



中共網電一體戰發展與我因應之道 ——以陸軍通資電部隊為例

作者簡介



張智嘉少校，國防大學理工學院102年班、陸軍通信電子資訊學校正規班107年班、國防大學陸軍指參學院113年班；曾任排長、連長、通信官、營參謀主任、研究教官，現任國防大學陸軍指參學院114年班少校學官。



李景民中校，陸軍官校93年班、國防大學陸軍指參學院106年班；曾任排長、連長、後勤官、作參官、營長，現任國防大學陸軍指參學院戰術組中校教官。

提要

- 一、共軍認為制資訊權、制電磁權是未來戰爭的致勝關鍵，2015年中共軍事改革之後成立戰略支援部隊，後續更在2024年4月19日宣布將戰略支援部隊調整結構為軍事航天部隊、網絡空間部隊、信息支援部隊及聯勤保障部隊等新兵種結構布局，使其能在支援其他軍種作戰之外，同時能獨立進行太空、網路、電子等領域的作戰。
- 二、我國雖於2016年成立資通電軍，負有統籌全軍資通系統、網路戰和電子攻防之任務，現今軍事研究、期刊、學術論文等文獻資料，大多探討網絡空間部隊與我國資通電軍對等軍事層級、戰術戰法、能力、限制及特、弱點，未見對我陸軍地面部隊的威脅。
- 三、本研究聚焦在聯合國土防衛階段，共軍網絡空間部隊運用網電一體戰術戰法對陸軍通資電部隊造成之威脅，最終透過對共軍網路戰及電子戰的探討

研析，對照陸軍通資電部隊現況與能力，提出精進與建議，藉以提高對共軍網電一體戰因應作為。

關鍵字：網路空間、電磁頻譜、網電一體戰、網路戰、電子戰

前言

2015年中共軍事改革之後，除成立陸軍指揮機構、建立聯合作戰指揮機制、火箭軍編成之外也成立戰略支援部隊，後續更在2024年4月19日宣布成立信息支援部隊，¹這次改革後，中央軍委領導指揮下的陸、海、空及火箭軍等軍種外，將戰略支援部隊調整結構為軍事航天部隊、網絡空間部隊、信息支援部隊、聯勤保障部隊等兵種的新兵種結構布局，²使其能在支援其他軍種作戰之外，同時能獨立進行太空、網路、電子等領域的作戰，對我國威脅大幅提升。

近年共軍以對臺作戰為基礎，進行各項實戰化軍事演訓，除強化對臺作戰能力外並進行區域拒止他國軍力介入臺海，亦藉三棲聯合登陸演訓，驗證各項作戰計畫，加大對臺海戰役軍事準備，並視區域情勢及兩岸關係變化，進行針對性軍事演

訓，就其通資電作戰能力而言，研判共軍已具備對我電子攻擊能力，運用干擾或遮斷方式，對我通信指管效能產生局部影響。另結合網軍之全球網路攻擊，潛伏於我國關鍵基礎設施內，於關鍵時刻實施破壞並影響軍事裝備運作，以支援對臺作戰。³

國軍雖依參謀本部組織法，於2016年成立資通電軍，負有統籌全軍資通系統、網路戰和電子攻防之任務，並負責全軍頻譜資料庫的管理、管制、運用、規劃與建議，然其特性屬戰略層級，對聯兵旅戰術層級的作戰單位在網路及電子作戰及戰術上的需求，恐難及時提供發展建議、協助規劃作戰單位建立防護及備援手段。

現今軍事研究、期刊、學術論文等文獻資料，大多探討戰略支援部隊(2024年4月19日調整為軍事航天部隊、網絡空間部隊及信息支援部隊)與我國資通電軍對等軍事層級、戰術戰法、能力、限制及

1 新華網，《中國人民解放軍信息支援部隊成立大會》，<http://cpc.people.com.cn/BIG5/n1/2024/0419/c64094-40219693.html>，檢索日期：2024年4月22日。

2 中華人民共和國國防部，《中國人民解放軍形成新型軍兵種結構布局》，<http://www.mod.gov.cn/gfbw/xwfy/16302080.html>，檢索日期：2024年4月22日。

3 中華民國國防報告書編纂委員會，《中華民國112年國防報告書》(臺北：國防部，2023年)，頁38、39。



特、弱點，同時信息支援部隊就其軍改前組織編裝，研判為前戰略支援部隊的直屬信息通信基地(61001部隊)，⁴其主要下轄分布於中國各地的信息通信團、通信旅及電波通信單位，也將負責國防光纜的維護，其類型與我資通電軍資訊通信聯隊性質類似，其任務為統籌網絡信息體系建設運用的關鍵支撐，研判不執行網路戰及電子戰等任務，⁵本次也不納入探討，對此本研究聚焦在聯合國土防衛階段，共軍網絡空間部隊運用網電一體戰術戰法，對陸軍通資電部隊造成之威脅，最終透過對共軍網路戰及電子戰的探討研析，對照陸軍通資電部隊現況與能力提出精進與建議，藉以提高對共軍網電一體戰因應作為。

共軍網電一體戰發展現況

一、軍事體制改革

(一)緣起

1990、2003年兩次波斯灣戰爭，

中共見證美軍優異的聯合作戰搭配與即時且高效率資訊傳遞，憑藉掌握資訊權及電磁權，精準導引各式導彈打擊敵政治中心、防空陣地，以及指、管、通、情系統，打敗當時號稱百萬雄師的伊拉克軍隊。此戰役不僅讓世界見證第二次世界大戰以來人類戰爭型態的劇變，也讓共軍意識到傳統的人海戰術與舊式武器已無法與新時代戰爭接軌，⁶1999年中共學者喬良、王湘穗提出超越傳統戰爭手段的「超限戰」，資訊無國界、手段無所不備且決戰於無形，傳統戰爭與非戰爭的劃分、軍事與非軍事的領域界線都已產生質變且模糊化。⁷

習近平於2012年提出「強軍目標」的軍隊指導思想與方針，針對國防及軍隊建設深化改革，後續依「軍委管總、戰區主戰、軍種主建」原則，針對軍隊體制實施改革，⁸2017年習近平在中共十九次全國代表大會中修正三步走的三階段基本目標為「2020年基本實現機械化並在信息

4 中國人民解放軍戰略支援部隊信息通信基地，《維基百科》，<https://zh.wikipedia.org/zh-tw/%E4%B8%AD%E5%9B%BD%E4%BA%BA%E6%B0%91%E8%A7%A3%E6%94%BE%E5%86%9B%E6%88%98%E7%95%A5%E6%94%AF%E6%8F%B4%E9%83%A8%E9%98%9F%E4%BF%A1%E6%81%AF%E9%80%9A%E4%BF%A1%E5%9F%BA%E5%9C%B0>，檢索日期：2024年4月22日。

5 人民網，《新成立的信息支援部隊是一支什麼樣的力量？》，<http://politics.people.com.cn/BIG5/n1/2024/0420/c1001-40220035.html>，檢索日期：2024年4月22日。

6 蔡昌言、李大中，〈不對稱戰爭相關理論及其應用於中國對臺戰略之研析〉《遠景基金會季刊》，第8卷第3期，2007年7月。

7 超限戰，《維基百科》，<https://zh.wikipedia.org/zh-tw/%E8%B6%85%E9%99%90%E6%88%98>，檢索日期：2024年1月5日。

8 王聖元，〈中共戰略支援部隊之研究〉《砲兵季刊》，2020年12月，第191期，頁69。

化建設取得重大進展；2035年達成基本實現國防與軍事現代化；2050年將共軍建構成世界一流軍隊」，⁹更加顯見共軍為因應現代戰爭而去不斷作出調整與改革。

2019年中共《新時代的中國國防白皮書》中提到網路空間是國家安全的關鍵領域，並指出，戰略支援部隊是「新質作戰能力的重要增長點」，即可理解及支撐，共軍的新質作戰能力就是網路戰及電子戰能力，可見共軍戰略支援部隊的發展重點為網路空間及電磁頻譜，¹⁰基於科技進步、戰史例證以及中共領導人的政策走向，中共軍隊正著力發展網路戰和電子戰。

(二)發展

共軍2015年底前太空、網路、電子戰等單位，均為按偵察、防禦、攻擊等任務類型編組，2015年底起中共實施軍事改革成立戰略支援部隊，將太空、網路、電子等領域的作戰支援單位整合後成軍，其中統合原聯合參謀部網路電子各局、總參情報部技術偵察部和電子對抗部和總參

裝備部的一部分，研判整合偵蒐、防護及攻擊等過去分散在各部隊網路戰及電子戰能力，並直接由中央軍委管轄依令支援各戰區的新型作戰力量，¹¹然在2024年4月19日宣布將戰略支援部隊調整結構為軍事航天部隊、網絡空間部隊、信息支援部隊及聯勤保障部隊等新兵種結構布局(其組織架構研判如圖1)。

共軍組織改革目的是要能部署一支類似美軍的多領域聯合部隊，以有效應對各種可能的事件，包括對我國的應急作戰。從長遠來看，該改革將建立起更強大的戰力，並能在多個領域進行聯合作戰。例如，東部戰區將可以整合陸、海、空軍及火箭軍部隊進行聯合訓練與作戰，且能獲得網絡空間部隊的支援。該部隊在進行網路戰及電子戰等非傳統領域作戰時具有關鍵性，這可能對我國安全構成更大的威脅。¹²

二、網電一體作戰構想

依中共國防三步走戰略發展進程，2020年時要完成基礎信息化建設，美國國

9 中華人民共和國國防部，〈跨越，向著世界一流軍隊〉，http://www.mod.gov.cn/big5/jmsd/2018-%2011/14/content_4829377.htm，檢索日期：2024年1月5日。

10 中華人民共和國國防部，〈《新時代的中國國防》白皮書全文〉，http://big5.www.gov.cn/gate/big5/www.gov.cn/zhengce/2019-07/24/content_5414325.htm，檢索日期：2024年1月6日。

11 朱鎰德、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〉《陸軍學術月刊》，2021年12月，第57卷第580期，頁69、70。

12 Joel Wuthnow, "What Do China's Military Reforms Mean for Taiwan" ((Joint Force Quarterly, 4th Quarter/2016), pp.63~65.

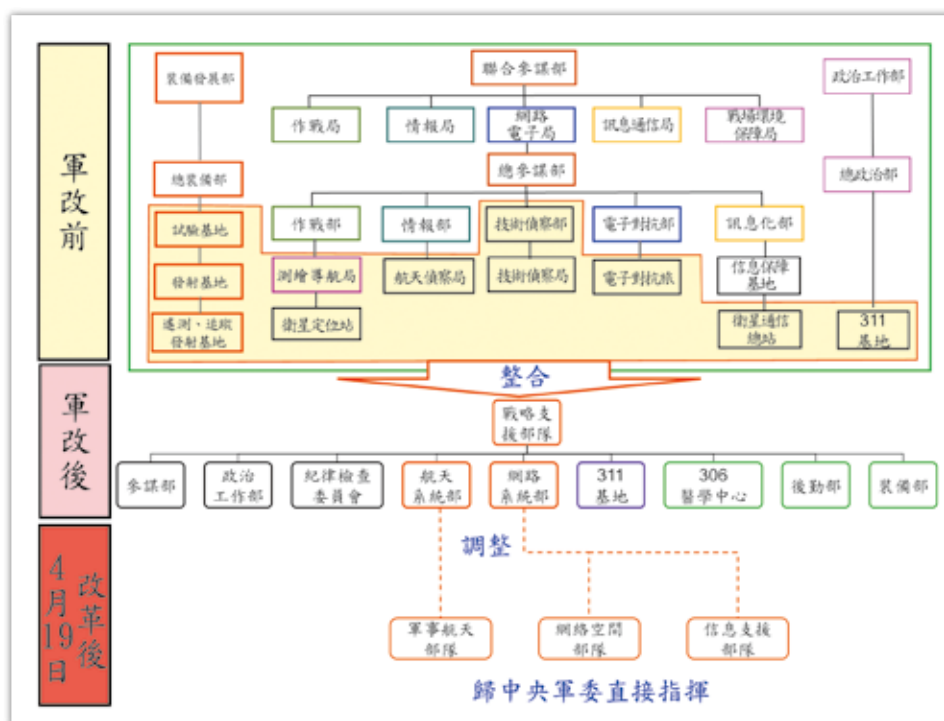


圖1 共軍編制研判圖

資料來源：1.朱銘德、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〉《陸軍學術月刊》，2021年12月，第57卷第580期，頁70。
2.作者整理。

防部也已於2022年「中國軍力報告」中強調共軍在網路空間及電磁頻譜空間中具備制資訊權及制電磁權能力，戰術戰法採網電一體作戰模式，對我網路空間、電磁頻譜平時潛伏、偵蒐相關參數，戰時運用各式手段制壓、癱瘓我國軍指管監偵系統，達到影響戰力發揮之戰略目的。¹³

網電一體戰是指綜合運用電子戰和網路戰手段，對敵指揮、管制、通信、資訊及情監偵系統進行的一體化攻擊，其目

的是奪取網路空間和電磁頻譜的主動權，共軍進入攻臺作戰指揮後，網路空間部隊負責戰略網軍及電子部隊指揮並支援五大戰區，戰時國土防衛階段，對我通資電部隊危害最大就屬網路空間部隊及其管制網路戰及電子戰單位，後續針對上述單位網路戰及電子戰能力深入探討及研析(指揮架構如圖2)。

三、網路空間部隊作戰效能

(一)網路戰定義

係指網路空間中所進行的衝突或行動，包括敵我雙方使用的電腦病毒攻擊、硬體摧毀、認知作戰等手段。對敵方重要資訊與網路系統進行干擾、摧毀、破壞或控制，藉此影響敵對國家基礎設施與重要軍事機構；同時也會對己方相關聯之重要機構實施網電防禦，免於遭受敵方類似行動之影響，¹⁴也因為如此，「制資訊權

13 美國國防部，《中共軍力報告》，2022年OFFICE OF THE SECRETARY OF DEFENSE Annual Report to Congress Military and Security Developments Involving the People's Republic of China 2022, p.68。

14 都世民，《看不見硝煙的格鬥》(北京：國防大學出版社，2000年)，頁190。

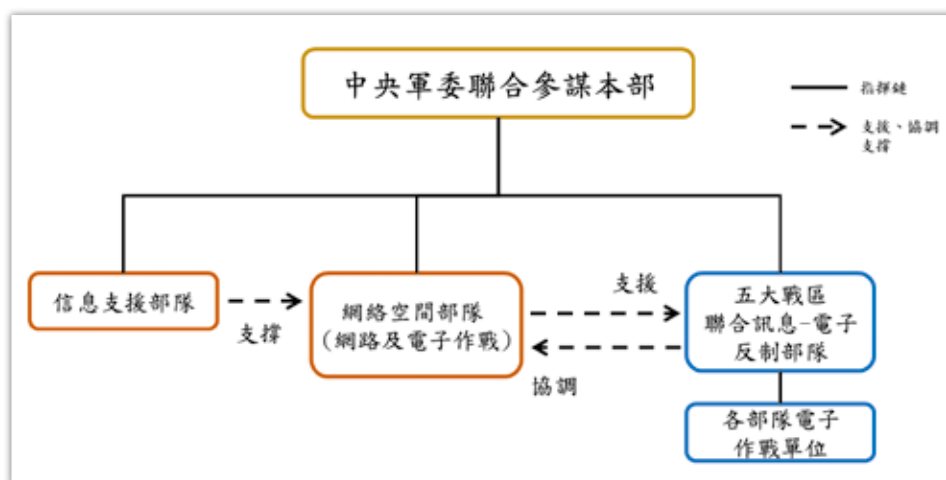


圖2 共軍網電一體戰指揮架構圖

資料來源：1.Joh.Costell.an.Jo.McReynolds.China'.Strategi.Suppor.Force..Forc.fo..Ne.Era(Washington.Nationa.Defens.Universit.Press.2018).p.34.

2.作者整理。

的行動，更可以透過阻斷對方運用網路空間的能力，癱瘓其關鍵基礎設施。共軍網路空間部隊整合原分散在各部門的網路戰能力，且偕同民間組織於網路空間中練兵，已具備各類型網攻手法，對我國政府機關、重要關鍵基礎設施及資通訊產業構成

」的出現也成為繼制海權、制空權、制天權後國際競爭的重點領域。¹⁵

(二)網路戰任務及能力

網路空間部隊負責共軍在網路空間的攻擊與防禦任務，整合過去負責監聽、偵察的總參謀部技術偵察部(局)以及負責網路攻擊與防護的聯合參謀部網路電子局，故軍改後網路空間部隊具備偵蒐、攻擊及防護等過去分散在各部的能力，¹⁶後續於2024年4月時調整為網路空間部隊，隸屬中央軍委直接指揮。

網路戰成為影響現代戰爭中勝負的關鍵，其攻擊程度差別取決於不同目的，可能是潛伏或情蒐，也可影響目標

威脅。

網路空間部隊發動與網路空間攻擊的方式，主要有入侵目標系統植入惡意程式、事先針對目標(對象)蒐集相關情資尋找突破口，或者藉由事先偵獲的系統或軟體漏洞直接攻擊破壞系統等手段(如表1)。

(三)電子戰定義

「電子戰」(Electroni.War)是現代戰爭的一種攻擊方式，自從電磁波應用在軍事，電子戰也就自此而生，隨著資訊技術及高科技武器裝備發展和投入戰場，制電磁權已成為重要的戰略目標，奪取制電磁權是拉開現代戰爭的序幕，它是集電子

15 Dennis F. Poindexter著，國防部譯，《中共資訊戰》(The Chinese Information War)(臺北：五南出版社，2021年10月)，頁30～35。

16 尹俊傑，〈網路戰 漢和：共軍駭客部隊增加〉《中央社》，2016年1月4日，<https://www.cna.com.tw/news/acn/201601040303.aspx>，檢索日期：2024年1月9日。



表1 網路戰手段

手段	行動	目標
網路釣魚	此種手段為社交工程的一種，透過通訊軟體方式騙取目標(對象)的訊息(個人帳號及密碼)。此種手段常透過電子郵件、假網站或社群媒體等各種平台。	特定用戶
勒索軟體攻擊	攻擊者使用勒索軟體將目標(對象)文件加密，並威脅將文件永久刪除或洩露，然後要求支付贖金來解鎖這些文件。	特定用戶
惡意軟體	包括特洛伊木馬、間諜軟體等病毒，攻擊者使用這些軟體在目標(對象)的設備上執行惡意操作，例如竊取資料、控制系統或加密文件。	資訊設備、公共(關鍵)基礎設施
零時差攻擊	零時差攻擊是指攻擊者利用廠商已知但尚未修補的漏洞入侵系統，稱為零時差。	資訊設備、公共(關鍵)基礎設施
進階持續性滲透攻擊	透過長期社交工程，配合病毒或是其他手段，直至攻擊目的達成，此種攻擊預先針對目標(對象)進行長期偵蒐及分析，掌握動態資訊，再對其發動客製化之攻擊，過程耗時長、多樣化且隱密，是未來資安攻擊趨勢。	特定用戶
分散式阻斷服務攻擊	利用大量電腦同時連線目標(對象)，藉由傳送過量封包阻塞網路頻寬，使系統負荷過大而無法正常運作，此種攻擊目的是使目標(對象)無法正常提供服務。	特定用戶、資訊設備、公共(關鍵)基礎設施

資料來源：1.孔德廉，〈紅色網戰：中國駭客組織發起網路攻擊鏈，臺灣百處基礎設施如何防備？〉《報導者》，2023年8月31日，<https://www.twreporter.org/a/prochina-hackers-cyberattack-taiwan-critical-infrastructure>，檢索日期：2024年6月9日。

2.作者整理。

戰支援、電子攻擊和電子防護三大功能的現代化作戰手段，攻勢取向的電子戰是掌握制空權、制海權、制電磁權乃至於戰爭致勝的前提與基礎。¹⁷

(四)電子戰任務及能力

網絡空間部隊除整合中央軍委會下轄電子對抗與雷達部隊外，並於戰時支援五大戰區，管制運用所屬電子作戰部隊，但共軍電戰部隊在屬性上較難以獲得精準編制及裝備資料，僅能就公開演訓影片、閱兵及網路報導等情資整理其特點，

在2019年中共建政70周年閱兵中，戰略支援部隊與陸軍電子對抗旅抽組成4支「信息作戰方隊」接受閱兵，其中戰略支援部隊的方隊，強調其具「破擊節點、癱瘓體系、初擊致勝」，就其特點可研判其任務重點在於作戰行動前或作戰全程初期；陸軍電子對抗旅的方隊，則稱其「偵擾一體、網電一體、軟硬一體、空地一體」，可見任務貫穿整個作戰全程重點取得「制電磁權」，研判在實戰上與砲兵、陸航、空軍結合，兩者間角色有明確

17 張東坡、彭小名、陳順陽，〈綜合一體化電子戰系統的發展探討〉《艦船電子對抗》，2010年2月，第33卷第1期，頁29。

分工。¹⁸

電子戰目的在使用電磁能量抵銷和降低敵方作戰能力，並藉由敵方電磁頻譜的使用尋求優勢，並確保有效使用自己的電磁頻譜，因此，電子戰依其目標分成三大類，電子戰支援(Electronic Warfare Support, ES)、電子攻擊(Electronic Attack, EA)及電子防護(Electronic Protection, EP)，¹⁹ 共軍在執行電子戰強調過程中的壓制、降級、干擾或欺騙敵方電子設備，並在作戰前或作戰過程中時運用電子戰手段來阻止對手在電磁頻譜的行動，²⁰ 手段區分如表2。

四、對我陸軍地面部隊之威脅

資訊化時代下的戰爭技術，使共軍

對網電一體戰運用更加多元化，成為決定雙方成敗的重要關鍵因素，所以共軍認為在網路空間上取得資訊優勢並拒止對手在電磁頻譜上使用電磁波，是掌握戰爭主動權的必要條件，對我國地面部隊威脅如下：

(一)網路戰

現代戰爭快速變化，戰場複雜度與不確定性日益增加，以目前我國演習重點驗證課目「去中心化指管」中作戰(分)區須遂行獨立防衛作戰，就共軍網攻手段對我國陸軍通資電部隊的影響，研判要進入到國土防衛作戰時，才有顯著效果出現，如透過特工對我部隊之通資系統實施惡意軟體攻擊，透過破壞通資鏈，使情報鏈

表2 電子戰手段

類別	定義	行動	目標
電子戰支援	從敵方的電磁頻譜中獲取數據和資訊。	電磁信號的截收、定位、分析、記錄和傳播，以獲取敵方的威脅、定位和意圖與可能採取行動。	指管中心、情監偵站台、海空軍遠、中程雷達、作戰平台及載具。
電子攻擊	使用電磁能量或武器、攻擊敵方資訊、通信及監偵等電磁波系統，以防止或減低敵方有效使用電磁頻譜行動。	對敵電磁系統實施軟殺(非破壞性)或硬殺，通常區分封鎖及屏蔽。	情監偵站台、海空軍遠、中程雷達、資通電軍資料鏈路、通信系統中繼台及光纖系統數據交換中心。
電子防護	確保己方有效(主動或被動)的使用電磁頻譜。	反制敵方的電子戰支援與電子攻擊措施。	己方指管中心、情監偵站台、海空軍遠、中程雷達、作戰平台及載具。

資料來源：1.王聖元，〈中共戰略支援部隊之研究〉《砲兵季刊》，2020年12月，第191期，頁78及舒孝煌，〈美國陸軍多領域作戰下的電子戰〉《國防情勢特刊》，2023年8月15日，第30期，頁15、16。

2.作者整理。

18 杜貞儀，〈共軍電子偵察能力發展與評估〉《國防科技趨勢評估報告》，2021年12月22日，頁74。

19 Victoria Artur, "Electronic Warfare," ResearchGate, Octobar 2019, 2021, https://www.researchgate.net/publication/336473867_Electronic_Warfare，檢索日期：2024年3月19日。

20 舒孝煌，〈美國陸軍多領域作戰下的電子戰〉《國防情勢特刊》，2023年8月15日，第30期，頁12。



、指揮鏈及擊殺鏈無法運作，讓作戰(分)區聯合泊地攻擊、聯合舟波攻擊、灘岸火殲及縱深作戰的守備、打擊力量及火力支援無法發揮，進而讓我國土防衛作戰任務失敗。

(二)電子戰

共軍對臺的軍事行動強調損小、效高、快打及速決的戰略構想下，對於國軍情監偵的站台、中遠程雷達、系統中繼台與資訊節點，都是首要攻擊目標之一，其手段平時運用電子戰支援方式，獲取我方重要電子參數，戰時運用軟、硬殺打擊我國指管中心、情監偵站台、作戰平台乃至於載具，目的使敵方作戰全程盲與聾，並實施電子防護確保自己耳聰目明，耳聰是作戰部隊作戰指管通資系統的有效運作，目明是明確掌握敵方部隊動態。

於登島作戰時共軍東部及南部戰區編組攻臺戰役指揮部統一指揮電子作戰部隊(含網絡空間部隊支援)，對我各級部隊進行偵蒐及測向等電子戰支援手段，目的在先期判明我作戰(分)區指揮所、主力(打擊)部隊、灘岸守備重點等位置，接續運用電子攻擊手段對我通資系統實施軟殺(干擾)或硬殺(導彈)，破壞我通資電部隊作戰效能，使作戰(分)區通資鏈中斷，無法獲取情資、下達指揮命令，而無法執行

反擊、反制或火力打擊等擊殺手段。²¹

(三)共軍目前網電一體戰現況區分平時及戰時(形式如圖3)。

1.平時

(1)網路空間

潛伏於對方重要公共基礎設施(如電力系統網、金融交易網、道路交通網及水利供水系統等)，不易被目標所察覺，並透過軍方資助隱藏於民間組織竊取敵方政治、經濟及軍事情資。

(2)電磁頻譜

偵蒐對方指管中心、數據鏈路、通資站台、雷達站、作戰平台及載具等各式參數實施戰場經營，俾得在戰時發揮影響戰局之效果。

2.戰時

運用各式攻擊性的技術手段，攻擊或破壞敵方重要資訊設施與機構實施癱瘓攻擊，進而影響敵方政治、經濟、軍事整體運作，削弱敵之戰力與作戰效能，並在軍事戰略上發揮先發制人的威懾效果；且運用電子戰手段針對敵方指管通情系統實施攻擊，例如將惡意軟體(病毒)先期潛伏或透過特工植入我地面部隊資訊設備或指管系統，等待適當時機癱瘓我作戰(分)區、打擊部隊及遠程火力指揮中樞，並在國土防衛作戰階段關鍵時刻，透過電子攻擊

21 〈兵推共軍攻臺 先占外島製造恐慌〉《聯合新聞網》，2023年11月8日，<https://udn.com/news/story/10930/7558585>，檢索日期：2024年9月20日。

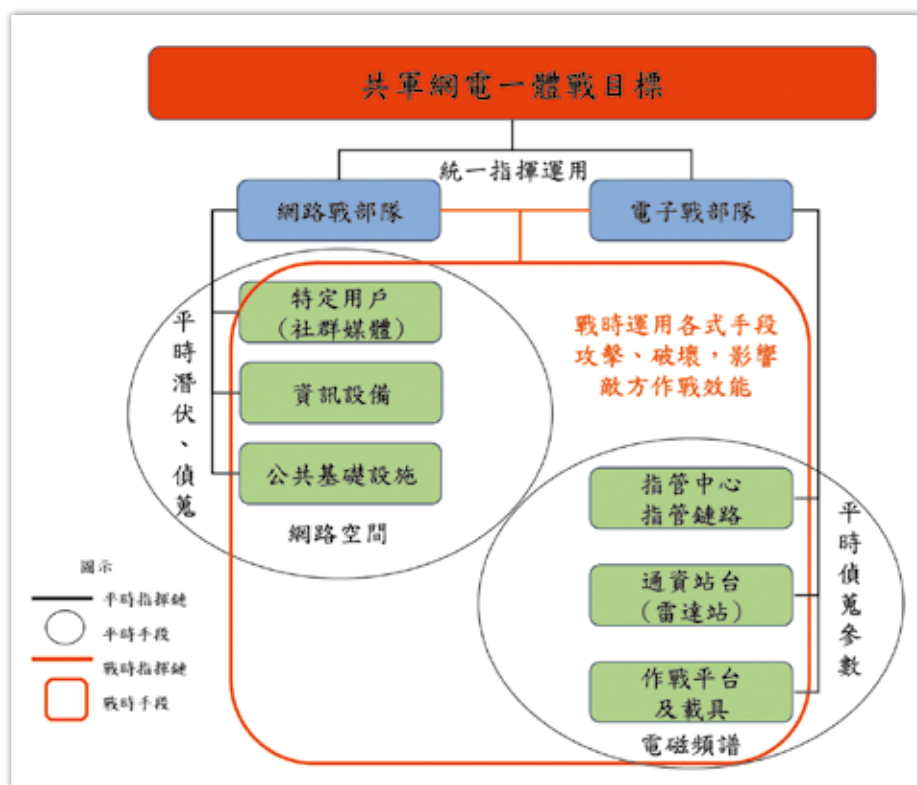


圖3 共軍網電一體戰攻擊示意圖

資料來源：1.王清安，〈從中共「網電一體戰」探討共軍戰略支援部隊作戰能力〉《海軍學術雙月刊》，2020年6月，第54卷第3期，頁85。

2.作者整理。

壓制、降級、干擾或欺騙我地面部隊指管站台、作戰平台及載具，甚至阻止我軍在電磁頻譜的行動、中斷我軍通資鏈，使我情報、指揮及擊殺鏈失效，迫使我地面部隊國土防衛作戰任務失敗。

陸軍通資電部隊網路戰及電子戰之能力與限制

一、現行指揮體系

戰時參謀本部成立聯合網電作戰中心，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。²² 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，相關網路戰及電子戰計畫官、部隊管制官皆為資通電軍負責派遣及管制。

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(資通電軍電戰中心所屬電戰中隊)，以支

22 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。



援聯合作戰之遂行。²³

二、網電作戰程序(如圖4)

將偵搜部隊或電戰裝備所蒐集到之敵軍徵候或參數回傳，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、判明敵情後，提供給網電作戰小組判斷是否須採取攻擊作為，若採取攻擊作為時，立即由網電小組提供軟殺(電子攻擊)及火力協調小組硬殺(精準火力打擊)手段之目標審查結果建議，最後指揮官下達作戰指導並管制各部隊戰果回報。

三、陸軍通資電部隊能力及限制

通資電部隊為國軍目前聯合作戰及陸軍各兵種間協同作戰不可或缺的要素，就陸軍現正推行的五鏈，以通資鏈整合情報鏈、指揮鏈，最終建立擊殺鏈，再輔以後勤支援力量，達「軍種聯合、兵種協同」作戰目標，²⁴當通資電部隊失去作戰效能，通資鏈中斷即無法有效構成情報鏈、指揮鏈及擊殺鏈。

(一)編制(如圖5)

陸軍司令部下轄軍團(防衛部)至聯(步)兵旅級(地區指揮部)，各層級皆有相關通資電部隊於平、戰時負責對上、對下各項通資系統開設、作業與維護。

(二)任務²⁵

1.平時

(1)負責所屬單位行政通資系統之建立與維護。

(2)負責通信、電子、資訊裝備保養、補給作業。

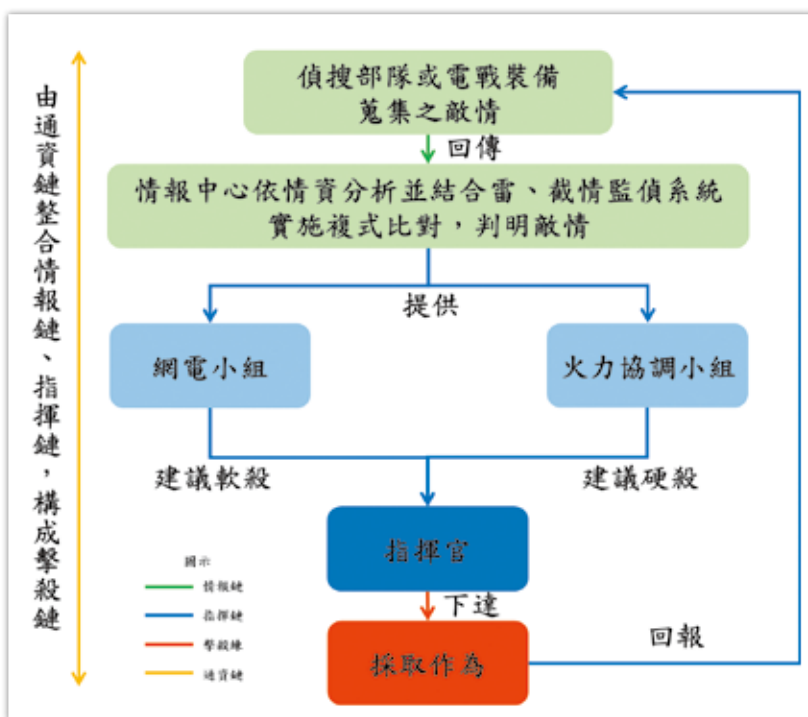


圖4 網電作戰程序圖

資料來源：1.溫宗毅，〈以網電作戰淺談作戰區網電作戰小組〉《通資半年刊》，2024年4月1日，第141期，頁129。

2.作者整理。

23 溫宗毅，〈以網電作戰淺談作戰區網電作戰小組〉《通資半年刊》，2024年4月1日，第141期，頁128。

24 〈美軍助我建立「擊殺鏈」〉《太報》，2023年10月19日，<https://www.taisounds.com/news/content/71/86905>，檢索日期：2024年1月24日。

25 吳佳紋，〈聯兵旅通資科組織功能之探討〉《通資半年刊》，2023年10月1日，第140期，頁54～60。

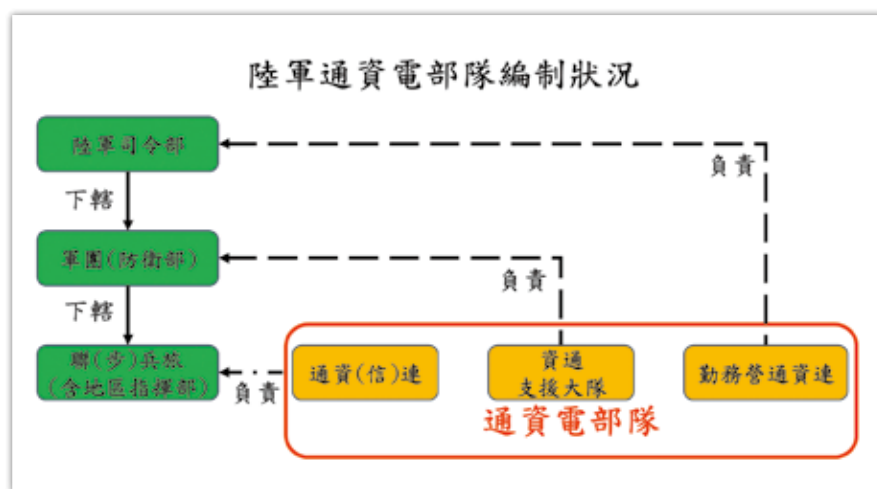


圖5 通資電部隊編制現況

資料來源：1. 〈中華民國陸軍組織與架構〉《中華民國陸軍》，<https://army.mnd.gov.tw/Article/Index/3018>。

2. 作者整理。

目前陸軍上從軍團下至聯(步)兵旅(含地區指揮部)，所有的通資電地面部隊，其所屬資訊組負責建立單位內部區域網路，戰時介接微波系統進入國軍資訊骨幹鏈路與外單位建立資訊網路系統，相關網路戰能力僅能實施資訊安全防護，僅資通電軍網路戰聯隊具備網路攻擊能力，其任務為網路攻擊

、資安防護與應變機制，確保國家關鍵通資基礎建設。²⁶

2. 限制

若國土防衛作戰時共軍針對我通資電部隊實施網路攻擊，雖軍用通資系統屬於封閉型網路，若資訊設備實體隔離不落實、人員專業能力不足，一旦遭受特工植入惡意軟體、誤用具有後門程式中國廠牌資通設備等網路攻擊手段，陸軍通資電部隊具備的能力無法有效防範攻擊，或者修復資訊網路。

(四) 電子戰能力與限制

1. 能力

從民國93~112年的國防報告書中，對於國軍電子戰之指導，大部分著重於

(3) 負責一般通信資訊勤務及行政支援。

(4) 依令支援責任區域內緊急災害(難)防救任務。

2. 戰時

(1) 任所屬單位作戰各階段通資系統開設作業與維護。

(2) 負責與責任區地境內軍、公、民營通資系統介接與整合。

(3) 負責火協中心內部之通資系統建立，並開設空援台。

(4) 管制小延伸節點組，協力戰術區域通信系統開設。

(三) 網路戰能力與限制

1. 能力

26 〈資通電軍成軍 蔡總統：捍衛數位國土〉《自由時報》，2017年6月30日，<https://news.ltn.com.tw/news/politics/paper/1114892>，檢索日期：2024年2月8日。



軍種戰略指揮層級以上的戰略電子戰部隊發展，對於軍種電子戰能力發展未納入優先的建軍目標，其中以陸軍更為明顯，依據陸軍各軍團及所配屬作戰部隊，計有步兵旅、機步旅、裝甲旅、陸航旅、地區指揮部、地區支援指揮部(編配)、砲兵指揮部、化學兵群、工兵群、資通支援大隊(編配)，²⁷其中軍團級作戰指揮中心電子戰需求，由資通電軍派遣電戰聯隊配屬各軍團執行；另陸軍因應未來作戰需求，將7個常備打擊旅所屬戰車營及機步營，重新編組為聯合兵種營，然而軍團以下旅、營級均未編制遂行電子戰所需的裝備與操作人員，²⁸陸軍通資電地面部隊，並無電子戰專業編制及裝備，故無法實施電子攻擊與電子戰支援等電子戰部隊能力，²⁹僅能利用設施、裝備之電子防護功能，以保護部隊作戰能力，此能力為部隊電子戰。³⁰

2. 限制

在國土防衛作戰時，作戰(分)區反擊力量即為聯兵旅等打擊部隊，也是共軍攻擊的首要目標之一，當我通資電部隊僅

具有有限度部隊電子戰能力時，通資系統遭受共軍電子戰攻擊軟、硬殺手段時卻無法反制，僅能實施有限度電子防護(3R)³¹，迫使我通資鏈中斷後，影響情報鏈、指揮鏈到擊殺鏈的整合與運用，有效限制作戰(分)區作戰效能。

四、小結

共軍為達成統一臺灣的目標，所採取的方式約略可區分為和平談判、脅迫談判及軍事占領等3種，其中最有可能採取的就是脅迫談判，從演訓武力展示、聯合封控並結合灰色地帶的運用，採取有限度的軍事行動，一步步進逼我國談判；若共軍採取軍事占領的方式，首先實施聯合空中及海上動態封鎖、大規模聯合火力打擊及奪取臺灣離島等手段，期間同步進行網電一體戰，運用網路戰孤立我國政府、軍隊及民眾、控制國際話語權，期瓦解我國作戰意志，奪取資訊權為戰爭首要目標後，電子戰目標針對我國指管中心、情監偵站台、系統中繼台及數據交換中心實施軟、硬殺打擊，對外使我國無法對國際發聲尋求支援、國外勢力無法介入，對內盲聾

27 〈中華民國陸軍組織與架構〉《中華民國陸軍》，<https://army.mnd.gov.tw/Article/Index/3018>，檢索日期：2024年3月19日。

28 劉維福，〈聯兵旅部隊電子戰能力發展之研究〉《通資半年刊》，2021年4月11日，第135期，頁31。

29 電子戰部隊：通常負責戰略電子情報的偵蒐與攻擊以及防護軍團以上作戰指管中心的運作。

30 部隊電子戰：主要負責旅級以下電子戰術情報的監偵、攻擊與防護，以利作戰部隊於行動中，有效掌握敵軍動態、干擾敵軍指管通信與資料鏈路系統的有效運作、防護我軍指管、武器系統戰力之發揮等。

31 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)。

啞，「盲」無法掌握共軍部隊動態、「聾」各級部隊無法接收上、下級及友軍情資、「啞」無法對下級及友軍行指揮管制及協調。

當國軍地面作戰部隊面對共軍開始遂行國土防衛作戰時，依據作戰戰場分析結果，地面部隊處於獨立作戰狀況是必然的，此種情況作戰(分)區指揮、分散式指管機制，獨立防衛作戰任務之能力勢必相當重要，共軍遂行島上作戰前，在聯合情監偵手段下必定運用網電一體戰之戰術戰法，打擊我作戰(分)區指揮所、打擊部隊及遠程火力，造成我通資鏈中斷，而無法有效整合情報鏈、指揮鏈及擊殺鏈，作戰(分)區最重要反擊力量就無法發揮其效能，使我防衛作戰任務失敗。

我軍因應作為及建議事項

一、因應作為

(一)確保實體隔離、建構安全環境

現有國軍軍用網路屬封閉性網路，理論上應可有效降低外來威脅及風險，但為避免共軍透過網路戰手法(如進階式持續攻擊)入侵國軍網路，須運用相關資訊設備嚴格落實軍、民網路「實體隔離」政策，並精進稽核機制，定時實施防護管控作為，杜絕各種可能之入侵行為，確保

戰時各單位野戰資訊系統橫向溝通及縱向指管暢通。³²

(二)禁止使用陸資廠牌資(通)訊產品

借鏡2022年8月初，美國前聯邦眾議院議長裴洛西(Nanc.Patrici.Pelosi)訪臺期間，不只政府機關網站遭到共軍、民間駭客組織的網路攻擊，甚至連民生超商和大眾運輸工具都遭入侵，其中包括7-11和臺鐵的數位看板，內容置換成各種詆毀簡體字，故須禁止使用陸資廠牌資(通)訊產品，避免我指管情監偵系統遭到入侵或破壞，在關鍵時刻造成影響。

(三)加強電子防護觀念

固定式通資站台須電磁脈衝防護能力及系統的隱蔽、偽裝性等電子防護措施，野戰通資系統須以分散、機動性為主以減少敵方攻擊的影響，加強部隊各級指揮官及專業兵科人員電子防護概念。

(四)評估電磁環境、加強戰場經營

作戰責任地境內電磁環境評估，國土防衛階段陸軍地面部隊都將面臨獨立作戰的戰場環境，故首先必須評估各地地面部隊作戰區域的電磁環境，其中包含敵我雙方電磁頻譜的運用，就現行通資系統而言，電磁頻譜的運用相當複雜，有長時間使用的、間接性使用的以及依據戰況需求短暫使用的電磁波頻道，均須確保我電磁

32 楊鎮璋、張景翔，〈中國大陸資訊戰對國軍資訊安全威脅之研究〉《空軍學術雙月刊》，2021年10月，第684期，頁65。



頻譜能有效運用並對共軍的運用實施干擾；另外在作戰區域內實施戰場經營，針對隱密、有利的制高點實施有線電節點設置，使作戰部隊獲取電子戰優勢，有效發揮部隊作戰打擊能力。

(五)軍公民營整合運用

我國為守勢作戰，應在作戰地區戰場經營上能佔據優勢，除通資兵要調查須先期完成外，更可以結合公、民營設施，在我野戰部署通資系統時可迅速克服障礙限制，增加通連距離、提升指管鏈路傳輸品質，並運用民間科技資源發展無人機、5G通訊、海底電纜及低軌衛星通訊等項目，加強我國軍於防衛作戰通訊韌性，提高戰場存活率，例如2022年行政院數位發展部頒布「應變或戰時應用新興科技強化通訊網路數位韌性計畫」，內容為確保緊急狀況發生導致通訊網路系統遭受破壞或失能，可藉由低軌衛星提供備援，³³另外配合中華電信微波系統等通訊設備，以多重手段進行通資系統備援，協力整合運用軍民通資資源及技術，必能達成防衛作戰時通資鏈暢通。³⁴

二、建議事項

(一)修訂或擴編通資電部隊編裝

國軍建軍備戰皆是依據打裝編訓的概念，打防衛作戰買防衛性武器及裝備，再依據裝備諸元性能完成編制修訂，最後實施訓練。制電磁權是現代戰爭的序幕，因此陸軍地面作戰部隊在遂行國土防衛作戰時，必須要有編制內電子戰部隊與裝備，才能有效發揮作戰效能，鑑於陸軍即將建置電戰裝備，³⁵所以聯(步)兵旅級(含地區指揮部)應在所屬建制下成立電子戰連(排)，或將現有通資(信)作業連擴大編制，包含旅級電子戰所需裝備與人員，甚至單獨成立涵蓋資訊、通信及電子戰3種專業連隊的通資作業營，使陸軍聯合兵種營真正具備獨立作戰的能力。

(二)建立正確觀念，完善準則編修

偵蒐、干擾為不同屬性之電戰裝備，就運用而言，偵蒐為電子戰支援情資蒐集手段為情報之一環，應由情報中心管制運用；干擾則為電子攻擊中軟殺手段，與火力硬殺手段同屬擊殺鏈，應受作戰中心及火協中心管制運用，故此使用時機與如何運用則是作戰部隊指揮官的職責，因此強化戰鬥兵科電子戰指揮與計畫作為能力是非常重要的工作，建議正規班、指揮參謀學院等深造教育增加電子戰專業

33 〈應變或戰時應用新興科技強化通訊網路數位韌性計畫〉《數位發展部》，2022年8月，<https://www.ey.gov.tw/File/25AFCB901E407DD2>，頁13。

34 〈中華電信強化網路韌性海纜、微波、衛星互為備援〉《中央社》，2023年4月9日，<https://money.udn.com/money/story/5612/7085485>，檢索日期：2023年4月17日。

35 溫宗毅，〈以網電作戰淺談作戰區網電作戰小組〉《通資半年刊》，2024年4月1日，第141期，頁132。

課程知識。

建議我陸軍通資電部隊在建置電戰裝備時，應同步發展相關準則及作業程序，使單位有所依循，並由兵監訓部研究共軍裝備之能力與限制，發展有效剋制對策，確保我陸軍通資電部隊通資鏈暢通及打擊部隊戰力發揮。而新式電戰裝備撥發後，可改變以往訓練時採取狀況模擬的方式，調整為實際干擾操作方式，針對部隊實施電子偵蒐及干擾，訓練部隊通信手段調整、通信頻率更換或指管中斷時應變機制等通信作業流程，同時藉演訓驗證各單位網路安全防護及電子戰計畫的適切性與可行性，從中發掘問題，透過訓後回顧討論並精進，且可作為年度通資電戰術戰法研究及準則編撰之參據。

(三)仿真、實戰化訓場

建立電子戰專用訓場，模擬複雜電磁環境，採無預警特別狀況方式，以兩軍電子對抗方式，實施仿真、實戰化訓練，驗證部隊電子攻擊與電子防護能力，並可務實提升單位、人員及裝備電子防護的認知與應變能力，所以建議將電子對抗納入專精管道、基地訓練及三軍聯訓中，以

模擬實戰對抗的方式，實施電子戰支援、攻擊及防護等演練，除增加作戰部隊指揮官電子戰運用與計畫作為能力外，並針對後續獲得電戰裝備，透過人員持續訓練及裝備效能的驗證，才可以提高專業素質和作戰能力。

(四)建構電子戰模擬器

囿於避免影響民間頻率使用或遭共軍電偵機獲取相關電子參數，且電子戰專用訓場建置不易，電子戰裝備又屬於高成本，為提升訓練成效及降低訓練成本，建議可由中科院建置電子戰模擬器，先期於模擬器上熟裝訓練後再實裝操作，可有效降低裝備損壞率及提升人員裝備熟悉度。目前中科院對於產製模擬器之技術已具備足夠能量，除在陸軍裝甲兵訓練中心(履帶型甲車駕駛訓練模擬器)以及通信電子資訊訓練中心(戰術區域通信系統實體模擬器)中使用多年，³⁶也用於海軍(潛艦教練儀)、³⁷空軍(F-16全功能模擬機)，³⁸另外可與民間廠商合作，藉由模擬器製作的相關技術實施交流，確保取得電戰模擬器的實用性；另考量戰場上不同的場景、頻率及設備等因素，選擇適切仿真技術，

36 〈陸用模擬器〉《國家中山科學研究院》，https://www.ncsist.org.tw/csistdup/products/product.aspx?product_Id=32&catalog=25，檢索日期：2024年7月9日。

37 〈海用模擬器〉《國家中山科學研究院》，https://www.ncsist.org.tw/csistdup/products/product.aspx?product_Id=33&catalog=25，檢索日期：2024年7月9日。

38 〈空用模擬器〉《國家中山科學研究院》，https://www.ncsist.org.tw/csistdup/products/product.aspx?product_Id=34&catalog=25，檢索日期：2024年7月9日。



後續提供完善的支援與維護能量。

(五)通資電人才培育

因應共軍網電一體戰作戰模式影響之下，針對國軍通資電人才培育，應積極於通信、資訊、電子戰等專業領域及職務交織歷練，藉以精進幹部通資電概念整合，可參據國外新型態準則，如美國陸軍多領域作戰FM3-0，瞭解網路空間、電磁頻譜等戰術戰法運用，以肆應未來戰場型態，並同步發展通資電戰術戰法支持我國防衛作戰。³⁹

結語

隨著資訊科技日新月異，戰場空間增加太空、網路及電磁頻譜等3個領域，網路戰及電子戰在2022年起俄烏戰爭中更可以體現到其重要性，俄羅斯在對烏克蘭實施關鍵基礎設施及指管情監偵系統重點打擊時，造成指管一度中斷之威脅，除影響戰力發揮之外，國家幾乎陷入存亡危機。綜合上述共軍網電一體戰的分析，可知未來作戰效能的發揮，除武器裝備的火力強大、射程遠近及快速與否之外，則是作戰指管及情監偵系統能否「耳聰目明」，「耳聰」就是確保部隊作戰指管通資系統的有效運作，確使各部隊能有計畫、有組織的發揮聯合作戰最大效能，「目明」則

是明確掌握敵軍動態，以利遂行火力分配與精準打擊。

我國陸軍通資電部隊因應新式電戰裝備的建置，首要調整或擴編其編制，並完善準則編修及修訂通資電計畫，在教育上給予正確運用觀念、訓練中輔以電戰模擬器及測考時設置仿真實戰化訓場，持續加以精進。在中共敵情威脅及網電一體戰術戰法威脅下，於國土防衛作戰時，我陸軍通資電部隊才能落實電子戰反制、網路戰安全防護及電磁頻譜管控，增加通資系統韌性，使情報鏈、指揮鏈及擊殺鏈能透過通資鏈整合運用，提升在未來戰場存活機率。

(113年11月22日收件，113年12月17日接受)

39 FM 3-0 Operations(Fort Monroe, Virginia: United States Army Training and Doctrine Command, October 6,2022), pp.1-16~1-22.