中共網路戰威脅我應有之戰略思維

陸軍上校　王佩陸

提　要

自二次大戰結束，軍事安全的維護成為國家安全的首要目標，隨著後冷戰時代的來臨，國家安全的範圍擴大了。除了傳統的國防問題外，舉凡環保、走私、販毒、族群衝突、恐怖活動等非傳統因素，及因全球化與社會資訊化所形成相互依賴的關係，對國家安全均產生連鎖影響。尤其透過資訊網路所散播電腦病毒、駭客或是國家關鍵基礎設施等攻擊，更是讓國家的安全無法區分平時與戰時，或是前方或後方，而透過此侵襲更會在心理上造成更劇烈的震撼與恐怖，直接影響國家安全。[1]

現今無論是軍事、金融、交通管理、電力調度乃至國家行政體系，都相當依賴資訊系統來進行作業處理與訊息管理。因此，資訊、網路系統與設施已經成為關鍵性的基礎設施之一。目前全世界各地每天都在發生資訊系統遭到入侵或破壞的案例。我國的資訊安全，除了一般商業性、駭客型玩家、犯罪性的資通攻擊之外，關鍵性的基礎設施的安全更面臨網路攻擊的嚴重安全性挑戰，現在，這種攻擊無日無之，已是我國國家安全的重大威脅。[2]

關鍵詞：駭客、網路攻擊、網路戰

前　　言

資訊時代來臨使得電子、電腦、通訊技術突飛猛進，網際網路突破了疆域之限制，電腦使用者可以瞬間取得世界各地的資訊。在通信、資訊科技創造出便捷的新生活，節省了許多繁瑣事務的同時，人們不知不覺地加深對通信與資訊產品與設備的依賴。各國國家安全的決策者，無不費盡心力藉由蒐集、處理、分析及運用資訊優勢，提升各層面的效率，資訊安全亦為國家安全中重要的一環，網路戰已漸漸成為國防計畫與情報作業中不可或缺的考量因素。

人類戰爭的型式與規模取決於文明的進步，遠古時期以石頭、棍棒即可解決一場紛爭，在歷經農業、工業社會武器系統不斷

1 翁明賢，《突圍－國家安全的新視野》(臺北：時英出版社，2001年11月)，頁40。
2 2006國家安全報告(2008修訂版)，國家安全會議，2008年3月26日。

更新與改良後，使得戰場變得更多樣化。艾文・托佛勒等所著的新戰爭論(War and Anti-War)，[3]作者認為未來資訊文明會把第二波的工業社會轉變成第三波以資訊科技為基礎的社會，在這個社會中，經濟的命脈就是資訊、電子、電腦、通訊以及媒體化趨勢。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，資訊科技與資訊安全自然對國家安全是益形重要。[4]

資訊時代的戰爭，由於數位化的通訊系統，作為作戰力量的「倍增器」，不僅造成戰場的「易毀性」，也相對增加戰爭的「不確定性」因素。網路戰在作戰中扮演著重要的角色，為戰爭勝負的關鍵。美國《華盛頓郵報》曾刊登文章，披露20餘年前中央情報局把病毒裝進軟體售給蘇聯，導致西伯利亞一條天然氣管道大爆炸，對當時蘇聯的經濟造成嚴重損害，這是一個十分重要的警示，如果資訊被控制，則所有安全都將受到威脅而受制於人。

網路戰的探討

資訊化社會對國家整體資源安全的威脅，改變了國家賴以生存的安全基礎，對社會、經濟、政治和軍事產生了重大的影響。作為國家安全的一個重要因素，資訊優勢與其他安全要素之間的聯繫更為緊密，由此提升為直接影響國家政治穩定、社會安定、經濟發展的全域性戰略地位。圍繞著資訊主權、資訊資源的維護等一系列「網路」優勢問題，成為資訊時代國家(防)戰略領域中的重大課題。

一、網路戰的定義

人類社會的發展過程歷經三個階段，第一階段是農耕社會型態，第二階段是工業社會型態，第三階段是後工業或是「資訊」時代，也就是現在的先進發展國家的社會型態。[5]美軍對資訊作戰(Information Operation，IO)定義為：運用電子戰、網路戰、心理戰、計畫安全(保密)、心理戰等資訊作戰核心任務與次要任務，對敵資訊及資訊系統產生具體影響力，並防護我軍資訊，進而影響敵決策(Decisionmaking)機制之運作；[6]另新版暫定的資訊戰準則，不同過往定義聚焦於資訊戰「範疇」，改將重點置於資訊戰的作為。提出「資訊戰係聯合軍事作戰各階段期間於資訊環境中發揮戰力的計畫與整體作為」。[7]

國軍軍語辭典所下的定義分為廣義之「運用各種手段影響敵方並防禦我方決策程

3 艾文・托佛勒等著，《新戰爭論》，(臺北：時報文化，1994)，頁2-23。
4 張欣，《資訊革命與國際關係－論信息安全在國家安全中的戰略地位》，(北京：時事出版社，2002年7月)，頁 339-357
5 Alvin Toffler著，黃明堅譯，《第三波》，(北京：時報出版社，1994年6月20日)，頁25。
6 FM 3-13，資訊作戰第一篇資訊作戰概論，P1-13， 2006年2月，DOA 。
7 Hans F. Palaoro，黃淑芬譯，〈資訊戰略：失落的環節〉，《國防譯粹》，第38卷第一期，100年1月，頁80。

序與資訊系統之行動，以創造資訊優勢。」以及狹義之「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。」[8]

目前中共文獻中，對信息戰定義較常引用的解釋為沈偉光:「信息戰是現代戰爭本質特徵之一，廣義指對壘的軍事(也包括政治、經濟、科技及社會一切領域)集團搶佔信息空間爭奪信息資源的戰爭；狹義指戰爭中交戰雙方在信息領域的對抗」。[9]而中共「信息作戰學」對於電腦網路戰之定義亦有廣義與狹義之分，廣義之電腦網路戰是指國家、民族、武裝集團甚至恐怖分子利用(運用)網路技術和手段為爭奪網路優勢或破壞資訊網路而進行的鬥爭。這些活動可以用於軍事、政治[10]、經濟[11]等一切領域，活動的主體可以是團體也可以是個人，既可以在戰時實施，也可以在平時實施破壞程度可大可小。[12]狹義網路戰是指敵對雙方在電腦網路領域為爭奪制網路權透過削弱、破壞敵方電腦網路系統的資訊和使用效能，保障已方電腦網路系統的資訊和安全運行而展開的資訊作戰行動。

這個定義表明，資訊網路戰屬於資訊作戰範疇，其作戰的目的在奪取制網路權，作戰的對象是敵方的電腦網路和資訊，作戰主體是運用資訊技術和裝備武裝起來的網路戰士，作戰區域是廣濶的電腦網路空間，作戰手段是根據電腦技術研製的各種病毒，邏輯炸彈和芯片武器等，致勝途徑是透過削弱、破壞敵方電腦網路系統的資訊和使用效能，以及保障已方電腦網路系統的資訊和安全運行達成電腦網路的作戰目的，這是電腦網路戰區別於其他作戰模式的根本標誌。故網路戰乃屬資訊戰[13]概念底下的一種攻防型態。[14]網路戰將發展成一種投入最少，影響範圍最大的重要作戰模式。[15]

8 國軍軍語辭典(九十二年修訂版)，國防部，2004年3月15日。

9 沈偉光，《信息戰》，(浙江：浙江大學出版社，2000 年10 月)，頁9。

10 中國駭客被控意圖滲透印度最敏感的政府部門，印度國家安全顧問納拉亞南告訴英國泰晤士報說，中國駭客於去年十二月十五日試圖入侵印度國安與其他政府單位，他說：「這不是第一次圖謀攻擊我方電腦。」。〈印度指控中國駭客攻擊〉，《自由電子報》，2010年01月19日，網址：http://www.libertytimes.com.tw/2010/new/jan/19/today-int8.htm，檢索日期103年04月28日。

11 電腦防毒公司邁卡菲(McAfee Inc.)2011年2月10日公布報告說，從中國境內作業的駭客闖進五家跨國石油及天然氣公司的電腦系統，竊取競標計畫及其他機密資訊。電腦安全專家表示，中國是網路犯罪的主要中心，包括針對大公司的工業間諜活動。他們指出，過去的網路攻擊顯示駭客手法高強，暗示身為「網路戰」先鋒的中國軍方及其他政府機構可能設法竊取科技和商業機密，藉以幫助中國國營企業。〈中國駭客竊取跨國能源公司機密〉，《聯合晚報》，2011年02月11日，網址：http://udn.com/news/WORLD/WOR2/6146142.shtml，檢索日期103年04月28日。

12 徐小岩主編，《信息作戰學》，(北京：解放軍，2002年6月)，頁158。

13 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。網絡中心戰是機械化戰爭形態向資訊化戰爭形態過渡的產物，是因為資訊網路的發展為工業時代機械化部隊注入活力而帶來作戰形態的更新。因此，無論是資訊戰還是網路戰和網絡中心戰，都離不開資訊技術的迅速發展，也離不開網路技術的應用與普及。錢逢水，〈解讀資訊戰、網路戰、網絡中心戰〉，《中國網》，2004 年7 月22日，網址：http://big5.china.com.cn/chinese/junshi/616534.htm，檢索日期103年04月18日。

中共認為「網路戰」，是指以電腦病毒攻擊、硬件摧毀等手段，對對方資訊網路系統進行干擾、破壞、摧毀或控制，並以此影響、破壞其以信息網路為基礎的軍事系統及國家信息基礎設施，同時保護己方以資訊網路為基礎的軍事系統及國家資訊基礎設施不受敵方類似行動影響的作戰行動。[16]本質上，網路戰是資訊戰的特殊形式，乃在網路空間進行一系列的襲擾、竄改、竊取、監視與破壞的作戰行動。[17]與傳統戰爭相比，網路戰具有作戰空間的無限性、作戰力量的廣泛性、作戰手段的知識性、作戰時間的連續性、作戰過程的突變性、作戰效率的高效性之特徵。[18]

資訊作戰應充分運用一切軍民資源，結合軟硬體手段並講求欺敵作為，對敵之資訊系統心理士氣、與各種實體設施，發起全面性之攻擊，作戰全程確保我方資訊系統軟、硬體設施，以掌握戰場主動爭取先制，其運用方式包含資訊嚇阻、資訊制壓、資訊遮斷、資訊摧毀、資訊封鎖、資訊欺騙等。而網路戰之運用特性亦等同之。[19]歸納如後：

(一)以奪取和控制網路權為首要目的

這是網路戰區別於其他作戰模式的重要差異。[20]由於在未來作戰中，電腦網路將各級指揮控制機構與作戰部隊甚至單兵，有組織地形成一個整體，如果在作戰中保持了制網路權，就意味著擁有強大的戰鬥力，如果喪失了制網路權即使己方人員完好無損，也是一盤散沙，如同一個孤島，無法形成一股戰鬥力。因此，電腦網路為軍事資訊系統的大腦和神經中樞，交戰雙方在爭奪制資訊權的過程中，必將其作為首先打擊的重點目標，亦即網路作戰的目的是奪取和控制制網路權。

(二)作戰力量的構成是軍民一體

相對於其他作戰模式，網路戰的參戰力量是軍民一體、軍政一體、亦軍亦民。由於資訊技術大量運用於軍隊又大量運用於民間。軍隊與民間的資訊化程度都在不斷的提升，而兩者的技術和手段都具有通用性。因此，網路戰參戰力量的軍民界線日益模糊，有些駭客或電腦高手在網路上發起攻擊的能力不比軍事資訊專家遜色；攻擊的目標很多屬於民生設施或與民用網路連接。從戰略上而言，網路戰已很難劃定邊界，短兵相接、

14 李承禹，〈中共網路作戰之戰略邏輯分析：網路戰與網路中心戰的區隔與應用〉，《復興崗學報》，第90期，2007年，頁252。
15 徐小岩主編，《信息作戰學》，(北京：解放軍，2002年6月)，頁158。
16 呂登明，《信息化戰爭與信息化軍隊》，(北京：解放軍，2004年8月)，頁217-218。
17 李承禹，〈中共網路作戰之戰略邏輯分析：網路戰與網路中心戰的區隔與應用〉，《復興崗學報》，第90期，2007年，頁252。
18 呂登明，《信息化戰爭與信息化軍隊》，(北京：解放軍，2004年8月)，頁242-244。
19 徐小岩主編，《信息作戰學》，(北京：解放軍，2002年6月)，頁161-164。
20 信息作戰樣式按內容可分為情報戰、電子戰、心理戰、計算機網路戰和信息設施摧毀戰。徐小岩主編，《信息作戰學》，(北京：解放軍，2002年6月)，頁137。

炮火連天的激烈戰爭場面將難以再現。

(三)作戰手段具有高技術性和多元性

資訊技術和電腦網路的軍民兼容性和一體性，決定了電腦網路可以透過多種途徑、各種手段實施。既可以利用駭客透過網路實施，又可以利用電磁干擾手段實施，還可以利用病毒實施；既可以利用傳統兵、火力進行，又可以使用現代高新技術武器，如電磁炸彈等高能量脈衝武器和芯片細菌等電子生物武器進行；既可以透過網路內的電腦設備實施，又可以透過網路間的通信頻道實施。充分展現電腦網路戰手段的多元性。

(四)作戰行動不受時空阻隔極具主動性

在以往戰爭中，攻擊的一方通常握有主動權，但必須考量武器裝備、協同能力、天候、地形等條件。但在網路全球化的今天，儘管存在的空間分布不同，也不會受空間距離而阻隔，只要打開電腦，輸入敵方目標資料，發出指令，即可精準擊中目標，準此，攻擊的一方更具有主動性和突襲性。

(五)作戰行動一體成本低效率高

網路戰是一種「攻中有防、防中有攻」互為補充、相輔相成的一體作戰，此種攻防兼備的作戰模式，形成攻防兩個主體之間在作戰目的上整體一致性，從而提升了作戰效益，包括：

1.作用效果好。

其攻、防的範圍廣泛，可涵蓋敵我雙方的整個電腦網路系統。其攻擊行動隱密、速度快，可以隨時實施、危害性大、危急面廣；並防禦我方整個電腦網路系統正常運作不被敵滲透破壞。

2.攻防的重點是敵我雙方的核心系統。

一旦核心遭受攻擊或破壞就會造成指揮中斷，嚴重時可破壞整個系統。

3.成本低、研發週期短、手段隱蔽、破壞力強。

研發一種新型的網路病毒比研發其它高技術武器成本要來得低，完全可以用「低投資，高報酬」來比擬。

二、網路戰的分類

根據不同的劃分標準，電腦網路戰有不同的分類方法如按層級劃分可區分為戰略網路戰、[21]戰術網路戰；[22]按時間劃分可區分為

21 戰略網路戰分為平時和戰時。平時戰略網路戰是在雙方不發生有火力殺傷破壞的戰爭情況下，一方對敵方的金融資訊系統、交通資訊系統、電力資訊系統等民用資訊設施及軍事資訊系統，以電腦病毒、邏輯炸彈、駭客等手段實施的攻擊。陳憶綾，《解放軍資訊戰對臺軍事安全影響之研究》，(臺北：政治作戰學校政治研究所／碩士論文)，2006年，頁74。

22 戰術網路戰也分為狹義和廣義兩種。狹義戰術網路戰是旨在攻擊、破壞、干擾敵軍戰術資訊網路和防護己方資訊網路的作戰行動，其主要方式包括利用敵方網路弱點，將病毒植入電腦，讓駭客得以利用漏洞植入木馬程式，以得取所需資料。廣義戰術網路戰強調以下基本點：作戰行動將主要圍繞電腦網路進行，網路是資訊實時流動的渠道；資訊既是戰鬥力，也是戰鬥力的倍增器；作戰單元的網路化可產出高效的主動協同，可使指揮員以更多的方式指揮作戰，增強作戰的靈活性和適應性。王保存，〈網絡戰解析〉，《國防報》2004。，6 月17 日，版3。轉引自陳憶綾，《解放軍資訊戰對臺軍事安全影響之研究》，(臺北：政治作戰學校政治研究所／碩士論文)，2006年，頁74。

平時電腦網路戰和戰時電腦網路戰；按作戰範圍劃分，可分為全球電腦網路戰和戰場電腦網路戰；[23]按任務性質劃分，可分為電腦網路偵察、電腦網路進攻、電腦網路防禦，而使用最普遍的是按任務性質區分。[24]

(一)電腦網路偵察

獲取敵方網路情報的過程稱之為網路偵察。網路偵察是奪取網路戰勝利的先決條件，透過網路偵察，獲取充分的情報，不僅能掌握戰場上的主動權，也為軍事競爭中奠定勝利的基礎。[25]網路偵察技術包括網路信息攔截、密碼破譯、網路常規偵察、網路隱蔽偵察、網路滲透偵察、網路偵察、網路反偵察等。

(二)電腦網路進攻

網路進攻是利用敵方網路系統的安全缺陷、竊取、修改、偽造或破壞，以及降低、破壞網路使用效能而採取的各種措施和行動。[26]網路攻擊並不像傳統攻擊那樣造成一個國家的瓦解，但對於依賴資訊程度越高的國家，其所造成的傷害便越嚴重，甚至不下一場戰爭所導致的損失。從網路戰的攻擊模式來看，主要有三種：第一，體系破壞模式，通過發送電腦病毒、邏輯炸彈等方法破壞敵電腦與網路系統體系，造成敵國指揮控制系統的癱瘓。第二，資訊誤導模式，向敵電腦與網路系統傳輸假情報，改變敵網路系統功能，可對敵決策與指揮控制產生資訊誤導和流程誤導。例如，在科索沃戰爭中，美軍就曾通過截取的通信鏈路把製造的假雷達圖像植入南聯盟防空電腦網路系統中，致使南聯防空系統陷於癱瘓。第三，綜合模式，綜合利用體系破壞和資訊誤導，並與其他資訊戰模式結合，對敵指揮控制系統造成多重殺傷功效。[27]其目的是在通過網路攻擊形成網路優勢進而奪取制網路權。

從上述可知，電腦網路進攻戰的手段包括電腦病毒戰和電腦駭客戰。電腦病毒戰

23 全球網路戰是指國家或集團圍繞和運用國際信息網路進行政治、經濟、文化、科技等領域的鬥爭。是以爭奪21世紀經濟制高點為直接目的。而戰場網路戰是指交戰雙方圍繞和運用戰場互聯網進行的對抗。所謂戰場互聯網，是利用網路技術把上至高級指揮所下至單個士兵以及各種武器系統的所有軍用電腦聯結成一個整體，能實現軍隊作戰信息共享，以滿足軍隊實施戰爭戰鬥要求的軍隊區域網。呂登明，《信息化戰爭與信息化軍隊》上下冊，(北京：解放軍，2004年8月)，頁241。

24 徐小岩主編，《信息作戰學》，(北京：解放軍，2002年6月)，頁158。

25 陳岸然、王忠，《信息戰視野中的典型戰例研究》(上海：學林，2009年4月)，頁74-75。

26 另有論者認為中共在網路戰攻擊方面是以癱瘓敵指管通情系統為主要目標，其攻擊是以網路超載、施放病毒、阻斷節點為主要手段，研究具體成果為「網路制敵五法」(斷電、精確打擊、超載廢網、散播病毒、駭客滲透)、「信息網路對抗法」(網路刺探、網路破節、網路動截、網路攻程、網路癱瘓)。李章瑞，《解放軍報》，2000年5月9日，第6版，檢索日期103年04月22日。

27 Arnaud de Borchgrave, Frank J. Cilluffo, Sharon L. Cardash, Michele M. Ledgerwood, Cyber Threats and Information Security：Meeting the 21st Century Challenge (Washington DC.：Center for Strategic and International Atudies, CSIS, 2001)pp.10-1.。轉引自王瑋琦，〈中共對信息時代軍事變革之觀點〉，《空軍學術雙月刊，第619期》，2010年12月，頁81。

是指利用電腦病毒作為武器，對敵方電腦系統中的信息進行破壞、篡改，從而使電腦系統不能正常工作的作戰行動；在軍事領域資訊系統的核心設備和由電腦控制的資訊化武器裝備，都可能成為電腦病毒攻擊的主要目標。電腦駭客戰是指以駭客運用各種手段侵入對方電腦網路系統，對敵方電腦網路系統進行破壞的作戰行動。[28]如北約空襲南聯盟的同時，南聯盟電腦專家曾攻入美「羅斯福」號航母指揮控制系統，使其通信一度失靈。[29]

(三)電腦網路防禦

電腦網路攻擊手段迅速發展的同時，電腦網路防護也日益重要。作為現代戰爭指揮控制系統核心設備的電腦系統，只有加強防護才能有效抵禦對方駭客襲擊，保證戰爭指揮控制系統的正常運行。作為一種作戰模式，電腦網路戰不涉及未用於軍事目的的民用電腦網路。而中共在防制駭客方面著重以實體區隔、安全防護、欺騙誘敵，並參酌外國駭客攻擊方式，提出反駭客侵襲戰法，主要防制方法有變更隔離、真偽鑑別、靈活組網、防洩保護、隱匿規避、誘敵欺騙及干擾摧毀等七種方法。[30]

三、網路攻擊事件之實例

2012年迄今發生一些大公司被駭成功的新聞，讓人不得不想問這問題。這一連串的受害者都是赫赫有名的，像是Google、RSA、VISA、萬事達、花旗銀行、EPSILON、美國參議院、英國國家醫療保健服務、Fox，當然還有SONY。甚而連美國中央情報局的網站也變成分散式阻斷攻擊(DDOS)的目標。我國畢業於大同工學院的陳盈豪設計的CIH病毒，於1999 年的4月26日透過網際網路傳播於當天發作，造成全球共有600 萬台電腦遭受毀滅性打擊，其中韓國損失最嚴重，共有30 萬台電腦中毒，俄羅斯有10 萬台電腦癱瘓，中共也有近十億元人民幣的損失。[31]

波灣戰爭期間，美國情報人員利用伊拉克購置用於防空系統的印表機途經安曼的機會，將帶有病毒的晶片換裝到這批印表機中，並在美國空襲伊拉克的沙漠風暴行動開始前，用無線遙控裝置啟動潛伏病毒，致使伊拉克防空系統癱瘓。

2013年6月6日爆發的「史諾登事件」—美國監聽洩密案：時任美國國家安全局(NSC)技術外包人員的愛德華・史諾登(Edward Snowden)，揭露了 NSC 正在發展的一項聳動

28 中共電腦病毒攻擊戰法強調先期將電腦病毒預植於敵電腦系統，並在特定時間啟動病毒程式，主要以破壞性、複製性與擴散性病毒癱瘓敵網路系統為主，其戰法有前潰潛伏、臨機預置、間接攻擊、接口輸入、探測攻擊等五種方式。黃俊麟，〈中共信息戰與網路戰結合未來網軍發展之研究〉，《聯合後勤季刊，第10期》，2007年8月，頁25。

29 趙中強、彭呈倉著，《信息戰與反信息戰怎樣打》，(北京：中國青年出版社，2001年9 月)，頁315。

30 高景鋒，《解放軍報》，2000年3月28日，第6版，檢索日期103年04月22日。

31 趙寧，<倚天硬體門戶>，中華網科技頻道，網址：http://216.239.33.100/search，2000年9月4日，檢索日期103年05月05日。

的機密計劃——計劃「US-984XN」，代號「PRISM(稜鏡)[32]」等多項秘密監測計畫，為美國高度國家機密行動。總體來說，PRISM的運作模式是在合法合作框架下，透過聯邦調查局(FBI)的程序提出個別資料要求(甚至有人懷疑是直接進入伺服器取得資料，但是這種說法並沒有足夠證據)，然後取得資料導入PRISM的資料庫。此運作模式，理論上只需要取得一次法院的授權即可藉由美國國家安全局和聯邦調查局通過進入微軟、Google、Apple、Yahoo等九大網路巨頭的伺服器，監控美國公民的電子郵件、聊天記錄、視頻及照片等秘密資料；就美國公民權利來說，具有兩個盲點：一、在這樣的計劃裡頭，境外的美國公民顯然也是被監控著的，因為你無法單純以IP等資訊辨認出使用者的身分；二、即使監視的通信方是外國人士，當他所通信的對象是美國人時，兩方的資訊都將被洩漏出來。史諾登認為美國秘密監控計畫侵犯人民隱私，違反人權，除收集美國公民的個人情資外，也進行世界各國間諜活動。他對美國政府感到失望，因而決定公開揭露「稜鏡」計畫。美國輿論隨之譁然。

中共為我國主要威脅敵人，在網路戰作為上，中共駭客的攻擊事件遍布全球，2009年12月間，中共駭客對谷歌中共(Google.cn)與其他至少12 家大型美國公司發動「高度精密」網路攻擊；[33]中共藍翔高級技工學校則由解放軍協助設立，為共軍培訓部分電腦專家，其電腦系統委由與大陸首要網路搜尋引擎百度關係密切的一家相關企業代為操盤。[34]2010年3月22日晚間，谷歌在其官方部落格上宣布，停止過濾大陸網站「Google.cn」的搜尋結果，「Google.cn」的使用者將導向至香港搜尋網站「Google.com.hk」。[35]2010年3月30日，谷歌將其大陸搜尋服務轉移至香港後，搜尋引擎仍一度幾近癱瘓，谷歌表示，是因為中共當局的防火牆改變所致。[36]

中共網路戰發展現況研析

一、中共網路發展現況

網際網路在中國大陸的出現始自於1986年，當時兵器工業計算機應用技術研究所實施的－中國學術網(Chinese Academic

32 PRISM 是一個由 NSC 從2006年開始發展的國家機密級網路監視計劃，其主要目的在於「通過與網路服務商的合作，更輕易地取得關於外籍人士的通訊資料。」加入計劃的，前前後後包含許多知名的服務商，包括微軟、Yahoo、Google、Facebook、Skype和Apple等資訊量巨大的服務商。

33 〈中國人權人士帳戶遭攻擊　谷歌考慮退出中國〉，《中央社》，2010 年1 月13 日，網址：http://www.cna.com.tw，檢索日期103年04月23日。

34 〈Google 遭駭　源頭追到中國學校〉，《聯合新聞網》，2010 年2 月20 日，網址：http://udn.com，檢索日期103年04月25日。

35 〈Google 局部撤出內地〉，《YouTube》，2010 年3 月23 日，網址：http://www.youtubehkvideo.com/2010/03/google_23.html，檢索日期103年04月26日。

36 〈Google.com.hk 一度癱瘓「防火長城是元凶」〉，《聯合新聞網》，2010 年3 月31 日，網址：http://udn.com，檢索日期103年04月26日。

Network，簡稱CANET) 國際聯網專案和德國卡斯魯大學(University of Karlsruhe)合作，首次將網際網路的技術帶入中國大陸進行學術上的應用；1990年錢天白教授代表中國大陸正式向史丹佛研究所的網路資訊中心(Stanford Research Institute – Network Information Center)註冊登記了中國大陸的國家代碼域名(cn)，由於中國大陸此時尚未實現於國際互聯網的完全接通，因此，中國大陸國碼域名伺服器暫時建立在德國卡斯魯大學[37]。中共為發展網際網路，立法管制網路規範，並以自建中文化軟體與網路系統，冀反制網路上可輕易進入中國大陸之資訊。在2001年5月起成立「中國互聯網協會」，納入各網路業者，發起自律行動，並建立舉報機制，期透過該協會作為中介組織，對日益增多的大陸網民進行新的管理機制，採嚴格管制，使網際網路可以在其規劃下，依其方向發展。

美國哈佛大學法學院「柏克曼網際網路與社會研究中心(Berkman Center for Internet and Society)」對大陸監控網路情況進行研究，發現中國大陸20萬個網站中，有5萬個網站被中共當局封鎖，包括紐約時報、英國廣播公司、哥倫比亞廣播公司、美國聯邦法院系統等媒體網站，都無法從大陸登入，而中共如此不顧國際形象的封殺網路，係因其一直揮不去國際社會對其進行「和平演變」的夢魘。[38]

由於網際網路的發展快速，網際網路所呈現的無國界、虛擬的世界，中國大陸的諸多網民在言論自由的管制下，求取訊息並對國外的新聞網站特別喜愛，而國外自由民主國家的網站也不斷地進入中國大陸，使得中共領導階層憂心危及政權，並擔心網際網路變成西方對中國大陸搞「和平演變」的工具和管道，乃訂定各種嚴厲的法規，又設立網路警察，設置防火牆等防範，以加強控制大陸網民上網的「出軌」行為。

中共加強網際網路安全作為，透過訂定網路相關法規，提高行政管理層級，並以網路市場商機為誘因迫使國內外廠商協助監控，及運用社會建立舉報和檢舉網路不法或不良內容，相關內容分述如下：

(一)嚴厲訂定法律，明確使用要求與責任。

1.制頒法律規章：

從1994年起，中共已制頒「計算機信息系統安全保護條例」、「互聯網信息服務管理辦法」及「互聯網資訊服務管理辦法」(簡稱ICP管理辦法)等60多項法律來規範網路活動，相關的規章制度越來越包羅萬象，從努力規範網際網路商務到對新網站和聊天室的限制，且隨著法規體系不斷發展，中共甚至還將監控網際網路的主要責任從公安部轉移到網路服務商。這些法規規定了「不准說」

37 中國互聯網信息中心(CNNIC)，「中國互聯網發展大事紀」，網址：http://www.isc.org.cn/，檢索日期103年04月25日。

38 許綏之、王執軍，「封鎖網站中國第一名」，《自由時報》，2002年12月26日，版15，檢索日期103年04月26日。

的言論範圍，並授予政府很大的解釋權，違者可處拘捕到死刑不等的懲罰。如同世界各國皆對違反網路的相關法律進行追究或處罰，但中共法律相對嚴厲，不只發表、製作者有罪，甚至閱覽相關資訊者亦可能被施以行政處罰；另將被禁網站內容的監督管理義務加諸於多方，如作者服務、網路供應商及末端使用者，有令人驚恐的效果。

2.實行聯名制：

2005年中共信息產業部要求對網路接入、網吧(咖)、資訊發布網站、電子郵件及網路遊戲業者等，不論公營事業單位、私人企業網站或個人網站，都必須以實名備案；甚至提供真實姓名，以便追查不當言論之發表人士；另於備案時應提供有效證件。

3.強化網吧(咖)管理：

據中共國務院制定之條例，大陸網吧(咖)業者需核對、登記消費者之身分證件，上網者須以實名登記並記錄上網資訊；另業者必須建立場內巡查機制，發現違法行為須制止，並向公安機關舉報。在部分經濟發達地區，消費者同時受到網路攝影之監視。

(二)提高管理層級，組建新的執行力量。

1.提高主管機關層級，以利統籌管理：

中共對互聯網的管理由宣傳、文化、工商、公安部門共同參與，每一部門從各自角度負責相應措施，行政級別多為「局級」，缺乏協調配合。2007年中共「外宣辦」成立專業統管部門「網路宣傳局」，規格高於國務院新聞辦的「網路局」，此一新機構專責管理互聯網資訊。

2.成立「網軍」，維護網路主權：

1999年11月解放軍報首次提出「網軍」，成為繼陸、海、空三軍及二砲後的新軍種，擔負保衛網路主權和從事網路作戰的任務，並師法美國，將網軍組成攻擊、防衛、維護三大部門。中共「網軍」成員包含吸收民間頂尖駭客，並視彼等專長編組，依任務別使用「間諜程式」、「蠕蟲程式」、「木馬程式」、「釣魚程式」及「電腦病毒」等，透過網路入侵各國政經電腦系統。[39]

3.組織「網路警察」，執行網路糾察：

自2000年12月起，中共高層指示擴大「網路警察」的編制。大陸公安機關陸續擴編原先所轄的電腦信息監管隊伍，增加人員編制，並將先前成立的公安部「公共信息網絡監察局」作更具體明確的分工，在全大陸省、直轄市級的公安廳局組建所謂的「公共網絡信息監察處」。目前中共「網路警察」的編制人數達30餘萬人，專責監視網路內容與封殺網頁、阻止所謂的「有害信息」之傳播，並對當前中國大陸各地流行的「網吧(咖)」，施以突擊檢查；中共高層對「網路警察」所提出的職能目標為：「依法管理、預防為主、確保重點、促進發展、保障安全」。

(三)研發網監技術，全面監控網路：

39〈中國佈「金盾」監控全民〉，《自由時報》，2008年12月9日，版3，網址：http://edwardso.dyndns.org/bo-blog/read.php?1547，檢索日期103年04月06日。

為建立全國性的遠距數位監視網路，即時取得大陸每位市民之登記紀錄，同時連接全國各地公安機構，以加快應變對付示威遊行等活動，中共公安部在1998年提出「金盾工程」計劃(西方稱之為「網路長城」)。[40]「金盾工程」就是全國公安資訊化工程，亦是全國公安機關的電子化警務建設，希冀實現監控的人工智慧技術，包括自動語音辨識、相貌識別等，最終目標是巨大的聯機資料庫，以及包含各方面的監視網路－綜合語言及面貌識別、閉路電視、智慧卡、信用紀錄和互聯網監視技術。

(四)以市場大餅為餌，誘逼國內外廠商協控：

中共向西方科技軟硬體大廠如微軟、思科、昇陽等，購買先進技術來協助其監控、封鎖網路，同時要求廠商主動配合，幫助政府過濾『敏感』言論。被要求配合的廠商基於市場因素，或是擔心觸犯那些隱晦的規章，多會順應中共要求。如微軟在大陸推出的MSNMyspace便設置篩檢程式、Google.cn會將違反中共官方規定之敏感字眼內容自動過濾掉，雅虎Yahoo.cn更以「服從當地法律是公司經營的準則」為由，洩漏了中國大陸作家王小寧、記者師濤的個人隱私資料，致遭中共逮捕、定罪。

除了西方跨國企業外，中共對大陸內地企業的配合要求更高，如大陸網民使用人數最多的即時通訊軟體QQ，即被發現在通訊軟體內建過濾機制的關鍵詞名單，用來協助其官方部門進行網路即時監控。

(五)利用社群力量，鼓勵民眾監督和舉報：

中共各級政府部門建立舉報網站和檢舉電話，用來接收對政治、色情暴力等有危害國家社會內容之網路資訊逕行舉報。如為因應北京奧運活動、共產黨第十八次全國代表大會及第十八屆三中全會召開期間，更加緊對宣傳的監控，建立網上綜合防控體系，進一步加強對網路的管理，並在境內各重點網站、論壇設立網上「報警崗亭」和「虛擬警察」，接收群眾舉報、求助與迅速處置，及時發現、制止網上有害資訊傳播行為和違法犯罪活動；公開警示網上輕微違法和不良行為，組織重點網站和論壇等網路公共資訊傳播場所，建立網路資訊安全巡邏、協管隊伍，協助維護網上秩序。[41]

二、中共網路戰的能力

中國大陸自 1984 年開始注意機敏部門的網路安全工作，於1986 年擬定「高資訊技術研究發展計畫」，成為中國大陸近年來科技專案的政策依據。專案執行期間，中國大陸亦參考美國發展一系列與國際接軌的國家資安標準，訂定資安相關法規與權責、驗證機構等，意圖大幅提高中國大陸資安水準。

40 同註39。

41 杜文娟，〈十部門嚴打網路淫穢色情 "虛擬警察"6月底前上崗〉，《人民日報》，2007年04月13日，版4，網址：http://203.91.55.40:9000/b5/fzj.sz.gov.cn/ho1120.asp，檢索日期103年05月04日。

政府方面，中國大陸於1999 年開始建設電子化政府，為保護其政務相關的機敏資料，將電子化政府網路劃分為涉密域(涉及國家機密)、非涉密域(不涉及國家機密，但涉及單位部門工作秘密)、公共服務域(僅涉及個人與企業敏感資料)三區。其中涉密域與其他兩個領域實施「實體隔離」，彼此僅能透過安全閘門(Security Gateway)進行溝通。

在軍事方面受波灣戰爭影響，中國大陸以「質量建軍，科技強軍」為原則，著手組織數位化部隊，研究新型態資訊作戰方法。軍方先後於1995 年和1996 年成立「國防科技信息中心」、「信息安全研究室」及於「總參二部(軍事情報部)」下成立「科學裝備局」等機構，進行研發資訊軟硬體、電腦病毒、駭客攻擊、電磁脈衝武器等技術。自1999年開始，中國大陸軍方已將訊息戰、駭客攻擊、網路攻擊等納入演習範圍。陸續建立與網路高速公路聯網的校園資訊網路、作戰模擬系統及初級戰鬥實驗室。1999年共軍合併「通信工程學院」、「工程兵工程學院」、「空軍氣象學院」以及「總參」附屬的63個相關研究所，重新組建「解放軍理工大學」，以進行網路戰的戰略規劃、理論研究和技術開發，欲將高科技成果廣泛運用到軍事領域中。[42]其網路戰之發展可概分為下列方向：[43]

(一)加強網路戰相關科技研發：研發各類衛星通信、數位化訊號處理、電腦監控顯示器、多媒體技術及模擬技術、癱瘓指管通情系統為目標之資料鏈、網路連線傳輸型電腦病毒程式等。

(二)積極向國外引進網路戰技術及設備：對外合資與技術合作，並以民用裝備名義引進先進科技。

(三)籌設信息戰模擬中心：包含專業人員編組及小規模資訊戰模擬部隊。波灣戰後，中共深知在傳統武力上已遠遠落後美國，尋求與美國正面對抗的方式，無異自尋毀滅。是故中共不得不另闢蹊徑，在不對稱戰爭中尋找致勝之道。

(四)編組民間網軍：中共在與國防部平行的國防動員委員會之下成立「信息動員辦公室」，各地國防信息動員辦公室的主要任務共7條，依據其新增第6條之規定：「制定國防信息保障力量建設規劃、組織民兵信息戰部隊教育訓練、為軍隊提供相關軍事信息保障」，軍方可以透過「動員辦」的機制整合民間信息力量發揮戰力，達到民為軍用、平戰結合的目的。[44]民間駭客組織為中共網軍的骨幹，繼承了人民戰爭的傳統。[45]2000年重

42 廖文中，〈中共組建國家網軍：全球資訊戰〉，2007年第3次「中共解放軍論壇」，2007年9月27日，頁3
43 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T96019》，頁15-16。
44 廖文中，〈中國網軍：國安、公安與解放軍〉，(臺北：全球防衛雜誌)，271期，2007年3月。頁-3。
45 李華球，〈沒有煙硝的戰爭－中共解放軍網軍資訊作戰的初步觀察〉，《2007年解放軍研究論壇彙編》，(桃園：國防大學出版，96年12月)，頁239。

慶警備區成立「民兵網路戰分隊」，由研究生、教授和電腦專家組成，旨在利用當地的電信設施、媒體、網路及民用技術設施來支援軍方，遂行網路戰。[46]2002年起，中共國務院在信息產業部(2008 年6 月29 日改制為工業和信息化部)底下成立「網路戰士」秘密組織，並化名為民間電腦駭客組織。該部在大學校園內和社會各個層面吸收、甄選具備軟體設計和破解密碼專長的人才，賦予網路戰士的封號，讓他們擁有測試最新電腦程式的完全自由，並提供工作和生活上的相關資源。[47]

2014年5月19日，美國司法部對五名中國人民解放軍61398部隊[48]第3支隊的成員—王東(Wang Dong)、孫凱亮(Sun Kailiang)、文新宇(Wen Xinyu)、黃振宇(Huang Zhenyu)和顧春暉(Gu Chunhui)提出起訴，指控他們對美國美鋁公司、美國鋼鐵公司、西屋公司、太陽能世界和阿勒格尼技術公司共五家著名企業以及主要工會組織美國鋼鐵工人聯合會進行經濟間諜活動，這是美國首次對外國提出對美企業進行網路犯罪的刑事指控。美國司法部長埃里克・霍爾德稱：世界許多國家互相彼此刺探情報，但是，美國「斷然譴責」中國人民解放軍駐上海某單位的經濟間諜活動，這些間諜活動向中國大陸公司提供了「重要」訊息作為回應。

根據麥迪安報告，該部隊技術嫻熟，有一套明確攻擊方法，駭客對象橫跨20個工業行業、近150企業及組機(其中87%總部設在英語國家，主要在美國，兩起受害者位於臺灣)，目標竊取大量寶貴知識產權資訊。[49]在成功入侵後，獲取訪問通道，部隊會在數月、數年內定期訪問受害者以持續竊取各種信息。七年中被監測到針對近150家公司組織的攻擊企圖，遭竊數據達數十萬GB，內容「包括技術藍圖、專有的製造工藝流程、測試結果、商業計劃、定價文件、合作協議、

46 陳憶綾，《解放軍資訊戰對臺軍事安全影響之研究》，(臺北：政治作戰學校政治研究所／碩士論文，2006年，頁74。

47 蕭懷湘，〈中共培育網路對抗人才之規劃及展望〉，《前瞻科技與管理特刊》，2010年11月，111頁。

48 「61398部隊」最有可能是中國人民解放軍策動駭客襲擊的後台，隸屬於解放軍總參謀部三部二局。依美國麥迪安網路安全公司的報告指出，實際地理位置是位於上海市北方郊區浦東新區高橋鎮大同路一棟12層大樓，建於2007年初，外有圍牆，院內的中心建築佔地約13萬平方英尺，高12層；此建物因此受到西方媒體的關注及探訪，如《每日電訊報》報導該大樓有解放軍哨兵看守、有中英文寫著「軍事禁區，不許拍照」的字樣，外面圍牆並有「忠於黨、熱愛人民，獻身國防事業」標語；2013年2月，美國麥迪安網路安全公司根據7年追蹤的記錄證據做出總結報告，指控中共解放軍是美國發生的一系列高層駭客攻擊的幕後操縱者，由於該駭客集團從事的是網路安全中所謂的進階持續性滲透攻擊(Advanced Persistent Threat，縮寫APT)中「最多產的團體」，將此團體命名為APT1，並推測61398部隊極可能是此團體。〈共軍網路駭客總參三部二局〉，《CNN新聞網》，網址：http://www.cna.com.tw/News/aIT/201302200334-1.aspx，2013年02月20日，檢索日期103年05月12日。

49 〈中國回應美國有關中國黑客襲擊〉，《BBC新聞網》，網址：http://www.bbc.co.uk/zhongwen/trad/world/2013/02/130219_china_hacking.shtml，2013年02月19日，檢索日期103年05月12日。

電子郵件、聯繫人列表。」美國電腦分析專家調查100多次攻擊過程發現，所有線索都指向位於上海的該座12層大樓。[50]

三、中共發展網路戰對我之威脅

美國仍是世界上資訊戰力最強的國家，中共以武力犯臺最大的顧忌亦是美國出兵干預。因此，在中共現階段的軍事理論中，高技術局部戰爭理論為指導方針，而以資訊戰為導向的軍事革命，其著眼在於中美未來有可能在奪臺戰役中發生衝突，在軍力劣勢狀況下，唯有運用資訊戰癱瘓美國軍方與民間電腦和網路系統才有獲勝可能，這種趨勢將發展成當安全環境不利或軍力處於劣勢時，會成為下一波軍事革命發起的動力。目前，中共網路戰的發展已頗具規模，一旦海峽兩岸發生衝突，資訊戰將為其第一波攻勢，於癱瘓我資訊網路後，再大舉武力進犯，使我防不勝防。本研究認為中共網路戰力對我造成的威脅如下：

(一)可適時支援作戰任務

中共各科研機構對網路戰理論研究之深化，近年來積極推行並落實於實兵演練與驗證中，因此，解放軍不斷的進行虛擬實戰，如1997年瀋陽軍區電腦病毒攻擊演練，1999年北京軍區兩軍電腦對抗演訓，2000年成都軍區的網際網路演訓，以及2001年的模擬對臺作戰等，均是以資訊攻擊為開端。[51]另2001至2003年間，解放軍在鄭州、濟南、北京、南京、西安等五大城市的相關信息戰部隊或研究部門組建性質不同的研究中心，及提出網路對抗戰法，中共網路戰中心思想為建構國家政治、經濟、軍事等方面之安全於資安之上，掌握政府、軍事與民間等三方面為其具體作法。

中共瞭解要發展信息戰，就必需要有基礎設施網路為發展之根本，自1992年開始由「國家發展改革委員會」主導8個部委共同主持研發「中國互聯網」計畫，成立了以中國官方為主控、商業為應用的互聯網。力圖能後發先至，成為世界華人圈的「因特網」(Internet)，擺脫美國的控制，進一步還可以和美國平分秋色。[52]2004年中共首先建立「中國互聯網」，打破來自美國的不對稱威脅，同時結合軍民力量組成網際軍隊，由專責部門負責網路的防禦與攻擊。[53]

(二)具網路不對稱攻擊戰力

科技落後的中共曾以「蛙跳式」或「跳島戰術」的方式獲得核武、洲際飛彈、人造衛星等尖端技術。「中共在2025年之前不可能與美國在軍事上成可匹敵的競爭者。」這

50 〈英媒：61398部隊—中國網戰中心〉，《BBC新聞網》，網址：http://www.bbc.co.uk/zhongwen/trad/china/2013/02/130220_press_61398_cyber.shtml，2013年02月20日，檢索日期103年05月12日。

51 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，82期，187-218頁。

52 廖文中，〈中國網軍：國安、公安與解放軍〉(臺北：全球防衛雜誌)，271期，2007年3月。頁1。網址：http://www.diic.com.tw/comment/9611/961109china%20net%20force.pdf。檢索日期103年04月26日。

53 〈中共建構網軍專責防禦攻擊〉，《國防部軍事新聞網》，網址：http://news.gpwb.gov.tw/news.php?css=2&rtype=2&nid=26216，2007年9月28日，檢索日期103年04月12日。

是阿米塔吉1997年11月21日在哈佛大學演講所說的。但是打贏資訊戰爭不需要全面軍事優勢，所以阿米塔吉警告在「不對稱戰爭」中，解放軍只落後美國10～12年。時至今日2014年，事實已證明，目前中共在資訊戰的能力已在「電腦病毒戰」及「網路駭客戰」等方面超越臺灣，甚至已經具備威脅美國的能力。

(三)資訊戰略關鍵技術突破

中共解放軍近來投入發展「資訊高速公路」基礎建設及致力資訊戰研究，從開發陸、海、空、二砲專業練習模擬器材至合成戰術、戰役層級之模擬架構，未來共軍將以推動「指揮決策智慧化」、「業務處理自動化」及「系統管理工具化」為目標，鼓勵全軍學習高科技資訊知識並使此熱潮持續高漲，另尋求C4ISR所需關鍵技術之突破，以開發具戰略層次智慧網；透過太空工具，使其在掌握「資訊優勢」上，增益其戰略層次智慧網路之研發與運用，冀望達到「決勝千里之外」之作戰目標。

(四)網路安全規範嚴謹

中共以公安部主管資通安全並強制驗證，其法源依據為1995年公布之「中華人民共和國警察法」與1994年公布之「中華人民共和國信息系統安全保護條例」。中國大陸對於資訊系統相關產品之銷售實行許可證制度，凡於境內銷售之相關產品，都必須通過有關機關對於加密技術、電磁波等之安全功能檢測。2007年6月中國大陸公安部會同國家保密局、國家密碼管理局、國務院資訊辦，聯合發布了「信息安全等級保護管理辦法」，將信息系統安全保護分為五級，為各部門、各單位進行信息安全等級保護工作的重要依據。

網路戰威脅我應有之思維

一、以SWOT分析我國遂行網路戰之能力

面對資訊化程度日深之趨勢，正視層出不窮的資安威脅，並思考改善之方法，則危機往往可以是一種轉機；西元2010年時，全球企業資料外洩增加47%，1～8月身分資料遺失案件達449件，超越前一年的446件，其中僅40%揭露受影響的資料筆數，即已超過2,200萬筆。[54]而同年地下經濟交易總額超過2.76億美元，其中信用卡占了59%。2013年全球安全、儲存與系統管理解決方案領導廠商賽門鐵克(Nasdaq: SYMC)與Ponemon Institute共同發表全球資料外洩成本調查報告(ISTR)，指出去(2112)年資料外洩事件較前年成長62%，造成5.5億筆個人資料曝光。顯見網路地下經濟活絡的程度，恐已干擾實體經濟活動，並可能影響社會安定，必須積極以對。[55]

再從臺灣的網路應用環境看：根據財團法人台灣網路資訊中心(Taiwan Network

54 資料來源：美國身分竊盜資源中心(Identity Theft Resource Center, ITRC)，2010年8月，檢索日期103年04月26日。

55 資料來源：賽門鐵克第16期賽門鐵克網路安全威脅研究報告 (Symantec Internet Security Threat Report，簡稱 ISTR)，西元2011年04月，檢索日期103年04月06日。

Information Center,TWNIC)調查，2013年我國12 歲以上曾經上網民眾比率在2013年上半年達到79.18%，人數達到1,645 萬人，全國可上網的家戶數達到694 萬戶，比例達84.81%，顯見臺灣上網普及程度；而線上購物人口262萬，線上付款人口僅約167萬，普及率面臨成長趨緩壓力。而線上購物普及率涉及寬頻建設完善度、線上交易機制之安全便利、法規及配套措施等，是否因為安全因素影響民眾使用意願，值得我們深思。

綜合上述，茲彙整強化我國網路戰力目前所面臨的挑戰以及所擁有的優勢，以SWOT分析如表一所示。

表一　我國網路戰力SWOT分析

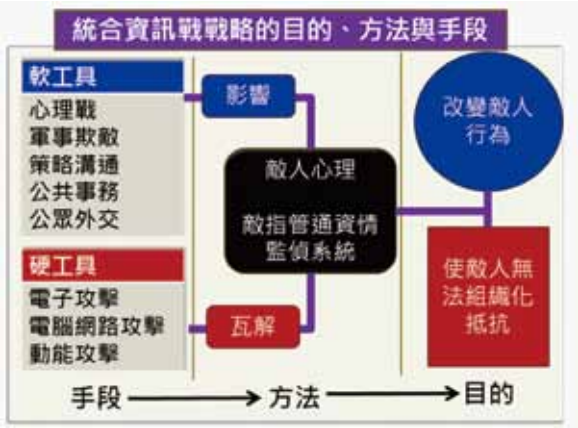
優勢(Strengths; S)	劣勢(Weaknesses; W)
1. 臺灣民間業者擁有豐富的網路防護經驗與駭客行為模式資料。 2. 臺灣業者多自行研發產品，且在郵件、網頁內容過濾與攔截等具技術優勢。 3. 臺灣資通訊產業發達，擁有質優的資通訊科技人才，創新性及對新科技接受度高。	1. 以民間業者發展為主，資源有限，政府及軍事部門整合與運用機制不足。 2. 國內網路安全防護法制體系未臻完備，政策工具之種類與效益受限 3. 基礎研究能量未能充分為產業所用。 4. 網路戰指揮機制不明確。
機會(Opportunities; O)	**威脅(Threats; T)**
1.在網路威脅蔓延，各國均著重網路安全環境建置。 2.政府持續發展資通訊基礎建設及應用服務，並以網路空間安全為目標。 3.各國皆須強化國際地位與影響力並積極拓展資安合作機會。 4.新興的整合式設備或服務不斷推陳出新，臺灣的資安及資通相關產業具備整合的條件與能力。	1.中共逐漸完成作戰整備。 2.中共官方與民間均已具網路攻擊戰力。 3.中共全力發展信息化戰爭。 4.中共全力發展資訊科技。 5.中共逐步強化網路安全法律規範。

資料來源：作者彙整。

二、建構符合國防與軍事戰略之網路戰略

美空軍中校Hans F. Palaoro於《資訊戰略：失落的環節》一文中指出：策定周延的資訊戰略不僅是發揮資訊國力的重要課題，彌補戰略目的、方法與手段的不足，更是當前刻不容緩的要務。[56]並依據美軍聯戰準則(2006)及資訊戰準則(2009)定義「統合資訊戰戰略的目的、方法與手段」如圖一。

圖一　統合資訊戰戰略的目的、方法與手段



資料來源：Hans F. Palaoro，黃淑芬譯，《資訊戰略：失落的環節》「國防譯粹」第38卷第一期，100年1月，頁83。

我國國防戰略係以確保國家生存與未來永續經營發展，並遵照馬總統「固若磐石」安全理念指導，達成「預防戰爭」、「國土防衛」、「應變制變」、「防範衝突」及「區域穩定」等五項「國防戰略」目標。[57]而軍事戰略係國家戰略(政、經、心、軍、科技)之一環，其目的在爭取戰爭勝利，以支持國家戰略，達成國家目標。國軍考量周邊安

56 Hans F. Palaoro，黃淑芬譯，《資訊戰略：失落的環節》「國防譯粹」第38卷第一期，100年1月，頁80。
57 國防部國防報告書編纂委員會，《中華民國102年國防報告書》。臺北：國防部，民102年10月，頁63。

全環境及敵我戰略態勢發展，依國防戰略指導，係以「防衛固守、有效嚇阻」為軍事戰略構想，採守勢防衛，絕不輕啟戰端。[58]

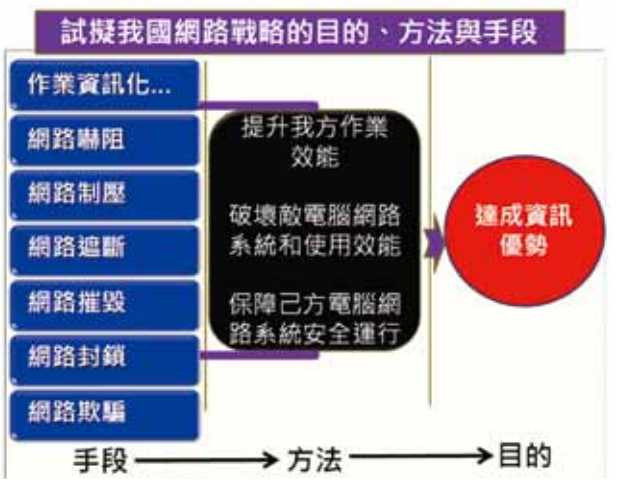
依據前述理論、網路戰史及中共、美國發展狀況並分析我國特弱點，筆者嚐試以軍事角度來敘述網路戰戰略的具體作為，可簡述如下：網路戰係於電腦網路環境下，運用提升我方作業效能，破壞敵方電腦網路系統和使用效能，以及保障已方電腦網路系統安全運行等「方法」，藉作業資訊化(信息化)、網路嚇阻、網路制壓、網路遮斷、網路摧毀、網路封鎖、網路欺騙等「手段」，以達成資訊優勢之「目的」，如圖二。

然如何具體發展資電作戰(含網路戰)攻擊、防護能力？除依作戰任務需求，結合公、民營通資網路建設，構建自動化、高速率、高可靠之通資網路。依據「全民防衛動員準備法」及其施行細則，訂定戰備各階段公、民營通信設施支援軍事管制運用辦法，結合動員物資徵購徵用辦法，充分管制運用公、民營機關專用通資資源，如各式有(無)線電機、電話電路、行動通信、數據網路、衛星通信等系統裝備設施，提供防衛作戰備援運用；定期協調及演練，掌握可運用之公、民通資資源及技術能量，並建立標準作業程序，達成平時可應用公、民營充沛資源於戰備整備與災害防救，戰時可立即支援軍事作戰之目標。

三、策進作法與建議

面對未來網路上的安全威脅與中共強大網路戰的壓力與挑戰，針對我國網路戰相關作為應以「達成資訊優勢」為目的，須以「全方位網路優勢作為」之戰略構想，本研究認為未來國家應可依據以下幾個方向推動：

圖二　我國網路戰略的目的、方法與手段簡圖



資料來源：作者自繪。

(一)建立一個有力的單位發現並解決資安問題。

這單位要有技術背景、執行的強制力、並且健全的通報機制，作為全國企業及政府單位的後盾，將資訊政策由國家戰略貫穿至各層級。我國相關重要通資資源防護政策與法規不足，針對網路戰之戰略指導或資訊政策亦未臻明確，應儘速邀集學者、專家及相關主管機關，定期加開研討會或專案研究計畫，共同律定我國發展網路戰(資訊戰)之戰略方針，藉以指導各層級增修相關政策與法規，以健全防護體制的規劃與執行。另同時

58 國防部國防報告書編纂委員會，《中華民國102年國防報告書》。臺北：國防部，民102年10月，頁70。

與民間業者合作，提供各作戰與後勤專業部隊之指揮官能於行動間，運用行動通訊系統掌握部隊動態、存取與交換資訊及下達作戰命令，形成網狀化與自動化資訊環境。

(二)發展資訊為政府重要且優先的施政目標

「資訊安全」應以達成「資訊優勢」與提升作戰(業)環境資訊化能力為前題，審慎評估在何種資訊設施與節點應加強資訊安全作為與採取適當之資訊防護裝置，並建立國軍同仁完整資訊教育與正確認知。未來應運用資訊安全風險管理評估作為，依資訊防護需求搭配資訊安全防護技術，藉由健全資訊安全認知與理念發展適當之資訊安全政策支援政府專業網路社群之推動。

近年來世界各國都非常積極的培育資安人才，籌組資安學校、科系，舉辦資安競賽、集訓出國競賽。如果不能投入資源從學校開始培育對資安有興趣的學生，臺灣的未來將沒有足夠的資安人才投入企業或政府單位。準此，政府應將資訊發展列為優先施政目標，有計畫地編列相關預算並落實執行，以強化我國總體資訊國力。

(三)作業流資訊化滿足科技需求

中共深刻體認到戰爭型態、作戰模式與各項武器裝備，均已呈現資訊化(共軍稱為信息化)趨勢，遂全面加速發展信息戰力，如1991年，江澤民在視察國防科技大學時，即提及現代戰爭已成為高技術戰爭，要求國家與軍隊要實施現代化；[59]翌年(1992年)，鄧小平復於十四大會議中，提出以「精兵、專業」為中心，以「質量建軍、科技強軍」為原則，大力推動共軍現代化的二次改革風潮，並作出「現代條件下的高科技戰爭」與「打一場高科技條件下的有限戰爭」的戰略調整。在波灣戰爭的影響下，中共解放軍發現美軍所引領的「軍事事務革命」與「信息化戰爭」的理論與實務，並從中掌握了「軍事事務革命」的性質與方向，了解到新軍事革命是以信息技術為核心的高科技技術推動下所出現的。[60]

面對中共於作戰型態之改變，國軍如何將各項作業流資訊化，以成為「知識」與「戰力」倍增器，達到適量、質精、戰力強之國防勁旅，實為我積極規劃、落實執行之策略目標。例如國軍通資基礎建設應建立共通作業環境，建立智慧化與多重備援之通資網路。以有線電路為基礎運用資訊技術，整合無線、數據網路、微波與衛星，構建多維與多重備援之無脆弱性關鍵節點網路，俾提升國軍平、戰時通資基礎建設之可用率與存活率，滿足各項國軍作業需求。

(四)掌握關鍵技術強化產官學界合作

如何捍衛「網路主權」，其中根本方法就是發展自主網路科技產業，並掌握核心技術，擺脫對網路科技設備與軟體系統的依

59 〈中央軍委主席江澤民簽署命令　組建新的國防科學技術大學〉，《新華網》，網址：http://big5.xinhuanet.com/gate/big5/news.xinhuanet.com/ziliao/2000-12/31/content_486019.htm，檢索日期103年05月06日。

60 莫大華，〈中共「軍事事務革命」之分析—資訊戰爭的探討〉，《中國大陸研究》，第41卷11期，頁51。

賴。政府部門應積極與產官學界合作發展評鑑風險、風險管理等分析技術與監測預警技術，通資安全的防護資訊系統的開發更是重要，以及防護實體安全的硬體技術，藉以認定、設定防護優先性與措施。

而企業的通病是上了媒體才叫出事，平常以鴕鳥心態看待資安。若不能未雨綢繆投入資源加強安全，出事後所要花費的成本將是原本的百倍。資訊安全應是企業必要的支出成本，鞏固企業的品牌形象，加強客戶的信賴，萬萬不能看待成多餘的無用支出。

(五)各部門明確分工加強整合與協調

網路戰涵蓋範圍廣泛，舉凡政治、心理、經濟、科技和軍事等各領域，均為敵運用資訊技術爭奪資訊優勢的目標，我國行政院雖已成立「通資訊基礎設施安全機制」，此機制主要防範「軟體破壞」為主，但對基礎設施防護之「硬體破壞」防護則顯不足，雖然政府已有行政院資通安全會報、調查局資訊室、國安局與國防部資電作戰指揮部等單位，但是各單位的程度不一，又沒有統一建設，而是各自為政。所以國家層級資訊戰指揮機制的運作，宜由行政院主導，結合內政、外交、國防、財政、教育、法務、經濟、交通等部會及國家安全局，針對電力、電信、金融、交通等國家基礎建設之安全防護，共同研析相關因應作為，並進行同步整合，防止工作重複、遺漏和偏移，並從策略推廣、分析及預警、人員組訓、調查、防制等，據以指導各部會策定計畫及行動準據，分層負責貫徹執行。

結　　論

在美軍聯戰準則2006年所頒之聯戰準則JP 3-13所提出：資訊戰係運用電子戰、網路戰、心理戰、計畫安全(保密)、心理戰等資訊作戰核心任務與次要任務，對敵資訊及資訊系統產生具體影響力，並防護我軍資訊，進而影響敵決策(Decisionmaking)機制之運作觀點下，可以說明網路戰屬於資訊作戰範疇，而其作戰的目的在奪取制網路權。若以國軍軍語辭典對資訊戰所下的廣義定義「運用各種手段影響敵方並防禦我方決策程序與資訊系統之行動，以創造資訊優勢。」以及狹義之「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。」亦仍顯狹隘，均在強調資訊系統(網路)間之攻防作為。共軍將領王保存在《網路戰解析》一文中將廣義網路戰定義為：作戰行動將主要圍繞電腦網路進行，網路是資訊實時流動的渠道；資訊既是戰鬥力，也是戰鬥力的倍增器；作戰單元的網路化可產出高效的主動協同，可使指揮員以更多的方式指揮作戰，增強作戰的靈活性和適應性。[61]更能說明網路戰之精義。

本研究綜整網路戰定義如表二：

61 王保存，〈網路戰解析〉，《國防報》2004年6 月17 日，版3。轉引自陳憶綾，《解放軍資訊戰對臺軍事安全影響之研究》(臺北：政治作戰學校政治研究所／碩士論文)，2006年，頁74。

表二　網路戰廣義及狹義之差異表

網路戰廣義及狹義之差異表		
區　　分	廣　　義	狹　　義
作戰的目的	爭奪網路優勢或破壞資訊網路	在奪取制網路權
作戰的對象	軍事、政治 、經濟等一切領域	敵方的電腦網路和資訊
作戰主體	國家、民族、武裝集團甚至恐怖分子	運用資訊技術和裝備武裝起來的網路戰士
作戰區域	廣濶的電腦網路空間	廣濶的電腦網路空間
作戰手段	網路技術和手段進行的鬥爭	根據電腦技術研製的各種病毒，邏輯炸彈和芯片武器等
致勝途徑	是透過削弱、破壞敵方電腦網路系統的資訊和使用效能，以及保障己方電腦網路系統的資訊和安全運行達成電腦網路的作戰目的	是透過削弱、破壞敵方電腦網路系統的資訊和使用效能，以及保障己方電腦網路系統的資訊和安全運行達成電腦網路的作戰目的

資料來源：徐小岩主編，《信息作戰學》(北京：解放軍，2002年6月)，頁158。

由上述觀點更能說明網路戰的爭奪不僅在攻防作為，應將達成網路優勢作為爭奪之目的，除了前述網路偵蒐、網路攻擊、網路防護等方法外，更須包含系統優化(如輔助決策系統、知識管理系統或任何協助相關作業與決策之系統)，亦為美軍所謂「系統中的系統」；或是共軍近年常提出的信息化戰爭作為。

未來以資訊優勢戰場管理發揮「比敵人先看見」、「比敵人先瞭解」、「比敵人先決策」功能，以形成制敵機先，將是戰場致勝關鍵。在我國遂行網路戰之「防衛固守」戰略指導部分，國防部除訂頒「國軍資訊安全」之各相關規範，嚴格落實資安管控措施外，並針對戰演訓部分，策頒「國軍演訓資通安全維護整備要點」，期能從軟硬體設備乃至於「人」的因素著手，避免違規情事肇生，建立安全的資訊作業環境，進而強化國軍整體資安防護能力。以資訊為核心所建構的國家基礎設施，新形態網際網路所衍生的電腦駭客等安全漏洞問題，已經是防不勝防，無論是國防科技或軍事武器等重要情資外洩，均將牽一髮而動全身。若透過敵方後門程式的植入或個人帳號的套取，導致資訊流的阻斷、篡改與監控，並肇生資訊安全危機將使敏感機密資訊受極大威脅與造成國家安全利益重大損失。因而，需要提升全民國防與網路作戰觀念，於使用網路資源時，要有維護網路安全基本素養，確遵安全規範，讓全體國人均保有高度資安警覺與防制能力，落實更綿密的國防資訊安全防護作為。

網路戰爭的攻擊是永無止盡的，在確立明確的攻擊目標、目的、時間後，執行單位就會開始規劃長期的攻擊計劃。以2013年3月份南韓DarkSeoul攻擊事件為例，傳言北韓花了8個月的時間規劃攻擊，入侵防毒軟體更新伺服器，利用其更新機制將32000台電腦植入後門，並刪除電腦資料使其無法啟動，更嚴重的是其中也包含了ATM提款機。這次事件造成部分銀行停止運作，南韓股市嚴重大跌。一次成功的網路攻擊會對國家造成如此

62 林勤經，〈兩岸資訊戰力之比較網路戰解析〉，《中共對信息戰之研發與影響研討會》，(臺北，臺灣綜合研究院)，民國89年2月，頁3-5。

嚴重的後果。南韓在48小時之內就掌握了受害狀況，並且恢復大部分的金融運作。很多人問，如果這次事件發生在台灣呢？

傳統的軍事網路戰攻擊只能指向對方的軍事力量和經濟潛力，而未來的作戰，將不排除透過官方或民間組織運用網路攻擊貫穿敵方的軍事、政治、經濟和整個社會，乃至國民的精神、觀念及心理等。有效運用網路心理戰和戰略欺騙等手段，破壞敵政治、經濟、軍事，乃至整個社會的重要基礎設施及其效能，動搖軍民士氣，進使敵喪失作戰能力。[62]目前國防預算不足的時刻，利用政府組織再造時機，落實政府雲端運算的推動應該是前瞻未來，符合趨勢的重要工作之一。而如何運用我國既有資訊科技優勢籌建網路戰嚇阻戰力，並結合軍民以鞏固優勢使敵不敢輕易來犯，或縱使來犯必然付出極大代價，更實為目前我國發展網路作戰尚欠缺且極待發展部分。

因此，我國網路戰之發展如何結合國家力量發展出有系統之組織架構與具體方針，據以結合軍事戰略構想並支持國家戰略，使敵不敢輕易犯我，以鞏固我國家安全，實為下一場戰爭致勝之關鍵。

作者簡介

王佩陸上校，陸軍官校80年班、陸軍指揮參謀學院年班、戰爭學院100年班。現任陸軍學院戰略教官。

英國二戰時蘭卡斯特轟炸機(照片提供：舒孝煌)