臺海作戰新思維—淺談共軍網路戰對我之影響

空軍中校　范元基

提　要

一、網路戰是指利用網際網路作為攻擊的媒介，破壞敵方資訊系統的使用效能和防護己方資訊系統而採取的綜合性行動，也是資訊戰概念底下的一種攻防型態。

二、自波灣戰爭後，共軍見識到西方強國高科技武器及資訊技術對戰爭的影響，開始為「打贏信息化條件下的局部戰爭」，調整了其傳統的作戰思維，積極發展數位化作戰技術。

三、國軍針對共軍網路戰攻擊模式，除應落實預警防護機制外，更應加強資安教育，並研擬因應之道，以確保我國家安全。

關鍵詞：資訊戰、網路戰、網電一體戰

前　　言

軍事作戰的型態在受到政治、經濟、科技、戰略等因素影響之下，其思維也隨之不斷的調整改變，近代戰爭中尤其又以1991年的波灣戰爭，作為開啟了現代化軍事科技作戰思維的經典戰役。[1]人類也從早期的大規模毀滅傳統作戰思維，發展進入了資訊化的作戰思維。面對傳統軍事作戰型態的改變，國軍應如何在有限的資源下，以創新的作戰思維建立不對稱作戰能力，來面對台海未來的作戰環境及軍事威脅，實為當前建軍備戰的重要方向。

俄羅斯軍事學者-斯里普琴科在2002年時提出「第六代戰爭」的理論，引起國際間廣大的關注，使20世紀後期開始出現，典型的「非接觸式」戰爭，其目的是透過強大空、天、電子實施突擊，癱瘓對方重要經濟和設施，這也表現出信息化技術的應用，已隨著高科技時代來臨而產生出新型作戰態勢。[2]2015年5月份，中共頒布了新版《國防白皮書》，對信息化作戰提出了更高的要求。白

1 謝游麟、葛惠敏，〈論戰爭型態之發展與因應〉，《國防雜誌》，第30卷，第1期，2015年1月，頁79。

2 何宜芬，〈習近平時期解放軍人才培育政策初探：傳承與創新〉，《2014中共解放軍研究學術論文集》，2014年12月，頁258。

皮書指出：「根據國家面臨的軍事安全威脅和信息化的建設發展，基於陸海空天電網的多維戰場環境，新的方針要把軍事鬥爭準備的基點，放在打贏信息化局部戰爭上」。[3]近年來，中共在波灣戰爭後見識到西方強國運用高科技武器在戰場上的優勢後，開始重視信息化軍事力量的建設和發展，調整其戰略思維及研發高科技武器裝備，為「打贏高技術條件下的局部戰爭」展開一系列準備。

中共「網軍」在其「質量建軍，科技強軍」的建軍理念下，成為繼陸、海、空軍及火箭軍之後的新一代的科技戰力，其近年來積極發展網路作戰技術，並延伸網路作戰領域，已對歐美各國及我政治、經濟、軍事、心理等層面形成威脅。

因此，台海軍事新思維在未來的戰場上將以空天戰及網路戰(太空和天空)為主，地面戰為輔的作戰模式，成為現代化軍隊建設的重要手段，更形塑出軍隊軟實力的重要工具。[4]

網路戰之定義與作戰手段

2007年初，愛沙尼亞政府計劃移走蘇聯時代的紀念銅像，引起境內俄裔人與俄國政府強烈抗議。同年四月底，愛沙尼亞政府機關、銀行、傳媒的網路系統，同時遭到駭客長達三週的大規模攻擊，事後調查，此次網路攻擊事件係俄國駭客組織透過西方國家電腦所為；隔年八月喬治亞戰爭期間，喬治亞政府網站「非常巧合地」在俄軍進攻前夕被駭客癱瘓，使得喬治亞政府無法在第一時間將俄軍入侵訊息傳遞到全世界；喬治亞電腦專家追蹤發現，這起網路攻擊事件是和俄國政府主導駭客組織Russian Business Network所為，也揭開了人類史上網路戰的序幕。[5]因此，針對於網路戰定義及相關攻擊手段分述如下：

一、網路戰定義

國軍《聯合資電作戰教則》將網路戰定義為：「於網路上實施破壞、阻絕、混淆、造假、摧毀敵存於電腦與電腦網路上之資訊；並為確保我之網路系統及相關設施，免遭敵方欺騙、破壞或降低系統功能，所採取之各種相應措施，以確保網路運用優勢」。[6]簡言之，網路戰是指利用網際網路作為攻擊的媒介，破壞敵方資訊系統的使用效能和防護己方資訊系統而採取的綜合性行動，也是資訊戰概念底下的一種攻防型態。其特色在於網路空間完全不受時間、地理區隔、天候的影響，讓傳統疆界變得模糊不清，而網路戰的低廉成本更使威脅的範圍與機會大增。[7]

共軍網路戰的概念類似於美軍的電腦網

3 華英豪，〈曝光中國神秘網軍信息化戰爭還得向美國學習〉，《環球軍事網》，2016年1月7日，〈http://www.armystar.com/jspl/2016-01-07_34098.html&prev=search〉，(檢索日期，2016年12月2日)
4 同註2，頁259。
5 辜樹仁，〈大陸駭客臺灣練兵〉，《天下雜誌454期》，2011年4月13日，〈http://www.cw.com.tw/article/article.action?id=5000012〉，(檢索日期：2017年1月6日)。
6 國軍聯合資電作戰教則(試行本)，2011年，頁1-2。
7 鈕先鍾，《21世紀的戰略前瞻》，（臺北：麥田出版社，2001年8月），頁148。

路作戰，電腦網路作戰是一種包含軍事與非軍事用途的作戰模式，傳統上認為資訊就是全力透過數位化，以及擴大電腦網路與電子設施，形成更多情報決策所需的資訊。而且電腦網路作戰是一種有計畫的行動，可以使用與擴大這些網路去改善人類行為與企圖，或在戰爭中獲得資訊優勢或防止敵人獲得此種能力。[8]

二、網路戰攻擊手段

近年來世界各國對網路戰的攻擊模式主要區分為：第一、電腦病毒；第二、網路駭客；第三、木馬程式；第四、邏輯炸彈；第五、飽和攻擊；第六、弱點攻擊等手段，[9]分述如下：

(一)電腦病毒

係指專門用來破壞電腦正常運作的惡意程式，其遂行破壞的方法有：傳染性、潛伏性、隱蔽性、破壞性病毒等等。根據網路防毒專業公司趨勢科技分析，中共「網軍」發展初期可能使用的木馬與後門程式可歸納為3隻主要病毒變種，代號分別為BKDR_NETBFX.A(網軍一號病毒)、BKDR_KOTN.A(網軍二號病毒)與TROJ_CONEDRPR.A(網軍三號病毒)。其中網軍一號與二號病毒為後門程式，網軍三號為木馬程式。[10]

(二)網路駭客

係指非法使用電腦系統入侵目標網路系統，隨意瀏覽、竊取與刪改有關資料進行犯罪活動者。駭客可藉由電腦作業系統的漏洞，透過技術手段進入對方的網路系統，也是目前駭客最常用的方法。當前中國駭客分成數群不同的聯盟，包括國際駭客聯盟、歲月聯盟、駭客基地等，約有250個駭客團體，中共當局甚至被外國懷疑其為背後主導黑手。[11]

(三)木馬程式

又稱為間諜程式，具潛伏、窺探等特性，可針對遭受入侵電腦進行秘密入侵，難以被使用者發現。

(四)邏輯炸彈

為一種任務導向的惡意程式，可被設計成獨立運作而不需與原攻擊方聯繫。一旦資訊系統及電腦被植入邏輯炸彈，可於特定的時間或條件下，自動發作而破壞資訊系統及電腦。[12]

(五)飽和攻擊

使被攻擊之目標產生大量的垃圾資訊，以消耗其網路寬頻或系統資源，讓其減低或

8 沈明室，〈解放軍網路戰戰略根源、手段與戰法發展〉，《2009中共軍力現代化國際研討會學術論文集》，2009年11月，頁113。

9 梁華傑，〈網路戰資訊安全探討與省思〉，《國防雜誌》，第23卷，第2期，2008?4月，頁111。

10 楊曉欣，〈中共網軍對我資訊安全威脅之探討〉，2008年1月14日，〈http://www.tcivs.tc.edu.tw/public/tcivsdata/20081144249438.doc〉，(檢索日期：2017年1月6日)。

11 《自由時報》，〈美國國會警告：中國精密網路戰威脅大增〉，2008年11月22日，〈http://www.taiwanus.net/news/news/2008/200811212144301144.htm 〉，(檢索日期，2016年12月1日)。

12 同註9，頁111。

喪失功能。[13]

(六)弱點攻擊

利用被攻目標的系統弱點或電腦弱點所進行的攻擊，使其系統發生錯誤，造成被入侵或是當機。[14]

共軍網路戰發展概況

自1984年中共前領導人鄧小平提出：「開發信息資源，服務四化建設」指導後，中共網際網路建設開始進入發展準備階段。1991年波灣戰爭後，中共受到西方強國高科技武器及數位化作戰的影響，為了「打贏信息化條件下的局部戰爭」，開始強調高科技資訊作戰的重要性，並積極發展資訊網路作戰技術。

目前負責網路戰的單位包括戰略支援部隊、五大戰區、國防科研機關、各級軍事院校等，平時以負責網路竊密滲透，戰時則實施網路攻擊，共軍並暗中扶植民間駭客組織，從旁協助網路間諜活動，據「美中經濟委員會」報告評估，中共「網軍」多達18萬人，另成立「中央網路安全及信息化領導小組」，統合相關部會職能，藉由頂層設計、統籌規劃、創新發展等，企圖建設網路強國。[15]

「網電一體戰」為共軍發展網路戰重要的戰略思維之一，主要在結合電子戰及網路戰力量，以電子武器及網路攻擊建立硬摧毀及軟殺傷能力，癱瘓敵網路體系，奪取戰場網路空間使用權，確保能於戰時，有效運用電磁頻譜與電腦及網路，遂行其一體化聯合作戰體系為目的。[16]共軍自1985年起，就開始規劃發展「網電一體戰」的能量，而其目標是預計在2020年建立全球第一支「信息化武裝部隊」。

2005年起，共軍開始將『電腦網路作戰』融入了演訓當中，特別是在發展攻擊敵人網路的第一擊能力之上。在2007年的《中共軍力報告》當中，美國國防部更是以相當篇幅說明了共軍「電腦網路作戰」。報告當中說：「共軍的『電腦網路作戰』概念」包括電腦網路攻擊、電腦網路防衛，以及其它電腦網路的使用。顯然共軍已經將『電腦網路作戰』當作獲取戰爭早期當中『電磁優勢』(electromagnetic dominance)的重要手段。美國國會的「美『中』經濟與安全檢討委員會」，認為中共「網軍」的「網路戰」作為已由「防禦性」轉變為「攻擊性」。[17]其「網路戰」任務發展概況分述如下：

(一)由共軍戰略支援部隊負責統籌規劃電腦網路運作及戰場網路情報蒐集。

(二)在五大戰區設置戰區聯合作戰指揮

13 同註9，頁111。
14 同註9，頁111。
15 江國顯、于誠森，〈中共網路發展暨威脅之研究〉，《陸軍學術雙月刊》，第51卷第五四四期，2015年12月，頁69。
16 呂兆祥，〈共軍網路作戰對我資電作戰之影響〉，《國防雜誌》，第30卷第六期，2015年11月，頁10。
17 鄭大誠，〈中共網軍的發展與評估〉，《空軍學術雙月刊》，第603期，2008?4月27日，頁9。

部，並成立資訊對抗中心，負責電子對抗及網路資訊體系的防護。

(三)中國軍事科學院及國防大學負責研發各種「網電一體戰」的作戰指導與準則，並積極培育訓練各項執行任務的人員。其運用手段包括：駭客、電腦程式病毒、硬體設備破壞、內部滲透破壞攻擊，以及電磁脈衝攻擊等。[18]

另根據共軍軍事科學院(AMS)發表的新版軍事戰略科學(SMS)顯示，共軍已經建立了網路攻擊部隊，並且將其劃分為三種類型：1.「專業軍事網路作戰部隊」，專門用於實施網路攻擊和防禦的軍事作戰單位；2.「共軍授權力量」，在國安部(MSS)、公安部(MPS)和其他授權組織展開軍事網路戰行動的專家團隊；3.「非政府力量」，自發地參與網路攻擊和防禦，但也可以組織和動員發起網路作戰行動的外部實體。特別值得注意的是，共軍不僅確認了軍事領域的網路作戰，還提到了民間政府機構的網路作戰能力。[19]

共軍近期演訓均模擬在複雜電磁環境下作業，戰時將藉由電子戰、網路戰及欺敵等不對稱方式削弱敵人獲取、傳輸及處理資訊能力。為因應現代戰爭趨勢。共軍也經由網路攻擊來蒐集目標情報以及結合其他攻擊作為，使網路成為其戰力倍增延伸工具；。[20]

近年來，共軍開始嘗試透過網路攻擊手段入侵美國外交、經濟與國防等單位，進行相關情報蒐集活動，並將所獲取之情資運用在其國防工業與高科技產業發展上。根據英國媒體報導，美國國會在「美『中』經濟與安全檢討委員會」表示，共軍網路戰能力不斷提高，可以利用網路戰能力打亂美軍的全球部署計畫。該委員會還表示，共軍的網路戰能力，可能使其得以在局部戰爭中取得優勢。

據該委員會發布的報告指出，美國政府、國防企業與商業部門頻頻遭到來自中國大陸電腦的遠端攻擊。這種遠端網路戰能力可以讓中共「隨時對世界上任何地點發動網路攻擊」。報告中透露，2007年美國共有五百萬台電腦遭到攻擊，美國網路共遭受到四萬三千八百八十起大規模網路攻擊，攻擊總數量比2006年增加了三分之一。此外，該報告也警告說，中共發動網路戰的能力「非常嫻熟」，美國可能無力阻止甚至無從察覺(網路間諜活動)。[21]由此可知，共軍在網路戰的技術發展已不可同日而語，在其國防預算充分的支持下，加速實現軍力現代化的目標，網路戰力逐年持續增長，並已開始挑戰美國在世界霸權的地位，嚴重威脅到美國國家安全與商業經濟利益。

中共在網路上的攻擊對象除了以我國為

18 曾復生，〈美中網路間諜戰最新情勢分析〉，《國改研究報告》，2014年6月9日。
19 華英豪，〈曝光中國神秘網軍信息化戰爭還得向美國學習〉，《環球軍事網》，2016年1月7日，〈http://www.armystar.com/jspl/2016-01-07_34098.html&prev=search〉，(檢索日期，2016年12月2日)。
20 《美國防部2016中共軍事與安全發展報告》，2016年5月13日。
21 〈共軍網路戰力破壞美軍全球部署〉，《青年日報》，2008年11月26日，版4。

主要目標外，其數位化網路戰場也隨著其資訊技術的提升，而逐步擴大到世界各國。近幾年來，各國的政府與商業網站也有曾遭到來自中國大陸網路攻擊的經驗，所遭受攻擊的國家包括南韓、美國、越南等，如表一。

表一　中國駭客攻擊事件表

報導媒體	時間	事件
香港《新唐人新聞網》	2013/5/7	中共利用網路入侵能力，來支援對美情報偵蒐，矛頭指向美國外交、經濟和支持國防計畫的國防工業基礎部門，目的在獲取美國和西方的軍事相關科技，以使中國大陸減少對外國軍火製造商的依賴。[22]
臺灣《ITHOME網站》	2014/12/25	負責南韓23個核電廠的南韓水力與核電公社（Korea Hydro and Nuclear Power，KHNP）在上周傳出遭到駭客入侵，南韓追查來源之後發現，攻擊IP位於中國大陸。[23]
臺灣《自由時報》	2016/10/27	在維州舉行的美台國防工業會議，有分別來自美、台國防工業的與會者收到從臺灣寄出的釣魚郵件惡意程式，但經過追蹤後發現是來自中國大陸的駭客所為。[24]
臺灣《蘋果日報》	2016/7/29	越南河內市的內排國際機場和胡志明市的新山一國際機場，在南海仲裁案宣判後隔日，遭來自中國大陸的駭客入侵，電腦系統首頁留下中共宣示南海主權等言論。[25]

資料來源：1. 陳祐欣，現代版木馬屠城，中共以網路向全球開戰，看雜誌雙週刊，(臺北：華人希望文化事業，第9期，2008年4月)，頁3-4。
2.作者自行整理

共軍網路戰發展對我之影響

1984年4月，美國納爾遜將軍來臺演講中提到：「主宰戰場，18世紀是陸軍，19世紀轉為海軍，20世紀時則是空軍。至於21世紀時，電子、資訊戰將決定戰爭的成敗。」[26]我國是世界資訊產業大國之一，各項產業對資訊設備施的依賴及需求程度有增無減，自2002年起臺灣網路資訊中心持續進行「臺灣寬頻網路使用調查」，至2016年已是第15年進行本項調查。依據財團法人臺灣網路資訊中心2016年臺灣寬頻網路使用調查分析，臺灣地區曾經上網人數已超過1,883萬人，較2015年上升5.7個百分點。[27]由此可知，網路與我們的日常生活愈來愈密切，金融消費、

22 〈中共網路情蒐威脅大〉，《新唐人新聞網》，〈http://www.ntdtv.com/xtr/mb5/2013/05/07/a893096.html〉(檢索日期：2017年1月1日)
23 〈南韓核電廠遭害，IP源來自中國〉，《ITHOME網站》，〈http://www.ithome.com.tw/news/93200〉(檢索日期：2017年1月1日)
24 〈美台國防工業會議遭中國駭客攻擊〉，《自由時報電子報》，〈http://news.ltn.com.tw/news/politics/paper/1046137〉(檢索日期：2017年1月1日)
25 〈中國駭客攻擊越南機場，宣示南海主權〉，《蘋果日報電子報》，〈http://www.appledaily.com.tw/realtimenews/article/new/20160730/918591/〉(檢索日期：2017年1月1日)
26 同註1，頁91。
27 〈2016年臺灣寬頻網路使用調查報告〉，《財團法人臺灣網路資訊中心》，2016年7月，頁57。

經濟貿易、交通及國防軍事等都有賴於這個作業系統。因此，如何維護資訊安全及防範來自網路的攻擊，已成為我國政府和民間所重視的一項課題。

近年來，共軍不斷投入大量人力物力研發提升網路戰能力，並運用其「網路駭客」不斷入侵測試我政府與民間網站資訊系統反應，企圖找出防火牆及系統弱點及漏洞，並進行相關情資蒐集。根據研究，共軍發展網路攻擊能力之目的，主要的考量就是解決臺灣問題，其網路戰戰力除了對我國防安全造成直接影響外，如我國在交通、能源、金融等民生設施及基礎建設遭到共軍網路攻擊，將嚴重威脅影響陸、空交通管制、水電供應、金融市場秩序及新聞傳播功能正常運作，造成民眾心理壓力及社會動盪不安。[28]依據共軍網路戰之發展趨勢研判，2020年共軍資訊戰能力已具備阻塞網路、入侵目標網路、觸發網上病毒及攻擊電子郵件系統能力，可入侵、竄改、竊取世界各國公開性政、經、軍等單位之網際網路，具備使敵方資訊系統癱瘓能力。同時可以攻擊敵方的基礎民生設施或基礎產業設施，及作戰指揮、管制、情報、監視及偵查系統等等。[29]

若對我實施網路攻擊，其影響我政治、經濟、軍事及心理層面分述如下：

一、政治層面

「戰爭是政治的延續」，戰爭是為了達成某種政治目的所採取的行動，「政治性」也是戰爭的本質特性。[30]在中共已將臺灣內部發生嚴重動亂及宣布獨立時機，列為武力犯台條件之一的威脅下，我國必需在健全的民主制度之下，發展穩定的政治局面。在美國總統大選前後，其相關情報顯示認為，俄羅斯駭客攻擊希拉蕊競選總幹事波德斯塔大量的電郵，並在2016年11月8日大選日前一週透過揭密網站「維基解密」把這些電郵公布出來，透露民主黨選戰操盤者令人難堪的一面，企圖影響選情；大選過後，美國前總統歐巴馬也表示，他「低估」傳播錯誤資訊和電腦駭客對民主制度的影響。[31]我國為民主法治國家，總統、縣市首長及各級民意代表，皆透過選舉制度產生。若大選期間中選會或候選人網站，遭駭客入侵竄改計票系統操弄選舉結果，或經蒐集政黨及候選人相關情資後，散布不實言論影響選情，煽動挑起統、獨意識形態對立，都將造成政治動亂不安的局面。

二、經濟層面

冷戰結束後，美、蘇兩大超級強國的軍備競賽也暫時劃下了休止符，此時，世界所面臨的問題是和平與發展，國與國之間的競

28 同註8，頁128。
29 楊太源、王惠民，〈2020解放軍作戰能力評估〉，《2014中共解放軍研究學術論文集》，2014年12月，頁243-244。
30 同註1，頁90。
31 〈俄羅斯駭客干預美國總統大選〉，《風傳媒網站》，〈http://www.storm.mg/article/210853〉(檢索日期：2017年1月13日)

爭也開始轉向以經濟實力為核心的綜合國力競爭。[32]臺灣為海島型國家，水力及電力除了與民眾生活關係密切外，與我國各項經濟產業發展更是息息相關。80年代臺灣經濟起飛，高科技產業出口外銷市場，佔有相當重要的地位，可見其為我國為主要經濟命脈之一。

以2013年半導體產值占我國GDP的比重高達5.33%為例，可見科技產業對我經濟層面的影響及重要性。[33]以目前南科實際用水已達每日 13.7 萬噸為例，其中又以半導體及光電產業用水為最大宗，約佔整體用水量9成以上，如水力及電力控制系統遭敵網路入侵攻擊並運用遠端遙控技術，控制水力及電力供應造成停水或電壓驟降，都將嚴重衝擊高科技產業，造成商業產值損失，連帶影響我國經濟發展。

三、軍事層面

孫子兵法曰：「知己知彼，百戰不殆」，說明情報對戰爭的重要性，未來戰場均講求高科技軍事技術，誰先掌握了敵情，誰就掌握了先機，因此，戰場情資蒐集整合通常是決定戰爭勝負的關鍵所在，指管通資情監偵(C4ISR)系統透過有／無線網路通訊系統，運用各式偵蒐系統及資料處理裝備，提供早期預警掌握敵情，強化戰場資電優勢，並整合三軍武器系統網狀化作戰，提供戰場指揮官下達適切作戰命令。

但在現代戰場透明化的需求下，為了滿足戰情傳遞及戰場資料交換之目的，勢必採取有限度的網路及鏈路開放連結，以建立全軍共通性的作業環境與資料庫，在失去既有封閉型網路系統的實體隔離防護下，也等於打開了一條進入國軍網路伺服器的通道，如未能提升防火牆及傳輸鏈路相關安全加密防護措施，將增加指管系統遭受網路攻擊入侵的風險。

四、心理層面

2011年橫掃整個中東與北非地區的阿拉伯之春(Arab Spring)運動，使社群媒體一躍成為促成政治變革的手段，且成為資訊與情報機構必須掌握的新來源。[34]泰國政府在推特(Twitter)上宣布戒嚴令，同樣可視為藉公開向更多民眾散布重要資訊，以提升透明度的一種途徑，推特(Twitter)仍是泰國民眾藉以和軍方領導的新政府的一種互動機制。[35]資訊心理戰與網路戰歸類為現代資訊戰場中可交互運用之相關攻擊手段，如利用網路社群媒體宣傳偽冒散布不實言論及消息，將可在短時間內對民眾產生極大恐慌及心理壓力。例：2013年4月23日美國知名媒體 AP 美聯社的 Twitter 帳號遭敘利亞電子軍入侵，在網路上發布「白宮恐怖攻擊、美國總統歐巴馬遭炸彈攻擊受傷」的假新聞，經新聞媒體報

32 同註1，頁90。
33 馬維揚，〈半導體產業對臺灣經濟的重要性分析〉，《Industrial Economics Analysis 產經分析》，2014年12月，頁16。
34 Bryan Leese，〈從社群媒體獲取軍事情報〉，《國防譯粹》，第43卷第2期，2016年2月，頁51。
35 同註34，頁10。

導後，立即造成美國道瓊工業指數瞬間暴跌127點。[36]

由此可知，在承平時期的網路攻擊行動，戰場地點不分前線、後方，對象不分武裝及非武裝人員，雖無法獲致決定性的戰果，但藉由新聞媒體播報宣傳，將間接造成民眾心理壓力及恐懼，這就是網路戰對心理層面的具體運用成效，也是最經濟、快速、直接、具威脅性的攻擊方式。

因應共軍網路戰之思考策略

一、以SWOT分析國軍發展網路戰之策略

一場網路戰的發動依其攻擊對象、企圖與目來分析，其攻擊者背後均存在或依附著不同型態的組織單位，以及不同層次的技術資源來操縱支持其網路攻擊行動，藉以達成所需目標任務，獲取相關利益及目的。

以網路「駭客」攻擊入侵國家政府機關與民間商業團體二者為例，因政府機關單位涉及國家政經軍心層面，如遭網路攻擊將影響國家安全與人民生活，故政府機關格外重視資安風險管控，其相關網路防護機制及監控作為，也較一般商業公司團體較為落實嚴密；故針對其網路攻擊入侵行動，往往需要經過長期規劃與訓練，耗費大量人力及物力，且入侵成功機率不高，因此，從事這類網路攻擊的「駭客」背後，均有國家專門特定組織團體長期訓練培養，以及提供相關軟硬體支援，有計畫的針對特定假想敵國家實施網路攻擊入侵及情蒐活動，因其攻擊技術層次高且支援裝備完整充足，對國家安全危害較大；後者則屬一般商業犯罪型的「駭客」所為，其成員僅為個人散戶或無政府組織者，網路攻擊技術屬中下層級，背後也無特定專業團體組織支援，且犯案動機多屬臨時性，其目的也只限於一般商業利益範圍。

近年來，國際間所發生的數起國防工業及民間企業，遭網路「駭客」攻擊入侵案件，經專家調查分析後，其攻擊源極可能來自中國。因此，國軍在面對中共編制組織規模龐大，且專業技術日漸現代化的「網軍」敵情威脅之下，為因應未來臺海戰場之資訊作戰環境，國軍必須積極結合引進民間高科技產業技術，並大量招募儲備資訊人才，跨部會整合政府相關資訊業務部門機構資訊能量，如國安局、調查局、警政署等單位，籌建整體性資訊戰力優勢，以面對敵人對我發起之資訊戰攻擊。

因此，現階段加強防護國軍各項資訊系統安全，避免遭敵利用網路攻擊，對我實施情蒐破壞，有效維護軍事指管能力，並發揮運用資訊戰力，進而攻擊威脅敵人之資訊系統與作戰指揮機制，使其指管系統無法正常運作，影響後續傳統火力發揮，實為國軍發展資訊戰力當務之急。[37]

受到國家當前整體經濟發展困難，以及財政資金短缺的衝擊影響，國防預算在有限的資源分配情況之下，將無法一一有效充

36 〈美聯社Twitter帳號被駭，假傳白宮遭炸彈攻擊新聞〉，《ithome網站》，〈http://www.ithome.com.tw/node/79927〉(檢索日期:2017年1月13日)

37 蔡輝榮、吳宗禮，〈面對資訊作戰之準備、發展與落實〉，《資通安全專論》，2007年，頁22。

分滿足三軍各單位在戰備整備上的需求。但我國在資訊戰力的優勢，在於國民資訊教育普及，資訊建設基礎雄厚，對電腦防毒軟體與網路防護產品的研究深入；對於國軍資訊戰的未來發展，近程應以強化資訊系統安全及建立安全機制為重點；中程則藉由系統整合，籌設電子戰軟、硬體研製能量，提昇頻譜管理技術及強化電子偵測、電子攻擊、電子防護等電戰能力為主；遠程則持續精進戰術、技術研發，以建立自動化、數位化科技部隊及構建攻守兼備的資訊戰力，以有效達成電磁作戰為目標。[38]

前瞻區域安全環境變化，評估敵情威脅，預判國防資源條件與防衛作戰需求等因素，訂定建軍規劃重點發展項目，建立所需的國防武力，以因應軍事衝突與非傳統安全挑戰，因此，強化資電攻防及關鍵基礎設施防護等資通戰力，並結合民間資安潛力，發揮加乘效果，應列為國軍整建新世代優質戰力首要目標。[39]

強弱機威分析法（Strengths-Weaknesses-Opportunities-Threats,SWOT），是一種組織競爭態勢分析方法，其目的主要是透過組織優勢（Strengths）、劣勢（Weaknesses）、機會（Opportunities）和威脅（Threats）等面向進行分析，藉以評估組織未來發展方針。國軍資訊戰力發展在國防預算、組織編裝以及相關軟、硬體設備有限的情況下，未來的發展策略思考方向，可運用優勢—弱點—機會—威脅的強弱機威綜合分析法，將國軍當前與未來的網路戰發展環境，以內部優勢(S)與劣勢(W)及外在的機會(O)與威脅(T)等相關因素，進行國軍發展網路戰戰力之相關策略分析，提供相關單位思考決策及計畫參考運用，其分析結果歸納列表如表二所示。

表二　國軍發展網路戰之SWOT分析表

內部條件	優勢 (Strength)	劣勢 (Weakness)
	1.國防部定期實施資安督檢及資安宣教，有效落實國軍人員資安觀念及危機意識。。 2.資安管控嚴謹，並落實實體隔離政策，有效提升資訊作業環境安全。 3.定期實施資訊戰演練，磨練人員臨場反應及處置作為，並有效偵測系統漏洞。 4.國防自主有效運用國防科技發展成果，厚植資訊作戰能量。 5.國防科技發展依創新不對稱思維，及「科技先導、資電優勢」建軍指導，符合國防科技發展趨勢。	1.因應國軍組織調整，資訊作業人力編制限縮，現行資訊作業負荷過重，影響網路戰執行人力及研發能量。 2.未能統合各單位資訊網路作戰能量。(國安局、調查局、軍情局、警政署)。 3.國軍資訊作業人員培訓練未能與國內大學及高科技產業交流訓練，無法有效全面提升專業水準。 4.國防預算限制，資訊系統設備及研發能量無法適時更新及提升。 5.國軍資訊專業人才退伍流失，基層部隊缺乏經驗傳承。
外部環境	機會 (Opportunity)	威脅 (Threat)
	1.我國在資訊軟、硬體產業(例.防毒軟體等)擁有領先亞太地區國家的實力，另國內寬頻上網普及，具備龐大資料中心運算資源與運作機制，顯示民間資訊產業具發展及支援「網路戰」潛力。	1.共軍積極研發網路戰技術，並結合民間資源，大量招募吸收中國頂尖理工學院學生，培養高科技資訊人才，逐步形成龐大網路攻擊能量。 2.網路社群及智慧型手機發展迅速，增加國軍資安事件風險。

38 同註37，頁21。

39 中華民國106年《四年期國防總檢討》編纂委員會，《中華民國106年四年期國防總檢討》，106年3月，頁30

外部環境	2.財團法人資訊工業策進會及工業技術研究院皆屬國際級的科研單位，藉由技術交流研討，可提升國軍資訊技術。 3.配合勞委會專業證照推廣，培訓國軍資訊類高技術水準專業人才。 4.運用民間大學及研究機構教育資源，簽訂資訊教育培訓交流協議，健全國軍高科技教育環境，培養資訊專業人才。	3.我國每年均肇生多起重大網路入侵資安事件，經查攻擊來源大部分均來自中國大陸。 4.中共逐年增加國防預算，投入高科技武力研發，臺海兩岸軍力已明顯呈現失衡狀態。
策略選擇	SO策略-增長性策略	ST策略-多元化策略
	利用優勢與機會： 利用國內優質資訊發展潛力及資源，擴大加強與民間高科技產業技術合作交流平台，厚植國防自主能量。	利用優勢，避免威脅： 落實營區網路實體隔離作業，加強資安稽核及智慧型手機使用管制作業，另擴大資訊戰攻防演練規模及次數，藉演訓過程加強我方防禦及攻擊能量，並磨練資訊人員臨戰反應。
	WO策略-扭轉性策略	WT策略-防禦性策略
	利用機會，改進內部弱點： 1.與民間大學、研究機構建立資訊人員培訓交流計畫，培養國軍網路戰人才，提升專業能量。 2.研擬增加或設置國防資訊科技專長人員加給或續服役獎金，避免軍中網路戰專業人才退伍流失，影響技術經驗傳承及網路戰力發揮。	克服弱點，避免威脅： 資通電軍指揮部編成，能有效整合網路戰攻防能量(國安局、調查局、資電部、軍情局、警政署)，及推動中科院與民間資訊技術交流。 強化官兵資安觀念，落實資安查核制度，避免肇生危安事件。

資料來源：參考(1)國軍應用「通資電」科技於不對稱戰力之研究，林明武，國防雜誌，第二十六卷第四期，頁89。(2)共軍發展網路戰對我之威脅，周駿賢，「空權與國防」學術研討會論文集，2012年8月2日，頁137。(3)作者自行整理。

二、因應之道

中共已於2016年8月16日成功發射全球首顆量子衛星，該項計畫的首席科學家潘建偉表示，量子通訊技術可確保身分認證、傳輸加密及數位簽名的絕對安全，根據物理力學研究，量子具有不可複製及無法量測的特性，因此透過量子通訊技術傳輸的資料幾乎不可能被竊取，更無從破解。該衛星與地面之間可透過量子通訊技術傳輸資料，大幅提升資訊安全程度，也顯示量子衛星讓中共在通訊資安技術及防駭客領域領先全球競爭對手。[40]

現代軍事科技的發展證明了軍隊人才的智力密集，已顛覆了傳統軍隊的勞力密集智力，在現代戰爭中所起的作用，不是降低而是更佳明顯，未來戰爭人在高技術中的地位，仍佔有決定性的作用。[41]在面對共軍科技戰力的大幅提升威脅下，我國如與其從事軍備競賽，將造成我國財政及軍費嚴重負擔，更增加兩岸軍事緊張之風險。因此，本文依據資訊專家、學者的研究與建議，提出因應共軍網路戰可思考之策略。

(一)健全網路安全機制 強化國軍資安觀念

由於網際網路的技術迅速發展，為生活環境帶來相當大的便利性，但也由於電腦網路功能具有開放性、連結性等特徵，在使用者缺乏相關資安觀念之下，易受到網路駭

40 〈陸發射量子衛星資安大躍進〉，《中時電子報》，〈http://www.chinatimes.com/newspapers/20160817000118-260203〉，2016年8月17日，(檢索日期：2016年11月16日)。

41 同註2，頁259。

客、電腦病毒和其他不法入侵攻擊，大幅提升資訊安全的風險性。尤其，現今雲端技術已成為資訊科技主流，也讓網路惡意攻擊的機率大增，只要雲端系統遭入侵，連接該系統的電腦使用者都會成為「駭客」攻擊的目標。

因此，國軍在網路安全防護的第一要務，就是採取實體隔離機制，控制軍網與網際網路的連結，使網路攻擊者無法透過網際網路入侵攻擊；目前國軍現行的軍、民網「實體隔離」與「專網專用」政策，以及在電腦病毒碼更新、提升網路防火牆、系統弱點掃描及入侵偵測等方面，建置軟、硬體嚴密的資安防護監控機制，雖可大幅降低國軍資訊系統遭到網路「駭客」的外來攻擊，但最大的威脅還是來自於內部的使用者。從國軍歷年來資安違規肇因分析，由於使用者的便宜行事及警覺性不足，如公務家辦、軍民網路混接、隨身碟儲存公務資料等，所造成的電腦病毒感染及機敏資料外洩比例最高。

近年來，各級部隊已奉准辦理智慧型手機試行作業，但由於網路攻擊無所不在，如未能有效管控使用，將增加資安風險。因此，在軍網上傳輸和處理軍事資料應採取相關加密措施，並嚴禁透過手機無線網路功能連接國軍電腦，傳輸相關公務資料，造成電腦病毒感染及網路「駭客」入侵。唯有持恒落實資安教育，強化官兵資安觀念，方能確保國軍整體資訊安全。

(二)結合民間科技產業 建立資訊戰力優勢

一場現代化科技戰爭的發動多以資訊戰手段作為開端，如果資訊戰發揮了作用，也就增加了作戰成功的勝算。近年來，由於國軍組織編裝調整，資訊技術人力及可運用資源有限；相對中共軍事日益現代化結果，已造成台海兩岸軍事逐漸失衡，如與其在傳統三軍武力上進行軍備競賽，將徒增國家經濟財政嚴重負擔；故我國防政策思維除朝向廉價、有效的創新戰術與不對稱武力發展，俾與中共持續成長的軍力相抗衡外，應以全民國防理念獲取全民總體力量支援為重點，確保國軍戰力有效發揮。

國軍網路戰攻擊與防護技術發展，可考量結合國內資訊領域研究單位，除涉及機敏性範圍由國軍自行掌控研發外，餘可針對民間單位不同研究專長領域，適度開放技術交流研發，利用軍民分工合作之效益，期獲得國軍網路戰力之技術提升。除了加強資訊安全防護機制的守勢戰力外，更應運用民間產、官、學界資源及人才，積極建構資訊戰攻擊能量，如發展電磁脈衝炸彈、網路攻擊技術、電腦病毒程式及反衛星武器等新型資訊戰武器，都將讓我國具備資訊攻勢戰力，增加對敵嚇阻力量，確保國軍在數位化戰場上的優勢。

(三)確遵國家資安政策 精進防護機制能量

為建構國家資訊安全政策與防制中共「網軍」等國際駭客攻擊，總統府與行政院日前召開擴大資安會議，將資安策略擴大調整，置重點在國家八大關鍵基礎建設，如能源、水資源、交通運輸、銀行等金融、資通訊、緊急醫療、中央與地方政府、高科技園

區的資安防護。[42]國軍為確保資訊網路安全，應依國安會及行政院資通安全會報指導，建構資安防護機制及網路主動監偵能力，並透過結合各項演訓時機，驗證各單位應變作為，以強化國家整體資安防護能量，精進國軍資安作業機制。

(四)落實設備採購認證 有效維護軍機安全

據softpedia網站11月15日報導，資訊安全公司 Kryptowire 在一些價格低廉的 Android 手機防火牆軟體上發現「後門」，從事資訊安全工作的承包商表示：「它有一個後門，會每隔 72 小時就把使用者所有的短訊都發送到中國。」涉嫌的企業為設計該軟體的上海廣升信息技術有限公司（Adups）。美國手機製造商 BLU 產品公司表示，其 12 萬部手機受到影響。[43]市面上來自中國所生產的相關資訊設備，價格較一般市價低，普遍獲得消費者接受；但不可不注意根據相關新聞媒體報導，中國所生產製造的部分產品疑似遭植入後門程式，能蒐集使用者相關資訊。

國軍現行使用之各項資訊軟、硬體設備及器材，絕大部分是經由委商外購，因此，為防範中共藉由所生產的資訊設備暗藏間諜程式，或植入電腦病毒程式伺機蒐集竊取我相關情資，國軍在資訊設備採購作業中，應確遵部頒涉及大陸地區財務勞務採購相關注意事項規定，不得採購使用中國大陸製造生產相關資訊產品；另採購單位及保防部門也應對承包商實施安全查核，確保國軍資訊設備採購作業流程完備。

結　　語

有鑑於網路戰已成為21世紀新型態的國家安全威脅，政府除了成立行政院資通安全處，也積極推動資通安全管理法的立法，在面對更多網路威脅的同時，國防部於106年6月29日正式編成資通電軍指揮部，擔負國軍資訊、通資及電子戰力整合發揮的任務，作為政府宣示「資安就是國安」的具體行動。[44]

近年來，國軍不斷致力於網路戰攻防軟、硬體建設及組織編裝擴充之際，惟在面臨民間知名科技企業以高薪網羅國防科技人才的影響下，往往造成軍中科技人才流失不足情形，嚴重影響資訊戰力發揮；國防資訊科技人才培養不易，國軍如何研擬設置提高科技資訊專長人員特種津貼及續服役獎金，或藉由改善部隊工作環境等有效措施增加誘因，吸引民間優秀青年加入國軍，並留住軍中人才，實為當前國軍發展科技作戰重要課題之一。

面對未來台海戰場，共軍作戰構想將

42 李欣芳，〈八大基礎建設，將強化資安防護〉，《自由時報》，2016?8月28日，〈http://news.ltn.com.tw/news/focus/paper/1026114〉，(檢索日期，2016年11月27日)。

43 〈中國軟體Adups公司被指在Android防火牆程式留後門〉，《INSIDE資訊網站》，〈https://www.inside.com.tw〉，2016年8月17日，檢索日期，2016年11月21日。

44 黃彥棻，〈臺灣網軍跨出第一步，資通電軍指揮部正式成立，第四軍種成軍在即〉，《ITHOME新聞》，2017年6月29日，〈http://www.ithome.com.tw/news/115209〉，(檢索日期，2017年7月4日)。

仿效美軍在第一次波灣戰爭的經驗，利用資電作戰之軟、硬殺武器及手段，作為第一波攻擊行動的發起，先期癱瘓我指揮、管制、通信、資訊、情報、監視及偵查中樞指揮資訊系統，大幅破壞我指管能力後，取得戰場資電優勢，進而擾亂分散我三軍指揮統合能力，藉以降低其攻臺作戰人員裝備，遭我陸、海、空兵火力反擊的傷亡及耗損率。

「重層嚇阻，防衛固守」，現為我國軍事戰略方向，在面對中共至今仍不放棄以武力解決臺灣問題的威脅下，為達成有效嚇阻甚至多重嚇阻之目的，國軍在網路戰的發展規劃及基礎建設上，如果只是單方面建構消極防禦態勢，已不足以應付這場沒有火藥味的網路戰爭。

因此，國軍除了鞏固提升既有的網路防禦及監控機制外，更應善加運用國內高科技產業優勢環境，招募培養民間優秀資訊專業人才，結合軍民技術及力量，深入發展網路戰攻勢能力，建立一支現代化的網路戰勁旅，以確保中共或任何國家在考慮對我發動網路攻擊時，產生威脅嚇阻作用，並有能力對其實施後續報復作為，也達到宣示我國在資訊數位化戰場上戰備整備的決心。

作者簡介

范元基中校，空軍通校84年班，空軍指揮參謀學院100年班。曾任分隊長、中隊長、作管長。現為國防大學空軍指揮參謀學院中校教官。

日本航空自衛隊E-2C早期預警機，隸屬航空總隊直屬的警戒航空隊。(照片提供：張詠翔)