DOI:10.6237/NPJ.201912_53(6).0008

資訊戰對國軍防衛作戰重要性之研究

林宜昌　備役陸軍上校

提　　要：

一、國軍是國家安定的力量，並以確保國家安全與人民福址為任務優先考量，然現在國家安全所面臨的威脅不同以往，且國防已全面進入資訊作戰時代，明顯超越傳統領土疆界。國軍如何展現堅定自我防衛決心，而其中將資訊作戰導入國軍防衛作戰領域，將能達成「防衛固守、重層嚇阻」的戰略目標。

二、面對中共信息戰威脅，國軍在資訊戰整備方面，從調整指管戰、情報戰、電子戰、心理戰等資訊戰的策略，建立符合資訊戰作業條件的整合資訊/指管/電子戰系統及作業環境，期能有效整合資通電資源，建構更精實之國軍指通戰力，方能支援臺澎防衛作戰任務遂行。

三、針對國軍防衛作戰構想中，資訊戰扮演極其重要角色，且資訊戰已由網路虛擬空間走向實體利益面向；而運用資訊戰力癱瘓、攻擊敵國關鍵資訊基礎設施之作戰思維已然確立。如何將敵、我對於網路、通訊可能的攻防，納入軍事戰略思維，以贏得複合式的資訊戰爭，將是國軍面對的嚴峻挑戰。

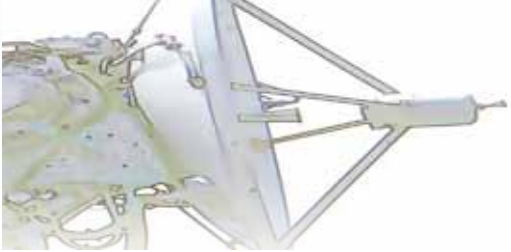
關鍵詞：資訊戰、資訊作戰、電子戰、指管戰、心理戰

壹、前言

國軍是國家安定的力量，並以確保國家安全與人民福祉為任務優先考量，然國家所面臨的安全威脅早已不同以往，且國防已全面進入資訊作戰時代，並在面對中共具備奪取「局部制信息權」進攻作戰能力之威脅[1]已明顯超越傳統入侵領土疆界的敵人。如果「資安」出現漏洞缺口，甚至遭到入侵，對國家造成的危害，絕不亞於傳統武力攻擊。所以，「資安」已成為國家新的安全威脅，也是國防軍事的重大核心；國軍如何展現堅定自我防衛決心，並將資訊作戰導入國軍防衛作戰領域，是我國軍事戰略的創新作為[2]。

註1：國防報告書編纂委員會，《104年國防報告書》(臺北：五南文化廣場，2015年12月)，頁50。

註2：〈資通電軍任務簡介〉，國軍人才招募中心網站，https://rdrc.mnd.gov.tw/關於中心/從軍簡介/資通電軍，2018年3月26日，檢索日期：2019年8月26日。



。再者，未來國軍的資訊戰將以網路攻防為核心，通訊安全為基礎，電磁發展為前瞻，把「資安」視為國安的具體行動，將可達成「防衛固守、重層嚇阻」的戰略目標。

當前資訊戰早已超越傳統的空中、海域及地面的防衛概念，成為「重層嚇阻」戰略下的第一層嚇阻兵力，並跳脫軍種的藩籬，做為當前國軍聯合作戰的典範，是值得深入探討的議題。本文針對資訊戰特性、運用與中共資訊戰發展及影響著手，強調國軍資訊戰的重要性及軍事思想，以及國軍資訊戰發展歷程與能力及限制，讓國軍在資源有限的現實條件下，以「資訊戰」整備調整國軍指管戰、情報戰、電子戰、心理戰等策略，建立符合資訊戰作業條件的整合資訊、指管、電子戰系統及作業環境，並有效整合資通電資源，建構更精實之國軍指通戰力，以支持臺澎防衛作戰任務遂行，這也是撰寫本文的主要目的。

貳、資訊戰特性與運用

國防部在民國106年《國防報告書》指出，我國在維護資訊安全方面，隨著資訊科技快速發展，如何維護資訊及網路安全已為各國新興課題。國軍近年來資訊戰的作為包括「資訊運用」與「資訊防禦與反制」等發展策略，亦即整合國軍心理、經濟、政治及資訊基礎建設，建立三軍通用的資訊戰數據傳輸鏈路，並擴大運用民間資訊資源、凝聚共識；另依單位任務特性，以「三軍聯合作戰」的觀點，就通信、資訊及電子戰的戰備整備、教育訓練、通資人力經管及後勤補保等方面之持續精進，以暢通三軍聯合作戰指揮管制系統，俾發揮戰場效益極大化，獲致最後勝利。基此原則，有必要針對資訊戰特性及運用逐一介紹。

一、資訊戰特性

美國高級戰爭及資訊研究中心(Institute for Advanced Warfare and Information Studies)定義「資訊戰」為：「尋求在軍事及商業領域獲得優勢，採取攻擊及防禦之手段，使用計算機科學與資訊系統來利用、誤導以及摧毀敵人之資訊系統，同時亦保護自己之相關系統」[3]；又說「資訊戰」係指對立雙方為爭奪資訊獲取權、控制權及使用權而展開的戰爭[4]。如同一般傳統戰爭型態，「資訊戰」也可分為防衛資訊戰與攻擊資訊戰(Defensive Information Warfare and Offensive Information Warfare)。

資訊戰主要特性為運用網路傳輸手段(包括有、無線電)，對敵人網路節點、資訊系統及儲存資料實施攻擊，以獲取或竄改情報，使敵人無法即時產生正確重要決策，進而癱瘓敵國重要基礎設施，造成人民恐慌，影響政府運作機制，達到「不戰而勝」之目標；同時，又要能保護己方資訊系統，不受敵人影響。然而資訊戰攻擊的目標是資訊系統和敵方心理(亦即武器與士氣)，此兩項目標一旦先遭到攻擊，將使整個部隊運作與戰場管理機制陷於癱瘓，達到《孫子兵法》中

註3：廖宏祥，〈資訊戰國家戰略〉，《世紀智庫論壇》(臺北市)，第23期，2003年9月30日，頁105-107。

註4：程文理，〈資訊戰概論〉，國防新聞網，2016年6月26日，http://www.ewmib.com/news.php?news_id=124&cate_id=9，檢索日期：2019年9月26日。

所謂「不戰而屈人之兵」的目的。

由於網際空間不明確的屬性，未來網路攻擊將會是國家政府與非國家團體緊密結盟。網際網路和社群媒體已讓所有人都可以運用資訊發揮自身力量，不論是個人、團體或社群，均可影響到外交、資訊、軍事與經濟等相關權力，其影響程度和過去各國政府戰略溝通訊息概等[5]。由此可知，未來網路戰對作戰攻擊對象之影響，將由過去攻擊敵方網路系統或節點，改變至擁有智慧型手機的每個人，作戰效益將會更快速，影響層面也會更廣大[6]；而資訊戰亦是弱化對手的另一種形態的戰爭。國軍面對強勢的中共網軍威脅，有必要建構國家最新的防衛作戰思維[7]。

二、資訊戰的運用

資訊戰運用的實例，就如同美軍在波灣戰爭歷時38天的「沙漠風暴」(Gulf War-Operation Desert Storm)行動中，始終將伊拉克軍隊的指揮、通信、情報、防空等軍事資訊系統做為打擊的核心，使伊軍從開戰的第一天起就處於混亂無序，甚至癱瘓的心態，直至戰爭結束也未能恢復[8]；而在對伊拉克戰爭的心理戰與宣傳戰方面，美軍也充分利用媒體，製造有利於己方的資訊，使得任務全程在打擊伊軍的士氣，與提高自我士氣上均有顯著的效果。「資訊戰」的實力和戰爭勝負可說是相互輝映[9]。國軍在資訊戰的運用方面，主要任務為建構以作戰為主的資訊環境，提供部隊各式指、管、通、資、情、監、偵系統，經營優質的通資基礎平台，並執行通資系統、網路戰及電子戰攻防能量整備與運用[10]，以「確保安全的國防網路環境」與「建立可恃的網路戰力」為資訊戰略兩大目標，並做為資訊戰建軍整備及用兵之指導[11]。國軍資訊戰力在網路防護及攻擊作為上，係以確保國防資訊運作正常，並發揮早期預警能力，洞悉敵人的作戰意圖，依令對敵進行攻擊，以癱瘓、阻滯及限制敵軍事行動，有關運用如后：

(一)確保安全的國防網路環境

建立可信任之國軍網路，並正確且迅速下達指管命令之關鍵，以鞏固國防網路安全，使網路於遭受干擾與破壞時，仍可維持運作；另整合新興科技，以提高網路存活率，其具體措施計有：

1. 早期預警，針對已知及未知的網路攻擊跡證，發揮預警機制；並透過國際及跨部會分享機制獲取預警情資，及早因應、防護各種網路刺探與攻擊。

2. 縱深防禦，強化資安防禦機制，運用多層級資安防護及機動備援系統，維護國軍指管等核心系統運作安全。

註5：Andrea Little Limbago著，章昌文譯，〈網路治國多面向本質〉，《國防譯粹》(臺北市)，第43期，第2卷，國防部，2016年2月，頁14。

註6：Joint Chief of Staff, Joint Pub 3-13, Joint Doctrine for Information Operations(Washington, DC: Joint Chief of Staff,1998),p.7。

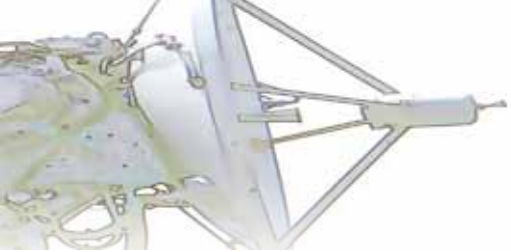
註7：陳友武、趙德榮，〈資訊作戰概論〉，《電子戰專輯》，第26輯，頁15-25。

註8：Daniel E. Magsig著，國防部史政編譯局譯，《資訊時代的資訊戰》(臺北：國防部史政編譯局，1997年)，頁250-252。

註9：同註8，頁252。

註10：同註2。

註11：〈國家資通安全戰略報告-資安即國安〉，總統府網站，2018年10月，https://www.president.gov.tw/Page/317/969/，檢索日期：2019年8月26日。



3.針對重大網路攻擊事件能迅速反應，並具備減損、限制擴散及快速復原能力，同時核心的情傳及指管網路仍可有效運作。

4.以區域聯防觀念，透過網路情資分享平臺與各單位、部會甚至國際友盟交流合作，共同維護網路系統安全。

(二)建立可恃網路戰力

平時針對中共重要指管、武器系統等目標實施戰場情蒐，戰前運用網路手段癱瘓敵政府關鍵資訊系統，擾亂其政治、經濟、交通、社會秩序，遲滯其作戰決心下達；戰時則對中共重要指管網路及相關武器系統、設施實施反制，以降低敵聯合作戰反應能力，其具體措施如后：

1.目標情蒐：透過多元之情報蒐集及分析能力，針對中共高價值目標，掌握其資安弱點伺機突襲，展現具有震懾之網路作戰能力，降低敵犯臺可能性。

2.主動打擊：作戰全程，藉散播偽訊息，使中共誤判情勢，擾亂其政策及軍事命令下達；另運用網路攻擊手法結合硬殺手段對中共指管、防空雷達等重要系統實施精準打擊，以降低共軍軍事作戰能力。

3.有效反制：運用國家整體資訊力量，對大規模及組織型駭客發動網路攻擊事件，並進行強力反制，確保網路通暢安全。

參、中共資訊戰發展與影響

中共近年演訓方向已朝多維聯合作戰體系邁進，並以完善指揮鏈結與橫向溝通聯繫，提升戰區聯合作戰效能與綜合戰力。並在「複雜電磁環境下打贏局部戰爭」之目標推動下，全面提升電戰戰力，以發揮有效威懾之作用[12]。我國近年飽受中國大陸網軍肆虐之苦，既造成社會互信潰堤，民眾惶惶不安，更影響各種選舉，亦危及國家安全；然中共網軍的獵殺目標，不僅是我國，連科技先進如美國都深受其害，像獲得中國大陸網路巨擘騰訊公司投資入股的美國網路論壇(Reddit)，也受到中共網軍「人海戰術」的嚴重干擾。且中共網軍有組織性地散布政治宣傳，吹捧中共政府，圍剿發表不利中國大陸言論的用戶，特別是法輪功、天安門事件、華為公司及孟晚舟事件等討論的文章，均遭到中共網軍「轟炸」[13]。因此，面對此種威脅，確有必要就中共在資訊戰發展現況及運用[14]，分別探討：

一、**中共資訊戰發展現況**

中共「網軍」乙詞，最早於1999年「解放軍報」出現。網軍成立於2015年底，總部設於北京，其任務是進行情報、網路攻防、心理戰等，透過釣魚網站、網路水軍等方式，進行「認知空間」作戰；目前中共的軍事思想，仍以「不對稱作戰」及「超限戰」為主導，也發展出「點穴戰」的構想[15]。所謂點穴戰略，就是重視點穴打擊，一擊而讓對方癱瘓；所謂的要穴，是指敵人的資訊系統、指揮中樞及力量重心。而如何才能精確擊

註12：同註1，頁60。
註13：王清安，〈中共網軍發展對本軍威脅評估之研究〉，《陸軍通資半年刊》，第127期，2017年4月，頁8。
註14：同註13，頁9。
註15：同註14。

中目標呢？關鍵有二：其一是情報資訊，另一為精確打擊。足見在資訊化時代戰爭中，想要確保點穴成功，精準實施是重點，而資訊控制權則是關鍵[16]。

在建制方面，中共已設置若干資訊兵團，如各戰區組建資訊戰營，還設立了資訊戰武器及戰略之專責研究機構，如中共電子科技學院、總參謀部第三部(以下簡稱總參三部)與資訊戰模擬中心等，而且還全面規劃相關訓練課程，使指揮層級軍官瞭解資訊戰發展，相關課程內容包括資訊戰理論、通訊網路技術、電子反制、數位化部隊、資訊戰略、戰術及電腦病毒攻擊等。除此之外，政治局還成立資訊戰專責單位，直接向中共領導人負責[17]。

中共賦予「網軍」的任務，在有效進行電腦網路的攻擊或防禦的網路戰，此係中共為了因應超限戰[18]內容，將建軍方向逐步朝向陸、海、空、天、電、網一體化的作戰方式發展，而「網軍」未來的發展也可能擴大。再者，中共組建「網軍」部隊新兵種，並且重點培訓具高科技作業能力的優秀人才，不是只有軍方人員，民間企業及學術機關也都在總參三部的協助下，執行對國外政府機關的網路滲透作戰。像是近年美、日兩國就多次遭到中共網軍大量的攻擊；另一方面，中共近年來不斷地進行虛擬實戰，如電腦病毒攻擊演練及大規模駭客入侵等，均是以資訊攻擊為開端，尤其全力培養網路作戰專業人才，期藉入侵我國家關鍵資訊基礎設施，破壞我政府部門、銀行及水電公司等官方網站與資訊系統，以影響我民生經濟運作，甚至癱瘓國軍軍事網路，阻絕我指管情傳線路，達成其軍事作戰之目的[19]。因此，可以大膽假設中共對臺武力攻擊前實施訊息戰的可能性是高度可能的，甚至可說不分平、戰時。

我國在《104年國防報告書》首度證實中共網軍部署於各總部、五大戰區、國防科研機關、國防動員信息及民兵等軍事部門，組成網路攻擊、防禦的基本戰力；另據一項研究揭露，共軍大約有16個(信號情報)技術偵察單位和局、處，和至少7個電子作戰/電子反制單位，且中共五大戰區均各自編配一個電子反制團，而火箭軍應該也有其電子支援單位。這些組織的任務，就是進行網路滲透、網路諜報及電子作戰[20]。

由於中共網軍主要受總參謀部的指揮，總參三部及下屬61398及61486部隊為中共網軍的主要來源，依據中共情報組織的分工推論，總參三部可能才是真正指揮的中樞[21]。畢竟該部為共軍信號情報(SIGINT)的蒐集機構，主要任務則為對無線電通信實施監聽、

註16：彭錦珍，〈資訊時代中共國防現代化之研究-解放軍資訊戰發展及其對臺海安全之衝擊〉，《復興崗學報》，2004年，第82期，頁187-218。

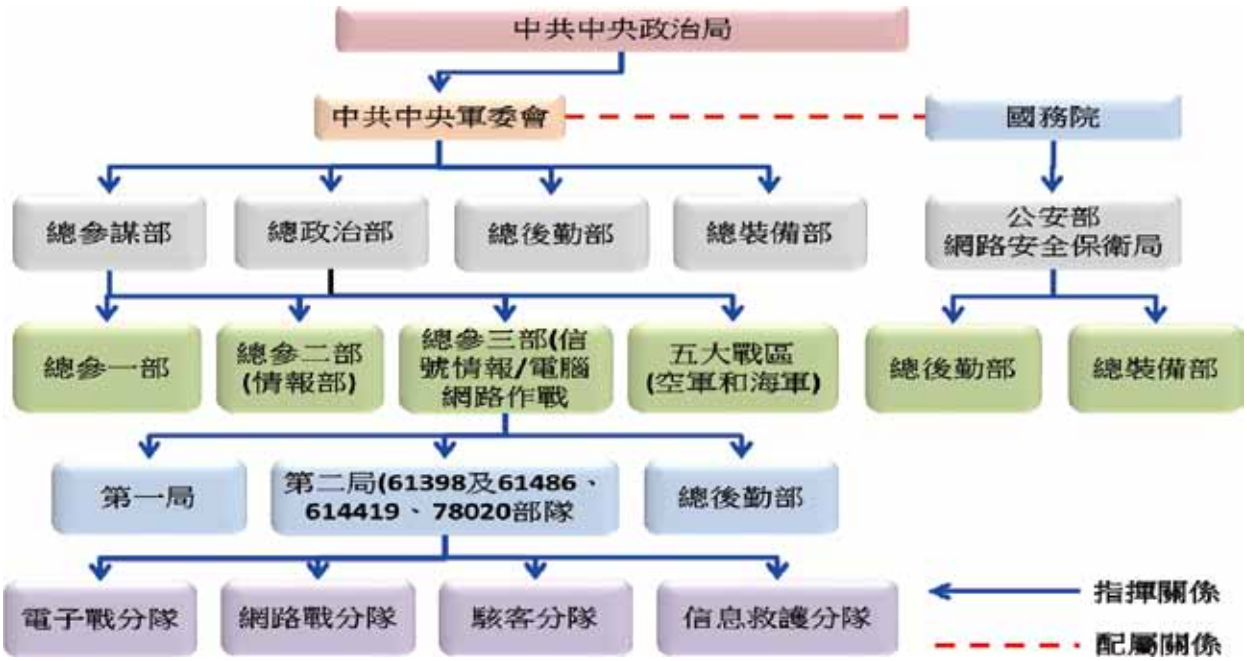
註17：中共研究雜誌社，〈對共軍發展高技術條件下信息戰之研析〉，《中共軍隊建設與發展》第9篇，中共研究雜誌社，頁33-40。

註18：同註14。

註19：同註13，頁12。

註20：鄧炘傑，〈中共軍事現代化及網路作為〉，《陸軍學術雙月刊》(桃園)，第52卷，第545期，陸軍司令部，2016年2月，頁139。

註21：同註14。



附圖：2015年中共網軍組織圖

資料來源：王清安，〈中共網軍發展對本軍威脅評估之研究〉，《陸軍通資半年刊》，第127期，2017年4月，頁11。

各種密碼破譯等工作；另在網路方面，負責網路安全維護及網路間諜防制。至於總參謀部第四部，主要任務為電子情報蒐集、分析、反雷達干擾等，以及資訊與電子戰之研究、電腦網路攻擊之反擊。由於中共為推展「資訊心理戰」，更在其總參謀部下建立心理戰指揮中心，遂行資訊心理戰的任務，包括組織部隊、院校和科研機構進行資訊心理戰理論的研究，以制定共軍資訊心理戰的發展規劃等[22](網軍組織，如附圖)。

二、中共資訊戰運用影響

2016年1月中共為縮減指戰層級，及適應現代戰爭的需求，其資訊戰有關軍改重點，係在「網電一體戰」目標下，發展戰系平臺，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，冀達癱瘓我重要目標及擾亂民心之目的[23]。主要任務也包括建設網路強國及培養資訊化作戰，積極培養資訊化作戰指揮、技術專業等作戰人才；另意識到未來作戰型態，網路人才將攸關網路戰勝負關鍵，故積極籌獲網路人才，以充實網路資訊戰實力[24]。此外，中共資訊戰發動方式，係以我國軍民網站為攻防戰的演練對象，植入木馬程式刺探國軍各機關、重要民間機構及企業集團等資訊系統之弱點等網路攻擊，並以不斷竊取我國的情資為主[25]；其攻擊能力與可能之行動如下：

(一)具電腦病毒破壞能力，可透過多種

註22：同註13，頁11。
註23：國防報告書編纂委員會，《中華民國108年四年期國防總檢討》(臺北：五南文化廣場，2019年9月)，頁40。
註24：陳君碩，〈戰略支援部隊打網經費提高30%〉，《旺報》，2016年1月30日，版6。
註25：同註17，頁33-40。

表一：近年中共網軍常見網路攻擊手法及防禦方式

常見攻擊	DDoS攻擊 (分散式阻斷服務攻擊)	SQL Injectio (隱碼攻擊)	APT (進階持續性滲透攻擊)
利用弱點	網路頻寬不足與系統效能負荷過大。	網站程式寫弱點。	各種方式。
攻擊手法	利用各國伺服器跳板或中木馬電腦同時連線網站，意圖癱瘓系統。	運用網站程式撰寫弱點，進行惡意語法注入，取得網站控制權。	持續且潛伏運用新型攻擊手法。
攻擊前兆	利用各國伺服器跳板或中木馬病毒電腦，同時連線網站意圖癱瘓系統。	先進行系統掃描動作。	無聲無息，僅能綜合判斷。
防禦步驟	1. 監測網路流量有無高於平常值(5Mbit/s)、連線數量有無高於平常值(如監測設定為10,000筆)。 2. 監控入侵偵測系統有無系統掃描情形。 3. 發現以上行為，進行綜合分析判斷。 4. 進行網路過濾，篩選可疑IP進行封鎖，必要時進行網段封鎖，直到流量恢復正常。	1. 監控入侵偵測系統發現有掃描行為進行自動化行為阻擋。 2. 監控網頁防置換軟體有無跳出警訊。 3. 將疊積掃描行為IP納入防火牆黑名單。	1. 監控入侵防禦系統、APT防禦資安設備、高階網頁型防火牆，綜合分析攻擊型式。 2. 主動瞭解該攻擊入侵目標，參考相關國際資安網頁消息。 3. 資安防禦設備發現該行為模式，將行為封包阻斷，並納入防火牆黑名單。
窒礙問題	若遇國際大規模攻擊，將難以阻擋。	須增加監控人員、時常進行軟體版本升級。	須增加監控人員、培養專才人員多角度判斷。

資料來源：〈國家資通安全戰略報告-資安即國安〉，總統府網站，2018年10月，https://www.president.gov.tw/Page/317/969/，檢索日期：2019年8月22日。

植毒管道，直接攻擊、破壞我政、經、軍等資訊系統。

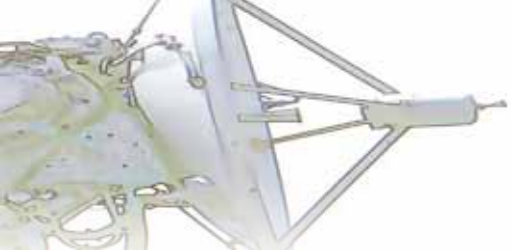
(二)具電磁脈衝炸彈，大規模干擾、癱瘓我C4ISR指管通情系統，及影響我武器系統的功能性。

(三)具資訊偵收能力，特別是藉助駭客的力量，竊取我機密資料。

中共網軍現階段已具備對我電磁參數及監偵與指管系統，遂行偵蒐、阻斷與干擾等電子軟、硬殺能力[26]。若以對應我之資訊防護技術，其主要攻擊方式計有分散式阻斷服務攻擊、隱碼攻擊及進階持續性滲透攻擊等三種(攻擊方式，如表一)[27]。

我國在《四年期國防總檢討》中曾提到，中共已成立資訊網路作戰部隊，積極研製平臺，並結合民間能量，大幅提升網路作戰能力[28]。面對中共網軍常態性攻擊，因應之道除將國軍軍民網路及各指管系統均採實體隔離、專網專用，各網系間部署相關資安防護硬體設備外，並落實定期資安稽核機制，強化執行各項資安管控措施，方能有效降低中共網路攻擊的行為[29]。

註26：同註24。
註27：同註11。
註28：國防報告書編纂委員會，《中華民國102年四年期國防總檢討》(臺北：五南文化廣場，2013年3月)，頁20-27。
註29：洪哲政，〈大陸網軍強攻 國軍這個單位網站一年擋三千多萬次不破〉，聯合新聞網，2018年7月11日，https://udn.com/news/story/10930/3246631，檢索日期：2019年8月22日。



表二：民國103-107年國防部所屬民網遭異常偵測、掃描及疑遭攻擊次數統計表

單位＼年度	103年	104年	105年	106年	107年
國防部網站	1,001,142	1,153,275	4,120,562	9,552,884	132,250,620
國防大學	877,450	995,312	219,522	198,469	39,911
人才招募中心	4,309,186	4,931,321	28,522,275	31,968,975	25,196,734
軍醫局	720,542,371	561,312,118	276,271,708	162,453,979	141,544,897
政戰局	133,587	856,889	194,621	492,549	456,246
總計	726,863,736	569,248,915	309,328,673	204,666,856	299,488,408

資料來源：洪哲政，〈大陸網軍強攻 國軍這個單位網站一年擋三千多萬次不破〉，聯合新聞網，2018年7月11日，https://udn.com/news/story/10930/3246631，檢索日期：2019年8月22日。

肆、國軍資訊戰發展運用及省思建議

國軍的防衛作戰構想為「迫敵奪臺任務失敗」之作戰指導[30]，為達成防衛作戰構想，應以不對稱手段、不對等力量與非傳統方式進行作戰，迴避敵人強點，並以適當的戰法、載具攻擊敵人的弱點，從而改變戰爭的結果，使戰爭朝向有利己方的方向發展。國軍依「防衛固守、重層嚇阻」之軍事戰略，思考與強化「創新/不對稱」戰力，並以共軍無法預期的裝備與戰術戰法，使對方難以察覺或防範，至於武器系統發展則應以「機動、隱匿、快速、價廉、量多、損小、戰高」為方向，做為未來軍事投資重點；並檢討各項軍備獲得優序，以打造重層防衛及嚇阻戰力，遏止中共武力犯臺行動。

再從「資訊戰」角度省思，發現中共網軍對於國軍民用網路攻擊一年平均皆已達3,000萬次以上，僅以國防部於民國107年7月公布[31]所屬單位民網遭受異常偵測、掃瞄及疑遭攻擊最多的單位為國防部軍醫局，民國107年就被疑似駭客或中共網軍刺探，高達1億4,154萬餘次；另統計國防部全球資訊網疑似遭受駭客異常偵測及掃瞄等活動次數也達1億3,225萬餘次，顯示國防部民網環境資安防護措施工作確實不容懈怠(如表二)，也唯有不斷精進資安防護工作，才能確實阻斷中共網軍不斷的竊取國軍情資。

隨著科技進步與發展，網路已成為關鍵的生活場域，且其特性使網路資源爭奪成為有別於陸、海、空及太空之外的新型作戰型態；就軍事作戰而言，網路作戰對於軍事嚇阻、戰力投射及戰略威脅，具有相當程度的影響力，進而左右他國之認知與決策，達到預期規劃作戰效益[32]。顯見網路作戰須於平時著手經營，戰時始可發揮戰力，以下就國軍「資訊戰」發展運用及省思與相關建議，分述如後：

一、未來發展運用及省思

註30：國防報告書編纂委員會，《中華民國106年四年期國防總檢討》(臺北：五南文化廣場，2017年3月)，頁20-27。

註31：同註29。

註32：〈中共政軍發展評估報告〉，國防安全研究院，2018年12月12日，https://indsr.org,tw/wp-content/uploads/2018/12/中共政軍發展評估報告，檢索日期：2019年8月26日。

國軍「資訊戰」發展運用的三大戰略目標，第一、打造國家資安機制，確保數位國家安全，第二、建立國家資安體系，加速數位經濟發展，第三、推動國防資安自主研發，提升產業成長；並以網路攻防為核心、通訊安全為基礎、電磁發展為前瞻，做為三大主要任務[33]。其中前兩個目標為建立有效資安防護體系，以確保政府體制的安全運行，並促使日漸數位化的民間經濟活動順利開展；而第三個目標則著重在我國自主資安技術能量的培養，以增強國防實力，並促進資安產業的建立。畢竟，資訊安全已成為現代資通訊系統應用不可或缺的要素；就整體國家戰略而言「資安即國安」。簡言之，「資安即國安」具兩層意涵，在消極層面，我國民間與政府組織必須建置精實完整、與時俱進的資安防衛機制，以有效抵擋平時和戰時的外部網路攻擊；在積極層面，因未來戰爭型態極有可能以資訊戰先行，我國必須具備如同「國艦國造」、「國機國造」的決心與魄力，有系統性的發展軍、民兩用的自動資安攻防技術，方得以確保在未來資訊網路戰爭中有與敵國有抗衡的實力。

由於國軍強調「首戰即決戰」概念，並以「創新/不對稱」戰術因應中共武力威脅。因此，在建軍規劃上須跳脫建立對等武力的傳統觀念，將國防資源及科技能力集中在關鍵戰力，建立實質嚇阻力量有效反擊能力。國防科技發展趨勢為確保國防網路能在安全架構下正常運行，以支援軍事作戰任務，有效進行網路攻防為主軸，並在遂行防衛作戰前提下，著重以下五項發展策略[34]：

(一)強化全方位資訊作戰組織

將網路戰力做有系統整合，強化攻、防、蒐一體之全方位網路戰運作機制，並將網路作戰部隊訓練以質精為導向，藉各項演訓及專案任務檢視指管流程、人力調派、實驗編裝及工作績效，逐步辦理編裝調整，以提升組織安全運作的全方位效能。

(二)發展新式資訊攻防戰具

籌劃網路戰攻、防、蒐之網路反制應處之能力，以防範中共對我網路實施攻擊，並藉由產、官、學多方合作，發展智慧型弱點漏洞探測、偽冒、欺敵及誘捕系統等網路攻防系統，以協助指揮官下達正確作戰指令，爭取我作戰時空優勢。另運用多重攔截及網路阻斷方式，遲滯敵作戰節奏，為國軍爭取反制作為。

(三)創造優質資訊戰人力留用環境

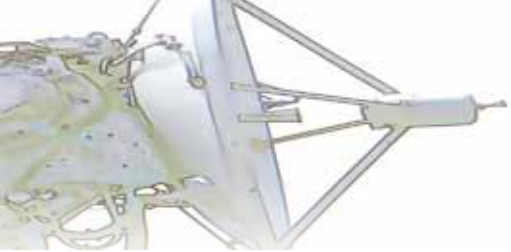
創新軍民網路人力招聘制度，建立網路戰穩固之戰力，並積極建立優質專技人才資料庫，網羅民間頂尖網路專才參與執行與創新網路戰法，以強化網路戰戰力，以利國軍網路作戰任務之遂行。

(四)推動資訊安全跨域合作

藉由資安聯防與溝通機制，定期執行緊急應變演練及網安情資分享，建立軍民一體的聯合網路防護架構體系。持續執行國際軍事交流，發展國際情資交換、人員協訓、議題研討及網安演習等交流，善盡維護網路安

註33：闕志克，〈何謂資安即國安〉，自由電子報，2018年11月26日，http://talk.ltn.com.tw/article/paper/1249488，檢索日期：2019年8月26日。

註34：同註23，頁69。



全之責任。

(五)研擬多元資訊作戰計畫

針對中共指管網路、軍事武器系統等相關重要設施，研發前瞻網路科技及資訊關鍵技術，置重點於提供網路偵蒐、預警及阻絕等功能，掌握網路威脅趨勢，制定多元之對中共網路作戰計畫，以提早封鎖、瓦解共軍網路攻勢。

二、強化資訊戰之建議

自第二次世界大戰結束至今，戰爭型態已從傳統的實體戰爭演化成資訊戰、金融戰、貨幣戰等型態，故資安攻防戰亦儼然成形[35]。資通安全涉及面向相當廣泛，並非單純採購硬體設備，而須同時以管理作為、軟體、認知意識相輔相成，才能有效。有鑑於此，國軍於民國106年6月29日由資訊網路戰、電子戰及資通平臺等三大區塊組成「資通電軍」，並以網路攻防為核心，通訊安全為基礎，電磁發展為前瞻做為三大主要任務[36]，但其資安戰力的養成策略僅以駭客人才的招募與培訓為主，對資安攻防軟體工具的理論探索與精進研發，幾無著墨[37]，實屬可惜。

考量，因應資訊系統運用目標軟體的弱點進行攻擊，已成為不可逆的趨勢，有效整合現有公民營資源，建立精實的國防通資電系統，滿足國軍聯合作戰需求，有效提升國軍整體資訊戰力[38]，至關重要。隨著科技發展日新月異，而如何在防衛作戰中，強化資訊安全已成為當前重要課題，有關重點建議如下[39]：

(一)建立優勢資訊戰力

資訊作戰首重「安全」，故資訊戰的重點乃在網路安全防護，以發展安全防護機制與系統裝備朝向構建自動化、系統化以及資訊化之安全防護系統目標邁進。由被動性的防護進而建立主動性的監偵能量及反制作為，才能確保國軍在防衛作戰中，資訊戰場的優勢，以遏制中共犯臺企圖。

(二)嚴密管控通資安全

配合政府資通安全政策發展，應即著手朝向建置國軍資訊戰防護及通資訊緊急應變、制變作業能量，並結合民間資安防護能量，發展主動積極資訊防護及主動網路監偵能力，以確保通資安全，維持完整指通力、機動力、打擊力，共同鞏固國家政府體制及軍隊通資安全。

(三)強化電戰作業能量

針對未來戰爭型態、電磁戰場環境、敵情威脅及作戰需求，完成國軍電子戰整備工作；並建立橫跨陸、海、空域的整體電戰防護網及局部優勢，俾在臺澎防衛作戰場景下，發揮資通電整合戰力。

(四)籌建聯戰指管鏈路

數據資料鏈路為未來戰場掌握情資、有

註35：謝君誠譯，〈突破資訊戰的枷鎖〉，《國防譯粹月刊》，第24卷，第2期，2007年，頁68-71。

註36：〈資通電軍指揮部編成典禮〉，總統府網站，2017年6月29日，https://www.president.gov.tw/NEWS/21451，檢索日期：2019年8月26日。

註37：陳學智、曾仁凱，〈政府資安防禦，這五步缺一不可〉，聯合新聞網，2018年3月22日，https://udn.com/news/ story/7240/3046715，檢索日期：2019年8月26日。

註38：同註11。

註39：同註23，頁29。

效遂行指揮管制、發揮兵火力之首要工具，國軍秉持聯合作戰需求與指導，整合現有通資能量，充分運用民間科技，整體規劃並建置一套完整的國軍指、管、通、資、情、監偵系統及三軍共通的自動化數據傳輸鏈路，俾以整合、提升新一代兵力、武器系統之有效戰力、制敵克敵。

(五)有效整合通信網路

傳輸平台之建設為爭取「資訊優勢」之關鍵要素，主要係以建置三軍通用戰術聯戰網路為目標，結合國軍現有資通電系統及民間通訊資源，形成軍民共用多重節點、複式網路的通聯手段，藉以充分發揮及運用整體國家資源，提升通資戰力，有效支援作戰。

伍、結語

由於資訊科技不斷更新，國軍的防衛作戰構想中，資訊戰已從配角轉換成重要角色，且資訊戰已從駭客利用網路來竊取機密資料，演進至由網路虛擬空間走向實體利益面向，進而破壞關鍵資訊基礎設施、運用資訊戰力癱瘓、攻擊敵國關鍵資訊基礎設施之作戰思維已然確立。未來戰爭的發展趨勢，不再僅侷限於制空、制海、反登陸的思維，必須適應戰爭型態的改變，將敵、我間對於網路、通訊可能的攻防，及透過社群網路傳播的真、假資訊，納入軍事戰略思維。國軍面對數位傳播時代的來臨，如何打贏複合式的資訊戰爭將是嚴峻的挑戰。

綜觀國軍資訊戰之規劃與整備，乃遵循國軍整體建軍規劃暨作戰需求，積極籌建資訊戰的能力，以發展資訊戰武器裝備。國家正處於現代科技導致未來作戰方式改變的關鍵時期，最重要的任務是在轉變我軍作戰型態時，既不能理想化，也不能無視於可能面臨的困難；然而在資源有限的現實條件下，準確對資訊戰時代的要求做出大膽預測研判，並依此預先做出整體的規劃與決策，以達精準打擊敵作戰節奏為任務，並蓄積國軍「不對稱」網路作戰能力，才能創造「勝兵先勝」之契機。

作者簡介：

林宜昌先生，備役陸軍上校，國防管理學院78年班、靜宜大學管理科學研究所碩士86年班，曾任陸軍第十軍團後指部排長、陸軍金防部後指部組長、陸軍601配置廠所長、國防部人事參謀次長室人參官，現服務於國防部政務辦公室。