淺析中共「網電一體戰」

Analysis of the PRC's "Integrated Network and Electronic Warfare"

劉宜友 上校 (Yi-Yu Liu)

國防大學陸軍指揮參謀學院主任教官

提　　要

當前，共軍正全面推動軍事轉型，不僅重視中國傳統的軌道謀略，亦加強運用於非對稱作戰、聯合作戰、網電一體戰，及非戰爭式動武手段。在未來聯合作戰模式的相關論著中，均強調「資訊攻防機先」與「制電磁權奪取」在作戰初期階段之重要性，並確保爾後戰場態勢的掌握。其理論人員在廣泛深入研究信息作戰的基礎上，更創造出「具中國特色」的「網電一體戰」名詞與作戰理論。顯見「網電一體戰」，已是共軍「一體化聯合作戰」的基本形式。

關鍵詞：信息作戰、電子戰、網絡戰、網電一體戰

Abstract

Currently, the PLA is comprehensively promoting the military transformation, with emphasis on traditional Chinese track strategy, as well as asymmetric warfare, joint operations, integrated network and electronic warfare, and military operations other than war. Related papers on models of future joint operations have emphasized the importance of "information offensive and defensive priority" and "seizing the electromagnetic dominance" at the early stages of the war, and to ensure mastery of the battlefield superiority. Based on information operations, the research staff, create a "Chinese-styled" and "integrated network and electronic warfare" term and a operational theory. Obviously, the "network and electronic warfare" is the basic form of PLA's "integrated joint operations".

Keywords: Information operations, Electronic warfare, Cyber warfare, Integrated network and electronic warfare

壹、前　　言

2010年8月，當美國公布年度例行之《中國軍力報告》，在其第二章〈瞭解中國戰略〉表示，共軍長期目標是打造一支能夠進行和贏得「信息化條件下的局部戰爭」。[1]

1〈美國2010中國軍力報告〉，《新浪網》，http://www.warchina.com/news/junshipinglun/2010-08-25/123336_4.html

當前，共軍正全面推動軍事轉型，不僅重視中國傳統的軌道謀略，亦加強運用於非對稱作戰、聯合作戰、網電一體戰，及非戰爭式動武手段。在未來聯合作戰模式的相關論著中，均強調「資訊攻防機先」與「制電磁權奪取」在作戰初期階段之重要性，並確保爾後戰場態勢的掌握。[2]其理論人員在廣泛深入研究信息作戰的基礎上，更創造出「具中國特色」的「網電一體戰」名詞與作戰理論。[3]另據美國國會2009年10月「美中經濟暨安全檢討委員會」(US-China Economic and Security Review Commission)提出標題為「中國的網路作戰與情報刺探」(Chinese Cyber Warfare & Espionage)的調查指出，中共推動軍力現代化10年以來，已經徹底強化科技戰力，並藉由網路組建特性，針對「信息化局部戰爭」發展出「網電一體」等先進概念，企圖影響敵軍訊息傳遞的流暢性，進而控制戰場優勢。其中亦大力宣傳：「自中共開始發展網路作戰能力後，共軍正大舉延攬工商團體、學界等民間機構專才，甚至還與國內駭客的技術人士組織合作，滿足對新興的資訊戰力大量人力需求，[4]致美國政府及民間企業，不斷遭遇源自中共駭客的攻擊，造成大量機敏資料外流」。[5]顯見網絡戰攻防，已是共軍戰役理論的核心，致「網電一體戰」更成為其「一體化聯合作戰」的一種基本形式。[6]在此思維下，凸顯出中共除已擁有成熟的網路作戰能力外，[7]共軍於平時也越來越重視電子戰，期能在戰爭發生前就能廣蒐情資與參數，為未來戰爭奠下勝利基礎。

本研究係針對共軍「網電一體戰」之理論與兵力編組實施研析，為求客觀與聚焦，採「文獻分析法」與「內容分析法」併用方式，以激起相關研究者之腦力激盪，尋求我預應對策及作為。

貳、中共「網電一體戰」理論探討

共軍鑑於20世紀90年代以來，信息技術在軍事領域廣泛運用，推動機械化作戰向信息化聯合作戰轉型的發展，成為局部戰爭先進且有效的作戰型態。從世界近期所發生的局部戰爭不難瞭解，無論是電子戰、網絡戰、[8]網電一體戰、心理戰、精確打擊、癱瘓戰等體系間對抗的作戰模式，戰場信息攻防顯得格外重要，也成為作戰體系的神經中樞；而攻擊和防護戰場信息傳遞系統，更成為信息化作戰的焦點與主軸，徹底顛覆昔以

2 黃引珊譯，〈中共軍事戰略與準則〉，《國防譯粹》，第36卷第7期，2009年7月，頁4-7。

3 美國防部《2008年中國軍力報告》宣稱：「網絡戰是中共正在積極發展的一種作戰能力，並推出『網電一體戰』的作戰理論」。請參見：錢程燦，〈中國應警惕美國吹捧，克服弱點強化網絡戰力〉，《東方網》，http://www.chinareviewnews.com 20080317

4「資訊」與「信息」一詞，前者以美軍為首之歐美國家所採用，而中共多採用後者，本研究為忠於原著，則採原作者之用語。

5〈美國2010中國軍力報告〉，《新浪網》，http://www.warchina.com/news/junshipinglun/2010-08-25/123336_4.html

6 李柏彥譯，〈無形的網路戰爭〉，《國防譯粹》，第37卷第5期，2010年5月，頁6。

7〈美國會報告指中國運用網路戰對美展開情搜〉，《海峽資訊網》，http://www.haixiainfo.com.tw/76584.html

8「網路」與「網絡」一詞，前者以美軍為首之歐美國家所採用，而中共多採用後者，本研究為忠於原著，則採原作者之用語。

殲滅戰、消耗戰為指導的機械化聯合作戰思想。然發展癱瘓戰為主及速決的信息化聯合作戰理念，[9]可說是戰場高度網絡化基礎上的一種作戰指導新思維。

當前渠等武器裝備仍處於半機械化水準，欲進行信息化聯合作戰，將面臨指揮機制轉型、武器裝備多重發展、兵力結構重整、作戰觀念更新等挑戰。儘管如此，信息化聯合作戰，在中共有心發展下，已經不是「打不打」這麼簡單，而是如何「打得贏」、「贏的漂亮」的問題。為此，綜合運用「電子戰」和「網路戰」諸般手段，對敵電子目標和網狀化信息系統，進行的一體化偵察、攻擊與防護，[10]已成為共軍未來強化信息作戰首要。

一、名詞界定

共軍認為「電子戰」的發展，孕育了信息戰的產生，「網絡戰」的興起，則加速了信息戰理論的提出和成形，兩種手段的結合，構成了信息作戰的主體。[11]軍事學者沈偉光認為「信息作戰」是「傳統的軍事攻擊，只能指向對方的軍事力量和經濟潛力，而資訊攻擊則將貫穿對方的軍事、政治、經濟和整個社會，甚至影響國民的精神、觀念、心理等，進而崩解其國家的政經軍結構；另藉由癱瘓敵方的軍事、金融、通信、電子、電力系統和資訊網絡，再結合心理戰和戰略欺騙等手段，動搖軍心、民心和政府信念，達到遏制敵對國家發動戰爭企圖，或使之喪失戰爭能力為目的」。[12]另共軍《軍語辭典》對「信息作戰」之定義：「係指在軍事為利用、干擾、破壞敵方的信息和信息系統，並保護己方的信息和信息系統而採取的行動」。其目的在奪取並保持信息優勢，主要包括信息作戰偵察、信息攻擊和信息防護等，並以電子對抗、計算機網絡戰、心理戰為主要作戰型式。[13]前述之定義，均明確表達中共對信息作戰的超限性質與攻勢取向。

「網電一體戰」一詞，首見於美國防部《2008年中共軍力報告》，宣稱：「針對中共民用和軍事網絡的攻擊能力，正是共軍發展不對稱戰法的『非接觸作戰』重要組成部分」。[14]後在其《2009年中共軍力報告》之定義為：「利用電子戰、電腦網路作戰、動態殺傷等方式，以阻斷支持敵方作戰與投射武力的戰場網路資訊系統」；[15]又《2010年中共軍事與安全年度報告》則為：「運用電子戰、電腦網路作戰和主動攻擊，來擾亂戰場上支援對手作戰和力量投射能力的資訊系統」。[16]惟在共軍相關《軍語辭典》中並

9 曹正榮、吳潤波、孫建軍主編，《信息化聯合作戰》（北京：解放軍出版，2008年8月第2刷），頁1-2。
10 張建昌，《走進信息化戰爭》（北京：國防大學出版，2003年3月第1刷），頁56。
11 梅軍、樊祥，〈未來網電一體戰〉，《解放軍報》，2000年9月6日，版7。
12 沈偉光，〈二十一世紀的戰爭型態與安全觀〉，《中國評論月刊》，1998年2月，頁13。
13 夏征農主編，《大辭海—軍事卷》（上海：上海辭書出版，2007年7月第1刷），頁199。
14 錢程燦，《中國應警惕美國吹捧，克服弱點強化網絡戰力》《東方網》，http://www. chinareviewnews.com 20080317
15 黃引珊譯，〈中共軍事戰略與準則〉，《國防譯粹》，第36卷第7期，2009年7月，頁4-8。
16《美國2010中國軍力報告》，《新浪網》，http://www.warchina.com/news/junshipinglun/2010-08-25/123336_4.html

無明確之界定，茲以其信息化專家諮詢委員主任戴清民少將之論著為定名，「網電一體戰」：「係指在信息戰場上，將『電子戰』與『網絡戰』兩種手段綜合運用，為破壞敵方戰場網絡化信息系統，並保證己方戰場網絡化信息系統之正常運行，而採取之一體化攻擊行動」。就其目的則是在奪取戰場電磁和網路空間的主導權。[17]可說是揭示了「電子戰」和「網絡戰」的互補互融，成為作戰體系對抗的必然要求。

基此，「網電一體戰」已不是簡單地把「電子戰」與「網絡戰」相疊加乘的粗淺認知，而是要求這兩種手段的互相彌補不足之處。[18]它著眼於對戰場的信息獲取、傳遞、處理和運用全過程的削弱和破壞，進而通過「電子戰」來干擾敵方的信息取得，並以「網絡戰」來癱瘓敵方的信息處理和運用，並藉兩者綜合運用形成整體戰力，達到全面破壞敵方的指管系統及信息傳遞管道。[19]鑑此，在現代信息化的戰場上，唯有取得電磁和網絡兩個領域的優勢，方能掌握現代戰爭的主動權，致「網電一體戰」成為共軍信息作戰的主要形式。

二、「電子戰」與「網路戰」關係分析

「信息作戰」乃交戰雙方體系的攻防，在這場對抗中，各種網路系統，將是各種作戰體系的樞紐和橋樑，而交戰雙方網絡對抗的成敗，已直接影響整個指管效能發揮，乃至戰爭的勝負。基此，「電子戰」頻譜與電腦「網絡戰」攻防的結合，將成為掌控信息作戰的必勝要件，也成為未來戰爭中，高技術戰爭發展的必然趨勢，[20]儼然已主導其國防和軍隊現代化建設。

是以，在「信息作戰」成為決定未來戰爭勝負關鍵因素同時，指揮官作戰思維，亦順應未來戰場武器系統自動化，與資訊系統網狀化的兩大發展趨勢。在網電一體作戰中，「電子戰」與「網路戰」的相互融合、相互依存，互為對方提高作戰效能創造條件，必將成為信息作戰的基本形式。茲就其關係分析如次：

㈠「電子戰」的攻擊目的，端賴「網絡戰」技術發揮

在兩者性能比較上，電子與網路技術的發展，在作戰時已到了一個可以相互輔助的契合點，電子戰需依賴於網路技術的優化組合，始能發揮更大的作戰效能；[21]而在戰術運用上，由於戰場信息在網狀化系統傳遞下，高智慧和自動化的武器載台，成為電子戰攻擊主要目標；為使「電子戰」發揮更高威力，就須先了解對方各種網路平台架構，攻擊節點癱瘓系統。[22]因此，「電子戰」需要借助於「資訊戰」的協同配合，運用「網絡攻防」技術，方能達到整體效果。[23]

㈡「網絡戰」的戰果擴張，須藉「電子戰」手段發揮

17 戴清民，《求道無形之境》（北京：解放軍出版，2009年1月第1刷），頁170。
18 陳岸然、王忠，《信息戰視野中的典型戰例研究》（上海：學林出版，2009年4月第1刷），頁13。
19 梅軍、樊祥〈未來網電一體戰〉，《解放軍報》，2000年9月6日，版7。
20 馬亞西，〈資訊戰日新月異，網電一體戰橫空出世〉，《解放軍報》，2001年11月14日，版2。
21〈電子戰的未來與新特點〉，《中國戰略網》，http://str.chinaiiss.com/html/20104/ 12/wa2d84.html
22 梅軍、樊祥〈未來網電一體戰〉，《解放軍報》，2000年9月6日，版7。
23〈縱觀網路戰爭〉，《解放軍報》，2004年10月26日，版1。

網路的正常運行離不開電子技術，而攻擊手法的運用，電磁頻譜的控制就顯得相對重要。[24]因為，大部分信息交換必須在開闊空間，經由無線電磁波信號的發送和接收，來完成網路系統的介接，實現部隊的指揮與控制；同樣的情形，對敵方網路的破壞，亦須透過電子戰手段，在電磁頻譜領域中展開，針對敵方戰場信息傳遞及網路管道實施攻擊，才能取得最佳效果。[25]

爰此，共軍深知「網電一體戰」，乃是戰場信息作戰本質規律的客觀反映，所以必須針對信息作戰力量、指揮體制建置和作戰組織等予以高度重視。[26]如：對敵指揮控制中樞實施病毒攻擊，最有效的方法，即是通過各種電子手段，將病毒侵入敵方信息網路的接收處理系統，癱瘓指管中樞。故現代化戰場就須由「電子戰」與「網絡戰」來共同捍衛信息權的重任，使兩者相輔相成，互為對方提高作戰效益創造勝利要件，[27]達成戰場信息化之目的。

三、共軍「網電一體戰」特性探討

「網電一體戰」的核心為一體化作戰，其戰鬥效能之發揮，為建立信息交換正常運轉機制之上；而其一體性主要表現，則在於指揮、力量、目標和行動等方面之集注。所謂指揮上的一體化，乃是對「電子戰」和「網絡戰」實施籌畫、組織、協調和控制。而力量上的一體化，就是將「電子戰」和「網絡戰」諸般手段結合運用，並互為補充。目標上的一體化，即是使「電子戰」和「網絡戰」的作戰效能，同時應用於戰場C^4ISR系統關鍵與要害。再者，行動上的一體化，則是對「電子戰」和「網絡戰」作為能密切配合，形成合力。[28]

是以，「網電一體戰」是戰場電子信息目標網絡化的客觀需要，是促進「電子戰」和「網絡戰」融合互補，實現體系對抗的必然要求。針對共軍信息化作戰發展，凸顯其「網電一體戰」具有思想理論的超越性、戰爭目的的全局性、作戰手段的整體性、戰鬥效益的綜合性、攻防方式的針對性、作戰效能的抗擊性，戰場空間的拓展性等特性，[29]可說是為其打贏未來信息化戰爭的重要方略。

㈠思想理論的超越性

「網電一體戰」為高科技時代新思維，其著眼於「電子戰」和「網絡戰」兩種信息攻防手段融合，為實現指管即時化及管控全程化，須使戰場上各個作戰單元有效整合為一體，並藉「電子戰」和「網絡戰」的綜合運用，針對敵之信息傳遞管道與系統，先行以電磁攻擊方式破壞傳遞機制，再以資訊攻擊手段，癱瘓信息處理與運用，造成資源共享的困難性。從軍事理論發展的規律來看，戰爭實踐就是不斷催促作戰新的思維變革，綜觀「電子戰」和「網絡戰」這兩種主

24 馬亞西，〈資訊戰日新月異，網電一體戰橫空出世〉，《解放軍報》，2001年11月14日，版2。
25〈縱觀網路戰爭〉，《解放軍報》，2004年10月26日，版1。
26 梅軍、樊祥，〈未來網電一體戰〉，《解放軍報》，2000年9月6日，版7。
27〈縱觀網路戰爭〉，《解放軍報》，2004年10月26日，版1。
28 戴清民，《求道無形之境》（北京：解放軍出版，2009年1月第1刷），頁170。
29 戴清民，《戰爭新觀點》（北京：解放軍出版社，2008年5月第1刷），頁94-106。

要信息應用模式，對於節奏快速的戰場信息交換，能構成的有效威懾，自然成為共軍主宰敵對雙方網絡中心的首選之策。[30]

基此，「網電一體戰」其實是「一體化聯合作戰」之表現，為使有效對抗敵方指管作為，共軍自創全新的信息作戰構想，為其整體作戰模式帶來不小的衝擊與改變，使其更具體展現共軍在未來作戰的超越與發展。

㈡戰爭目的的全局性

在高科技時代，以計算機網絡為核心的作業系統，已成為國家經濟和軍事命脈，試想若信息交換網絡系統陷入癱瘓，國家安全即面臨重大威脅。同時，部隊因使用計算機網絡的依賴性愈來愈大，各種設備普遍連網傳遞資訊，形成了錯綜複雜的C^4ISR系統，並為現代軍隊作戰的神經中樞。而面對未來戰爭，掌握敵信息基礎和戰略命脈，攻擊C^4ISR系統、通信樞紐、金融中心及交通機構等重要目標，實施有效的網電一體作戰，將直接制約敵方的戰略運籌和決策。[31]

據此，在「網電一體戰」的支持下，未來信息化戰場所屬各作戰要素，可藉其掌握運用，削弱對方政治、軍事、經濟等多方面的綜合戰爭潛力，進而影響敵全面性的作戰效能。

㈢作戰手段的整體性

「電子戰」和「網絡戰」的共同作戰目標，在以削弱敵方並保護己方信息系統整體運作完整，也因為作戰目標的一致性，決定了「電子戰」和「網絡戰」行動，應在攻擊對象、作戰時機等方面取得一致的共識。鑑此，在實施電子進攻時，必須同步「電子戰」和「網絡戰」的計畫和組織行動，使之密切協調，形成整體，對同一目標進行綜合性攻擊；或於實施電子防禦時，將電磁和網絡防護納入同一的體系之中，整體籌畫，協調進行。[32]

㈣戰鬥效益的綜合性

「電子戰」和「網絡戰」手段的高度融合、相互增益，形成一個有機體，使得「網電一體戰」在作戰效益上，表現的更顯著綜合特性。就傳統作戰效益而言，僅針對包括敵方軍事、政治、經濟和社會上等較顯性機制；而「網電一體戰」則是將前述運行系統，賴以串聯的信息的管道為主要攻擊目標，斷其神經、癱瘓關節，可說是全面的隱性破壞，低能高效之最佳註解。[33]因此，其帶來的作戰效益，將遠大於任何傳統或單一的作戰型式。

㈤攻防方式的針對性

「網電一體戰」，它緊緊抓住未來信息化戰場特徵和信息作戰的特點，無論從力量構成、戰術技術及指揮控制等方面，將「電子戰」和「網絡戰」融為一體，使其分布在戰場上各個不同空間的電子信息系統設備，藉由計算機網絡的介接，形成一個完整的系統，產生一個巨大的結構效益，提高作戰系統的整體化與集成化程度，即時對敵信息傳送機制進行全維打擊。就其作戰目的則是要破壞敵方整體作戰網絡，對敵信息系統

30 戴清民，《戰爭新觀點》，前揭書，頁103-104。
31 戴清民，《求道無形之境》（北京：解放軍出版，2009年1月第1刷），頁170-171。
32 戴清民，《求道無形之境》，前揭書，頁171。
33 戴清民，《求道無形之境》，前揭書，頁171。

進行整體打擊。[34]

爰此，「網電一體戰」即是針對敵網絡中心的各作戰體系信息流實施攻防，破壞其信息獲取、傳遞、處理和截取所要資訊，達到擊敵要害與關節癱瘓之效果。

㈥作戰效能的抗擊性

「信息作戰」的實質效益，乃為破壞敵方指管通情系統，削弱其指揮控制能力，同時保護我方系統效能的正常發揮。而網絡技術在軍事領域得到廣泛運用，和戰場高度信息即時化為前提條件下，做為共軍未來信息作戰的主要表現形式。其著眼於對敵信息交換過程中，將「電子戰」和「網絡戰」諸般手段綜合運用，對網絡中心形成干擾，並綜合電磁（或截取）與信息兩個層次的綜合攻勢，從根本上破壞其基本架構與實施打擊。[35]

為此，當面臨敵方網絡中心的各作戰體系信息流時，用任何單一的作戰手段都很難將其全面癱瘓，而必須綜合運用多種手段，以網絡化的信息系統為作戰目標，實施系統對系統、體系對體系的整體對抗。

㈦戰場空間的拓展性

現代信息技術廣泛運用，各種信息網絡常被當成攻擊的首要目標時，電磁波和網絡可及之處，都可能存在信息作戰攻防行動，致使作戰範圍擴及整個信息領域。尤當「電子戰」和「網絡戰」的一體化運用，突破了原先僅能在武器射程的傳統侷限。因此，作戰空間將更加抽象和廣闊，全縱深一體化、非接觸性及非線性作戰等方式，將充斥在信息化戰場的整個作戰進程中，[36]使其比現有的任一作戰方式，都具有更廣大的空間。

參、共軍「網電一體戰」力量編成探討

現代軍事信息系統，隨著科技的進步，特別是計算機網絡技術的快速發展與廣泛應用，在縱向上多層次貫通，並延伸向主戰武器系統乃至單兵操作武器；在橫向上則互聯為一體化，將陸、海、空、天、電、心理戰場串聯成一個巨大的全維作戰網路。這種以信息攻防為平台中心的作戰模式，使得作戰體系產生結構性之變化，致深入影響軍隊指揮控制和武器系統，作戰目標通常也以指向敵方的指管通情系統為主。顯見，未來作戰已不是單一設備與力量之間的較量，而是交戰雙方作戰體系的對抗，[37]故無論是單一的「電子戰」或「網絡戰」手段，都將難以達成全般破壞敵作戰體系之目的。

再從戰場設備電子化及網絡化發展趨勢來看，無論從技術面或實用面，「電子戰」係隨著訊息裝備在戰場傳遞而產生，在不同類型與規模的戰役、戰鬥中，都發揮了重要作用；而「網絡戰」則起源於民間的駭客組織，而後被軍方運用於針對特定戰場範圍內計算機網絡的作戰活動。[38]據此，唯有在互

34 戴清民，《戰爭新觀點》（北京：解放軍出版社，2008年5月第1刷），頁104-105。
35 戴清民，《戰爭新觀點》，前揭書，頁105-106。
36 戴清民，《求道無形之境》，前揭書，頁171。
37 戴清民，《戰爭新觀點》，前揭書，頁100-101。
38 戴清民，《戰爭新觀點》，前揭書，頁101-102。

補互融前提下實施「網電一體戰」，從整體上與已成體系的信息系統進行對抗，使作戰目標將趨於一致，方能獲致加乘的攻擊效果。

一、共軍「網電一體戰」發展概況

共軍認為「網電一體戰」，係集中體現高技術戰爭本質特點，和規律的作戰方式，其演進與發展的歷史軌跡，其雛形始於1991年第一次波灣戰爭空襲作戰，美軍一方面利用侵入的電腦網路病毒，癱瘓伊軍防空系統，另一方面，則採用大功率的電子干擾，迫使伊拉克的指管系統無法工作；同時，攜帶反輻射導彈的AH-64武裝直升機，又一舉摧毀伊科邊境防空雷達，在伊軍防空網上打開缺口。[39]此舉開啟中共師法第一次波灣戰爭美軍對伊拉克所實施的資訊戰的概念。

1995年12月，共軍於石家莊陸軍學院召開「迎接世界軍事革命的挑戰」研討會，會中通過以資訊技術為核心的軍事革命浪潮，發展具「中國特色的資訊戰法」，總結出10種作戰方式，正式著手進行因應資訊作戰的工作，經過3年由下至上、由部隊至機關院校，逐級討論；[40]並於總參謀部第二部（人力情報、研究和分析）下設「科學技術蒐集局」，[41]翌年，共軍在「聯合九六」、「機動二號」、「中南九六」等聯合作戰演習中，都將電子戰納入演訓科目之中，[42]突顯出為因應未來戰場的複雜電磁環境，已將電子戰廣泛運用於年度重大演訓中。

1997年中共成立由國家主席親自領導的「國家信息安全工作領導小組」，召開全國信息化工作會議，藉整合軍、情、公安與信息產業等各相關部門，進行網路安全保障與網路攻防能力的整體建置，其中由總參擔任對敵方軍事與政治單位進行網路情蒐及攻擊，並組建信息民兵負責信息安全保障；[43]而國務院則遲至1998年方成立「信息產業部」，對全國各相關部門進行分工。1999年6月，總參總結科索沃戰爭經驗，北約為奪取資訊優勢，分別從高中低三個層次，採取綜合電子戰行動。然南聯在北約強大電磁壓制下仍另闢蹊徑，在全球發動對北約的網路攻擊，曾使美國白宮網站一整天無法工作，「尼米茲」號航母的指揮控制系統，竟也被迫停止運行3個多小時。[44]將原信息工程學院、測繪學院與電子技術學院整併組建為信息工程大學，[45]並將原資訊戰10種作戰方式精簡為6種。[46]藉鑑小國面對優勢軍事強國實施電

39 馬亞西，〈資訊戰日新月異，網電一體戰橫空出世〉（北京：解放軍報，2001年11月14日），版2。
40 廖文中，〈中國網軍：國安、公安與解放軍〉，《全球防衛雜誌》，271期，2007年3月出版，頁73-74。
41 David Shambaugh原著，高一中譯，《現代化中共軍力：進展、問題與前景》（臺北：國防部史政編譯室，2004年4月版），頁194-195。
42 李文忠、張國城、陳文政、陳宗逸、蘇紫雲，〈民間版「國防白皮書」〉，《臺灣新社會智庫網》，http://www.taiwansig.tw/index.php?option=com_content&task=view&id=1383&Itemid=117
43 李文忠、張國城、陳文政、陳宗逸、蘇紫雲，〈民間版「國防白皮書」〉，前引文。
44〈電子戰的未來與新特點〉，《中國戰略網》，http://str.chinaiiss.com/html/20104/12/ wa2d84.html
45〈中國人民解放軍信息工程大學〉，《維基百科網》，http://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%E4% BF%A1%E6%81% AF%E5%B7%A5%E7%A8%8B%E5%A4%A7%E5%AD%A6
46 廖文中，〈中國網軍：國安、公安與解放軍〉，《全球防衛雜誌》，2007年3月第271期，頁74。

磁作戰時，亦能憑其有限之資訊戰力遂行反制作為。

2000年起，共軍積極推動軍事自動化指揮環境的構建，將情報蒐集、資訊傳遞、定位導航、精確打擊、海洋監視、戰場控制及作戰指揮等能力進行提升與整合。繼之，2002年，由時任共軍總參四部部長戴清民少將規劃全國性國家戰略級的資訊戰分工確定，明定共軍階層僅負責「電子戰」和「網絡戰」—即「網電一體戰」，並由總參四部負責規劃成軍，完成全軍指揮自動化網路，使其具備聯合作戰所需指揮與通信能力；而負責網路安全、心理戰、情報戰等防禦性作為，另有不同部門分主其事。[47]經多年努力，如其引以為傲的「華東電戰網」為例，係整合共軍各軍種在浙閩境內的電子對抗部隊，專司對臺灣方面電子作戰，於2007年優先完成東南沿海一帶的區域綜合電子信息系統，藉以有效整合戰區內指揮管制、情報偵蒐、預警偵察、通信與電子作戰等系統，建構完成其所謂「三級聯戰體制」（中央軍委—地方作戰集團—實際參戰部隊），[48]藉此提升部隊戰時應變能力，進而奪取電子戰場的主控權。

二、共軍執行「網電一體戰」能力分析

據2008年美國情報機構報告：「中共正在把軍事力量從傳統的陸海空戰場擴展到太空和網絡空間，並已組建自己的駭客精英部隊—信息戰部隊，用以發動網絡攻擊，目的是研製用來侵入敵軍電腦系統和網絡的病毒，制定用以保護友軍電腦系統和網絡的戰術與措施」。[49]另2009年4月，美智庫「國家亞洲研究局」和陸軍戰院的戰略研究所聯合出版《Beyond the Strait: PLA Missions other than Taiwan》專書，其中一篇題為〈PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability〉研究報告，[50]乃針對共軍發展「網電一體戰」的能力虛實，提出深入剖析。

咸信，目前共軍可運用的「網電一體戰」工具包括：駭客、電腦程式病毒、硬體設備破壞、內部滲透攻擊，以及電磁脈衝攻擊等。至於執行任務的平台則包括：電腦、全球網路連線，以及具操作能力的作戰人員。對於軍事科學院及國防大學而言，其當前的重要任務之一，就是要訓練出能夠成功執行任務的「網電一體戰」軍官。而其執行「網電一體戰」任務的主要機構包括：[51]

㈠總參三部通信局負責國防信息化保障任務並執行戰場網路情報蒐集。

㈡總參四部電子雷達對抗部負責電腦網路運作及電子反制能量的組建。

47 廖文中，〈洞察中共使用網軍遂行心理戰之影響〉，《青年日報》，2007年4月13日，版7。

48 李文忠、張國城、陳文政、陳宗逸、蘇紫雲，〈民間版「國防白皮書」〉，《臺灣新社會智庫網》，前引文。

49 錢程燦，《中國應警惕美國吹捧，克服弱點強化網絡戰力》，《東方網》，http://www. chinareviewnews.com 20080317

50〈共軍發展「網電一體戰」的虛實〉，《大陸情勢雙週報1561期》，http://www.kmt. org.tw/hc.aspx?id=44&aid=3636

51 曾復生，〈臺北—北京—華府軍事動態平衡虛實〉，《國政研究報告》，國安（研）099-003號，April 2, 2010, http://www.npf.org.tw/post/2/7240

㈢在七大軍區設置戰區聯合作戰指揮部，並成立信息對抗中心，負責電子對抗及網絡信息體系的防護。

㈣軍事科學院及國防大學則是負責研發各項「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軍官和士兵。

再者，其發展「網電一體戰」的作戰能量，主要項目則包括：[52]

㈠透過電腦網路攻擊來完成長距離的攻擊破壞任務；

㈡運用電腦網路攻擊癱瘓對手的重要經濟活動能力，達到警告嚇阻的效果；

㈢運用電腦網路瓦解美軍C^4ISR系統；

㈣運用電腦網路攻擊，發揮「先發制人」的戰略威懾效果；

㈤結合電腦網路和電子戰特種部隊的奇襲能量，達到心理威懾的戰略目標，並迫使臺灣接受政治談判的條件；

㈥運用電腦網路攻擊破壞美軍的後勤補給系統；

㈦運用電腦網路攻擊癱瘓臺灣的電力運輸和通訊系統等。

綜整前述可知，共軍積極發展「網電一體戰」能量，不再強調大規模殺傷進而重視體系癱瘓、交戰的模式由接觸轉向非接觸作戰、行動模式從線性向非線性轉變、兵力組成由規模組合轉為效能融合、作戰指揮從預先計畫變成同步指揮。[53]這種作戰方式，基本上是貫徹「巧戰而屈人之兵」的思想，以「非對稱性戰略」創造有利的戰略態勢，減少附帶傷亡的數量，並迫使對手快速進入政治談判階段，接受其所提出的條件。

三、共軍「網電一體戰」作戰方式

共軍戰略規劃圈的主流意見認為，應積極發展「電腦網絡作戰」能力，並建立「非對稱性戰略優勢」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「網絡對抗」為主要的作戰形式（如圖1）。此外，透過整體的「電腦網路作戰」能量，隱藏在非官方的民間公司組織中，並藉由電腦網路的連結，可以在世界上各個角落，直接或間接地對攻擊目標，進行「網路戰」而不容易被察覺。[54]這種「巧戰而屈人之兵」的作戰型態，儼然已對我政軍重要機構之電腦網路系統，造成相當程度的威脅。

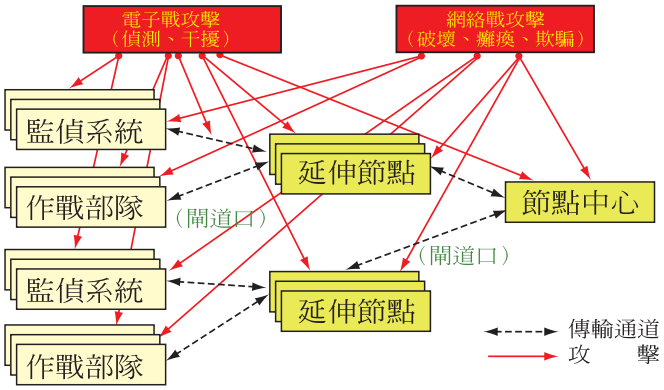

圖1　共軍「網電一體戰」示意圖

資料來源：本圖依雷怡妮少校指導調繪。

52〈國民黨雙週報：大陸發展「網電一體戰」的虛實〉，《中國評論新聞網》，http://www.chinareviewnews.com

53 社論，〈美網路風暴演習凸顯建構資安環境重要性〉，《青年日報》，2010年10月4日，版2。

54 曾復生，〈臺北—北京—華府軍事動態平衡虛實〉，《國政研究報告》，國安（研）099-003號，April 2, 2010, http://www.npf.org.tw/post/2/7240

㈠網電一體化偵察

網電一體化偵察，為利用計算機網絡設備、各種電子技術設備，截獲、探測、分析、識別敵網絡系統、電子系統技術性能和情報，而進行的偵察行動。主要包括網電一體化技術偵察和情報偵察兩種。其中網電一體化技術偵察，主在對各種輻射源設備（雷達）、網絡系統結構、伺服器及無線裝備等設施進行的特性偵察；而網電一體化情報偵察，則是對敵各種電子發射源信號，和網絡系統所載的情報信息進行參數的偵察行動，如截獲敵電報內容、下載敵方情報資料等，[55]顯見網電一體化偵察，除為「網電一體戰」的基礎和前提外，並可結合其他聯合作戰行動。

共軍鑑於網電一體化偵察，在超視距、高速度、多變化的數字化戰場上，具有超限探測、快速獲取信息、偵察行動隱蔽、受戰場環境影響小等傳統偵察手段無法比擬的優點，能即時並準確地探測、蒐集、分析和傳遞情報；反之，若無法實施網電一體化偵察，則攻擊開始即失去制敵機先優勢，網電一體化防禦亦失去支撐，難以為聯合作戰開創有利態勢。[56]為此，共軍正積極運用偵察衛星、作戰機艦、戰甲車、場站等網電偵察載（平）台，運用網電一體化偵察觸角，延伸向更廣泛的領域，以期在任何時間點上，將戰場上所有的信息透明地呈現出來，為聯合決策提供較可靠的依據。

㈡網電一體化攻擊

網電一體化攻擊，即是利用計算機網絡和電子戰系統，在極短時間內發動從戰略到戰術層級的全面攻擊，對敵指管通情作業系統，所進行的一體化攻擊，為奪取網絡權和制電磁權的主要作戰行動之一。是以，當信息化聯合作戰的重點目標，已由消滅敵有生力量為主，轉變成破壞聯合指管通情機制，和武器系統為主的電子設備；而網電一體化攻擊，則是破壞敵網絡化系統、機械化作戰平台及信息化武器系統之有效手段選項（如圖2）。[57]研判共軍汲取美軍在波灣及科

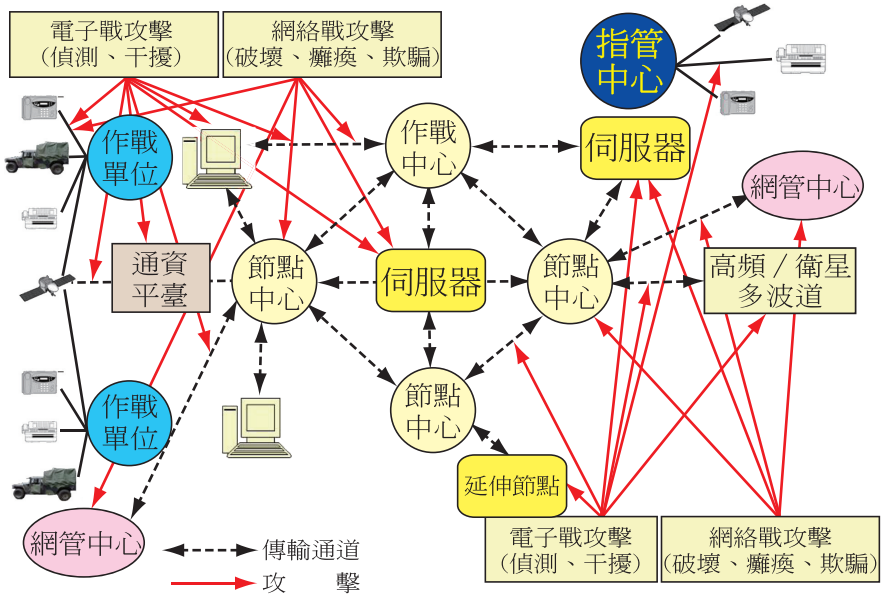

圖2　共軍網電一體化攻擊示意圖

資料來源：本圖依吳建忠少校指導調繪。

55 曹正榮、吳潤波、孫建軍主編，《信息化聯合作戰》（北京：解放軍出版，2008年8月第2刷），頁116-117。
56 曹正榮、吳潤波、孫建軍主編，《信息化聯合作戰》，前揭書，頁116-118。
57 曹正榮、吳潤波、孫建軍主編，《信息化聯合作戰》，前揭書，頁119-120。

索沃作戰經驗，採取網電一體化攻擊主要手段有：[58]

1.無線啟動網路病毒，癱敵C^4I系統

通過各種手段，先期將電腦病毒植入敵C^4I系統，於戰時依其所需，採遠端遙控方式啟動病毒，癱瘓敵指管系統。如：1991年的波灣戰爭，美軍在戰略空襲直前，即啟動於戰前植入伊拉克指管系統的列表機病毒，造成伊國防空指揮中心電腦系統當機，癱瘓整個防空體系中的預警和C^4I系統。

2.無線注入網路炸彈，毀敵飛行武器

共軍面對敵方隱形戰機、巡航導彈、武裝直升機等，進入其電子設備有效影響空域時，渠等可用無線電注入，並引爆各種電腦網路炸彈方式，迫使敵方的武器系統失去控制、迷失方向、自動墜毀。

3.無線修改網路指令，使敵失去控制

無論是美、俄、歐盟等強國，若無全球衛星定位系統的支援，則無法精密掌控打擊和準確定位優勢。雖然干擾和破壞敵方全球衛星定位系統，為一非常困難之工程，但採用對衛星定位系統接收機干擾，和對傳輸信號管道的壓制或欺騙干擾方式，也未嘗不是阻敵之好方法。因為，當系統受到干擾後，用來制導的巡航飛彈就有可能偏離航向軌道，甚至會錯飛至干擾指定的地域。對此，共軍可以通過無線電磁進入網路系統，用指令篡改的方法達到此一目的。

㈢網電一體化防護

網電一體化防護，乃利用計算機網絡和電子戰系統，採取綜合的各種防禦措施，保證己方網路、電子裝備和系統正常運作，使網電一體化防護變得極為複雜，遠遠高於傳統意義上的防禦作戰行動。據此，在數位化戰場中，只要任何電磁輻射源、探測傳輸系統，與無線裝備系統，都可能遭敵偵察定位，或面臨敵精確制導武器和常規火力打擊的狙擊目標。同時，先進的信息技術，使得網絡化聯合指揮和作戰系統的效能得到空前的提高，但正因如此，也使其信息在開放空間的傳遞下洩露無遺，若無法有效運用加密保護技術，將可能導致暴露作戰企圖，甚至引來敵火打擊。研判其網電一體化防護手段如后：[59]

1.注重網電電磁遮罩，防敵偵察監視

電子和網路設備，在工作時都會發出電磁訊號，一旦被敵人偵收截獲，易遭攻擊。如敲擊電腦鍵盤時發出的電磁波，可遠在1,000公尺以外接收下來並還原信號。據此，在設計和使用無線電時，應盡可能減少微波輻射曝露在無安全防護空間的機會；並選用加固的元器件或密譯技術，並減少裸露的電纜與各種連線，將重要部件裝入金屬閉封盒內或保密器，使電路入、出口成為一個遮罩，微波無隙可乘。

2.實施電磁佯動偽裝，防敵精確打擊

選擇在海上、河流、空中漂浮，或動物身上捆綁電磁波輻射源，定時定點施放電磁波輻射源等方式，使敵人難辨真假，產生錯誤跟蹤。並可通過上述途徑，使用角反射器和金屬箔條等方法，進行無源干擾，誘敵錯誤打擊，並使消耗其導彈、暴露目標。

3.採取網電跳頻工作，防敵電子鎖定

在各種電子武器頻譜波段運用中，

58 任久華，〈網電一體戰—未來作戰新樣式〉《國防科技》，2002年3月期，頁61。
59 曹正榮、吳潤波、孫建軍主編，《信息化聯合作戰》，前揭書，頁120-122。

與之相連結的有網路、通信、雷達、光電、武器控制與制導系統等。各種干擾與反干擾，均圍繞著時間、空間、頻率、調變樣式，網路結構等進行對抗。在執行指揮、偵察監視過程中，可採不定時改變資訊傳輸路由，和不斷轉換發射頻率的間斷工作方式，防敵電子偵蒐干擾，從而得到保護我方指管系統的目的。

肆、我應有認知與作為

2009年9月15日，美軍太平洋總部司令基亭指出，隨著中共經濟實力的成長，其軍事能力也將會同步強化，尤其是在反衛星武器、雷射武器，以及執行「非對稱性戰略嚇阻」的「網電一體戰」能力等，都會對美軍的安全構成挑戰。同年9月28日，美國防部亞太安全事務助理部長葛雷森柏表示，中華民國未來的國防應尋求「非對稱性優勢」，一方面可因應考量臺灣國防支出的比例，另一方面也可嚇阻中共，讓共軍必須付出比臺灣更昂貴的代價，才能取勝。[60]

面對中共無時不在進行的網電作為，及近年政府與軍方資安事件頻傳，大多因個人的無知、好奇、僥倖心理及疏失，為敵方開闢了攻擊管道。鑑此，面對共軍「網電一體戰」戰力尚未成熟，在初步驗證階段，我建置網路戰攻防能力時，應將軍、公、民營機構一體併同考量，以形成一個周全的防護網，此外更應明確責任分工，強化資訊安全教育，建構立體化的信息安全屏障，[61]確保我國資訊傳遞安全，實是值得努力的方向。

一、明確責任分工

資訊與通訊為國家與軍隊的神經系統。在國家層次，資通能力不僅攸關政府工作運作正常之基礎，更是社會各系統、機制交換的重要媒介，為民生活動所必需。以軍事層面來講，現代化作戰行動高度依賴資通系統，優勢的資通能力，可使不對稱的戰力效果倍增。因此，面對數量居於優勢的共軍，國軍資通能力的強化，應是平時維持臺海戰力均勢、發揮以寡擊眾的關鍵之一。是以，在建立國家資通防護能力與反制能量方面上：

㈠在組織上，我國最高負責網路安全的是行政院「國家資通安全會報」，主要負責「強化政府資通安全防護能量、防衛國家資通設施、建立資通安全預警機制、主動偵防降低實質危害因素、推動資通安全技術研發、提升執法機關偵防能力」等。[62]鑑此，國安會應儘速訂定國家資通安全戰略；行政院則應明確並提高資通安全專責單位權責，政府各部門與國軍各單位應嚴守資安紀律、強化網路安全，各重點設施更應建立多重備援系統，加大抗毀性及延長存活時間。[63]

㈡國防部應以「資電優先」為重點，厚植資電攻防設備與專才，部本部宜成立資電

60 曾復生，〈臺北—北京—華府軍事動態平衡虛實〉，《國政研究報告》，國安（研）099-003號，April 2, 2010, http://www.npf.org.tw/post/2/7240

61 楊太源，〈淺析中共網軍的「攻」與「防」〉，《青年日報》，2009年1月7日，版7。

62 鄭大誠，〈中共網軍的發展與評估〉，http://tw.myblog.yahoo.com/jw!0RhCSD.LHwIcZmpXnmtWD_6tdQ—/article?mid=319&prev=320&next=308&page=1&sc=1

63 李文忠、張國城、陳文政、陳宗逸、蘇紫雲，〈民間版「國防白皮書」〉，《臺灣新社會智庫網》，前引文。

司，以銜接國家整體資通安全建設與防護作為，且鑑於資電建軍用兵多具有跨越各軍兵種之特性，宜於參謀本部增設資電專責上將副總長，並由直屬參謀本部之資電作戰指揮部，[64]與國安會及行政院各部會，定期或不定期召開協調會，以收實效。

二、強化資通戰力

我國為中共信息戰作為的首要目標，國內各重要政軍單位乃至民間機構，均受其日以繼夜、毫無間斷的網路攻擊。對資訊、通信的威脅除了針對破壞設施實體的「硬殺」外，也有癱瘓、干擾、減效、混淆機制效能的「軟殺」。對此，在「科技先導、資電優勢」指導下，以資通安全能力做為重要之戰略資產，自當成為敵方所欲率先打擊的目標。是以，資通防護應以強化抗毀性，及建立一定反制能量，兩者相互為用；另資通產業為我國科技產業強項，建置適當的先制能量實有必要，而「信息確保」則為國軍防衛固守之核心任務之一。[65]

另據《大紀元報》分析，中共在網路戰方面仍存在致命漏洞，其最大的問題就是沒有自己的電腦操作系統，和硬體製造技術，致現在使用的操作系統和硬體核心技術，都掌握在外國外廠商手上，一旦在售賣前留下「後門」，就可能失去控制權。[66]據此，以共軍依賴資電裝備日深，我可轉換資通能力為強項「資產」，使其成為「武器」，不僅可以增強傳統戰具的戰鬥效能，更可以師敵之長，藉「軟殺」之反制手段，減耗共軍對我打擊之動能。[67]

三、落實隔離政策

我國為世界最大的電腦零組件製造地之一，網路化程度及技術居亞洲領先地位，因此，對於共軍的入侵，並不會一味處於挨打的局面。[68]但攻擊漏洞奪取先機，乃共軍具操作網電作戰人員入門功，為避免其遊弋於網上伺機下手目標，我應採積極防護作為，主動偵蒐敵方作為，並強化操作及管理者技能。

另因應網路資訊戰的新威脅，在國家層級，應加強與美軍「網路戰司令部」結盟合作，發揮國軍在網路資訊戰中的專長與優勢，強化臺美軍事合作的能量與價值。[69]在政府部會層級，須鞏固政府機關電腦防護作為，每一部公務電腦除具作業功能外，餘光碟機、燒錄機、軟碟機、資訊儲存媒體(USB)等，藉有效監控管制，維護作業環境之純淨。重要軍政中心、民生設施等，均應設立虛擬主機及異地建立備援系統，避免公務電腦遭受攻擊而危害系統運作，並能即時接替癱瘓系統運作。

64 同註63。

65 同註63。

66〈揭祕中共網路戰之致命漏洞〉，臺北：大紀元報，2008年3月19日，版5。

67 李文忠、張國城、陳文政、陳宗逸、蘇紫雲，〈民間版「國防白皮書」〉，《臺灣新社會智庫網》，前引文。

68 鄭大誠，〈中共網軍的發展與評估〉，前引文。

69 2009年6月23日，美國國防部長蓋茲下令組建美軍的網路戰司令部，以因應來自共軍及俄軍的網路作戰威脅。請參見：曾復生，〈臺北—北京—華府軍事動態平衡虛實〉，《國政研究報告》，國安（研）099-003號，April 2, 2010, http://www.npf.org.tw/post/2/7240

四、強化電磁防護

「信息作戰」主由作戰保密、軍事欺騙、心理戰、電子戰、電腦網路戰、實體摧毀等六大要素構成，其在本質上都是對信息系統的削弱和破壞，其中，作戰保密、軍事欺騙、心理戰自古以來一直運用於戰爭活動之中；另實體摧毀則是通過包括電子戰在內的多種手段綜合運用，來達成其作戰目的。[70]如運用電磁脈衝的硬殺手段，可瞬間造成敵供電和通信系統短路，毀損正在工作的電子元件；亦可運用駭客等軟殺手段，發送病毒或垃圾郵件阻塞；或運用電磁設備發射輻射信號，進行電子干擾等。

基於「電磁脈衝」乃是未來爭奪制電磁權的殺手武器，政府機關應強化電磁防護觀念，指揮中心應具備抗電磁作為，如電子設備須安裝接地線、錫鉑包裹元件、鉛防護罩。庫存備用品，應先完成產品放電等消極防護作為，方可避免敵以電磁癱瘓我系統之目的。另對其可能採取之竊密作為，實體隔離為現階段資訊安全之最低標準，政府機關與軍方除應落實執行封閉型區域網，嚴禁軍網、公務網、行政網、網際網路等混用情形，肇生洩密事件；另可普設謀略網站，其來可達欺敵誤敵效果，並可藉機查明其進出路徑，及伺機回擊敵方網軍。[71]

伍、結　　語

或許，傳統戰爭或非軍事衝突，通常會引發國際法和地緣政治的脈動，因此相關國家莫不維持相當的自制，但電子頻譜與網絡上的煙硝，卻常常逾越當下國際規範。面對現今發達的網際網路世界，連結的國家已多達233個，用戶數更高達12億人口，這正是「電子戰」與「網絡戰」的潛伏危機所在。[72]再對照美國防部自2008年公布《中共軍力報告》，中共為提升網路戰戰力，已推出「網電一體戰」的作戰理論，並強化其軍事和民用網路的攻擊能力，其正是共軍刻正發展非對稱作戰中「非接觸作戰」與「一體化聯合作戰」的重要戰法。

以美軍於波灣與科索沃作戰尚存不久的「實戰經驗」來看，凸顯「電子戰」與「網絡戰」不再只是存在於科幻小說，或是未來發展的預期，而是當下的真實戰爭的現在進行式。基於此一認知，如何有效適應共軍「網電一體戰」，確保國軍戰力、維護國家安全，正是未來建軍備戰必須納入考量的重大因素。

收件：99年11月12日
修正：99年11月28日
接受：99年12月01日

作者簡介

劉宜友上校，陸軍官校74年班、陸軍學院84年班、戰研班85年班、師範大學政研所國家事務與管理碩士班；現任職於國防大學陸軍指揮學院情報組主任教官。

70 張建昌，《走進信息化戰爭》（北京：國防大學出版，2003年3月第1刷），頁57。
71 楊太源，〈淺析中共網軍的「攻」與「防」〉，《青年日報》，2009年1月7日，版7。
72 社論，〈強化網路資訊攻防戰力　防範駭客入侵竊密〉，《青年日報》，2008年4月1日，版2。