空軍軍官雙月刊 183
Air Force Officer Bimonthly

資訊安全

資訊作戰與網路情監偵理論技術研究

教授　吳嘉龍

提　要

資訊科技的進步改變了人類社會的面貌，包含戰爭的型態。由於整個社會結構的變動，各組織間相互的資訊交流，造成國家之間有更多的互動關係，資訊科技與資訊自然對國家安全是益形重要。儘管資訊戰不是資訊時代的唯一作戰方式，但是近期以數倍成長的資訊科技卻為資訊戰開創了前所未有的時機。資訊電腦及網際網路帶給人們極佳的便利性，不僅使得科技加速發展更拉近人與人、國與國的距離，世界變得日趨扁平化，使得人們對於電腦資訊設備的依賴性變得密不可分。隨著電腦網路在軍事領域應用的普及，網路已經成為提升軍隊作戰能力的倍增器。如同制海權、制空權、制天權一樣，爭奪網路空間控制權已逐漸演變成為美軍維持軍事霸權的重要組成部分。未來的戰略競逐中電腦網路本身就是一種武器與戰場，前線無所不在，奪取戰場控制權將不只是導彈、飛彈和士兵，還包括電腦網路與數位通訊機制。近年網路駭客攻擊政府，且全球化、資訊化時代來臨，國家安全不再限於實體，國家主權範圍的概念除領海、領土、領空外，並擴及到網際空域及資通安全，威脅國家安全的來源不再僅以國家為主體，更有恐怖主義份子或網路駭客入侵等跨國性或無國界犯罪活動。有鑒於網路戰爭的重要，本論文針對於資訊作戰發展與網路情監偵理論技術深入分析探討，並提出相關因應與建議作為。

關鍵字：資訊化作戰、C⁴ISR、資電優勢、網路空間、電子戰場。

壹、前言

在軍事作戰方面，多著重於情報的蒐集及部隊的部署，屆時正式開戰後，飛機、戰車、船艦、火砲及人員等項的數量及性能都將影響戰爭的結局；然隨著資訊發達及科技進步的同時，戰爭的型態也隨之改變，「通資電優勢」將主導戰爭初期的重要因素，在1991年的波灣戰爭及2003年伊拉克戰爭中，都可以看到美軍使用資訊戰的身影，就連2007年以色列對敘利亞以F-15戰機實施空中攻擊前，也用資訊網路戰方式將敘利亞的防空系統癱瘓，這些例子都可以看得到資訊戰已經成為戰爭中的前哨戰，其重要性不言而喻。傳統軍事戰爭戰場將以資訊戰為導向，進而規劃完善的資訊戰，具有低成本、高效益及不受操作人員、週邊環境因素的限制，未來可能成為以小博大不對稱作戰的一種手段，更將是二十一世紀主導戰爭成敗的決勝王牌。網路戰是一把雙刃劍，一旦運用網路部隊進攻別國的網路，導致網路癱瘓，而國家的網路作用也將急劇下降，所以國際間的網路必須靠合作，才能提升網路的便利性與使用價值。值得注意的是，面對各國網軍較勁升溫的新形勢，未來的戰爭中電腦本身就是一種武器與戰場，戰爭前線無所不在，奪取戰場控制權將不只是導彈、衛星、無人載具、飛彈和士兵，還包括電腦網路與數位通訊機制。網路空間儼然成為各軍事強權優先奪取目標之一，如何能發揮己身所長，從而打擊敵人關鍵要害，是戰爭行為中自古至今不變的道理。依據韓國《中央日報》日文版2013年11月5日報導，北韓正動用勞動黨統戰部、宣傳部、國防部和國家安全保衛部等部門展開對韓網路宣傳戰攻勢，225個部門在對韓實施心理戰。據日本《讀賣新聞》日報導，韓國國家情報院在國會情報委員會上透露，北韓建立了一支共約1700人的駭客組成的專門部隊，加強網路戰能力。據出席國會情報委員會的韓國議員稱，北韓這支專門部隊被配置於北韓勞動黨和國防委員會旗下，北韓還設立了以對外工作部門“偵察總局”為中心的“網路司令部”[1-5]。

南韓國家情報院分析認為，約4200名工作於北韓計算機中心(KCC，Korea Computer Center)、對外身份為軟體開發的相關技術人員將成為網路戰的支援力量，“北韓已經建立起一個防止事態發生的網路攻擊組織。”日本《每日新聞》5日引述韓媒的報道稱，北韓設立以網路研究所為主的網路司令部，並設置了7個由國防委員會和北韓勞動黨內共約1700名重要工作人員組成的駭客組織。韓國《中央日報》日文版5日稱，北韓正動用勞動黨統戰部、宣傳部、國防部和國家安全保衛部等部門展開對韓網路宣傳戰攻勢，225個部門在對韓實施心理戰。北韓電子戰特種部隊現已有3萬人韓國政府和企業網站過去數年不時受駭客攻擊，外界都估計是北韓

駭客所為。有逃亡到美國的北韓人聲稱，北韓電子戰特種部隊現已有3萬人。韓國軍方對北韓駭客能力的評價亦很高，認為其水平僅次於美俄。韓聯社稱，北韓駭客部隊直接由人民軍總參謀部指揮自動化局和人民武力部偵察總局領導，其中1998年成立的第121部隊，是北韓第一支專門從事網路攻擊與防禦的駭客部隊，負責收集韓美日等國的軍事情報，並執行網路戰任務，諸如入侵敵方軍事機構計算機網路、盜竊數據，甚至散佈計算機病毒。至於總部位於平壤的「110號實驗室」，則是偽裝成開發計算機軟體公司的駭客部隊，於1990年代成立。北韓領導人金正恩曾說過，「網絡戰能力是與核武器和導彈共同保障北韓軍隊打擊能力的尚方寶劍」。南韓傳媒聲稱，北韓多年來致力培養網路戰人員，當局會從各大學中挑選成績最優秀的學生，送往「秘密學校」，學習駭客技術和網路襲擊戰術。2009年3月，北韓駭客部隊曾涉嫌對韓國陸軍第3軍司令部發動襲擊，竊取了2000多項韓國國家機密，包括700多家企業和機構相關情報。要數北韓網戰部隊最成功的戰績之一，應是2009年7月7日涉嫌運用阻斷式服務攻擊(DDoS)，導致韓國主要網站、美國紐約證券交易所及白宮主網頁癱瘓，韓國媒體將此稱為「7・7網路事變」[6-10]。

韓國網路安全中心公佈研究報告，確認北韓駭客可能攻擊的多個主要目標，呼籲政府及企業防患未然。報告指北韓自1986年起訓練駭客，憂慮北韓可能同時向韓電力設施、交通網路、通訊系統、股市、軍方及其他基建發動網路攻擊。最令人關注的是供應韓國36%電力的核設施，可能被入侵。除航空交通面臨威脅，韓國高鐵亦有遇襲風險。一旦運作系統失靈，列車無法控制速度及路線，最壞情況是列車路線被調動，導致列車相撞。美國有線電視新聞網(CNN)2015年1月7日播出一段新聞節目引述一名「脫北者」(北韓難民)的消息說，北韓設有名為「121局」的「秘密駭客機構」，該機構長期在大陸的瀋陽市大規模運行。該節目的消息來源，是一位名叫金恆光(Kim Heung-Kwang)的電腦工程師，2004年從北韓逃至

圖一　CNN報導宣稱：北韓駭客部隊在大陸瀋陽設秘密據點[3](摘自網路)

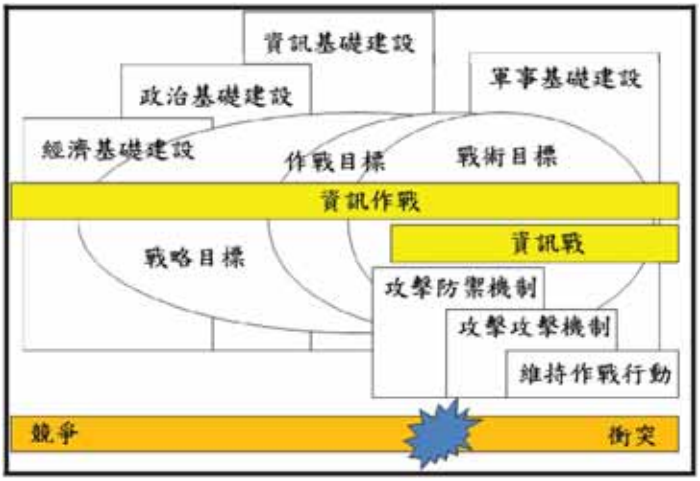
南韓。金恆光指出，「北韓駭客」已經在瀋陽秘密地進行網絡攻擊活動多年，他們「每打一槍就換個地方」，該機構被稱為「121局」(Bureau 121)。他還指出，「121局自2005年起開始了在大陸境內的大規模活動，而該局在上世紀90年代末就已建立」。北韓方面在瀋陽的這些動作雖然發生在多年前，但他相信，「現在仍有北韓駭客在瀋陽活動」，美國CNN電視報導畫面如圖一所示[11-15]。

網際空間是現代最新的作戰領域，其地位相當於情報、監視與偵察在傳統作戰中重要性一般，在網際空間作戰不只需要取自網路的情監偵，也包括任何可以提供重要情報價值的情資。網路入侵攻擊與惡意程式威脅事件層出不窮，2014年11月，美國索尼影業遭到駭客攻擊，事件起因於該公司發行的“以刺殺朝鮮最高領導人金正恩”為主題的電影《採訪》(The Interview)，美國稱索尼影業遭網路攻擊是北韓駭客所為。美國國防部在削減預算和軍力的同時卻大力擴產網軍，網軍人數2016年將增加三倍到6000人，全球各地的美軍指揮部均配備網軍。《紐約時報》報導，早在國防部長海格七日開始訪問中國前數月，歐巴馬政府就私下向中國通報了美國的擴充網軍計畫，並希望中國投桃報李和增加透明度，也向美國介紹中國的網軍計畫。美軍擴大網軍是要利用先進的網路技術，防範敵方對美國的網路攻擊，包括來自中國的攻擊，中國軍方許多單位策畫和發動了對美國企業和政府網站的攻擊行動。五角大廈高級官員表示，美軍希望加強與中國軍方交流網軍發展計畫，是為了避免兩國間的網路攻擊與反攻擊活動日益升級，海格和他的顧問都對未來的前景感到擔憂，尤其是在中國擴大在南海和東海的領土主權要求，和設立東海防空識別區之際。國防情報局前任網路戰專家蘿拉・加蘭特說：對中國而言，網路攻擊還不是最重要和首先使用的軍事武器，而是一種經濟武器。五角大廈準備未來五年投入兩百六十億元發展網路技術。美國國防部2014年6月5日於白宮公布的2014年中國軍力報告指出「中國軍事現代化已經讓台灣原本的優勢被侵蝕或成為負債，中國有能力在未來五到十年內對台進行全面軍事封鎖」。報告指出，台灣傳統上的優勢包括：擁有海峽屏障，解放軍沒有足夠投射能力；台灣軍隊在科技上的優越性；海島防衛的地理優勢。但中國日增的現代武器與載具，彈道飛彈、反艦彈道飛彈、潛艦和戰艦，還有改良的指管通資情監偵系統(C⁴ISR)能力，將嚴重侵蝕這些優勢[11-12]。

貳、資訊作戰理論技術與發展研究探討

欲了解網路戰先認識資訊作戰(Information Operation，IO)，所謂資訊作戰，可以定義為：「對立雙方為爭奪對於資訊的取得權、控制權及使用權，而展開的一

種戰爭形式，其目的在於利用這些資訊優勢使對方屈服，或是使對方喪失這些優勢而達到干擾對方之作用。」而就美國、中共及國軍的定義來探討如下：美國對資訊戰的定義為：「藉由採取影響敵人資訊、資訊相關程序，資訊系統和電腦網路等行動，以奪取資訊優勢；同時亦須對已方資訊系統採取防護措施。」。中共對資訊戰的定義為：綜合運用資訊技術和武器，打擊敵人的資訊系統(偵察與指揮控制系統)，使敵情不明、決策錯誤或放棄抵抗；同時運用一切措施，保護自己資訊系統不受敵人干擾和破壞，得以充份發揮功能；這種戰爭核心是爭奪控制資訊權，以掌握戰爭的主動權；對立雙方為爭奪對於資訊的獲取權、控制權和使用權而展開的鬥爭。國軍對資訊戰的定義包括廣義資訊戰係運用各種手段影響敵方並防護我方決策程序與資訊系統之行動，以創造資訊優勢；狹義資訊戰係運用資訊科技影響敵方並防護我方指管程序與資訊系統之行動，以獲取戰場資訊優勢[12-14]。



圖二　資訊作戰與資訊戰的範圍[12]

許多軍事理論家認為，資訊戰是資訊作戰失敗後所採用的作戰方法，並把資訊戰侷限在自衝突或危機發生後所進行的作戰方法，而這些方法也包含在資訊作戰的各種手段之中；資訊作戰，本身應是不論在平時或戰時皆應持續進行的形塑環境的有效工具，所以當然資訊作戰包含了資訊戰，只是資訊戰是當危機或衝突發生時，才須採取的資訊作戰，對於資訊作戰及資訊戰的描述，圖二為資訊作戰與資訊戰的範圍示意圖，圖中分析，資訊戰是衝突發生時進行的，資訊作戰則是隨時都在進行；美國、中共及國軍對資訊作戰定義探討如表一。透過指管系統，藉情報戰、心理戰、資訊攻擊、電子戰及傳統武力攻擊等方法，對敵之資訊與系統，加以遲滯、干擾、癱瘓、摧毀，並獲取敵方資訊，供我軍爭取資電優勢，以遂行反制；藉由軍事欺敵、安全措施、資訊防護等手段，防制敵對我資訊系統遂行入侵、破壞、瓦解、封鎖、竊密，以有效支援全般作戰[15-16]。

資訊戰意指包括資訊及資訊系統之特定力量的整合，並將高科技資訊武器取代傳統武器廣泛運用於戰場上。這個概念類似整合各軍種能力的聯合作戰，或整合二個以上部隊或單位或聯盟的協同作戰，並運用資訊及資訊系統去影響所望目標決策

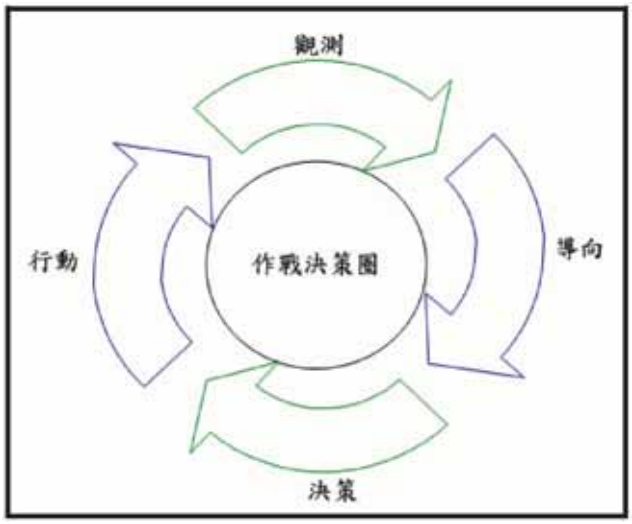
表一　資訊作戰定義分析(自行整理)

資訊作戰定義	資訊作戰(Definition of Information Operations)定義分析
美國資訊作戰定義	美軍聯戰準則 3-13 資訊作戰(1998 年版)中，將資訊作戰定義為影響敵方資訊及資訊系統，同時保護己方資訊和資訊系統所採取的各種行動。包括指對敵實施資訊攻擊，以干擾、摧毀、破壞、影響敵方之資訊、資訊化處理、資訊系統及電腦網路，以獲取資訊控制；並維護我方資訊、資訊化處理、資訊系統及電腦網路之安全與完整，以確保資訊優勢所採取的各項行動。
中共資訊作戰定義	中共將資訊戰稱為信息戰，又稱為點穴戰與針頭攻擊，對於資訊作戰定義：敵對雙方在資訊領域的對抗活動，主要是通過爭奪資訊資源、掌握資訊的生產、傳遞、處理等的主動權，破壞敵方資訊傳輸，為遏制或打贏戰爭創造有利條件。點穴戰意指針對資訊系統最薄弱部位，點其要穴，癱其全身，以尋求最佳作戰效益。針頭攻擊意指攻擊時要像長針一般直插敵人心臟。
國軍資訊作戰定義	2004 年 1 月 9 日由國防大學編撰國軍資訊戰要綱準則，此準則參考美軍 1998 年出版美軍聯戰準則 3-13 聯合資訊作戰，空軍也在 2006 年 6 月 14 日頒行了空軍資訊戰教範；國軍資訊戰要綱將資訊戰廣義定義在運用各種手段以創造資訊優勢。

者及使用者的作為，相對地，資訊戰亦防護友軍決策者及使用者免於敵人資訊或資訊系統的不當影響。就是強調資訊優勢或資訊支配，攻擊癱瘓敵方的資訊系統，確保己方資訊系統的安全，摧毀敵方資訊，保護己方資訊的一種作戰方式。根據美軍相關準則定義，資訊作戰相關範疇即包含了狹義的網路戰型態-電腦攻擊。關於資訊作戰，此一名詞見於1996年美國在「2010年聯戰願景」(Joint Vision2010)中率先闡述這個概念，將之定義為「影響敵方資訊及資訊系統，同時保護己方資訊與資訊系統所採取的行動」。在聯合出版品3-13-資訊作戰(JP3-13-Information Operations)(1998年版)便指出資訊作戰能力的相關行動包括：電腦網路攻擊(Computer Network Attack)等7種[17-20]。

資訊戰是一種新的戰爭型態，資訊戰一詞最早是出現在1976年，這個觀念是由一位羅納博士(Dr. Thomas P. Rona)在提交給波音公司題目為「武器系統與資訊戰爭」的研究報告中首度引用。羅納博士的論點在於美國商業資訊基礎建設已成為其經濟發展不可或缺的要件，但卻也是在平、戰時中，極易受到攻擊的目標。在1980年代，美國空軍掀起一股討論資訊戰的熱潮。「資訊」既可以是目標，也可以是武器。資訊戰須有完善的電腦與通信基礎設施為後盾，在此時期，美國空軍上校約翰博伊德(Col. John Boyd，1927-1997)提出「觀測(Observe)、導向(Orient)、決策(Decide)、行動(Act)，OODA」作戰決策循環理論(如圖三)，作為參謀作業及指揮官決心下達之流程，約翰博伊德憑藉多年戰鬥機飛行員經驗與對能量機動理論(Energy Maneuverability theory)的研究，最初是以空戰戰術應用為目的發明此項理論，因此OODA循環理論又被稱為「博伊德循環」，他認為任何戰略都應著眼於改

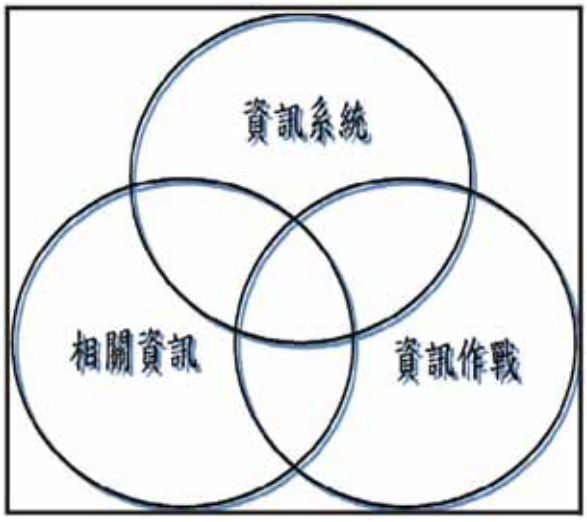
變和影響敵方的行為，而不是消滅其軍事力量。敵我雙方的決策循環過程有快慢之分。我方目標應設法比敵方更快完成OODA循環，進而干擾、延長、打斷敵方的OODA循環，造成敵方的迷惑、誤判、喪失作戰意志，最終取得戰爭勝利。近年來OODA循環理論除被當成軍事戰略的重要理論外，已被廣泛應用於商業管理與策略規劃等領域。在OODA循環理論(OODA Loop)中，觀測功能是以人為或科技的方法蒐集指揮官所需的戰場情資；然後在導向功能中，藉由資料挖掘技術或人工分析方法，萃取出敵軍作戰型態模式，從這些模式中得以洞悉敵軍之意圖；再經由指揮官的判斷或自動指管程序決策過程，以致最後下達行動命令[21-23]。



圖三　OODA循環理論(OODA Loop)決策模式(自行整理)

資訊戰是由聯合或軍種參謀在特定資訊官的指導和監督之下所計畫，必須全然整合融入整體聯合計畫程序，做它的緊急或危機作為，以提供指揮官額外選擇，達成所望目的。聯合計畫的資訊戰部份之執行是由專業資訊戰部隊(心理、電子戰、電腦網路戰等)及一般授命執行此任務的部隊(軍事欺敵、作戰安全等)所執行，其計畫是否成功執行評估是透過效果辨識量測(其判定計畫達成所望效果的程度如何)及表現量測(其判定計畫執行成效)，基於對所接收資料的及時性及正確性的真實期望，效果辨識量測及表現量測必須被識為資訊戰計畫程序的一部份。個人電腦與網際網路的結合，使參謀作業及指揮官決心下達的流程得以不受時空的限制，然而，這卻造成了指揮機制易受攻擊的缺點。1993年，在一篇名為「網際電腦戰爭即將來臨」的論文中，作者阿奎拉(John Arquilla)與隆菲德(David Lang Ronfeldt)提出網際電腦戰爭與網路戰爭的新理論。他們將藉由網路設施攻擊軍事作戰相關事務之作為歸類為網際電腦戰爭，而攻擊社會大眾之資訊基礎建設則歸類為網路戰爭。而美國國防部公開性官方討論開始於1993年「參謀聯席會議主席政策備忘錄30號(MOP-30)—指管戰」，指管戰定義為：「於戰場上遂行資訊戰軍事策略」，這是美軍對資訊戰下過最早的定義。美軍廣泛定義出指管戰是資訊戰在軍事作戰中的應用，亦就是使用各種不同的科技與技術去攻擊或防衛指揮與管制機制。美國空軍對資訊戰的基本定義：「資訊戰為任何用來運用、篡改或破壞敵方資訊與資訊功能及保護我

方資訊與資訊功能不受到敵方攻擊的行動」。美國空軍在制訂這項基本定義時，也提出了一項前提：「資訊戰是任何形式對資訊與資訊功能的攻擊，不考量其攻擊的方法」。因此，轟炸電話交換機系統是資訊戰，而破壞交換機設備的軟體也是屬於資訊戰。同時，「資訊戰是任何形式對資訊與資訊功能的防護，不考量其防禦的方法」。所以，強化防禦工事，防止敵軍空中攻擊我方交換機設備是屬於資訊戰；利用防毒軟體，保護我方之交換機軟體，免於遭受電腦病毒攻擊，也是資訊戰的範圍[24-25]。



圖四、資訊優勢(Information Superiority)構成要素(自行整理)

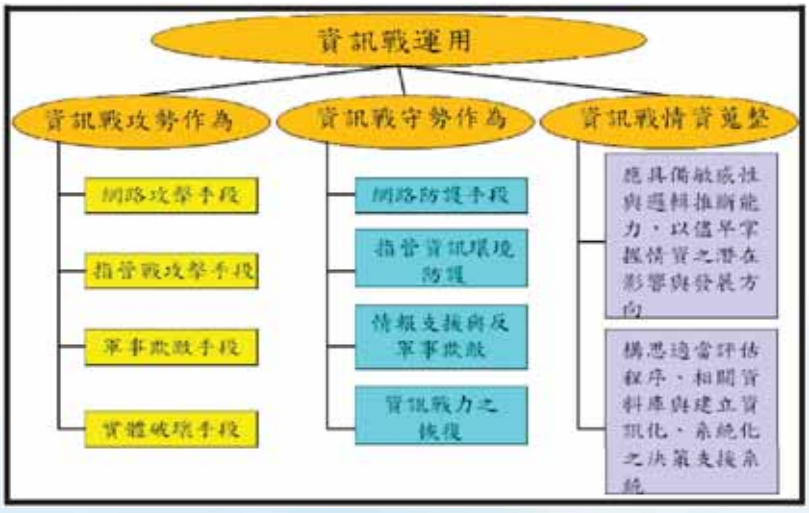
資訊作戰是美國政府研擬一套準則方法，以利軍隊及外交人員運用資訊力量的正式訴求，資訊作戰的對象是敵方決策人士，因此首要工作重點將會是迫使該人(或一群人)從事或不從事某項行動。為影響敵方決策階層，展開資訊作戰時會嘗試運用許多不同的戰力，如欺敵、心理戰及電子戰，以形塑和影響資訊環境。針對網路戰定義部分，美軍高級資訊戰研究機構(Institute for the Advanced Study of Information Warfare, IASW)對於其定義為：「當防護某一需要使用資訊及資訊系統攻擊或防禦，藉以阻止、應用及破壞敵對方資訊、資訊化流程、資訊系統及電腦化網路。此等行動是為獲取軍事上或經濟上利益」。美國主管反恐與網路安全專家理查德．克拉克(Richard A. Clarke)在《網路戰》(Cyber War)一書中將網路戰定義為「出於造成破壞或干擾的目的，一國侵入他國電腦或網路系統的行為」；書中提到網際空間(Cyberspace)不僅包含網際網路(Internet)也包含私有網路(Private Network)；惡意人士可侵入其中，進行破壞、竊取等行為。1996年美國政府在「2010聯戰願景」中率先闡述這個概念，將之正式定義為「為影響敵方資訊及資訊系統，同時保護己方資訊及資訊系統所採取的行動」。為了獲致「全面優勢」美國政府提出優勢機動、精準接戰、全方位防護及集中後勤等4項作戰概念，該4項概念的根本條件統一概稱為資訊優勢，其定義係「能持續不斷收集、處理、散播資訊，同時善用或阻絕敵方從事同樣活動之能力」。這項優勢稱為資訊優勢，係由資訊系統、資訊作戰及相關資訊等3項要素所構成(如圖四)，其中以資訊作戰最重要[26-30]。

現代戰爭之作戰速度正急劇加快中，精兵策略下所發展之資訊戰，全面結合指

表二　資訊作戰核心能力(自行整理)

核心能力	資訊作戰核心能力分析
心理戰(Psychological Operations，PSYOP)	傳播適當資訊給敵軍，以影響或改變想法，轉支持我國的軍事行動。心理戰的最終目標是在影響相關國內外團體、組織與政府，形成孤立敵軍的態勢，以協助我軍軍事任務之遂行。
軍事欺敵（Military Deception，MILDEC)	以敵軍指揮決策者為目標，藉由誘餌、欺敵或誤導、謠言傳布等各項作為，以影響敵軍之情報蒐集、分析與傳遞系統，使敵軍指揮官在真真假假的情報中，作出錯誤的決策。
作戰安全（Operations Security， OPSEC)	作戰安全範圍包含通信及資訊安全，防範軍事機密由各種管道洩漏。藉由各項安全措施，延緩敵軍決策過程，使能制敵機先。
電子戰（Electronic Warfare，EW)	電子戰（Electronic Warfare，EW）定義為任何牽涉到使用電子及指向性能量，以支配電磁光譜或攻擊敵人之軍事行動
電腦網路戰（Computer Network Operations，CNO)	指利用電腦病毒、邏輯炸彈、植入破壞晶片裝置等方式，攻擊敵國政、經、軍之電腦及電腦網路系統；此項作戰方式是最廣為社會大眾所認知之資訊戰戰法。

揮、管制、通信、資訊及電子戰等範疇的作戰方式，開啟了資訊戰爭新型態作戰。資訊戰是指使用和管理資訊來保證與對手的比較優勢，包括收集情報，驗證，向對手散佈宣傳和假情報等等。資訊戰廣泛定義指現代戰爭在大量使用資訊技術和資訊武器基礎上，構成資訊網路化的戰場，也就是透過通訊、雷達、電腦、衛星、雷射等資訊技術及裝備，爭奪對資訊的控制權及使用權，其核心為爭奪戰場資訊控制權，以影響和決定戰爭的勝負。資訊戰具有戰場透明化、整體協調化、行動同時化、打擊精確化、空間廣闊化的特徵；其作戰範圍包括指揮控制戰、電子戰、情報戰、心理戰、經濟戰及電腦病毒戰。2006年美國聯合出版品3-13-**資訊作戰**(JP3-13-Information Operations)中闡述資訊作戰包含五大核心能力美軍訂定資訊的作戰能力上提供重要核心能力，將核心能力形成資訊戰的基礎，都可造成資訊戰目標的達成，資訊作戰核心能力整理分析如表二[31-32]。



圖五　資訊戰運用區分架構圖(自行整理)

電腦網路作戰屬於資訊作戰範疇並與電子戰(Electronic Warfare)同為攻擊、欺騙等作用並防護電子資訊及基礎建設，並區分為網路攻

表三　資訊戰運用原則分析表(自行整理)

原則	資訊作戰核心能力分析
1	資訊戰攻擊以掌握敵人決策過程，並加以利用與影響為最終目的。採主動監偵與積極防護手段，建立早期預警與應變制變通資安全防護能力，確保通資優勢。
2	工具通用化、便利化是靈活資訊戰的要件，資訊戰攻擊之目的要必須明確，同時能支援整體國家與軍事目的，更必須包含可衡量的成功指標。
3	知己知彼，百勝不殆，針對敵國，遂行資訊戰必須依據任務狀況與國家目標，建立周詳的接戰規範，並且符合國際法與國內法律規範，選定與部署特定之攻擊能力，以確保我方資訊資源並枯竭敵方資訊資源。
4	資訊戰必須整合及協調產、官、學、研界之資源，以充分支援主作戰任務達成。資訊戰並可為聯合作戰或各軍種作戰的主要任務、支援任務或是階段性任務。

擊(Computer Network Attack，CNA)、網路防禦(Computer Network Defense，CND)及網路運用(Computer Network Exploit，CNE)等，其目的在確保作戰任務遂行。針對電腦網路攻擊、防禦及運用詳細意義，茲分述如下：網路攻擊範疇包含透過網際網路達到擾亂、拒止、退化或破壞常駐於電腦及電腦網路中資訊，甚或是電腦及電腦網路。網路防禦涉及利用電腦網路防護、監控、分析、偵測及對國防部資訊系統及電腦網路相關非法行動予以反應。中共資訊戰的攻擊能力包括：一、具電腦病毒破壞能力，可透過多項植毒管道，直接攻擊、破壞我政治、經濟、軍事資訊系統；二、具電磁脈衝彈大規模干擾、癱瘓我國C4I系統，使我武器系統失效；三、資訊偵搜能力(特別是借助駭客的力量)，竊取我軍事機密。目前而言，網路防禦對軍事行動已是不可或缺之功能。網路運用使得作戰及情報蒐集能力可行，並植基於運用電腦網路對目標及敵對勢力自動資訊系統及網路實施資料蒐整[33-34]。

在波灣戰後，前線的定義已日趨模糊，在未來戰爭中，處處可以是戰場。美國對資訊倚賴的程度，使得美國防部不得不正視美國本土是美國防中最脆弱一環的事實。如果電力、電信、金融、空中交通管制等任何一種系統遭到破壞，則對美國社會所造成的影響將是難以估計的。而防護這些系統權責，則超出了美國國防部層級，必須加以提升至國家層次來處理。資訊戰運用區分為情資蒐整、攻勢作為與守勢作為，圖五為資訊戰運用區分架構圖，資訊戰運用原則整理如表三，圖五為資訊戰運用區分架構圖[35-36]。

參、網路(絡)戰、電子戰、資訊攻防與C⁴ISR理論技術分析探討

此章節針對網路(絡)戰、電子戰、資訊攻防與C⁴ISR理論技術分析探討，事實上，中共歷經改革後，其對於網路戰的重視程度，已不可同日而語，甚至超越歐美

各國。加強指揮、管制、通訊、情報系統建設；成立網路部隊專司資訊戰攻防作為，並設置信息戰模擬中心，利用高科技模擬技術與設備，營造資訊戰及模擬戰場環境，以進行對抗演練。中共對於網路戰之定義如下：「網路戰爭是以國際互聯網為依託，通過交互網絡秘密進入他人的計算機系統竊取情報或者毀壞數據，是一場不見硝煙的戰爭，是交戰雙方通過網絡系統進行的信息戰」。對於網路戰有所研究的德國學者克勞斯．彼得．薩爾巴赫(K.SAALBACH)在著作「Cyber War-Methods and Practice」，指出網路戰定義為：一種複合型戰爭的組成，並且使用資訊技術畫定軍事衝突。其具體實行於對電腦及其資訊攻擊、並包括電腦資訊網路及其系統附屬之網路，2014年6月17日出版到第9版。

現階段，大陸發展「網電一體戰」的作戰能量，主要項目包括：透過電腦網路攻擊，來完成長距離的攻擊破壞任務、運用電腦網路攻擊癱瘓對手國的重要經濟活動能量，達到警告嚇阻的效果、運用電腦網路瓦解對手國的C^4ISR系統並運用電腦網路攻擊，發揮先發制人戰略威懾效果、結合電腦網路和電子戰特種部隊奇襲能量，達到心理威懾戰略目標，並迫使對手國接受政治談判條件、運用電腦網路攻擊破壞美軍的後勤補給系統，以及運用電腦網路攻擊癱瘓敵國金融、電力運輸與通訊系統等。而針對易遭網路攻擊之高風險對象所執行的行動有以下幾個特點：網路攻擊無距離之分，可以由遠距離執行攻擊行動；允許小團體對抗大目標，執行不對稱攻擊(Asymmetric Attack)[37-40]。

依據維基百科定義，C^4ISR系統係提供軍事信息化指揮和管理系統以提高指揮效率，又稱為指揮自動化系統，它由指揮、管制、通信、資訊、情報、監視和偵查(Command、Control、Communications、Computers、Intelligence、Surveillance、Reconnaissance)首字母縮寫而來，簡稱「指管通資情監偵系統」已成為現代軍隊的神經中樞；C^5ISR，增加的字母C指作戰系統(combat systems)。傳統電子戰區分方式包括電戰支援、電戰反制與電戰反反制三部分，傳統定義內容說明如表四；現

表四　傳統電子戰定義分析(自行整理)

電子戰區分	電子戰技術分析
電戰支援（Electronic Warfare Support Measure，ESM）	指利用各類裝備與手段，對於電磁波訊號進行分類，辨識，定位與分析等等的工作。常見的任務包括對各種雷達的區分，辨識與方位標定等等。
電戰反制（Electronic Warfare Countermeasures，ECM）	指對敵方使用電磁波的裝備和手段，進行壓制或者是破壞的行動。常見的任務包括干擾敵人接收的電磁波訊號，或對敵人的裝備進行實質上破壞等等。
電戰反反制(Electronic Warfare Counter Countermeasures，ECCM)	指我方降低或者是壓制敵人的反制行動所產生的影響。常見的手段包括更換雷達使用的頻道或者是操作地點，更換無線電通訊使用的頻道等等。

表五　現代電子戰定義分析(自行整理)

電子戰區分	電子戰技術分析
電子攻擊（Electronic Warfare Attacks，EA）	包括使用電磁能量，指向性能量，或反幅射武器攻擊人員、設施或裝備，以減低或破壞敵人作戰能力或使之無效，且被認為是一種形式的火力。
電子防護（Electronic Warfare Protection，EP）	包括採取被動及主動方式防護人員、設施或裝備免於任何因友軍或敵軍有效使用可減低或破壞作戰能力，或使之無效的電子戰。
電子戰支援（Electronic Warfare Support，ES）	包括由作戰指揮官所採取或受其直接控制之作為，以搜索、攔截、辨識及找出意圖或非意圖的幅射電磁能量來源。因此，電子戰支援係提供關於電子戰及其他戰術行動決策所需之資訊。

表六　電子攻擊(Electronic Warfare Attacks，EA)軟殺分類分析(自行整理)

軟殺分類	電子攻擊軟殺分類技術分析
主動干擾	主動干擾是以發出訊號的方式阻止敵人有效接收與利用電磁訊號的方式。譬如發出干擾電波使敵人無法使用無線電進行通訊。
被動干擾	被動干擾是自己不發出訊號的手段，對於敵人使用電磁波的行動與以干擾。譬如說利用干擾絲製造雷達假目標，或者是以特殊塗料降低紅外線訊號的強度，降低敵人偵測的距離或者是機率。

代電子戰定義區分包括電子攻擊、電子防護與電子戰支援三部分，現代電子戰區分內容說明如表五[40-45]。

電子攻擊依任務型態說明如下，針對電子攻擊或是電戰反制任務型態可以區分為軟殺與硬殺兩大類，其中軟殺是以非物理性，非實質上的摧毀方式降低或者是壓制敵人使用電磁波的行動與能力。硬殺是以實質上破壞或者是殺傷敵人的系統，人員與相關設施，以阻絕敵人進行各種電子作戰行動的能力。常見的硬殺手段包括以反輻射飛彈摧毀雷達等訊號發射系統，以各種飛彈或者是炸彈等武器摧毀敵人的通訊設施與單位。擔任硬殺任務的載具或者是武器不一定具備截收與使用目標所散發的訊號的能力。常見的軟殺方式又可以區分為兩類，內容說明如表六。此外，在心理戰、軍事欺敵、作戰安全、電子戰、及電腦網路戰等5個核心能力外亦由5個其他能力所支援，這些支援能力整理如表七。資訊戰攻勢作為，乃運用我方之資訊戰資源，對敵各種資訊、資訊流、資訊系統與設備、資訊基礎建設等能力與設施，遂行

表七　資訊作戰支援能力(自行整理)

支援能力	資訊作戰支援能力分析
資訊安全	藉由確保其可用行、完整性、鑑別性、機密性及不可否認性來保護及防護資訊及資訊系統之措施。
實體安全	係關於防護人員的具體措施，以避免未經授權者進入裝備、設施、工具及文件，且防護其免於刺探、破壞、損害及偷竊。
實體攻擊	透過破壞性力量瓦解、損害或破壞敵人目標。
反情報	係指發掘敵人對我資訊及資訊系統安全威脅之情報，並據以採取適當防護作為與檢管稽核措施。
戰鬥情蒐	包括獲得與利用靜態及動態影像支援戰鬥、資訊、情報、偵察、及其他有關軍事之行動。

表八　資訊作戰攻擊作為(自行整理)

攻擊作為	資訊作戰攻擊作為分析
網路攻擊	電腦病毒：電腦病毒(Virus)為一種小型程式，具有潛伏、發作、感染、破壞等典型的行為特色，有如生物病毒一般，一旦於對方的資訊系統內感染發作，經常會在極短時間內造成極顯著的破壞與大量的傳染散播；也會依策略參數不同而產生大量的變種電腦病毒。
	殭屍網路：BotNet，又稱為「機器人網路」(Robot Network)，病毒通常會隨著 e-mail、即時通訊軟體或電腦系統漏洞，侵入電腦，再藏身於任何一個程式裡，一遇到有漏洞電腦主機，就自行展開攻擊。
	木馬程式：木馬程式(Trojan Horse)為一種任務導向的間諜程式(Spyware)，經常具有潛伏、窺探、匿跡、遙控等特色。一旦對方的資訊系統被植入木馬，可對其進行長時間的秘密入侵而不被發現。
	飽和攻擊：對被攻目標產生大量的垃圾資訊，以消耗其網路頻寬或系統資源，使其減低或喪失資訊系統功能。
	邏輯炸彈：邏輯炸彈(Logic Bomb)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。當資訊系統被植入邏輯炸彈，可於特定的時間或條件下，自動發作而破壞對方的資訊系統。
	弱點攻擊：弱點攻擊(Vulnerability attack)利用被攻目標的系統弱點對其產生攻擊，使其系統發生錯誤、被入侵或當機。
	分散式阻斷服務攻擊：為阻斷服務攻擊(Denial of Service，DoS)的延伸，通常會伴隨Botnet(殭屍網路)進行，大量殭屍電腦接收攻擊者控制命令，同時間對同一目標發動特定類型攻擊，將被攻擊者網路資源及系統資源耗盡，導致無法提供使用者服務，伺服器看似異常停擺，因此稱作阻斷服務攻擊；由大量殭屍電腦造成的阻斷服務攻擊則稱做分散式阻斷服務攻擊(Distributed Denial of Service，DDoS)，其工具包括 Smurf、Trinoo、TFN、Stacheldraht、Mstream 等。
	進階持續性滲透攻擊：進階持續性滲透攻擊(Advanced Persistent Threat，APT)，APT攻擊重點在於利用社交工具(Social Engineering)手法，逐步掌握目標並竊取鎖定資料；所以能發動這種 APT 攻擊手法的駭客，都是以長期滲透特定組織為目標，擁有高超複雜的入侵技巧，並且有足夠資金，才能支持這樣的滲透及攻擊活動。
	監聽：(Monitoring)，網路封包監聽工具包括 Sniffit、NetXRay 等。攻擊程式 Snooper則為電腦系統監聽技術。
	零時差攻擊：零時差攻擊(Zero Day Attack)，所謂零時差攻擊就是當系統或應用程式上被發現具有風險性之弱點後，但是在修正程式發佈之前，或是使用者更新前所進行的惡意攻擊行為。
	掃描：掃描(Scanning)包括本機與遠端兩種掃描方式，本機掃描工具包括 Tiger 與check.pl 等，遠端掃描工具包括 SATAN、SAINT、Nessus、NMAP 以及 Internet Scanner等。
	密碼破解：密碼破解包括字典攻擊，攻擊者會複製使用者帳戶及密碼雜湊和加密複本檔案，然後使用自動程式來破解每個帳戶密碼。密碼破解(Password Cracking)，工具包括Crack5.0a、L0phtCrack。
	惡意程式碼(後門程式 Backdoor Program)：惡意程式碼(Malicious Code)，工具包括BO2K、NetBus 等。
指管攻擊	致命性武器：包括一般殺傷武器、電磁脈衝武器、指向性能量等。
	非致命性武器：包括電腦病毒、電磁干擾、指向性能量等。
軍事欺敵	可運用敵我雙方情報人員、情監偵武器、資訊技術、欺敵器材等提供假冒資訊，使敵決策錯誤，創造有利我方之態勢，其具體手段包括： 部隊佯動、資訊科技武器、衛星反制、結合資訊戰欺敵之偽裝設施、結合資訊戰欺敵對武器載台之隱蔽與掩蔽與網路工具。
實體破壞	可使用特種作戰部隊、游擊武力、精準武器系統、指向性能量武器、奈米科技武器(微型武器)等，自空中、地面、海上來摧毀或破壞敵人部隊、載台及基地之資訊能量與設施，以破壞敵方直接、間接武力。

表九　資訊作戰攻擊網路防護作為(自行整理)

網路防護	資訊作戰網路防護分析
生物特徵辨識器	開發和管理生物識別裝置，利用生物特徵辨識合法人員的身分，如：指紋辨識器、聲紋辨識器、視網膜辨識器。
單次密碼產生器	單次密碼〔簡稱 OTP(One-Time Password)〕產生器與主機校對時間後，產生單次使用的密碼，以回應主機的密碼盤問之用。
通信保密器或模組	通信保密器或模組意指通信裝備的收送雙方各種裝置保密器或模組，對往來的資訊自動加解密。
媒體內嵌器(資訊隱藏)	媒體內嵌器(資訊隱藏技術)將機密資料內嵌於無敏感性多媒體資料，唯有知道其內嵌過及解密密鑰，才能解讀隱藏其中的機密，如將重要文件內嵌於風景、美女照片或將一段影片內嵌於另一影片。
弱點掃描器	弱點掃描器(Vulnerability Scanner)：使用電腦軟體(software)，對網路主機進行掃描，試圖找出主機上任何可能的被入侵點，例如 OpenVAS 是全功能型軟體，利用各式規則列，從主機安裝軟體的版本，到網頁程式漏洞無一不查。可對網路上網路伺服器，例如：郵件伺器、檔案伺服器、網頁伺服器、網域名稱伺服器等，及個人工作站進行有系統的掃描，以發現是否有已知的系統弱點存在。
防火牆與防毒牆軟硬體	防火牆可管制進出區域網路的用戶與存取服務，防毒牆軟硬體可對流經網路上郵件、檔案、網頁等所有流通訊息進行病毒掃描及過濾。
入侵偵測系統(IDS)	入侵偵測系統(Intrusion detection system，IDS)可偵測網路攻擊與非法入侵等行為，分為主動式與被動式兩種，前者可即時阻絕攻擊與入侵，而後者僅能產生警示或化解部份的攻擊或入侵。
具位址過濾功能路由器	具位址過濾功能路由器技術只路由器應具有位址過濾功能，以過濾掉假冒內部位址的外來封包或假冒外部位址的外送封包，以減少各式以位址假冒為基礎的網路攻擊。

表十　美軍資訊網路戰作戰手法(自行整理)

網路戰術	美軍資訊網路戰作戰
虛擬現實資訊網路欺騙戰	美空軍已把這種技術運用於空軍飛行員訓練。就是把己方電腦與對方聯網，或戰前通過各種途徑，將虛擬現實技術植入敵方的指揮控制資訊系統中，把己方的虛擬資訊即假情報、假決心、假部署傳輸給敵方，迷惑敵人，誘敵判斷失誤。
資訊網路駭客滲透戰	美軍在防止外來駭客入侵的同時，也在積極籌建主動式駭客，即組建一支網路戰士部隊，以電腦為武器，用鍵盤來癱瘓敵人，操作敵人的媒體，破壞敵人的財源，從而達到不戰而屈人之兵的戰爭目的。美軍要求，在未來作戰中，要對敵方實施強烈的電子干擾和飽和攻擊，打開資訊網路突破口，破除敵方口令。
資訊網路病毒干擾戰	電腦病毒一出現，立即受到美軍軍事專家高度重視。目前，已經發現電腦病毒達 5000 多種。由於電腦病毒具有隱蔽性、傳染性等特點，實施電腦病毒破壞戰將在未來高技術戰爭中廣泛使用。

攻擊與制壓，以破壞或限制敵資訊運用能量，其相關為說明如表八。而資訊戰守勢作為，乃係保護已方的指揮、管制、通信、電腦與情報、監聽、偵蒐系統資訊系統及相關設施免遭敵方或不特定對象的欺騙、破壞或降低功能，其防護方法包括指管防護、電子防護、資訊網路安全防護與資訊戰力恢復等型式，網路防護作為相關作為說明如表九，美軍資訊網路戰作戰手法分析整理如表十[45-49]。

肆、網路中心戰與網路情監偵系統發展分析探討

據預測，未來戰爭中不動槍炮的資訊網路戰，可能將不會傷害大量人員，也不會破壞工業企業和基礎設施以及生態環境，但卻能給對方軍事系統造成致命癱瘓。由此，美軍提出了打贏資訊網路戰的種種新式作戰手法，統一網路化以部署指管系統。隨著美軍第一支數字化部隊建立，美軍早已開始著手運用虛擬現實技術進行模擬對抗性演習，並專門成立了虛擬現實技術欺騙戰研究小組，由其具體負責技術研製和試驗。美國總統歐巴馬在2012年1月發佈《21世紀美國國防戰略綱領》將網路空間能力列為最優先發展、重點保障的六大軍力之一。隨後，美國白宮於2013年祭出13636號行政命令，要求改進美國關鍵基礎設施的網路安全。目前，美國為防範重要基礎建設資訊系統，遭遇敵國破壞與入侵，已經制定「網路安全戰略」，採取「攻守一體」的策略措施[50]。

在未來戰爭中，電腦網路本身就是一種武器。網路作戰與防衛能力越來越重要，美軍持續投資開發，因為現今的所有戰力都離不開網路，不論是戰場情偵、目標鎖定，或是聯合作戰，都需要運用網路。目前，在世界軍事變革中，網路戰特別吸引全球軍事戰略家的眼球，各國競相成立網路司令部、研製網路戰武器、擴編網路部隊，制定網路戰士培養路線圖，通過電腦遊戲吸引網迷從軍，特招地方電腦精英入伍，軍地院校聯合培養網路戰士，組織駭客大賽甄別遴選網路專才等等，拉開了資訊竊密與反竊密、入侵與反入侵、滲透與反滲透等全新方式爭奪網路控制權的序幕。依據人間福報外電報導，華府智庫「戰略暨國際研究中心」網路安全專家路易斯，接受《華盛頓郵報》訪問表示，由於美國作戰能力相當仰賴資訊科技，如果美國和中國人民解放軍發生衝突，網路會是兩軍交戰的第一步。美國國會報告指出，中國大陸正在進行一連串網路戰演習，很可能在與美國發生實際衝突前，鎖定攻擊美國的運輸和後勤網路，以擾亂美軍作戰能力[51-52]。

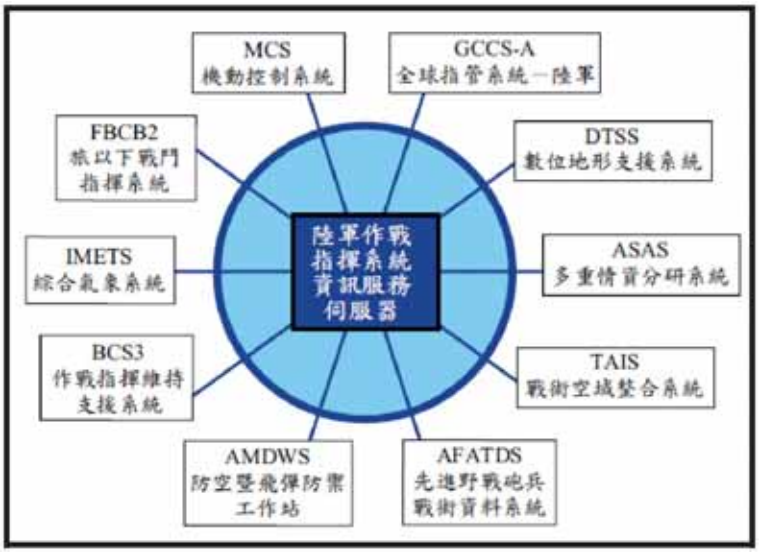
觀察中共網路戰整備，現階段，大陸發展「網電一體戰」的作戰能量，項目包括：透過電腦網路攻擊，來完成長距離的攻擊破壞任務、運用電腦網路攻擊癱瘓對手國的重要經濟活動能量，達到警告嚇阻的效果、運用電腦網路瓦解對手國的C⁴ISR系統、運用電腦網路攻擊，發揮「先發制人」的戰略威懾效果、結合電腦網路和電子戰特種部隊奇襲能量，達到心理威懾戰略目標，並迫使對手國接受政治談判條件、運用電腦網路攻擊破壞美軍的後勤補給系統，以及運用電腦網路攻擊癱瘓對手國的金融、電力運輸與通訊系統等，圖六為美軍網路作戰示意圖。中共執行「網電一體戰」任務的主要機構包括：解放軍總參四部負責電腦網路運作及電子反制能量的組建；解放軍總參三部負責國防信息化保障任務，並執行戰場網路情報蒐集；在大陸七大軍區設置戰區聯合作戰指揮部，並成立信息對抗中心，負責電子對抗

及網路信息體系防護；陸軍事科學院及國防大學則是負責研發各種「網電一體戰」的作戰指導與準則。此外，大陸可以運用「網電一體戰」工具包括：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，執行任務平台包括：電腦、全球網路連線，以及有能力的操作人員[51-52]。

圖六　美國與中共間網路危機升級，美國遭受來自中共的網路攻擊持續發生。(U.S. Navy photo by Mass Communication Specialist 3rd Class Kasey Krall/ Released)[52]

網狀化作戰(Network Centric Warfare，NCW)，或稱為網路中心行動(Network Centric Operations，NCO)是一種美國國防部所創的新軍事指導原則，以求化資訊優勢為戰爭優勢。其做法是用極可靠的網路聯絡在地面上分隔開但資訊充足的部隊，這樣就可以發展新的組織及戰鬥方法。1998年，網路中心戰NCW概念在美國海軍研究所會議錄文集阿瑟・塞布羅夫斯基海軍中將(Vice Admiral Arthur Cebrowski)和約翰・加特斯卡(John Gartska)合著論文公開發表。1999年在聯六(J6)主導下，美軍完成了網狀化作戰具體化的計畫指導作為。2001年由國防部提交國會備案，並將原先的遠程建軍規劃擴充為《2020聯戰願景》，明確的指出聯合作戰的四大目標－主宰機動、精準接戰、全面防護、後勤為先－作為未來20年三軍建軍的準據。美國國防部指令全球資訊網格將成為支援網路中心行動的基本技術架構。據此行政指示，全球資訊網格最後還是要包含所有先進的武器平臺、感應器系統及指揮控制中心。系統集成一語就常用來描述這種大規模整合工程。美國不少重要軍事計劃也都開始試支援網路中心戰技術；其包括美國海軍的合同聯合迎戰能力(CEC)及美國陸軍的未來戰鬥系統(FCS)計劃。網路中心相容問題專案為每一階段的網路中心問題，提供符合美國國防部NCW目標的可執行指導，網狀化作戰並成為美軍軍事轉型「整體化聯合作戰」的核心指導理論。這些指導都來自各指令、政策及命令中的高層次抽象的概念，網路中心行動是前任美國國防部長唐納德・拉姆斯菲爾德推行的國防部轉型的基石；它亦是美國國防部秘書辦公室軍力轉型辦公室五個目標之一，圖七為美軍網狀化作戰陸軍作戰指揮系統圖[53-58]。

美軍網狀化作戰建設強調從統一觀念著手，將各軍種提出作戰理論與其結合；第二步是要求三軍未來所有系統須與此網路聯連；第三步是將各種武器系統、作戰平臺、各級部隊比照「網際網路賦予IP」的方式納入管理。在美國國防部「全球資訊電網」(Global Information Grid，GIG)理念與架構之下，陸軍以其5個司令部－北方、南方、中央、歐洲、太平洋做為「網路勤務中心」(Network Service Centers，NSC)，與「全球資訊電網」構連，以企業總部的型態在全球建立美軍的「陸戰網」(Land WarNet)，將陸軍的作戰網路、基礎架構、通信設施與應用系統，結合成為一個全球性標準、保密又經濟的網狀化作戰體系。美國空軍第10-17號政策指令「網際空間作戰(Cyberspace Operation)」將網路情監偵清楚定義賦予空軍情監偵確保提供合作分析、綜合情報與情監偵『計畫作為與蒐整、蒐集、處理與運用、分析與產出、分發』(PCPAD)跨領域、綜整與自動化能力，以遂行網際空間作戰。空軍情監偵處處長羅伯・奧圖(Robert P. Otto，Director of Air Force ISR Agency)強調美國空軍將『用於網路情監偵』廣泛定義在支持網際空間優勢所遂行的情監偵，不論來源、方法或媒介為何。美國國家情報局前局長麥可・麥康納(Mike McConnell)觀察認為最先進的網路空間情監偵與防禦，是依賴「事後鑑識」(after-the-fact-forensics)來評估損害並辨識出惡意攻擊犯罪者[54-58]。



圖七　美軍網狀化作戰陸軍作戰指揮系統圖[58]

2014年6月初，美國國家安全局和美國安全公司確定了位於上海閘北區的中共番號為61486部隊，對歐美和日本的政府機構、軍事承包商和太空衛星行業研究公司進行的駭客攻擊。美國國安局及其合作夥伴此前在追蹤中國逾20個駭客團體中，發現一半以上是中共網軍，其網絡攻擊範圍從衛星、無人機和核武器元件製造商，到科技能源公司和研究機構。蘭德公司此項研究兩位作者，全球安全委員會主席、蘭德公司資深研究員龔培特(David C. Gompert)和國際戰略研究所資深管理科學家、蘭德公司網絡戰分析師利比奇(Martin Libicki)表示，美、中採取網路戰作為應

對雙方策略的一部份，只會導致不穩定的危機更為加劇。目前，中共施用的網路戰呈現「升級」狀態，目標不僅針對國家、政府及商業基礎設施和網絡，更大的可能是破壞對方的軍事系統運作，即毀損對方的軍事防禦及攻擊能力。此項研究中談到，網路戰就是要從根本上破壞對方軍隊運作所依靠的網路系統。一旦網路攻擊得逞，就會導致這些系統中的信息操作失靈、出現惡意信息或指令，從而降低指揮自動化系統(C4ISR)、武器性能、軍隊後勤或其它發揮「關鍵任務」的運作功能。根據2014年美國國防部研究指出，網際網路空間有七個關鍵戰略高地，包括作業系統、搜尋引擎、通信裝備基礎設施、雲端運算、治理論壇、密碼體系，以及網際網路協定第六版，網際網路空間七個關鍵戰略高地整理如表十一[53-58]。

2011年3月，日本首次舉行網路安全戰略兵推，自衛隊組建網路防護隊徵求民間專家，充實網路安全防護，並與美國合作，提高防禦能力。隨後日本政府在陸續發佈的「防衛白皮書」，更強調自衛隊因應網路攻擊的必要性，並指出情報通訊是

表十一　美國網際網路空間關鍵戰略高地分析(自行整理)[57]

關鍵戰略高地	美國對網際網路空間七個關鍵戰略高地分析
作業系統	美國微軟作業系統全球市佔率高達 92%，在行動作業系統領域，美國公司 Google Android 佔全球市場 43%。
搜尋引擎	作業系統決定電腦系統技術特性，但搜尋引擎卻能對觀念造成巨大影響。美國公司 Google 在搜尋引擎的全球市場佔有率達 91%，藉由優異性能來吸引使用者，自然形成議題設定與偏好形塑的力量。
通信裝備基礎設施	幾乎所有網際網路的資訊流量，都通過美國公司的通信裝備基礎設施。近年來大陸積極創建通信裝備骨幹，並運用華為公司拓展東南亞、中東及非洲市場，以降低其資訊流量通過美國基礎設施的需求。
雲端運算	雲端是一種將圖片、文件和電子郵件等資料儲存到遠端電腦方式，不會占用電腦、手機或其他裝置空間。通信裝備基礎設施主要在保持對全球通信路徑的影響力，而雲端運算則是擁有網路上，集中處理及儲存資訊趨勢的影響力。隨著雲端運算服務市場成長，越來越多資料將會流經美「中」兩國所擁有基礎設施，使其成為網路空間戰略競逐焦點，並直接衝擊國家安全結構與內容。
治理論壇	全球網路空間治理論壇由許多利害關係人組成集團，共同決定網際網路空間的通信標準，如「電機電子工程師學會」(IEEE)、「國際電信聯盟」(ITU)、「全球資訊網聯盟」(WWWC)等組織，在形塑網路領域特性上，均扮演不可或缺的角色
密碼體系	密碼體系的數學基礎提供網際空間安全根基。如果保護資料安全的方法出問題，則網際網路的整個經濟引擎可能毀於一旦。美國政府在密碼體系領域扮演重要角色，但密碼體系也代表網際空間中的軟實力要素，因為政府無法對其本身以外的網路發號施令，然而，國家標準技術協會所制定開放、具競爭性的標準程序，有助於吸引重視安全的民營公司並壯大美國主導的密碼體系。
網際網路協定第六版(Internet Protocol Version 6，IPv6)	目前大陸當局已決定在新一代網際網路架構中，採用此種標準的大型計劃；同時大陸地區有超過六億網際網路使用者，且其經濟仍在成長中，故有潛力對網際網路協定第六版、其硬體設備執行面與治理論壇發揮極大影響力。美國政府也協助美國企業克服採用新版本的財務障礙，並避免喪失其對網際網路重要領域的優勢地位。

指揮系統的基礎，資訊技術的進步，將可提升軍隊對通訊網路的依賴程度；值得注意的是，針對各國政府和軍隊的網路攻擊，將可能產生重大危安事件，日本提高情報系統和網路通訊防護能力，顯示日本針對網路空間強化攻防能力的重視。根據我國國防部2012年10月8日公布的國防報告書指出中共2020年具全面犯台能力，中共對台以武促統思維與軍事準備工作並未隨兩岸關係改善而有所調整，中共規劃於2020年建置完成對台用武全面性作戰能力，顯見其對我國的威脅未曾稍減。美國與中共積極發展網軍能量，不強調大規模殺傷而重視體系癱瘓。分析這種作戰方式，基本上是貫徹「巧戰而屈人之兵」的用兵思想，以「不對稱性戰略」創造有利的戰略態勢，減少附帶傷亡數量，並迫使對手國快速進入政治談判階段，接受其所提出的條件。美國認為網際空間是最新的作戰領域，在此新領域的網路情監偵作為上須取得並有效利用情資以全面支持各種軍事作戰行動[48-50]。

我國國軍聯合指管通資情監偵系統願景係以建構網狀化系統，藉先進通資科技，整合指管中心、武器載臺及監偵系統，並運用創新思維與戰場管理系統，掌握戰場即時資訊。國軍已整合主要指管與情監偵系統數據鏈路，建構自動化防空指管系統、制定指管共通作業環境規範、提升聯合通信系統能量、強化通信保密機制，語病建置中、長程偵蒐系統，提升並擴大籌建聯合指管通資情監偵能力。國軍須強化戰場管理、指管情傳以及早期預警能量，俾精準掌握敵情動態，靈活指揮部隊作戰。聯合資電作戰係以建立「早期預警、快速反應、有效反制、遲滯攻擊」能力為目標，俾防衛我方指管系統、武器射控、雷達系統與通訊平臺安全，避免遭敵利用、癱瘓與破壞，確保我防衛作戰全程資電安全與優勢。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。面對複雜資電作戰環境，國軍必須精進資訊、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[51-52]。

未來整建目標在於聯合資訊戰能力與聯合電子戰能力，事實上，聯合資訊戰能力整備除了持續發展綜合性資訊戰力，以確保國軍資電優勢外，更需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，提升我資訊安全防護與作戰能量；並積極規劃國軍資訊組織及人力編配基準，並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。聯合電子戰能力整備則著重點於運用國軍電子戰初步能量，並統籌規劃電磁防護能力，提升戰場存活率；且運用各主戰兵力之威脅預警能力，結合各主要陣地電磁防護能量，建立全面聯合電子戰防護戰力以及結合各國電子戰發展趨勢與國軍電子

表十二　聯合指管通資情監偵支援戰力整理表(自行整理)

聯合C⁴ISR系統	聯合指管通資情監偵支援戰力分析
聯合指管系統	提升指管效能：提升現有指管系統性能，擴充鏈路頻寬及保密、抗干擾能力，以強化指管情傳作為，精進戰場存活度。
	完備載臺鏈結：擴建載臺數據鏈路系統，以有效遂行指揮管制、目標分配、火力協調、戰損回報等戰術指管作為，確達殲敵致勝目標。
	建構地面部隊指管系統：依據聯合防衛作戰構想，籌建地面部隊指管通資情監偵系統，強化戰場管理及指管效能，提升部隊整體戰力。
聯合通信系統	整合通信傳輸平臺：整合指揮所之各類頻段無線電網路、有線電話及網路電話，提升通信裝備互通能力，強化語音指管功能。
	強化無線通信網路：採購研製超高頻、高頻無線電機，建構具跳頻、安全及抗干擾無線電網路，強固機動通信與支援指管情傳能力。
	運用民間通訊資源：結合國內公民營行動通信設施，規劃、發展國軍地面行動寬頻網路平臺，以滿足地面行動指管訊息通聯，並可支援災害救援通聯所需。
	發展通資保密裝置：研製新式通資裝置保密器模組，加強密式邏輯架構安全強度，提升保密器維管能量，確保通資保密安全。
聯合情監偵系統	延伸監視涵蓋範圍：有效運用中、長程電偵系統，延伸地面及海、空監視能力，並結合指管系統，建立共同作戰圖像，共享戰場情資，俾提升早期預警能力及戰場透明度。
	精進偵蒐技術：加強對敵電子參數偵蒐能力，逐步擴增機動偵蒐裝備，整合預警情資，以供各級作戰中心與指揮所來運用。

戰發展作為，逐步提升並整合未來電子戰指管平臺，以統合整體戰力。針對於聯合指管通資情監偵能力未來目標包括指管系統、通信系統與情監偵系統，表十二為聯合C⁴ISR支援戰力系統整理表[53-55]。

伍、結論與因應作為

2008年俄羅斯對喬治亞共和國進行一系列廣為人知的網路攻擊，《經濟時報》2010年8月5日以「間諜戰：印度網軍就緒」為題報導，依據報導，印度參考中國網路戰爭做法，催生一支由軟體專家組成的團隊，將透過入侵電腦系統手法，打探敵國機密資料。加拿大多倫多大學公民實驗室指出，中國有一幫駭客對印度進行廣泛間諜活動，並自國防部竊取機密文件。事實上，美國與中共積極發展「電腦網路作戰」(Computer Network Operations)能力，是建立「不對稱性戰略優勢」的重要環節，而其中的內涵包括「制信息權」和「制電磁權」，並以「電子對抗」、「通信對抗」，以及「網路對抗」為主要作戰形式。此外，美國與中共兩國將整體的「電腦網路作戰」能量，隱藏在作戰部隊和非官方的民間公司組織中，並透過電腦網路的連結，可在世界上各個角落，直接或間接地攻擊目標，進行網路作戰而不易被察覺。這種「看不見的新一代戰爭」與「巧戰而屈人之兵」作戰型態，已對相關國家軍事電腦網路通訊及重要機構和設施的電腦網路系統，造成相當程度的威脅，同時

也對國際關係的競合格局，營造新的挑戰。面對美國與中共兩國網軍舖天蓋地、無孔不入的活動，世界各國多已策訂相關資訊安全措施。德國資訊安全局為反制大陸網軍行動，特別製作網路安全手冊；英國政府為對抗駭客攻擊，也積極發展一套網路武器系統，在國安戰略會議中，更將網路安全列為第一要務。美國由於是駭客組織攻擊的主要目標，美國國防部每天對其網路進行600萬次偵測，並透過定期的「網路風暴演習」，以期及時發現防禦漏洞，作為增進安全維護的參考；另以美國為主導的英、法、日等約六十多個國家，亦相繼締結資訊安全合作協定。美國深知為維持各項優勢的戰略能力，網路領域需迅速與其他軍事作戰領域相結合，美軍更將投資於新增與擴充的網路戰力及部隊，俾加強遂行網路作戰與支援世界各地軍事作戰行動，並於作戰司令規劃與執行軍事任務時給予支援，同時反制對美國的網路攻擊[55-59]。

現代化戰爭不僅是國防科技的整合運用，更注重聯合作戰的效能。前國防部長嚴明先生於主持104年元月份月會時強調，國軍必須提升C4ISR系統，強化網路、資訊、電子戰攻防能量，研發兼具偵蒐與攻擊的無人飛行載具，和戰術性制壓飛彈等新銳武器系統，以爭取作戰優勢。此外，未來國防施政，須以創新、不對稱戰力建構為主軸，以達「防衛固守、有效嚇阻」的目標，整合裝備提升國防自主能量，強化三軍聯合作戰訓練和災害防救整備。中國大陸自1985年起，就開始發展「網電一體戰」的能量。大陸國防部發言人耿雁生於2011年5月間證實，中共已經建立「網路藍軍」，並且強調「組建網路藍軍，就像組建陸軍、空軍一樣。自2006年起，中共網軍大約竊取115家美國大企業數據，美國企業在2013年總計損失約3000億美元，且大部份是中共網路間諜所為。美國國防部於2011年7月中旬發佈「網路作戰戰略」，除明確要求五角大廈將網路視同作戰領域，並對來自其他國家的網路駭客攻擊，認定為已構成戰爭行為，將比照陸、海、空三軍，從被動防禦轉為主動攻擊，以因應日益升高的網路安全威脅，同時計劃與民間企業，以及其他美國盟邦共同發展網路作戰能量。在世界戰略競逐格局下，電腦網路本身就是一種武器與戰場。網路作戰與防衛能力越來越重要，因為現今的所有戰力都離不開網路，不論是戰場情偵、目標鎖定，或是聯合作戰，都需要運用網路。現階段，美國與中共兩國在國家安全戰略架構中，已將網路空間視為新戰場，爭奪網路空間控制權已勢在必行，導致兩國網路安全競合關係更加複雜與不確定。日前，中共正式成立「中央網路安全和信息化領導小組」，由習近平領軍，顯示中共高層已將網路安全及發展，提升為國家安全戰略一環。而中共領導習近平特別強調，「沒有網路安全，就沒有國家安全；沒有信息化，就沒有現代化」。美國總統歐巴馬亦於《21世紀美國國防戰略綱

領》，將網路空間能力列為最優先發展重點。目前，共軍目標是在2020年建立全球第一支「信息化武裝部隊」；國軍應積極籌建專業之關鍵技術與能量，期在有限的國防預算及人力條件下，建構「創新與不對稱」戰力，達成「嚇阻威脅、預防戰爭」目的[60-63]。

國防部於2014年11月18日「103年通資電工作檢討會」中，提出「發揮創新思維，建構優勢戰力」、「結合關鍵科技，提升資電能量」、「統合指管規劃，滿足聯戰需求」、「落實教育生根，培育專業人才」及「貫徹政策指導，強化資安作為」等五項指示，要求各單位依據建軍構想及兵力整建計畫，落實各項整備工作，以聯合作戰為目標，整體統合規劃，逐步提升通資電整體戰力。值得注意的是，我國為落實資安防護應變作業，國防部依行政院國家資通安全會報指導，設置「資通安全處理小組」，並策頒相關行政規則，以有效掌握國軍資通安全事件通報及應處，釐清資安事件責任歸屬；另配合行政院資通安全辦公室，執行資通安全事件應變、處置及相關演練作業，適時調整回報、處置與復原等機制。2014年11月20日國防部通信電子資訊參謀次長室在立法院外交及國防委員會報告「國軍資安防護整備作為」，國防部表示國軍持續發掘資安威脅與弱點，輔導各單位建立資安風險評鑑能力，妥擬風險對策及管控措施，另藉資安相關預算編列，挹注資源於高風險項目的整備，以降低資安風險肇生。國防部秉持管理與科技運用並用原則，以有效管理作為，降低資安風險，提昇國軍人員資安認知與防護觀念，運用資訊科技技術強化因人員精簡造成之資安漏洞。面對駭客之肆虐與對岸中共不斷致力於網路作戰力量之提昇，為確保國軍資訊安全，國軍人員都必須建立正確的資安防護認知，確實遵守相關規定要求的各項防護措施，才能堅守資安防線，防堵中共駭客入侵[64-66]。

資訊戰特性為戰場透明化、指揮管制即時化與指管體系網路化，面對中共不斷擴張發展軍事武力，對資訊化戰爭所需之整體策略資訊系統須詳加規劃，針對資訊作戰方面，未來因應與建議探討十點分述如下：第一、有效整合通信網路：建立三軍通用戰術聯戰網路為目標，結合國軍有、無線電通訊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，以充分有效運用整體國家資源，提升通資戰力，有效支援作戰。；第二、強化資訊作戰教育訓練：加強包括網路化作戰與網路情監偵等相關教育訓練確保資訊安全；第三、強化電子戰作業能量：依照國軍未來電子戰作戰構想及任務特性，更進一步積極強化電子戰對抗能力，指導三軍電戰部隊定期演訓外，並研製先進電戰裝備，以加速推動國軍電子戰戰力整備，建立跨領域整體電戰防護網，以發揮整體戰力。第四、精進網路戰理論技術：吸收現代網路作戰科技理論技術與新知，加強網路攻防技術與演練；第五、精進預警系統：

研發長程雷達、預警衛星與預警機，並加強預警系統的反電子干擾、反制、反反制能力及抗空中攻擊能力；第六、整合力量強化資訊戰策略：整合政、軍及民間組織力量確保網際安全，並與友邦建構穩固網路安全合作機制等，尤應針對網路安全政策議題制定嚴格規範，律定安全技術與使用者遵守之規範；第七、建立資訊優勢戰力：目前資訊戰的重點乃在網路安全防護，且以全方位思考與創意運用為原則；在發展安全防護機制與系統裝備之外，更朝向構建自動化、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網路情監偵能量及反制作為，俾確保國軍在資訊戰場優勢；第八：籌建聯戰指管鏈路：依據現況賡續整合三軍通資現有能量，充分運用民間科技，整體規劃並建置出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；第九、嚴密管控通資安全：發展軍種積極資訊防護及主動網路監偵能力，以確保三軍部隊通資安全，維持部隊完整指通力、機動力、打擊力，鞏固部隊安全；第十、落實資安風險控管：強化資訊安全風險控管，可定義超出預期狀況之緊急應變程序、處理方法及目標，保護關鍵資訊資產機密性、完整性、可用性管制方法，對於資訊安全風險之控管提供完整週延的作業機制，以達成組織資訊安全確保目的。尤應針對遭到網路攻擊後之應變能力及復原措施與機制，應促使其制度化。因應未來作戰，我們應針對敵情威脅，確定我資訊戰需求，從健全組織、落實戰訓、人才培育、裝備研發、整合體系等方向及早完成準備，建立一支具備現代化能力的資訊戰部隊，以優勢資訊戰開創對我有利的態勢，同時建立全民認知資訊戰對國家安全的重要性，確保國家之生存與發展[67-70]。

陸、參考文獻

〔1〕維基百科，http://zh.wikipedia.org/wiki/%E4%BF%A1%E6%81%AF%E6%88%98，存取時間，2015年1月31日，取自維基百科網。
〔2〕Richard A. Clarke and Robert K. Knake，譯者王文勇，“網路戰爭下一個國安威脅及因應之道Cyber War-The Next Threat to National Security and What to do about it”，中華民國國防部發行軍官團教育參考叢書642，2014年9月。
〔3〕萬仁奎，“CNN：北韓駭客部隊瀋陽設秘密據點”，中時新聞電子報，http://www.chinatimes.com/，2015年1月7日。
〔4〕E-NEWS，“Web Security網站安全基礎篇(二)”，2010年第15期,取自中央研究院計算中心通訊電子報。
〔5〕翁興國，中山科學研究院資訊通信研究所，“網路攻擊與防禦訓練系統之建模與模擬技術探討”，新新季刊，第42卷第2期，210-213頁，2014年4月。
〔6〕James C.Mulvenon et.，楊紫函譯，“中共對美國軍事變革之反應”，台北：國防部史政編譯室，2010年12月。
〔7〕郭勝偉，“信息化戰爭與網電部隊”，北京：國防大學出版社，2008年7月。
〔8〕楊中漢、溫世峰，“現代信息戰”，北京：星球地圖社，2009年1月。
〔9〕里．阿米斯德，余佳玲、蕭光霈譯，“資訊作戰-以柔克剛的戰爭”，台北：國防部史政編譯室，2008年8月。
〔10〕呂炯昌，“美印組成網路聯合部隊對抗中國大陸網軍”，尖端科技雜誌，第348期，2010年7月。

〔11〕曹郁芬，“軍力報告-美報告：中國五至十年內可全面封鎖台灣”，2014年8月14日，取自自由時報。
〔12〕資通安全資訊網，“國家資通安全會報”，2014年1月3日,取自第201401002期資通安全資訊網電子報。
〔13〕美國國防部，“2014四年期國防總檢報告Quadrennial Defense Review QDR 2014”，2014年3月4日。
〔14〕陳清泉，“制霸網路者，制霸世界”，2014年8月14日，取自蘋果日報。
〔15〕劉宜友，“淺析中共網電一體戰”，國防雜誌，第26卷第3期，台北：國防雜誌社，2011年。
〔16〕崔敬熙編譯，綜合外電報導，“加強防駭美軍網路特遣隊成立”，2014年10月28日，取自青年日報網。
〔17〕政戰局保防安全處，“建立安全共識防敵滲透蒐情”，青年日報，2014年9月22日。
〔18〕李建興，IThome電週文化網，“虛擬攻防成戰爭前哨戰美海軍打造網路戰爭支援決策系統”，2014年11月23日。
〔19〕陳嘉宏，中山科學研究院資訊管理中心，“新型態戰爭及資安防護策略探討”，新新季刊，42卷第21期，2014年1月，226-232頁。
〔20〕湯佳玲，“中國18萬網軍威脅我將分級聯防”，2015年1月13日，自由時報。
〔21〕翁浩正，“更大的網路攻擊等著台灣-資安危機就是國安危機系列之二”，2015年1月14日，取自蘋果日報網。
〔22〕張晏彰，“陳鎮湘：正視大陸網軍對我威脅”，青年日報社，2014年11月22日。
〔23〕張晏彰，“國是論壇陳鎮湘：提高資安指揮層級確保網安”，青年日報社，2014年9月27日。
〔24〕李忠憲，“未來戰爭是數位戰爭”，2014年7月26日，取自蘋果日報。
〔25〕王能斌，“正視網路統合今年美軍發展要務”，青年日報社，2015年1月20日。
〔26〕吳柏毅，“跨部會強化資安防護完備安全機制脅”，青年日報社要聞，2014年11月21日。
〔27〕王明華、嚴寒冰、李佳、賀敏、紀玉春，“2013年中國網際網絡安全報告”，2014年12月10日，http://www.cert.org.cn/publish/main/。
〔28〕胡光曲，“美軍秘密制定網路戰規則從國內防禦到全球攻擊”，華夏經緯網，http://big5.huaxia.com/，2013年5月24日。
〔29〕青年日報社，“國軍落實資安防護整備-嚴防駭客攻擊手段”，2014年11月20。
〔30〕梁華傑，“青年日報專論：共軍駭客入侵劇增美掌控「制網路權」應戰”，http://news.gpwb.gov.tw/news.aspx，2013年3月27日。
〔31〕阿波羅新聞網，“中華民國：中共網軍18萬人研發各類的惡意病毒”，2014年11月20日阿波羅新聞網5232-11-21訊，2015年01月13日存取。
〔32〕C⁴ISR Go South，陳克仁譯，“擴大籌建指管通資情監偵戰力(C⁴ISR Go South)”，國防譯粹，40卷5期，35-46頁，2013年5月。
〔33〕USA Department of Defense，李永悌譯，“2014美國四年期國防總檢討Quadrennial Defense Review2014”，中華民國國防部發行軍官團教育參考叢書640，2014年6月。
〔34〕林盈達，“媒體被駭政府怎能置身事外－資安危機就是國安危機系列之一”，2014年7月22日，取自蘋果日報。
〔35〕林盈達，“媒體被駭政府怎能置身事外-資安危機就是國安危機系列之一”，2015年1月14日，取自蘋果日報網。
〔36〕王力等，“病毒武器與網絡戰爭”，北京：軍事誼文出版社，2001年1月。
〔37〕David Alexander，李育慈譯，“網路戰時代來臨(Cyberwar comes of age)”，國防譯粹，第36卷第2期，2009年2月。
〔38〕The Epoch US，“北約首度談網路安全將成立防禦小組”，大紀元網站，2013年06月05日，http://www.epochtimes.com，2015年2月7日存取。
〔39〕USA Department of Defense，黃文啓譯，“2010美國四年國防總檢討Quadrennial Defense Review QDR 2010”，台北：國防部史政編譯室，2010年11月。
〔40〕Elinor Sloan，黃文啓譯，“軍事轉型與當代戰爭”，國防部史政編譯室，2010年6月。
〔41〕蔡仁照，“信息化戰爭論”，北京：國防大學出版社，2007年12月。
〔42〕Information Security資安人科技網，“台灣名列全球惡意網站造訪第五名防護刻不容緩”，取自資安人科技網，2014年10月3日。
〔43〕資安人科技網，“掌握未來十大資安技術，有效做好攻擊防禦”，2014年7月31日，取自資安人科技網。
〔44〕資通安全資訊網，“國家資通訊安全發展方案(102年至105年)”，2013年12月，取自行政院國家資通安全會報。
〔45〕陳曉莉，IThome電週文化網，“Sony Pictures 25GB員工資料被放上網，FBI發出「毀滅性網路攻擊」警告”，2014年12月3日。
〔46〕陳曉莉，IThome電週文化網，“資安業者分析「毀滅性網路攻擊」惡意程式：Sony Pictures內部網路早就被摸透”，2014年12月5日。
〔47〕呂熠昌，“軍武論壇-電磁脈衝大陸犯台秘密武器”，NOWnews，2014年12月27日。

〔48〕國防部，“中華民國102年四年期國防總檢討(QDR)”，第四章國防組織與轉型，2014年9月。
〔49〕USA Homeland Security，“Executive Order 13636: Improving Critical Infrastructure Cybersecurity”，Department of Homeland Security Integrated Task Force，Incentives Study Analytic Report，2013年6月12日。
〔50〕胡光曲，“揭秘美軍網路攻擊戰術：已研2千多種病毒武器”，華夏經緯網，http://big5. huaxia.com/，2015年1月21日。
〔51〕人間福報，“中國網軍無孔不入美無對策”，綜合外電報導，http://www.merit-times. com.tw/NewsPage.aspx?Unid=255100，2010年3月10日。
〔52〕中央日報，“ 美「中」網路競逐最新情勢”，中國國民黨中央政策委員會大陸情勢雙週報第1668期，2014年6月13日，取自中央網路報。
〔53〕C⁴ISR GO SOUTH，陳克仁譯，“擴大籌建指管通資情監偵能力”，國防譯粹，第40卷第5期，2013年5月，35-41頁。
〔54〕維基百科，“網路中心戰”，http://zh.wikipedia.org/wiki，存取時間，2015年1月31日，取自維基百科網。
〔55〕Matthew M. Hurley，章昌文譯，“網路情監偵概念(For and from Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance)”，國防譯粹，第40卷第5期，2013年5月，17-25頁。
〔56〕FireEye，“網路安全的馬其諾防線：實際評估深度防禦模式”，FireEye及Mandiant共同完成2014年測試報告，http://www.fireeye.com，2015年2月4日存取。
〔57〕曾復生，“七個關鍵戰略高地”，財團法人國家政策研究基金會，國安(析)103-020號，2014年3月5日。
〔58〕曾祥穎，“美陸軍網狀化作戰之檢討與展望”，陸軍學術雙月刊，第48卷，第526期，2012年12月，4-20頁。
〔59〕國防部通信電子資訊參謀次長室，“認識駭客攻擊趨勢落實資安防護”，青年日報，2014年5月12日。
〔60〕蔡宗恆，“嚴部長：專注戰訓本務打造精銳勁旅”，國防部軍事新聞通訊社，2014年12月29日。
〔61〕中央日報網路報，“特稿/美「中」網路競逐最新情勢”，http://www.cdnews.com.tw，2014年06月13日。
〔62〕蔡宗恆，“國防部持續加強資安防護機制妥擬風險對策”，國防部軍事新聞通訊社，2014年11月20日。
〔63〕Benson，“資安危機就是國安危機系列之三台灣可以成爲資安強國”，2014年7月24日，取自蘋果日報。
〔64〕中國國民黨雙周報，1668期，登載於中國國民黨全球資訊網，http://www.kmt.org.tw，103年6月11日。
〔65〕青年日報，“強化網安歐巴馬擬砸4448億”，編譯組／綜合外電報導取自青年日報，2015年5月6日。
〔66〕行政院國家資通安全會報，第201502001期資通安全電子報，財團法人國家實驗研究院科技政策研究與資訊中心，2015年2月6日。
〔67〕人間福報，“加入間諜戰印度催生網軍”，外電報導，http://www.merit-times.com.tw，2010年8月6日。
〔68〕吳明芳，“憂網路力量撼政權陸鎖國網攻應對”，大紀元新聞網The Epoch USA，2015年02月02日。
〔69〕何伊，“蘭德公司：美中一旦開戰中方首攻網絡”，大紀元新聞網The Epoch USA，2014年11月18日。
〔70〕Rosemary M. Carter, Brent Feick, and Roy C. Undersander，李永悌譯，“攻擊性網路(Offensive Cyber for the Joint Force Commander: It’s not that Different)”，國防譯粹，第40卷第5期，2013年5月，47-55頁。

作者簡介

教授　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：航空技術學院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。