通資安全

建立國防資電優勢與網路戰攻防理論技術發展分析研究

空軍上校　吳嘉龍

提要

一、邁克菲實驗室(McAfee Labs)2014年元旦發布了《2014年預測報告》，借助其獨有的邁克菲全球威脅智慧感知系統，對2013年安全趨勢進行分析並對新一年的威脅態勢作出預測，未來移動資訊化將進入建設高峰期，在2014年研究發展的移動平臺技術將主導成為惡意程式攻擊威脅之無形戰場。

二、針對日新月異的網路駭客手法，已有演變成國家層級大區域範圍的趨勢，正由於現代戰爭作戰速度急劇加快，國防戰略所發展之資訊戰，全面結合指揮、管制、通信、資訊及電子戰等範疇的作戰方式，已演進為資訊戰爭之新型態作戰，建立國防資電優勢與深入探討網路戰攻防理論技術發展為本論文研究目的。

三、就國家安全方面而言，資訊網路攻擊可以成為一種強大的軍事武器，它是屬於資訊戰的一環(資訊戰的武器中就包括電腦病毒、蠕蟲、木馬、殭屍程式、邏輯炸彈及分散式阻斷攻擊DDoS等)，惡意程式將成為新的網路作戰攻擊手段，在未來戰爭中資訊武器將扮演重要角色，我們應加強資安防護能量以確保國家安全。

關鍵詞：資安威脅、資訊作戰、國家安全、資訊優勢、惡意程式攻擊。

壹、前言

隨著資訊科技快速發展與創新，無線網路傳輸快速與普及，使得資料存取管道及傳輸更加便利，【註1】在此同時，機密資訊遭受竊取與破壞的風險也隨之大幅提升，網際網路已成為一個沒有邊界與無聲的戰爭平臺，資訊戰是一種低成本、高效益的攻擊武器，技術高超的網路駭客，隨時可能藉由網路侵入防護能力薄弱的電腦進行破壞。【註2】「網路即戰場」，做好資訊安全工作就是做好戰場管理，這是資訊安全防禦應有的認知。【註3】美國國防部對戰略的定義是「戰略是平時和戰時，發展和運用政治、經濟、心理、軍事權力，以達到國家目標的科學與藝術」，將網路活動歸類在「電腦網路作戰」的範疇(包括防禦、攻擊與運用3個要素)，而對「軍事戰略」的定義是「運用或威脅使用一國的武裝力量來確保國家政策目標的科學與藝術」；美國陸軍戰院則將「戰略」定義為目的、方法與手段之間的一種平衡關係，未來美國軍事作戰將包括網路領域，聯合作戰與武器系統控制均於網路進行。【註4】軍事戰略規劃目的在使國家武力之整建、發展與運用等一切軍事工作，能在整體考量下，密切協調配合，循一定之目標、戰略構想與統合之政策，做有系統之規劃與建設，以達成創機先制與危機應變的有效國防。【註5】

資訊安全防護技術在身分識別與存取管理考慮包括不同應用軟體、硬體平台與作業系統外，更須針對儲存方式、目錄管理、存取管理、使用者管理與申請流程、密碼管理以進行審核與規範管理，並落實網路安全風險管理與有效強化資訊防禦能力，以因應層出不窮資安威脅，【註6】2013年12月美聯社報導德國《明鏡周刊》揭露美國國家安全局駭客部門作業，披露偵監人員攔截電腦交貨、利用硬體漏洞，甚至劫持軟體巨擘微軟公司資安漏洞回報系統以監控網路攻擊目標。中央社華盛頓2013年11月20日法新報導顯示，電腦和行動裝置惡意軟體愈來愈多，原因在於駭客具備迴避關鍵安全措施能力。網路空間已成為全新作戰領域，在這個新戰場，美軍採取積極措施以保持其網路戰能力的領先優勢。2014年以來，美軍網路空間司

註1　陳勁甫，〈論國防戰略規劃之思維架構－國防二法之角度〉國防雜誌，第18卷第14期，2003年，頁15~16。
註2　張大順，〈資訊作戰之研析-論網路攻防〉《國防大學第一屆國家安全軍事戰略學術研討會論文集》，2000年11月30日。
註3　歐陽宜珊，〈對抗中國「網軍」防毒公司加入戰線〉《東森新聞報》，2003年9月5日。
註4　資通安全資訊網，〈國家資通安全會報第201401002期資通安全資訊網電子報〉，2014年1月3日。
註5　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》，第82期，2004年，頁187-218。
註6　資通安全資訊網，〈國家資通安全會報第201312002期資通安全資訊網電子報〉，2013年12月31日。

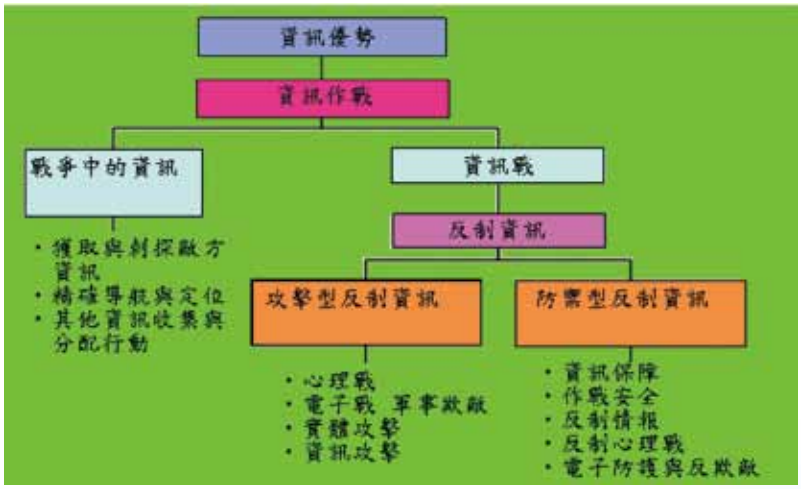
令部大幅擴編，宣布成立40支全球作戰網路戰部隊，秘密制定網路戰規則，並由北約率先推出塔林手冊，意圖作為網路戰國際法典，美軍網路空間國際化明顯加快。【註7】根據國家實驗研究院科技政策研究與資訊中心2013年3月「國安層級應變-我防駭大作戰資安納入兵推」報導，研究指出全球網路戰爭煙硝瀰漫，我政府也全面提升備戰準備，應變機制拉高到國安層級，包括行政院配合修法，由政務委員張善政、國安會諮委袁桂笙共同擔任國家資通安全會報召集人，協調政院資安辦公室、國土安全辦公室、國安局組建一支台灣版網路部隊，全面展開防駭大作戰。【註8】

資訊戰就其層次可分為社會國家、戰略、戰術及戰場等層次，在此，針對中共發展與威脅加以分析，中共將資訊戰稱為信息戰，共軍積極整備朝建立整體優勢電子戰能力的目標努力。網軍利用網路對我實施資料竊取與情蒐工作，侵入敵方指揮網路系統，進行瀏覽、竊取、刪改有關數據或輸入假命令、假情報、破壞敵方整體作戰自動化指揮系統。中國電子戰(稱之為電子對抗)相對各項武器系統中電子設備所占成本大為增加，電子設備技術為先進武器、裝備核心及神經中樞；未來戰爭並積極爭奪制電權成為戰場核心，亦為戰爭「第五種戰場」，武器與裝備能否發揮效力，作戰行動能否成功，均取決於掌握制電權優勢一方。【註9】中共主要攻擊模式發展趨勢是利用衛星、通資網路偵搜系統來竊取政治、經濟、軍事戰略，並透過電腦病毒、電磁脈衝炸彈攻勢作為，來干擾武器、戰情系統。共軍自1993年起，歷次重要演訓均將三軍聯合作戰電子對抗列為重要課題。攻勢作戰任務包括節點破壞、系統癱瘓、電磁封鎖及實體摧毀；守勢作戰任務包括輻射控制、隱真示假、網狀配置以攻助防等。中共國防大學並針對未來高技術戰爭中聯合作戰方式作系列研究，將成果頒發部隊全面施行與進行論證。共軍已完成編制內電子對抗團、營組建及對抗課目演練，且配合戰區內戰役指揮體制、指揮所內部結構、程序及資訊傳遞等重要環節運用，具戰區電子對抗作戰基本能力。中國軍方對信息戰籌建方面，包括自美輸入超級電腦、電腦輔助設計軟件等技術；在東南沿海建置16條光纖通訊網路，分別是南北向及東西向各8條，並利用全球衛星作遠程航海精確導航；加強指揮、管制、通信、情報等抗干擾能量，軍事演訓更加入電腦病毒植入科目；加快量產並戰備部署電磁脈衝微當量核彈。依據中共發展策略分析，未來共軍資訊戰力包括軟殺傷與硬破壞的攻擊能力將普遍獲得提升，對於我通資系統影響不容輕估。【註10】

註7　廖宏祥，〈中共資訊戰攻擊能力與可能行動〉《聯合報》，2000年8月23日。
註8　劉德彥，〈論中共電子戰戰力與我因應之道〉《陸軍月刊》，第41卷第481期，2005年9月1日，頁59-62。
註9　新華網，〈新華軍事美軍網絡中心戰的理論與實踐：有九大核心系統〉，http://big5.xinhuanet.com，2008年03月25日

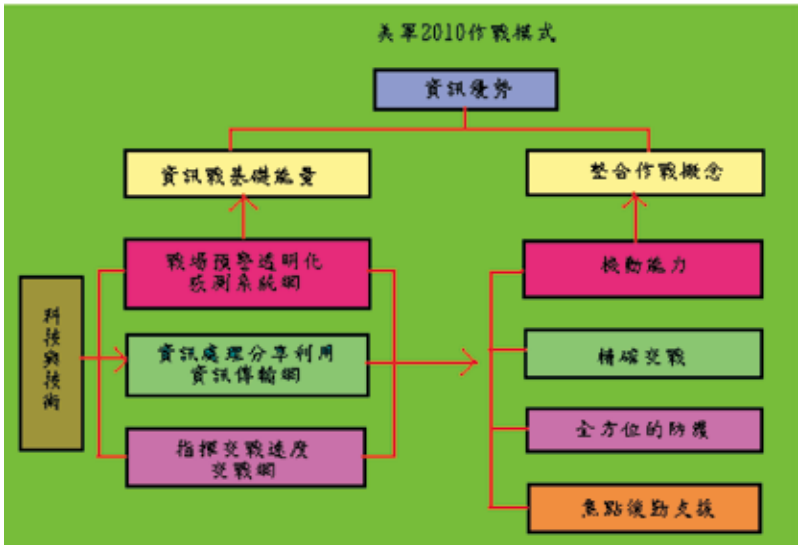
貳、美國與中共資訊電子戰發展探討

資訊戰是資訊化戰爭的核心，網路戰是資訊戰的特殊形式，屬於資訊戰範疇，網路中心戰是傳統戰爭型態向資訊化戰爭型態的產物，因為資訊網路發展而帶來作戰型態的更新【註11】。中共在1981年底由共軍總參謀部頒布「六大作戰能力」綱領，自1985年中共整編陸軍電戰部隊後，電戰部隊的構建開始邁向發展階段。根據美國國防部2010《中共軍事與安全發展》報告指出共軍在2004年首次提出資訊化，中共認為戰前加強對敵電子裝備之偵察，為其取得電子對抗主動權的首要措施，電子戰戰力包括陸、海、空三軍，以共軍目前龐大之電偵能量，於大陸東南沿海廣設電子偵測及通訊偵察基地，60多年來對我通資電設施及陣地使用之各項電子參數蒐集從未間斷，其所偵獲的電子情報，可供平時演訓與戰時運用。在2004年《中共的國防白皮書》指出，共軍加強質量建設，推進以信息化為核心的中國特色軍事變革，中共將資訊戰界定為知識戰爭，藉由「中國特色軍事變革」，致力取得不對稱的「資訊戰」優勢，在與美國、日本交手相對不利的戰略態勢下讓共軍立足打贏『信息化條件下』的局部戰爭，期能獲致對全局有決定性影響的戰果。由此可見，在台海衝突中，共軍各類『信息化條件下』的攻擊形態都有可能出現，包括「戰略訊息戰」。【註12】中共北京軍區於2007年9月中旬在某戰術訓練基地舉行代號「北劍



圖一、傳統美國資訊戰模式(資料來源：作者自行整理)

註10　陳岳揚，〈中共陸軍電子戰發展之研析〉《陸軍月刊》，第49卷第528期，2013年4月，頁50-66。
註11　陳偉寬，〈試論歷次戰役中電子戰運用與影響〉《國防雜誌》，第19卷第12期，2004年12月，頁64-65。
註12　梁正綱，〈台海衝突終的戰略資訊戰〉《國防雜誌》，第23卷第1期，2013年2月，頁51-60。



圖二、新一代美國資訊戰模式(資料來源：作者自行整理)

-0709(T)」軍演，演練目的是驗證電子戰複雜電磁環境下資訊作戰與訓練，假想敵部隊配屬裝備先進電子對抗分隊實施軍事訓練，以提升部隊抗干擾和防自擾能力，而美國在國土安全防衛部分，會加強與重視是在九一一恐怖攻擊事件，美國並進行了各種的組織變革，以確保國土安全。所有這些措施的目的均在於強化及整合聯邦政府與政府個部門內部的國土安全作為，圖一為傳統美國資訊戰模式；圖二為美國2010資訊作戰模式【註13】。

美國陸軍戰院把戰略架構視為目的、手段與方法的一種關係，亦即依據目的(目標)，考量手段(用以追求目標可用資源)，策定方法(組織與運用資源方式)。美

表一、美軍資訊戰發展原則(資料來源：作者自行整理)

項目	內容
使用時機	資訊戰在戰爭爆發前使用：在宣戰及採取實際軍事行動前，即打敗潛在的敵人
相互配合	資訊戰負責機構與情報界的資源密切結合，以確保對電腦與資訊網路目標能有效的識別與處理
攻擊模式	利用攻擊性資訊系統，如電腦病毒和高能微波武器等，摧毀敵方的電腦、通訊系統及資料庫
科技防衛	因應今日網路攻擊多以竊取重要資料及原始碼為攻擊目標，積極發展智慧型軟體能量，以侵入敵方的資訊系統

註13　朱豔芳，〈美軍聯戰願景塑造全方位建軍圖騰〉《青年日報》，2007年9月5日，版4。

軍運用全球資訊網格(Global Information Grid, GIG)建立數位資訊與通訊戰鬥力(包括戰術、作戰與戰略層面的行動)，支援「2010年聯戰願景」與「2020年聯戰願景」的全方位資訊作戰概念，保護及防禦資訊及資訊系統，以有效規劃、指導、執行與協調執行資訊作戰行動之資料，資訊作戰行動可能包含攻擊工具，如公共事務、民事、心理作戰及電腦網路攻擊，且均可能於潛在衝突開戰初期展開作業表一為美軍資訊戰發展原則。

【註14】「戰略」是運用各種手段來達成政策目標的指導與構想，為有效發揮目標、手段與有限國家資源的戰略，必須建立一套戰略規劃(strategic planning)制度來達到整合的效益。美國在改進國防管理與指導功能方面的建議包括配合新總統任期之始執行「四年期戰略總檢」(QSR)，並建議由國家安全會議之跨部會工作小組來執行；運用不同的兵力規劃概念來評估各種不同的兵力/能力組合的可能性及相對效益；完全地重新建構國防部現行的「計畫預算制度」(PPBS)。【註15】戰略制度必須依據國家使命、目標與利益價值，考量未來國家安全所將面臨內外部的機會、威脅、挑戰與國家資源的限制，透過戰略規劃的程序作有效的垂直與平行整合。五角大廈研究部門「國防先進研究計畫局」(DARPA)2012年12月發布名為「基礎網路戰」，簡稱「X計畫」的文件，這份52頁的綱要揭露美國對於未來網路戰的規劃。X計畫最優先目標是一套能標出全世界數十億台電腦網路位址的綜合地圖，美國軍方希望能藉此加強軍隊精準打擊敵對電腦網絡的能力。「X計畫」專案指出，希望能針對未來任務，發展出各種獨特且針對特定情況的戰術，針對不同情況，採取不同戰術，除徹底整頓國防情報局，美軍也希望能創造更強健作業系統進行更快速的網路惡意程式攻擊行動並有效防禦來自外界的網路攻擊。過去十年來，美國國防情報局主要重點放在與伊拉克和阿富汗的戰事。華盛頓郵報指出，五角大廈的情報蒐集重點是非洲的伊斯蘭激進組織、北韓和伊朗的武器移轉，以及中共軍事現代化進程。依據2013年3月22日報導，中美網戰上升至國家層級，在美國副國務卿荷姆茲發出警語後，美國國安顧問杜尼隆近日亦首次點名北京，要求嚴肅面對網路駭客。中美網戰多年，2013年2月19日《紐約時報》發布資安公司Mandiant的報告指出，浦東外高橋路一幢十二層建築，是代號「61398」的解放軍網軍總部所在。該部隊自2006年起竊取141家公司數據，其中115家位於美國，目標包括資訊、電信、航空等。【註16】

註14　曹乙帆，〈2013資安防衛戰七大元件缺一不可〉《網路資訊雜誌》，254-255新春號，2013年1月10日。
註15　張道宜，〈美砸33億推X計畫確保網戰優勢〉《國防部軍事新聞》，2012年12月3日。
註16　同註13。

表二、美國全球資訊網格內容分析表(資料來源：作者自行整理)

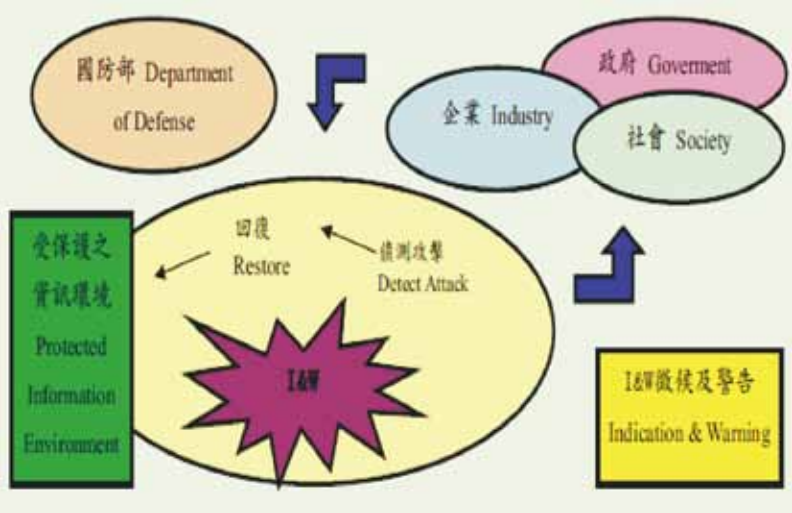
GIG內容	內容
資訊網格	網格計算是一種經由網際網路分享電腦運算能力和資料儲存容量的服務，目的為處理複雜資料龐大的科學運算。
感測器網路	感測器網路元件包括太空、空中、海上、地面及連網的偵測器，擴展了傳統資源管理能力(如涵蓋範圍、精確性及目標識別)，尤其在資料收集與獲取上更突破以往無法達到的優勢。
接戰網路	可定義為安裝在資訊網格上的多重武器載台或系統的集合，以互聯網路取代單一載台或系統，其組成包括指揮與管制、機動武器載台及支援部隊

參、美國資訊中心戰與建立不對稱戰力

在1999年9月美軍國防部首席資訊官發布了全球資訊網格的備忘錄，強調網狀化作戰基礎-全球資訊網格(GIG)包括資訊網格(Information Grid)、感測器網路(Sensor Networks)及接戰網路(Engagement Networks)等三部份組合而成。美國國防部亞太安全事務助理部長葛瑞格森(Wallace C. Gregson)2009年9月28日在維吉尼亞州夏洛斯維爾舉行的美台商會國防工業會議中以“2009年美台防禦關係”發表專題演講，在公開演講表示「對中國快速經濟成長與軍事現代化，應尋求重質不重量的方式，考量未來國防預算分配與軍事轉型，台灣再也沒無法以量的優勢，取勝中國；台灣必須專注在『創新』與『非對稱』的作法，尋求質的優勢」，【註17】國軍面對太空、空中、地面、水面等多維的威脅，應以網狀化作戰(Network Centric warfare, NCW)的先進概念為核心，運用通資電科技的創新，以發揮國家資訊優勢進行不對稱戰力之建構。美軍「2010年聯戰願景」強調運用資訊優勢遂行機動、精準接戰、全方位防護及集中後勤之作戰構想，最終目的在達到全面主宰戰局。從網狀化作戰之定義：「主要是藉由各作戰實體之有效鏈結或網路連結以提升戰力，其特性在於經由自行同步及網狀作戰模式，以提升分散部署兵力之情蒐作業(戰場知覺)能力，並有效加以利用以達成指揮官之意圖」，作戰模式與傳統作戰環境相較，具以下四個特性：打破距離限制；網路資源多元化；指揮管制方式互動化；部隊間合作緊密性。表二為美國全球資訊網格GIG內容分析表，圖三為美國資訊作戰攻勢流程示意圖。【註18】

美國認為資訊安全所造成威脅，已出現在諸多層面，包括對個人、團體、政府

註17　林明武，〈國軍應用通資電科技於不對稱戰力之研究〉國防雜誌，第26卷第4期，2013年，頁87~102。
註18　國防部，〈四年期國防總檢討〉，國防部首次「QDR」建立四年一期檢討機制，2011年11月12日。



圖三、美國資訊作戰攻勢流程示意圖(資料來源：作者自行整理)

表三、資安攻防資訊戰三要素(資料來源：作者自行整理)

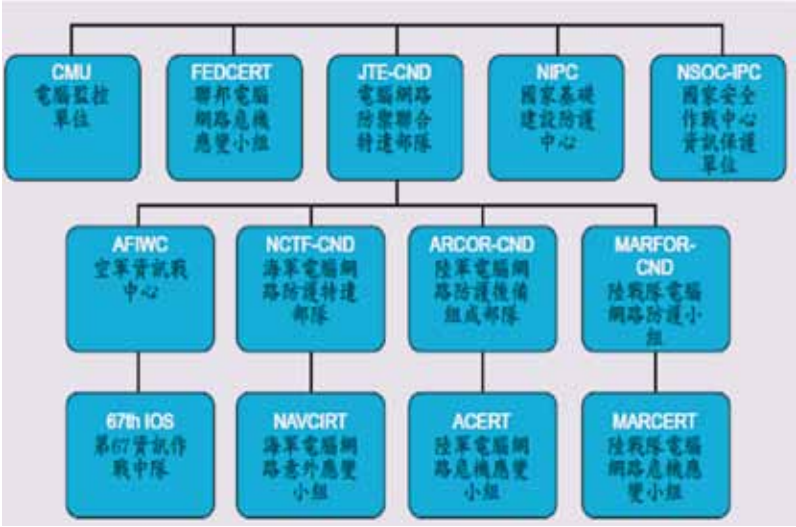
項目	內容
構成要素	攝影機、電腦、電視、電話、電纜、微波、有線電、光纖、衛星等
服務內容	網際網路、公用電話網、線上服務、公用資料網、廣播電視網、直撥衛星、手機網、運輸網、防禦資料網、加密及商用衛星網等
應用領域	新聞、運輸、健康安全、娛樂、航海、情報、天氣、軍事、政府部門等

表四、美國資訊戰作戰模式分析(資料來源：作者自行整理)

項目	內容
裝備優勢	以資訊戰武器裝備優勢，實施資訊威嚇
偵察敵情	以先期偵察，先發制人手段，實施資訊壓制與攻擊
形式壓制	資訊壓制與攻擊實施資訊中斷
攻擊摧毀	以電腦病毒摧毀敵方資訊系統
資訊封鎖	以資訊保密和資訊攻擊手段，實施資訊封鎖
攻守兼備	以資訊攻擊和資訊防護，爭取資訊優勢

部門，乃至整個國家，幾乎已無所不在。而從軍事革命的特色觀之，未來軍事革命的不斷被深化，將對軍事領域的空間、時間、效能與觀念產生重大的變革影響，導致其發生一系列的變化。[註19]「四年期國防總檢」是重新制定戰略與檢討國防政

註19　國防部，〈四年期國防總檢討〉，國防部發布新聞稿說明「102年《四年期國防總檢討(QDR)》」報告，2013年3月13日，存取時間2014年1月4日。



圖四、美國國防部CERT組織架構示意圖(資料來源：作者自行整理)

策優先順序及國防資源分配的有用機制，美國國防部於2008年將網際空間定義為一種作戰領域，值戰爭的作戰層級時，網際空間作戰與陸、海、空作戰最為相似。美軍認為聯合部隊指揮官必須具備網際空間指管能力，以遂行聯合作戰任務，美國國防資訊系統局(Defense Information System Agency)強調在戰爭作戰層級中，電腦網路防禦(computer network defense, CND)是網路最主要的工作，表三為資安攻防資訊戰三要素，美國資訊作戰準則主要目標為美國在實行資安防衛部分主要以應用領域、內容服務及構成要素三個方面去動作，美國資訊戰作戰模式分析如表四。[註20]圖四為美國國防部電腦緊急應變小組(Computer Emergency Response Team, CERT)組織架構示意圖。

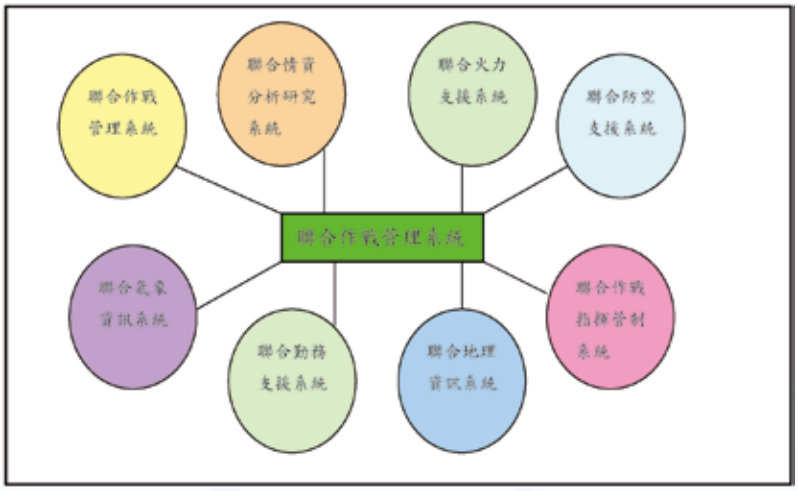
肆、我國四年期國防總檢討與精進方向

我國國防係以保衛國家安全、維護世界和平為目的。對中共而言，資訊戰是共軍建構數位戰場首要指標，資訊戰中電腦病毒戰是一種作戰手段，是以電腦病毒為作戰武器而進行干擾、破壞、竊取、摧毀等攻擊。中共就建制專責網路作戰的網軍，網軍是專門負責資訊戰中的電腦病毒戰、電腦網路戰和駭客戰，一旦病毒發作，會癱瘓整個網路甚至資訊指揮控制系統，造成嚴重的影響，共軍戰略家將資訊戰力與資訊化視為軍事發展躍進的一種戰力，資訊戰全面結合指揮、管制、通信、資訊

註20 行政院科技顧問組，〈2010資通安全政策白皮書〉，http://www.nicst.ey.gov.tw，存取：2014年1月4日。

及電子戰等範疇的作戰方式，開啟了所謂資訊戰爭之新型態作戰。數位化戰場係以科技為主導、資訊為中心之數位戰爭，資電優勢、科技先導是決定數位化戰爭的先決條件。隨著資訊技術和高科技工業高度發展，使得戰場指揮管制作為、武器接戰效能與情報資訊傳遞程序迅速邁向數位化時代，高科技與數位化技術影響，使傳統作戰型態改變，尤其在指揮管制程序與情資傳遞數位化戰場時代，指揮戰力整合系統為戰爭獲勝關鍵，網路成為軍事作戰重要工具，而數位化戰爭內容包含指管通資情監偵(C⁴ISR)系統，在敵暗我明的網路世界，要取得網路戰、資訊戰勝利，勢必得投入可觀經費與人力進行研發。

「四年期國防總檢討」即所謂的「QDR」(Quadrennial Defense Review)，我國「QDR」最重要的意義，在於國防部可透過這項法定文件的檢討與編纂，將總統的國防理念貫徹在國軍的各項建軍備戰工作中，並接受立法院的監督，也使國軍可以建立以四年為一週期的通盤檢討機制，針對重大政策、國防戰略、計畫及施政措施，定期檢視其適切性，進行適當的修訂或調整，使其更為週延可行。《四年期國防總檢討》係我國防最高戰略指導文件，為國軍「十年建軍構想」及「五年兵力整建計畫」策訂之準據，對內具有指導建軍整備方向的功能，對外則有助國內民眾及國際社會瞭解政府國防目標。【註21】三軍聯合作戰為戰爭致勝關鍵因素，面對當前各項安全威脅及有限的國防資源，國軍必須以「創新/不對稱」思維，提升聯合制空、制海、地面防衛作戰等主要戰力，持續發展聯合指管通資情監偵及資電作戰能力，同時整合後勤整備能量、加強後備動員與協同救災作為，俾達「平時能救災、戰



圖五、數位化戰場管理系統示意圖

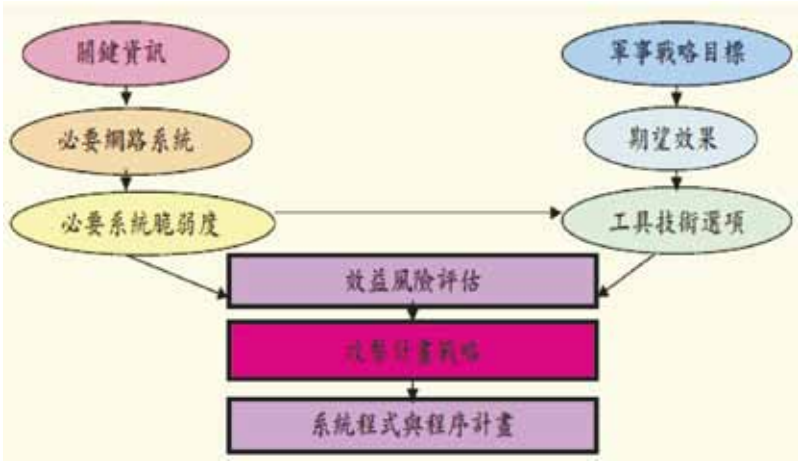
註21　同註17。

時能作戰」的整體效能。民國102年《四年期國防總檢討》架構秉承總統國安理念、黃金十年國家發展願景及「上兵伐謀」戰略思維，從不同的領域凝聚全民國防共識，因應現代戰爭科技型態急速發展，國軍早已積極發展高科技武器資訊系統，國內主要由中科院發展各式軟硬體，並區分資訊系統、電信網路技術、指管通情技術、雷達天線技術、寬頻天線研製技術、自動化控制技術、資訊處理技術、微波技術等技術。為確保國家長治久安，在此對於國軍精進方向加以建議與探討，面對未來戰爭的迅速發展，建立通資電不對稱戰力之國軍數位化戰場管理系統至為重要，透過網路資訊快速傳遞、資訊系統資訊處理及現代武器裝備快速反應能力，使各項武器的精準效能得以整合與發揮，通信及自動化指揮系統在戰場上運用自如；國軍數位戰場管理系統應包括「聯合作戰管理系統」(提供國防部各聯參與戰略執行單位作業運用)、「聯合兵種管理系統」(提供軍種參謀與聯兵旅級作業運用-以陸軍為例說明)與「部隊管制系統」(供營級含以下部隊的機動載台作業運用)三個層級，圖五為數位化戰場管理系統示意圖、表五為未來防衛作戰需求整理表、[註22]圖六

表五、102《四年期國防總檢討》未來防衛作戰需求整理表(資料來源：作者自行整理)

項目	內容
1	兵力規劃、籌建與部署應防範敵之封鎖作戰，以及可能的奇襲、斬首或其他不對稱戰法，另置重點於強化遠海快速反應與應援能力，以逐步建立符合我防衛作戰需求之現代化國防武力。
2	各軍(兵)種戰力、部隊組織、指揮機制、準則教範、戰術戰法及教育訓練等，持續朝聯合作戰形態整合，以求戰力倍增，創造局部戰場優勢。
3	各主要武器系統與載臺之間應獲得更高程度的系統構連，縮短「偵測—處理—決策—行動」之決策循環，使整體戰力達到指揮管制有效便捷、通訊聯絡即時無礙、打擊火力精準高效之目的。
4	面對敵突襲之威脅，國軍在防禦上應力求作戰功能備援與存續，並加強關鍵基礎設施防護，避免於作戰初期遭受突襲而癱瘓，無法遂行戰略。
5	各項戰力發展應講求作戰效率與兵、火力機動轉用，力求反應更迅速、運動更靈活，俾於戰術上制敵機先，扭轉不利態勢。
6	針對敵作戰重心與關鍵要害，國軍發展「創新/不對稱」戰力，俾於遂行防衛作戰時，運用有利時間與空間，阻滯或癱瘓敵攻勢。
7	依軍事戰略構想，本「常備打擊、後備守土」之理念，落實人、裝、訓合一之軍隊動員整備工作；並精進與行政動員體系相結合之規劃作法，以迅速動員後備人、物總力，充實三軍部隊戰力，達成防衛作戰任務。
8	網路資安防護是當前重要國防課題。網路空間已成為現代戰爭之重要戰場，一旦衝突爆發，將癱瘓我指管、後勤網路，以遲滯國軍應變。據此，國軍須嚴加因應，並配合政府各部門力量，確保資訊安全及網路暢通。

為攻擊性資訊作戰戰略示意圖。



圖六、攻擊性資訊作戰戰略示意圖(資料來源：作者自行整理)

伍、結論與未來因應作為

JGospel 2011年9月21日報導，日本三菱重工等軍事工業服務器接連遭中共駭客襲擊，導致大量資料外洩，引起日本政府的高度重視。網際網路的發展讓全世界的資訊可以共享，對組織來說，網路帶來無比的工作便利性並大幅提升了工作效率，但卻也同時成為有心人士利用做為電腦犯罪的最佳途徑。【註23】越是發達及資訊化程度越高的國家，對資訊設施的依賴性就越重，所以在個人方面，我們必須加強對資訊安全的重視及惡意程式的認知，才能有效防止這些惡意程式的氾濫；在國家安全方面，應積極研究資訊網路攻擊、防護及反制的方法，以確保國家的安全。【註24】在敵暗我明的網路世界，要取得網路戰、資訊戰的勝利，勢必得投入相當可觀經費與人力進行研發，相較之下中共近幾年成立的網軍相對的對於我國造成嚴重的威脅。無論是資訊戰還是網路戰和網路中心戰，都離不開資訊技術的迅速發展。為有效因應敵人無煙硝資訊戰，國軍須以新思維審慎檢視當前資安政策，投注更多資源及努力以建立多層防護與及時資安管控的資安防護網，精進各項管理作為與方式，期能兼顧資訊科技的便利性及安全性，確依標準作業程序，建構最縝密週延的資安環境，才能有效降低風險與危害，有效降低資訊風險與損害。面對中共網軍威脅，我們除應積極建立國家層級資訊戰指揮體制外，並應有以下因應作為：強化資訊暨基礎作戰能力、具備監偵及反偵蒐全軍節點能力防止指揮管制機能遭破壞、具備電磁脈衝防護能力防敵癱瘓、推動資安認證提升資訊系統安全防護網建置安全通資作業環境、研發安全保密通道與加密技術確保資料安全、結

註22 國防部，〈四年期國防總檢討〉，國防部發布新聞稿說明「102年《四年期國防總檢討(QDR)》」報告，2013年3月13日，存取時間2014年1月25日。

註23 梁華傑，〈共軍駭客入侵劇增美掌控「制網路權」應戰〉，國防部青年日報，http://news. gpwb.gov.tw/news.aspx，2013年3月27日。

註24 Gospelcity.net，北大西洋公約組織和俄羅斯進行聯合信息戰演練，2010年9月17日。

合C⁴ISR指管通情系統建置聯合作戰資訊戰反制能量、構建滿足聯戰需求通資電平臺防護系統；落實資安通報應變機制提昇資安防護能量等，以確保國軍資訊安全與國防整體戰力。

2013年4月德國軍事科技月刊之「網路防務戰略方案」專文指出，網路威脅或攻擊對重要基礎設施造成的風險，與戰爭及全球恐怖活動幾乎等量齊觀。面對現代戰爭產生的資訊戰威脅，除要能夠熟悉各項新科技武器的使用方法，更須建立相關防護機制，方能確保國防資訊安全。為建構網路作戰防禦與攻擊能力，美日兩國國防與外交首長在2013年東京舉行的二加二會談，就特別將包括兩國合作對抗網路攻擊議題、強化兩國網路軍演及提升政府機構網路攻擊應對能力等網路作戰項目納入，充分說明在現代戰爭中，網路防衛與作戰能力已具有關鍵影響力。隨著電腦網路發展和網路共用性及互連性程度擴大，網際網路已成為資訊交換主要手段，而軍事機密資料等敏感資訊對網路安全則需更高標準要求。【註25】ISO27001資訊安全管理認證，是國際標準化組織對於資訊安全管理的認證規範，透過PDCA模式(P：計畫、D：執行、C：檢查、A：改善)，建立一套完善作業流程，並為國際資訊安全管理的準則。資訊安全稽核將可確保單位資訊安全管理意向與策略獲得落實外，透過資安稽核，讓資訊安全持續自我提升，降低組織因資訊風險形成對工作的影響，並使內部具備長期自我維護安全能力，進而創造優質資訊安全環境。【註26】事實上，落實資訊安全作為是全年無休的，嚴密資訊安全也無百分之百的絕對安全，資安防禦是防患未然工作，但資訊安全並不保證絕對安全與永久安全，資安管理技術不保證電腦不被惡意程式入侵，因此唯有加強資安教育，讓電腦使用者確切瞭解資安惡意攻擊預防工作的重要性，以有效落實資訊安全防護作為。有鑑於此，2009年1月行政院訂頒「國家資通訊安全發展方案(2009-2012年)」，該方案考量資安政策延續性，以達成「安全信賴的智慧台灣，安心優質的數位生活」為願景，朝「強化整體回應能力」、「提供可信賴的資訊服務」、「優質化企業競爭力」及「建構資安文化發展環境」四大政策目標努力。ISO/IEC 27005架構內容包括全文建立、風險評估、風險處理、風險接受、風險溝通及風險監視審查。【註27】

在資訊數位化及網路科技日益發達的環境下，網路攻擊適用範圍極為廣泛，網路入侵被廣泛視為係一種對於國家安全、公眾安全和經濟最嚴重的潛在挑戰。【註28

註25　國防部通資次長室，〈謹慎使用網路防範機密外洩〉《國防部青年日報》，2012年2月8日。
註26　蔡安曜，〈來論：完善資安防護網阻敵入侵竊密〉《國防部軍事新聞》，2013年3月24日。
註27　林相吉，〈『網路中心戰』我們的機會與挑戰〉《海軍軍官雙月刊》，第21卷3期，1992年。,
註28　青年日報社論，〈嚴密資安防護防範網攻人人有責〉《國防部青年日報》，2013年11月27日。

]未來戰爭中網路科技將影響戰局勝負，無論攻方或守方，網路戰都存在相當多的限制與風險，如何掌握先機並確保資訊基礎建設與強化緊急應變作為，都是不可忽視的重要議題。[註29]國防部長嚴明先生在102年通資電工作檢討會中，期勉國軍運用通資電科技，逐步進行不對稱戰力的建構，期能滿足聯戰實需，有效掌握資電優勢，支援防衛作戰任務遂行，嚴部長會中並強調要求各單位依據十年建軍構想及五年兵力整建計畫，落實各項整備工作，以聯合作戰為目標。現階段國軍已整合各項資安防護機制，並持續擴充電磁參數資料庫及重要指管陣地電戰防護能力，有效提升聯合資電作戰能力。面對未來複雜資電作戰環境，國軍須精進資訊、網路與電戰防護能量，俾確保資訊、網路安全，強化電戰防護效能；針對聯合資訊戰能力建議方向提供參考：強化聯合作戰指管系統能力、精進重要通訊資訊基礎與關鍵資源建設、建立緊急應變與系統資源備源機制、提昇資訊確保能量、整合各項資安防護系統及機制以提升早期預警及聯合資訊安全防護能力、統籌規劃國軍網路資安防護措施透過聯合監偵等方法持續強化各項資安防護網能量、導入最新通資安全技術於軍事用途提升資訊安全防護與作戰能量、規劃國軍資訊組織及人力編配基準執行資訊專業人員培育及訓練流路以強化資安應變處置能力與持續發展綜合性資訊戰力以確保國軍資電優勢。總而言之，國軍資訊戰發展正是發揮統合戰力的關鍵因素，其牽涉範圍廣泛、影響深遠，因此必須審慎整體規劃，除打造安全資訊作業環境以深度、廣度及速度三維度，強化資安防禦縱深、建立資安聯防，擴大整體防護網路共同防範駭客攻擊並強化基礎網路設施維護有效發揮統合功能，以達克敵制勝之國家安全目標。

作者簡介

空軍上校　吳嘉龍

學歷：中正理工學院電機系電子工程組77年班、美國俄亥俄州空軍理工學院電腦工程研究所84年班、國防大學理工學院國防科學研究所電子工程組93年班。經歷：電子官、區隊長，教官、講師、助理教授、校教評秘書、科主任、副教授、資訊安全學會永久會員、危機管理學會理事、危機管理學會資訊安全主任委員、教授、系主任。現職：航空通訊電子系上校專任教授兼任系主任。專長領域：資訊戰，通資安全，無線通訊，網路通訊協定。

註29　蔡宗恆，〈掌握資電優勢建構不對稱戰力〉《國防部青年日報》，2013年11月27日。