惟仰賴地面行動基地台作為訊號傳遞與接收，當戰線拉長時俄羅斯基地台無法使用，並需仰賴烏克蘭衝突地區內 3G/4G 行動基地台。研判烏克蘭為有效竊取俄羅斯軍事情報，於衝突地區建置偽基地台監聽設備，使俄羅斯智慧型手機用戶被迫與其基地台連結後，入侵用戶通話系統、監聽及定位，造成俄羅斯各項戰術行動暴露。
Starlink低軌道衛星運用	俄烏軍事衝突開戰後，俄軍持續向烏克蘭電信站台及網路電纜進行攻擊，烏克蘭透過馬斯克提供星鏈系統低軌道衛星網路服務，並使用虛擬專用網路，使駭客無法進入該封閉網路，降低資料於傳輸時遭敵竊取。
部署無人機防禦系統	1.俄羅斯於烏東地區部署高密度電戰裝備，用以干擾烏克蘭無人機的頻率，使其飛往不同方向以利俄軍擊落，據報導烏克蘭每個月在戰場上約損失一萬架無人機。 2.據德國《圖片報》報導，烏克蘭將英國提供的反無人機系統(Anti-Uav Defence System, AUDS)投入實戰中，該系統號稱集「檢測、跟蹤、干擾」於一身的反無人機系統，可在 8 公里內發現、干擾各類小型無人機，甚至有能力接管其控制權。

資料來源：作者整理

(四)小結

戰場環境在高科技影響下，已朝資訊化方向發展，不對稱、不接觸、非線性的作戰型態逐漸成熟，「制電磁權」成為戰場綜合控制權之核心，關鍵在於網路空間、電磁頻譜(空間)所進行看不見的戰爭，也是沒有煙硝之戰爭。

為此，美國於 2009 年成立「網路司令部」，負責進行網電作戰並加強防範網電空間之威脅，美國前總統川普亦於 2017 年 8 月 18 日將「網路司令部」，升格為聯合作戰司令部的第 10 部；中共軍改亦朝著「質量建軍，科技強軍」，於 2016 成立「戰略支援部隊」，成為中共陸軍、海軍、空軍及火箭軍以外的第五支新型態「作戰力量」；而我國發展亦同步與時俱進，國防部於 2017 年 7 月 1 日整合各式通資部隊，編成「資通電軍指揮部」，成為現有陸、海、空三軍外，獨立的第四軍種，以提升我國整體網電作戰能力。

除成立「資通電軍指揮部」外，藉由烏俄戰爭中網電作戰手段，對我防衛作戰建軍備戰的啟發如下。

1.國防工業自主發展，強化軍民通用科技

因應作戰型態改變，戰場資電優勢掌握已為首要，科技作戰猶如另類軍備競賽，因此我軍通資電未來發展，應以肆應科技不對稱作戰防護手段為首要考量。軍用裝備獲得，應以自製為優先，向外採購時應落實技術移轉，達成國防工業獨立自主發展之目標，推動國防自主，強化軍民通用科技，以國防科技研發能量為基礎，研發具前瞻性國防科技及軍民通用科技，建構國防帶動產業、產業支持國防之循環效益。

2.強化國軍資訊安全防護整備作為

除加強國軍資安教育，並持續掌握新型網路威脅型態，落實「實體隔離」、「定時實施網路健檢」及「資安人才培訓」等管控機制，以增強國軍網路戰力。

3.強化指管作為，精進電戰防護能力

因應中共匿蹤戰機、無人攻擊機等威脅，除籌建新式電戰裝備外，應同時整合電磁頻譜管理與參數比對能量，以建立電子參數資料庫，另強化電戰偵干能力之距離，並朝符合城鎮作戰、快速部署及強化偵干頻率及範圍等作戰需求發展，以達先期預警之目的。

網電作戰威脅

共軍戰略指導方針由1993年「打贏高技術條件下局部戰爭」、2004年「打贏

信息化條件下的局部戰爭」，2015年調整為「打贏信息化局部戰爭」，並向外表達堅定維護國家領土主權及打贏戰爭決心。2017年19大後，調整發展戰略為「國防和軍隊現代化建設三步走」，期在2020年實現「機械化、信息化建設」，2035年實現「國防和軍隊現代化」，持續至2050年全面建成世界一流軍隊，以維護國家利益、提供戰略支撐。共軍戰略發展上，由「被動反擊」走向「主動先制」，從「機動作戰、立體攻防」戰略轉變「區域防衛型」向「全域作戰型」，[10]導入信息化作戰能力，加速戰場指揮與資訊管理升級，全面推動組建陸航及特戰等新型戰力。

信息戰一詞源於中共，相當於國軍資訊戰，依中共軍事科學院作戰條令部編著的《信息化作戰理論學習指南》提及信息戰是以信息為基礎，保持己方訊息系統避免被敵方利用、破壞或干擾，同時利用、破壞或干擾敵方訊息系統，並以信息化武器、裝備獲得訊息優勢的過程，作戰內容包含三個層次：一是以物質摧毀和消滅有生力量為主的物理層面作戰；二是以控制信息基礎設施和電磁頻譜的信息層面作戰；三是以瓦解人意志及情感為主的心理層面作戰。[11]

一、戰略支援部隊

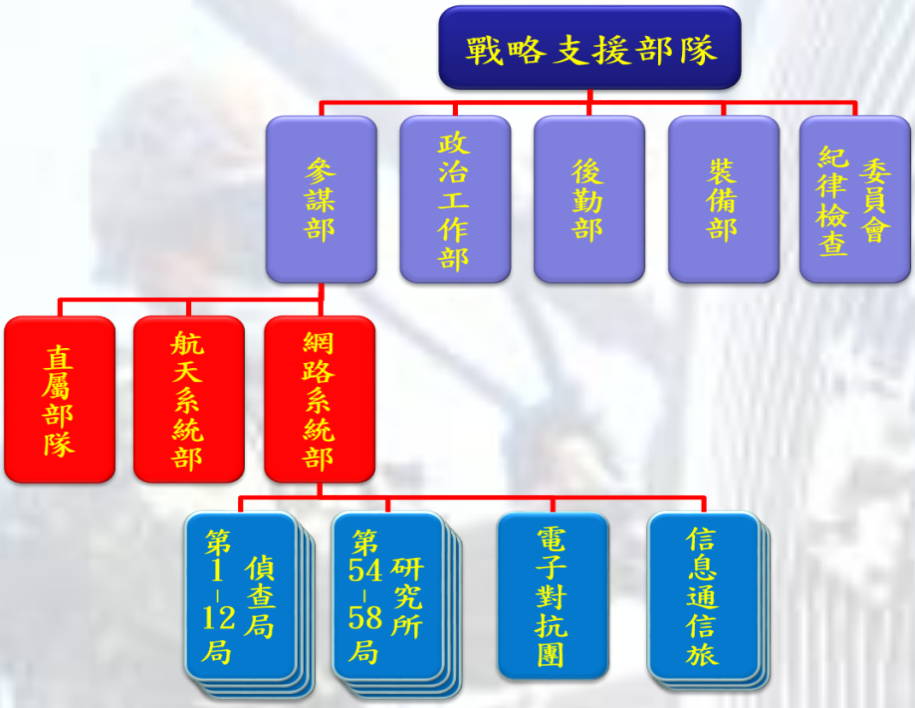
中共中央軍委於2016年成立了戰略支援部隊，作為戰區司令部級組織，其組織架構(如圖1)以集中戰略太空、網路，電子和心理戰任務和能力，中共的網電一體化作戰主要在取得資訊優勢並拒止對手使用電磁頻譜與網路空間有用的信息，是搶占和維持其戰略主動權之必要條件。戰略支援部隊由曾隸屬於共軍各部隊及中共中央軍委的總參謀部組成，其目標是在先前各種不同的訊息戰能力之間建立協同作戰能力，藉整合這些任務於同一個組織下，使資訊優勢成為中共在未來戰爭中，能發揮決定性作用的主導地位。[12]

戰略支援部隊所屬的網路系統部，為接收原總參謀部「技術偵查部」(三部)和「電子對抗部」(四部)，及原總參情報部(二部)和原總參裝備部的一部分而成。專責執行電子偵察、網路空間及信息安全、網路攻防、電腦網路系統、情蒐作業及心理戰等，並藉由偵察衛星、偵察機、無人機及電戰裝備等設備蒐整暨分析無線電信號、電磁信號及紅外線信號等電子參數，以實施欺騙和干擾、入侵網路與頻率，拒止敵人在電磁頻譜與網路空間有用的信息。同時負責戰略網軍與電戰部隊的組織、訓練與裝備。軍種仍然主管戰役與戰術層級網軍與電戰

10同註2，頁30。
11學史泛舟，〈信息化戰爭概述〉《知乎-國防教育》，2020年12月27日，https://zhuanlan.zhihu.com/p/339819714，檢索日期：2023年8月3日。
12財團法人國防安全研究院，《聯兵旅級部隊電戰裝備運用現況與指管機制之研究》，民國109年12月30日，頁23

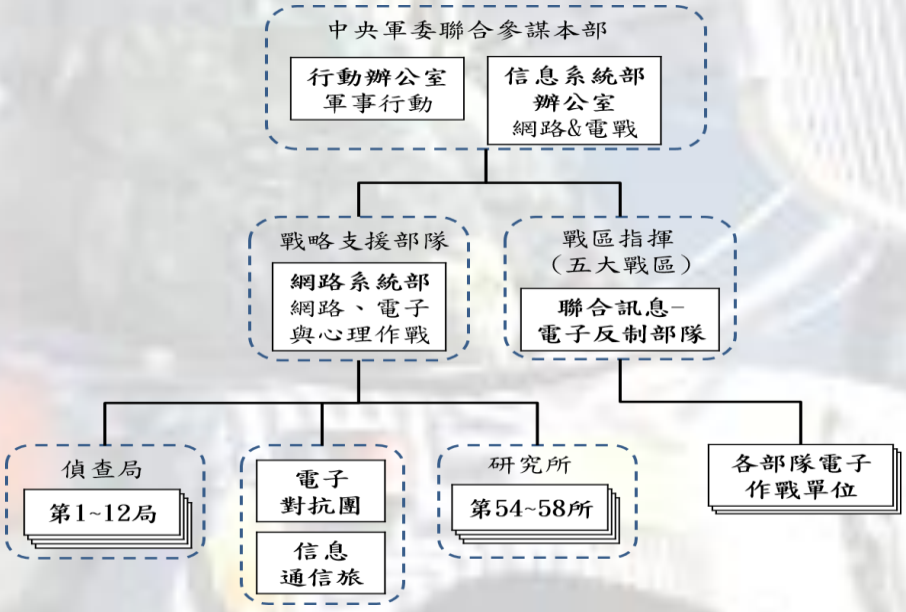
部隊的訓練與裝備，[13]進入攻臺作戰後其指揮架構如圖2。

圖 1 戰略支援部隊編制架構圖



資料來源：作者整理，參考財團法人國防安全研究院，《聯兵旅級部隊電戰裝備運用現況與指管機制之研究》，民國109年12月30日，頁122。

圖 2 共軍網電作戰一體化指揮架構圖



資料來源：作者整理，參考財團法人國防安全研究院，《聯兵旅級部隊電戰裝備運用現況與指管機制之研究》，民國109年12月30日，頁122。

13同註11，頁122。

二、太空電子戰運用及發展概況

中共認為信息戰是獲取主動權並獲得海空優勢必要條件，其資訊封鎖概念可能是設想將跨越太空和網路領域的軍事能力與非軍事性國家權力手段結合起來。其電子戰是現代戰爭不可或缺的組成部分，其電戰策略強調壓制、破壞或欺騙敵方電子設備。潛在電子戰目標包括敵方在無線電、雷達、微波、紅外和光學頻率範圍內操作系統，以及電腦與資訊系統，並透過上述方式以電子戰、網路攻擊和信息戰配合其空中和海上封鎖行動，進一步孤立我國政府和民眾，並控制臺海衝突的國際話語權。[14]

中共航天（太空）企業持續發展，並投入大量經濟和政治資源發展太空計畫，戰略支援部隊航天系統部負責所有共軍太空作戰。儘管中共公開反對太空武器化，但仍在繼續加強其軍事太空能力，同步提高在天基情報、監視和偵察、衛星通信、衛星導航和氣象學以及人類太空飛行與機器人太空探索方面的能力並建立太空站。同時也建立廣泛地面設施，以支持其不斷增長之在軌衛星和相關功能，此外繼續發展對抗太空能力，包括直升式（Direct Ascent）反衛星武器(Anti-satellite Weapon, ASAT)、同軌、電子戰和導能武器，以拒止對手進入太空能力。

為配合其在衛星導航、發射能力以及空間物體監視和識別方面的顯著改善，中共正在發展電子戰能力，例如衛星干擾器、進攻性網路能力和定向能量武器。此外，中共已經展示出複雜，可損害天基技術的在軌行為。中共可能擁有一種旨在打擊低地球軌道衛星運行之地基反衛星導彈，且正在採用更為先進的衛星業務，並同時測試可用於對空任務及太空的兩用技術。[15]

正當低軌衛星「星鏈」在俄烏戰爭中大放異彩的同時，中共同樣在發展「天鏈」系列衛星，可用於通信、導航、中繼等領域，並具備衛星與地面間通聯系統，形成星地網路融合，天鏈速率至少達到了地面4G的通信速率，可供中共享用高速網路，提升整體航天戰力。[16]

中共近年來完成「北斗三號」全球衛星導航系統建置，具備支援其它軍兵種遂行遠海作戰、導彈精準突擊、防空反導等能力，並加速「尖兵」、「天通」、「天鏈」系列等偵察及通信衛星部署，以強化制天、制電磁權優勢。[17]

三、信息結合心理戰，打擊我精神戰力

14同註2，頁24。
15同註12，頁24-25。
16財團法人國防安全研究院，《2021國防科技趨勢評估報告－中共新世代軍事科技評估》（臺北市:五南圖書出版股份有限公司，民國110年12月），頁99-101。
17同註12，頁24-25。

中共透過俄羅斯併吞克里米亞相似的手法，以網路戰部隊結合時事脈動製作假訊息，影響我國政、軍、經、心，特別利用我國民主社會、資訊高度傳播及相關法律漏洞不斷對我國實施混合性威脅，帶動社會輿論風向，企圖影響我國政治和民心。一方面可以對我國人民心理施加刺激和壓力，使其朝預定方向變化，營造成有利於己、不利於敵的心理狀態，從而達到分化瓦解敵人，以小的代價換取大的勝利，另一方面則是可以鞏固己方士氣，企圖達到「不戰而屈人之兵」的心理戰略目標。[18]

另外，中共對我國民間交流方面，將主要目標放在青年人身上，中共當局正在一步步地把過去中華民國對臺灣人的教育思想，從對敵(中共)認知加以洗腦，改變成為兩岸皆屬中國人、中國人不打中國人、兩岸前往民族復興的道路等概念，改變我國民眾思想、認知、認同，從民間形成親共輿論，在無形中進而實現認知作戰的目標。[19]

2022年8月美國聯邦眾議院議長斐洛西訪問團至我國訪問，為此中共透過網軍對我國各地實施駭客入侵，其中就包含了南投竹山鎮公所、臺鐵、統一超商的電視牆均出現了「戰爭販子斐洛西滾出臺灣」等字樣，惡意散布假訊息，且總統府官網及外交部網站等也遭受境外DDos攻擊，造成網站癱瘓，除表達中共當局的不滿外，亦展示中共網路戰能力，威脅意味濃厚。

四、入侵我防空識別區

近年來，中共軍機頻繁逾越海峽中線及其延伸進入西南空域，於2021年逾800餘架次，2022年更高達1,700餘架次。中共利用各式戰機及電偵機等混合機隊，長期入侵我防空識別區亦或利用各式軍演實施共機擾臺，除了宣示主權及武嚇意味外，另一方面是利用電子對抗偵察能力針對我國實施偵察、蒐集、研究我國相關區域的航線、無線電和雷達訊號等參數及各種設施部署，包括軍事基地、重要基礎設施位置等，可視為武統的先期準備。另外，當共軍機群繞臺時，我軍機緊急起飛同時，也有利於共軍掌握我緊急應對措施及戰機相關電子資訊參數。[20]

五、小結

戰略支援部隊成立後，整合航天、電子、網路、心理等各式作戰能量，除傳統陸、海、空軍作戰領域外，皆已納入戰略支援部隊作戰範疇。

(一)特點

18劉文傑，〈淺談中共當前對臺三戰作為〉《裝甲兵季刊》(新竹)，第259期，民國110年3月，頁21-23。
19同註18，頁21-23。
20王逸雲、郭晃男，〈中共軍機繞臺對我國謀略戰之運用與影響－以平、戰時為例〉《陸軍學術雙月刊》(桃園)，第五十五卷第565期，民國108年6月，頁60-61。

1.具備多維作戰能力

共軍因應未來多領域的作戰空間型態轉變及為打贏信息化條件下戰爭，藉戰略支援部隊成軍，將太空、電子、訊息、心理戰等，統一整合為網電一體戰，發展為可隨時藉衛星、網路執行遠距通訊、持續監控敵方部隊動態、蒐集所需資訊等戰略保障力量。戰時發動網電一體戰、心理戰，藉各式電子干擾設備對敵衛星、通信、資訊及雷達等各項指管系統執行多維、全面性干擾、抗干擾作戰，並運用衛星導引遠距精準武器，對重要關鍵資訊節點、雷達設施等實施硬殺破壞，削弱、破壞敵資訊作戰能力，達其制電磁權之目的。[21]由此可知共軍對多領域作戰及跨海武力投射能力已獲得強化。

2.提升聯合作戰效能

共軍執行聯合作戰成敗關鍵在於是否具備安全、可靠及有效的指管系統。藉由戰略支援部隊之網路、情蒐、航天系統，可為指揮官提供即時作戰情資、指揮管制外，並能夠強化其他軍種兵、火力投射效果，實現遠距離的精準打擊目標，同時運用網路及電子攻擊敵人，將網電作戰與火力相結合，以削弱敵網電作戰優勢，進而確保其軍事行動順遂。[22]

(二)弱點

1.指揮機制不明確

共軍軍改後，在「軍委管總、戰區主戰、軍種主建」原則下，奠定戰區主導作戰的方向。戰略支援部隊需要支援戰區執行作戰任務時，是否可完全主導網路、電子戰及衛星之部署及兵力運用，亦或由戰區指導，軍種間如何協調、整合相關資源與任務分配及達成預想之作戰成效仍有待釐清與考驗。[23]

2.聯戰、專業人才不足

軍隊改革須歷經組織、裝備、人才等三個階段，裝備為作戰的工具，人才是作戰之核心，無聯戰、專業人才，相關戰術戰法及裝備的運用，就無法與時俱進，而人才對中共而言實為迫切需求。中共自 2003 年參考美軍實施聯合作戰、網狀化作戰後，才提出一體化聯合作戰理論，於 2010 年才由機械化進展至信息化，組織方面至 2016 年才完成改革。觀察其於 2017 年實施軍事院校改革，就可知共軍的人才並不足以跟上部隊之改革，於是提出了 2035 年實現軍隊現代化，研判中共尚需數年的人才培育，才能滿足部隊需求。[24]

21舒孝煌，〈中共軍改意涵及其影響〉《戰略與評估》(臺北)，第八卷第二期，2017年冬季，頁38。
22朱鈷德、李建鵬，〈中共戰略支援部隊功能發展與對我資訊戰影響之研究〉《陸軍學術雙月刊》(高雄)，第五十七卷第580期，民國110年12月，頁84。
23同註22，頁85。
24同註22，頁85。

網電作戰組編組

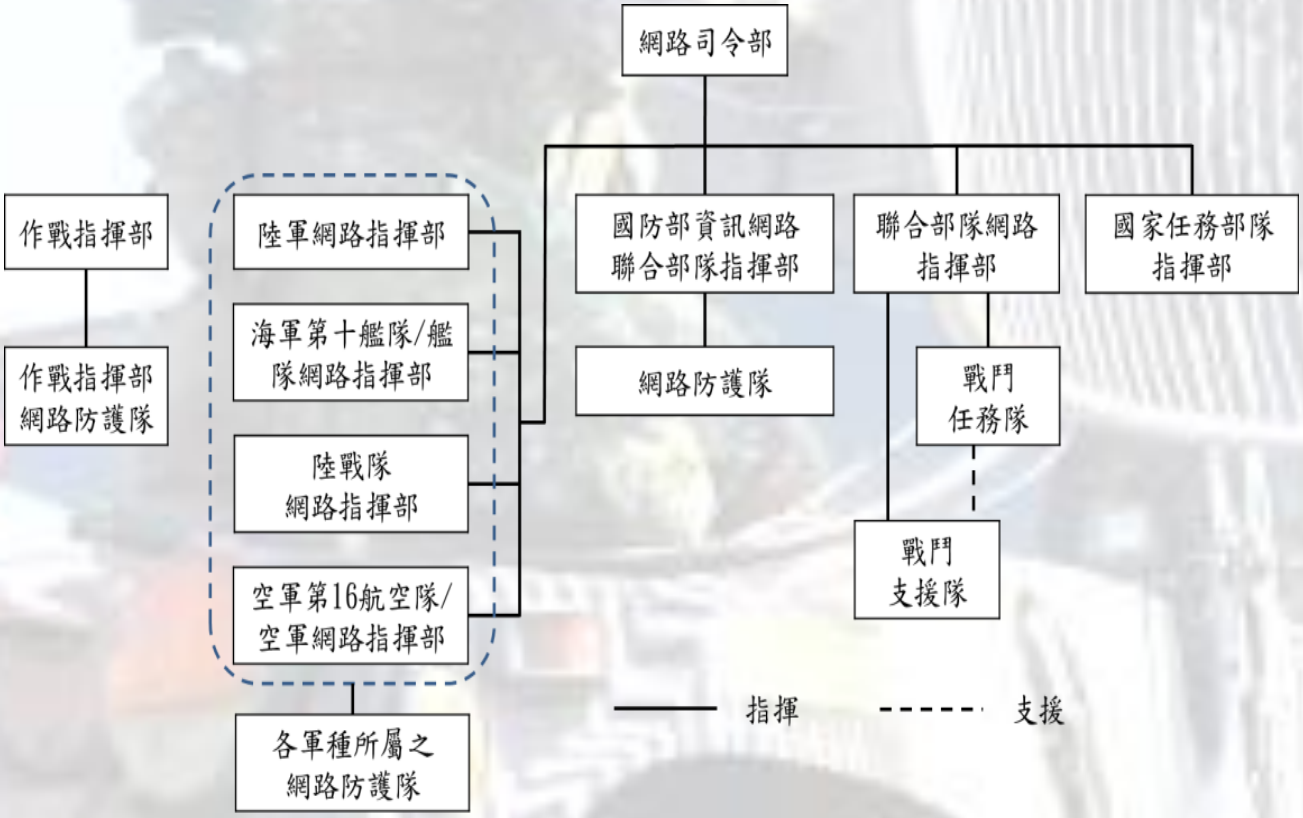
一、美軍編組

美軍已將作戰範圍擴及到陸、海、空、太空、網路及電磁頻譜等多領域作戰。面對作戰型態改變，美陸軍已意識到未來聯合作戰，若無法獲得多領域作戰優勢，將無法獲得戰場優勢。

(一)指揮體系

美軍計有 11 個聯合作戰司令部，其中 7 個為地域型司令部(北方、南方、中央、非洲、歐洲、印太、太空司令部)，4 個為職能型司令部(戰略司令部、特種作戰司令部、運輸司令部及網路司令部)，其中網路司令部統管全軍網路安全、網路作戰指管及電磁頻譜作戰等，網路司令部編制共 133 個網路任務部隊，分別編入直屬網路司令部的國防部資訊網路聯合部隊指揮部、聯合部隊網路指揮部、國家任務部隊指揮部與軍種網路指揮部及區域作戰指揮部(如圖 3)。[25]

圖 3 美軍網路司令部編制及網路任務部隊配屬



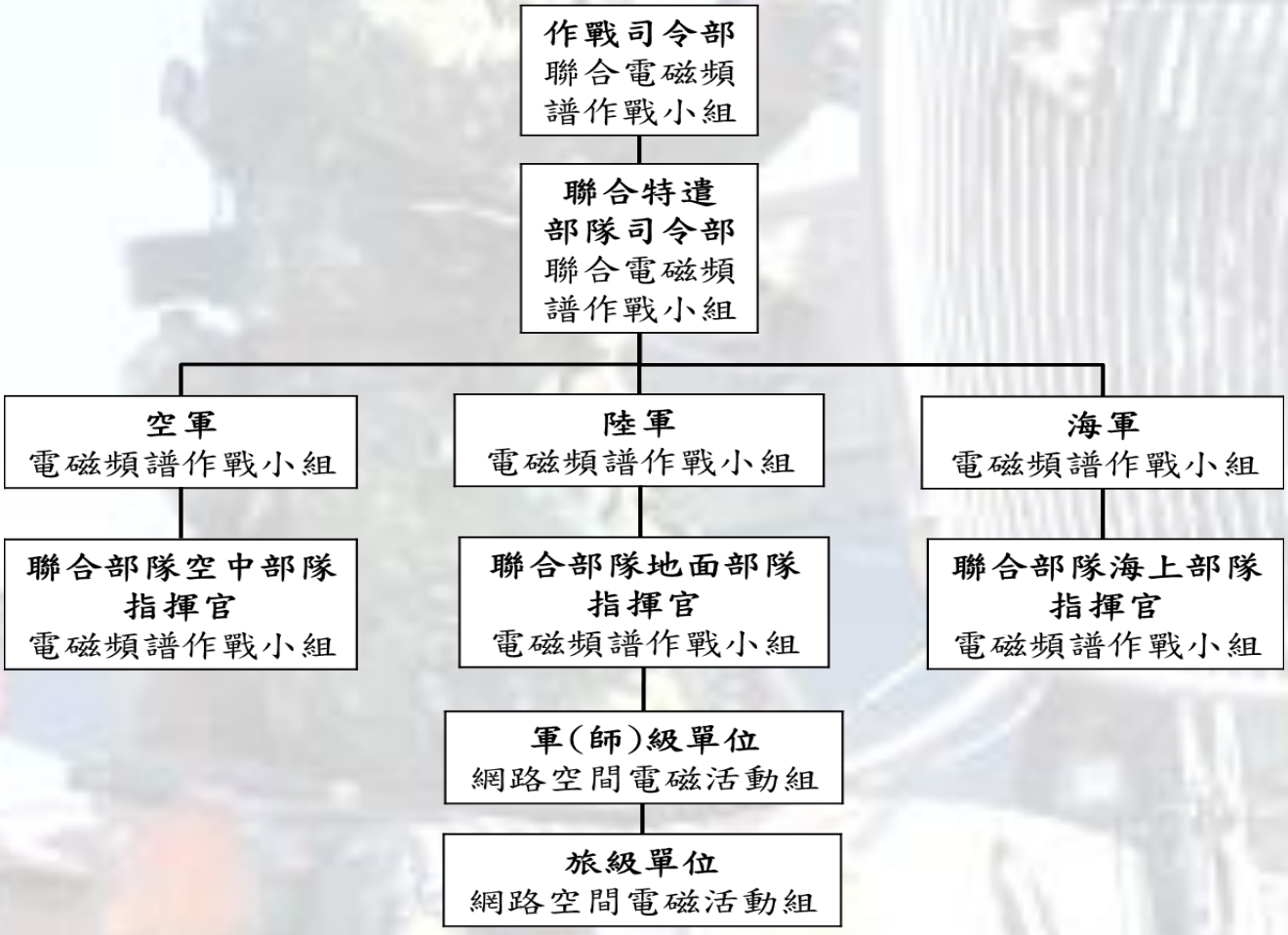
資料來源：作者整理，參考杜貞儀，〈軍文交織的美國網路防護體系〉《國防情勢特刊－網路作戰》(臺北)，第13期，民國110年11月9日，頁16。

25財團法人國防安全研究院，《網路戰與科技發展探討建軍規劃之因應策略》，民國110年12月23日，頁28。

(二)網電作戰體系

美陸軍指揮官為了解網路空間作戰和電子戰對作戰環境的影響，透過網路空間電磁活動組(Cyberspace Electromagnetic Activities, CEMA)來整合陸軍聯合網路空間和電子戰能力。美軍在聯合作戰期間，由聯合特遣部隊司令部或聯合部隊司令部的軍或師級單位，將其頻譜管理負責人與其網路空間電磁活動組結合起來，建立一個電磁頻譜作戰小組(Electromagnetic Spectrum Operations, EMSO)，以支持聯合電磁頻譜作戰小組(Joint Electromagnetic Spectrum Operations Cell, JEMSOC)，其架構圖如圖 4，另美國陸軍網路司令部為強化網路空間電磁活動組，可派員至各層級擴充其編組，強化其網路空間和電子作戰能力。[26]

圖 4 美軍電磁頻譜組織架構圖



資料來源：United States Of America, DEPARTMENT OF THE ARMY 3-12：CYBERSPACE OPERATIONS AND ELECTROMAGNETIC WARFARE, AUGUST 2021,pD-9

26United States of America, DEPARTMENT OF THE ARMY 3-12：CYBERSPACE OPERATIONS AND ELECTROMAGNETIC WARFARE, AUGUST 2021,p3-1~3-12.

而其中網路空間電磁活動組(CEMA)，為編制人員或例行編組，小組成員為網路暨電子戰軍官、網路戰軍官、電子戰技術員、電子戰士官長、電戰士等人員所組成(人員職責如表5)。[27]

表 5 網路空間電磁活動組成員與職責

成員	職責
網路暨電子戰軍官	是指揮官特業參謀，負責整合、協調和同步網路空間和電磁頻譜中的行動。網路暨電子戰軍官負責了解網路空間和頻譜相關政策，以協助指揮官規劃、協調和同步網路空間作業，將可能存在的網路空間和電子戰漏洞及對手能力所帶來的任務風險，向指揮官提出建議
網路戰軍官	網路戰軍官協助網路暨電子戰軍官整合、協調和同步網路空間作戰和電子戰作戰，並提供有關網路空間作戰影響的信息，包括用於向指揮官提供建議的相關交戰規則、影響和限制，將網路空間作戰整合併同步到作戰流程中，並與網路空間電磁活動支援組協調。
電子戰技術官	電子戰技術員是 CEMA 的常駐技術和戰術專家。通過協調、整合及制定和管理敵方電磁作戰序列，並進行更新電磁環境調查和維護。以利削弱對手和敵人對網路空間和電磁頻譜的利用，取得其優勢，並擔任組織內電子戰培訓的認證者。
電子戰士官長	電子戰士官長是網路暨電子戰軍官的高級電子戰顧問。協助網路暨電子戰軍官和網路戰軍官整合、協調和網路空間作戰以及電子作戰。另協助電子戰技術員更新和管理電子戰鬥序列，而電子戰訓練是也是其核心職責，對下屬組織內的成員進行訓練，使其達成網路與電子作戰任務要求。
電戰士	管理及分配給下級單位的電戰裝備和維護電戰資料庫。協助頻譜管理、解決頻率衝突問題，並協助電子戰士官長實施電子戰相關的駐地訓練。

資料來源：作者整理，參考United States of America, DEPARTMENT OF THE ARMY 3-12：CYBERSPACE OPERATIONS AND ELECTROMAGNETIC WARFARE, AUGUST 2021,p3-5~3-12.

27United States of America, DEPARTMENT OF THE ARMY 3-12：CYBERSPACE OPERATIONS AND ELECTROMAGNETIC WARFARE, AUGUST 2021,p3-5~3-12.

網路空間電磁活動支援組是一個來自其他部門的專職人員，以任務編組方式組成。協助網路空間電磁活動組將網路空間作戰和電子戰同步並整合到作戰概念中，[28]其編組成員將根據任務要求而有所不同(人員職責如表 6)。

表 6 網路空間電磁活動支援組成員與職責

成員	職責
情報參謀官	向 CEMA 提供敵情威脅，如作戰環境中網路空間攻擊或電子攻擊的威脅，另將所有高價值目標整合到高效益目標列表中。
通信參謀官	滿足 CEMA 的通信需求，提供有線和無線電的專業知識並監督電磁頻譜運用。針對敵方網路空間威脅特徵及相關能力，提供行動方案建議。
訊息作戰官	將網路空間作戰和電子戰與其他訊息相關能力同步，評估任務風險和部隊風險，以達成指揮官在訊息環境中的目標。與其他軍種或聯合部隊協調訊息相關能力，以彌補部隊的不足。利用網路空間操縱和電子戰手段來支持軍事欺敵。
頻譜管理官	協調組織的頻譜資源，如頻率分配和使用，必要時與上級及友軍協調頻譜使用，並與 CEMA 合作，確保頻譜管理操作與電子戰的整合和同步。
火力支援代表	與情報參謀官合作和管理高效益目標列表、目標選擇、攻擊指導，並將網路空間攻擊、電子攻擊及火力相結合，達成指揮官作戰任務。
法務官	確保網路空間和電子戰遵守適用的政策和法律，並為 CEMA 網路空間運營和電子戰提供法律諮詢。

資料來源：作者整理，參考United States of America, DEPARTMENT OF THE ARMY 3-12：CYBERSPACE OPERATIONS AND ELECTROMAGNETIC WARFARE, AUGUST 2021,p3-5~3-12.

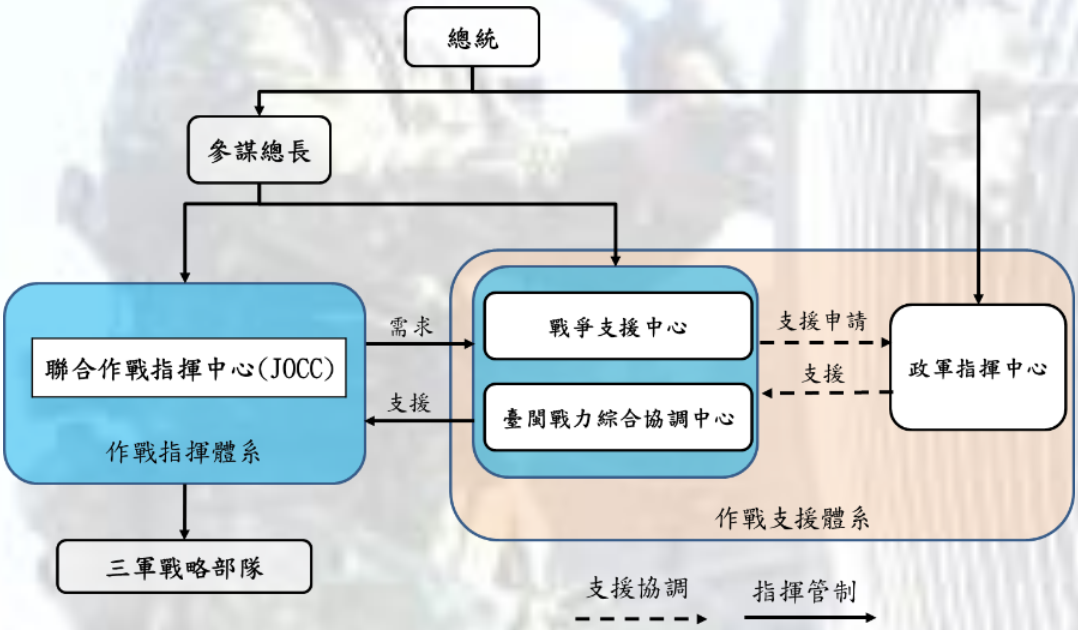
二、國軍編組

(一)指揮體系

28United States of America, DEPARTMENT OF THE ARMY 3-12：CYBERSPACE OPERATIONS AND ELECTROMAGNETIC WARFARE, AUGUST 2021,p3-5~3-12.

國軍區分為「軍令」、「軍政」、「軍備」等三個體系，而聯合作戰權責區分平時整備及戰時執行兩個層級。平時由國防部、參謀本部、各軍種司令部、作戰區（含比照）及作戰部隊，依權責遂行聯戰規劃與整備工作，建立聯合作戰能力，戰時由參謀總長運用聯合作戰指揮機制（聯合作戰指揮中心）直接指揮軍隊；軍政、軍備體系及全民防衛動員署依「功能任務屬性」編成作戰支援協調機構，負責跨部會協調獲取所需全國總力，充分支援聯合作戰任務執行，達成聯合作戰目標(如圖 5)。[29]

圖 5 戰時聯合作戰指揮體系示意圖



資料來源：作者整理，參考張忠銘，《國軍聯合作戰要綱》（臺北：國防部，民國111年8月23日），頁1-12。

作戰區遵循參謀總長「聯戰任務行動要項」，向下發展「聯戰任務行動清單」，並實際執行各項戰訓整備工作及制定聯合作戰計畫。戰時各作戰區、防衛部，依作戰任務設置「次級聯合作戰指揮中心」，比照參謀本部以「建制聯合參謀組織」或採取「單一軍種加強型參謀組織」編設，上承「聯合作戰指揮中心」命令，執行聯合作戰任務，對下有效管制所屬及編配之作戰部隊行動，完成綿密協調作業與統合，發揮聯合作戰指揮功能。[30]

(二)網電作戰體系

29張忠銘，《國軍聯合作戰要綱》（臺北：國防部，民國111年8月23日），頁1-4。
30同註29，頁1-6、1-16。

於戰時成立聯合作戰指揮中心，並於作戰中心成立網電作戰組，主要整合網路戰與電子戰力量與資源，並規劃各網路戰部隊、電子戰部隊運用，協調各軍種共同作戰模式，融入聯合防衛作戰計畫。另與國安會、行政院與民間機構進行情資共享、資安聯防與資源運用，以發揮統合戰力。區分計畫作業計 5 席位(資電作戰官、網路戰計畫官、電子戰計畫官、心理戰計畫官、情報支援官)及部隊管制計 2 席位(網路及電子戰部隊管制官各 1 員)，提供指揮官下達網路暨電子作戰決心之依據，並指揮各作戰區網電小組網路及電子作戰運用。

而作戰區作戰中心以任務編組方式編成網電作戰組，編設作戰、情報(含軍事欺敵)、電戰、網戰、心理戰與實體攻擊等 6 個席位，依指揮官作戰指導、情蒐要項，執行電子暨網路作戰行動並依戰況提供建議，下達指管命令至電子戰部隊，以支援聯合作戰之遂行(各成員職責如表 7)。

表 7 網電作戰組成員與職責

成員	職責
資電作戰官 (兼小組長)	1.掌握綜合情資與作戰共同圖像(Common Operational Picture, COP)，整合小組專業意見判斷，據以提供資電攻擊與防禦之建議。 2.協調作戰區火協機構及各作戰部隊遂行資電作戰作為。 3.掌握各單位資電作戰全般工作之推行。
網路戰計畫官 (兼資安防護)	1.掌握敵網路情資並提供專業判斷，提出運用網路攻、防建議。 2.負責協助各單位資訊網路弱點分析、風險評估及入侵事件掌握處置。 3.協助執行網路心戰作為，以強化部隊精神戰力。
電子戰計畫官 (兼實體攻擊)	1.掌握敵電子戰情資並提供專業判斷，提出運用電子戰攻、防建議。 2.負責管制各單位電子戰執行與管制。 3.負責戰場頻譜運用之建議與電磁干擾之協處與管制
情報支援官 (兼軍事欺敵)	1.依據綜合情資提供情報專業判斷。 2.擬訂情資需求項目，並協調情資之獲得與分析。 3.依戰場情勢提供軍事欺敵建議，並負責欺敵計畫、判斷之撰擬。
心理戰計畫官 (兼媒體、廣播)	1.掌握戰場情勢，提供心理戰結合欺敵作戰措施建議。 2.敵心理戰術作為分析並提供因應建議。
電子戰部隊 管制官	1.負責作戰區內電戰部隊戰況掌握、處置與回報。 2.依據電子作戰計畫與命令進行電子戰作為管制。

資料來源：作者整理

(三)網電作戰流程

由偵搜部隊或電戰偵蒐裝備所蒐集到的敵軍徵候或參數，回傳到情報中心，情報中心依情資分析並結合雷、截情監偵系統實施複式比對、判別敵情後，提供給網電作戰小組判斷是否需採取攻擊作為，若採取攻擊作為時，立即由網電小組召開作戰會議，各席位幕僚及火力協調小組提供軟殺（電子攻擊）或硬殺（火砲攻擊）手段之目標審查結果建議後，由指揮官下達作戰指導並管制各部隊戰果回報。

三、小結(分析)

(一)美、國軍網電作戰小組差異

由上述美軍網電編組可知 CEMA 為編制人員或慣常編組，係固定成員編成，而 CEMA 支援組則為任務編組，會依據任務屬性不同，而編組不同的專業參謀，協助 CEMA 達成網電作戰任務；國軍作戰區以任務編組模式，編成網電作戰小組，其中相關電戰席位由資通電軍派遣擔任(國軍與美軍編組差異對照如表 8)。

表 8 美、國軍編組差異對照表

	國軍	美軍
編組方式	僅電子戰計畫官及電子戰部隊管制官為慣常編組，餘均為任務編組方式實施。	CEMA為建制或慣常編組，僅CEMA支援組採任務編組。
人員編組	小組成員內包含作戰、情報、網電、政戰，無其他專業人員，需橫向協調。	1.CEMA編組人員均為網電專長人員。 2.支援組依任務需求，由各專業人員實施編組，包含作戰、情報、通資、火力、法律等人員。
任務	戰時掌握電子戰、網路戰、心理戰之戰場情勢，透由情報分析，管制相關計畫執行，並與各作業組橫向協調。	CEMA負責平、戰時網電作戰計畫、任務及訓練，餘情報分析、火力支援、心理戰等，由CEMA支援組協助、規劃執行。
綜合分析	1.就編組方式而言：國軍網電作戰小組僅在戰時以任務編組方式編成；美軍CEMA小組為建置人員，在平時需負責駐地訓練及人員考核，戰時則執行相關網電作戰計畫及管制相關作為。 2.就成員編組而言： (1)美軍均為網電專業人員且職責分工明確，國軍則採取各兵科混合編組。 (2)支援組內其他專業人員亦比國軍增加法務官及火力支援代表等。 A.法務官：可提供網路戰國際法－塔林手冊2.0版之相關法規。 B.火力支援代表：視需求可提供火力支援。 3.就任務而言：美軍將網電以外各專業人員納入CEMA支援組，可直接實施支援，橫向協調過程較精簡。	

資料來源：作者整理。

(二)專業人才不足，較難發揮作戰效能

1.在運用各類型部隊前，應先對部隊的裝備性能、能力限制要有基本認識及瞭解，在瞭解部隊能力後，針對部隊屬性，發展出該類型部隊之戰術戰法，才能有效運用該類型部隊。而現今作戰區中推測僅有通資組長及電戰官對電戰部隊的裝備及部隊運用較為瞭解，因此網電作戰小組之電子戰計畫官是否能明確瞭解指揮官企圖並在作戰各階段，針對電戰部隊轉換階段時機、部隊位置轉移及攻擊手段等，向指揮官建議電戰部隊運用，使作戰區指揮官運用電戰部隊發揮其完整戰力，支援戰鬥部隊達成作戰任務。

2.作戰區網路戰以網路防護為主，以資通聯隊或聯兵旅資訊組為主體，組成電腦緊急應變小組(Computer Emergency Response Team, CERT)，負責掌握網路攻擊態樣，做好網路安全防禦、處理網路安全緊急事件等。在資安攻防演練中，通常以弱點掃描或不開啟來路不明郵件等方式實施演練，然人員素質在眾多因素(如學歷、任務、政策等)的影響下，其網路戰專業能力恐無法與資通電軍網路戰聯隊相比。

(三)電戰部隊多以程序演練，無法驗證成效

資通電軍下轄的電戰中隊僅於重大演訓(如三軍聯訓、漢光演習等)配合陸軍實施操演，而在操演時囿於避免影響演訓部隊的指管通聯、實施電子干擾會影響民間用頻及避免遭敵或他國電偵機及船偵獲國軍電戰參數等因素，因此電戰部隊配合演練時，多以偵蒐系統為主，干擾系統多以程序演練，無法驗證其干擾實際成效。

(四)心理戰缺乏攻勢作為

心理戰是「攻心」作為，「三戰」之中「心理戰」與「輿論戰」之界線，著實不易分明。「心理戰」與「輿論戰」通常是兩者結合著實施，我國軍長年面對中共「心理戰」威脅，而中共將原「心理戰」結合現代化資訊與科技，發展為「資訊化心理戰」，也就是將傳統的「心理戰」併隨著新載體、內容及技術交織演進，發展成運用網路戰方式對我實施心理戰等攻擊。[31]因此我國軍心理戰多數以心防為主，如對假訊息澄清、產製戰場快報、文宣海報、主官精神講話及心防影片等，皆為從精神意志去鞏固我軍官兵的心理與行為，而心理戰攻勢作為多以心戰喊話車、心戰傳單、心戰文宣品打擊、轉化敵人心理，削弱其戰志，未能結合現代高科技技術實施心戰攻勢作為。

31曾雅琦，〈「後疫情時代」中共對臺「認知作戰」威脅淺析〉《海軍學術雙月刊》(臺北)，第56卷第4期，民國111年8月1日，頁125。

結論

電磁戰與網路戰在全方位作戰中可協助我們取得優勢，但要能夠獲得可觀效益，卻非得具備高深而廣泛之專業知識不可。它的出現已經改變我們原本對網路作戰之思維，讓我們不得不用更寬廣、更前衛的看法來面對它，要在網路與電磁作戰這個領域贏得勝利，不但要在專業技術方面有嫻熟技能，還必須熟知電子物理學、複雜電腦網路行為，以及如何將這些知識運用到作戰領域中的戰術、作戰、戰略等各個層面。應付現階段複合式作戰環境及與日俱增之網路駭侵威脅。

就美軍而言，戰爭型態已演變為多領域作戰，且已朝著電磁頻譜結合網路作戰優勢邁進，建立相關電磁頻譜作戰及網路戰等相關聯戰準則，並將電磁頻譜作戰及網路戰系統由上而下完成垂直整合，這有助於電磁頻譜作戰及網路戰，可將作戰單位、人員、組織做一系統的規劃，並且靈活運用，創造有利態勢。而國軍作戰區網電作戰小組，更應加強人才培育、專業知識等面向，使國軍可充分發揮本身優勢，克敵致勝。

建言

為確保在有限國防資源條件下，依序完成網電建軍整備與戰力發展，秉「資安即國安」、「國防自主」、「整合情資」、「防護為先」、「快反先制」的用兵指導創造國軍優勢網電作戰環境，[32]以向上支持戰略構想，向下指導軍種執行戰力整建，逐步精進網電戰力，達成戰略目標，相關建言如下：

一、擴編網電作戰組

(一)作戰區網電作戰小組編組方式應效仿美軍，建議採正式編組。因採任務編組方式，在戰時各編組成員可能會兼任其他各中心職務，導致任務重疊，致定位不明確及業務無法整合，進而喪失其原本組織之功能。

(二)我陸軍建置戰術型偵蒐及干擾車，主在偵蒐、干擾及欺騙敵各式通信指管系統，因此網電作戰小組成員應將軍團電戰官編入，輔助電子戰計畫官，整合兩軍的電戰裝備，使電子戰配置與運用更加靈活及全面，將可大幅提升部隊戰力。

(三)因應旅級部隊即將成立通資科及通資連下轄的電戰組，應效仿美軍於旅級成立網電作戰小組，通資科除科長以外成員均納入網電作戰小組，亦或重新

32同註6，頁1-12。

檢討旅級通訊中心編組，強化旅級網電作戰能力。

二、培育網電專業人才、精進網電作戰能力

(一)網電專業人才培育應先軍後民，官兵先於各兵監學校取得相關專長後，鼓勵官兵積極考取民間證照(丙、乙級)及國際網路安全證照(Cisco)，以民間證照輔助專業認證，並予以相關補助，廣儲人才，不僅可以增強國軍基層網電作戰能力，於人員離退後，更可轉用於政府部門或民間資安公司，以利國軍奪取網路戰主導權。

(二)於漢光演習期間，由網電作戰小組情報參謀之敵情依據，驗證網電作戰小組縱向指揮、橫向協調，並結合網路、電子戰、心戰及火力部隊實施綜合演練，落實網路防護以及於火力發揚前、後實施心理戰及電子戰攻擊作為，強化人員指揮職能及作戰效能。

(三)建議將通資、網路、電子戰幹部，不分軍種納入相互交流機制及交織歷練，透過不同系統運用及部隊實務經驗，使幹部對網電作戰運用有更深刻的瞭解，俾熟悉網路空間、電磁頻譜等多維戰場型態上搶占優勢。

(四)恢復電子戰巡迴講習，結合軍團軍官團教育，並請各旅級電戰官共同參加，藉由電戰巡迴講習，強化通資電兵科及構築各兵科對電子戰基礎概念，瞭解電戰部隊特性及各時期各式電戰裝備運用。納入陸軍戰術戰法，建立聯合作戰基本概念，並透過各式演訓實施驗證，於訓後回顧檢討編組、裝備技術、運用戰術等反覆修正，確保戰力發揮。

三、落實實戰化訓練及完善準則、訓場

(一)鑒於陸軍即將建置電戰裝備，通信偵蒐、干擾為不同屬性之電戰裝備，就作戰運用而言，偵蒐為電子情資蒐集手段，為情報工作之一環，應受「情報部門」管制運用；干擾則為電子戰軟殺手段，與火力硬殺手段同屬攻擊性質，應受「作戰部門」或「火協中心」管制運用。建議我陸軍應發展相關網電之準則及作業程序，使單位有所依循，並研究敵網電裝備之特性與限制，發展有效克敵之戰術戰法，確保我網電優勢及部隊戰力發揮。

(二)透過人員持續訓練及裝備效能的驗證，才可以提高人員專業素質和作戰能力。而新式電戰裝備撥發後，可改變以往電子戰防護訓練採「狀況模擬」或「裝備空操」演練方式，調整為「實戰化」干擾方式。對部隊實施通信制壓，訓練部隊通信手段臨機調整、網路頻率變換及指管中斷應變機制等通信戰術作為，同時藉演訓驗證各單位通資電應變計畫以及偵蒐、干擾指管作業流程的適切性與可行性，從中發掘問題，透過訓後回顧實施反覆修正，並可作為年度戰術戰法研究及後續準則編撰之參據。

(三)建立電子戰專用訓練場，模擬戰場複雜電磁環境景況，以兩軍對抗方式，實施實戰化模擬訓練，採無預警方式，磨練裝備與人員，同步驗證雙方「電子戰攻擊」與「電子戰防護」能力，並可務實提升我電子防護及3R[33]的認知與應變能力，找出其中缺點加以改進，使其成為有效戰力。

四、心理戰與網路戰融合，創造攻勢防禦

我國軍雖以防衛作戰為主，惟心理戰部分可從「攻勢防禦」做思考，例如透過心戰大隊和網路戰聯隊等單位合作，由政戰部門針對中共情勢進行研判，研擬中共民眾之相關新聞、觀點等訊息，影響中共輿情，並透過資通電軍將進行網路戰和假訊息等攻勢，藉此干擾中共，以分散中共對臺「三戰」的力道。[34]

參考文獻

一、官方文件

(一)財團法人國防安全研究院，《聯兵旅級部隊電戰裝備運用現況與指管機制之研究》，民國109年12月30日。

(二)財團法人國防安全研究院，《網路戰與科技發展探討建軍規劃之因應策略》，民國110年12月23日。

(三)財團法人國防安全研究院，《中共對兩岸交流之「三戰」新攻勢與我對應策略》，民國108年。

(四)Joint Chief of Staff, Joint Publication 3-85：Joint Electromagnetic Spectrum Operations,May 20, 2020。

(五)Joint Chief of Staff,Joint Publication 3-13：Inform Operations,November20,2014。

(六)United States of America, DEPARTMENT OF THE ARMY 3-12：CYBERSPACE OPERATIONS AND ELECTROMAGNETIC WARFARE, AUGUST 2021。

二、書籍

(一)財團法人國防安全研究院，《2020國防科技趨勢評估報告》(臺北市：五南圖書出版股份有限公司，民國109年12月)。

(二)財團法人國防安全研究院，《2021國防科技趨勢評估報告－中共新世代

33 3R為國軍反敵電子干擾作業步驟之簡稱，分別為辨認干擾(Recognize Jamming)、報告干擾(Report Jamming)、透過干擾工作(Read Through Jamming)，辨認干擾由操作人員判別機內或機外、自然或人為、無意或蓄意之干擾；報告干擾則是一旦遭受干擾，應立即將遭受干擾情形，確實且詳盡報告上級，以便採取各項有效措施；透過干擾工作則為遭受干擾時，應利用各種手段持續保持通聯，使敵誤以為干擾無效，進而放棄干擾。

34 財團法人國防安全研究院，《中共對兩岸交流之「三戰」新攻勢與我對應策略》，民國108年。頁88-90。

軍事科技評估》(臺北市:五南圖書出版股份有限公司，民國110年12月)。

(三)國防部，《中華民國108年國防報告書》(臺北：國防報告書編纂委員會，民國108年9月)。

(四)張忠銘，《國軍聯合作戰要綱》(臺北：國防部，民國111年8月23日)。

(五)林予令，《國軍聯合作戰網電教則》(臺北：國防部，民國111年12月8日)。

(六)張雪光，《陸軍作戰要綱》(桃園：國防部陸軍司令部，民國112年1月7日)。

三、期刊

(一)黃郁文，〈淺析俄羅斯「網路戰」–以2022年「烏俄戰爭」運用為例〉《海軍學術雙月刊》(高雄)，第56卷第4期，民國111年8月1日。

(二)杜貞儀，〈軍文交織的美國網路防護體系〉《國防情勢特刊－網路作戰》(臺北)，第13期，民國110年11月9日。

(三)舒孝煌，〈中共軍改意涵及其影響〉《戰略與評估》(臺北)，第八卷第二期，2017年冬季。

(四)劉文傑，〈淺談中共當前對臺三戰作為〉《裝甲兵季刊》(新竹)，第259期，民國110年3月。

(五)朱銈德、李建鵬，〈中共戰略支援部隊功能發展與對我資訊戰影響之研究〉《陸軍學術雙月刊》(桃園)，第五十七卷第580期，民國110年12月。

(六)曾雅琦，〈「後疫情時代」中共對臺「認知作戰」威脅淺析〉《海軍學術雙月刊》(臺北)，第56卷第4期，民國111年8月1日。

(七)王逸雲、郭晃男，〈中共軍機繞臺對我國謀略戰之運用與影響－以平、戰時為例〉《陸軍學術雙月刊》(桃園)，第五十五卷第565期，民國108年6月。

四、網路：

(一)錢高陞，<歷代戰爭中電子戰史實與評析>，https://top81.ws/show.php?f=6&t=107956&m=403606，西元2003年4月30日，(檢索日期:2023年1月4日)。

(二)學史泛舟，〈信息化戰爭概述〉《知乎-國防教育》，2020年12月27日，https://zhuanlan.zhihu.com/p/339819714，檢索日期：2023年8月3日。

作者簡介

温宗毅中校，國防大學陸軍指參學院111年班 。經歷：排長、連長、通信官；現職為陸軍通信電子資訊訓練中心學員生大隊大隊長