國立政治大學國際事務學院

戰略與國際事務碩士在職專班碩士論文

指導教授：李登科博士

中共發展網路戰之研究

研究生：王清安　撰

中華民國一百零三年五月

謝誌

筆者自 2010 年踏入政治大學學習戰略與國際事務相關課程，迄今已近四年，而本論文之付梓，正象徵一個求學階段的跨越。一路走來，得到許多貴人的協助，筆者謹以此誌，敬表謝忱。

首先，本文承蒙恩師李登科教授悉心指導，方得以順利完成。回想本文撰寫初期，筆者內心充滿緊張與恐懼，深怕因自己能力不足與參考文獻有限，而無法如期完成。所幸在恩師指導下，本文得以完成。恩師學識淵博，思想新銳，在學習研究與為人處事等方面，惠我良多。此外，選寫本文過程中，正逢筆者職務調整之際，恩師除教授課業外，並時時給予鼓勵。對於恩師的提攜與關懷，筆者將永誌不忘。

其次，筆者也相當感謝兩位口試委員-國防大學管院院長曹雄源將軍與本校俄羅斯研究所王定士教授。曹將軍以軍中長輩，慷慨將其著作《戰略透視:冷戰後美國層級戰略體系》等十餘本專書相贈，讓筆者得以參考相關寶貴文獻。另外王教授以數十年教學研究經驗，指正學生撰寫本文不足之處，謹此敬申謝忱。

再者，筆者也要感謝政大外交系全體教師及系上助教儀芳與文琪，對筆者求學與研究期間的教導與鼓勵。最後，要深深感謝內人佩倩，在我求學過程中默默的支持與加油，

當然，筆者更必須感謝雙親與我尊敬的大哥及大嫂，他們始終如一的關愛與支持，永為筆者策進之動力，筆者也謹將此論文獻給摯愛的雙親、大哥與大嫂。

王清安　謹誌

2014 年夏於國立政治大學

政大綜院，遙望貓空山光嵐影

摘　要

2013 年 2 月，美國一家網路安全公司公開指出，中共的網軍就是位於上海浦東的共軍總參謀三部第 61398 部隊。消息傳出後，各界議論紛紛，因為中共的網軍被認為是竊取許多國家軍事及商機密的元凶。

到底網路戰對戰爭有何影響？網路戰與不對稱作戰的關係為何？中共何時開始發展網路戰？其戰力如何？我國又應如何對抗中共的網路戰威脅？本文的目的即在探討這個重要的問題。

關鍵字:中共網軍、網路戰、不對稱作戰、國家安全、駭客、病毒、基礎設施。

Abstract

In February 2013,Mandiant Network Road Security Company,an American cyber security company,indicated that the People's Republic of China(PRC)had set up a cyber force located in Pudong,Shanghai. The special force,codnamed 61398 unit,belonged to the third department of the General Staff of the People's Liberation Army .When the American company revealed this information,heated debates took place in many parts of the world because of the fact that the PRC's cyber force was responsible for numerous cyber attacks against foreign military and business networks over the years.

How important is the cyber warfare to the modern war？ What is the relationship between cyber warfare and asymmetric warfare？When did the People's Republic of China(PRC) ,begin to develop cyber warfare capability？How is the capability of the PRC's cyber forces？And how should we do in dealing with the threat from the PRC's cyber warfare？ The purpose of this essay is to study these important issues.

Keywords:PLA cyber forces.cyber warfare, asymmetric warfare, national security, hackers, viruses, infrastructure

目錄

表次

圖次

第一章 緒論

第一節 研究動機與目的

一、研究動機

美國未來學家「托夫勒」(Alvin Toffler)預言:『電腦網路的建立與普及將徹底改變人類生存及生活模式，誰掌握了信息，控制了網路，誰就將擁有整個世界』。[1]在全球化中最重要的一個特質，莫過於網際網路，網路可將各式載具、武器所獲情資，即時整合分享給所需要的指管機制，如果能癱瘓、破壞敵人的網際網路，戰爭可能幾個小時就會結束。[2]美國著名軍事預測學者亞當斯(James Adams)在其著作《下一場世界戰爭》一書中，亦曾預言:『在未來戰爭中，電腦本身就是一種武器，前線無處不在，戰爭控制權將不是砲彈和子彈，而是電腦網路』。[3]

2009 年 5 月，美國公開宣布將陸、海、空軍及陸戰隊之網路部隊整合成一支網絡司令部(Cyber Command)，並受美國「戰略司令部」指揮與管制。[4]隔年 2 月，美國國土安全部向國會遞交的〈四年度國土安全報告〉指出，網路安全將列為美國國土安全五項首重任務之一。[5]2012 年 11 月 19 日，美國國防部長潘內達(Leon Panetta)於紐約表示:『網路是未來戰場』。[6]此外，在 2008 年英國政府宣布成立網路安全作業中心，建立一支擁有反擊能力的網路部隊，並於 2010 年國安戰略會議中，決議投入 6 億 5,000 萬英鎊，將網路安全列為第一要務。[7]2013 年 2 月 3 日美國「紐約時報」(New York Times)報導，網路武器已成為當今最新的軍備競賽。[8]這些事例顯示，網路戰的重要性已確實增加。

首次把網路攻擊手段引入戰爭的是 1991 年的波灣戰爭。該場戰爭前，美國中央情報局(Central Intelligence Agency,CIA)派特工人員到伊拉克，將伊拉克從法國購買的防空系統使用的印表機晶片換上了染有電腦病毒的晶片，其目的使伊拉克防空指揮中心主電腦系統程序錯亂，進而指揮失靈。[9]根據 2013 年俄羅斯資安專家、同時也是卡巴斯基實驗室執行長卡巴斯基(Yevgeniy Valentinovich Kasperskiy)的爆料，俄羅斯的國際太空站因 USB 硬碟而感染了病毒，如同 2010 年，伊朗核電廠也因 USB 而遭電腦病毒 Stuxnet 感染(代號為「奧運」(Olympic Games))。從上述案例顯示，現行網路攻擊手段已不再是網路竊取、拒絕服務及垃圾郵件，而是提升至可以癱瘓、摧毀國家重要基礎設施，影響層面擴及至國家

---

[1]東鳥，《中國輸不起的網路戰爭》，北京:中南出版傳媒集團，2010 年，頁 2。
[2]蕭示恩，〈符合戰略需求提升國家競爭力長役期發揮戰力-裨益國家發展需求〉，《青年日報》，2012 年 1 月 9 日，引註劉德海於 2012 年青年日報社舉辦「平募戰徵 戰力升級 打造精銳新國軍」專題座題。
[3]張蜀平、禚法寶、王祖文，《直面信息化戰爭》，北京:國防工業出版社，2007 年，頁 54。
[4]楊立傑、劉淑萍、劉強，〈 美國概況 〉，《新華網》，＜http://big5.xinhuanet. com/gate/big5/news.xinhuanet.com/ziliao/2002-01/28/content_ 257426_2. htm＞(2013 年 12 月 2 日)。
[5]〈 美網路風暴演習凸顯建構資安環境重要〉，《青年日報》，2012 年 10 月 14 日，版 7。
[6]〈 未來戰場在網路〉，《青年日報》，2012 年 11 月 20 日，版 7。
[7]沙沙著，〈網路版朝鮮戰爭爆發-兩韓網路戰對抗升級〉，《亞太防務》，第 61 期，2013 年 3 月，頁 22。
[8]Dindo Lin 著，〈卡巴斯基 CEO 爆料:俄國太空站與核電廠曾遭病毒入侵〉，《科技新報》，http://technews.tw/2013/11/14/kaspersky-ceo-stuxnet- iss -nuclear-plant/ (2013 年 11 月 22 日)。
[9]東鳥，《中國輸不起的網路戰爭》，北京:中南出版傳媒集團，2010 年，頁 42。

安全層級。故未來要摧毀、破壞一個國家的基礎設施，將不必透過轟炸或派員實施摧毀、破壞，僅須藉由遠端的鍵盤，即可如同武器般向敵實施攻擊，而受攻擊的國家，還無法辨識攻擊來自何方。

2013 年，俄羅斯資安專家卡巴斯基透露，全球有一半的惡意軟體來自中共。[10]同年 1 月 31 日，美國國防部長海格(Chuck Hagel)在國會聽證會指出，中共大規模竊取美國科技、智慧財產及商業資訊，將威脅美國軍事優勢及影響國家安全。[11]據美國谷歌(Google)董事長施密特(Eric Emerson Schmidt)新書《新數位時代》(The New Digital Age)揭露，中國政府與國營企業為取得政治與經濟優勢，不惜利用網路犯罪，入侵外國企業網路，在網路全面化的世界裡，中共是一個既危險且具威脅性的強權。[12]另根據報導，近期華爾街日報《Wall Street Jurnal》網站遭中共駭客人侵，其目的不在取得商業利益，而是要監督該報對中國的事務報導。[13]由此可知，中共發展網路戰手段已日趨成熟，其影響範圍包含政治、經濟、心理及軍事等國家安全議題。

2013 年 4 月 29 日，我國國安局副局長張光遠於立法院質詢表示，中共為全面掌握我國防、政治、外交、兩岸等發展動態，網路攻擊對象將以我國較疏於防護網路節點，或車量交通號誌設備、寬頻路由器、工業微電腦控制器等嵌入式系統裝備為主要攻擊，以取代以往政府機關、駐外館處，轉向民間智庫、電信業者、委外廠商等，預判未來恐將擴及我國關鍵基礎設施與個人。[14]張副局長的透露，顯示中共並不因兩岸關係和緩而放棄謀我之企圖。事實上，這種無煙哨的網路戰爭，已逐漸成為中共謀我之手段。因此，知己知彼，正是筆者撰寫本論文第一個動機。

儘管網路戰如此重要，截至 2013 年 11 月 22 止，根據我國期刊統計，僅有 21 篇有關中共網路戰之文獻，其中僅有一篇探討中共網路戰之網軍，餘均側重於中共網路戰(信息化)發展與中共信息戰之理論，對中共「網軍」編制、作戰模式等，則鮮少觸及與研析，而這也是正是本人撰寫本論文之另一主動機。

[10]Dindo Lin，〈卡巴斯基 CEO 爆料:俄國太空站與核電廠曾遭病毒入侵〉，《科技新報》，< http://technews.tw/2013/11/14/kaspersky-ceo-stuxnet- iss -nuclear-plant/ > (2013 年 11 月 22 日)。
[11]〈中國網路竊取 威脅美軍事優勢〉，《民眾日報》，2013 年 2 月 2 日， 版 4。
[12]〈中國是全球是最危險的超級強權〉，《聯合報》，2013 年 2 月 3 日， 版 4。
[13]張沛元，〈中國網軍危駭 美擬積極反制〉，《自由時報》，2013 年 2 月 2 日， 版 18。
[14]〈 立法院第 8 屆第 3 會期外交及國防委員會第 20 次全體委員會議記錄〉，《 立法院公報》，第 102 卷，第 29 期， http://lis.ly.gov.tw/lgqrc/lgqrkm1?4^850847759^15^^^1022902^1-62^102 卷 29 期 ^@@14047(2014 年二月 9 日)。

二、研究目的

探討中共網路戰「網軍」的發展、優點與弱點，不僅有助於我們瞭解中共網軍的規模、作戰能力，而且也有助於評估中共對我的安全威脅，有鑒於此，本論文之研究目的如下:

(一)探討現今網路戰對戰爭的重要性。網路戰與不對稱作戰的內容及關係為何？為何重要？這是本文第一個要探討的問題，也是第一個研究目的。

(二)瞭解中共發展網路戰之經過，以及與其國家安全之關係。中共何時開始重視網路作戰？如何發展網路戰？本文的第二個研究目的，即為研析此一問題。

(三)評估中共網路作戰之能力及其優、缺點。中共「網軍」的規模多大？其編制、經費為何？戰力又為何？本文第三個目的即在探究這幾個問題。

(四)提出我國之因應建議。當中共以國家資源支撐駭客鑽研技術，積極發展網路戰之際，我國應如何因應，俾能化解中共對我進行網路戰之威脅，的確刻不容緩，而也是本文另一重要研究目的。

第二節　研究途徑、方法研究、章節安排與研究流程

一、研究途徑

社會科學研究包括理論(theory)、資料蒐集(data collection)，以及資料分析(data analysis)等三大層面。[15]其中資料蒐集和資料分析牽涉到研究方法(research method)與研究途徑(research approach)的選擇與應用。依照方法論(methodology)上的界說，研究途徑與研究方法實為兩物，不能混為一談。[16]米勒等學者(Delbert C.Miler,Neli J.Salkzna)在《研究設計與社會評會手冊》(Handbook of Research Design and Social Measurement)乙書指出兩者的差異，研究者必須先確定所要採取的研究途徑，然後才能選擇所要的研究方法。[17]

載克(Vernon Van Dyke)在其所著《政治學:哲學的分析》(Political Science:A Philosophical Analysis)乙書曾指出，所謂「研究途徑」是指選擇問題運用相關資料的標準(criteria for selecting and utilizing data)，研究途徑宜採一種(若有必要亦可採二種研究途徑，但不宜過多)。「研究途徑」乃指研究者對研究對象的研究，到底從那個層次為出發點、著眼點、入手處，進行歸察、歸納與分析，其可幫助吾人決定所要切入的面向，並選擇適當的理論來作為研究的依據。[18]本文主要探討中共發展網路戰能力，作戰方式、能力評估及未來發展，所產生的威脅與我國因應之道，涉及多種不同領域，因此在研究途徑上採「跨學科整合途徑」(inter-disciplinary approach)。

二、方法研究

所謂「研究方法」是指蒐集資料的方法。[19]從事研究，無論自然、人文、社會科學之學術著作，皆著重觀察與分析、解釋問題與現象、探討原因與結果、符合理論與邏輯等。而「方法」就是研究者為了要達成認識世界和改造世界的目的，必須採用一切工具、方式、手段與程式的總稱。[20]「研究方法」所指便是蒐集與處理資料之手段和過程，本文的研究方法採文獻分析法及歷史研究法，茲扼要說明如下:

(一)文獻分析法：所謂文獻分析法就是使用各種既存的史料檔、官方書籍及回憶錄等資料，來發掘事情真相，或印證某些主觀的看法。文獻資料的來源包羅萬象，可以是政府部門的報告、工商業界的研究、文件記錄資料庫、企業組織資料、圖書館中的書籍、論文與期刊、報章新聞等。其分析步驟有四，即閱讀與整理(reading and organizing)、描述(description)、分類(classifying)及詮釋(interpretation)為一種層次化的客觀界定、評鑑與綜合證明的研究方法，確認過去事件的真實性，主要目的在「瞭解過去、洞悉現在、預測未來」。[21]在緒論中所做的文獻探討，旨在說明此主題上目前已有

[15]李美華等譯，Earl Babbie 原著，《社會科學研究方法（上）》，台北：時英出版社，1998 年 2 月，頁 18。
[16]朱宏源主編，《撰寫博碩士論文實戰手冊》，台北：正中書局，2000 年 4 月，頁 184。
[17]同前註。
[18]同前註。
[19]同前註。
[20]曹雄源，《戰略透視:冷戰後美國層級戰略體系》，台北:五南圖書出版社，2013 年，頁 15。
[21]葉至誠、葉立誠，《研究方法與寫作》，台北：商文化出版社，2001 年，頁 102。

的研究，或是已知道的內容，進而描述需要執行本研究的理由。另一部份所做的文獻探討，主要在顯示研究者對此主題的熟悉度，整理與評論相關文獻，以為自己的研究主題、內容和方法尋求合理的立論點。因此，文獻分析法目的在幫助吾人分析和解釋資料，與本研究的結果互動討論，並引發未來研究的方向。[22]在資料蒐集採取此一研究方法，雖然國內針對中共網路戰之專書不易見，但英、美各國對中共網路戰發展的相關書籍及期刊文物卻不缺乏，加上各類相關官方機構或民間學術網站資訊，透過廣泛收集整理後，仍可瞭解到中共網路戰起源、發展背景，並進一步分析其網軍編組、預算及作戰模式。本文研究過程，將廣泛收集文獻資料(如中、英文件、專書、學術期刊、報紙、雜誌及網路資料)，尋找有關中共發展網路戰重要部份，再將資料整理、分析、比較及歸納，透過描透、探索、解釋與演譯的過程，得到整體歸納與比較分析方式。[23]使論文接近客觀、全面、完整的探索與結果，期對中共發展網路戰獲得全般性瞭解。

(二)歷史研究法：歷史研究緣起於歷史學，是透過有系統地收集史料，回溯過去的某項議題或重要事件，透過深入瞭解和詮釋，以對目前的現象與問題有更清楚的理解。俗話說：「前事不忘，後事之師」，藉由歷史研究，讓我們得以鑒往知來。[24]本文在資料陳述方面，將採取此一方法。透過閱讀過去中共網路戰的相關史料，發覺其中的因果關係，並在重建過去的同時，找到中共發展網路戰的歷史轉折關鍵因素。

[22]鈕文英，《教育研究方法論文寫作》，台北：雙葉書廊，2007 年 1 月，頁 311。
[23]郭華倫，《關於研究中國大陸之方法》，《中共問題集》，台北:政大國關中心，1982 年，頁 392-393。
[24]同註 22，頁 117。

(三)章節安排

本論文總計六章，第一章為緒論，說明研究動機與研究目的、研究方法、研究範圍、資料來源與限制、文獻回顧、章節安排與研究流程等。

本文第二章為網路戰與不對稱作戰之探討。第一節，將說明網路戰與不對稱作戰的定義;第二節，說明網路戰與不對稱作戰之關係;第三節探討網路戰的重要性與作戰方式，並以美軍發展網軍編組與網軍預算為主要說明對象，並輔以英、日、韓、以色列等國家，以證明網路戰重要性;另說明網路戰的作戰方式。

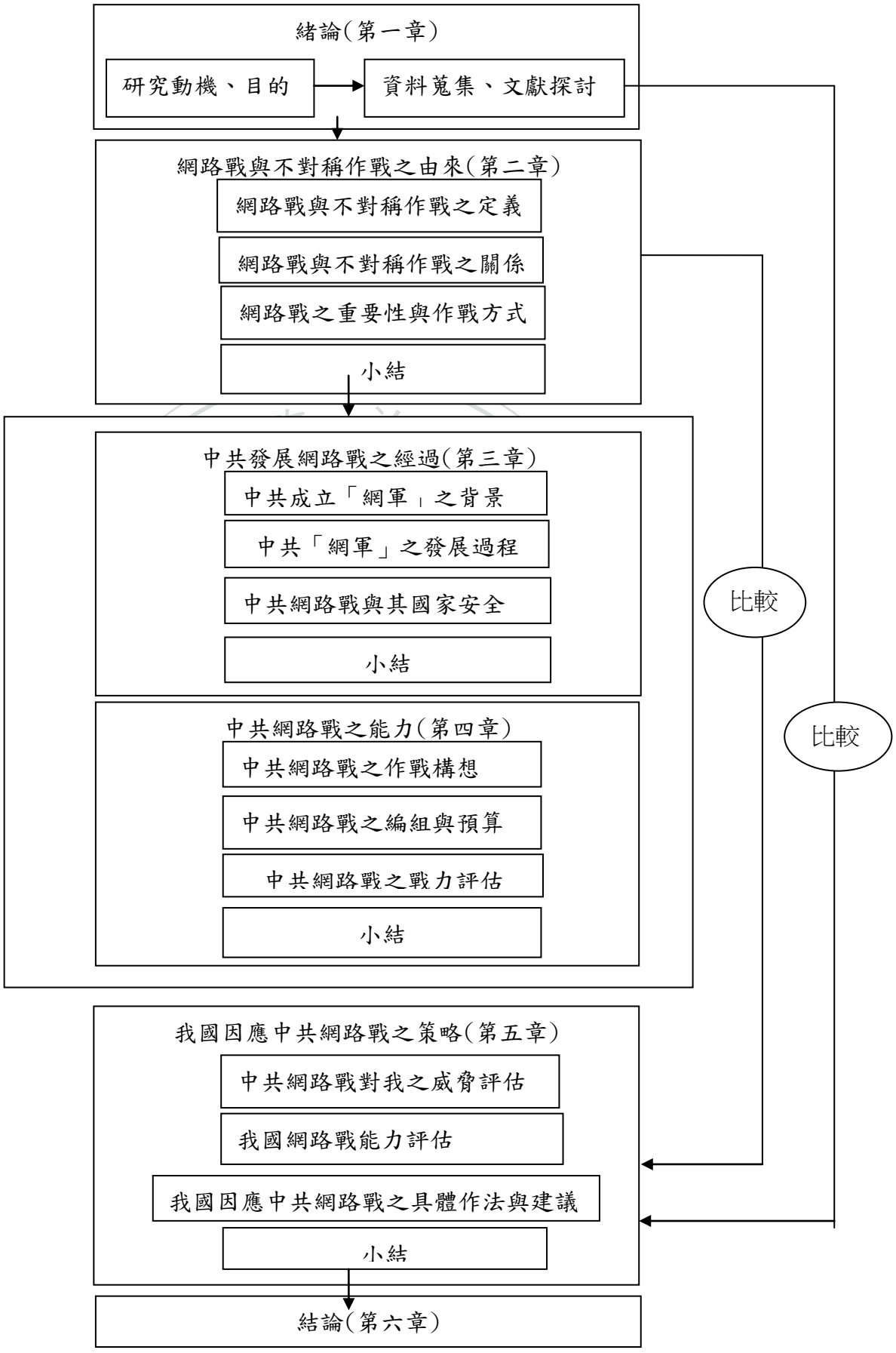
第三章為探索中共發展網路戰之經過。第一節，探討中共成立「網軍」的背景;第二節，說明中共「網軍」發展過程;第三節，說明網路戰與中共國家安全之關係。

第四章為評估中共網路戰之能力。第一節，分析中共網路戰之作戰構想;第二節，說明中共網軍編組及網軍預算;第三節為中共網路戰之戰力評估，從中共網路戰作戰構想及網軍編組、預算，分析出中共網軍作戰能力優、缺點。

第五章則依據第三、四章之研究結果，提出我國因應中共網路戰之策略。第一節，為中共網路戰對我威脅評估;第二節，為我國網路戰能力之評估;第三節為我國因應中共網路戰之具體作法與建議。

第六章是結論。將針對論文之研究目的提出研究心得。並對我國因應中共網路戰發展，提出具體建議。

(四)本論研之研究流程如下:



第三節 研究資料與限制

有關中共發展網路戰之中國大陸出版品，包括一般民間學術刊物之論述及軍方之出版品，為掌握中共軍方之立場，本研究將積極蒐集軍方及官方之文獻，如解放軍軍事科學院、解放軍國防大學等機構出版之刊物、解放軍報及人民日報，以及中共國防白皮書等。另外，國內外專家學者的相關著作亦為研究資料來源。

二、研究限制

本文研究之文獻來源係來自國內、外，及中共軍方公開發行的相關刊物及媒體資料，然而中共與軍方期刊係對內發行，不接受海外個人的訂閱。目前國內僅有國防部與政大國關中心等構機，對於中共的軍事期刊有較完整的蒐羅。惟因網路戰涉及國家安全屬國軍機密，國防部之資料僅允許內部人員查閱，因此政大國關中心陳列之軍事期刊，乃為本研究資料之主要來源。

本文以宏觀的角度為論述之基點，凡涉及軍事參數及性能數據等資料，除非業經公開且有文獻可證明者之外，本文均不引用，以避免涉及洩漏或國家機密的疑慮，而觸犯相關法定。

第四節 文獻探討

文獻探討有助於確定論文研究重心，並助了解他人如何研究類似的問題，吸收寶貴的經驗與防止同樣錯誤，[25]與本研究主題相關之文獻如下:

(一)超限戰與不對稱作戰

1. 1999 年，中共二位空軍大校喬良及王湘穗提出備受矚目的「超限戰」。書中表示，隨著資訊技術的出現，戰場空間將發生根本性的改變，從陸、海、空、天，延申至「人造空間」，作戰人員不再是職業軍人，而開始呈現出「平民化」傾向，作戰手段將超越傳統範圍的新戰爭型式，除傳統戰爭手段外，同時也包括貿易戰、金融戰及新恐怖主義網路戰。戰爭的目的，從武力手段強迫敵方接受自己的意志，轉化為用一切手段，包括暴力及非暴力、軍事和非軍事、殺傷及非殺傷等手段，以滿足自己的利益與安全。[26]故「超限戰」旨在超越一切傳統戰爭形式，以各種方式打擊敵人，並強調了技術在未來戰爭的重要性，以不流血手段達到傳統戰爭不可能達到的效果。

2. 資訊戰與不對稱作戰

(1)2000 年，美國專研中共軍事專家柏理斯(Mark Burles)及夏勒斯基(Abram N.Shulsky)兩位學者發表論文〈高技術條件下的局部戰爭〉認為，中共現今發展的網路戰最為與眾不同，乃在強調對敵人之資訊或電腦系統發展「軟」攻，以作為不對稱戰略的基礎，而這種戰略最主要的就在對付一個比自己擁有更為強大傳統軍軍力的敵人。[27]

(2)2005年，林宗達先生在其專書《以劣勝優-中共信息戰之不對稱作戰》指出，中共信息戰之不對稱作戰，為充分瞭解敵方使用資訊戰手段，從而找出其弱點，做為發動攻擊準備，以達極小傷害、獲致極大成果的以劣勝優之法。但因資訊系統本身存有系統脆弱性和易毀性，從戰略、作戰角度來看，過份依賴資訊及網路的國家，相對而言，也亦遭網路戰攻擊的脆弱性也就提高。[28]故中共認為美軍過於依賴資訊科技與裝備，將嚴重成為軍事弱點，針對這個軍事強國的致命缺陷，發展信息戰爭相關作戰的武器系統，以摧毀美國所依賴的龐大精密的網路系統，達到以劣勝優，以小搏大之目標。

(3)2012年，我國國防大學林明武上校在《國防雜誌》所發表的〈國軍應用「通資電」科技於不對稱戰力之研究〉指出，面對來自太空、空中、地面、水面以至水下等多維的威力，我國應以網狀化作戰的先進概念為核心，運用通資電不對稱戰力，發揮資訊優勢，進行不對稱戰力之建構，達成以小搏大、避實擊虛、以弱擊強的目的。[29]

(4)2013年，中華戰略協會梁華傑先生在其論文〈資訊時代戰場如何優劣轉換及

[25]《軍事論文研究方法教材》，國防大學陸軍指參學院，頁 26。
[26]喬良、王湘穗，《超限戰》，台北:左岸文化出版社，2004 年，頁 111-129;188-196。
[27]國防部史政編譯局譯，〈高技術條件下的局部戰爭〉，《中共動武方式》，台北:國防部史政編譯局，2000 年，頁 69。
[28]林宗達，《以劣勝優-中共信息戰之不對稱作戰》，台北:晶典文化出版社，2005 年。頁 52-59。
[29]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 27 卷，第 4 期，2012 年 7 月，頁 88-89。

以小搏大〉強調，資訊化戰爭的戰場主動權，係為精準快速掌握戰場資訊，無論是集中兵力或火力都必須依賴即時的資訊。故無謂是制空權或是制海權都必須奪取制資訊權，掌握資訊化戰爭的優劣轉化之機，發揮主觀能動性，才能趨利避弊，揚長避短。此外，處於劣勢或相對較小的一方，也可藉由發展網路戰以削弱敵的優勢。[30]

(二)美國網路戰之發展

1. 2001 年，美國阿爾吉拉(John Arquilla)、朗斐德(David Ronfeldt)二位在主持的「網路及網路戰」(Networks and Netwars)研究報告指出，網路的興起意味著非國家行為者擁有了權力，也意味經由網路交戰的衝突可能日漸增加。此外，以網路為基礎的衝突與犯罪型態將成為未來的主要現象。網路戰行為者將屬非國家行為，由無政府組織之電腦駭客發起，最終將演變成「新層次戰爭」(neo-cortical)及「認識論」(epistemological)，網路戰以迷惑、誤導百姓對其文化、社會及政府本質的基本信仰為目標。[31]

2. 2008 年，美國學者阿米里特德(Leigh Armistead)在其著作《資訊作戰》(Information Operation)一書指出，資訊作戰為影響敵方資訊及資訊系統，同時保己方資訊與資訊系統所採取的行動。[32]

3. 2010 年，美國公佈《四年期國防總檢討報告》(Quadrennial Defense Report,QDR)，該報告指出，美國必須改善在反制網路空間威脅方面的能力，積極培養更多的網路專家，以防護及保衛其資訊網路安全。同時，也投資購置及開發最新的科技，使美軍部隊能在各種狀況下使用網路空間。網路指揮部將主導國防部資訊網路的運作與防禦，在獲得指示後，執行全方位的網路空間軍事行動，並加強與國土安全部合作，以強化網路戰反制能力。[33]

(三)網路科技與網路戰

1. 2010 年，中共學者東鳥在其專書《中國輸不起的網路戰爭》表示，首次把網路攻擊手段引入戰爭的是 1991 年的波灣戰爭。該場戰爭戰前，美國中央情報局派特工到伊拉克，將伊拉克從法國購買的防空系統使用的印表機晶片換上染有病毒的晶片，使伊拉克防空指揮中心主電腦系統程序錯亂，進而指揮失靈。其次，在 2007 年愛沙尼亞戰爭期間，俄羅斯藉由電腦病毒入侵銀行網路伺服器，致法無法使用信用卡消費，最後到 2009 年，北韓藉由網路病毒，使韓國國會、國防部、外交部及主要媒體《朝鮮日報》等網站分布式拒絕服務，無法上網。[34]故網路戰的運用階層從軍事提升至國家安全。

---

[30]梁華傑，〈資訊時代戰場如何優劣轉換及以小搏大〉，《尖端科技》，第 352 期，2013 年，12 月，頁 93-97。

[31]國防部史政編譯局譯，約翰.阿爾吉拉(John Arquila)、大衛.朗斐德(David Ronfeldt)，《網路及網路戰》(Networks and Netars:The Future of Terror,Crime,And Militancy)，台北:國防部史政編譯局，2003 年，頁 1-17。

[32]國防部史政編譯局譯，阿里斯德(Leigh Armistead)，《資訊作戰》(Information Operation)，台北:國防部史政編譯室，2012 年，頁 26。

[33]國防部史政編譯局譯，《2010 美國四年期國防總檢討報告》(Quadrennial Defense Review Report)，台北:國防部史政編譯局，2010 年，頁 99-100。

[34]東鳥，《中國輸不起的網路戰爭》，北京:中南出版傳媒集團，2010 年，頁 41-52。

2. 2012 年，美國學者沙卡良(Paulo Shakarian）在其所著〈震網—掀起網空戰爭軍事革命〉專文表示，2010 年伊朗核電廠遭電腦病毒(Stuxnet 震網)攻擊，其影響結果至少拖後伊朗的核計畫至少兩年。Stuxnet 病毒將成為史上第一個可直接破壞現實世界中工業基礎設施的病毒，此舉代表美國成功開啟網路戰的新時代。[35]

(四)中共網路戰的發展與能力

1. 中共最早提出資訊戰的專家是沈偉光，並被譽為中共的「資訊戰之父」，在 1990 年出版名為《資訊戰》乙書指出，『資訊戰』為毀壞敵方的電腦系統，擾亂和摧毀其資訊接收和傳遞機制，乃至金融、電信、能源、交通等，一切與戰爭有關的網路系統，從而使敵方軍心動搖、民心大亂而喪失作戰能力。無聲無息的『資訊戰』還可採用隱蔽或公開的形式，以電腦駭客、電腦病毒、電磁脈衝、微波光柱和鐳射光束等為武器，在敵方毫無知覺或無法防備的情況下實施。[36]

2. 目前西方最重視的共軍資訊戰專家是戴清民少將，他曾任共軍總參謀部通信部部長、總參謀部電子對抗與雷達部部長，軍隊資訊化專家諮詢委員會主任等職。2002 年，在其主編《直面信息戰》乙書披露，網路已成為國家的戰略命脈和戰略資源，一旦重要的網路陷入癱瘓，整個國家安全將面臨崩潰。網路攻擊能力，將是未來衡量一個國家軍事實力的重要指標。此外，當網路戰涉及到廣大民眾，即形成一股網路威懾力量，當敵對雙方都具有侵入、破壞對方網路的能力，就可以帶來雙向的網路遏制，只有形成一定的網路進攻能力，才能有效遏制資訊發達國家的威懾。另外值得一提為「網電一體戰」，此種作戰理論為一種全新的作戰思想，將「電子戰」和「網路戰」兩種手段綜合運用，對敵電子化和網路化的資訊系統進行攻擊，才能最大限度保證己方對資訊的獲取和利用。[37]

3. 張蜀平

曾任中共「國防總裝備部」軍用電子元器件合同管理辦公室主任張蜀平，在與禚法寶、王祖文合著的專書《直面信息化戰爭》中表示，網路戰應分為兩大類，一類是戰略網路戰，另一類是戰場網路戰。平時戰略網路戰是雙方不發生大火力殺傷破壞的戰爭情況下，一方對另一方的金融、交通、電力、民、軍網路系統，以病毒、邏輯炸戰、駭客等手段實施攻擊。另戰場網路戰，則區分狹義和廣義戰場網路戰兩種，狹義為攻擊、破壞、干擾敵軍戰場資訊網路和防護我方資訊網路的作戰行動，廣義為網路中心戰，軍隊所有偵察系統、通信聯絡、指揮控制及各種器裝備整合在一起，網路是作戰行動倍增器。[38]

[35]保羅·沙卡良，〈震網——掀起網空戰爭軍事革命〉，《空天力量雜誌》，2012 年 10 月，頁 35-37。
[36]沈偉光，《資訊邊疆-無影無形的第五邊疆》，北京:新華出版社，2003 年，頁 36。
[37]載清民，《直面信息戰》，北京:國防大學出版社，2002 年，頁 57-60。
[38]張蜀平、禚法寶、王祖文，《直面信息化戰爭》，北京:國防工業出版社，2007 年，頁 97-99。

4. 楊世松

2007 年，中共學者楊世松在其著作《軍事信息能力論》一書中披露，網路戰的資訊技術和核心裝備是用錢買不來，必須組織有關專長，集中力量聯合攻擊，以提高資訊保障核心技術。另外要加快軍事資訊保障基礎設施，建設網路監管中心及應急處置中心，對電腦病毒及駭客進行有效防範及網路定時安全檢查，遭網路攻擊時，第一時間進行反擊，確保我方網路系統能正常運作。[39]

5. 張黎上將、閔振范少將、王保存少將

2007 年，中共解放軍副總參謀長張黎上將主編，及軍事科學院世界軍事研究部長閔振范少將及和研究員王保存少將在共同撰寫的《信息化軍隊的組織體制》乙書指出，隨著各種軍事力量的重新分化組合，各軍種結構將被打破，新的軍種將運運而生，資訊時代的主要軍隊形態，是規模小、質量高，強調軍隊精幹、兵力數量少。資訊戰決定陸、海、空、天戰的勝敗，資訊戰部隊將來可能成為一個新的軍種。[40]

(五)網路戰之作戰方式

2003 年,中共學者王正德在其專書《決勝賽柏空間-網路軍事技術及其運用》指出，網路作戰之作戰方式，區分網路偵察、攻擊與防護。網路偵察，其重點為重點網站偵察、網址偵察、網路密碼偵察，及世界各國重要的網路技術發展、動向偵察。網路攻擊，在信息基礎設施上投擲信息器，利用、獲得、失效或摧毀對手基礎設施。如偷竊安全性信息、干擾服務、破壞數據，其攻擊運用手段為加重超載負荷堵網(潛伏病毒攻擊法)、注入傳染病癱網(固態病毒攻擊法)、釜底抽薪的斷電制網(空間注入病毒法、有線節點攻擊法)、精準打擊擊節破網(納米機器人攻擊法)等。網路防護為建立網路預警系統、自主的信息網路及構築網路防護柵欄，防止駭客入侵、病毒侵害，及防止網路受到襲擊。[41]

[39]楊世松,《軍事信息能力論》，北京:軍事科學出版社，2007 年，頁 144-148。
[40]張黎,《構建信息化軍隊的組織體制》，北京:解放軍出版社，2004 年，頁 37-42。
[41]王正德,《決勝賽柏空間-網路軍事技術及其運用》,北京:軍事科學出版社,2003 年,頁 197-201。

第二章　網路戰與不對稱作戰

2001 年，美國學者阿爾吉拉(John Arquilla)、朗斐德(David Ronfeldt)二人在主持的「網路及網路戰」(Networks and Netwars)研究報告指出，網路戰與資訊戰爭(Information war)、資訊作戰(Information operation)、戰略性資訊戰、網際網路戰爭、資訊破壞行動(cybotage，破壞資訊設施為主)等名詞同義，[42]到底資訊作戰、網路中心戰以及信息戰的意義為何？網路戰的定義又為何？網路戰與不對稱作戰是否相同？網路戰有何重要性？科技發展對網路戰有何影響？本章將逐一探討這幾個問題。

第一節　網路戰與不對稱作戰之定義

一、資訊作戰、網路中心戰與信息戰

(一)資訊作戰：「資訊作戰」乙詞最早於 1996 年，由美國學者阿米里特德所提出，其定義為『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。』[43]該定義，並於 1998 年正式納入美軍準則「第 3-13 聯參之部」資訊行動範疇。[44]2012 年，中共學者陳恒、胡成軍在二人合撰論文-〈美軍資訊戰理論的發展及啟示〉中指出，資訊作戰為『在軍事行動中，整合運用與資訊相關的能力，影響、擾亂、破壞或者篡奪敵方和潛在對手的決策能力，同時保護己方。』[45]

(二)網路中心戰:我國國防大學 2008 年出版之《美國國防暨軍事戰略》一書中說明，網路中心戰為藉資訊與通信技術，將分散的部隊整合在一起，經由資訊系統及有用的資料鏈結，並以網路為中心的作戰，彼此分享有用資訊、情資及具彈性的作戰構想。[46]

(三)信息戰:中共最早提出信息戰的專家是沈偉光。在 1996 年沈偉光對「信息戰」下的定義是：『交戰雙方通過控制資訊與情報資源來爭奪戰場主動權的戰爭』。[47]1998 年中共軍事科學出版社出版的《高技術條件下的信息戰》一書指出，信息戰為敵對雙方使用信息技術手段、裝備、系統實施的作戰行動，通過信息武器與其它武器的綜合運用，爭奪信息優勢並形成戰術、戰略優勢，以達到戰爭目的一種新的獨特的戰爭形態。[48]2000 年，中共王普豐少將認為，信息戰為對敵信息及信息系統實施竊取、篡改、刪除、欺騙、擾亂、阻塞、干擾、癱瘓等一系列的入侵活動和電腦病毒攻擊，最終使敵

---

[42]國防部史政編譯局譯，約翰.阿爾吉拉(John Arquila)、大衛.朗斐德(David Ronfeldt)，《網路及網路戰》(Networks and Netars:The Future of Terror,Crime,And Militancy)，台北:國防部史政編譯局，2003 年，頁 5-6。

[43]國防部史政編譯局譯，阿米里特德(Leigh Armistead)，《資訊作戰-以柔克剛的戰爭》(Information Operations:Warfare and the Hard Reality of Soft Power)，台北:國防部史政編譯室，2008 年，頁 26。

[44]同前註，頁 95。

[45]陳恒、胡成軍著，〈美軍資訊戰理論的發展及啟示〉，《艦船電子工程》，第 32 期第 11 卷，2012 年第 11 期，頁 35-36。

[46]曹雄源，《美國國防暨軍事戰略》，桃園:國防大學，2008 年，頁 35-36。

[47]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(2008 年 04 月 27 日)

[48]李承瑀，《中共高技術條件下信息戰之研究》，政治作戰學校政治研究所碩士論文，2000 年 6 月，頁 139。

方電腦網路無法正常工作。[49]

二、網路戰

(一)美國:2001 年，由美國阿爾吉拉及朗斐德等兩位學者認為，網路戰為非國家行為，是由無政府組織之電腦駭客發起，最終演變成「新層次戰爭」(neo-cortical)及「認識論」(epistemological)。[50]此外，美軍 3-13 號聯戰出版品指出，網路戰為資訊戰核心戰力，是以阻斷、擾亂或破壞電腦與電腦網路或儲存之資訊，包含電腦網路攻擊、電腦網路防禦，及電腦網路運用。[51]

(二)中共:2003 年，被稱為中國首席軍事評論家張召忠將軍，在其著作《網路戰爭》乙書強調，在網路戰屬於信息戰範疇，而信息戰又分為戰略信息戰和戰術信息戰兩大類，所謂戰略信息戰有的稱做為戰場之外的信息戰，通過破壞或操作電腦的信息流的辦法，對敵人的電話網、油氣管道、電力網、交通管制系統、國家資金轉移統、各種銀行轉帳系統和衛生保健系統等實施破壞，以達到戰略目的;戰術信息戰，運用信息技術手段和各種信息化彈藥、信息化作戰平台和 C4ISR 系統，在偵察探測預警、信息處理與傳遞、器控制和制導、作戰指揮與控制、偽裝欺騙干擾與軍事謀略等方面開展的對抗與戰鬥。[52]2009 年，由隸屬於中國共產黨中央委員會紅旗出版社出版的《中國信息安全報告-預警與風險化解》一書強調，信息戰有多種樣式，主要有網路戰、電子戰、心理戰等，其中網路戰是信息戰的主體，廣義上，網路戰涉及政治、經濟、軍事等國家生活的各個領域，包括平時及戰時，狹義指為軍事領域或與戰爭有關的網路戰，為對敵對雙方透過民用或軍用網路，主要利用計算機技術偵察、獲取、干擾、破壞對方指揮、武器系統的重要信息，從而達到影響、加速甚至決定戰爭進程的行為。[53]

(三)中華民國:2013 年，國內學者林穎佑指出，網路戰是指利用網際網路作為攻擊的媒介，資訊戰概念底下的一種攻防型態，是資訊戰的一種特殊發揮形式。[54]另依中共學者及近期國內研究中共信息戰學者之看法，中共網路戰即為信息戰一環。[55]綜合上述，筆者認為網路戰，即為透由有、無線電等網路傳輸手段、或特攻人員及先進電子科技武器，對敵人網路節點、資訊系統(含機房)及儲存資料實施實體及虛擬(雲端伺服器)攻擊，以獲取或竄改所需情報、癱瘓、摧毀敵國重要基礎設施，進而使敵人無法及時產生正確重要決策，或造生人民恐慌而影響政府機制運作及國家整體安全，達到不戰而屈兵之目標，同時保護己方資訊及資訊系統(含基礎設施)，不受敵人所影響。

---

[49]沈偉光主編，《中國信息戰:知名學者聚焦信息戰權威專家解讀信息化》，北京:新華出版社，2005 年，頁 36。

[50]同註 42，頁 7-16。

[51]黃文啟譯，Balne R.Clark，〈以資訊戰做為武裝衝突嚇阻手段〉(Information Operations as a Deterrent to Armed Conflict)，《國防譯粹》，第 37 卷，第 12 期，2010 年 12 月，頁 6。

[52]張召忠，《網路戰爭》，北京:解放軍出版社，2001 年 1 月，頁 87-90。

[53]潘小剛、周亞明、肖琳子，《中國信息安全報告-預警與風險化解》，北京:紅旗出版社，2009 年，頁 27。

[54]林穎佑，〈大陸網軍與 APT 攻擊〉，《展望與探索》，第 11 卷，第 3 期，2013 年 3 月，頁 97。

[55]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 24-25; 陳漢強、蘇文德，〈中共信息戰之網路攻擊型態研究〉，《新新季刊》，第四十卷第二期，2012 年 4 月，頁 234; 同註 53，頁 27。

三、不對稱作戰

(一)美國:「不對稱作戰」(Asymmetrical Warfare)一詞，首見於 2001 年的《四年國防總檢》(QDR-2001)，其定義為『一方面迴避或削弱對手的優勢，另一方面又利用其弱點，所採手段則截然不同於對手慣用作戰模式之企圖。』[56]在 2000 年，美國學者科普蘭(Thomas E.Copeland)表示，不對稱作戰如同武術，將敵人的優點變成弱點。[57]

(二)中共:中共最早提出不對稱作戰理論，為 1999 年出版的《超限戰》。根據該書的說法，不對稱作戰係運用各種方式打擊敵人，以不流血手段達到傳統戰爭不可能達到的效果。[58]另外，在 1999 年，我國中共軍事分析家林中斌博士指出，中共「信息戰」，為 80 年代的「點穴戰」或「針頭攻擊」的作戰方式，此種接近美方所謂「不對稱戰爭」，採取「以弱戰強，避實擊虛」戰爭哲理。[59]

(三)中華民國:國內學者林中斌教授強調不對稱作戰，是以「戰術手段達成戰略目的」的手段，並以「改變遊戲規則，你打你的、我打我的」各自表述的思考形態。[60]國防大學戰院主任教官謝游麟上校認為，不對稱作戰為『避開敵人強點，集中我方相對優勢(relative dominance)，來對付敵人相對劣勢的一種作戰方式。』[61]而國防大學林明武上校則表示，國軍應以網狀化作戰為核心，運用通資電不對稱戰力，進行不對稱戰力之建構，達成以小搏大、避實擊虛、以弱擊強、以劣勝優的原則。[62]

(四)綜合上述，不對稱作戰就力量而言是以小搏大，就態勢而言，是劣勢一方運用有利態勢，創機、造勢，勝得戰爭勝利。就效益而言，就是用最小的成本，使敵人付出慘痛的代價。

[56]倪耿，〈台式不對稱作戰與戰力組合〉，《亞太防務》，第 63 期，2013 年 1 月，頁 36。
[57]國防部史政編譯局譯，科普蘭(Thomas E.Copeland)，《資訊革命與國家安全》(Information Revolution and Natonal Security)，台北:國防部史政編譯局，2001 年，頁 99。
[58]喬良、王湘穗，《超限戰》，台北:左岸文化出版社，2004 年，頁 111-129。
[59]同註 48，頁 20。
[60]同註 55，頁 38。
[61]謝游麟，〈國軍發展「不對稱」軍事思想之途徑與實踐〉，《國防雜誌》，第 27 卷，第 4 期，2012 年 7 月，頁 54。
[62]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 27 卷，第 4 期，2012 年 7 月，頁 88-89。

第二節　網路戰與不對稱作戰之關係

一、網路戰是不對稱作戰的一種手段

不稱作戰就是敵方利用優異科技能力手段，以精準打擊獲取不對稱優勢，以尋求精準、簡單、價低的戰略力組合，精確計算攻擊所需花費，以期建構損小、廉價、效高的獲勝成功手段，如同美軍一艘軍艦可載面對面飛彈(SSM)2048 枚，同時能接戰百餘公里的多個目標與精準摧毀。另不對稱作戰，也可以是軍事弱國對付強國之戰術手段，藉以小搏大，利用強敵弱點、以智取勝，打擊敵人痛處，以扭轉傳統的強弱關係，進而有效嚇阻防止對手發動戰爭的手段。[63]

網路戰對經濟、社會與實體領域造成的潛在破壞力，如同核子武器威力一般，抵禦網路攻擊如同抵禦核武攻擊，因為攻擊可能採取任何形式、來自任何地方，且靜態防禦將遭巨大或非傳統打擊摧毀;但不同於核子武器的是，網路戰的匿名與散布特性，更加使得嚇阻手段無用武之地。[64]美國學者法加德(David Faggard)即指出，以網路為基礎的資訊戰術，可以運用規模較小、裝備較差的個別部隊行動，以數位媒體影響人數眾數的電子公民，甚至還可運用社交群集戰術來推翻體制、決策者或是關鍵決策。[65]

資訊戰的核心戰略目的就是嚇阻潛在敵人構成之威脅，運用資訊戰做為武裝衝突嚇阻手段，既符合國際法律與道德標準，又可發揮低損耗、高效能的最大戰略效應。[66]在網路化時代，網路已融入社會生活的各個領域，尤其是通信、管理等系統與軍事指揮系統更與國家安全緊密聯繫息息相關，對這些網路攻擊實際也就是對一個國家安全的攻擊。網路戰不但可以「兵不血刃」地破壞敵方指揮系統、情報信息等軍用網路系統，還可以悄悄無聲無息破壞、癱瘓和控制敵方的商務與政府網路系統，最終實現不戰而屈人之兵的效果。[67]2001 年，美國達特茅斯大學(Dartmouth University)的研究人員預測，網路攻擊將成為未來敵對團體和國家的最佳不對稱作戰武器。[68]

從網路戰發展趨勢，各國已體會出網路戰的「不對稱」作戰效益，影響層面不再局限於軍事行動的指管戰，而是提升國家安全的戰略議題。現今資訊科技的快速發展，已為平時及戰時的經濟運作、社會互動與軍事作戰的本質帶來重大的改變。[69]

---

[63]同註 55，頁 37-39。
[64]高一中譯，Soren Olson，〈檯面下較勁:網路戰與戰略經濟攻擊〉(Shadow Boxing: Cyber Warfare and Strategic Economic Attack)，《國防譯粹》，第 39 卷，第 12 期，2012 年 12 月，頁 42-49。
[65]章昌文譯，David Faggard，〈風起雲湧的社會運動:不對稱衝突的隱憂〉(Social Swarming: Asymmetric Effects on Public Discourse in Future Conflict)，《國防譯粹》，第 40 卷，第 10 期，2013 年 10 月，頁 43-44。
[66]黃文啟譯，Balne R.Clark，〈以資訊戰做為武裝衝突嚇阻手段〉(Information Operations as a Deterrent to Armed Conflict)，《國防譯粹》，第 37 卷，第 12 期，2010 年 12 月，頁 4-5。
[67]毛峰，〈日本創建網軍聯美反制中國〉，《亞洲週刊》，第 27 卷，第 21 期，2013 年，6 月，頁 37。
[68]同註 64，頁 45。
[69]國防部史政編譯局譯，史利芙爾(Frank J.Cilluffo)，《網路威脅與資訊安全》(Cyber Threats and Information Security)，台北:國防部史政編譯局，頁，ＸＸⅨ。

二、網路戰的成本比其他不對稱作戰手段低廉

(一)飛機、船艦:美國學者盧福偉(Bernard Loo)指出，因全球軍事事務革新，高科技武器的價格持續飛漲，從 2000 年起，英國國防部規劃建案之 8 億英鎊的「監視者」(Watch keeper)無人飛行載具、兩艘數十億英鎊的新世代航艦、英國空軍高達 130 億英鎊的空中加油機，及陸軍高達總價 60 億英鎊的新世代裝甲車等 20 項主要國防專案的成本亦增加 17 億英鎊，對國防預算造成很大的挑戰。[70]其實，美國國防部也因為新式戰機與戰艦的成本日益高昂，不得不削減許多新式機、艦的建購案。

(二)導彈:不論是攻擊性或防禦性的導彈，成本都很高。以我國為例，根據王志鵬的研究，台灣於 2008 年 10 月 3 日與 2010 年 1 月 30 日自美國購得 444 枚愛國者三型(PAC3)及相關雷達、地面設施等裝備，花費約 59.1 億美元。同時為將 3 個連的舊型愛國者飛彈提升(依據單枚約 70%，雙枚約 90%的攔截率估計，這 550 枚愛國者飛彈，最多也只能夠攔截中共 275 枚來襲飛彈，不過戰時很可能在十數分鐘內即遭摧毀)，我國又得支付 9.3 億美元，如此昂貴的反飛彈建置作為，誠然不符合台灣現有的國防財政和經濟效益。[71]

(三)無人攻擊載具:一般人常認為無人攻擊載具應該很便宜，其實並不便宜。美軍「掠奪者」無人攻擊機為例，成本約略要四、五百萬美元。[72]雖然比一般軍用戰機便宜，但動則花費數百萬美元，仍然是國防上的負擔。

(四)網路戰:2000 年，中共學者張軍表示，網路戰是最廉價的武器。並指出，電腦病毒是一種技術含量很高，且又十分廉價的高技術武器。隨著技術成長，電腦病毒已能破壞敵軍的硬體，利用電腦病毒控制供電系統，讓控制系統瞬時產生高壓，進而達到破壞硬體目的，故網路戰和導彈、核武器將成為戰略武器。[73]美國前國防部副部長林恩(William Lynn)曾說:『敲擊一下鍵盤，就可使訊息在 300 毫秒繞行地球兩圈，但為追查攻擊者而進行的鑑識工作，卻得費時數月。』網際網路已經成為恐怖分子的廉價全球指管網路，不僅擁有數不盡的網路節點，而且完全不需支付日常開銷及保養。[74]相對而言，在第二次波灣戰爭，美軍為擊敗伊拉克的百萬大軍，總共出動 53 萬部隊、2200 輛坦克，數以百計的飛機以及數十艘軍艦，這些人力與裝備上的佈署，耗費的金錢高達 870 億美元。[75]根據美國陸軍戰院戰略研究所《Strategic Studies Institute》2002 年 10 月-2003 年 2 月的研究指出，第二次波灣戰爭美國所付出的代價約 870 億美元，另還須斥資約 1000 億美元對伊拉克實施重建。[76]

---

[70]國防部史政編譯局譯，盧福偉(Bernard Loo)，《軍事轉型與戰略》(Military Transformation And Strategy)，台北:國防部史政編譯局，2011 年，頁 79-82。

[71]王志鵬著，〈面對中國大陸軍力成軍，台海空優成空憂!思維必須大轉變〉，《尖端科技》，第 347 期，2013 年 7 月，頁 11。

[72]羅添彬，〈反制中國 軍方發展無人攻擊機〉，《自由時報》，2012 年 9 月 3 日， 版 1。

[73]張軍主編，《IT 戰爭》，北京:科學出版社，2000 年，頁 169。

[74]高一中譯，G.Stavridis and Elton C.Parker Ⅲ，〈航向網路之海〉(Sailing the Cyber Sea)，《國防譯粹》，第 39 卷，第 8 期，2012 年 8 月，頁 7-8。

[75]丁志宏，《陸軍數字化部隊建設研究》，北京:國防大學出版社，2003 年，頁 56-57。

[76]國防部史政編譯局譯，韓力(Eric L.Haney)、湯姆生(Brian M.Thomsen)，《論 21 世紀戰爭超越震撼與威懾》(Beyond Shock and Awe: Warfare in the 21st Century)，台北:國防部史政編譯局，2010 年，頁 40。

三、網路戰的效益比其它不對稱作戰手段高

2013 年美國知名資訊安全《infosecisland》網站報導指出，只需 15 分鐘的網路攻擊就能讓任何依賴西方資訊技術的社會癱瘓，它既可以攻擊隔壁的目標，也可以攻擊世界另一端的目標，而重建被破壞的社會則需要好幾年的時間。[77]

網路戰是較不血腥，但具有潛在廣大效果的恐怖活動，網路駭客只須利用一具電話或電子郵件連線就足以通達眾多不同電腦。因被偵測到的風險極低，遭受反擊的風險也低。[78]現今要破壞一國的重要目標，如水壩或電力網路，已經不需要像以往花那麼多時間，網路戰所具有的價值，已從以往被認為戰術階層的攻擊，迅速提升成為戰略階層的攻擊。[79]網路攻擊不致於造成人命損失，但資訊之喪失、作業之中斷、文獻之受損、伺服器遭清除等加總起來，損失卻是非常驚人。[80]

2014 年俄羅斯併吞克里米亞半島事件，更證明網路戰是既非血腥但又可達到戰爭勝利的成功案例。根據 2014 年 4 月 21 日《約紐時報》的報導，俄軍在併吞克島的每個階段，均成功的運用網路戰及高度訓練的特戰部隊，以獲得制勝的先機。該報導亦指出，這是 21 世紀嶄新的戰法，行動一開始，俄軍便切斷克島對外通訊電纜，並搭配網路戰，使克島的烏克蘭軍隊與本土隔絕。同時運用網路媒體及流言力量，塑造出在烏克蘭極右派動亂之下，俄軍必須派遣部隊干預，以保護當地使用俄語的民眾的合法性。[81]

此外，據報導，在過去二十年來，駭客從美國企業、大學、政府機關竊取的智慧財產估計約 4 兆美元，誠如前美網路指揮部指揮官亞歷山大中將(Keith B.Alexander)所言:『這是史上最大宗的財富轉移。』2013 年 3 月，美國國防部據報導，遭網路間諜竊取就高達 2 萬 4,000 件檔案。[82]同年 4 月 25 日，據《聯合報》指出，美聯社的推特帳戶，於 2013 年 4 月 23 日下午約 1 點零 7 至 9 分鐘，遭電腦駭客入侵，於網路上發佈兩起假消息，分別為白宮發生兩起爆炸及歐巴馬總統受傷，美國道瓊工業指數大跌 144 點，標準普爾五百指數的市價瞬間損失 1 千 365 億美元(約四兆台幣)。[83]

我國學者陳漢強與蘇文德因此認為，網路戰與軍事作戰相較，網路作戰的成本效益遠遠大於軍事作戰，一個電腦機房、幾部作業主機及少數精通資訊攻防的專業人員，即可透過網路深入敵營輕易竊取重要資訊、從事情報作戰或癱瘓局部區域的資訊作業，達其戰略目的。[84]而中共學者，李健與嚴美也指出，網路戰可以最低的成本投入，獲取巨大的回報，因此，為實施不對稱戰作戰提供了無與倫

---

[77]Jarno Limnéll ,"Resilience – The way to Survive a Cyber Attack,"*infosecisland,* <http://www.infosecisland.com/blogview/23137-Resilience--The-way-to-Survive-a-Cyber-Attack.html> （2013 年 12 月 15 日）。

[78]行政院研究發展考核委員會，《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》，台北:五南文化出版，2002 年，頁 72。

[79]國防部史政編譯局譯，史利芙爾(Frank J.Cilluffo)，《網路威脅與資訊安全》(Cyber Threats and Information Security)，台北:國防部史政編譯局，2002 年，頁 13。

[80]同上註，頁 24。

[81]王熊斌，〈併吞克島 俄盡展 21 世紀新戰術〉，《青年日報》，2014 年 4 月 23 日， 版 5。

[82]王文勇譯，(David Alexander)，〈網路防衛戰略方案〉(A SDI for Cyberspace)，《國防譯粹》，第 40 卷，第 9 期，2013 年 9 月，頁 55-56。

[83]張佑生，〈美聯社遭駭 美股 2 分鐘跌 144 點〉，《聯合報》，2013 年 4 月 25 日， 版 17。

[84]陳漢強、蘇文德，〈中共信息戰之網路攻擊型態研究〉，《新新季刊》，第四十卷，第二期，2012 年 4 月，頁 235。

比的能力。即使相對貧窮的國家或非國家實體，都能隨時獲得必要的工具和接入點對美國構成威脅。[85]綜合正規作戰與不對稱作戰成本、效益之比較，如表 2-1。

表 2-1:正規作戰與不對稱作戰成本、效益比較表

作戰手段 / 區分	正規戰		網路戰
	飛機、艦載	導彈	
攻擊源	容易定位		非常難以定位
速度	與飛機、艦載、坦克相同		光速
效果	物理區域有效		主要對通資系統,物理系統也有副作用
方面	武裝部隊兩方面		個人、小組或一個國家
成本	取決於武器成本		非常便宜，甚至一台電腦
武器	常規武器		用於電腦及軟體
技術要求	需要先進技術		不需要先進的技術，但先進的技術可以增加有效性
攻擊指標	可以探測		多數難以探測
損害探測	戰爭的物理效果容易探測		攻擊的結果多數不可能探測

作者整理

資料來源:國防部史政編譯局譯，盧福偉(Bernard Loo)，《軍事轉型與戰略》(Military Transformation And Strategy)，台北:國防部史政編譯局，2011 年，頁 79-82;王志鵬著，〈面對中國大陸軍力成軍，台海空優成空憂!思維必須大轉變〉，《尖端科技》，第 347 期，2013 年 7 月，頁 11;羅添彬，〈反制中國 軍方發展無人攻擊機〉，《自由時報》，2012 年 9 月 3 日，版 1。

[85]李健、嚴美譯，Larry K.wentz、Charles L.Barry、Stuart H.Star，《網路戰美軍稱霸世界的第五戰場》(Military Perspectives on Cyberpower)，香港:新點出版公司，2010 年，頁 130。

第三節　網路戰之重要性與作戰方式

一、網路戰之重要性

(一)學術界的論點

美國著名軍事預測學者亞當斯在其著作《下一場世界戰爭》一書中曾預言:『在未來戰爭中，電腦本身就是一種武器，前線無處不在，戰爭控制權將不是砲彈和子彈，而是電腦網路』。[86]英國皇家三軍聯合研究院(RUSI)亞洲部主任尼爾(Alexandra David Neel)也曾預測:國際間各國將在不久的將來，在網路空間發動進攻性和防禦性戰爭，粉碎敵人之前的傳統戰爭，未來網路的普及和網路空間的重要性，將帶來全球性的戰略價值。[87]

美國國家安全在第五代隱形空戰及夜戰的科技優勢程度，面對全球下一波生物武器、核彈、網路攻擊、氣候變遷及跨國犯罪等五大威脅，美國沒有做好足以對付這些複雜且多面向威脅的準備。此外，在這五大威脅當中，以網路攻擊對國家安全、公眾安全和經濟帶來最嚴重挑戰。面對這些複雜且日益增多的攻擊手段，美國必需跳脫傳統方法來解決。[88]2013 年，美國另一位學者哈密德(Ahmad Zahid Hamidi)也指出，在近期局部衝突中，任何實體部隊或後勤物質部署前，應爭取網路空間的優勢，並應用於任何階段，直到成功為止。網路戰最終目的乃是造成敵國戰略癱瘓，使其無法運作，攻守一體，乃是網路戰核心所在。[89]同年，杜迪克(Charles E. Dudik)及波爾格(Jesse Bourque)更認為，美陸戰隊應在無人飛行載中隊培養電磁頻譜作戰專家，在分散式酬載且轉移重心至「頻譜管制」的新環境下，由網路/電子作戰協調組擔任主要「戰鬥」職務。[90]

另外，根據 2013 年美國資訊安全《infosecisland》的網站報導，美國國防部國防科學委員會[91]下屬的一個工作組發佈一項名為「彈性軍事系統和高級網路威脅」(Resilient Military Systems and the Advanced Cyber Threat)的最終報告，認為網路是個複雜的領域，沒有銀色子彈能消除利用網路作為力量倍增器所帶來的威脅，也不可能完全防禦多數高級的網路攻擊。但是，類似過去解決複雜的國家安全和軍事戰略挑戰，如二戰期間反制德國的潛艇戰略及冷戰時期的核威懾， 美國國防部需要數年才能建立起對網路威脅的有效防禦，包括威懾要素、任務確保和進攻性網路能力。[92]

---

[86]同註 38，頁 54。
[87]黃基禎，〈中國大陸網路戰思維〉，《中共研究》，第 47 卷第 10 期，2013 年 10 月，頁 148。
[88]章昌文譯，Sandra I.Erwin，〈國家安全未來五大威脅〉(The Five Treats To National Security in the Coming Decade)，《國防譯粹》，第 40 卷，第 2 期，2013 年 2 月，頁 42-43。
[89]梁正綱譯，Ahmad Zahid Hamidi，〈新戰爭型態:網路結合無人飛行載具與新興威脅〉(New Forms of Warfare: Cyber, UAVs and Emerging Threats)，《國防譯粹》，第 40 卷，第 11 期，2013 年 11 月，頁 42-45。
[90]余忠勇譯，Charles E. Dudik ,Jesse Bourque，〈電子戰與網路作戰:未來聯合兵種〉(Electronic Warfare and Cyber Operations)，《國防譯粹》，第 40 卷，第 11 期，2013 年 11 月，頁 23-27。
[91]國防科學委員會是由文職專家組成的一個委員會，為美國國防部提供科技諮詢。這個委員會成員都不是軍工聯合體的代表，他們只代表個人。
[92]Don Eijndhoven,"The Chilling State of Cyber Affairs,"*infosecisland,* http://www.infosecisland.com/blogview/23248-The-Chilling-State-of-Cyber-Affairs-US-DoD-Report.h

在國內方面，重視網路戰的學者也逐漸增加。例如 2012 年 4 月 11 日，李登科教授即警告說，近年來中共不斷提升網路戰力，積極研發病毒與研擬戰術戰戰法及成立網軍作戰單位，企圖透過網路攻擊，竊取政經軍重要機密資料，網路威脅對國家安全已產生嚴重影響。我國政府各部會及國軍，應投注更多的資源及努力專業人才，以嚴防中共發展網路作戰。[93]2014 年 3 月 5 日，國內另一位曾復生教授亦指出，美、中兩大國各依照自己的國家安全考量，積極成立專責的網路戰機構，以爭取網路戰 7 大網路高地領域的制高點，[94]以強化競爭力與綜合實力，並為建立網路空間競爭的優勢地位做好準備。[95]

在另一方面，中共航天機電集團在南京的 8511 研究所，於 2012 年 12 月在《航天電子對抗》雙月刊發表一篇稱為〈空間賽博戰研究〉(Study on Space Cyber Warfare)的論文指出，資訊時代決定戰爭勝敗的關鍵不是核武，而是網路。為此，中共軍方已擬定在太空發動反衛星攻擊及同時動員軍人與平民發起數位網路「人民戰爭」的方法，來打贏這場戰爭，這兩者將是中共軍方咸認可以擊敗美國的兩大王牌。這報告引起美國國防部高度的重視，此外，研究中共軍事事務專長美國學者費學禮(Richard D. Fisher Jr.)即表示，這項報告顯示，中共將投入更多資源在網路戰與太空戰。中共一邊迫切要求簽署太空軍備協議，讓潛在敵手卻除武裝，但同時建立自己的太空軍力。[96]

---

tml(2014 年 3 月 21 日)。

[93]李登科，〈網路攻擊威脅日增 慎防無聲戰爭〉，《青年日報》，2012 年 4 月 14 日， 版 2。

[94]根據美國國防部研究報告指出，網際網路空間至少有 7 個關鍵網路戰略高地，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(Internet Protocol Version 6,IPV6)。

[95]曾復生，〈美中網路戰略七大高地〉，《財團法人國家政策研究基金會》，http://www.npf.org.tw/post/3/13321(2014年3月10日)。

[96]陳維真，〈中國數位人民戰爭 全民抗美〉，《自由時報》，2013 年 8 月 1 日， 版 AA2。

(二)建立網軍與網軍預算

2013 年 5 月初，聯合國裁軍研究所(United Nations Institute For Disarma -ment Research,UNIDIR)揭露，全球已有 46 國家設立網路部隊，前一次在 2011 年調查時，設有網路部隊的國家僅有 33 個。這項調查數據，顯示網路安全已成為國家安全問題。[97]

1. 成立網軍

(1)美國

第一次波灣戰爭後，美國認為資訊時代的戰爭形態將以網路戰為首，故自 1994 年起，美軍依據資訊作戰需求改革部隊體制、調整部隊裝備研發，並停止投資不適應資訊戰場的重型武器裝備(如「科曼奇」武裝直升機)，改以建設指揮扁平化、保障一體化、編組模組化的資訊化部隊為重要建軍發展方向。[98]

在柯林頓時期，美國國家安全戰略強調，美國必須有計畫與準備去對抗敵人採不對稱戰爭的非傳統方法，如資訊作戰及大規模毀滅性武器，此一戰法在攻擊美國之弱點，以避開美國的強項，這是一個重要及特別的挑戰。[99]鑒於網路襲擊、網路恐怖主義，對國家安全的衝擊日益升高，小布希政府開始思考成立資訊戰指揮單位。[100]美國國防部 2006 年出版的「四年期國防總檢」首次指出，未來國家及非國家將運用電腦網路技術與能力，反制美國現有軍事優勢，對美國構成嚴重的挑戰。[101]2011 年歐巴馬政府以「60 天網際空間政策檢討」(60-Day Cyberspace Policy Review)展開網路安全作為，認為總統應任命一名網路安全政策官員，擔任政府與國家作為的核心協調人，並策頒「穩固網際空間的國際戰略」(International Strategy to Secure Cyberspace)。[102]

2009 年 6 月 23 日，美國國防部長蓋茲(Robert Gates)下令將陸、海、空及海陸陸戰隊之網路部隊，整合成美國網軍司令部(United States Cyber Command)受美國戰略司令部(United States Strategic Command)指揮與管制，負責美國網路軍事行動及保護軍方電腦系統，總部設於美國馬里蘭州米德堡陸軍基地(Fort Meade)，如表 2-1。[103]由當時國家安全局局長亞歷山大(Keith B.Alexander)中將為首任司令，並於 2010 年 10 月全面運作。[104]根據 2014 年美國公佈的四年期

[97]戴定國，〈新新人類戰爭 網軍納入正規部隊〉，《人間福報》，http://www.merit-time.com.tw//NewsPage.asp?unid=306788(2014年3月10日)。

[98]莊加勝、王磊，〈美軍推進資訊化軍隊建設的主要經驗〉，《湖北經濟學院學報》，第 9 卷，第 10 期，2012 年 10 月，頁 32。

[99]曹雄源，《柯林頓政府時期:新世紀的國家安全戰略》，桃園:國防大學，2008 年，頁 30。

[100]呂炯昌著，〈美印組成網路聯合部隊對抗中國大陸網軍〉，《尖端科技》，第 311 期，2010 年 7 月，頁 90。

[101]曹雄源、廖舜石譯，《布希政府時期國家安全戰略》(The National Security Strategy of The United States of America,2002、2006)，桃園:國防大學，2008 年，頁 153。

[102]章昌文譯，Kevin P.Newmeyer，〈誰該主導美國的網路安全作為〉(Who Should Lead U.S Cybersecurity Efforts？)，《國防譯粹》，第 39 卷，第 8 期，2012 年 8 月，頁 17-18。

[103]米德堡被列入 IT 行業十大行列，很大一部分原因在於美國最大的技術情報機構國家安全局總部設於該地。美國國家安全局做為美國保密級別最高的情報機構之一，國家安全局共有 2.5 萬人左右。年預算經費 100 多億美元。一大任務就是監控世界各國的電話及電郵，因此網羅了一大批美國最頂尖的電腦與資訊技術人才，也裝備有世界上最先進的電子電腦。該局於上世紀 50 年代成立，但實現大規模擴張還是在電腦技術全面發展之後，規模已經是中央情報局(CIA)的四倍。

[104]〈美軍網戰司令部〉，《維基百科》，

國防總檢討《QDR,2014》強調，美國國防部將繼續投資最先進的網路工具和擴展網絡能力，並持續招聘、培訓和留住網絡人才，以捍衛網絡安全，確保美國目前在太空和網絡空間優勢。[105]

圖 2-1:美國網路司令部隊徽及總部成立地址位置圖

	
美國網軍司令部徽章	**總部位於美國馬里蘭州米德堡陸軍基地**
備註: 1. 米德堡被列入美國 IT 行業十大行列，美國國家安全局（NSA）總部也設於該地。一大任務就是監控世界各國的電話及電郵，因此網羅了一大批美國最頂尖的電腦與資訊技術人才，也裝備有世界上最先進的電子電腦。 2. 馬里蘭州:著名軍火生產商洛克希德.馬可公司總部也在馬里蘭州(據 2013 年 10 月 22 日，中共《防務新聞》報導：洛克希德馬丁公司獲得美國國防部 7 年 46 億美元合同契約。另陸軍研究實驗室;美國國家安全局國家航鑿暨太空總署在馬里蘭州。	

作者整理

資料來源:〈美國網戰司令部〉,《維基百科》http://zh.wikipedia.org/wiki/%E7%BE%8E%E5%9C%8B%E7%B6%B2%E6%88%B0%E5%8F%B8%E4%BB%A4%E9%83%A8;〈馬里蘭州〉,《維基百科》http://zh.wikipedia.org/wiki/%E9%A6%AC%E9%87%8C%E8%98%AD%E5%B7%9E(2013 年 12 月 24 日)

根據 2013 年 1 月 28 日《華盛頓郵報》(Washington Post)報導，美國國防部希望增強網路安全防護能力，並通過一項網路司令部網軍擴編至現行人力 5 倍計畫，而且在未來五年內擴編網軍司令部，讓網軍人員從目前 900 人增加至 4900 人，其中 20%將是具備熟練分析與制訂反制策略技能的文職人員。[106]中共的資料也指出，2014 年美國將繼續落實「亞太再平衡」戰略，報導稱美軍為強化「反介入」作戰和資訊戰能力，將調整部隊體制與編組，計畫在未來三年內增加 976 網路操作手人員和建立 40 個網路作戰小組。[107]其中，網路司令部下轄三個部門，分別為「國家任務部隊」(National Mission Forces)負責保護關鍵基礎設施，如電

〈http://zh.wikipedia.org/wiki/%E7%BE%8E%E5%9C%8B%E7%B6%B2%E6%88%B0%E5%8F%B8%E4%BB%A4%E9%83%A8〉(2014 年 1 月 2 日)。

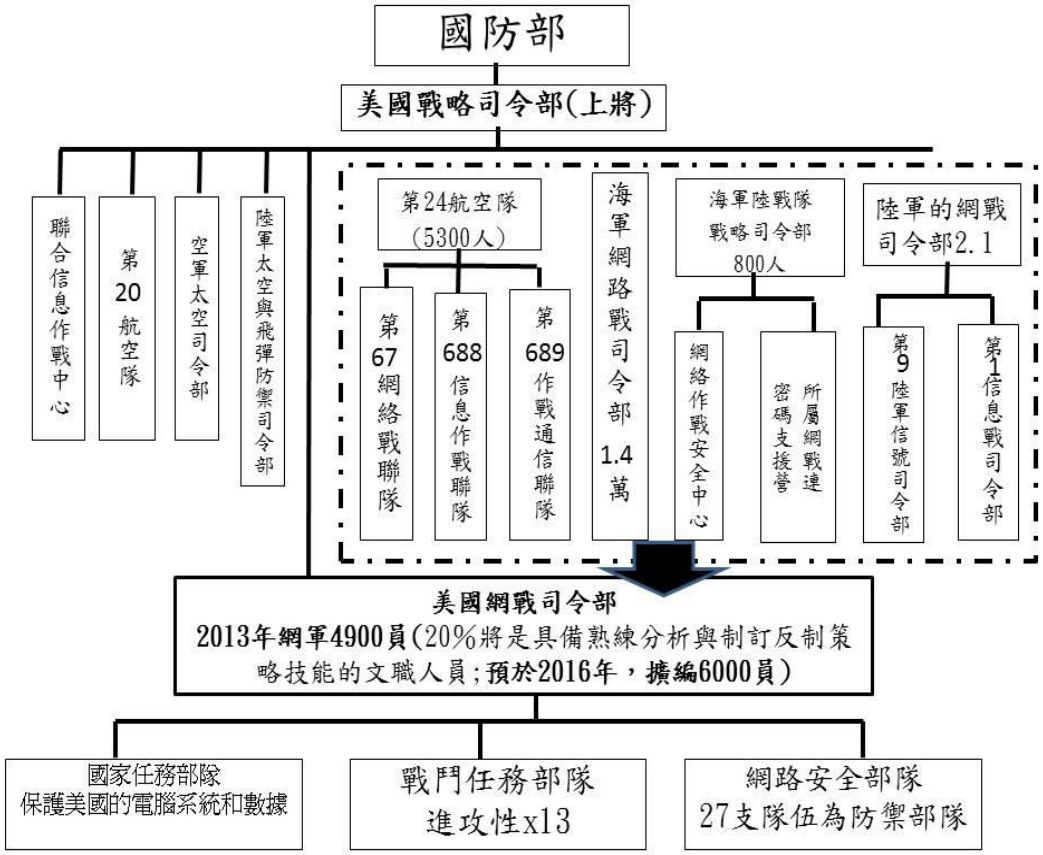
[105]Department of Defense,"Quadrennlal Defenes Review 2014",Washington.DC,2014,pp32-33。〈http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf〉(2014 年 4 月 16）。

[106]柯宇倩,〈美國對解放軍黑客無可奈何〉,《明鏡網》,〈http://city.mirrorbooks.com/news/?action-viewnews-itemid-79840-page-3〉(2014 年 1 月 3 日)。

[107]黃德潔,〈中共持續關注 美日亞太軍力發展〉,《青年日報》,2014 年 1 月 2 日，版 5。

腦和發電廠;「戰鬥任務部隊」(Combat Mission Forces)配合國外指揮部計畫，應付各種形式的攻擊;「網路安全部隊」(Cyber Protection forces)保護國防部自身的網路系統。[108]此外，在 2014 年 3 月 28 日，美國國防部部長黑格主持「網路司令部」首任司令美國陸軍上將亞歷山大榮退時宣布，美國網路部隊將於 2016 年擴編至 6000 人，以現代化網軍來防範網攻對美國國安的威脅。[109]美軍網軍編組架構，如圖 2-2。

圖 2-2:美國網軍編組架構圖



作者整理

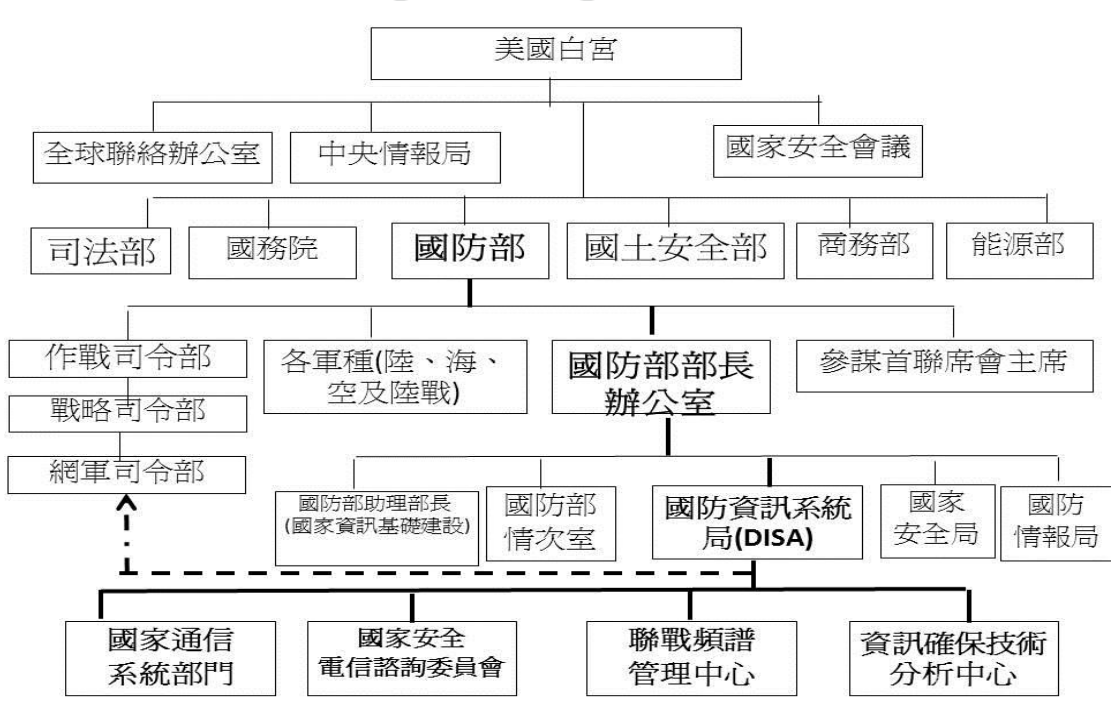
資料來源: 國防部史政編譯局譯，阿里斯德(Leigh Armistead)，《資訊作戰-以柔克剛的戰爭》(Information Operations:Warfare and the Hard Reality of Soft Power)，台北:國防部史政編譯室，2008年;美國網戰司令部，維基百科 http://zh.wikipedia.org/wiki/%E7%BE%8E%E5%9C%8B%E7%B6%B2%E6%88%B0%E5%8F%B8%E4%BB%A4;William Welsh,"DOD plans to expand nation's elite cybersecurity force",*defensesystems*, http://defensesystems.com/articles/2013/01/28/agg-dod-cybersecurity-workforce-expansion.aspx。

[108]William Welsh,"DOD plans to expand nation's elite cybersecurity force",*defensesystems*, 〈http://defensesystems.com/articles/2013/01/28/agg-dod-cybersecurity-workforce-expansion.aspx〉(2014年2月20日)

[109]崔敬熙，〈防網攻 美網軍 2016 年擴編至 6 千人〉，《青年日報》，2014 年 3 月 30 日， 版 5。

值得一提的是，網軍司令部前身為國防部資訊系統局(DEFENSE INFORMATION SYSTEM AGENCY,DISA)之「電腦網路作戰聯合特遣部隊」(Joint Task Force- Computer Network Operations,JTF-CNO)，該部隊於 1998 年成立，成立之際為「電腦網路防禦聯合特遣部隊」(Joint Task Force-Computer Network Defense,JTF-CND)，負責與政府其他機構溝通，包括司令部、聯邦、國安局與各軍種的電腦網路危機應變小組，2001 年 4 月該部隊更名為「電腦網路作戰聯合特遣部隊」，並於 2003 年，併入美國戰略司令部。其他組織包國家通信系部門、國家安全電信資詢委員會、聯戰頻譜管制中心，以解決公共交換網路問題，其美國國防資訊系統局組織架構，如圖 2-3。[110]據報導，美國國防資訊系統局(DISA)於2013月11月5日編組人員，參加美國網絡司令部發起的網路攻防演習(Exercise Cyber Flag 14-1)，如圖 2-4，以強化美國國防部網絡遭攻擊防護能力。[111]

圖 2-3:美國國防資訊系統局組織架構圖



作者整理

資料來源: 國防部史政編譯局譯，阿里斯德(Leigh Armistead)，《資訊作戰-以柔克剛的戰爭》(Information Operations:Warfare and the Hard Reality of Soft Power)，台北:國防部史政編譯室，2008年，頁38-49。

此外，美國各軍種司令部為確保資訊優勢，紛紛成立網路部隊。據 2013 年 3 月 1 日，美國海軍軍令部長格林納(Jonathan W.Greenert)上將出席眾議院撥款委員國防小組委員會表示，美海軍在 2009 年採取大膽且前瞻的做法，集結海軍情報、資訊戰、氣象/海洋學、資訊專業，以及網路工程師等領域專家，設置「資訊優勢部隊」(Information Dominance Corps,IDC)，並納入建軍備戰的一項重點工

[110]國防部史政編譯局譯，阿米里特德(Leigh Armistead)，《資訊作戰-以柔克剛的戰爭》(Information Operations Warfare and the Hard Reality of Soft Power)，台北:國防部史政編譯室，2008 年，頁 47-48。

[111]David Cenciotti,"DISA PARTICIPATES IN ANNUAL EXERCISE FOCUSED ON CYBER OPERATIONS AND DEFENSE",*DISA*,
< http://www.disa.mil/News/Stories/2013/Cyber-Flag-Exercise>(2014 年 4 月 10 日)

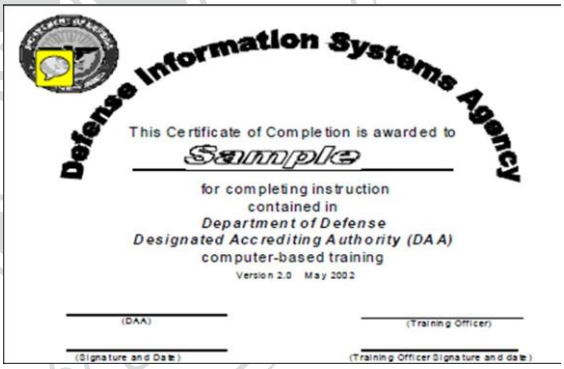
作;[112]同時，美陸軍網路司令部正打造一支能夠在網際空間提供全方位優勢成效的網路戰士部隊，以軍事情報第 780 旅為核心，對關鍵技能、執行信號情報與電腦聯網作戰，以實現美陸軍與國防部網路的「動態電腦聯網防衛作戰」(dynamic computer network defense operations)等日益增長的需求。[113]從上述資料得知，美國投入網路戰備戰不僅只有網路司令部，而是更多隱藏看不見的實力，可見網路戰的攻、防愈來重要。

為提升人才素質，美國產業界、國防部與空軍學校(Air Force Association)聯手致力於「網路愛國者計畫」(Cyber Patriot program)，藉由全國性的中學生層級網路競賽，以鼓勵中學生儘早加入網路安全部門，以發掘人才。另產業界諾斯洛普格魯曼公司(Northrop Grumman)，與學術界卡內基美隆大學(Carnegie Mellon University)、麻省理工學院(Massachusetts Institute of Technology)、普度大學(Purdue University)締結夥伴關係創辦了「網路安全研究集團」(Cybersecurity Research Consortium)以協助阻止攻擊。[114]根據 2012 年美國國防部〈資訊保障工作人員提高計畫〉(Information Assurance Workforce Improvement Program)手冊表示，為保證美國軍隊的戰鬥效能，美國國防部已要求各作戰部隊和國防合同承包商從事網路和資訊保障相關工作的人員，除必須具備相關資格，並不斷須定期參加繼續教育，已提升業務技能。並舉辦網路競賽以提升網路戰能力，競賽挑戰證明書，如圖 2-5。[115]

圖 2-4:美國 DISA 參加網路攻防演練圖

資料來源:David Cenciotti，“DISA PARTICIPATES IN ANNUAL EXERCISE FOCUSED ON CYBER OPERATIONS AND DEFENSE”,*DISA*,< http://www.disa.mil/News/Stories/2013/Cyber-Flag-Exercise>

圖 2-5:國防部網路競賽挑戰賽證書



資料來源: Department of Defense Chief Information Officer,“DoD 8570.01- M:Information Assurance Workforce Improvement Program,” http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf (Jan.24,2012)，頁 42。

[112]章昌文譯，Nancny Brown,Danelle Barrett,and Jesse Castillo，〈訓練官兵網路戰力〉(Creating Cyber Warriors)，《國防譯粹》，第 40 卷，第 4 期，2013 年 4 月，頁 47。
[113]陳嘉容譯，Rhett A.Hernandez，〈美陸軍在網際空間的全方位策略〉(Preparing the Army to Prevent,Shape and Win in Cyberspace)，《國防譯粹》，第 41 卷，第 1 期，2014 年 1 月，頁 5-6。
[114]章昌文譯，Sandra I.Erwin，〈國家安全未來五大威脅〉(The Five Treats To National Security in the Coming Decade)，《國防譯粹》，第 40 卷，第 2 期，2013 年 2 月，頁 50。
[115]Department of Defense Chief Information Officer,“Information Assurance Workforce Improvement Program,” Washington D.C DoD ,8570.01, 〈http://www.dtic.mil/whs/directives/corres/pdf/857001m.pd〉(2014 年 4 月 10 日)。

根據 2013 年 1 月 4 日《紐約時報》的報導，美國因應網路武器將如同核子武器，因此通過法規，在足夠可信證據顯示美國將遭受重大的網路攻擊時，可由三軍統帥命令啓動破壞性程式(如 2010 年伊朗震網事件 Stuxnet[116])，對敵實施先發制人攻擊。[117]2014 年 2 月底，美國網路司令部司令亞歷山大中將參加參議院軍事委員會明確表示，促使美國發動網路戰的底線，將是美國網路因遭受網路攻擊而癱瘓。[118]除此之外，美國國會亦曾向中共說明未來美國的網路攻擊計畫，希望透過這種公開合作交流方式，讓對方清礎知道美國發動網路戰的底線，以避免不必要的誤解，導致發生雙互網路攻擊。[119]由此可知，網路戰已成為美國打擊敵人的重要武器，除藉由立法使其戰爭行為合法外，更公開表明美國網路戰的底限，及越線的後果，以期對潛在敵人產生一定的威嚇作用。

為避免網路戰引起戰後爭議，根據 2013 年 3 月 18 日英國《衛報》(The Guardian)的披露，北約已在「卓越合作網路防禦中心」(位於愛沙尼亞首都塔林)邀請 20 名法律專家，在國際紅十字會及美軍網路戰司令部的協助下完成《網路戰手冊》編撰，故又稱為《塔林手冊》(Tallinn manual)，其內容有 95 條則，強調由國家發起的網路攻擊行為，必須避免敏感的民用目標，如醫院、水庫、核電廠等，並允許經由常規攻擊來反擊造成人員死亡和重大財產損失的網路攻擊行為。[120]

(2)英、德、以色列、日、韓等國

據我國國安局副局長張光遠透露，英國已於 2010 年，成立「反網路威脅中心」，延攬通訊總部(GCHQ)及軍情五處(MI5)網路專家保護網路安全;德國繼英國之後，已於 2013 年 4 月組建「網路戰爭處」，招募相關人才，並於國防部組建約 6,000 人的網路部隊至阿富汗執行網路監控任務。[121]

2012 年《美國戰略之頁》(strategypage)的網站報導指出，以色列國防軍（Israeli Defense Forces,IDF）正在加緊篩選軍方招募的所有新兵，以找出那些適合網路戰部隊工作的人員，其中的一項重要措施就是，發現人才，然後培養他們。這也是以色列高科技公司和新技術專利的數量不成比例的一條重要原因。以色列的人口總數不到美國的人口總數的 3%，但是其組建的網路戰小組卻同美國的網路戰小組一樣強大。以色列現在有十多個網路戰機構，幾乎所有的都是秘密機構，以色列的大多數網路戰專家在許多軟體公司就業，如有實施網路戰行動必要他們就回到軍隊。以色列網路人才方面，無論男性或或女性網路戰人員，不僅要具備合適的技能，而且還要具有正規突擊隊員那樣堅忍不拔的心理素質。[122]

---

[116]Stuxnet（震網）是一種 Windows 平台上的電腦蠕蟲，2010 年 6 月首次被白俄羅斯安全公司 VirusBlokAda 發現，其名稱是從代碼中的關鍵字得來，它是首個針對工業控制系統的蠕蟲病毒，利用西門子公司控制系統（SIMATIC WinCC/Step7）存在的漏洞感染資料採集與監控系統（SCADA），能向可編程邏輯控制器寫入代碼並將代碼隱藏。

[117]馮克芸，〈美軍網路武器 總統才能發動〉，《聯合報》，2013 年 2 月 6 日， 版 14。

[118]宋偉豪，〈威嚇潛在敵人 美為網路戰劃紅線〉，《青年日報》，2014 年 3 月 30 日， 版 5。

[119]中央社紐約，〈避免誤解 傳美曾對中共說明網攻計畫〉，《青年日報》，2014 年 4 月 8 日，版 5。

[120]梁華傑，〈奪取制網路權 搶先制定網路戰規則〉，《尖端科技》，第 351 期，2013 年 11 月，頁 53。

[121]立法院，《我國如何因應網軍與駭客攻擊並強化資訊安全措施》，《 立法院公報》，第 102 卷，第 29 期，頁 6。

[122] "Israel and U.S. Admit Joint Cyber War Effort",*strategypage* http://www.strategypage.com/htmw/htiw/20120605.aspx（2013 年 12 月 8 日）。

根據 2013 年 6 月 2 日《亞洲週刊》的報導，日本於 2013 年 5 月 16 日，由日本防衛大臣小野寺五典與海陸空聯合總參謀長岩崎茂親自為創建目本第一支網路部隊掛牌，日本創建的網路部隊直屬於統合幕僚監部(聯合總參謀部)，其編制人數為 90 員。該報導亦指出，日軍網軍編制人數，實際上只是籌組網路部隊司令部的核心骨幹，更多反駭客的專業軍官則分散於海、陸、空等各部隊中。新設網路部隊將針對海、陸、空各自負責的網路安全進行統一管理，負責監控可能受到網路攻擊，強化防衛省及各部隊的安全。[123]日本一家名為 LAC 的資訊技術安全公司的網路安全實驗室總經理 Hiroshi Itoh 指出，由於日本網路防禦部隊的人員是內部招募，被派遣到部隊的公務員可能缺乏足夠的專業技能，不能與駭客對手過招，且網路防禦部隊網路安全軍官人數太少，訓練不足，更像一支民事員警部隊，他們不具備網路勇士堅強的心態。他說日本網路防禦部隊需要 2000 到 3000 名網路勇士，至少有一部分是從私營部門招募的白帽子駭客。[124]

北韓於 1986 年在金正日指示下，在平壤成立美林大學，以每年培養一百二十餘名網路工作人員，而北韓偵察總局下屬作戰局管理的牡丹峰大學和金日成軍事綜合大學，每年也培養超過一千名網路工作人員，畢業生被安排在偵察總局下屬專門負責網路的部門-第一一研究所、四一四聯絡所、一二八聯絡所等單位來工作。另外，2009 年，南韓也創立網軍司令部。為擴充培養管道，韓國高麗大學於 2011 年，在韓國大學中第一個設立網路戰軍官的學科-網路國防科學，並於 2012 年設立網路國防研究中心，2011 年秋季開始招生，共選拔三十名學生，畢業前至網軍司令部實習。[125]另一報導，南韓網軍司令部已擁有 200 名電腦專長人員。[126]據報導，南韓網路戰略第一部則是利用對北韓社群網站和社交媒體進行線上宣傳，第二步是研發破壞北韓核電廠和飛彈設施的武器。[127]

除此之外，2012 年挪威已建立了歸國防部管理的專門網路防禦部隊，該單位將武裝部隊司令部下的挪威軍事情報局、國家安全局和挪威員警安全局等機構的網路威脅和防禦能力進行合併。同年 1 月，瑞典將軍隊信號情報機構、軍事情報機構和瑞典國家警察局的網路部隊整合起來，建立國家網路防禦機構。[128]

在我國方面，國防部部長高華柱先生於 103 年 4 月 29 日在立法院外交及國防委員會表示，國防部資安部隊現有三千多人，未來將成新的資電作戰部隊第四中隊，以強化攻擊能力。高華柱並表示，將台電公司遭駭客入侵，影響政軍中心供電狀況，首度列入我國「漢光演習」重點驗證項目，提升國軍總整資安能量。[129]高部長的報告顯示我國將以資安部隊為基礎，建立網軍。

---

[123]毛峰，〈日本創建網軍聯美反制中國〉，《亞洲週刊》，第 27 卷，第 21 期，2013 年，6 月，頁 36。
[124]PAUL KALLENDER-UMEZU,“Experts: Japan's New Cyber Unit Understaffed, Lacks Skills”,*defense*, <http://www.defensenews.com/article/20130709/DEFREG03/307090007/Experts-Japan-s-New-Cyber-Unit-Understaffed-Lacks-Skills> （2013 年 12 月 8 日）。
[125]沙沙，〈網路版朝鮮戰爭爆發-兩韓網路戰對抗升級〉，《亞太防務》，第 61 期，2013 年 3 月，頁 25-27。
[126]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》，第 311 期，2010 年 7 月，頁 90-92。
[127]編譯組，〈美韓機密通訊〉，《青年日報》，2014 年 2 月 23 日， 版 5。
[128]Cheryl Pellerin,“DOD at Work on New Cyber Strategy, Senior Military Advisor Says,”*defense,* <hhttp://www.defense.gov/news/newsarticle.aspx?id=120397> （2014 年 3 月 8 日）。
[129]王光慈，〈國防部第 4 支網路中隊成軍〉，《聯合報》，2013 年 4 月 30 日， 版 11。

2. 網軍預算

根據研究報告，美國於柯林頓政府時期曾投入 20 億美元，來打擊美國網路恐怖活動，遂行未來的網路戰爭，以強化電腦的安全。[130]2011 年 7 月 14 日美國國防部首次發布《網路空間行動戰略》(network space action strategy)具體表示，美國將規劃在未來 5 年內撥款 5 億美元給國防部高級研究項目，以加快網絡武器及防禦性網絡技術的研發。[131]同年 8 月底，美國通用動力公司(General Dynamics 之 C4 Systems)獲得高達 37 億美元合約，提供美陸軍合約指揮部「亞伯丁試驗場」(Aberdeen Proving Ground)所需之強固區域網路、伺服器平台、通信閘道器、路由器與膝上型電腦。[132]

美國開始增加預算來發展網路防護設施或基礎建設，可追塑至小布希政府時期。[133]此外，為因應網路對國防領域的影響力逐漸擴大，加上來自中共、北韓的「數位炸彈」攻勢不斷，「網路安全」已成為美軍新年度預算的重頭戲。在 2012 會計年度的美國國防授權法，「網路安全」字眼被提及 12 次，2013 年 61 次，2014 年則已到達 17 次。[134]美國國防部先進研究計畫署(Defense Advanced Research Projects Agency,DARPA)主管杜甘(Regina Dugan)表示，美國計畫在 2012 年預算中，增加該機構網路研究從 1 億 2 仟萬美元提高到 2 億 8 百萬美元，避免洩密與網路攻擊。[135]

因應當前資訊技術環境龐大且複雜的情況，美國國防部於 2013 年會計年度將網路安全預算調升至 370 億美元，以確保網路安全防護。[136]另外，於 2013 年在美國猶他州威廉斯營(Camp Williams)完成一座價值 12 億美元的「網路安全中心」，這是美軍近數十年來最大的一項軍事建設計畫。[137]2014 年，美國計畫在操作程序、研究與器材方面投入數億美元預算，包括限制可用於網路攻擊的設備交易行為。其中，將挹注 6,800 美元投入網路指揮部運作、1,400 萬美元發展網路空間攻擊程式，並投入 1,900 萬美元於網路安全研究及 2,000 萬美元進行網路安全進階研究用。最後在設備建置上，將擴大網路指揮部聯合作戰中心既有規模及所需設備。[138]除此之外，美國國防預算在全面縮減的情況下，國防部仍計畫在 2014-2018 年期間，增加投入 260 億美元發展網路科技，主要用於保衛軍方的網路，並投入數十億美元來發展網路攻擊武器。[139]

---

[130]國防部史政編譯局譯，史利芙爾(Frank J.Cilluffo)，《網路威脅與資訊安全》(Cyber Threats and Information Security)，台北:國防部史政編譯局，2002 年，頁ⅩⅦ。
[131]楊立傑、劉淑萍、劉強著，〈美國概況〉，《新華網》，http://big5.xinhuanet. com/ gate/big5/news.xinhuanet.com/ziliao/2002-01/28/content_ 257426_2. htm(2013 年 12 月 2 日)。
[132]余忠勇譯，Andy Oppenheimer，〈網路戰對抗無的大規模毀滅性武器〉(Fighting the Quiet WMD-Cyber-Warfare)，《國防譯粹》，第 39 卷，第 8 期，2012 年 8 月，頁 31。
[133]曹雄源、廖舜石譯，《柯林頓政府時期:全球時代的國家安全戰略》(A National Security Strategy for A Global Age,2000)，桃園:國防大學，2008 年，頁 52。
[134]張道宜，〈美軍 2014 年要務應對網路戰〉，《青年日報》，2014 年 1 月 1 日，版 5。
[135]王光磊，〈美網路戰預算倍增〉，《青年日報》，2011 年 11 月 9 日，版 5。
[136]李洳錞譯，Teri Takai，〈更靈活的國防資訊能力〉(Creating a More Agile Defense Department info-Tech Enterprise) ，《國防譯粹》，第 39 卷，第 8 期，2012 年 8 月，頁 36。
[137]同註 132，頁 29。
[138]張道宜，〈美軍 2014 年要務應對網路戰〉，《青年日報》，2014 年 1 月 1 日，版 5。
[139]田思怡，〈美向陸簡報網軍數 盼投桃報李〉，《聯合報》，2014 年 4 月 8 日，版 12。

美國國家安全局（National Security Agency,NSA）正試圖發展量子電腦[140]，名為「滲透艱難目標」(Penetrating Hard Targets)的機密計畫，經費達 7970 萬美元(約台幣 23 億.9 元)外包給馬里蘭大學帕克分校的一所實驗室，該計畫的目的在破解包括網路、銀行、醫療、商業與世界各國政府使用的各種所有加密程式，同時提升自身的保密能力。[141]自 2011 年起，美國洛克希德馬丁公司(Lockheed Martin)購買全球第一部商用量子電腦，並於 2012 年，由谷歌公司(google)和太空總署(National Aeronautics and Space Administration,NASA)聯手買下另一部量子電腦。[142]據報導，該項計畫最常對付中共軍方單位(如解方軍駭客組織 61398 部隊)，也曾成功入侵俄羅斯軍方網路、歐盟貿易機構等。[143]

上述資料顯示，美國為因應網路戰，不僅持續擴編預算費用，而且結合國安部門、科研部門及民間科技力量，共同打造網路戰優勢屏障。除此之外，根據美國聯邦時報《federal times》的網站報導，美國國土安全部將投入 1.85 億美元資金用於監控工具，對民用網路於每 24 小時到 72 小時實施幾十億次的自動安全檢查。並規劃在 2013-2015 年期投入 60 億美元，以實現政府網路安全防護標準化，如表 2-2。[144]

表 2-2:美國成立網軍費用年度統計表

單位 年度	美國國防部			國土防衛部
	國防部暨 軍種司令部	國安局	先進研究 計畫署	
2011 年	5 億美元(國防部高級研究項目);另 37 億美元(美陸軍「亞伯丁試驗場」所需網路設備	1 億 6000 萬美元		
2012 年			2 億 800 萬美元(研發網路武器避免洩密及網路攻擊)	
2013 年	370 億元美元(網路戰費用);4.14 億美元雲端技術服務			1 億 85 億美元資金(網路監控),並規劃在 2013-2015 年陸續投入 60 億美元
2014 年	6,800 百萬美元			

[140]量子電腦可同時進行多種運算，能更快有效率地正確解答萬進。據稱，量子電腦強大的運算能力高出一般電腦逾 10 兆倍，只消 30 秒時間就能解決一般電腦 100 億年才能完成的問題。
[141]黃文正，〈美國安局研發量子電腦 破解加密〉，《中國時報》，2014 年元月 4 日，版 19。
[142]〈美 NSA 量子電腦可可全球加密技術〉，《青年日報》，2014 年元月 4 日，版 5。
[143]管淑平，〈無線電波植間碟美滲透 10 萬電腦〉，《自由時報》，2013 年 12 月 16 日，版 9。
[144]NICOLE BLAKE JOHNSON,“ DHS kicks off $6B cyber program”, *federaltime*s 〈http://www.federaltimes.com/article/20130825/IT01/308250001/DHS-kicks-off-6B-cyber-program〉（2013 年 12 月 8 日）.

2014-8年	260億美元發展網路科技(保衛軍方的網路);另投入數十億美元發展網路攻擊器。			

作者綜理:

資料來源: 李洳錞譯,Teri Takai,〈更靈活的國防資訊能力〉(Creating a More Agile Defense Department info-Tech Enterprise),《國防譯粹》,第39卷,第8期,2012年8月,頁36;張道宜,〈美軍2014年要務應對網路戰〉,《青年日報》,2014年1月1日,版5;田思怡,〈美向陸簡報網軍數 盼投桃報李〉,《聯合報》,2014年4月8日,版12;余忠勇譯,Andy Oppenheimer,〈網路戰對抗無的大規模毀滅性武器〉(Fighting the Quiet WMD-Cyber-Warfare),《國防譯粹》,第39卷,第8期,2012年8月,頁31;王光磊,〈美網路戰預算倍增〉,《青年日報》,2011年11月9日,版5。黃文正,〈美國安局研發量子電腦 破解加密〉,《中國時報》,2014年元月4日,版19。楊立傑、劉淑萍、劉強著,〈美國概況〉,《新華網》,http://big5.xinhuanet.com/gate/big5/news. xinhuanet.com/ziliao/2002-01/28/content_257426_2. htm(2014年3月21)。

2011年12月,美國Visiongain公司發表的一份研究報告指出,2012年各國政府將在資訊技術安全上花費159億美元。[145]例如英國政府的新「網路安全戰略」(Cyber Security Strategy)指出,於2011年1月投入6億5,000萬英磅之預算將用於防護關鍵國家基礎設施。[146]2013年1月10日《美國國防部新聞網站》(defensenews)站揭露,英國財政大臣奧斯本(George Osborne)宣佈,在2015-16年政府財政縮減措施中,英國的網路安全費用並未受影響。該網站表示,網路是國家安全優先事項,這一領域的投資,在2015年將繼續增長,包括2.1億英鎊(3.2億美元)的國家網路安全計畫的投資。最初的4年預算費用計畫,從2011年開始,給情報部門分配額外的3.48億英鎊,其中國防部分配9000萬英鎊。此外,英國政府通信總部已經投資新能力識別和分析敵對的網路攻擊,成立新的聯合網路小組,與國防部共同打擊英國的網路威脅。[147]

2012年1月「日本富士通公司」(Fujitsu)和日本防衛省簽訂價值230萬美元,為期3年的專案,該公司宣稱已發展出「虛擬網路武器」。[148]另外,日本總務省將耗100億日圓,在石川縣能美市建立日本國內最大的網路防禦技術研發實驗設施。新設施將建在總務省所轄「情報通信研究機構」(National Institute of Information and Communications Technology,NICT)的技術中心內,該技術中心投入3,000台服務器,構建相當於300萬台電腦組成的網路,對電腦病毒的感染途徑、入侵痕跡及防禦手段展開研究,以提升網路戰力。[149]2014年3月,日本防衛省宣佈將投資1.419億美元預算,以組建聯合網路防禦部隊,為日本自衛隊提供24小時的網路安全監控、檢查、分析、防禦、清理及訓練職能。[150]

[145]同註132,頁27。
[146]同註132,頁29。
[147]MONS, BELGIUM," NATO Steps Up Efforts To Ward Off Cyberattacks,"*defensenew*s, <http://www.defensenews.com/article/20130710/DEFREG01/307100018/NATO-Steps-Up-Efforts-Ward-Off-Cyberattacks> (2013年12月8日)。
[148]同註132,頁30。
[149]毛峰,〈日本創建網軍聯美反制中國〉,《亞洲週刊》,第27卷,第21期,2013年,6月,頁37。
[150]PAUL KALLENDER-UMEZU"Experts: Japan's New Cyber Unit Understaffed, Lacks Skills,"

南韓為保護網路安全，在 2012 年 7 月投資 19 億南韓元，將於 2013 年 3 月之前選拔 6 員頂級網路專長(南韓稱白客)，以每人獲得二千萬韓元獎學金赴海外進修，畢業後至網軍司令部、國情院及員警廳工作。[151]各國網軍人數及預算統計如表 2-3。

表 2-3:網軍兵員人數與預算投入統計表

區分 / 國家	成立年份	網軍數量		投入預算
		部門	網軍人數	
美國	2009 年	網路司令部	6000 員	370 億元美元
英國	2010	網際安全作戰中心(延攬通訊總部及軍情五處網路專家保護網路安全		9000 萬英磅，另投資 6 億 5,000 萬英磅之預算將用於防護關鍵國家基礎設施。
德國	2013 年 4 月	網路戰爭處	6000 員	
南韓	2009 年	網路司令部	5 百餘員	投資 19 億韓元
北韓	1988 年	北韓人民軍總參謀部指揮自動化局和人民武力部偵察局	3 千員	700 多萬美元
日本	於 2013 年	網路部隊直屬聯合總參謀部	核心編制 90 人，但實際上駭客專業軍官分散於陸、海空各軍種，約 2000 到 3000 員	140 多億日圓此外，投資一百億日圓建立國內最大網路防禦技術研發實驗室。
中華民國	2013 年	資電部成立網路第 4 中隊	預估約 3000 餘人	

作者整理

資料來源: 崔敬熙，〈防網攻 美網軍 2016 年擴編至 6 千人〉，《青年日報》，2014 年 3 月 30 日，版 5;管淑平，〈北韓下一步對美發動網攻〉，《自由時報》，2013 年 4 月 8 日，版 12;李泇錞譯，Teri Takai，〈更靈活的國防資訊能力〉(Creating a More Agile Defense Department info-Tech Enterprise)，《國防譯粹》，第 39 卷，第 8 期，2012 年 8 月，頁 36;沙沙，〈網路版朝鮮戰爭爆發-兩韓網路戰對抗升級〉，《亞太防務》，第 61 期，2013 年 3 月，頁 27;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》，第 311 期，2010 年 7 月，頁 86-89;李忠謙，〈防俄中網路攻擊 英將組建網軍〉，《青年日報》，2010 年 4 月 28 日，版 5;余忠勇譯，Andy Oppenheimer，〈網路戰對抗無的大規模毀滅性武器〉(Fighting the Quiet WMD-Cyber-Warfare)，《國防譯粹》，第

---

*defens*e,
<http://www.defensenews.com/article/20130709/DEFREG03/307090007/Experts-Japan-s-New-Cyber-Unit-Understaffed-Lacks-Skills> （2013 年 12 月 8 日）。

[151]沙沙，〈網路版朝鮮戰爭爆發-兩韓網路戰對抗升級〉，《亞太防務》，第 61 期，2013 年 3 月，頁 27。

39 卷第 8 期，2012 年 8 月，頁 29-30；MONS,BELGIUM,“NATO Steps-Up-Efforts-Ward-Off-Cyberattacks ” ,*defensenews*, <http://www.defensenews.com/article/20130710/DEFREG01/307100018/NATO-Steps-Up-Efforts-Ward-Off-Cyberattacks>（2013 年 12 月 8 日）。

（三）將網路戰納入演練課目

資訊戰的戰略已經成為美、英、法、以色列、中共與俄羅斯等國防計畫與情報計畫中所不可或缺的考量因素。[152]在美國防部最新的戰略指導下，美陸軍部隊要能在網際空間確保作戰自主及網路暢通，並於 2013 年將網際空間作戰整合至所有作戰司令部演習課目。[153]

2011 年 9 月，美軍歐洲司令部舉行「結合努力」(Combined Endeavor)的通信與電腦網路演習，召集來自 28 個國家和組織的軍方、業界與學界的專業人士共同實施演練。2012 年美軍舉行「聯軍資訊控制」演習(Coalition Information Dominance)，並置重點於提升國際網路防衛態勢、落實網路資訊分享。此外，在 2011 年北約舉行「網路聯軍 2011」(Cyber Coalition 2011 年)的年度重大網路演習，測試聯盟網路技術與作業能力。[154]2013 年「北約快速反應部隊」(NATO Response Force)為主的部隊，執行代號「堅定爵士」(Steadfast Jazz)的軍演，除實兵演習外，並將網路攻擊納入演練課目。[155]同年，美日「山櫻六五」(Yama Sakura65)[156]首次將網路戰防禦納入應對操演，測試兩國部隊辦敵軍網路攻擊和防禦網攻的能力。[157]

除此之外，2013 年 1 月 1 日，美國國防部網站報導指出，美軍在內華達納內斯空軍基地連續 2 年實施網路旗幟演習，這是聯合的全頻譜網路空間作戰演習，利用逼真的敵方部隊和虛擬的環境反映當前的網路威脅，而「國家任務部隊」則將準備好反擊敵人的網路攻擊。[158]南韓方面，南韓國家情報院旗下的國家安全戰略研究所亦指出，北韓可能在 2014 年南韓軍演後，向南韓發動挑釁，網路攻擊為可能選項之一。[159]此外，日本自衛隊「網軍」則於 2014 年 3 月正式成軍，預定編制為 90 人員，任務為全天侯監視自衛隊的網路情況與分析網路病毒，並於「二加二會議」中，討論出共享遇駭時資訊的機制。同時，日本並計畫於 2015 年派遣自衛官接受美軍網路防衛教育課程，以吸收美國的技術與經驗。[160]將網路戰納入軍演演練課目，證明網路戰將是未來爆發戰爭決勝的關鍵要點。

---

[152]國防部史政編譯局譯，史利芙爾(Frank J.Cilluffo)，《網路威脅與資訊安全》(Cyber Threats and Information Security)，台北:國防部史政編譯局，2002 年，頁 23。
[153]陳嘉容譯，Rhett A.Hernandez，〈美陸軍在網際空間的全方位策略〉(Preparing the Army to Prevent,Shape and Win in Cyberspace)，《國防譯粹》，第 41 卷，第 1 期，2014 年 1 月，頁 5-6。
[154]高一中譯，G.Stavridis and Elton C.Parker Ⅲ，〈航向網路之海〉(Sailing the Cyber Sea)，《國防譯粹》，第 39 卷，第 8 期，2012 年 8 月，頁 12-13。
[155]王光磊，〈北約三軍聯訓 重點演練快速反應部隊〉，《青年日報》，2013 年 11 月 4 日，版 5。
[156]2013 年山櫻六五聯合美日演習，於北海道千歲市實施，強化聯合防禦能力，美軍動員二千員士官兵以上，並透過網路通訊、遠端指揮所夏威夷、路易斯麥科得基地，日本自衛隊則出動四千五百人員實施。引註崔敬熙，” 美日山櫻軍演 首列網路戰防禦” 《青年日報》，2013 年 12 月 13 日，版 5。
[157]崔敬熙，〈美日山櫻軍演 首列網路戰防禦〉，《青年日報》，2013 年 12 月 13 日，版 5。
[158] Cheryl Pellerin” DOD at Work on New Cyber Strategy, Senior Military Advisor Says,”*defense*, <hhttp://www.defense.gov/news/newsarticle.aspx?id=120397> （2014 年 3 月 8 日）。
[159]〈北韓恐以網路挑釁南韓〉，《青年日報》，2014 年 1 月 1 日，版 5。
[160]〈鞏固第 5 戰場 美日將聯手防駭〉，《青年日報》，2014 年 1 月 28 日， 版 5。

二、作戰方式

自 1990 年代中期以來，網路攻擊所需的資源已從奧秘難懂變成了稀鬆平常。現今有數以千計的網址可提供網路武器，如蠕蟲(worms)、特洛伊木馬(Trojan Horses)、邏輯炸彈(logic bombs)、天窗(trap door)、阻斷服務(denial of service,DOS)攻擊及惡意程序碼(malicious code)等，茲扼要說明如下:[161]

(一)定時炸彈(中共稱為固態病毒攻擊法):此種病毒預先植入某個電子元件，並組裝於電子資訊設備。當戰爭需求，利用軍、民網路或通過空間無線電遙控等方式，將病毒激活，進而破壞或癱瘓敵方網路系統。[162]此種網路戰作戰方式，最早運用於軍事領域為 1991 年美伊波灣戰爭。戰前，美國中央情報局派特工人員到伊拉克，將伊拉克從法國購買的防空系統使用的印表機晶片，換上了染有病毒的晶片，於戰略空襲前，美國利用遠端遙控激活晶片病毒，使伊拉克防空指揮中心主電腦系統程序錯亂、指揮失靈。[163]

(二)超載型式(拒絕式服務):此種病毒侵入後會巨量自我複雜，致使主機超載而無法工作，而此種網路攻擊型態雖然是破壞性最小，但也是最難以防禦的，因為網路主機永遠不可能拒絕接受外來資料，此種手段可以輕易突破最高段防禦措施，暫時癱瘓對方主機。[164]如 2007 年，俄羅斯利用網路戰力量(拒絕式服務)向愛沙尼亞發起網路攻擊(拒絕式服務攻擊(DDOS))。[165]這支看不見的軍隊與無法量化的戰力，重創愛沙尼亞網際網路系統，使該國政府國會、媒體、銀行及通信等網站無法正常運作，此戰役，正式將網路戰從軍事層面推升到國家安全層級。[166]誠如美國學者賈斯伯(Scott Jasper)指出，網路戰的效果隨著資訊科技的發展，已如同使用常規野戰火炮攻擊削弱甚至擊敗敵人，使敵人屈服有異曲同工之處。[167]

(三)空間注入病毒法(無線電):通過各種偵察手段，弄清敵方無線電接收設備的電磁頻譜標準，並由無線電發射裝置，將病毒轉換成電磁輻射，植入敵方無線電接收設備，並通過傳遞信道進入敵方的網路系統，使病毒迅速繁殖，占據系統空間，篡改程序數據。[168]據報導，美國國家安全局一個名為「專門存取行動」小組(Tailored Access Operations,TAO)的機密駭客菁英單位，專門滲透全球各地電腦，甚至會其鎖定對象訂購電腦的運送過程，半路攔截以植入後門程式竊取資訊。[169]此外，美國國安局也曾利用無線電波隱蔽頻道和 USB

---

[161]國防部史政編譯局譯，史利芙爾(Frank J.Cilluffo)，《網路威脅與資訊安全)》(Cyber Threats and Information Security)，台北:國防部史政編譯局，2002 年，頁 4。
[162]王正德，《決勝賽柏空間-網路軍事技術及其運用》，北京:軍事科學出版社，2003 年，頁 127。
[163]東鳥，《中國輸不起的網路戰爭》，湖南:人民出版社，2010 年 11 月，頁 42。
[164]行政院研究發展考核委員會，《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》，台北:五南文化出版，2002 年，頁 55。
[165]2007 年 4 月，愛沙尼亞決定將首都塔林的蘇俄時代軍事紀念像移到軍人墳場，2007 年 4 月 27 日，愛沙尼亞多個網站開始受到攻擊。大量網站被迫關閉，一些網站的首頁被換上俄國宣傳口號及偽造的道歉聲明，該國總統的網站同樣倒下，一些網站每月原本僅上線 1000 次，遭攻擊時每秒 2000 人次登入。
[166]同註 163，頁 51。
[167]國防部史政編譯局譯，賈斯伯 (Scott Jasper)，《國防能力轉型-國防安全新策略》(Transforming Defense Capabilities)，台北:國防部史政編譯局，2012 年，頁 35。
[168]同註 162，頁 128
[169]管淑平，〈專門存取行動到特定電腦〉，《自由時報》，2013 年 12 月 31 日，版 13。

卡，入侵全球近十萬台電腦，執行監控任務。國安局大多是透過網路植入這些軟體，不過也有秘密技術，讓軟體侵入沒有連接上網的電腦，該報導指出，這項技術至少從 2008 年就開始使用，仰賴的是小型電路板傳導的無線電波隱蔽頻道，及秘密插入電腦中的 USB。[170]

(四)有線節點攻擊:預先對敵的軍事網路系統實施偵察，摸清網路組成、電子技術設備配置和有線電路，然後再派出信息作戰分隊、深入其網路設置地域，在敵方軍事網路中的有線電路上或節點開缺口，將病毒植入敵方系統。[171]

(五)間諜型:此種病毒進入對方主機後，會按程式設計並竊取特定文件，而自動轉發至特定地點，同樣的手法亦可用來攻擊金融機構主機，竊取主機內的資料，大規模的入侵將造成被入侵國的經濟混亂。2013 年 6 月 9 日美國前中情局(CIA)雇員史諾登(Edward Joseph Snowden)[172]在香港公開接受英國《衛報》記者採訪，披露了美國國家安全局的「棱鏡」(PRISM)計畫，該計畫允許美國國家安全局和聯邦調查局(FBI)進入包括臉書、歌、微軟、雅虎、蘋果等九大網路通訊巨頭的伺服器，通過音頻、視訊、照片、電子郵件等跟蹤網路使用者的一舉一動，以及他們的聯繫人，並為此建立龐大的資料庫。[173]

(六)邏輯炸彈型(Logic bomb):類似定時炸彈，同樣潛伏在對方主機中等待突擊，可在發作時完全控制對方主機而為所欲為，如潛伏此一病毒於某國戰管系統，邏輯炸彈發作時控制戰管系統，令戰管系統下錯誤指令，造成對方誤擊發生敵機/潛混亂事件;亦可潛伏敵國交通管制系統如航空管制或捷運控管電腦，誤導機或電聯車路，令其發生重大交通事故，造成被入侵國社會秩序完全失控。[174]例如 2010 年 11 月，伊朗總統艾哈邁迪內賈德 (Mahmoud Ahmadinejad)公開承認，在伊朗的納坦茲總共部署的 9000 台離心機，因遭一種專門針對工業設備的惡意軟體病毒 Stuxnet(震網)攻擊，致使約 1000 台的離心機損壞。負責調查伊朗核計畫的科學與國際安全研究所（Institute of Science and International Security，IISS）專家認為，由於震網病毒攻擊的不確定性，已經顯著打擊了伊朗人的士氣。[175]此外，2012 年，紐約時報指出，美國官員已承認 2010 年伊朗核電廠遭震網病毒損壞事件，是由美國國安局在以色列協助下所研發的蠕蟲病毒，目的在破壞伊朗基礎核設施，阻止發展核武。[176]這一事件代表美軍成功地開啟網路戰的新時代。

(七)另外值得一提的是，隨著社群網站 facebook、twitter 普及，例如 2011 年阿拉伯之春，已證明宣傳戰在網路時代，對於公眾意見的影響力。雖然阿富汗境內網路覆蓋率不高，但隨著手機持有率，讓塔利班能利用社群網站、衛星

---

[170]〈電波助威 NSA 入侵全球 10 萬電腦〉,《青年日報》, 2013 年 12 月 16 日，版 5。

[171]王正德,《決勝賽柏空間-網路軍事技術及其運用》, 北京:軍事科學出版社，2003 年，頁 128

[172]史諾登（Edward Joseph Snowden)前美國中央情報局雇員，美國國家安全局技術承包人，於 2013 年 6 月在香港將美國國家安全局關於棱鏡計劃監聽專案的秘密文件披露給了英國《衛報》和美國《華盛頓郵報》。

[173]畢誠倢著,〈史諾登洩密案有如網路戰 911〉,《尖端科技》, 第 347 期，2013 年 7 月，頁 5

[174]行政院研究發展考核委員會,《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》, 台北:五南文化出版，2002 年，頁 55。

[175]知遠,《網路戰及其發展演變》, 北京:中南出版傳媒集團，2012 年 8 月。

[176]Dindo Lin 著,〈卡巴斯基 CEO 爆料:俄國太空站與核電廠曾遭病毒入侵〉,《 科技新報》, http://technews.tw/2013/11/14/kaspersky-ceo-stuxnet- iss -nuclear-plant/ (2013 年 11 月 22 日)。

電視與地方媒體宣揚理念，這些打帶跑宣傳，總是希望讓外界認為他們是贏家。網路時代讓這一切變得很容易，雖然在現實戰場失利，但塔利班仍透過包括社群網站在內各種媒體，在宣傳上與美軍打個五五波。[177]2014 年 2 月上旬在烏克蘭反政府示威衝突中，1 名烏克蘭女子透由網際網路，將政府暴行影片告知世人，並強調烏克蘭民眾為自由而抗爭，但電話及網路可能會被切斷，她呼籲全球支持，影片上傳後隨即被熱烈轉載。[178]網路戰作戰方式暨成功案例，如表 2-4。

表 2-4：網路戰作戰方式暨成功案例統計表

項次	網路戰作戰方式	網路戰成功之戰史
1	定時炸彈（中共稱為固態病毒攻擊法）	1991 年美伊波灣戰爭。戰前，美國中央情報局派特工人員到伊拉克，將伊拉克從法國購買的防空系統使用的印表機晶片，換上了染有病毒的晶片，於戰略空襲前，美國利用遠端遙控激活晶片病毒，使伊拉克防空指揮中心主電腦系統程序錯亂、指揮失靈。
2	超載型式（拒絕式服務）	2007 年，俄羅斯利用網路戰力量(拒絕式服務)向愛沙尼亞發起網路攻擊(拒絕式服務攻擊(DDOS))，這支看不見的軍隊與無法量化的戰力，重創愛沙尼亞網際網路系統，使該國政府國會、媒體、銀行及通信等網站無法正常運作。 2013 北韓對南韓示威，癱瘓多家電視台、銀行網路服務在政府部門電腦中植入惡意程式，發動阻斷式(DDos)，影響 3 萬 2 千台電腦及伺服器
3	空間注入病毒法（無線電）	2014 年 3 月馬航 MH370 班機失縱，據 2014 年 3 月 18 日《自由時報》報導指出，馬航客機恐遭人以手機或 USB 隨身碟控制，網路恐佈份子製造的「程式碼」架構，可進入客機的機上娛樂系統，並改寫安全軟體，一旦飛機被駭客入侵即可透過遙控方式，讓飛機改向降落，這可能是全球第一宗網路劫機案。
4	有線節點攻擊	2014 年 2 月 28 日，俄軍一名武裝男子突襲烏克蘭克里米亞地區，破壞其電信公司設施及光纖、電纜，導致當地網路、電話中斷，造成烏克蘭主要政府網站斷線 72 小時。
5	間諜型	2013 年 11 月 27 日，美國安局利用網路監控 6 名身分不明的伊斯蘭「激進分子」，並連結色情網站紀錄，希望找到方法讓他們名聲掃地，讓他們號召追隨者時，可能遭到質疑。

[177]王光磊，〈美軍與塔利班新戰場-社群網站〉，《青年日報》，2012 年 9 月 5 日， 版 6。

[178]陳伃軒，〈烏克蘭實彈鎮壓 死傷逾 600 人〉，《自由時報》，2012 年 2 月 21 日， 版 18。

5	間　諜　型	2014 年，西方情報官員與電腦專家表示，歐洲、美國以及烏克蘭等地的政府電腦網路，被一套俄羅斯所研發的間諜軟體 Turla 所感染，Turla 與 2008 年攻擊美軍中區指揮部，造成歷年來美國最嚴重的資安危機的惡意軟體(Agent.BTZ)系出同門，儘管華府從未點名，但部分官員透露，該網路攻擊來自俄羅斯。 2014 年 1 月 29 日，憤怒鳥遊戲的開發商 Rovio 證實，美國和英國情報機構運用移動應用程序，通過智慧型手機用戶安裝遊戲軟體，跟踪用戶，得到的數據是用戶的姓名，位置，電子郵件地址，電話號碼和應用程序要求，包括種族和婚姻狀況的任何其他信息
6	邏輯炸彈型(Logic bomb)	2010 年 11 月，伊朗總統艾哈邁迪內賈德公開承認，一種專門針對工業設備染可移動式儲存媒體(USB)的惡意軟件病毒 Stuxnet，對伊朗核離心機的機台造成破壞，使得鈾濃縮受到了極大限制。伊朗在納坦茲總共部署了 9000 台離心機，其中的 1000 台離心機遭震網蠕蟲攻擊中損壞。

作者整理

資料來源:參考東鳥，《中國輸不起的網路戰爭》，湖南:人民出版社，2010 年 11 月，頁 42、51;楊舒媚，〈新戶政系統 轉包中國網路公司〉，《中國時報》，2014 年 3 月 11 日，版 11;俞智敏，〈伊朗網路劫機？陰謀論 滿天飛〉，《自由時報》，2014 年 3 月 18 日，版 8;編譯組，〈俄軍入侵 克里米亞遭網攻〉，《青年日報》，2014 年 3 月 6 日，版 6;何世煌著，〈恐怖分子上色情網站 美國監控〉，中央社，<http://tw.news.yahoo.com/%E6%81%90%E6%80%96%E5%88%86%E5%AD%90%E4%B8%8A%E8%89%B2%E6%83%85%E7%B6%B2%E7%AB%99-%E7%BE%8E%E5%9C%8B%E7%9B%A3%E6%8E%A7-205335672.html ＞，(2013 年 11 月 28 日)。"'Spying Birds': Hackers deface Angry Birds website following NSA revelations,"RT, <http://rt.com/news/angry-birds-nsa-hackers-374/>(2014 年 3 月 16 日)。

第四節 小結

網路戰，即為運用有、無線電等網路傳輸手段，將電腦病毒植入對方資訊系統內，或運用特攻人員及先進電子科技武器，對敵人網路節點、系統(資訊機房)及儲存資料實施實體及虛擬(雲端資料)攻擊，以獲取或竄改所需情報、癱瘓、破壞、摧毀敵國重要基礎設施及軍事設備，進而使敵人無法及時產生正確重要決策，或造生人民恐慌而影響政府機制運作及國家整體安全，達到不戰而屈兵之目標，其效果已可達到如同原子彈嚇阻之效，進而達到不戰而屈人之兵目的。

21 世紀是網路的世代，誰掌握了網路的控制權，誰便擁有戰爭的主導權，也因網路技術蓬勃發展，加速了現代戰爭的作戰節奏。以往戰爭的勝利，可能須動員數以百計的特攻、各式載具，及巨大的花費才能完成，隨著網路戰的發展，未來的戰場可能不花一槍一彈就已經結束，取而代之將是依奉國家利益與安全分散在各地的網路高手，藉由手中的鍵盤所完成。美國於 2009 年將陸、海、空及海軍陸戰隊等網路部隊實施整併，並於美國馬里蘭州「米德堡陸軍基地」成立網路司令部，直屬於美國戰略司令部，於 2010 年正式運作。另據 2013 年美國戰略與預算評估中心指出，因應美國經濟不景氣，各項國防預算於遭刪減，惟獨無人行載具及網路戰繼續加強投資。此外，據聯合國裁軍研究所指出，截至 2013 年 5 月，全球成立網軍部隊已有 46 個國家。另值得注意，自 2011 年網路戰課題已納入歐、美、日及韓等重要軍演項目。從這些報導顯示，網路戰的重要性的確不容忽視。

網路作戰模式因科技帶來變化。從最早利用網路病毒入侵及網頁竄改，以癱瘓敵軍指管系統，再到 2010 年美國在以色列協助下，發展出史上第一個可以直接破壞伊朗重要核設施離心機的震網病毒，最後到 2013 年美國暴發史諾登事件，報導美國安局如何藉網路手段，監聽及追縱各國政府及伊斯激進分子通聯及上網紀錄，無疑將網路戰發揮到不戰而屈人之兵的最高作戰境界。因此，資訊科技能力將是未來衡量網路戰的重要標誌。

除此之外，未來的戰場將是數位化戰場，網路將可將偵察系統、武器載台系統整合在一起。故擁有網狀化部隊將可如預期地勝過缺乏網路能力的部隊，而網路、電力及通信基礎等缺乏的國家，將無法佔有先機，如同孫子兵法所強調的，先處戰地而待敵者逸，後處戰地而屈戰者勞。網路戰的目標，不只是透過大量的技術提高效率而已，它還可能讓所有兵員從戰場上撤出，並確保避免傷及無辜百性，故網路戰的未來的確值得重視。

第三章 中共發展網路戰之經過

1991 年美伊波灣戰爭爆發後，中共瞭解到以往農業時代的人海戰術，以及工業時代的鋼鐵戰爭，將無法打贏資訊化時代的網路戰爭，同時瞭解到網路戰與電子戰將成為當今主宰戰場至關重要的作戰武器，地面戰僅用在擴張戰果。[179]因此，對中共而言，網路既是力量的倍增器，又是重要戰略資源，網路攻擊將左右未來戰爭的型態和前途，善於控制與利用網路將與勝利同在。[180]另據中華民國 102 年《四年期國防總檢討》指出，中共已成立『資訊網路作戰部隊，積極研製資訊作戰平臺，並結合民間能量，大幅提升網路作戰能力。』[181]從上述資料顯示，中共網路戰實力已不容小覷。本章探討中共網軍成立背景、發展過展，以及網路戰與中國安全。

第一節 中共成立「網軍」之背景

一、波灣戰爭獲取之教訓

美國國防部指揮控制政策局前局長坎彭(A.Campen)在《第一場信息戰爭》(The First Information War)一書中指出:『波灣戰爭是人類社會進入資訊化時代之所經歷的第一場資訊戰爭。』[182]中共從波灣戰爭得到教訓，未來戰爭型態隨著科技發展已明顯變化，戰場範圍將由陸、海、空延伸至太空，戰爭規模，將是交戰雙方在政治、經濟、外交、科技和力全面對抗，建軍、用兵發展趨勢，將朝「高科技」、「量少質精」方向實施改革。[183]

除此之外，中共從波灣戰爭軍事變革與戰爭經驗得知，掌握戰場的資訊優勢的一方，將可獲得一場絕對勝利的高科技戰爭。[184]中共體認到，惟有對大規模及裝備參差不齊的地面部隊，進行裁撤減併和調整軍兵種規模比例，才能建立一支符合「精實、合成、高效」的新型態軍隊。[185]2008 年，美國學者阿米里特德亦披露，中共的戰略家在吸取波灣戰爭教訓後，體認出技術裝備落實的軍隊，在面臨高科技裝備的強國，如美國與歐洲部隊，將處於絕對的劣勢。[186]

1999 年，中共解放軍出版社的《2020 年的武器》一書指出，波灣戰爭是體系與體系對抗的高技術局部戰爭，是在地面、海上、空中、太空、電磁等 5 維戰場同時進行的戰爭，要打贏戰場上的各種控制權，就是要把三軍各類武器的軟體和硬體結合起來，以發揮整體作戰優勢。[187]2000 年 3 月，中共學者張軍亦指表示，

---

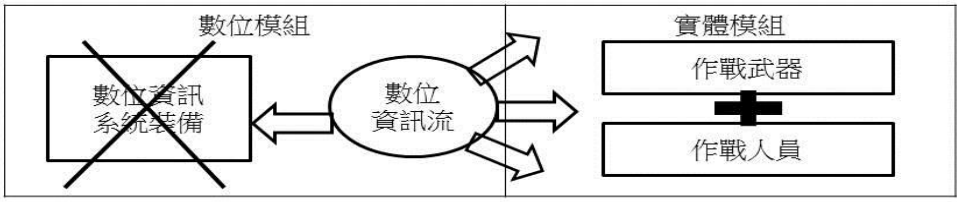
[179]國防部史政編譯局譯，阿里斯特德(Leigh Armistead)，《資訊作戰-以柔克剛的戰爭》(Information Operations :Warfare and the Hard Reality of Soft Power)，台北:國防部史政編譯室，2008 年，頁 237。
[180]行政院研究發展考核委員會，《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》，台北:五南文化出版，2002 年，頁 95。
[181]國防部，中華民國一〇二年《四年期國防總檢討》(Quadrennial Defense Review)，台北:五南文化出版，2013 年，頁 18。
[182]唐仁俊，〈中共信息戰之發展與限制〉，《空軍學術雙月刊》，第 619 期，2010 年 10 月，頁 27。
[183]劉慶元，《解析中共國家安全戰略》，台北:揚智文化出版社，2003 年，頁 59。
[184]行政院研究發展考核委員會，《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》，台北:五南文化出版，2002 年，頁 45。
[185]黃鈴，《「信息化戰爭條件」下之共軍對台戰略》，政治作戰學校政治研究所碩士論文，2005 年 6 月，頁 42。
[186]同註 179，頁 259。
[187]林宗達，《中共軍事革新之信息戰與太空戰》，台北:全球防衛雜誌社，2002 年，頁 27。

以往工業時代軍隊的指揮體制呈多層次樹狀結構，這種結構有很多弊端，如資訊傳遞時效過長、偵察系統與武器不能橫向構通、抗毀能力差，一旦某個節點遭受破壞指管通連系統便受影響，甚至嚴重到癱瘓。[188]根據美國《2005 年中國軍力報告》的透露，中共解放軍已將心理戰與打擊敵人領導中心及指揮通訊節點列為各階段優先主要攻擊目標。[189]

2002 年，我國行政院研究發展考核委員會所出《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》一書批露，中共當局研究資訊戰，是以國家戰略從資訊技術、相關基礎建設、戰術戰法以及戰略思維等方面同步著手，並以支持打贏「高技術條件下的局部戰爭」為著眼。在戰略上，以 863 計畫，採取「有限目標」、「突出重點」的方針，選取包括「信息技術」，建立優勢的高技術條件，並為資訊戰科技奠定基礎;另外在戰術上，積極建立網狀化指揮管制能力及網路攻擊技術，並構想組建網軍新兵種，企圖以發展「電腦病毒」、「邏輯炸彈」等武器，達成「以破壞數位模組癱瘓實體模組」的資訊戰槓桿戰略，如圖 3-1。[190]

圖 3-1:中共資訊戰槓桿戰略圖

信息槓桿戰略	1. 以破壞「數位模組」使「實體模組」失能。 2. 以「四兩」癱瘓「數位模組」，取代以「千斤」摧毀「實體模組」。 3. 以「間接、無形、虛擬」奇襲資訊裝備的「數位模組」，達成使「實體模組」系統，如作戰系統以及政府機制、經濟、社會機能等運作癱瘓效果。



資源來源: 行政院研究發展考核委員會，《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》，台北:五南文化出版，2002 年，頁 89。

[188]張軍著，《IT 戰爭》，北京:科學出版社，2000 年 3 月，頁 3。
[189]陳憶綾，《解放軍資訊戰對台軍事安全影響之研究》，政治作戰學校政治研究所碩士論文，2006 年 6 月，57。
[190]行政院研究發展考核委員會，《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》，台北:五南文化出版，2002 年，頁，89。

二、網路作戰符合不對稱作戰

1999 年，中共二位空軍大校喬良及王湘穗在所著《超限戰》一書指出，隨著資訊技術的出現，戰場空間將發生根本性的改變，從陸、海、空、天，延申至「人造空間」，作戰人員不再是職業軍人，而開始呈現出「平民化」傾向。作戰手段超越傳統範圍的新戰爭型式，它包括了傳統戰爭手段，同時也包括了貿易戰、金融戰、新恐怖主義及生態戰。[191]同時，曾任國內通次室次長的林勤經中將表示，中共「信息戰」是一種「不對稱戰爭」的新戰爭型態。[192]

中共了解自身三軍武器現代化程度遠遠落其假想敵美、日，然而這些國家卻又依賴資訊化、科技化，而這個「脆弱環節」便成為共軍「電子珍珠港」(An Electronic Pearl Harbor)侵襲極佳目標。[193]此外，中共也認為癱瘓敵方金融、交通、電力、電信及軍事核心機制，可以獲得最作戰效益。[194]網路空間對抗，就戰術層面而言，網路入侵(cyber invasion)絕對是「不對稱」，因為此種駭客式軍事行動不需要先進科技，只針對網際網路 TCP/IP 協定開放性弱點，便可瓦解敵軍指揮系統。[195]我國 2004 年《國防報告書》亦指出，中共面對優勢之敵，將以各種軍事或非軍事手段爭取勝利，運用精準武器打擊，配合多樣化的不對稱作戰戰術戰法例如太空威脅、導彈威脅、巡戈彈、無人攻擊載具、電腦戰、電磁脈衝彈等，對敵政、經、軍重要設施實施破壞，用最小代價獲致最大成果。[196]

2012 年，美國學者歐森(Soren Olson)表示，運用網路戰來打擊諸如戰略資訊這種意想不到的目標，極符合中共的「殺手鐧」作戰構想。一旦確認敵人的強、弱點並加以評估後，避開其強項，而以殺手鐧攻擊其弱點，如同 2004 年至 2012 年，中共至少發動至少 14 次大規模網路攻擊，攻擊目標從「埃克森美孚石油公司」(Exxon Mobile)與德國經理辦公室，到印度與美國國防部軍事網路。[197]同年，中共學者莆勛、區肇威亦表示，中共刻正積極發展「殺手鐧」手段的東風 21D 型反艦彈道飛彈系統及反衛星飛彈，以構成中國以不對稱的手段對抗美國優勢海、空軍，使美國無法承受高代價，而讓中共獲取主動權。[198]

2012 年，我國國防大學戴政龍上校表示，自 2003 年第 2 次波灣戰爭後，中共體認出世界新軍事變革加速發展，戰爭形態正由機械化向資訊化轉變，資訊化成為提高軍隊戰鬥力的關鍵因素，各項武器載具資訊系統的對抗將成為戰場對抗的主要特徵，非對稱、非接觸、非線性作戰成為重要作戰方式。[199]2013 年，美國加州大學國際關係研究中心「中國大陸創新及科技研究計畫」副執行長包克文

---

[191]喬良、王湘穗，《超限戰》，台北:左岸文化出版社，2004 年，頁 111-129;188-196。
[192]李承瑀，《中共高技術條件下信息戰之研究》，政治作戰學校政治研究所碩士論文，2000 年 6 月，頁 20。
[193]行政院研究發展考核委員會，《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》，台北:五南文化出版，2002 年，頁 49。
[194]同前註，頁 1。
[195]同前註，頁 54。
[196]國防部，《中華民國 93 年國防報告書》，台北:五南文化出版，2004 年，頁 48。
[197]高一中譯，Soren Olson，〈檯面下較勁:網路戰與戰略經濟攻擊〉(Shadow Boxing: Cyber Warfare and Strategic Economic Attack)，《國防譯粹》，第 39 卷，第 12 期，2012 年 12 月，頁 48。
[198]莆勛、區肇威，〈美國在亞太區域的不對稱作戰〉，《軍事連線》，第 52 期，2012 年，12 月，頁 63-64。
[199]載政龍，〈中共網軍發展與網路攻防:兼論我國資通安全之政策規劃〉，《戰略評估》，第四卷，第四期，2012 年冬季，頁 101。

(Kevin L.Pollpeter)指出，中共將網路戰視為未來新型態作戰及不對稱「殺手」武器，具有改變傳統作戰概念之潛力，在未來將扮演作戰成功關鍵角色。[200]由上可知，中共期藉由網路戰做為不對稱作戰的主要作戰形態，以發揮最大獲益效果。

研究中共軍事專長的美國學者穆文濃(James C.Mulvenon)曾表示，中共和美國的不同，是中共基本上把網路視為一種國力的工具，故利用網路達到戰略與政治目的，被中共視為一種理所當然的手段。[201]另一位美國學者成彬(Dean Cheng)也曾表示，中共期藉綜合國力以戰略嚇阻以脅迫或嚇阻敵人，其中關鍵要項就是可提供各類所望戰爭的實際軍力，此點意味著部署 1 支能行「資訊化條件下局部戰爭」的軍隊，亦即運用現代資訊技術，俾在陸、海、空、外太空和網際空間遂行非接觸、非線性及不對作戰的聯合部隊。[202]據此，中共刻正發展一支網路部隊力量，以爭取不對稱作戰勝利目標。

三、科索沃戰爭之影響(中共意識到加強研發網路戰之重要性)

1999 年科索沃戰爭及 2001 年阿富汗戰爭後，中共觀察北約(North Atlantic Treaty Organization,NATO)以及美國為首的聯軍的作戰模式後，更加確認「資訊化」是未來戰爭必然要件與趨勢。[203]2004 年 3 月，中共前中央軍委主席江澤民在參加第十屆全國人大二次會議時表示:推進中國特色軍事變革，必須抓住資訊化這個本質和核心，建設資訊化軍隊、打贏資訊化戰爭為目標。[204]

2004 年，《中國的國防》白皮書揭櫫:人民解放軍按照建設信息化軍隊、打贏信息化戰爭的目標，積極推進以信息化為核心的中國特色軍事變革。該白皮書在第二章國防建設「加緊軍事鬥爭準備」指出:「人民解放軍立足打贏信息化條件的局部戰爭。」[205]2006 年《中國的國防》白皮書在國防政策之目標指出，解放軍必須做好準備打贏資訊化條件下的局部戰爭，著眼維護國家主權、安全和發展利益的需要。[206] 2008 年《中國的國防》白皮書指出，『以資訊化為國防和軍隊現代化的發展方向，立足國情軍情，積極推進中國特色軍事變革，科學制定國防和軍隊建設戰略規劃、軍兵種發展戰略，2010 年前打下堅實基礎，2020 年前基本實現機械化並使資訊化建設取得重大進展。』[207]由此可知，中共已將網路戰納入國家安全重要指標。

---

[200]王明達，〈共軍發展 A2/AD 戰略層級政治作戰須特別關注〉，《青年日報》，2013 年 12 月 4 日，版 3。

[201]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》，第 311 期，2010 年 7 月，頁 86。

[202]高一中，Dean Cheng，〈中共對嚇阻的觀點〉(Chinses Views on Deterrence)，《國防譯粹》，第 38 卷，第 4 期，2011 年 4 月，頁 52。

[203]載政龍，〈中共網軍發展與網路攻防:兼論我國資通安全之政策規劃〉，《戰略評估》，第四卷，第四期，2012 年冬季，頁 102。

[204]〈中共中央軍委主席江澤民、中央軍委副主席胡錦濤參加十屆全國人大二次會議解放軍代表團全體會議發表講話內容。〉，《解放軍報》，
http:big5.xinhuanet.com/gate/big5/news.xinhuanet.com/newscenter/2004-03/11/content_1360725.htm(2004 年 3 月 11 日)

[205]黃鈴，《「信息化戰爭條件」下之共軍對台戰略》，政治作戰學校政治研究所碩士論文，2005 年 6 月，頁 12。

[206]中華人民共和國國務院新聞辦公室，〈2006 年中國的國防白皮書〉，《中華人民共和國國防部》，< http://www.mod.gov.cn/affair/2011-01/06/content_4249948_6.htm >（2013 年 12 月 8 日）。

[207]中華人民共和國國務院新聞辦公室，「《2008 年中國的國防》白皮書」，《 中華人民共和國國防部》，< http://www.mod.gov.cn/affair/2011-01/06/content_4249949.htm>（2013 年 12 月 8 日）

中共的戰略家認為，中共必須尋求一種能跨越世代戰力的方式，以為打贏下一場戰爭做好準備。中共解放軍將不會揚棄舊有系統，而是在新式系統加強資訊化概念，提升整體戰力。[208]大陸知名軍事評論家劉亞洲上將表示，資訊化戰爭時代，已經孕育著一個世界新帝國的雛形，任何國家若不能明白這點，長遠後果將令人感到「恐懼」。[209]根據 2014 年 1 月 14 日《旺報》的報導，面對新一輪軍事革命浪潮和發展，中共解放軍將繼續加強資訊作戰能力。[210]

2009 年，美國戰略司令部主管全球網路行動的克隆上校(Colonel Gary McAlum)亦表示，中共逐漸意識到以網路作為一種新型態的戰爭工具的重要性，因此軍事務革新的重點聚焦在資訊戰發展上，藉由不斷地加強資訊戰相關訓練，以取得任何時間、地點的資訊優勢。[211]由此可知，中共對網路戰是愈來愈重視。

另值得一提的是，中共歷來年首任直升解放軍總參謀長，由北京軍區司令房峰輝上將擔任，據報導簡歷中表示，他對電子科技鑽研的十分深入，最大樂趣就是鑽到電腦房，研究開發軍事指揮的新軟體。在擔任北京軍區司令員期間，房峰輝加快北京軍區部隊轉變戰鬥力生成模式，持續開展實實戰化訓練，全面提升了信息化條件下作戰能力，先後參加上合聯演、跨區演習等重大演訓活動。[212]中共學者易予聖表示，此舉代表為未來中共解放軍重要人事應具備「科技知識背景」與「學位」，而「根紅苗正」將逐漸過去式;且昔日南京軍區總掌大位的慣例，似乎因兩岸關係緩解而轉變(由北京軍區司令出任)。[213]

[208]周敦彥譯，Thomas Henderschedt，〈共軍資訊人作戰之借鏡〉(Learn from the PLA？)，《國防譯粹》，第 39 卷，第 10 期，2012 年 10 月，頁 3。
[209]劉俊英主編，《中共研究》(China Studies)彙編，台北:國防部部長辦公室，2006 年，頁 150。
[210]陳曼濃，〈軍事革命浪潮 生化戰將登場〉，《旺報》，2014 年 1 月 14 日， 版 8。
[211]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》，第 311 期，2010 年 7 月，頁 86-89。
[212]〈中國人民解放軍高階將官更換〉，《尖端科技》，第 340 期，2012 年 12 年，頁 77。
[213]易予聖，＜遠眺亞太 2013 避險或再平衡＞，《尖端科技》，第 340 期，2012 年 12 月，頁 42。

第二節　中共「網軍」之發展過程

一、理論探討

在中共有關網路戰理論研究方面，具有軍職身份的沈偉光堪稱第一人。1985年沈偉光首度提出網路戰爭的概念，並撰寫出數萬字相關的學術文章。1987年，中共軍方《解放軍報》以專刊開始介紹沈偉光對網路戰研究的學術觀點，然而並未引起廣泛的討論。時至波灣戰爭後，於1995年12月，在石家莊中共陸軍參謀學院，邀集來自全軍的30多位高級專家研討。會議的題目是:「迎接世界軍事革命的挑戰」，在這次的會議上，軍事專家們一致認為，一場以信息技術為基礎和核心的軍事革命浪潮，正在把世界各國的軍隊推向這場新的軍事革命的入口處。中共軍隊也應該勇敢地迎接這場革命，走入新的軍事革命理論和實踐的殿堂。[214]從此中共便開始積極投入如何打贏高科技的局部戰爭之研究。

1999年，喬良及王湘穗二位中共海軍大校提出備受矚目的「超限戰」論點，二人在書中表示，資訊技術的出現，為各種新、舊技術匹配使用，提供無限的可能。在未來戰場，藉由網路將任何武器載台與資訊系統整合，可有效提升攻擊能力。此外，利用駭客、媒體等非戰爭的行動，將成為未來戰爭的新構成因素，從而打破戰爭與非戰爭、軍事與非軍事之界限。簡言之，所謂「超限戰」，即運用一切手段，包括武力和非武力、軍事和非軍事、殺傷和非殺傷的手段達到戰爭的目。「超限戰」旨在超越一切傳統戰爭形式，以各種方式打擊敵人。[215]

2002年，曾任中共總參謀部四部部長載清民少將表示，網際網路時代，網路成為國家的戰略命脈和戰略資源，一旦重要的網路陷入癱瘓，整個國家安全面臨崩潰。網路戰手段將導致未來戰爭的平民化，攻擊目標由軍用網路拓展到民用網路，一個國家網路建設越發達，對網路的依賴程度越高，受到網路攻擊的威脅也越大。當網路戰的戰略地位更加突出，戰爭主體、客體涉及到廣大民眾，網路戰向另一個方向發展，即形成「網路威懾」，當敵對雙方都具有確保侵入、破壞對方網路的能力，就可以帶來雙向的網路遏制。另指出現代間諜手段的發展有一個新領域，就是網際網路，電腦網路是機密集中的地方，因此網路正在成為一種重要的間諜手段。[216]

2007年，中共副總參謀長張黎上將，及軍事科學院世界軍事研究部長閔振范少將及和研究員王保存少將指出，信息時代的主要軍隊形態為高素質、兵力少、整體性強，並因應網路戰決定陸、海、空、天戰的勝敗，故部隊將來可能成立一個新的軍種-「網軍」。[217]同年，中共學者楊世松表示，要確保軍事信息保障能力，應組建統一和權威的軍事信息保障領導機構，從戰略的高度來統纜資訊保障工作，制定宏觀的政策，協調各種關係，進行統一管理，統一保障，提高資訊保障工作的整體效能。[218]

為了能有整合有關網路戰相關理論的研究，中共軍方於2001年至2003年間，分別在鄭州、濟南、北京、南京、西安5大城相關的網路戰部隊或研究部門

[214]唐仁俊，〈中共信息戰之發展與限制〉，《空軍學術雙月刊》，第619期，2010年10月，頁31。
[215]喬良、王湘穗，《超限戰》，台北:左岸文化出版社，2004年，頁81-83。
[216]載清民，《直面信息戰》，北京:國防大學出版社，2002年，頁57。
[217]張黎，《構建信息化軍隊的組織體制》，北京:解放軍出版社，2004年，頁37-42。
[218]楊世松，《軍事信息能力論論》，北京:軍事科學出版社，2007年，頁144-148。

組建性質不同的研究中心，分別為:1.鄭州組:於濟南軍區建「網路戰」模擬研究中心;2. 濟南組:於濟南軍區建立「網路戰」保密研究中心;3.北京組:於北京軍區建「網路戰」作戰研究中心;4 南京組:於南京軍區建立「網路戰」情報研究中心;5 西安組:於蘭州軍區建「網路戰」裝備發展中心。[219]將網路戰理論的研究系統化，對中共發展網路戰理論的建構具有正面的效果。

二、科技研發

(一)科技技術規劃

中共自 1970 年代末期以來在經濟與科技方面的驚人成就，及是共軍推展現代化與戰略方案的重要助力，例如，中共的電信市場能夠吸引國外資金挹注與引進科技，並且促使本國的資訊科技欣欣向榮，進而直接影響共軍的指管通資情監偵(C4ISR)的革命。[220]我國林勤經中將亦表示，中共早在 1980 年代中期已經開始發展下一代戰爭的能力，並對當前信息戰裝備的研究，更是不遺餘力積極開創這種戰爭武力。[221]

1986 年 3 月，由中共科學家王大珩、王淦昌、楊嘉墀、陳芳允等 4 位上書中央軍委，要求中共建立《高技術研發綱領》成立「863 計畫」，這計畫對中共建立現代化軍事具有深遠的影響。在「863 計畫」中，涉及資、電作戰領域有:太空、網路技術、雷射技術及自動化技術。1996 年，中共宣布實施「超級 863 計畫」，規劃 2010 年前中共的技術發展綱要。為落實國家中長期科學和技術發展，中共提出《國家中長期科學和技術發展規劃綱要(2006-2020 年)》，加強面向國家戰略需求的基礎研究。2006 年 10 月 10 日中共在北京召開國家重點基礎研究發展計畫(973 計畫)專案，由中共科技部副部長程津培和副秘書長王志學出席會議，並向專案首席科學長頒發聘書。2006 年，經過三輪專長評論，中共科技部共批准 65 個專案立項。在信息領域，部署納米尺度矽集成電路器與工藝，寬頻光纖與無線電信息網路中的光子集成與微納入電集成，瞄準智慧信息處理和下一代網路等方面的基礎研究。[222]

此外，1995 年，《中共中央關於制定國民經濟和社會發展「九五」計劃和 2010 年遠景目標的建議》揭露，資訊產業被列入經濟建設的主要任務和戰略佈局重要內容之一。[223]為使資訊戰能獲得更大之突破，2000 年 3 月中共國家主席江澤民簽署一項名為「126」計畫(此一計畫包含 35 個主題項目於六大項目內)，電子訊息技術系統即被列作此一發展計畫中。[224]

隨著高科技戰爭的來臨，如何縮短與西方國家的科技距離，成為中共發展網路戰必須要走的路，中共中央政治局常委、國務院總理溫家寶曾表示，資訊化是當今世界發展的大趨勢，是推動經濟社會發展和變革的重要力量。制定和實施

[219]唐仁俊，〈中共信息戰之發展與限制〉，《空軍學術雙月刊》，第 619 期，2010 年 10 月，頁 31。
[220]國防部史政編譯局譯，毛文杰(James C.Mulvenon)、譚睦瑞(Murray Scot Tanner)、蔡斯(Michael S. Chase)、傅里林格(David Frelinger)、龔培德(David C.Gompert)、李比奇(Martin C.Libicki)、包克文(Kevin L. Pollpeter)，《中共對美國軍事變革之反應》(Chinese Responses to U.S.Military Transformation and Implications for the Department of Defense)，台北:國防部史政編譯局，2010 年，頁 20。
[221]林勤經，〈兩岸資訊戰力之比較〉，《全球防衛雜誌》，第 187 期，2000 年 3 月，頁 70。
[222]唐仁俊，〈中共信息戰之發展與限制〉，《空軍學術雙月刊》，第 619 期，2010 年 10 月，頁 34。
[223]張軍主編，《IT 戰爭》，北京:科學出版社，2000 年，頁 245。
[224]林宗達，《中共軍事革新之信息戰與太空戰》，台北:全球防衛雜誌社，2002 年，頁 43。

國家資訊化發展戰略，是順應世界資訊化發展潮流的重要部署，是實現經濟和社會發展新階段任務的重要舉措。[225]2013 年，中共上海國際關係研究院網站一篇〈當前網路空間全球治理困境〉專題指出，國家在網路空間中的能力大小，決定了其對網路空間中權力與資源、開放與穩定、發展與繁榮，而網路能力評鑑的標準是從一個國家的高科技技術及重要基礎設施來評斷。[226]

2013 年 7 月，共軍政工「星網工程」2,500 套改進型接收裝備系統全面配發野外駐訓部隊，達到執行非戰爭軍事任務部隊的資訊需求，連隊網路聯通率已達 91.4%，並強調『輻射全軍的政工網站集群，蔚然列陣』。軍政共網「星空版」網站目前開設 28 個頻道，2013 年下半年，「星網工程」展開後繼建設，實現網路多媒體資訊、電影和電視、廣播節目直接收、實施播放功能。[227]同年 8 月，中共《遠望雜志》報導，漢東湖國家自主辦新示範區暨「中國光谷」是中共最大的光纜和光電器件研發產基地。2001 年獲批為國家光電子產業基地，截至 2013 年 8 月示範區注冊企業已達 2 萬多家，初步形成光電子信息產業的生產聚落，去年企總收 5006 億元。[228]由此可知，中共在網路戰的基礎建設，也是納入影響未來網路戰的一個重要因素。

(二)購置超級電腦

1996 年 1 月，中共以「學術用途」向美採購 6 台超級電腦，此種每秒運算可達數兆次設備，除了可用於民間科學用途外，也是發展核武不可或缺的裝備，更危險是它的運算能力是一般個人電腦的千倍，應用在「網路戰」上是牛刀小試，這些超電腦絕對有能力在極短時間內癱瘓、破壞整個中、小型國家網路。[229]

2013 年 6 月 19 日，《中共解放軍報》報導，中共國防科技大學所研製成功「天河二號」超級電腦系統，在 2013 年 6 月德國萊比錫舉行的 2013 國際超級計算機大會上，以優異性能位居榜首。[230]同年，中共《遠望》雜誌披露，中國首台自主設計的「龍芯 3B」八核心處理器的萬億次高性能電腦「KD-90」[231]已由中國科學技術大學與深圳大學聯合研製成功，並在通過專長組鑑定，其評鑑結果認為「KD-90」是高性能計算機國產化的一次重要突破，在編程模型和網路等關鍵技術上達到世界先進水平，適用於高性能計學教學、大規模科學與工程計算，以及軍事科學、國家安全和國民經濟建設等領域。[232]

---

[225]潘小剛、周亞明、肖琳子，《中國信息安全報告-預警與風險化解》，北京:紅旗出版社，2009 年，頁 33。

[226]魯傳穎，〈試析當前網路空間全球治理困境〉，《上海國際問題研究院》，http://www.siis.org.cn/index.php?m=content&c=index&a=show&catid=15&id=557(2014 年 2 月 14 日)

[227]張淑中，〈中國大陸 12 五規劃執行成效及對台灣經濟的影響〉，《中共研究》，2013 年 9 月，第 47 卷，第 9 期，頁 159。

[228]新華網，〈習近平:科技是國家強盛之基〉，《遠望》，第 299 期，2013 年 8 月，頁 4。

[229]行政院研究發展考核委員會，《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》，台北:五南文化出版，2002 年，頁 53。

[230]〈習近平對天河二號超級電腦系統研制成功作出重要批示〉，《解放軍報》(北京)，2013 年 6 月 19 日，版 1。

[231]「KD-90」是中共國家科技重大專項「高性能多核 CPU 研發與應用」支持項目，由中科院院士、中國科技大學教授陳國良為負責人的科研團隊，歷時一年成功。「KD-90」較上一代，「KD-60」實現了三低一高的特性，成本低於 20 萬元，功率低於 900W，占地面積降低 0.12 平方米，性能高達每秒 1 萬次。

[232]徐海濤、鮑曉菁，〈我國首台基於龍芯 3B 的萬億次高性能電腦研制成功〉，《遠望》，第 293 期，

另據報導，中共陸軍師、團級指揮所及海軍各種艦船所使用的筆電，主要廠商來自中共武漢數字工程學院。此外，全軍使用的筆電主要的廠商為航天科工(CASIC)的二院 706 所。為防止網路洩密，軍隊和國家祕密單位的電子郵件加密、安全系統也是 706 所研發重心。[233]綜合上述得知，中共為實現建設現代化軍隊，打贏下一場資訊化戰爭，在科技方面投注相當心力。

(三)重要基礎設施

根據中共學者崔國平的透露，中共自 1996 年 6 月，在國家的「九五計畫」中，建立 30 個省市的 CHINANET 骨幹網總長度 32,000 公里的信息高速公路。此外，在 1998 年 8 月，歷時 8 年建設的全國 8 縱 8 橫光纖網建成。1999 年 3 月 31 日，中國通信信息網路開通，它是一個基於網際網路，面向政府、企業、社會，提供面方位多層次服務的通信專業信息庫。[234]此外，據報導，中共在國家引導和支持下，北京、上海、寧波等城市均完成光網城市建設計畫，以提升通信網路頻寬，促進產業轉型升級。截至 2010 年年底，中共光纖線路已達到 9990,000 公里，光纖網路覆蓋到全國所有城市、98%鄉鎮和 80%的行政村。[235]

國內戰略學者蔡翼先生曾指出，中共解放軍的軍用電話網路、全軍數據通信網路及野戰綜合通信系統，已由代號為 975 號通信幹線工程完成專用光纖網路、通信衛星系統、微波通信系統、短波無線電台及自動化指揮和控制網路組成，使得中央軍事指揮機關與基層部隊，及駐沿海島嶼、邊與海防部隊的連繫大大提升。[236]由中共學者潘小剛、周亞明、肖琳子等 3 人於 2009 年披露，到 2010 年，中國信息產業市場規模預計將翻兩翻，資訊產業增加值佔 GDP 的比重將超過 8%，成為支撐國民經濟持續增長的戰略產業。[237]

此外，1990 年 4 月，由中共國家計委、國家科委、中國科學院、國家自然科學基金會、國家教委配套投資和支持的中關村地區教育與科研示範網路(NCFC)工程啟動，主要目標將北京大學、清華大學和中科院等三個單位之關建設高速網路，並建立一個超級計算機中心，中關村地區教育與科研示範網路於 1992 年全部完成建設，1994 年 4 月 20 日正式開通以全功能訪問國外網路的專線。同年，5 月 21 日，中國科學院計算機網路信息中心完成中國國家頂級域名(CN)注冊，設立了中國自己的域名註冊器，1996 年 1 月全國骨幹網路建成並正式開通。[238]

2013 年 2 月，頁 3。

[233]山本進一、平可夫，〈中國陸軍數據鏈 使用更多加固式電腦〉，《漢和防務評論》，第 101 期，2013 年 3 月，頁 49。

[234]崔國平主編，《國防信息安全戰略》，北京:金城出版社，2000 年，頁 94。

[235]高光耀、鄭從卓，〈我國光網城市建設的主要問題及對策研究〉，《未來與發展》，第 4 期，2013 年，頁 4。

[236]蔡翼主編，《崛起東亞-聚焦新世紀解放軍》，台北:勒巴克顧問出版社，2009 年，頁 143

[237]潘小剛、周亞明、肖琳子，《中國信息安全報告-預警與風險化解》，北京:紅旗出版社，2009 年，頁 37-38。

[238]馬亞西、成冀、王漢水，《網路戰-地球村時代的戰爭》，北京:國防出版社，1999 年，頁 15。

三、網軍建立

(一)部隊規模

在江澤民時期(1989 年-2002 年任中共總書，1989 年-2004 任中央軍委主席)，中共為能縮短與先進國家軍隊間的技術差距，推動軍事事務革新，規劃將現代化重點自「機械化」扭轉為「發展資訊技術為主的網路與硬體」，人力密集的部隊轉變成技術本位的勁旅。中共並分別於 1997 年裁撤 50 萬，及 2002 年裁撤 20 萬員額。[239]此外，自 2000 年以來，中共解放軍最重要轉型之一，就是努力建立「資訊化」部隊，係以運用電腦、通信系統、網路等資訊科技，以尋求美國所謂的「資訊優勢」(information dominance)。[240]

國內學者黃玲曾指出，中共為打贏未來信息化戰爭的必然要求，必須高度優化軍隊內部結構，並加強航天部隊、戰役戰術導彈部隊、電子戰部隊和特種部隊等技術密集型等軍兵種建設。[241]2013 年，中共「十八屆三中全會」在軍隊改革部分強調，在網路盛行時代，中共解放軍編制改革重點，必須發展符合未來戰爭需求的「網軍」部隊。[242]中共將全面深化改革軍事建設的方向，修正已往奉行的「大陸軍」主義，致力發展海、空軍及信息化部隊，目標將解放軍從人力密集型轉向技術密集型。[243]

根據 2011 年 4 月 23 日，中共中央軍發表的「2020 年前軍隊人才發展規劃綱要」中披露，因應科技的變遷，中共兵力將從 230 萬大幅裁減 150 萬人，以培養網路戰等新型人才。另外，還首次允許海外華人加入，走向所謂的「高素質之路」。針對軍人素質方面，未來十年著養培養四種人才，分別適合作戰的指揮人才、資訊化建設管理人才、資訊化技術專業人才以及新裝備與維護人才。[244]

中共為有效管控境內網路安全，於 1996 年年初，由國務院正式成立由一位副總理擔任組長的全國信息化工作領導小組，負責全國信息產業的領導和協調工作。[245]在此浪潮下，1998 年國務院成立「信息產業部」，對全國各相關部門進行分工。[246]鑒於網路安全自身之脆弱，中共自 1999 年 8 月成立「網路安全中心」，以管制不良信息和保護信息安全。[247]

2001 年 8 月中共重新組建國家信息化領導小組，加強對全國信息工作的指導。同時，中共並成立國家信息化專家諮詢委員會，對國家信息化發展戰略做出

---

[239]袁平譯，Nan Li，〈中共擴張海權之企圖〉(Scanning the Horizon for “New Historical Missions”) ，《國防譯粹》，第 37 卷，第 12 期，2010 年 12 月，頁 86。

[240]國防部史政編譯局譯，費學禮 (Richard D. Fisher Jr.)，《中共軍事發展-區域與全球勢力佈局》(China’s Military Modernization-Building for Regional and Global Reach)，台北:國防部史政編譯局，2011 年，頁 190。

[241]黃鈴，《「信息化戰爭條件」下之共軍對台戰略》，政治作戰學校政治研究所碩士論文，2005 年 6 月，頁 42-43。

[242]王莉絹，〈調舊、建新、優化 軍隊改革迎擊科技戰〉，《聯合報》，2013 年 12 月 9 日， 版 13。

[243]張國威，〈海空精兵化 10 次軍改裁 200 萬人〉，《旺報》，2014 年 2 月 12 日， 版 6。

[244]陳思豪，〈共軍轉型 要裁 80 萬人〉，《聯合報》，2011 年 4 月 23 日， 版 15。

[245]崔國平主編，《國防信息安全戰略》，北京:金城出版社，2000 年，頁 94。

[246]張軍主編，《IT 戰爭》，北京:科學出版社，2000 年，頁 245。

[247]行政院研究發展考核委員會，《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》，台北:五南文化出版，2002 年，頁 52。

全面部署，為未來信息化發展提供明確指導。[248]2003 年 9 月，國務院信息辦公室成立網路與信息安全領導小組，成員有信息產業部、公安部、國家保密局、國家密碼管理委員會、國家安全部等部間，各省、市、自治區也設立了相應的管理機構。[249]2014 年 1 月 9 日香港報導指出，中共將成立『信息化和互聯網信息安全領導小組』[250]，以嚴控網路言論，並由中共總書記習近平擔任組長。[251]

(二)軍隊發展

1999 年 11 月《解放軍報》首次使用「網軍」這個名詞，並將成為繼陸、海、空三軍種後的新軍種，以擔負保衛網路主權和從事網路作戰的艱巨任務。同時共軍也以美國為借鏡，將網軍組成攻擊、防護、維護三大部門，攻擊部隊負責滲透、監控、摧毀敵方網路系統及竊取與竄改情資;防衛部隊負責組建中共資訊防護系統，抵禦外來網路攻擊;維護部隊負責在遭受駭客入侵後，於第一時間內修補網路漏洞，並追查攻擊來源。[252]

據 2001 年的一項報導，中共在廣州、南京和濟南軍區都設有電腦作戰單位，每個單位大約有 500 名專長人員。[253]同年，另一份報告表示，共軍已經在山西大同、福建廈門、上海鄂城、四川宜昌和陝西西安等城市成立了資訊作戰後備單位。這些後備單位可能包含許多在民間電腦發展和製造部門工作的專長。[254]

中共自 2002 起擴充網路戰能量，發展初期雖遠落後各先進國家，然近年來蓄積相當能量且業務分工佈總參 4 大部、7 大軍區、國防科研機關與各級院校等，任務包括戰時網路攻擊，及平時網路竊密、滲透等諜報活動;另國防動員亦將信息民兵納入編組，整體軍事機關網軍架構基本成形，預判其正式編制人力約 10 餘萬人。[255]2002 年，我國行政院亦曾指出，在 1996 年，共軍「瀋陽軍區」舉辦一場「網軍」模擬對抗，進攻方的網軍成功瓦解敵方司令部通信、指揮系統。[256]

中共的網軍部隊由解放軍和國動委民間 IT 產、官、學界的信息民兵共同組成。2003 年 3 月中共信息民兵編組完成，基本架構分三級，最基層是省屬縣市和鄉鎮的信息民兵分隊，至於性質則視單位的特性而定，編組電子戰分隊、網路戰分隊、黑客(駭客)分隊、信息救護分隊模式[257]

---

[248]潘小剛、周亞明、肖琳子，《中國信息安全報》，北京:紅旗出版社，2009 年，頁，35。

[249]潘小剛、周亞明、肖琳子，《中國信息安全報告-預警與風險化解》，北京:紅旗出版社，2009 年，頁 42。

[250]由現階段黨政體制下本已有兩個網安小組，「國家信息化領導小組」及「中央互聯網信息工作領導小組」，前者由國務院總理李克強兼任組長，後者由主管意識形態的政治局常委劉雲山兼任，將由該兩小組合併而成。

[251]〈打壓網路 習近平使陰招〉，《蘋果日報》，2014 年 1 月 9 日， 版 25。

[252]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 26。

[253]中華民國「高等政策研究協會」楊念祖之估計，見 Glenn Scholss,"Mainland Cyber-soldiers,"South China Morning Post,March 29,2001.

[254] Lt.Col.Timothy Thomas,U.S.Army retired ,"china's Electronic Strategies,"Military Review,May/June 2001,www-cgsc.army.mil/milrev/English/May Jun01/Thomas.htm.

[255]立法院，〈我國如何因應網軍與駭客攻擊並強化資訊安全措施〉，《 立法院公報》，第 102 卷，第 29 期，頁 6。

[256]行政院研究發展考核委員會，《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》，台北:五南文化出版，2002 年，頁 54。

[257]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 11 月，頁 59-61。

根據美國學者費學禮披露，中共在 2004 至 2005 年期間，7 個軍區中有 6 個軍區設立了「特種技術偵察部隊」(Special Technical Reconnaissance Unit)，遂行守勢和攻勢資訊作戰。因此，共軍可能在「特種技術偵察部隊和比較不正式的後備和民兵單位之間，擁有一支由數千人組成的「網軍」。似乎唯獨北京軍區沒有這種單位，可能因為北京為共軍的指揮總部。[258]

2007 年，美國學者哈里斯(Shame Harris)表示，美國政府與企業電腦網路攻擊似乎來自中共，並指出，中共已建立資訊戰部隊，發展病毒，以攻擊敵人之電腦系統與網路。[259]此外，根據「美中經濟暨安全審查委員會」(US-Chian Economic and Security Review Commisssion,USCC)提交的《2008 年對國會報告》，中共約有 250 個駭客組織，受到官方的監控及鼓勵，入侵其他國家網路。[260]

2010 年，中共學者東鳥強調，西方安全專家們相信，中國已經授權軍方起草一份網路戰爭藍圖，旨在 2050 年前獲取使西方軍隊火力失效的能力，該藍圖是北京是在 2050 年前對每個對手實施，電子統治計畫的一部份，計畫的主要目標國包括美國、英國、韓國及俄羅期，有關部門正在全國範圍內舉行「黑客」(駭客)大賽(駭客)，以招募「黑客」(駭客)加入「網路軍隊」。[261]

2011 年 5 月 25 日，在中國國防部例行記者會上，中共國防部發言人耿雁生大校表示，為提高部隊的網路安全防護水準，中共解放軍已設立了網路藍軍。他並強調，網路藍軍並非是由電腦專業人士組成的所謂駭客部隊，只是常規部隊的訓練科目之一。

2013 年 2 月 19 日，美國麥迪安網路安全公司(Madiant Corporation)公佈一份名為「APT1[262]:揭露中國大陸網路間諜單位」(APT1:Exposing One of China's cyber Espionage Units)的報告，在該報告附加一份超過三千餘筆技術資料證明，美國遭網路攻擊，是來自中共代號為 APT1(Advanced Persistent Threat 1)的攻擊行動。[263]該報告還指出，中共網軍(61398 部隊)是位於上海浦東新區高橋鎮大同路一棟 12 層高的建築，成員約在數百人至 2 千人之間，並直接從大學甄選具電腦和英語專長人才，專責進行網路行動。根據追蹤，就是中共解放軍總參謀部三部二局。[264]

根據 2014 年 5 月 20 日《中國時報》報導指出，美國司法部正以「網路間諜」

[258]國防部史政編譯局譯，費學禮 (Richard D. Fisher Jr.)，《中共軍事發展-區域與全球勢力佈局》(China's Military Modernization-Building for Regional and Global Reach)，台北:國防部史政編譯局，2011 年，頁 201。

[259]柴惠珍譯，Shame Harris 著，〈中共網軍〉，《陸軍軍事譯粹選輯》，第十八輯，2008 年 5 月，頁 748。

[260]美國國會於 2000 年 10 月通過《2001 年佛洛德.斯彭國防授權法案》，(Floyd D.Spence National Defense Authorization Act)根據這項法案成立「美中經濟暨安全審查委員會」，目的為監督與調查美國和中國大陸進行雙邊貿易和經濟關係時，對美國國家安全可能產生的影響。根據這項國防授權法案規定，該委員會必須針對美國與中國大陸之間交往的八大領域進行監督與研究，並每年向國會提交年度報告。

[261]東鳥，《中國輸不起的網路戰爭》，北京:中南出版傳媒集團，2010 年，頁 252

[262]麥迪安公司認為共軍總參謀部二局三處 61398 部隊，就是造成此「先進持續性威脅」(Advanced Persistent Threat ,APT)的單位，並將該部隊賦予 APT1 代號。

[263]載政龍，〈中共網軍發展與網路攻防:兼論我國資通安全之政策規劃〉，《戰略評估》，第四卷第四期，2012 年冬季，頁 104-105。

[264]同註 263。

罪名起訴中共解放軍計王東、孫凱亮、文新宇、黃鎮宇、谷春輝等 5 員，這是美國首次以以「網路間諜」起訴外國官員，該報導並表示，遭美國以「網路間諜」起訴 5 員全都是中共 61398 部隊成員。[265]這項最新的報導，可說進步證明中共已具備一支網路部隊。

另外，為掌握全國網路信息安全，中共公安部所屬的「公共信息網路安全監察局」(簡稱網監局)各省、市、自治區的公安廳(局)下設立「網監處」，負責轄區內的網路信息安全監察和違法查處工作。根據 2004 年非正式統計，公安部負責網路保密、偵防和查處的網路警察和網路安全人員人數，已多達 23 萬人，另有 4 萬人屬各相關單位的網路科研機構人員，總計 27 萬人員。[266]另據一項報導，2013 年 10 月 14 至 18 日，中共將首次舉行輿情分析師培訓，並教導輿情分析等 8 門課程，考試合格者將獲「網路輿情分析師」身分證明及從業憑證。該報導並指出，目前全中國大陸約有 200 萬人從事網路輿情分析師的工作，且這些人多半分布在黨政宣傳部門與入口網站等單位。[267]

(三)人才培育

中共軍事專家認為，從機械化戰爭到網路戰，不單單是作戰樣式、方式的改變，而是戰爭形態的改變。網路戰的崛起，加速了以資訊及網路技術為基礎和核心軍事革命的到來。在新的軍事革命面前，拋棄舊知識與學習新知識同等重要，打網路戰，不僅要看到「技術差」，更要看到「知識差」。知識在人的綜合素質中所占的比重越來越大，因此戰爭勝負的決定因素仍然是人。[268]中共海軍副司令兼全國人大代表徐洪猛中將強調，『只有加大人才，特別是高層次人才培養力度，才能跟上世界新軍事變革的潮流，人才的價值往往比武器更為重要。』[269]

根據江澤民「人才戰略工程『五支隊伍』建設」的指示，軍事資訊人才包括軍事資訊指揮人才、資訊參謀人材、資訊研究人材、資訊技術人才和資訊作戰人才等五個方面。基此思維，2003 年 8 月，共軍強調，打贏資訊化戰爭的需要，著眼於資訊化軍隊建設，對未來人才建設應達到的數量規模、知識機構、複合素質等提出了相應的目標要求，並提出了具體的對策和措施。[270]2005 年 10 月，中共 16 屆五中全會通過《中共中央關於制定國民經濟和社會發展第十一個五年規劃的建議》，確立「十一五」期間信息建設的主要任務和方向，其中第七項為加強信息化人才隊伍建設，提高國民信息能力。[271]

除了發表人才規劃之官方文件，中共軍方也展開相關資源的整合與規劃。如中共軍委主席江澤民於 1999 年 7 月，下令重新組建了「解放軍信息工程大學」，合併了信息工程學院、電子技術學院和測繪學院，其用意不言可喻，顯然有意將此學院做為「網軍」培訓搖籃，這是全世界第資訊作戰的軍事學術機構「網路技

[265]劉屏、朱建陵，〈美政府告解放軍 5 軍官〉，《中國時報》，2014 年 5 月 20 日， 版 1。
[266]廖文中，〈中國網軍〉，《全球防衛雜誌》，272 期，2007 年 11 月，頁 3。
[267]〈監控網路陸培訓洗腦大軍〉，《蘋果日報》，2013 年 10 月 6 日， 版 26。
[268]唐仁俊，〈中共信息戰之發展與限制〉，《空軍學術雙月刊》，第 619 期，2010 年 10 月，頁 32。
[269]周敦彥譯，Thomas Henderschedt，〈共軍資訊人作戰之借鏡〉(Learn from the PLA？)，《國防譯粹》，第 39 卷，第 10 期，2012 年 10 月，頁 33。
[270]唐仁俊，〈中共信息戰之發展與限制〉，《空軍學術雙月刊》，第 619 期，2010 年 10 月，頁 32，
[271]潘小剛、周亞明、肖琳子，《中國信息安全報告-預警與風險化解》，北京:紅旗出版社，2009 年，頁 44。

術研究中心」。[272]2013 年，美國載爾電腦公司花了逾 1 年時間，追縱到一名中國駭客，其職業為任職於中國人民解放軍信息工程大學。[273]此舉顯示，中共網軍成員確實來自中共「解放軍信息工程大學」。

囿於中共軍事院校體系畢業不敷中共現代化需求，從 2000 年起，中共實施類似美國 ROTC 計畫的「國防生計畫」，直接從民間院校招募軍官，與軍事院校出身之軍官待遇完全一致。中共國防生吸引的對象為具有高等理工知識背景之人才，主要培訓探測制導與控制(戰管)、資訊安全(通資安全)、通信工程(硬體)、電子資訊工程(軟體)、資訊對抗(資電戰)5 項專業，其目的就是要打贏資訊化條件的高技術戰爭。2006 年新進之軍官有一半是國防生，2009 年已有 117 所民間大學有此計畫。[274]

另外值得一提的是，隨著手機遊戲逐漸取代電腦遊戲，自 2003 年起，中共遊戲業者包括騰訊、盛大、網易、完美時空等大廠，均積極投入自主研發實力，中共當局，允許遊戲軟體公司人員到大專院校授課，以培養科技人材。[275]從上述數據顯示，中共除有系統、組織在發展網路戰外，更積極培育網路人才。

[272]行政院研究發展考核委員會，《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》，台北:五南文化出版，2002 年，頁 52。
[273]〈美肉搜 1 年 揪中國網軍〉，《蘋果日報》，2013 年 2 月 17 日， 版 29。
[274]洪志安、王官德，〈轉型中之中共陸軍〉，《陸軍學術雙月刊》，第 532 期，2013 年 12 月，頁 51-52。
[275]顏瓊玉，〈中國遊戲業抓牢手機熱 打趴台灣〉，《商業周刊》，第 1336 期，2013 年 7 月 1-7 日，頁 52-53。

第三節　中共網路戰與其國家安全

中共第十六屆四中全會，把信息安全、和政治安全、經濟安全、文化安全、國防安全的五大範疇，信息安全在國家安全佔有十分重要要的戰略地位，並成為國家安全的基石。[276]在網際網路的時代，網路本身已成為國家利益的一個組成部分，網路力量成為衡量國家間利益均衡的一個重要參數，網路空間將成一個新的戰略空間。[277]以下將從中共防止敵人的網路戰攻擊、攻擊敵人(軟殺力量、不對稱作戰)兩個層面的分析，茲說明如下:

一、防止敵人的網路戰攻擊

2001 年 7 月 11 日，中共國家主席江澤民主席在一次關於促進信息網路健康發展的法制講座強調，要高度重視信息網路化帶來的挑戰及信息網路安全問題，並要求保障國家的政治與經濟安全，促進信息網路健康有序發展;另一位中共國家主席胡錦濤表示，面對網路問題，要堅持依法管理、科學管理、有效管理，綜合運用法律、行政、經濟、技術、思想教育、行業自律等手段，加快形成依法監管、社會監督、規範有序的互聯網信息傳播秩序，確維護國家文化信息安全。[278]

2008 年，由中共學者曹峻、楊慧、楊麗娟等三人共同撰著《全球化與中國國家安全》一書指出，在網際網路時代，各國對資訊和網際網路的依賴性越大，一旦遭受其進攻及破壞，資訊流動被鎖定中斷，導致整個國家的財政金融瓦解、能源供應短缺、交通運輸中斷、國防能力下降，整個國家都可能陷入癱瘓，人民生活將陷入困境，直接危及國家安全和民族生存。[279]鑒此，在中共黨的十六屆四中全會，把信息安全和政治安全、經濟安全、文化安全、國防安全並列為國家安全的五大範疇，信息安全的重要性被提升到一個空前的戰略高度。信息安全在國家安全的十分重要的戰略地位，已成為國家安全的基石。[280]由上述可得知，中共已將信息安全列入國家安全中最核心的問題。

信息資源是經濟和社會發展的戰略資源，是國防實力重要組成部份和決定戰爭勝負的關鍵要素，是衡量一個國家國力的重要標志。信息產業最關鍵是國家信息基礎設施。[281]根據大陸學者越英的觀點，『國家安全戰略是指的是從政治、軍事、外交、經濟、心理、反恐怖活動、科技等方等等方面綜合考慮，綜合運用國力，維護獲取國家利益與安全的綜合安全保障戰略。』[282]美國國防部在其 2012 年「中共軍事與安全發展」報告中提及，北京當局可能將其網路作戰行動視為戰略情資的工具。[283]顯示中共對網路戰的重視，已提升至國家安全層級。

由於科技全球化導致信息處理平台及其操作軟體趨於標準化，這種標準化的信息處理平台及其操作軟體達到高度壟斷時，將帶來信息安全問題，而這種技術

[276]潘小剛、周亞明、肖琳子，《中國信息安全報》，北京:紅旗出版社，2009 年，頁，11。
[277]張春江、倪健民主編，《國家信息安全報告》，北京:人民出版社，2000 年，3。
[278]同註 273，頁，3。
[279]曹峻、楊慧、楊麗娟，《全球化與中國國家安全》北京:社會科學文獻出版社，2008 年，頁 264。
[280]同註 273，頁，11。
[281]崔國平主編，《國防信息安全戰略》，北京:金城出版社，2000 年，頁 92-93。
[282]劉慶元著，《解析中共國家安全戰略》，台北:揚智文化出版社，2003 年 11 月，頁 13。
[283]同註 257，頁，201。

被擁有國用於其狹隘的國家利益時，後果更為嚴重。如美國英特爾的處理器設置的識別用戶身份序列碼及微軟公司的操作系統存在的兩個密碼，對使用該系統的國家的安全構成了潛在威脅。因為，如果用戶是政府部門，上網可能導致洩密，另由於隱藏於晶片和操作系統的電腦病毒，能夠被美國某種秘密啟動，一旦發生國際衝突，對方利用網路攻擊將造成經濟、社會及軍事安全不堪設想。[284]

根據行政院的一份報告，中共於2008年舉行的第16屆中國共產黨四中全會，將資訊安全列為國家安全的重要組成部分，明確提出「增強國家安全意識、完善國家安全戰略」，以確保「國家的政治安全、經濟安全、文化安全與信息安全」。在「國家中長期科學和技術發展規劃綱要」中，提出將「信息產業及現代服務業」列為國家長期重點發展產業，在「面向核心應用的信息安全」中點出關鍵資安技術方向，以研發減稅、政府採購、軍民合作及國際合作四大面向之鼓勵措施，推進中共資安技術發展。[285]

為能確保網路安全，中共於 2001 年 5 月成立了中國信息安全產品測評認證中心(CNITSEC)，負責對國內外信息安全產品和信息技術進行測評和認證、對國內信息系統和工程進行安全性評估和認證、對提供信息安全服務的組織和單位進行評估和認證。目前建有上海、東北、西南、華中、華北五個授權評估認證中心機構和兩個系統安全與測評技術實驗室。[286]中共另於 2003 年 7 月成立國家計算機網路應急技術處理協調中心(CNCERT/CC)，專門負責收集、滙總、核實、發布權威性的應急處理信息。同年，中共透過第一筆信息安全專項撥款(1800 萬元人民幣)支持重大安全事項，並且組織召開「第一屆中國信息安全技術與產品展」。[287]為使信息化基礎工作進一步改善，信息化法制建設持續推進，《電信法》及《政府信息公開條例》於 2008 年 5 月 1 日起正式實施。[288]

此外，中共為確保境內免受網路戰攻擊，於 2001 年頒布國際網際網路保密管理規定，緊抓網路控管權，監督網際網路上的資訊流動。[289]據報導，中共 18 屆三中全會結束後，成立「信息化和互聯網信息安全領導小組」，由國家主席習近平任組長。其成立主要原因，是關注中國未來整體資訊化戰略發展，包括資訊安全、工業產業資訊化、全球化意義上的資訊戰、全球資訊一體化的政治意義與影響。此項行動顯示中共試圖透過資訊化建設，實現經濟、政治、意識形態等三方面目標。經濟意義方面，促使中國未來在資訊技術產生極強競爭力，出現如蘋果等民族品牌公司;在政治意義方面，國際資訊戰、國內外資訊安全都是未來擺在中國領導人面前的重要課題;在意識形態方面，促使輿論管理手段與時俱進。[290]另根據一項報導，中共總書記出任網信組長後，可根本上改變以往由國務院領導擔任「國家」信息化領導小組組長，難以協調黨中央、軍委、人大等一些弊端，大大提高中共綜攬網信全局的整體規劃能力和高層協調能力。[291]

---

[284]曹峻、楊慧、楊麗娟，《全球化與中國國家安全》北京:社會科學文獻出版社，2008 年，頁 176
[285]〈國家資通訊安全發展方案》，《行政院國家資通安全會報〉，2013 年 12 月 25 日，頁 4-6。
[286]潘小剛、周亞明、肖琳子，《中國信息安全報告-預警與風險化解》，北京:紅旗出版社，2009 年，頁 43。
[287]約翰(Juhn chang)，〈中國信息安全發展現況〉，《漢和防衛》，2013 年 9 月，頁 44。
[288]潘小剛、周亞明、肖琳子，《中國信息安全報告-預警與風險化解》，北京:紅旗出版社，2009 年，頁 37。
[289]劉慶元，《解析中共國家安全戰略》，台北:揚智文化出版社，2003 年，頁 127。
[290]藍孝威，〈習領軍信息化小組 因應資訊戰〉，《中國時報》，2014 年 1 月 23 日， 版 13。
[291]黃德潔，〈中共網信組成軍 意圖建設網路強國〉，《青年日報》，2014 年 4 月 24 日， 版 4。

二、攻擊敵人

網路時代競爭首先是科技的競爭，而科技的競爭的重點就是網路技術制高點的爭奪。在 21 世紀，世界各國都積極調整發展戰略，把研究和開發技術作為為主要方向，以爭取在政、經、軍上取得優勢，以戰勝對手，確保己方安全。[292]網路技術不僅已成為各種戰爭資源發揮效能的基本保證，而且本身就是重要的作戰武器。全面爭奪制信息權的鬥爭促進了把指揮、決策、控制、通信、情報、作戰、支援保障聯結合一個有機整體的自動化網路，提高信息鬥爭的戰爭地位。[293]

通過網路戰攻擊，可對敵國的金融、郵電、交通、商業、航空航天、國防及大型企業等部門的電腦管理系統產生相當程度的破壞，從而影響經濟效益和社會效益，甚至動搖國家的戰爭意志。[294]在現代戰爭中，持續不斷的戰場因素緣於敵對雙方激烈殘酷的武裝對抗，重要目標就是干擾敵參戰人員的認知系統，摧毀其認知過程，直至促使其認知癱瘓，確實使持久不息的戰場因素起到震攝、嚇阻、迷網、困惑敵人的作用，進而達到少戰而屈人之兵、小戰而屈人之兵，軟戰而屈人之兵之目的。[295]

中共信息戰略共通的原則為取得信息優勢，就是擁有防禦自己信息的能力，同時又能攻擊敵人的信息系統，即干擾敵人獲取、處理、傳送、與使用信息的能力，並同時可以癱瘓它個作戰系統。[296]中共對資訊作戰基本的戰略戰術概念，『是研究如何將「作戰人員及作戰裝備形成的作戰運用體系」與「資訊及資訊裝備所形成的功能體系」二大部份，進行實質或無形破壞的戰術，使敵人因不能結合此二大運用系統，而達到癱瘓其戰力目標。[297]

中共網路戰專家認為利用敵人仰賴精密電腦的弱點，只要摧毀敵人的電腦系統，高技術武器就無法發揮效能，不論是低強度衝突、大規模毀滅性戰爭、或是戰術及戰略衝突，均可獲致最大發揮。[298]美國蘭德公司(RAND)公司亞太政策中心副主任穆文濃研究發現，認為中共網路戰戰略具有，屬非傳統「戰爭」武力、不是場戰武器、屬先發制人的利器、兵不血刃之特性。[299]另據國內學者林中斌博士研究指出，中共「點穴戰爭」戰略目標是破壞或操縱敵人指揮中心、電話網、電子網、交通管制系統、各種銀行轉帳系統。故中共所建置的點穴作戰能力，亦即資訊作戰能力。因資訊作戰可達「速效、損小、兵不血刃」之政經軍心綜合戰略目的。[300]

隨著科學技術的進步與發展，國際上間諜與反間諜的鬥爭也日趨複雜，西方一些國家花費巨資資大力加強情報工作，並且把中共的國防信息作為他們活動的

[292]崔國平主編，《國防信息安全戰略》，北京:金城出版社，2000 年，頁 89-90。
[293]同上註，頁 35。
[294]李曉、陳乘風、郭鑄文，《揭開網路戰神祕面紗-鍵與屏的博殺-網路戰掃描》，湖北:科學技術出版社，2003 年，頁 12。
[295]祝延軍著，〈淺論未來戰爭中信息主導型思維〉，《未來與發展》，第 237 期，2013 年 7 月，頁 10。
[296]李承瑀，《中共高技術條件下信息戰之研究》，政治作戰學校政治研究所碩士論文，2000 年 6 月，頁 114。
[297]同註 287，頁 130。
[298]同註 293，頁 116。
[299]林宗達，《以劣勝優》，台北:晶典文化出版社，2005 年，頁 41。
[300]同註 295，頁 129。

重要目標。因此，國防信息安全在戰爭特殊重要的地位。[301]2011 年美國出版的《致命中國》(Death by China)乙書指出，中共將利所有可能的武器，如保護主議、網路攻擊到間諜活動等每一條戰線，向美國發動攻擊。[302]中共學者對於資訊係戰爭中之主要戰略資源，以及情報在當代戰爭中之重要性等相關議頗有研究。一位作者寫道:在強化資訊概念以成為指揮官的戰力倍增器時，我們必須視資訊為作戰效能的倍增器，並將其做為較人員、物質及經費更重要之戰略資源。[303]

華府智庫「戰略與國際研究中心」認為，中共軍方正在想方設法癱瘓或者嚴重破壞美國的基礎設施，例如電力網、金融交易網、供水系統，以及飛航管制系統等。前美國中情局長海登(Michael Hayden)強調，中共的網路破壞行為給美國傷害最深的，就是經濟領域的網路間諜活動，而這些間諜活動包括，竊取國家機密、竊取私人企業的商業機密、盜取知識產權和工業技術機密，以及竊取談判策略等。[304]如 2012 年 3 月 2 日美國國家航空暨太空總署監察馬丁(Paul Martin)於在國會報告中指出， 2011 年 11 月入侵美國太空總署的噴射推進實驗室遭駭客入侵，導致美國有關太空船發展與太空任務支援系統也敏感資料遭受破壞為中共駭客所為。[305]據 2011 年 12 月 16 日美國《華盛頓郵導》報導，中共解放軍滲透美國政府、國防部機構、高科技公司與公共單位網路竊取機密資料，歐巴馬政府必須採取強硬手段，並要求關閉中國大陸軍方為背景的情報滲透機構，如果中方不配合，必須採取反制之道。[306]

[301]崔國平主編，《國防信息安全戰略》，北京:金城出版社，2000 年，頁 13。
[302]吳惠林，〈中國悄悄佔領全世界〉，《蘋果日報》，2013 年 12 月 2 日，版 18。
[303]國防部史政編譯局譯，阿里斯特德(Leigh Armistead)，國防部史政編譯局譯，《資訊作戰-以柔克剛的戰爭》(Information Operations Warfare and the Hard Reality of Soft Power)，台北:國防部史政編譯室，2008 年，頁 259。
[304]曾復生，〈國際網路安全競合情勢剖析〉，《國家政策研究基金會》，
http://www.npf.org.tw/post/2/12290(2014 年 3 月 19 日)
[305]網路科技，〈中國大陸駭客入侵 NASA〉，《尖端科技》，332 期，2012 年 4 月，頁 104。
[306]網路科技，〈美方應對抗中國大陸軍方網路攻擊，《尖端科技》，第 330 期，2012 年 2 月，頁 105。

第四節　小結

自 1991 年美伊波灣戰爭以來，中共已體會到資訊化時代作戰勝利的關鍵將是網路戰爭，人海戰爭的總體戰爭將不在適合未來資訊戰爭的需求，高科技、高素質的網路戰士才將是主宰戰爭勝敗重要因素。此外，在 1999 年科索沃戰爭後，中共更體認出，要求打贏未來戰爭，必須著手於網路戰之準備，從 1999 年中共兩位大校提出「超限戰」理論後，有關中共資訊戰、網路戰的研究，如同雨後春筍般相繼提出，例如癱瘓戰、資電一體戰等理論。就證實中共對網路戰是愈來愈重視。

中共「網軍」一詞，最早於 1999 年 11 月「解放軍報」出現，其任務負責擔負保衛網路主權和從事網路作戰的艱巨任務。此外，中共為擴充網路戰能量，於 2002 年在總參 4 大總、7 大軍區、國防科研機關與各級院校等投入相關網路戰編組，任務包括戰時網路攻擊，以及平時網路竊密、網路滲透遂行諜報活動等，並將信息民兵納入編組。根據 2005 年美國《國家期刊》揭露，在 2003 年美國所遭受的停電，就是中共網軍所為。此外，在 2011 年中共國防部發言人耿雁上大校也證實中共為確保網路安全已成立網軍部隊，最後在 2013 年，美國網路安全麥迪安公司披露，美國自 2007 年來遭受網路駭客攻擊，均是位於中國大陸上海市某一棟大樓的中共網軍 61398 部隊所為。

網路戰對中共國家安全影響層面越趨重要，中共為加強網路安全防護，自 2001 年 5 月，成立中國信息安全產品測評認證中心(CNITSEC)，負責對國內外信息安全產品和信息技術進行測評和認證、對國內信息系統和工程進行安全性評估和認證、對提供信息安全服務的組織和單位進行評估和認證。同時，為做好管控網路發言，監督網際網路上的資訊流動，中共於 2001 年，頒布國際網際網路保密管理規定，並於 2014 年 2 月 18 日成立「信息化和互聯網信息安全領導小組」(國內稱為網信組)，並由中共國家主席習近平擔任組長，以提高中共綜攬網路安全的整體規劃能力和高層協調能力。此外，為達到以最小的成本，獲致最大的成果，近年來，中共正積極發展網路戰，以竊取必要之軍事、商業技術，甚至必要時，以網路戰癱瘓或破壞敵國的基礎設施，例如電力網、金融交易網、供水系統，以及飛航管制系統等。網路戰儼然已成為中共增強國力的最佳手段。

第四章　中共網路戰之能力

2010 年，我國《資安政策白皮書》指出，中共受第一次波灣戰爭影響，著手組織數位化部隊，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，更已將訊息戰、駭客攻擊、網路攻擊等納入演習範圍。[307]2013 年 9 月，美國學者(David Alexander)披露，中共參二部 61398 部隊在一些國家安裝伺服器，估計其核心成員從數十人到數百人，甚至多達數千人不等，暗指此即為共軍在網際空間中設置的數位灘頭堡，且其網軍已厚植實力。[308]本章將從中共網路戰之作戰構想、以及網軍編組與預算，來評估中共網路戰之能力。

第一節　中共網路戰之作戰構想

一、威脅來源

(一)美國

自網際網路誕生以來，全球網路域名(DNS)[309]與位址(IP)一直由美國政府(商務部)授權「網際網路名稱與號碼分配組織」(The Internet Corporation for Assigned Names and Numbers，ICANN）[310]統一管制及掌握。在特殊情況下美國需要使中共對外網路中斷，只要中斷伺服器，中共馬上就成為網上孤島，無法在網上與外界聯繫。目前全球域名 IPv4(即第 4 版網際通信協議)總量為 42 億個，其中 2/3 已分配完畢，美國則利用網路發源地的優勢，占有 42 億中的 12 億。事實上美國任一所大學所擁有的 IP 位址，幾乎是中國全國的 IP 位址數量，中國 IP 位址長期的匱乏，被迫大量使用轉換位址，嚴重影響網路效益和安全。[311] 2000 年，深圳金智塔軟體公司、上海美亞在線等公司「域名」先後都受到美國同行質疑，聲稱 gameicq.com、gameicq.net 等域名歸美國所有，最後結果域名爭議仲裁中心裁決給美國線上。[312]

2010 年，美國國家安全局成功讀取中共「華為」總裁任正非的電郵。此一行動是在美國白宮、中情局、聯邦調查局的共同協調下進行，行動初始目標為調查華為與中共解放軍之間關係，並企圖對中共「華為」販售給其他國家的電腦和電話網路進行偵聽。消息指出，美國情部門已進入中共「華為」伺服器近 100 個端口，獲取「華為」路由器和交換機相關工作資訊(含電郵存檔)及近 1400 位

[307]行政院科技顧問組，《2010 年資安政策白皮書》，(台北:五南文化出版)，2010 年，頁 20。
[308]王文勇譯，(David Alexander)，〈網路防衛戰略方案〉(A SDI for Cyberspace)，《國防譯粹》，第 40 卷，第 9 期，2013 年 9 月，頁 53。
[309]「網域名稱系統」(Domain Name System,DNS)在於簡化網路位址的管理，「網域名稱系統」將各個「網際網路傳輸協定」數字排列為可辨識之字母組、文字組或數字組，藉由各種區塊及一個結構性的分層式位置來達成目的。
[310]ICANN 於 1998 年 9 月在美國成立，並於同年 10 月，由美國商務部授 ICANN 負責域名及技術問題的國際管理，核心是管理網際網路的根服務器。位於美國加州的 ICANN 雖自稱非盈利私營公司，但事實上是網際網路最高管理機制，它決定著網路技術的取捨、網路通信協議的制定、域名和 IP 地位的分配、域名登記與出售，如”.com”” .net”等。
[311]東鳥，《網路戰爭:互聯網改變世界簡史》，北京:九洲出版社，2009 年，頁 83-85。
[312]東鳥，《中國輸不起的網路戰爭》，北京:中南出版傳媒集團，2010 年，頁 2。

客戶資料訊息。此外，中共前國家主席胡錦濤、中國商務部、外交部、銀行以及電訊行業也在監控範圍內。[313]另據報導，史諾頓擔任國安局包商顧員期間，工作鎖定的對象就是中共的情報運作，並針對中共的網路反情報議題開班授課。[314]

2011 年，美國國家安全局曾希望日本協助，將中共通往日本的國際海底光纖電纜加裝監聽設備，以便從中攔截傳輸的郵件、電話等個人情資。由於監聽光纖的龐大情資訊息，必須有量人力與民間企業的合作，據報導，美國國安局至少編制三萬人，而日本情報人員的規格遠遠不及，無法負荷此項任務。[315]此外，美國利用情報員以外交身分，在全球各地的使館或辦事處設立 90 個監聽中心，以攔截電話、網路、衛星通訊為目的。而美國在東亞的監控站情蒐焦點則是中共，這些監控站位於北京、上海與成都的使領館內。[316]由此可知，美國正是中共網路戰威脅的首要來源。

2011 年，中共互聯網應急中心(CNCERT)[317]公布的《中國互聯網網路安全報告》資料指出，2011 年中共境外有近 4.7 萬個 IP 位址作為木馬或僵屍伺服器控制中共境內主機。經查明後，境內 IP 位址分別為日本 22.8%、美國 20.4%及韓國 7.1%分居前三位(而美國在 2009 年及 2010 年則高居榜首)。另參與控制中共境內主機數量，則美國以 9528 個 IP 控制大陸境內近 885 萬台主機(由 2010 年近 500 萬增加至近 890 萬呈現大規模的趨勢增加)，仍居榜首。[318]2012 年中國境內有 1419.7 萬餘台主機受到境外木馬或僵屍網路控制，較 2011 年增長 59.6%。其中，被來自美國 IP 地址的木馬或僵屍網路控制的服務器和主機數量，占全部的 17.6%和 74%，均名列第一。[319]

特別讓中共擔心的是，美國逐年增加對中共的網路攻擊。2013 年上半年，中共互聯網應急中心向國際網路安全應急組織和其他相關組織投訴 1760 件，其中向美國相關組織就投訴 1110 件。[320]此外，據「中國國家互聯網信息辦公室」數據統計，2014 年 3 月 19 日至 5 月 18 日僅 2 個月內，共有 2077 台位於美國的電腦伺服器透過木馬程序或殭屍惡意軟體，直接控制中國境內 118 萬台電腦主機同期間在美國的電腦 IP 位址對中國發動約 5,7000 次植入「後門」攻擊、14,000 次網路「釣魚」詐欺侵害事件。[321]

另外值得一提的是，根據 2014 年 5 月 26 日中共國務院新聞辦所屬的互聯網新聞研究中心發表的〈美國全球監聽行動記錄〉一文透露，美國政府大規模入侵中國的中國移動、中國電信、中國聯通等主要通信公司，以竊取用戶的手機資料，監聽訪美的中國公民大量通話資訊。[322]該專文還強調，美國國家安全局於 2013 年 1 月還對中共清華大學的主幹網絡發起大規模的網路攻擊，至少有 63 部電腦

[313]朱建陵，〈紐時:美國安局駭進華為竊密〉，《中國時報》，2014 年 3 月 25 日， 版 13。
[314]魏國金，〈美機密檔案史諾頓:中俄拿不到〉，《自由時報》，2013 年 10 月 19 日， 版 16。
[315]林翠儀，〈攔截中國情資？日拒美監亞太海底光纜〉，《自由時報》，2013 年 10 月 28 日，版 10。
[316]管淑平，〈美全球 90 監聽中心 台北也設點〉，《自由時報》，2013 年 10 月 31 日， 版 17。
[317]CNCERT/CC，為中國國家計算機網路應急技術處理協調中心。
[318]王超群，〈中美網路軍演 資安全作又較勁〉，《旺報》，2012 年 4 月 19 日， 版 8。
[319]昊銘，〈黑客關注中國 600 個網站〉，《視野》，16 期，2013 年 8 月，頁 17-18。
[320]昊銘，〈境外對華網路攻擊報告〉，《瞭望東方周刊》，第 30 期，2013 年 8 月 8 日，頁 17。
[321]管淑平，〈美起訴解放軍 中國暫停網路合作〉，《自由時報》，2014 年 5 月 21 日， 版 10。
[322]陳言喬，〈查證反擊 大陸萬言書控美竊聽〉，《聯合報》，2014 年 5 月 27 日， 版 12。

和服務器遭網路攻擊而癱瘓。[323]這些資料表示，美國與中共正在進行一場無煙哨的網路戰。

(二)台灣

中共軍事科學阮研究員趙捷明表示，台灣的信息戰能力也對中共構成威脅，他進一步說，台灣曾公開表示，要積極準備打信息戰，因此一旦台灣要推動獨立，中共的信息安全就可能沒有保障。[324]2013 年 8 月，中共學者昊銘透露，2012 年中國境內有 1419.7 萬餘台主機受到境外木馬或僵屍網路控制，來自日本及台灣的 IP，分別為第二、三名，分別占 9.6%及 7.6%，從控制中國境內主機數量，來自韓國及德國的 IP 地址分列第二、三位，分別控制 78.5 萬和 77.8 萬台。[325]

(三)其他國家

據中共學者透露，自 2010 以來，來自日本、韓國的攻擊始終對中國境內的網路安全造成較威脅，甚至連印度、土耳其等也成為重要的攻擊源頭。此外，在 2010 至 2012 年，中共境內遭網頁竄改及電子釣魚郵件等不法行為，所利用的惡意域名半數以上在境外註冊，而且境外註冊比例不斷提高。[326]這些事實顯示，中共也面臨來自其他國家的網路攻擊與威脅。

(四)中共境內

2014 年 1 月 22 日，中共總書記習近平在「中共中央全面深化改革小組」會議指出，在未來八大國安戰略領域方面七項要求事項中，有關網路要求事項就佔有 3 項(第 1、4、7 項)，首先是對海洋、太空、網路、極地等領域加大投入，搶占制高點，其次為中共對內應確保網路資訊傳播秩序，從日常安全到打擊犯罪的網際網路管理能力，及改進網路時代輿論與意識形態滲透。[327]

2008 年 11 月，美國微軟公司發布安全報告指出，中國網路用戶已經成為網路犯罪的第一個目標，大多數對安全漏洞都發生在語言選擇為中文的電網上。2008 年上半年大約 47%惡意軟件的攻擊針對中文電腦，23%為英文，攻擊包括利用用戶鍵盤盜取密碼及信用卡。在中國，網路竊取、詐騙等網路侵財犯罪日漸增多，竊取網民銀行卡密碼的網銀木馬，每年就給中國網銀用戶帶來近億元損失。另外則是網路黑幫問題，他們利用駭客犯罪，威脅網路安全，針對中、小網站長，先通過網路攻擊向站長示威，隨後要求繳交保護費至指定帳戶，否則就持續攻擊。2007 年 5 月，中國一著名網路游戲公司遭到長達 10 天的網路攻擊，服務器全面癱瘓，網路游戲被迫停止，損失人民幣 3460 萬元。[328]

根據 2014 年 1 月 9 日中共《瞭望東方周刊》的披露，中共「.cn」頂級域名系統於 2013 年 8 月 25 日遭受大規模拒絕服務攻擊(DDoS)，致使連結到「.cn」和「.com.cn」無法上網。據中共業界專家指出，這是中共有史以來受到最大規

[323]〈美國全球監聽行動紀錄〉，《人民網》http://military.people.com.cn/BIG5/n/2014/0527/c1011-25067956.html(2014 年 5 月 30 日)。
[324]劉台平，《島計畫-2008 年中共發動對台割喉戰》，北京:時英出版社，2004 年，頁 31。
[325]昊銘，〈境外對華網路攻擊報告〉，《瞭望東方周刊》，第 30 期，2013 年 8 月 8 日，頁 17。
[326]昊銘，〈黑客關注中國 600 個網站〉，《視野》，16 期，2013 年 8 月，頁 17-18。
[327]曾復生，〈習近平的戰略時間表〉，《中國時報》，2014 年 1 月 25 日， 版 16。
[328]東鳥，《網路戰爭:互聯網改變世界簡史》，北京:九洲出版社，2009 年，頁 336。

模的拒絕服務攻擊。中共「國家互聯網應急中心」運行部主任王明華表示，從技術上分析，是網路一些組織或個人向游戲軟體公司收取保護費不成所造成的網路攻擊。此外，中共「互聯網路信息中心」執行主任李曉東強調，中共的網路安全每天都會遇到成千上萬的各種網路攻擊，但最擔心為國家域名服務器的拒絕服務攻擊(DDoS)遭受攻擊。[329]

2009 年，中共學者東鳥透露，隨著中國網站及網民數量高速增長，網際網路已成為民意表達的主要平台，網路輿論的影響愈來愈大，中共民眾透過網際網路獲取資訊的依賴程度居各國之冠，只要在國內某一知名網站載出一條爆炸性新聞，4 小時左右就會被國內超過 500 家以上的網站轉載，網民針對此資訊以臉書方式評論迅速形成網上公眾輿論，造成很大影響;另外，中共也出現了形形色色的網路群體，如中國民主黨、中華新黨等透過網路發佈建黨消息，吸引黨員，推動中國顏色革命訓練營，因中國網路輿論泛政治化，很容易被敵對勢力利用。[330]

2013 年，根據中共「國家互聯網網路中心」信息辦公室的不完全統計，僅 2013 年 3 月，有關部門清理的各類網站謠言就高達 21 萬多條，據《法制網》調查，在 2012 年網路謠言中，51.7%來自微搏，27.6%的網路謠言源自論壇或主要在論壇者傳播。據報導，截至 2012 年 6 月底，中共網路人數已達到 5.38 億人，是 15 年前 867 倍，網路普及率達到 39.9%，越來多人傾向透過網路來獲取和傳播資訊，而網路的匿名性更是加速謠言傳播。[331]

2014 年 3 月 9 日，我國國防大學張玲玲中校指出，中共為有效管控網路言論建立許多審查系統，但卻抵不過人民對於「真相」的追索，透過推特及臉書(facebook)等各種社群軟體的串聯、代號的使用。中共當局因此使出更強硬的手段，關閉網站的使用，中共聲稱其為了國家利益而控制大陸人民，但隨著網民只會愈來愈多的現實，中共就不斷加大封銷力道。[332]

二、戰略構想

(一)強化積極防禦能力

美國國家情報總監發表的〈全球威脅評估報告〉專文透露，中共為反制美軍介入亞太戰局，正積極發展高科技武器，提高奪取制空權、制海權、制網路和電磁頻譜權。[333]事實上，在 2013 年發表的一份文件中，中共即公開表明，將維護國家主權、安全、領土完整，保障國家和平發展，並堅定不移實行積極防禦軍事戰略，維護國家海洋權益和太空、網路空間的安全利益。[334]

2010 年，我國《資安政策白皮書》披露，中共為掌握政府、軍事與民間等三方面的資訊安全為其具體做法，自 1984 年開始注意機敏部門的資安工作，並

[329]昊銘，〈".CN" 攻擊疑犯已從國外帶回〉，《瞭望東方周刊》，第 2 期，2014 年 1 月 9 日，頁 37。
[330]東鳥，《網路戰爭:互聯網改變世界簡史》，北京:九洲出版社，2009 年，340。
[331]龐小寧，〈政府危機管理中的網路謠言控制研究〉，《未來與發展》，第 4 期，2013 年，頁 12-13。
[332]張玲玲，〈中共管控網際網路 對內維穩對外情蒐〉，《青年日報》，2014 年 3 月 9 日， 版 7。
[333]曾復生，〈美中俄日太空爭霸〉，《旺報》，
http://tw.news.yahoo.com/%E7%BE%8E%E4%B8%AD%E4%BF%84%E6%97%A5%E5%A4%AA%E7%A9%BA%E7%88%AD%E9%9C%B8-213000573.html(2013 年 4 月 23 日)
[334]中華人民共和國國務院新聞辦公室，〈中國武裝力量的多樣化運用〉，《 中華人民共和國國防部》，< http://www.mod.gov.cn/affair/2013-04/16/content_4442839_4.htm >（2013 年 12 月 8 日）。

於 1986 年擬定「高資訊技術研究發展計畫」，為近 15 年來「八五」(1991-1995)、「九五」(1996-2000)、「十五」(2001-2005) 三項科技專案的政策依據，三項專案執行期間，訂定資安相關法規與權責、驗證機構等，大幅提高其資安水準。另外，中共於 1999 年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。[335]

2009年，中共學者潘小剛、周亞明、肖琳子等三人表示，積極防禦、綜合防範是信息安全管理方針，並以促進經濟發展、維護社會穩定、保障國家安全、加強精神文明建設的基石。[336]2010年，美國學者穆文濃等人表示，掌握主動乃是中共「積極防禦」全面性戰略構想的核心要素，積極防禦強調，只有在遭到第一波攻擊之後才會發動攻擊，而且是以本土為基地，但是積極防禦的作戰指導卻是強調積極作戰以掌握主動。由此，積極防禦乃是戰略採取防禦，作戰採取攻勢。[337]

據報導，中共在網路戰積極防禦方面是，並不主動進攻其他國家，網路戰是中共在和平時期開展戰略活動的一部份。一個國家只有在網路戰先奪取主權取、或是建立起資訊優勢，才可能獲取戰爭的勝利，這就需要在作戰之前開展偵察和情報蒐集活動，為網路部隊的運行奠定基礎。中共認為從國家層面來看，網路戰已經到了白熱化的程度，針對美國有規劃、有計畫、成系統的全面部署，中共不能用個別的、無序的措施來應對，必須以眼還眼、以牙還牙，採用體系對抗反擊。網路戰第一是防禦，第二要實施積極防禦，要有反制手段，不能光被動挨動。[338]

2014 年 1 月 7 日，中共信息大學校長鄔江興少將[339]指出，中共應從編制、體制、組織架構上來落實國家網絡空間的防禦問題，在法律上和制度層面給予職責使命任務相適應的行動授權。鄔江興還強調，要特別重視開發革命性或顛覆性的科技，透過創新來改變美國一家獨大的游戲規則。近期由解放軍信息工程大學的科學家聯合國內復旦大學、上海交大、同濟大學和華東計算所等著名研究所聯合開發出的模擬計算和模擬安全技術，就屬於可能改變游戲規則的顛覆性技術。[340]

[335]行政院科技顧問組，《2010 年資安政策白皮書》，(台北:五南文化出版)，2010 年，頁 20-21。
[336]潘小剛、周亞明、肖琳子，《中國信息安全報告-預警與風險化解》，北京:紅旗出版社，2009 年，頁 42。
[337]國防部史政編譯局譯，穆文濃(James C.Mulvenon)、譚睦瑞(Murray Scot Tanner)、蔡斯(Michael S. Chase)、傅里林格(David Frelinger)、龔培德(David C.Gompert)、李比奇(Martin C.Libicki)、包克文(Kevin L. Pollpeter)，《中共對美國軍事變革之反應》(Chinese Responses to U.S.Military Transformation and Implications for the Department of Defense)，台北:國防部史政編譯局，2010 年，頁 79。
[338]東鳥，《中國輸不起的網路戰爭》，北京:中南出版傳媒集團，2010 年，頁 251;鄭文浩、楊雷，〈網路戰比核彈威脅更大〉，《瞭望東方周刊》，第 47 期，2013 年 12 月 12 日，頁 40-42。
[339]鄔江興少將，中國工程院院、中國著名通信與資訊系統、網路技術專家。截止 2013 年底止,他先後主持完成了十餘項國家重點或重大科技關鍵項目與工程,為我國資訊網路領域的跨越式發展及其產業他作出了歷史性貢獻。
[340]鄭文浩 王玉山，〈院士：我國網絡基本算不設防成網絡攻擊最大受害國之一》，《人民網》http://military.people.com.cn/BIG5/n/2014/0107/c1011-24045169.html (2014 年 3 月 23 日)

(二)建立攻擊能力

1. 摧毀敵人特定目標

2002 年，林宗達認為，中共網路戰最為與眾不同，在強調對敵人之資訊或電腦系統發展「軟」攻，以作為不對稱戰略的基礎，而這種戰略最主要的就在對付一個比自己擁有更為強大傳統軍軍力的敵人。[341]

中共《戰役學》一書指出，面對高科技強敵時，應選擇敵之資訊系統、指揮系統與支援系統，做為重點打擊的目標，以達降低功能或是將之摧毀以達到改變平衡態勢。同時應集中所有資訊攻擊部隊，在戰役開始之時，即直接攻擊敵軍資訊系統的重要部分與主要連接點，先將敵之資訊系統摧毀，再癱瘓敵軍所有的戰鬥系統，期能以最低的代價，贏得最大的勝利。[342]

中共的網路戰包括網路攻擊、網路防禦和網路利用。在網路攻擊區分「軟殺」(soft-kill)及「硬殺」(hard-kill)方式，「軟殺」包括電腦網路攻擊與電子干擾，以癱瘓軍用或民用電腦網路、武器或電子裝備為目的，利無線激活網路病毒，癱瘓敵作戰系統，毀敵武器系統，如導彈、攻擊直升機進入我方電子設備的有效空域時，利用無線電注入並引爆各種網路病毒炸彈，使武器系統失去控制、迷失方向，最後是利用無線電修改網路指令，使敵失去控制。另一方面，「硬殺」則是使用彈道與巡戈飛彈、反衛星武器反幅射飛彈、特戰部隊、空中打擊、微波武器，以及核子與非核子電磁脈衝(Electromagnetic Pulse ,EMP)武器，攻擊重要的電子目標，造成實質性摧毀，包括指揮人員、指管設施、通信中心、電腦系統、指管飛機及衛星通信，中共已發展出用以攻擊電腦系統和網路的病毒，及保護友軍電腦系統和網路的戰術和措施，將電腦網路作戰納入軍事演習中演練。例如，中共從 2005 年開始在演習中納入攻勢作戰，主要對敵網路發動先制打擊。[343]2013 年 2 月 19 日，美國電腦公司曼迪安(Mandiant)一份報告揭露，中共網軍攻擊不僅針對美國的高科技公司、關鍵的基礎設施，如網路、水利、石油和燃氣管道、航空管制等，甚至進一步要入侵美國政府機要資料庫。[344]

2012 年，美國中國經濟與安全審查委員會公佈一份報告，指出中國軍隊越來越重視網路戰，中國的商業企業與一些外國合作夥伴提供了解放軍網路攻擊、防禦及網路支援(情搜)先進的技術和研究，已成為解放軍戰略戰役初期奪取資訊優勢根本。[345]2014 年美國《四年期國防總檢討》透露，中共將繼續發展新的網路和

---

[341]林宗達，《中共軍事革新之信息戰與太空戰》，台北:全球防衛雜誌社，2002 年，頁 40。
[342]同註 331，頁 85-88。
[343]曹正榮、吳潤波、孫建軍，《信息化聯合作戰》，北京:解放軍出版社，2006 年，頁 120;國防部史政編譯局譯，毛文杰(James C.Mulvenon)、譚睦瑞(Murray Scot Tanner)、蔡斯(Michael S. Chase)、傅里林格(David Frelinger)、龔培德(David C.Gompert)、李比奇(Martin C.Libicki)、包克文(Kevin L. Pollpeter)，《中共對美國軍事變革之反應》(Chinese Responses to U.S.Military Transformation and Implications for the Department of Defense)，台北:國防部史政編譯局，2010 年，頁 89。國防部史政編譯局譯，費學禮 (Richard D. Fisher Jr.)，《中共軍事發展-區域與全球勢力佈局》(China's Military Modernization-Building for Regional and Global Reach)，台北:國防部史政編譯局，2011 年，頁 190
[344]陳破空，〈中共網軍曝光 潛伏上海浦東〉，《開放》，第 315 期，2013 年 3 月，頁 8。
[345]"US report: China's cyberwar skills a risk to military," *BBC NEWS CHINA* ,http://translate.google.com.tw/translate?hl=zh-TW&sl=en&u=http://www.bbc.co.uk/news/world-asia-china-17308921&prev=/search%3Fq%3Dchina%2Bcyber%2Bability%26biw%3D1229%26bih%3D562（2013 年 12 月 8 日）

太空科技，及結合數量愈來愈多且日益精準的巡戈飛導來抗衡美國，對美國及其盟國的海軍及陸地設施形成額外的挑戰。[346]由此可知，中共已將網路戰納入發展戰略目標優先項目之一。

2.削弱敵國作戰能力

1999 年，中共學者馬亞西、成冀、王漢水等三人共同指出，在網路化戰場中，火力集中將代替了兵力集中，在網路內可將陸、海、空、天各種作戰器整合在一起，對目標同時實施打擊，同時網路力量也加強火力的威力，故打擊對象不再是通過消滅敵兵力來破壞對方的火力，而是以癱瘓敵通信網路或者打擊敵偵察網路來實現。[347]

中共學者張軍表示，資訊嚇阻造成己方的信息戰聲勢，並以資訊武器的威力，使敵不敢輕易使用戰場資訊，從而影響其指揮和控制，降低其信息攻擊的效果。基本方法，首先要依靠高效、實時的網際網路和處理系統，獲得情報優勢，進行強烈的資訊壓制，配合以威懾性的宣傳，震憾敵人的戰鬥意志，破壞敵人信息系統，切斷其信息神經，使敵方信息攻擊能力減弱。[348]2002 年，中共網路戰專長戴清民少將亦表示，未來網路時代，網路進攻的能力將成為衡量一個國家軍事實力的重要標誌，從技術角度而言，網路進攻比網路防禦容易，換言之，網路防禦滯後網路進攻，沒有一種防禦技術能夠在網路防禦上永遠取得領先，只有一種新的網路進攻手段產生後，才能尋求相應的防禦措施。作為信息不發的國家，只有形成一定網路進攻能力，才能有效遏制信息發達國家的威懾。[349]

中共資訊戰專家沈偉光及現行解放軍信息工程大學校長鄔江興少將兩人均強調，非接觸、非線式作戰將成為網路戰為主要形式，首先是對資訊通信基礎設施至各種通資網路系統實施攻擊，進而影響武器精度與打擊能力。其次尤其網路威力巨大，在敵人毫不知情的狀態下，幾個網路間諜就讓敵國經濟、和社會陷入癱瘓。最後就是傳導至實體世界產生擾亂金融、交通、能量系統，從而影響戰爭實力，也就是間接的方式影響戰局，從而迅速達成戰爭目的。[350]

除此之外，美國學者穆文濃等人亦表示，中共網路攻擊準則，特別重視瓦解與癱瘓，而不是摧毀，其目的就是困惑敵軍指揮官的思考，而贏得勝利。電腦作戰就是要標定電腦，亦即武器與指管通資情監偵系統(C4ISR)的核心，以癱瘓敵人，就是給予敵人致命打擊。或是嚇阻敵方，將衝突的代價提高到無法接受的程度，特別是對非軍事目標進行電腦網路攻擊，其目的是要動搖作戰決心，摧毀戰爭潛力，進而破壞敵方人民參與軍事衝突的政治意願[351]

---

[346]黃郁芬、林翠儀譯，〈美國防部:中國軍事力及意圖不透明〉，《自由時報》，2014 年 3 月 6 日，版 3。

[347]馬亞西、成冀、王漢水，《網路戰-地球村時代的戰爭》，北京:國防出版社，1999 年，頁 109。

[348]張軍主編，《IT 戰爭》，北京:科學出版社，2000 年，頁 35。

[349]載清民，《直面信息戰》，北京:國防大學出版社，2002 年，頁 60。

[350]沈偉光主編，《電子軍務-敲開未來戰爭之門》北京:新華出版社，2003 年，頁 24;鄭文浩、楊雷，〈網路戰比核彈威脅更大〉，《瞭望東方周刊》，第 47 期，2013 年 12 月 12 日，頁 41。

[351]國防部史政編譯局譯，穆文濃(James C.Mulvenon)、譚睦瑞(Murray Scot Tanner)、蔡斯(Michael S. Chase)、傅里林格(David Frelinger)、龔培德(David C.Gompert)、李比奇(Martin C.Libicki)、包克文(Kevin L. Pollpeter)，《中共對美國軍事變革之反應》(Chinese Responses to U.S.Military Transformation and Implications for the Department of Defense)，台北:國防部史政編譯局，2010 年，頁，120-121。

2011 年 4 月，美國學者成斌披露，中共認為資訊嚇阻為擴大運用資訊科技以影響外國政府、軍方和人民，被視為一種獨立形式的交互作用，且具備不戰而屈人之兵的潛力。有個兩個面向，其一偏向作戰面，係影響戰場上資訊流的能力，另一面則趨戰向戰略，影響本國、敵國和第三方的決策者與民眾。並運用綜合國力來維持國家安全，達成戰略嚇阻的最佳手段不僅限於軍事力量，包括經濟、外交和政治手段。[352]

3. 蒐集情報

2010 年，美國學者穆文濃等人共同指出，情報蒐集乃是資訊優勢的基礎，在作戰開始之前或初期階段，必須攻擊敵之偵察與早期預警系統，戰役開始後，資訊戰的主要任務，就是攻擊敵方的偵察系統，進行資訊欺敵，進而掩蔽我方的作戰意圖，防護我軍部隊發動攻擊。[353]穆文濃，並引用 2001 年《人民日報》的一篇報導指出，中共就毫不隱諱引用美國海軍瀏覽器網站有關海中國演習 2 個航艦戰鬥群來源、目的地與意圖，但在 911 事件後，公開性的資料已大幅下降，運用非保密網際網路協定路由器網路所獲得的情報利益，因而也變得更為重要。[354]

中共學者東鳥表示，在十二五規劃(2011-2015)中，中國以網路為基礎的戰爭的研究將佔據顯要位置，其中包括網路間諜和反間諜。胡錦濤把加強電子戰的能力，列為中共未來 10 年國防和安全部隊的工作重點，並給予與 IT 安全相關的商業計算機和電子企業一定的優惠政策。自 20 世紀 80 年代以來，這些企業就與中國人民解放軍、中國人民裝警察、國家安全部及公安部的某些相關單位共享數據和資源。[355]

2011 年，美國學者費學禮指出，中共對美國遂行網路作戰與間諜活。單單美軍電腦腦路遭受中共網路作戰攻擊所造成的損失就多達數千萬美元，中共也可能正在「準備作戰空間」，以攻擊並癱瘓美國軍方和民間電子基礎設施，俾支援其針對美國目標的軍事作戰。[356]根據美國國防部的研究，2012 年世界各地許多電腦系統的入侵與中共解放軍網軍有關，相關攻擊已不僅僅是進行平時作戰情報之資料收集，甚至以商業對象，可以想見在戰爭爆發衝突時，網路戰結合並發揮火力攻擊效果貫穿全程，而成為美軍隱憂。[357]

國內學者陳漢強及蘇文德指出，中共目前的資訊作戰大約分為兩個方面:第一就是對內進行全面的互聯網(Internet)監控，監控的精密程度則是全球第一，動員無數的國家機構和成千上萬的公、私人員，審查包括網頁、網路日誌、討論區、大學的留言版以及電子郵件之內容。中共推行了龐大的互聯網監控的過濾工程，最著名莫過於「金盾工程」[358]及其重要組成部分「防火長城」不僅是資訊和

---

[352]高一中，Dean Cheng，〈中共對嚇阻的觀點〉(Chinses Views on Deterrence)，《國防譯粹》，第 38 卷，第 4 期，2011 年 4 月，頁 53-54。

[353]同註 331，頁 102

[354]同註 347，頁 124-126。

[355]東鳥，《中國輸不起的網路戰爭》，北京:中南出版傳媒集團，2010 年，頁 252。

[356]國防部史政編譯局譯，費學禮 (Richard D. Fisher Jr.)，《中共軍事發展-區域與全球勢力佈局》(China's Military Modernization-Building for Regional and Global Reach)，台北:國防部史政編譯局，2011 年，頁 425。

[357]于揚，〈中國裝力量的多樣化運用白皮書 vs 中國軍力報告〉，《亞太防務》，第 63 期，2013 年 1 月，頁 34。

[358]「金盾工程」是中共國家保安控制機構，主要包括(1)包括全中國成年人口的全國性資料庫;(2)

言論自由的最大敵人，更可能對全球的安全造成威脅，因此可能就是利用當中的電腦運算能力來進行各種戰略運動，第二種就是網路戰方式-駭客攻擊。[359]

2013 年 3 月 12 日，無國界紀者組織(RSF)表示，敍利亞、中共及伊朗等政府監控網路活動最嚴重，中共經營的數位帝國才是全球最大的。該組織並表示，中國大陸個人及企業均須向國家或國營公司租借寬頻。自 2003 年起，中共藉「防火長城」過濾國外網站，並封鎖當局禁止的訊息。目前有 30 名記者和 69 員網民因新聞和資訊入獄，屬全球最多。[360]國內國防大學教官張玲玲表示，中共當局不僅全面掌握了「網路主權」，更可使共軍藉由網際網路管控來直接提高網路作戰和情蒐能力，對各國造成威脅已是不爭事實。「十八大」召開期程，美國谷歌被大面積阻礙連線，嚴重程度促使 2013 年歐習會將「駭客網攻」列為首要議題。[361]

除此之外，根據 2014 年 5 月 29 日《青年日報》報導指出，中共工業和信息化部、公安部、國家互惠網信息(網路資訊)等三大部門，將對微信(We Chat)等移動即時通訊工具展開為期一個月的專項治理行動，以遏制少數人借此類平台向公眾發布「不良」或「違法有害」等資訊。[362]該報導並表示，中共新疆當局將對部分即時通訊工具(微信)實施臨時管制措施，這是新疆自 2009 年「七五事件」斷網以來，第二次對網路工具採取限制使用，當年管制措施歷時近一年。[363]從以上資料得知，中共在蒐集情報方面，除積極蒐集軍事強國軍事及民間重要資料外，對於境內掌握網路論談也不敢掉以輕心。

全民要隨身攜帶的智慧卡，讓當局可在幾米的距離內在持卡人不知情下掃描;(3)設立監視電視以監控公眾地方;(4)發展一種可讓公安當局可以即時進行對照指紋的技術;(5)據目前估計，投入「金盾工程」來監控民眾的人數高達三十萬左右。

[359]陳漢強、蘇文德，〈中共信息戰之網路攻擊型態研究〉，《新新季刊》，第四十卷第二期，2012 年 4 月，頁 235。

[360]〈全球網路監控 敘中最嚴重〉，《青年日報》，2013 年 3 月 13 日， 版 5。

[361]張玲玲，〈中共管控網際網路 對內維穩對外情蒐〉，《青年日報》，2014 年 3 月 9 日， 版 7。

[362]黃德潔，〈六四前夕 中共加壓箝制通訊輿論〉，《青年日報》，2014 年 5 月 29 日， 版 4。

[363]同註 362。

第二節　中共網路戰之編組與經費

一、中共網路戰之編組

(一)編制

中共學者馬亞西、成冀、王漢水等三人指出，網路兵是負責網路保障的兵種，在網路兵下面也許還可以分為通信兵或資訊兵，資訊兵是網路化部隊的新面孔，網路兵直接負責情報保障，一方面，軍事網路由網路兵負責維護、管理，另一方面，信息的獲取是由網路兵中的偵察部隊獲得，信息的傳輸是由網路兵的中的計算機通信部隊來執行。[364]

中共載清民少將強調，網路戰部隊肩負網路安全及網路攻擊的雙重使用。具體地講，主要包括:一是確保己方軍用網路系統及網路信息暢通，就是需要的時候，支援多個部個部隊編制結構方案，遂行消除電腦病毒對我方網路安全程，最大限度地保障部隊準確、及時獲取所需資訊，二是破壞敵方軍用網路系統，向敵網路系統中的某一未加防護的接收處理系統，輻射電腦病毒，使其接收信息後感染病毒，從而造成網路癱瘓。[365]

中共學者沈偉光指出，按照有獨立的基本武器、戰鬥使用方法，及兵種劃分原則，網路特攻必將成為新的兵種。網路特工將編屬於各軍兵種及總司令部的直屬部隊，擔負著各類部隊和戰略級、戰役級和戰術級別的資訊系統及網路使用安全的任務，由網路特工由以下擔負不同任務的網路防竊部隊、網路防病毒部隊、網路防毀部隊、網路對抗部隊部隊組成。[366]

2004 年 11 月，由副總參謀長張黎上將，及軍事科學院世界軍事研究部長閔振范少將及和研究員王保存少將共同撰寫的《構建信息化軍隊的組織體制》乙書指出，資訊化戰爭，不戰是單位或數個作戰單位之較量，而是作戰力量系統的對抗，另外，各戰區部隊面臨的任務和環境條件差異很大，在這情況下，部隊編制改革須加強或創建新部隊，如戰役戰術導彈部隊、陸軍航空兵部隊、電子對抗部隊、特種作戰部隊和海軍陸戰隊，創建航天部隊、信息戰攻防部隊、計算機應應急分隊。[367]

根據 2012 年 9 月 2 日《自由時報》的報導，中共網路作戰是由軍方、公務部門編組，同時也結合民間資源與資訊人才，形成龐大的網路攻擊能量，藉以網路駭客、病毒攻擊，實施竊取、竄改、刪除等作業，對敵國政、經、軍等相關網站、系統進行網路攻擊。[368]中共解放軍信息工程大學校長鄔江興亦表示，網路部隊跟一般軍隊一樣有進攻、也有防禦，有正規軍有預備役，整個技術和保障方面的佈局以及相關策略和戰術也都有相應的支撐。未來網路戰是越來越激烈，將是綜合國力的較量，是軍隊素質的較量，是全民信息素質的較量。[369]

---

[364]馬亞西、成冀、王漢水，《網路戰-地球村時代的戰爭》，北京:國防出版社，1999 年，頁 142。
[365]載清民，《直面信息戰》，北京:國防大學出版社，2002 年，頁 141。
[366]沈偉光主編，《電子軍務-敲開未來戰爭之門》北京:新華出版社，2003 年，頁 116。
[367]張黎，《構建信息化軍隊的組織體制》，北京:解放軍出版社，2004 年，頁 306-307。
[368]羅添斌，〈反制中國網軍我建構網路戰攻防驗測環境〉，《自由時報》，2012 年 9 月 2 日，版 6。
[369]鄭文浩、楊雷，〈網路戰比核彈威脅更大〉，《瞭望東方周刊》，第 47 期，2013 年 12 月 12 日，頁 42-43。

中共總參謀部，分為「部」、「局」的格局，每一個部，都主管一個兵種，一旦成立「部」，就意味著形成了新的兵種成立。總參謀部成立「信息化部」，意即在軍區、集團軍層次會成立信息處、在師層次成立信息化科，另在部隊結構層次，集團軍、師現有的「通信營」「通信連」基礎上轉換信息化營、連等。中國軍隊在 2011 年，將原通信部的基礎上，成立了「信息化部」[370]，其意味著中共將正式組建了編制化的資訊化部隊，其重要使命在於「資訊防護」、「資訊進攻」。[371]

中共總參三部總部位北京海淀區廂紅旗，監聽人員至少 2 萬人員以上。總參三部下屬 56、57、58 研究所，各自負責電腦、通訊監聽、及信號情報處理、信息安全，並且在珠海航空展上亮相過，分別為江南計算機科技研究所、西南電子電信技術研究所及西南自動化研究所。[372]

此外，據瞭解，中共解放軍總參謀部第四部門(電子對抗和雷達)可能利用干擾/電子戰、計算機網路戰和欺騙等在內的資訊戰工具，以增強戰時爭奪空天和其它作戰能力，最有可能的作戰行動即解放軍干擾美軍導航與雷達。其報告並透露，中共網軍已不僅僅是進行平時作戰情報之數據收集，甚至以商業為對象，限制和降低其後勤與通信的反應時間可以想見在衝突階段，一旦須結合並發揮火力攻擊效果，網路戰勢必貫穿全程，為戰力的倍增器。[373]

另外，在 2012 年《中華人民共和國中央人民政府》網站指出，2012 年 2 月 27 日，由中共工業和信息化部副部長劉利華率部辦公廳、財務司、人教司、無線電管理局等部門有關同志，赴共軍預備役電磁頻譜管理中心視導。劉利華並表示，「預備役電磁頻譜管理部隊」是國務院、中央軍委的戰略決策，是走中國特色軍民融合式發展道路的重要探索和具體體現，對未來打贏資訊化條件下局部戰爭具有重大意義。[374]

除此之外，根據美國學者的研究，中共特戰作戰係運用特別組成、訓練及裝備的菁英單位，藉由非傳統或非正規的作戰手段，來達成特定的作戰及戰略目標，其核心構想包含特種偵察、特種打擊、破壞敵設施，及特種技術性戰鬥，包括不同形式的電腦網路攻擊、文宣攻擊，及擾亂敵導航及定位系統，並指出，中共特戰部隊將在未來「信息化條件下的局部戰爭」中占有重要位階，包括發動直接攻擊、提供目標標定資訊，以及影響敵軍可用軍需資訊。[375]由此可知，中共在建制網軍發展上，除吸納各方面網路人才，並結合原建制電子戰部隊、通信信站及特戰部隊，外加以人海戰術為基礎民兵整合而成。中共網軍發展編制，如圖 4-2。

---

[370]信息化部(原通信部改制)隸屬於總參謀部，成於 2011 年 6 月 30 日，主要職能，統籌全軍資訊化工作，制定相關政策，促進電信、廣播電視和電腦網路融合、指導協調電子軍務發展，推動跨軍兵種的互聯互通與重要資訊資源的開發利用、共用。統一規劃、配置與管理安全全軍無線電頻譜資源，協調處理軍地間無線電管理相關事宜。

[371]史可夫，〈中國軍隊正式成立駭客部隊〉，《漢和防務評論》，第 87 期，2012 年 1 月，頁 23-25。

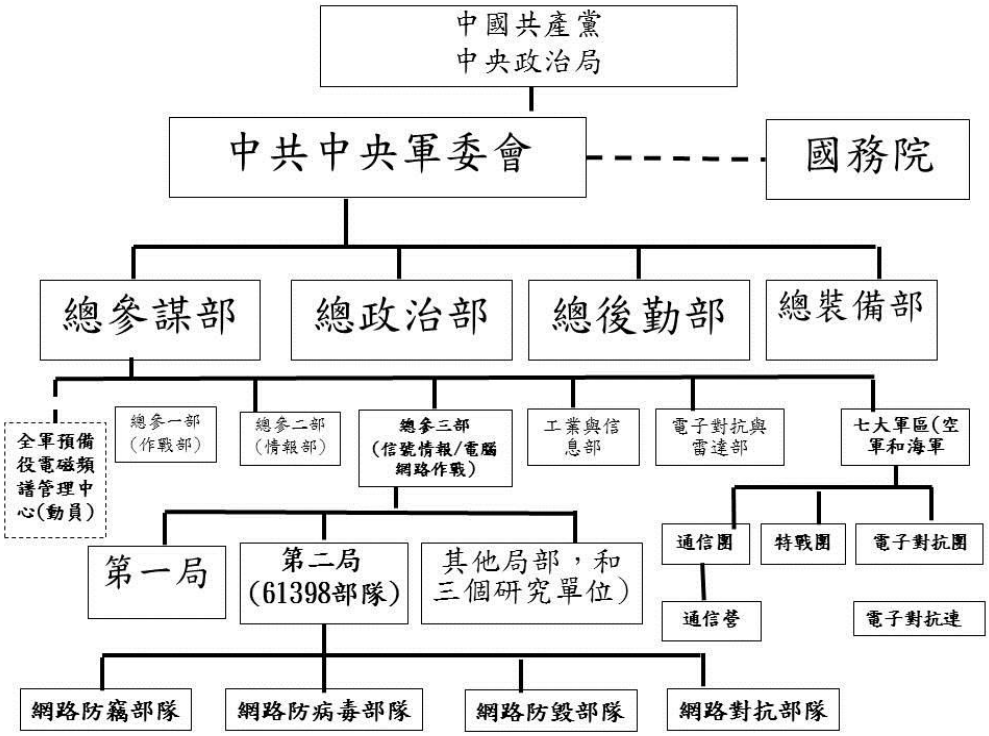
[372]平可夫，〈中國在西藏建設監聽站〉，《漢和防衛評論》，第 93 期，2012 年 7 月，頁 36-37。

[373]易予聖著，〈新與舊酒-淺析美國國防部公布的 2013CMPR〉《尖端科技》，第 347 期，2013 年 7 月，頁 35。

[374]〈劉利華一行赴全軍預備役電磁頻譜管理中心調研》，《中華人民共和國中央人民政府》http://big5.gov.cn/gate/big5/www.gov.cn/gzdt/2012-03/14/content_2091612.htm (2014 年 3 月 23 日)

[375]黃淑芬譯，Dean Cheng，〈共軍特種作戰〉(The Chinese People's Liberation Army and Special Operations)，《國防譯粹》，第 39 卷，第 12 期，2012 年 12 月，頁 87-91。

圖 4-2:中共網軍發展編制圖



作者整理
資料來源: 國防部史政編譯局譯，費根保 (Evan A. Feigenbaum)，《中共科技先驅: 從核子時代到資訊時代的國家安全與戰略競爭(China’s Techno-warriors National Security and Strategic Competition from the Nuclear to the Information age)》，台北:國防部史政編譯局，2006 年，頁 143; 蔡翼主編，《崛起東亞-聚焦新世紀解放軍》，台北:勒巴克顧問出版社，2009 年，頁 221、229。; 史可夫，〈中國軍隊正式成立駭客部隊〉，《漢和防務評論》，第 87 期，2012 年 1 月，頁 23-25。沈偉光主編，《電子軍務-敲開未來戰爭之門》北京:新華出版社，2003 年，頁 116。賴昭穎、程嘉文，美抓駭客 揪出解放軍網戰部隊，聯合報，2013 年 2 月 21 日，16 版。

(二)中共網軍人數

1.解放軍建制內的網軍

2004 年，曾任中國時報系政治、軍事記者的劉台平先生指出，中共發展網軍共分兩個階段，前一階段是以軍方為主導體，後半段則依靠民間企業力量，中共早期「網軍」並無此稱呼，勉強可歸類到「電子通訊部隊」，早期的人才都從通信學校培養，優秀的才集中到具有情特性質的學校，畢業後就分發到部隊，擔任通訊及監聽工作，軍中最大的諜報單位算總參二部、三部，以及總政、科工委、國安及公安兩部。中共為了應付網路戰到來，已成立一支約為 40 萬人的「網路部隊」又稱為「網路警察」或第四軍，他們的任務就是積極發展自己的網路王國，消極的打擊任何網上的敵人，包括政治、軍事、經濟及社會人文方面不容於己的異議對象。[376]

中共自 2004 年決心開始在全球「網際網路」的信息高速公路上急起直追，

[376]劉台平，《島計畫-2008 年中共發動對台割喉戰》，北京:時英出版社，2004 年，頁 30-32。

首先組合全國相關 IT 產官學界，建立有自主權的「中國互聯網」，以打破來自美國的「不對稱威脅」，這是中國面對全球網際戰爭中的頂層設計。運用廣大的民間力量結合高科技和國家機制組成「網際軍隊」，由信息產業部、公安部負責網軍的安全與防禦;由軍隊和國安部負責網軍的攻擊。而更重要的是，由「國家動員委員會」所轄的「信息動員辦公室」所負責的龐大的「信息民兵部隊」才是真正的「網軍」所在。[377]

2010 年 7 月，我國學者呂炯昌引用 2010 年 1 月初美國聯邦調查局(FBI)的一份機密報告指出，中共已經組一支超過 18 萬人的網路軍隊，其中 3 萬人為網路特工，15 萬為民間駭客，目標是在 2020 年建立全球第一支「資訊化武裝的部隊」。[378]另在 2013 年，我國學者徐佳學者亦指出，中國網軍屬於正式國防編制，各個省份都有完組織體系、分工。美國聯邦調查局估計，中國網軍人數高達近 20 萬人，主要研究各種網路偵察技術、攻擊軟體，竊取各國國防機密，甚至可癱瘓作戰指揮系統。[379]

根據美國網路安全公司曼迪安認為，中共總參三部二局三處的 61398 部隊，就是造成美國網路安全先進持續性威脅的單位，並將該部隊賦予 APT1 代號。美國曼迪亞公司估計，中共網軍部隊人數從數十人到數百人，甚至多達數千人不等，並表示，中共已在網際空間建立數位灘頭堡，並持續厚植實力。[380]另據美國學者表示，中國上海交通大學的學者，與被指控對美國政府機關與企業發動網路攻擊的中國人民解放軍「61389 部隊」研究員有多年合作關係。也有報導顯示，上海交大信息安全工程學院為 61398 部隊提供技術支援，該校計算機科學與工程系也與另支解放軍部隊在研究上合作，負責監聽外軍信號。此外，研究和分析情報的解放軍總參三部(總參三部二局就是 61398 部隊)上海基地，與上海交大信息安全工程學院大樓於同一工業園區，上海交大信息安全工程學院大樓對街，是國家資訊安全工程技術研究中心的大樓。[381]

除此之外，據林宗達的研究，中共解放軍提供清華大學和北京大學信息相關科系的資優生領取獎學金，並利用寒假至軍隊接受網路戰課程訓練。21 世紀初，畢業於清華大學和北京大學的電腦專業的資優生，就有超過 300 名服役於中共解放軍。[382]我國黃銘俊上校亦指出，中國軍方對網軍的訓練是很有系統訓練，在它的資訊產業單位支持下，提供大量經費與工作實習機會相關院校、除訓練碩、博士生外，也分配了若干研究案給師生實作，並結合重點高校的人力、物力，如武漢的通信指揮學院、鄭州的資訊工程大學、南京的理工大學、長沙的國防科技大學、武漢的海軍工程大學。這些院校提供解放軍訓練資訊戰人才來源，也提供中國國防工業中資訊產業所需的專業人員。[383]另據中共浙江大學「招生頁面」指出，中共 61398 部隊將召收浙江大學資訊系碩士生，並提供每年 5000 元人民幣的國防獎學金，以增進網軍實力，如圖 4-3。[384]

---

[377]廖文中，〈中國網軍〉，《全球防衛雜誌》，272 期，2007 年 11 月，頁，6。
[378]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》，第 311 期，2010 年 7 月，頁 87。
[379]徐佳，〈網軍來襲，新一代國防戰開打〉，《數位時代》，第 228 期，2013 年，5 月，頁 91-92。
[380]王文勇譯，(David Alexander)，〈網路防衛戰略方案〉(A SDI for Cyberspace)，《國防譯粹》，第 40 卷，第 9 期，2013 年 9 月，頁 53。
[381]張沛元，〈上海交大遭爆與解放軍駭客部隊合作〉，《自由時報》，2013 年 3 月 25 日， 版 12。
[382]林宗達，〈中共信息戰之「網軍」作戰初探〉，《展望與探索》，第 5 卷第 9 期，2007 年 9 月，頁 67。
[383]蔡翼主編，《崛起東亞-聚焦新世紀解放軍》，台北:勒巴克顧問出版社，2009 年，頁 231。
[384]李文慧，「中共黑客部隊「61398」外招研究生通知曝光」，《大紀元》，<

圖 4-3. 中共網軍網址及招生網頁圖

美國網路安全業者Mandiant指出，以美國為主要對象駭客攻擊，來自中共上海一浦東一棟12層建築，即61398部隊所在地。估計部隊成員約在數百人到2000人之間。	在浙江大學的計算機與技術科學學院的「招生頁面」，有一個2004年浙江大學的招生通知，標題為「中國人民解放軍61398部隊招收定向研究生的通知」。以下為該通知全文：『接研究生院通知，中國人民解放軍61398部隊（地點在上海浦東）擬招收2003級計算機專業碩士研究生為定向生，對簽定協議的學生將提供5000元/學年的國防獎學金，學生畢業後定向到部隊工作。我院2003級碩士研究生如有意向，請在5月20日前與學院研究生科彭老師聯繫。（曹光彪108室，電話：87952168）研究生科』

作者整理

資料來源: 李文慧，「中共黑客部隊「61398」外招研究生通知曝光」，《大紀元》，<http://www.epochtimes.com/b5/13/2/21/n3806067.htm >（2014 年 3 月 16 日）；「神秘 61398 部隊 隸屬總參三部二局？」，《Etoday》，<http://www.ettoday.net/news/20130221 /165797.htm>（2014 年 3 月 16 日）。

2. 中國民兵之網軍

網路戰部隊，作為常備的軍事力量，還必須有一支強大的後備力量，網路戰後備力量在戰爭中可以在許多方面發揮作用，包括直接參與對敵國的駭客攻擊、病毒傳播，集體發送郵件進行拒絕式服務，還可以致使敵國網路伺服器癱瘓，對網路戰相關的能源設施、網路設備等開展保護工作。全球眾多的的網民，無疑會在未來的網路戰中扮演重要的角色，有效動員和組織廣大網民和網路專業人員進行「人民網路戰爭」，將是網路戰一個制勝的法寶。[385]

中共網路戰不光只是在戰術上運用電腦傳送情報、指揮作戰，作為「火力戰」配角，而是提升到「軟打擊」的程度，並將力量放在「資訊化部隊」和「智囊團」建設。[386]林宗達指出，中國民兵已步入資訊戰戰場，山西已經有熟悉網路戰的民兵，這支民兵網路分隊建於 1998 年年初，編班有程序班、操作班、保障班和培訓中心等，四十多名網路戰士，都已經通過全國計算機等級考試，百分之六獲得技術職稱。在信息安全防護和網路攻防戰術，已有一些實用的研究，取得一些初步成果，並先後在北京軍區和華北各地區進行演習。中共的軍事專家亦指出，中共已經在一此城市編組小型信息戰預備役部隊。例如，在湖北省宜昌市，軍分區組織了 20 個市政部門的技術人員成立了預備役信息戰團。該部擁有網路戰營、電子戰營、情報心理戰營及 35 個技術分隊。該部還建立中國第一個能容納 500 人的預備役信息戰訓練基地，然而宜昌不是組織預備役和民兵進行信息戰

---

http://www.epochtimes.com/b5/13/2/21/n3806067.htm >（2014 年 3 月 16 日）

[385]載清民，《直面信息戰》，北京:國防大學出版社，2002 年，頁 139-140。

[386]行政院研究發展考核委員會，《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》，台北:五南文化出版，2002 年，頁 46-47。

訓練的唯一基地，在此基地，中共民兵的網軍可以進行人民戰爭之信息網路作戰模擬演習。[387]

中共為增強「資訊作戰」或「電子作戰」能力，積極研發配套裝置。資訊戰裝備方面，共軍近年來除積極研發電腦病毒，建立攻擊敵人電腦與網路系統外，並結合民間資源與資訊人才，形成龐大網路攻擊能量。[388]2012 年 12 月底，中共四名學者指出，中共能擊敗美國的兩大王牌，將是太空戰及網路戰的兩者軍事實力相結合，並強調，網路戰不限於軍事人員，所有擁有資訊系統特殊知識與技能的人，都能參與網路戰爭，讓網路戰爭真的成為人民戰爭，網路攻擊手段包括放出電腦病毒、竊取或竄改資料、分散式阻斷服務攻擊(DDoS)、引爆網路炸彈，導致敵軍的資訊網路立即癱瘓或毀壞，網路攻擊的另一特性能夠迅速發動攻擊，而且能不留痕跡，不傷害任何實體設施或人員，但卻能夠造成巨大影響。[389]

中共近年來陸陸續續規劃、建置及投資網路建設，甚至舉辦所謂「駭客擂台」，藉以吸收大陸民間技術精湛之駭客，將其納入至網軍中，並視其專長編組，各組依據任務需求，入侵各國網路，伺機竊取機敏資料。[390]中國大陸 13 億人口，具有巨大的優勢實施任何網路活動。例如，即使是原始的網路攻擊方式，中國大陸可以利用人民的電腦建立殭屍網路，進行簡單的分散式阻絕服務(DDos)攻擊，癱瘓任何一個目標網站。因此，人民戰爭思想在網路空間發展前所未有的前景。為此，已準備動員大規模群眾，以實現其網路戰的戰略目標。[391]

2013 年 3 月，中共寧夏軍區司令員昌業庭少將指出，國防後備力量體系，按照作戰隊伍類編，應急隊伍常態建、專業隊伍重點儲，結合國防動員潛力調查，摸清高學歷、懂技術、有專長人員分佈狀況，並將編組範圍向大專院校、科研院所、高新技術拓展，向行業系統廷伸，最大限度高技術人才編入民兵組織，提升編組質量。積極推動國防動員向新一代資訊技術、生物技術、新能源拓展，重點在民用航空、資訊通道及無線電管理，計編組戰役投送、網路攻防和電磁頻譜管理等新型保障分隊和網路技術支前分隊、加強網路防護、偽裝保障等國防動員特種專業保障隊伍建設及資訊、網路專業人才儲備，達到不求所有，只求所用。[392]

此外，2013 年 10 月 17 日，中共「預備役電磁頻譜管理部隊」第一批編入的 100 名預備役軍官中，有資訊綜合與頻譜管控等領域的專家骨幹，也有預編單位主要領導，其中黨員佔 80%，50%人員具有高級職稱。為解決解決裝備維護保障難題，還將工信部相關司局、頻管研究機構和設備製造企業納入預編單位，預編單位的預備役軍官，操作設備均在 8 年以上，一旦有任務下達，能迅速進入情況，成為該中心的一支優質力量。該消息指出，在 2011 年 7 月，該中心擔負深圳世界大學生運動會無線電安保任務。他們依託深圳、北京、上海、成都 4 個國

[387]林宗達，〈中共信息戰之「網軍」作戰初探〉，《展望與探索》，第 5 卷，第 9 期，2007 年 9 月，頁 71。
[388]張淑中著，〈中國大陸軍事及科技發展的全球戰略意涵分析〉，《中共研究》，第 47 卷，第 10 期，2013 年 10 月，頁 101-116。
[389]陳維真，〈中國數位人民戰爭 全民抗美〉，《自由時報》，2013 年 8 月 1 日， 版 AA2。
[390]陳漢強、蘇文德，〈中共信息戰之網路攻擊型態研究〉，《新新季刊》，第四十卷，第二期，2012 年 4 月，頁 236。
[391]黃基禎，〈中國大陸網路戰思維〉，《中共研究》，第 47 卷，第 10 期，2013 年 10 月，頁 150。
[392]昌業庭，〈以十八大精神為指導 在新的起點上推進國防動員建設科學發展〉，《國防》，第 2 期，2013 年，頁 14。

家級固定監測站，建立了異地組網、機固結合的監測機制，僅用 15 分鐘就排除了計時計分系統干擾。[393]綜合上述，中共網軍兵力人數預估統計約為 7 萬餘人，如表 4-1。

表 4-1:中共網軍兵力推算表

區分 / 項目	單位	預估兵力人數	備註
	總參三部	20000 員	總參三部下屬 56、57、58 研究所，各自負責電腦、通訊監聽、及信號情報處理、信息安全。
	全軍預備役電磁頻譜管理中心（民兵）	600 員	第一批編入的 100 名預備役軍官中既有資訊綜合與頻譜管控等領域的專家骨幹。而在 2000 年時，中共已經整建可以訓練的 500 學員，以作為人民武警進行信息作戰武力的基地
解放軍	電子對抗團	11000 員	瀋陽軍區(1 電子對抗團;約 1500 員) 北京軍區(無) 蘭州軍區(1 電子對抗團;約 1500 員)
解放軍			濟南軍區(1 電子對抗團;約 1500 員) 南京軍區 1 個電子對抗旅、1 個電子對抗團(約 3500 員) 廣州軍區(1 電子對抗團;約 1500 員) 成都軍區(1 電子對抗團;約 1500 員)
	通信團	21000 員	瀋陽軍區(第 16 集團軍、第 39 集團軍各 1 個通信團)約 3000 員。預估其它軍區也同為 3000 員，故換算約為 21000 員。
	特戰人員	18000 員	瀋陽軍區特種團(1500 員) 濟南軍區特種團(1500 員) 蘭州軍區 1 個特種團(1500 員) 成都軍區 1 個特種團(1500 員) 南京軍區 3 個特種旅(6000 員) 廣州軍區 2 個特種旅(4000 員)
共計		70,600 員	

作者整理

資料來源: 國防部史政編譯局譯，甘浩森(Roy Kamphausen)，施道安(Andrew Scobell)

[393]胡光曲，〈全軍預備役電磁頻譜管理中心打造高技術尖兵》，《華夏經緯網》http://hk.huaxia.com/thjq/jsxw/dl/2013/10/3573880.html (2014 年 3 月 23 日)

著，《解讀共軍兵力規模(Right-Sizing the people' Sliberation Army)》，台北:國防部史政編譯局，2010 年。頁 261-282; 編輯部，〈中國軍隊在西藏的部署與軍事訓練〉，《漢和防衛》，第 103 期，2013 年 5 月，頁 58-59。平可夫，〈中國在西藏建設監聽站〉，《漢和防衛》，第 93 期，2012 年 7 月，頁 36-37;林宗達，〈中共信息戰之「網軍」作戰初探〉，《展望與探索》，第 5 卷第 9 期，2007 年 9 月，頁 71。中華網，《外媒:EP3 可助中國電子科技實力提升十年》，http/military.china.com/20010405/159262.Html;中共七大軍區專題系列，http://www.youth.com.tw/db/epaper/es001001/m970506-b.htm〈中共軍隊遭起底 實力最強軍區曝光〉，《新唐人》，2014 年 2 月 17 日訊 http://www.ntdtv.com/xtr/b5/2014/02/17/a1063521.html 胡光曲，〈全軍預備役電磁頻譜管理中心打造高技術尖兵》，《華夏經緯網》http://hk.huaxia.com/thjq/jsxw/dl/2013 /10/3573880.html;換算基準:依 2008 年國務院新聞辦發佈《2008 年中國的國防》之中共「陸軍部隊實行集團軍、師（旅）、團、營、連、排、班體制」換算。旅由營編成，隸屬於集團軍，為戰術兵團。團由營編成，通常隸屬于師，為基本戰術部隊。營由連編成，通常隸屬於團或旅，為高級戰術分隊。連由排編成，為基本戰術分隊。以現行一個連約 120 人換算，一個營約為 500 人、團 1500 人、旅 2000 旅。

二、中共網軍經費

(一)人員維持費

2013 年 4 月 29 日，我國國安局副局長張光遠向外交及國防委員透露，中共自 2002 年起擴充網路戰能量，發展初期雖落後各先進國家，然近年來積畜相當能量及業務分工廣佈總參 4 大總部、7 大軍區、國防科研機關與各級院等，任務包括戰時網路攻擊，以及平時網路竊密、網路滲透遂行諜報活動等;另國防動委員會亦將信息民兵納入編組，預判其正式編制內人力約 10 萬人，2013 年投資經費推已超過 8,000 餘萬元。[394](依 2013 年人民幣與美元兌換率以 1 至 8 月平均滙率為 1:6.19 換算為 99,040 萬人民弊,平均每人每年薪貿為 4952 人民幣)。依《中華民國共和國統計局》網站供佈顯示，「國有單位」就業人員平均工貿為每人 48,357 人民幣/年為基準[395]，故報導數字僅為 1/10，較為不合理。

依我國國防部出版 102 年《國防報告書》的資料，中共解放軍兵力約 227 萬餘人(陸軍 125 萬、海軍 26 萬、空軍 37 萬及第二砲兵約 14 萬 9 千餘)。[396]中共網軍 10 萬人員計算，約佔全體解放軍 0.04%。依這些資料估計，中共 2013 年國防預算為 7,201.7 億人民幣[397]。根據《中華人民共和國中央人民政府》網站之《2010 年中國的國防》白皮書，中國國防費主要由人員生活費、訓練維持費和裝備費 3 部分組成，各部分大體各佔三分之一。[398]中共網軍人員維持費為大約為 960.22 億人民幣。(每人每年平均 96,022 仟人民幣)。

(二)裝備硬體費

1. 網路戰系統提升

中共 2013 年國防預算為 7,201.7 億人民幣，[399]裝備費佔大體三分之一。[400]經換算後，中共 2013 年投資裝備費約為 2400.3 人民幣。2006 年，由中共解放軍出版社出版《信息化聯合作戰》一書指出，隨著資訊化技術的不斷發展，一些軍事強國以資訊技術為基礎，在作戰平台及武器系統開始運用於實戰。這些資訊化度的武器，以資訊、機動、火力為基本作戰效能，為精準火力打擊、網路戰系統提供了物質的基礎。[401]2007 年，中共解放軍對國防科技專長人員張蜀平、禚法寶、王祖文等三人指出，隨著美國近幾年的軍費持續攀升，其中 40%以上直接用於軍事轉型。[402]這些資料顯示，中共投資網路戰武器費用約為 960.13 億人民幣。

---

[394]立法院，〈我國如何因應網軍與駭客攻擊並強化資訊安全措施〉,《立法院公報》，第 102 卷，第 6 期，頁 6。
[395]中華人民共和國國務院新聞辦公室，〈中國統計年鑑 2013〉,《中華人民共和國國家統計局》，< http://www.stats.gov.cn/tjsj/ndsj/2013/indexch.htm>。(2014 年 2 月 10 日)
[396]國防部，《中華民國 102 年國防報告書》，台北:五南文化出版，2013 年，頁 51。
[397]同上註，頁 44。
[398]中華人民共和國國務院新聞辦公室,〈2010 年中國的國防〉白皮書,《中華人民共和國國防部》，< http://www.mod.gov.cn/reports/201101/bpsz/2011-03/31/content_4235224.htm>(2013 年 12 月 8 日)。
[399]同註 387，頁 44。
[400]中華人民共和國國務院新聞辦公室,《2010 年中國的國防》白皮書,《中華人民共和國國防部》，< http://www.mod.gov.cn/reports/201101/bpsz/2011-03/31/content_4235224.htm>2013 年 12 月 8 日
[401]曹正榮、吳潤波、孫建軍，《信息化聯合作戰》，北京:解放軍出版社，2006 年，頁 47。
[402]張蜀平、禚法寶、王祖文，《直面信息化戰爭》，北京:國防工業出版社，2007 年，頁 342。

2. 科技研發

2003 年，任職於美國國務卿辦公室計畫處學者費根保(Evan A. Feigenbaum)指出，中共 863 計畫其目的在縮短中國科技和世界先進技術的差距，在於發展 20 世紀後期和 21 世紀期的高科技產業，及研究尖端技術領域，另外 863 計畫被視為中國的戰略性目標，其計畫勢必會影響長期產業競爭力與軍事力量。[403]中共為落實國家中長期科學和技術發展，提出〈國家中長期科學和技術發展規劃綱要(2006-2020 年)〉，以加強國家戰略需求的基礎研究，並確立國家重點基礎研究發展計畫(973 計畫)專案。此外，在資訊、電子領域，以寬頻光纖、無線電信息網路中的光子集成與微納入電集成，瞄準智慧資訊處理和下一代網路等方面基礎研究。[404]綜合上述，參考中共《中國主要科技指標數據庫》網站之科技計劃中央 2011-2012 財政撥款綜合情況，如表-2[405]，中共在 2013 年投入網路戰科技研發預算約為 95,15 億人民幣。

表 4-2. 中共科技計劃中央財政撥款綜合情況(2011-2012)統計表

指標名稱	單位	2011	2012
按計劃類別分（2011-）			
國家重大科技專項	億元	240	
863 計畫	億元	51.15	55.15
國家科技攻關/支撐計畫	億元	55	64.26
基礎研究計畫	億元		
國家自然科學基金	億元	140.43	170
國家重點基礎研究發展規劃項目(973)計畫	億元	30.92	26.78
國家重大科學研究計畫	億元	14.08	13.22
際科技合作重點專項	億元	12.5	7
重大科技創新基地建設	億元		
國家重點實驗室建設專案計畫	億元	29.61	33.78
國家科技基礎條件平臺建設專項	億元	2.46	2.65
國家工程技術研究中心計畫	億元	1.95	1.05
政策引導類計畫及專項計畫	億元		
星火計劃	億元	3	2
農業科技成果轉化資金	億元	5	5
科技富民強縣專項行動計畫	億元	4	
火炬計畫	億元	3.2	2.2
科技型中小企業技術創新基金	億元	46.4	51.14
國家重點新產品計畫	億元	2.99	2

[403]國防部史政編譯局譯，費根保 (Evan A. Feigenbaum)，《中共科技先驅:從核子時代到資訊時代的國家安全與戰略競爭》(China’s Techno-warriors National Security and Strategic Competition from the Nuclear to the Information age)，台北:國防部史政編譯局，2006 年，頁 188。
[404]唐仁俊，〈中共信息戰之發展與限制〉，《空軍學術雙月刊》，第 619 期，2010 年 10 月，頁 34。
[405]〈科技計畫中央財政撥款綜合情況〉，《中國主要科技指標數據庫》，<http://www.sts.org.cn/kjnew/maintitle/MainMod.asp?Mainq=2&Subq=1>(2014 年 2 月 10 日)

國家軟科學研究計畫	億元	0.35	
科研院所技術開發研究專項	億元	2.5	3
科技基礎性工作專項	億元	1.84	2.25
國家磁約束核聚變能發展研究專項	億元	4.5	
國家重大科學儀器設備專項	億元	8	

資料來源:〈科技計劃中央财政撥款综合情况〉,《中國主要科技指標數據庫》,<http://www.sts.org.cn/kjnew/maintitle/MainMod.asp?Mainq=2&Subq=1>。

整體而言，中共 2013 年投資網路戰費用共計為 1920.35 億人民幣(網軍人員維持費以推算 960.22 億人民幣億人民幣，中共投資網路戰武器費用為 960.13 億人民幣，得算中共投入網路戰科技研發預算為 95,15 億人民幣)。2012 年 8 月美國學者 Teri Takai 指出，美國防部因應當前資訊技術環境龐大且複雜，2013 年會計年度預算需求約 370 億元美元，約為 2290.3 億人民幣。[406]

必須注意的是，中共為因應國防任務需求，其國防科研、武器銷售收益、武器採購支出、國防工業對外營收及武警部隊經費(編列於公共安全預算)等均未列入國防預算中，研判仍有龐大經費隱藏於非軍事項下，其實際國防軍費，應為公布金額之 2-3 倍左右。[407]以 2 倍換算後，判其網路戰費用約為 3840 億人民幣(約為中共 2013 年國防預算三分一)。總之，中共近年來不斷深化改革，將軍費集中投資在不對稱戰爭、電磁脈衝武器、網路戰，以及核武研發，進而建構以中國大陸為核心的兩邊或多邊的合作架構。[408]

[406]李泇錡譯，Teri Takai，〈更靈活的國防資訊能力〉(Creating a More Agile Defense Department info-Tech Enterprise) ，《國防譯粹》，第 39 卷，第 8 期，2012 年 8 月，頁 36。
[407]國防部，《中華民國 102 年國防報告書》，台北:五南文化出版，2013 年，頁 44-5。
[408]洪健元，〈軍費投注不對稱戰爭、電磁武器、網路戰〉，《青年日報》，2014 年 3 月 21 日，版 5。

第三節　中共網路戰之戰力評估

一、中共網路戰能力

(一)攻擊能力

1.駭客能力

中共學者劉偉表示，在網路戰中，以駭客攻擊、病毒攻擊最為危險。隨著駭客的攻擊手段不斷翻新，使駭客程序被植入電腦系統不易察覺，一旦電腦被駭客程序入侵，使攻擊行動變的很容易，在未來作戰中，駭客將與導彈、飛機和士兵一樣成為軍隊的重要作戰力量;另外病毒攻擊對網路安全威脅很大，在軍事領域，電腦病毒是一把殺人不見血的軟刀子，雖不傷害有生有力量，但却可以喪失作戰能力，在未來的戰爭中成為重要的戰場殺手。[409]

根據美國學者蘭柏司(Benjamin S.Lambeth)的研究，中共網路戰攻擊的能力已有長足進步，且有足夠證據顯示，中共早已對美國非保密資料傳輸遂行敵對活動。[410]2012 年 7 月，美國另一位學者指出，中共駭客發起攻擊手段，首先利用社交媒體網站來蒐集個人的資料，有系統、有方法的長期追縱攻擊對象，第二步利用「網路釣魚式攻擊郵件」，對看似朋友或生意夥伴的郵件進行網路滲透，最後偽造網站的附件或連結一旦被開啟，將由駭客接管並探尋其網路弱點，這意謂著接管電郵帳戶，俾利產生更令人信賴的偽造電郵。[411]

2012 年美國確認全球網路駭客 621 起攻擊事件中，30%來自中國和 28%來自羅馬尼亞及 18%來自美國，且中國駭客多半由政府操控，目的是竊取資料。其網路間活動將影響美國成本約占國內生產總值 0.1%至 0.5%,或約 250 億至 1250 億美元。[412]此外，據美國網路服務供應商 Akamai 公布 2013 年〈第四季的全球網路狀態報告〉，全球網路攻擊流量最高的來源國家，中國以 43%位居第一。[413]及美國威訊通訊（Verizon Communications）發佈年度資料外洩調查報告指出，2013 年企業資料外洩的三大主因，分別為網路應用攻擊、網路間諜，及 POS 入侵造成。該報導亦指出，在網路間諜事件中，來自外部的網路間諜事件有 87%來自政府相關的單位。若分析網路間諜的來源地區，則有 49%來自東亞，東歐的 21%次之。而中國與北韓則為東亞的代表。[414]

事實上，自 2013 年美國總統歐巴馬與中共習近平在歐習高峰會上，公開提出美國遭到來自中共的網路攻擊後，中共對美國的網攻則有增無減，許多網攻是由中共軍方網攻單位國有企業發動的。美國國防情報局前網路戰專長蘿拉加蘭特

[409]劉偉，《信息化戰爭作戰指揮研究》，北京:國防大學出版社，2009 年，頁 82-83。
[410]李永悌，Benjamin S.Lambeth，〈空權、太空權與網路權〉(Airpower、Spacepower,and cyberpower)，《國防譯粹》，第 38 卷，第 4 期，2011 年 4 月，頁 26。
[411]高一中譯，Stew Magnuson，〈阻絕中共駭客狂襲〉(Stopping the Chinese Hacking Onslaught)，《國防譯粹》，第 40 卷第 2 期，2013 年 2 月，頁 75。
[412]盧永山，〈去年駭客網攻三成中國幹的〉，《自由時報》，2013 年 4 月 25 日， 版 5。
[413]陳曉莉，全球網路狀態報告：台灣是第五大攻擊來源，尖峰網速排名第六〉，《iThome》，http://www.ithome.com.tw/news/87119
[414]林妍溱，〈網路應用、間諜，POS 攻擊為去年資料外洩三大主因〉，《ithome》，http://www.ithome.com.tw/news/87039(2014 年 3 月 10 日)

(Laura Galante)表示，對中共而言，網攻不是軍事武器，而是一種經濟武器。[415]

此外，美司法部長霍德(Eric Holder)於 2014 年 5 月 19 日主持記者會表示，美國遭中共網路攻擊受害者都是著名品牌，包括西屋(Westing house)電力公司、美國鋁業公司(Aloca World Alumina)、美國鋼鐵公司(U.S. Steel Corp.)等。霍德並表示，中共竊密範圍很廣，而且項目敏感，歐巴馬政府絕不容許任何外國在自由市場中以非法手段破壞公平競爭。[416]從這些事實證明，中共正積極運用網路戰以削弱美國在經濟上的實力。

2013 年 5 月 28 日美國《華盛頓郵報》網站報導指出，美國多項重大武器系統設計遭中國大陸駭客竊取，包含項目:高級愛國者彈導系統、陸軍戰區高空區域的防禦系統、海軍「神盾」彈道導彈防禦系統、海軍新型瀕海戰鬥艦、「F/A-18」戰機、黑鷹直升機及「F-35」戰機等。這些資訊將加速共軍武器系統研發，若兩軍武裝衝突時，據此破壞美方通信及數據網。[417]根據俄羅斯《Russian Today, RT》網站報導，2014 年 3 月 1 日中共 J-20 隱形戰鬥機試成功飛設，其設計是由總部設在成都的中國「技術偵察局」所提供「中共航空工業股份有限公司」中航工業）的一間附屬公司所設計。此外，並引用美國眾議員邁克·羅傑斯，董事長眾議院情報委員會表示，這是一個嚴重的問題，我們必須花費更多甚至高達數十億美元的額外確保我們保持領先我們的敵人與技術。[418]

[415]田思怡，〈美向陸簡報網軍數 盼投桃報李〉，《聯合報》，2014 年 4 月 8 日， 版 12。
[416]劉屏、朱建陵，〈美政府告解放軍 5 軍官〉，《中國時報》，2014 年 5 月 20 日， 版 1。
[417]中印邊界爭議及戰略競合面面觀，中共研究，2013 年、6 月，第 47 卷第六期，頁 164。
[418]〈New Chinese stealth jet built with stolen F-35 component designs〉，《RT》，< http://rt.com/news/chinese-jet-cyber-espionage-stolen-718/>(2014 年 3 月 10 日)

2. 病毒能力

根據林宗達的研究，中共對網路作戰之戰法相當注意，並已經研發出 250 種以上的木馬程式，其中即涵蓋最新研發的「智慧型木馬」(Intelligent Trojans)和「真空木馬」(Vacuum Trojans)。這些木馬程式其病毒利用各種不同途徑植入，並且攻擊關鍵性的電腦，而此種電腦病毒很難破解。例如，真空木馬程式可以在隨身碟插入 USB 槽時，自動從隨身碟存取資訊(我國漢光演習 18 號軍事機密外洩，據研判就是這種電腦網路作戰手段所致)。而現今中共網軍網路戰手段是在目標網站植入更難測察的假資料或者是部分假資料。[419]

中國學者東鳥表示，世界主要國家的網路攻防能力，以美國、俄羅斯及中國佔據了世界網路戰力的三甲，俄羅斯的威脅在於數十年的經驗，而中國則是具有巨大的人力資源，並表示中國有能力入侵美國的電力系統，將全美的電力中斷一周左右。[420]隔年，並引用美國聯邦調查局評估透露，中共在網路戰場上的技術，足以對美國經濟、電信、電網和軍事準備造成實質性破壞，一次大規模網路攻可能達到「大規模殺傷性武器」的破壞等級。[421]

美國研究中共學者費學禮透露，中共已經發展出「高級數據武器」(advanced date weapon)，並有能力加以使用。這此武器包括「自我漸變」(self-morphing)惡意程式碼的應用、電子電路摧毀能力、惡意程式碼的自我加密和自我解密、無線網路的外部破壞能力、對通用商業軟體中未經報導的弱點加以利用。[422]根據我國國防部對中共網路軍事能力的評估，中共自 2010 年起進行新款間諜軟體研改作業，於網際網路空間伺機竊密，其軟體功能朝「自動化」作業模式發展，具變更資料加密模組、隱匿傳輸通道、反制網路安全人員追縱等能量。[423]

2012 年 10 月 8 日，美國眾議院情報委員會一份調查報告指出，全球第二大電信設備供應商的中共「華為技術有限公司」及「中興通訊股份有限公司」(ZTE Corp)所製造通訊系統或零組件可能植入惡意軟體、硬體，可在發生危機或戰爭時讓美國重要的國安系統關閉或功能受損，對美國的國家安全構成威脅，並呼籲美國政府禁止華為和中興併購、收購美國相關企業，此外，該報告並指出華為提供特別的網路服務給中共網軍使用。[424]例如俄羅斯關人員在中國出口的家電，包括熱水壺、熨斗、手機與行車紀錄器中發現藏有微型竊聽晶片，通電時藉由未加密無線網路 WiFi 連結兩百公尺的電腦，將在俄國蒐集的資料傳回中國伺服器。[425]

據報導，全球擁有兩億用戶的微網誌推特(Twiter)，約有 25 萬用戶的密碼其他資料遭竊。另紐約時報、華盛頓郵報遭網路攻擊，均為中共網軍所為，其目

[419]林宗達，〈中共信息戰之「網軍」作戰初探〉，《展望與探索》，第 5 卷，第 9 期，2007 年 9 月，頁 79。

[420]東鳥，《網路戰爭:互聯網改變世界簡史》，北京:九洲出版社，2009 年，頁 161。

[421]東鳥，《中國輸不起的網路戰爭》，北京:中南出版傳媒集團，2010 年，頁 93

[422]國防部史政編譯局譯，費學禮 (Richard D. Fisher Jr.)，《中共軍事發展-區域與全球勢力佈局》(China's Military Modernization-Building for Regional and Global Reach)，台北:國防部史政編譯局，2011 年，頁 200。

[423]國防部，《中華民國 102 年國防報告書》，台北:五南文化出版，2013 年，頁 54。

[424]編譯組/綜合外電報導，〈美國會報告指空 2 陸企威脅國安〉，《自由時報》，2012 年 10 月 9 日，版 20。

[425]唐立群，〈俄海關截獲中國製熨斗、電熱壺藏間諜晶片〉，《自由時報》，2013 年 11 月 1 日，版 20。

的為監控兩報如何報導中國當局認為重要的新聞事件，華盛頓郵報員工指出，華郵編輯部電腦網路 2012 年遭中國網軍入侵，花了一年才擺脫中國網軍植入的惡意軟體。[426]2013 年月 9 月 9 日，美國學者傑斯佩(Scott Jasper)表示，96%的國家和工業間諜都可歸咎於中共。還有一項稍早的報導指出，2011 年 2 月，名為「夜龍」(Night Dragon)的網路入侵者，從 2009 年 11 月就開始對石油、能源和石化工業及在希臘、哈薩克、臺灣和美國的公司主管採取行動，是由位於中共山東省的資訊寄存服務(hosting service)及北京上班日期間從該區 IP 位址發出的「資料暗渡」(date infiltration)所下的指令，中共網路戰攻擊成功統計表，如表 4-3。[427]

據報導，澳洲大型企業和多數資深政治人物也遭中共網路病毒攻擊，甚至連澳洲安全情報組織(A ustralian S ecurity I ntelligence Or ganization,ASIO)位於坎培拉的高科技新總部也法無例外。消息更指出，澳洲安全情報組織截至 103 年 4 月 22 日還無法正式啟用新總部。[428]澳洲政府情報局，據瞭解已做出明確的結論，認為中共間諜應為入侵國會網路負責，並已告知政府高層入侵者身分。除此之外，澳洲總理亞伯特(Tony Abbott)在 2013 年上任後，即以網路安全顧慮為由，宣布繼續禁止中國華為科技公司參與澳洲全國寬頻網路(NBN)工程競標。[429]

表 4-3:中共網路戰攻擊成功統計表

區分	手法
1995 年 5 月	中共位於前南斯拉夫貝爾格勒的大使館遭到北約轟炸以後，中共駭客攻擊美國政治、軍事和外交網站，並且同時動員數以千計的網友，以傳送電子郵件和病毒的方式進行的信息網路戰，造成了許多伺服器當機，癱瘓相關可觀的網站，即有許多來自中共民兵網軍的傑作。
2001 年	中共最大的駭客組織「紅色聯盟」號召大陸網民對美國各大網站進行網路攻擊。這波網路攻擊，美國高達 800 個政府及企業網站網頁更換為五星旗，或殉職飛行員王偉的遺照。
2003 年	中共也控進入美軍位於亞伯丁(Aberdeen)的基地，並竊取有關美軍未來戰鬥系統的資料.
2003 年	中共對美國密西根、俄亥俄、紐約等城市發動網路攻擊，造成許多地區停電，影響範圍計達 9,300 平方英哩，估計 5 千萬人受影響。
2005 年	美國聯邦調查局首次進行有關的電腦犯罪調查，結果發現美國工商業遭受的電腦攻擊，有 25%來自中國大陸。
2005 年	以廣東為基地的中共駭客，對個別人員而設計的電子郵件寄送給英國

[426]〈Twiiter 也遇駭 25 萬用戶資料遭竊〉,《中國時報》, 2013 年 2 月 3 日，版 11。
[427]童光復譯，Scott Jasper，〈美國與中共的網路戰爭〉(Are US and Chinese Cyber Intrusions So Different)，《國防譯粹》，第 40 卷第 12 期，2013 年 12 月，頁 79。
[428]俞智敏，〈監控九萬留澳生 中國廣布情報網〉,《自由時報》, 2014 年 4 月 22 日，版 13。
[429]俞智敏、林翠儀，〈澳洲 2011 年遇駭 共諜恐已竊國會機密〉,《自由時報》, 2014 年 4 月 29 日，版 12。

	國國會議員，意圖植入碟軟體，俾搜尋資訊並將其傳送送回中國大陸。
2007 年	美國防部五角大廈 6 月份曾遭中共網路黑客嚴重攻擊，致使國防部長蓋茲辦公室的部分電腦系統關閉逾一週。
2007 年	紐西蘭安全調查局主管 Truker 對外宣布，政府的電腦系統被中共間諜黑客襲擊，並被安裝了難以檢測的木馬程序，導致信息外洩。
2007 年	美國商業部長(Commerce Secretary)古提拉茲[430](Carlos Gutierrez)及美貿易代表團訪問北京期間，其他團員的電腦中發現被植入間諜程式，其作用為秘密移除個人電腦及其他電子裝備資料
2008 年	美國聯邦調查局透露，美國政府和軍方的保密電腦廣泛使用的不受管制或由中共仿製的「思科公司」(Cisco)電腦路由器，可能已經製造了大量無法察覺的後門，讓共軍的駭客有機可乘。
2009 年	印度總理辦公室 30 多名政要的電腦在 2009 年 12 月遭到來自中共駭客入侵，並有部份資料洩漏。
2011 年	中共竊取三菱重工及國會眾參兩院資訊為目的網路攻擊，2012 年日本將釣魚台國有化後，一些網站先後受到駭客攻擊癱瘓。
2012 年	2012 年美國發生 189 起對能源部門、自來水公司、化學工廠和核能公司等基礎設施的網路攻擊事件，中國大陸、俄羅斯和伊朗被美國視為發動者
2013 年	德國一家巴士製造公司和美國一家家具製造公司的專利設計遭竊，不久後中共的公司便以較低價格販售其仿製品，導致這兩家公司倒閉，另有的公司智慧財產權遭竊仍不自知。

作者整理

資料來源: 東鳥,《中國輸不起的網路戰爭》,北京:中南出版傳媒集團,2010 年賴昭穎，〈2015 年前美將組 40 支網路部隊〉,《聯合報》,2013 年 3 月 25 日，版 8。高一中譯，Stew Magnuson,〈阻絕中共駭客狂襲〉(Stopping the Chinese Hacking Onslaught)，《國防譯粹》,第 40 卷第 2 期,2013 年 2 月，頁 75。柴惠珍譯,Shame Harris 著,〈中共網軍〉,《陸軍軍事譯粹選輯》,第十八輯，2008 年 5 月，頁 726-32。陳祐欣，〈現代版木馬屠城 中共以網向全球開戰》,《看雜誌》http://www.watchinese.com/%E7%9C%8B%E4%B8%AD%E5%9C%8B/2008/280(2014 年 3 月 29 日);毛峰,〈日本創建網軍聯美反制中國〉,《亞洲週刊》,第 27 卷第 21 期，2013 年，6 月，頁 36-37。

[430]古提拉茲當時在大陸帶領的商貿聯委員(Joint Commission on Commerce and Trade)，是包含美國貿易代表的高階代表團，與中共官員會談智慧財產權、市場通路及消費品安全等議題。

(二)防禦能力

中共網路安全機構人士認為，在面對世界各國駭客網路攻擊，中共普通民用網路會基本癱瘓，而關係到國計民生的行業，由於大多與公共網際網路物理隔離，情況會比較好。[431]2012 年 6 月 7 日，在北大西洋公約組織網路防禦中心 IT 專家第四屆年度會議時，其中心負責人譚姆表示，針對近期網路病毒 Stuxnet 和火焰病毒，對負責保護重要基礎設施的所有專家來說是極大的考驗，他並指出，中共和俄羅斯近年來透過新的 IT 設施，顯著提昇網路防禦能力。[432]

中共國家計算機網路應急技術處理協調中心(CNCERT/CC)運行部主任王明華〈境外對華網路攻擊報告〉曾表示，截至 2012 年 12 月 31 日止，中共國家計算機網路應急技術處理協調中心(CNCERT/CC)共監測到涉及 90 個部門的 142 個網站被”匿名者”組織篡改，其織的活動很有周期性，每週都要攻擊兩三個網站，中共境內大量網站的漏洞，可能採用了預先植入後門等手段，控制了一些網站服務器。至 2012 年 3 月到 12 月底，中共國家境內超過 1250 個政府網站被”阿爾及利亞 Barbaros-DZ”篡改，2012 年中國境內至少有 4.1 萬餘台主機感染具 APT 特徵的木馬程式，涉及多個政府機構，重要資訊系統部門及高新技術企，2012 年，中國境內政府網站被篡改數量為 1802 個，較 2011 年的 1484 個增長 21.4%，省部級對網路安全的認識比較到位，但地市級及以下網路安全防護較不理想，因地方政府只側重網站建立，對維護重視程度遠遠不夠。[433]

據報導，中共網路於 2014 年 1 月 21 日長達一個半小時嚴重癱瘓，大約讓三分之二的使用者無法連線至變數名稱「.com」「.net」「.org」等功能網站。據中共「國家互聯網應急中心」判斷，係因遭網路攻擊所引起，導致大陸互聯網用戶通過國際頂級功能變數名稱服務解析時出現異常。後來經查證，乃係美國研發自由門(Freegate)翻譯軟體公司所為。中共國家創新與發展戰略研究會「網路空間戰略研究中心」主任秦安表示，美國隨時可從國際網路協定清除「.cn」，把中國打回「石器時代」。美國曾於戰爭時清除伊拉克、利比亞國家根功能變數名稱，使兩國家全部網站從國際互聯網消失，中國的能源、電力網路很難與國際網路做出完全隔離。[434]

2010 年 4 月，中國全國人大委會規定互聯網及其化公共資訊網路營運商和服務商，應當配合公安機關、國家安全機關對密案件進行調查。2009 年 7 月新疆維吾爾人爆發種族衝突，中共立即關閉 Twitter 和 Facebook，全面封銷網路，減少手機通話，以抑制事件報導。[435]據報導，2012 年 11 月 9 日，Google Inc.在中國的網路搜尋、電子郵件及地圖等服務無法使用，很可能是中國政府在中國第十八次全國代表大會期間，蓄意封鎖 Google 服務，讓中國網友在這段敏感時刻，無法透過網路搜尋、傳遞或發布任何不利於中國政府的任何訊息。[436]

2014 年 5 月 16 日中共〈中央機關採購中心發佈訊息〉報導，為避免資訊外

[431]東鳥，《網路戰爭:互聯網改變世界簡史》，北京:九洲出版社，2009 年，頁 161。
[432]林秉學，〈專家警告 智慧網路武器將興起〉，《青年日報》，2012 年 6 月 9 日， 版 5。
[433]昊銘，〈境外對華網路攻擊報告〉，《瞭望東方周刊》，第 30 期，2013 年 8 月 8 日，頁 15-16。
[434]王銘義，〈美隨時可以把陸打回石器時代〉，《中國時報》，2014 年 1 月 23 日， 版 13。
[435]盧永山，〈商業秘密暫行規定 中國紅線包山包海〉，《自由時報》，2010 年 4 月 28 日， 版 5。
[436]〈中國政府疑似於十八大期間封鎖境內 Google 服務〉，《行政院國家資通安全會報技術服務中心》http://www.icst.org.tw/NewsRSSDetail.aspx?seq=14276 (2014 年 3 月 21 日)

洩，中共規定境內所有資訊產品不得安裝美國 windows 8 作業系統。[437]另據一項報導揭露，中共自 2014 年 5 月 2 日起，將加強網路安全審查，舉凡涉及國安的資訊產品，皆須通過網路安全審查;此外，中共《外商投資項目核准項目和備案管理辦法》亦強調，外商投資項目管理將由全項核准，改變為有限核准和普遍備案相結合的管理體式，確維護國家安全。[438]根據最新消息證實，中共近期已勸導銀行棄用美國 IBM 高階伺服器，改以國產品牌替代，此舉將使美國微軟等公司，損失百億人民幣。[439]

另外，根據國防大學教官張玲玲的研究，中共在管轄網際網路內部建立多套網路審查系統，公安部門、國安部門及新聞宣傳等部門聯合承擔相關行政權責，並輔以各式管制軟體如防火長城等技術手段，對網路活動進行機密監控，封銷著可能影響其國家安全的資訊傳播，同時也對政治內容進行監視和過濾，涉及敏感性的政治事件和人物都被為封鎖的對象。另為有效控制網路所引起的「反動思想」，透過立法使其手段合法化，所以是少數以獨立的法律，來控制網上的言論的政權之一。[440]也有媒體指出，中國大陸仍是「全球最大的網路監獄」，中共、俄羅斯等網路公敵政府，已開始向外國輸出這類大規模監控技術。例如中共開始為伊朗架設一套「清真互聯網」(Halal Internet)，企圖建構一個所有網路隔絕，完全在德黑蘭政府掌握下的國家網路系統。中共也非洲國家尚比亞建立網路監控系統，阻擋批評政府的網站。[441]中共網路遭癱瘓事故統計，如表 4-4。

表 4-4:中共網路遭癱瘓事故統計表

時間	網路癱瘓事故	主因
2006 年 12 月 27 日	台灣恆春地震震斷海底光纖，致使中共至台灣、美國、歐洲等網路中斷。	海底光纖損毀
2007 年 5 月 1 日	中共網路游戲公司，遭到長達 10 天的網路攻擊，伺服器癱瘓，網路游戲被迫停止損失 3460 萬人民幣。	服務器全面癱瘓
2009 年 5 月 19 日	暴風網站的域名解析系統受到網路攻擊出現故障，伺服器收到大量異常請求引發壅塞	DNS 遭攻擊
2010 年 1 月 12 日	伊朗駭客入侵更改中共百度網站(域名 baidu.com)傳輸協議，致使中共白度網站無法登入長達 8 小時	DNS 遭攻擊
2011 年 2 月 21 日	中國電信寬頻維修至大規模網路故障，北京、上海、湖南、河南、廣東、四川、甘肅、內蒙斷網 3 小時	寬頻維修
2010 年 1 月 12 日	DNS 域名根伺服器故障，網路攻擊導致大陸網友無法正常拜訪網址以「.com」「.net」等結尾的網站	DNS 遭攻擊
2012 年 11 月 9 日	中國部份用戶受不明原因干擾而中斷，據報導指出很可能是中國政府在第十八次全國代表大會期間，蓄意封鎖 Google 服務，讓中國網友無法透過網路搜尋、傳遞或發布任何不利於中國政府的任何訊息。	DNS 遭攻擊
2013 年 7 月 7 日	上海聯通 DNS 設備發生故障，導致 2G、3G 手機用戶無線上網。	DNS 遭攻擊

[437]管淑平，〈美起訴解放軍 中國暫停網路合作〉，《自由時報》，2014 年 5 月 21 日， 版 10。
[438]陳柏廷，〈封殺美產品 陸際出網安審查〉，《中國時報》，2014 年 5 月 23 日， 版 22。
[439]陳柏廷，〈陸銀或棄 IBM 伺服器 中美諜戰升級〉，《中國時報》，2014 年 5 月 28 日， 版 13。
[440]張玲玲，〈中共管控網際網路 對內維穩對外情蒐〉，《青年日報》，2014 年 3 月 9 日， 版 7。
[441]胡蔥寧，〈無疆界記者:美英網路監控 不輸中俄〉，《自由時報》，2014 年 3 月 13 日， 版 10。

2014 年 1 月 21 日	中共網際網路長達一個半小時嚴重癱瘓，約使用者達三分之二無法連線至變數名稱「.com」「.net」「.org」等功能網站	DNS 遭攻擊

作者整理

資料來源:王銘義，〈美隨時可以把陸打回石器時代〉，《中國時報》，2014 年 1 月 23 日，版 13。;齊先予，〈大陸網癱「秦始皇」賊喊捉賊〉，《新紀元》，第 363 期，2014 年 1 月 30 日，頁 46-48。〈中國政府疑似於十八大期間封鎖境內 Google 服務〉，《行政院國家資通安全會報技術服務中心》http://www.icst.org.tw/NewsRSSDetail.aspx?seq=14276（2014 年 3 月 21 日）

二、中共網路戰弱點

網路涉及國家安全和國計民生，在中共經濟社會發展方面發揮著重要作用。截至 2012 年年底，中共的互聯網普及率達到 42.1%，網民規模達到 5.64 億。同時，中共也是世界上駭客攻擊的主要受害國。國家互聯網應急中心數據顯示，2012 年，中共境內 1400 萬餘台主機遭受攻擊 3.8 萬個網站遭受遠程控制。[442]

(一)人才限制

中共資訊戰專長沈偉光等人均強調，資訊是人才是決定一個國家信息的關鍵因素之一，教育體制不完善(3.6%的人口接受過大學教育)，在資訊人才培養方面較為落後，同時，有些先進發達國家通過優惠的移民政策與高薪聘請等方式，挖走大量的高素質的資訊人才，使得中共的資訊人材嚴重不足。另外，中共網路防禦側重於民用系統，一般性的網路犯罪活動，及大規模的網路作戰入侵難以抵抗，缺少網路安全保密管理系統的規劃設計人才、應用軟件的研發開發人才、終端用戶的操作使用人才、硬件設備的維修保養人才和安全性能的監測評估人才[443]

中共民眾上網普及率仍然很低(中網網民總數達 2.98 億，普及率 22.6%)，遠遠落後美國、日本。[444]與西方先進國家相比，目前中共仍是一個發展中國家，12 億人口，文盲、半文盲率為 15.8%，佔全人口總數 1/6 強，比 150 年前的美國 22%文盲率只低不到 7 個百分點。因此，人才的培養的客觀結構上，面臨一定的限制。此外，中共在軍事教育經費投資方面，亦明顯不足，目前，中共軍事院校人均教育經費是美國西點軍校的 0.3%，是日本軍校的 1.4%。[445]美國學者毛文杰披露，中共改進「人力資本」後，將可獲得更多高科技的專業人才，參與各種重大的軍事現代化戰略工作，但亦可能投入高薪的非軍事工作，使得召募與留住等科技專才官兵更加困難。[446]

---

[442]戚魯江著，〈美國國會網路安全立法探析〉，《中國人大》，第 340 期，2013 年 8 月，頁 53。

[443]沈偉光主編，《中國信息戰》，北京:新華出版社，2005 年，頁 97;楊世松，《軍事信息能力論論》，北京:軍事科學出版社，2007 年，頁 20;約翰(Juhn chang)，〈中國信息安全發展現況〉，《漢和防衛》，2013 年 9 月，頁 44。

[444]東鳥，《網路戰爭:互聯網改變世界簡史》，北京:九洲出版社，2009 年，頁 308。

[445]唐仁俊，〈中共信息戰之發展與限制〉，《空軍學術雙月刊》，第 619 期，2010 年 10 月，頁 39。

[446]國防部史政編譯局譯，毛文杰(James C.Mulvenon)、譚睦瑞(Murray Scot Tanner)、蔡斯(Michael S. Chase)、傅里林格(David Frelinger)、龔培德(David C.Gompert)、李比奇(Martin C.Libicki)、包克文(Kevin L. Pollpeter)，《中共對美國軍事變革之反應》(Chinese Responses to U.S.Military Transformation and Implications for the Department of Defense)，台北:國防部史政編譯局，2010 年，頁 27。

(二)基礎設施不足

中共在資訊與網路技術方面是一個落後的國家，主要在於技術不足，其水準仍為發展中國家，整體上仍處於技術落後、科學落後的狀態。其根本問題在於缺乏大量的核心技術，電腦硬體、網路設備主要依賴進口，另外操作系統、晶片和大型應用軟體則受制於人，這類設備和平台難免潛藏各種各式的後門和安全漏洞，因此，存有不可預知的安全隱患。此外，在能源、交通、金融等國家要害或敏感部門，大量使用了國外的軟、硬體產品，造成了資訊單向的不利態勢。[447]

中共信息資源建設薄弱，主要是因為是「多頭管理、職能交叉」各自為政，缺乏統一有效管理。如中共數據庫 1000 多個，是世界數據庫的 1/10，但中國數據庫容量僅占世界總量的 1/100，其產生的社會價值占世界信息資源的 1/1000。[448](如 2009 年，中共學者東鳥指出，中國網站登記備案、IP 地址分配、域名申請等基礎管理分散、不協調，加上數量巨大，審核困難，一些網路接入服務商只求經濟利益，致使許多網站沒有案審批，一些網站為規避管理，採取網站 IP 地址與備案所在地分離的辦法，使無主管部門、無主辦單位、服務器地托管的非法網站不斷出現，給查處工作帶來極大困難。[449]

中共學者周宏仁等人指出，中國的電腦使用數 2000 年達到 2200 萬台;2009 年達到 2.2 億台，每百人擁有量為 16.7%，其增長的速度主要原因為，電腦大量進入城市及農村家庭，而中國的伺務器擁有量約 1260 萬台，相對於增長率則較慢，說明中國資訊化應用系統開發的規模和速度還不規理想，大型或超大型資訊系統的建設有極大的發展空間。[450]此外，周宏仁等人亦表示，在整體經濟發展實力、研究開發與經費投入以及電腦人機比與發達國家差距仍然很大，在 2007 年，中國基礎設施指數相當於該類指數最高瑞典的 25%，[451]

中共在光纖網路建設水準與先進國家相比仍存在較大的差距，網路基礎存在光纖寬頻網路覆蓋率較低，在 2011 年 6 月，中共網路寬帶的家庭覆蓋率僅為 31%，世界發達國家普遍在 50%，排名第一的韓國更高達 95%。[452]連網速率太慢是中共光纖網路建設的另一弱點。據美國 CDN 服務商 Akamai 發佈的 2012 年第二季報告顯示，全球平均連網速度呈現上升趨勢，其中韓國仍以 14.2Mbps 的平均連網速度排名全球第一，而國中共平均連網速度僅 1.5Mbps 排名全球第 69 名。最後，則是中共國內的大多網站與應用程序尚不能支持 IPv6 服務，且上網費率相對較高，在一定程度上限制了光纖網路的普及。據美國 Akamai 統計，2009 年 12 月全球平均住宅 DSL 每兆帶寬價格為 8.8 美元，中國為 13.45 美元，是全球平均

---

[447]沈偉光主編，《中國信息戰》，北京:新華出版社，2005 年，頁 283 頁;潘小剛、周亞明、肖琳子，《中國信息安全報告-預警與風險化解》，北京:紅旗出版社，2009 年，頁 50-51;辛毅，〈電子信息裝備軍民融合式發展的思考〉，《國防》，第 3 期，2013 年，頁 13;鄭文浩、楊雷，〈網路戰比核彈威脅更大〉，《瞭望東方周刊》，第 47 期，2013 年 12 月 12 日，頁 40-43。

[448]楊世松，《軍事信息能力論論》，北京:軍事科學出版社，2007 年，頁 20;白德華，〈習近平領軍 網路安全成國家戰略〉，《中國時報》，2014 年 2 月 28 日， 版 22。

[449]東鳥，《網路戰爭:互聯網改變世界簡史》，北京:九洲出版社，2009 年，頁 340。

[450]周宏仁主編、徐愈副主編，《中國信息化形勢分析與預測》，北京:社會科會文獻出版社，2010 年，頁 13。

[451]同上註，頁 24。

[452]高光耀、鄭從卓，〈我國光網城市建設的主要問題及對策研究〉，《未來與發展》，第 4 期，2013 年，頁 4。

水準的 1.5 倍。[453]綜合上述中共網路戰能力，並參考美國〈美中網路戰略七大高地〉專文及網路戰基本攻、防能力後，其中共網路戰能力評估表如表 4-5。

表 4-5:中共網路戰能力評估分析表

評鑑項目		重大事件	評鑑結果
攻擊能力		代號奧運(Olympic Game)網路攻擊事件，於 2009 年，由美國對伊朗發動震網電腦蠕蟲攻擊，透過干擾轉換器頻率致使伊朗納坦茲的離心機約 1/4(1000 台)受損;據美國威訊(Verizon)電信公司指出，96%國家和工業間諜來自中共	美國勝
防禦能力		美國(空軍科技)網站報導指出，由兩家世界軍火巨擘:泰勒斯(Thales)公司和雷神公司合股建立的(泰勒斯雷神系統公司)(TRS),正在研發簡單又有效的反駭客入侵設備CybAIRRadBox。為傳統的網路安全系統尤其是軍用或民用雷達系統網路,增強多層次的監控能力	美國勝
作業系統	個人電腦	美國 Windows 作業系統佔全球市場第一 92%(約 12.5 億)、蘋果麥金塔(Mac)佔全球市場第一 6%;中共 Linux 佔全球市場約 1%	美國勝
	手機	美國谷哥安卓「Google Android」43%、「諾基亞寶班」(Nokia Sybian)22%、蘋果網際網路作業系統 Apple iOS 18%。微軟公司不到 2%此外，晶片是美國高通的、網絡路由器或交換機是思科的	美國勝
	搜索引擎	美國「谷歌」(google)搜索引擎全球市場 91%，其演算法從召一兆個全球資源定位器的索引中找出最符合使用者需求;而中共百度(Baidu)是中國四億人口唯一的選擇。	美國勝
	通信裝備基礎設施	網際網路的資訊流量都通過美國的通信裝備基礎設施;中共電子資訊裝備的關鍵設備和核心技術還很多受制於國外，如核心 CPU 及系統軟體，如中共的中心銀行及四大國有商業銀行的電腦主機都是 IBM 製造的，此外在通信線路的設計美國一些有代表性的資訊企業均有參與。中國的國際網路幹線的容量僅為 46.3GB/秒，還不到國際最高水準的一半水準	美國勝
	雲端運算	亞馬遜(Amazon)、微軟和谷歌等雲端運算提供者，可讓使用者租用其侑儲存及處理能力的基礎設施	美國勝

[453]同上註，頁 5。

	治理論壇	中共在管轄網際網路內部建立多套網路審查系統，公安部門、國安部門及新聞宣傳等部門聯合承擔相關行政權責，並輔以各式管制軟體如防火長城等技術手段，對網路活動進行機密監控，封銷著可能影響其國家安全的資訊傳播，同時也對政治內	中共勝
	密碼體系	密碼體系的量子計算(quantum computing)研發工作。212 年，谷歌公司和美國太空總署(NASA)聯手買下另一部量子電腦，預估 1 台為 1000 萬美元。[454]該項計畫最常對付中國軍方單位(如解方軍駭客組織 61398 部隊)，也曾成功入侵俄羅斯軍方網路、歐盟貿易機構	美國勝
	網際網路基本路由協定	全球網路域名(DNS)與地址(IP)一直由美國政府(商務部)授權「際網路名稱與號碼分配組織」統一管制及掌握。在特殊情況下美國需要使中共對外網路中斷，只要中斷根服務器，惟 IPV4(40 億)已於 2011 年 2 月 3 日分配完畢。現階段 IPV6 面臨經濟上門檻，許多公司擔心，率先進入這個領域，必會負擔改進安全或設計缺失所需的成本。中共已擬定 IPV6 計畫，大陸地區有超過 4 億名使用者，經濟成長，故有 IPV6、硬體設備的優勢及影響力	概等

作者整理:衡量的基準，為參閱美國〈美中網路戰略七大高地〉專文，及網路戰基本攻、防能力所調製。

資料來源: 〈電波助威 NSA 入侵全球 10 萬電腦〉,《青年日報》,2013 年 12 月 16 日，版 5;〈Twiiter 也遇駭 25 萬用戶資料遭竊〉,《中國時報》,2013 年 2 月 3 日，版 11;王銘義,〈美隨時可以把陸打回石器時代〉,《中國時報》,2014 年 1 月 23 日， 版 13;張玲玲,〈中共管控網際網路 對內維穩對外情蒐〉,《青年日報》,2014 年 3 月 9 日，版 7;〈美 NSA 量子電腦可可全球加密技術〉,《青年日報》,2014 年元月 4 日， 版 5;管淑平,〈無線電波植間碟美滲透 10 萬電腦〉,《自由時報》,2013 年 12 月 16 日，版 9;陳漢強、蘇文德,〈中共信息戰之網路攻擊型態研究〉,《新新季刊》,第四十卷，第二期,2012 年 4 月，頁 236-237;曾復生,〈美中網路戰略七大高地〉,《財團法人國家政策研究基金會》,〈中印邊界爭議及戰略競合面面觀〉,《中共研究》,2013 年 6 月，第 47 卷，第六期，頁 164;王光磊,〈抗駭新時代國防要務〉,《青年日報》,2013 年 2 月 29 日，版 5。高一中譯,Kris E. Barcomb,〈從海權到網權:以史為鑑勾革未來的戰略〉(From Sea Power to Cyber Power: Learning from the Past to Craft a Strategy for the Future),《國防譯粹》,第 41 卷，第 2 期,2014 年 2 月，頁 29-37。

鄭文浩、王玉山,〈院士：我國網絡基本算不設防 成網絡攻擊最大受害國之一〉,《人民網》
http://military.people.com.cn/BIG5/n/2014/0107/c1011-24045169.html（2014年3月23日）

第四節　小結

中共隨著經濟發展發展，投資國防經費更是逐年以二位數字增長。但受限於軍事科技短時間無法追求歐、美軍事強國，網路戰乃成為中共不二選擇。另外，隨著教育普及，中共人民擁有電腦、手機等資訊化設備也隨之增加，中共境內的網路駭客及輿論均造極大的網路安全威脅。中共也因此對網路戰的發展，積極投入研究。中共網路戰戰略構想，依循以往的人海戰術思想，在國防政策是積極防禦指導下，中共網路戰對外的作戰構想就是以優先癱瘓敵政、經、軍(指揮所)、交通(如高鐵、航管)為目的，對內，則是利用網路監控軟體，嚴控各項衝突，以確保國家安全，以達損小、效高的戰爭勝利。

自 2009 年，美國網軍司令部正式對外公佈成立，日、韓、以色列及歐洲軍事強權也相繼成立網軍，網路戰已從防護進化至攻擊。根據各項官方報導指出，中共已成立網軍，其部隊人數從 10 萬至 20 萬不等。中共於 2011 年將總參謀部之通信部更名為信息部，及於 2012 年成立全軍預備役電磁頻譜管理中心均證明，中共已編組網軍。另從國防經費(含科技研究費)研判，中共已對網路戰挹注相關可觀的經費，在發展裝備、培養人才，期能在網路戰奪取制高點。

近年來，中共雖積極投入網路戰，但受限制核心科技現階段仍以美國廠商為主，且網路通訊標準制定、網域、IP 等都由美國律定規則，故中共網路戰攻、防能力，僅能以削弱及竊取為主要手段，其實力應落後歐、美軍事強國。此外，據美國國防部的一份評鑑報告指出，在網路力量美國、俄羅斯以及一些西方國家位居領先，中共次之，而伊朗因最近才開始開發網路戰能力，故排名最後。[455]

[455]paganinip" The cyber capabilities of Iran can hit US," defense, <securityaffairs > http://securityaffairs.co/wordpress/17064/cyber-warfare-2/the-cyber-capabilities-of-iran-can-hit-us.html（2013 年 12 月 8 日)。

第五章　我國因應中共網路戰之策略

2006 年美國提出的《中國軍力報告書》指出，兩岸軍力已經向中共傾斜，其報告一改過去聲稱兩岸軍力「逐漸向」中國失衡觀點，而改稱兩岸軍力已向北京傾斜，同時美方評估，中共軍力已超過攻台所需。此外，面對解放軍要以打贏資訊化條件下的局部戰爭為目標的台灣。[456]2013 年 3 月 29，馬英九總統接受英國金融時報《FINANCIAL TIMES》專訪坦承，中共對我國發動網路攻擊，比未開放大陸政策之前數量還多，並表示，隨著兩岸開放大量旅客來台，其潛在危安風險也自然增加。[457]據移民署統計，自 2006 年大規模遣返 1595 名中國偷渡犯後，隨著馬政府門戶大開，每年遣返人數逐年遞減，並由 2011 年 53 員減至 2012 年 17 名及 2013 年 21 員。截至 2013 年底止，在台中國不明人行，計有 784 名。[458]本章將就中共對我網路戰威脅評估、我國網路戰能力評估，及我國因應中共網路戰之具體作法與建議進行探討。

第一節　中共網路戰對我威脅評估

一、中共對我之企圖

2013 年，我國備役空軍中將李貴發指出，近 20 餘年來，由於中共的改革開放政策奏效，經濟實力大幅躍進，每年投入解放軍的國防預算成二位數成長，小米加步槍和胡志明小徑的游擊戰爭的時代已經成為過去。目前中共已經是世界矚目舉足輕重的大國，整體國家實力已超越日本、俄羅斯。再加上從以色列、俄羅斯、法國等國家獲得現代化先進技術，在太空武力發展、飛彈、航母等先進武器研制，均已有相當成果。[459]李貴發的論點正指出中共對我構成的嚴重威脅。

2014 年 1 月 22 日，中共總書記習近平在「中共中央全面深化改革小組」會議中表示，將分階段落實國安戰略目標:首先於 2013 年至 17 年的 5 年期間，增加國家安全工作的能量，保持經濟中高速增長，創造有利的內、外安全環境，第二階段在 2020 前即為建黨百年，推進國家治理體系和治理能力現代化，全面構成小康社會戰略目標;第三為 2021 至 2049 年，落實國家統一和領土完整。習近平的談話顯示中共不僅把台灣問題視為民族主義問題，也視為國家安全重大問題。畢竟一個分裂的「中國」，將成為中國拓展海疆戰略縱深優勢的障礙，台灣問題不解決，將給中共周邊安全增加新的不確定因素。[460]其實，美國國防部官員石明凱(Mark Stokes)也指出，中華民國仍是中共解放軍政治作戰的目標，因為台灣的民主政府體系是中共獨裁模式的對照，象徵中共政治權威的存在的威脅，在國際場域中，兩岸的政治合法性仍被視為零和遊戲。[461]

2013 年 10 月 14 日，中共〈使命行動 2013B〉指揮所作戰地圖，清楚出現台灣地圖，同時標註了澎湖列嶼的位置，而參演單位正是中共攻台廣州軍區第 42

[456]陳憶綾，《解放軍資訊戰對台軍事安全影響之研究》，政治作戰學校政治研究所碩士論文，2006 年 6 月。頁 58。
[457]彭顯均，〈馬坦承:對中開放 駭台更多〉，《自由時報》，2013 年 4 月 2 日， 版 4。
[458]姜翔、羅添斌，〈治安國安隱憂 784 中國人非法滯台〉，《自由時報》，2014 年 3 月 3， 版 1。
[459]李貴發，〈2023 年東亞軍事情勢分析之二〉，《尖端科技》，第 351 期，2013 年，11 月，頁 16。
[460]曾復生，〈習近平的戰略時間表〉，《中國時報》，2014 年 1 月 25 日， 版 16。
[461]賴昭穎，〈中共政治作戰 台灣是首要目標〉，《聯合報》，2013 年 10 月 23 日， 版 13。

集團軍，可預期未來如果發起解放台灣戰役，第 42 集團軍應該是充任登陸台灣南習翼的主攻部隊，將與第十五空降軍、第一集團軍(北翼主攻)共同擔當殲滅台軍的重要任務。[462]同年 10 月 29 日，我國軍事發言人羅紹和少將證實，10 月上旬中共出動 2 萬多名陸、海、空兵力，進行代號(使命行動 2013B)的跨區機動戰役演習，是以台灣作為假想目標，國防部全程掌握。[463]

國內學者林中斌於《核霸》一書指出，中共若以海、空軍及導彈攻擊等硬殺武器，應可順利占領台灣。惟一切基礎建設均毀於戰火，且耗時費日必然引起國際干預和制裁，到時中共不但得不到經濟利益，還會負擔沈重重建經費而得不到償失。而點穴戰、不對稱戰爭只破壞資訊、網路等電子設備則無此顧慮，並且可以減少對他國干預意願，達到速戰速決之目標。[464]美國智庫蘭德公司表示，資訊戰力可提升中共戰力，使中共有能力干擾美國的指揮部署，如果台海發生衝突，美國出面協防台灣，中共勢必運用其資訊技術，迅速建立有效電腦網路攻擊能力，面對美國的高科技強國對陣時，將發揮不對稱作戰的優勢。蘭德公司因此認為，在當前中共以經濟發展作為國家戰略主軸下，資訊作戰的攻台方式，在各方面的風險成本評估中，實為最經濟又能兼顧戰略效果的戰法。[465]

根據國防部所發表的我國《102 年國防報告書》，中共網路軍事發展及駭客攻能能力已成為當前我國國防安全之威脅。中共網軍持續入侵我相關網站，並透過遠端滲透、病毒(惡意程式)感染、竊取或監控等侵入行動。一旦衝突爆發，將癱瘓我指導、後勤網路，影響國軍資訊系統正常運作並遲滯國軍應變能力。[466]此外，據美國網路安全曼迪亞公司研究分析證明，中共 61398 部隊有 6 部伺服器擁有台灣 IP 位址，並曾利用台灣當做駭客跳板。[467]

事實上，民進黨於 2014 年發表的「二〇二五年中國對台軍事威脅評估」亦明白指出，中共未來對台將以網路戰、導彈、防空及制海等四大面向軍事威脅，中共以網路戰對我數位國土的襲擾，將對台灣社會活動與政府運作形成威脅，可能對我關鍵基礎設施造成實體的破壞，造成生命財產的損失，台灣國防的前線已不再是地理上的外島，而是由各個網路空間組成的「數位國土」，目前我國數位國土每天遭受二十萬次的襲擾，並指出儘管國軍內部網路採取實體隔離的保護措施，專家仍認為國軍的資通系統脆弱性高，在敵方網路攻擊，國軍作戰體系可能會被癱瘓，而且未來 2025 年比 2013 年更為險峻。[468]另外，中共還企圖利用兩岸詐騙集團，吸收在台服役三名軍中同袍，以智慧型手機拍下高階軍官任務職掌及兵力部署，並以新臺幣 50 萬回饋其代價。[469]

---

[462]賴錦宏，〈央視畫面 驚見對台作戰地圖〉，《聯合報》，2013 年 10 月 14 日， 版 13。
[463]蔡和穎，〈共軍演訓動態 國防部全程掌握〉，《中央社新聞網》，。
http://tw.news.yahoo.com/%E5%85%B1%E8%BB%8D%E6%BC%94%E8%A8%93%E5%8B%95%E6%85%8B-%E5%9C%8B%E9%98%B2%E9%83%A8%E5%85%A8%E7%A8%8B%E6%8E%8C%E6%8F%A1-143211709.html (2013年10月20日)
[464]行政院研究發展考核委員會，《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》，台北:五南文化出版，2002 年，頁 504-509。
[465]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 19。
[466]國防部，《中華民國 102 年國防報告書》，台北:五南文化出版，2013 年，頁 59。
[467]〈破天荒 美跨海通緝解放軍網諜〉，《蘋果日報》，2014 年 5 月 20， 版 17。
[468]羅添斌，〈中對台導彈民進黨評估 2025 年增至 1850 枚〉，《自由時報》，2014 年 3 月 3， 版 4。
[469]李奕明、劉時均、鄧桂芬，〈詐團吸收同袍 LINE 拍圖傳軍情〉，《聯合報》，2014 年 5 月 9，

二、中共網路戰對我之威脅評估

(一)駭客能力

2004 年，國內曾任中國時報系政治、軍事記者劉台平先生表示，兩岸若發生戰爭，中共將直接針對重要指管通情資訊系統進行攻擊，手段包括駭客戰、電磁戰，甚至運用特務人員佔領指揮管制網，進而從內部操其他管制網路，影響通訊工具及金融體系，甚至可能利用虛擬技術，製作總統下令軍方投降不實影片。[470]

根據我國黃俊麟上校的研究，中共已明確將資訊作戰網路戰視為未來戰爭之一重要型態，可替作戰部隊在武力犯台登島創造有利之作戰條件，「攻台戰役聯合指揮部」除編成集團軍的「陸、海、空作戰集團」與「戰役後勤保障集團」外，另將編成集團軍級的「電子作戰集團」與「信息作戰集團」以執行攻台首戰中的序戰。於台海戰端初啟，破壞我雷達設備、電力系統、指管中心所屬精密電子儀器，以乘勢奪取戰役制空、制海及制電磁權。[471]另根據林宗達指出，中共網軍對台的威脅，不僅止於軍事安全方面，亦含括對經濟和社會等非經濟方面實施網路攻擊。林宗達還表示，中共網軍非軍事面向的網路攻擊，將會對台經濟、交通及能源產生重大的威脅與挑戰。一旦台海發生戰爭，未來台灣經濟和社會遭受到解放軍專業部隊的攻擊，尤其是運用網路駭客攻擊的挑戰將無法避免。[472]

國防大學教官載政龍上校在 2012 年的一篇論文又指出，當前中共「網軍」為突破我國資通安全之防禦機制，大量利用「社交工程」手法，藉機敏機關或重要人士周邊關係，「由近而遠」或「由疏而密」等迂迴方式對我發動突穿、滲透等駭客攻擊，在獲取我遭駭單位內部網路最大控制權限後，大肆進行盜竊、偽造資訊或癱瘓網路通聯等。[473]

根據 2013 年 3 月 25 日《聯合報》報導，台灣是駭客攻擊攻擊活動最頻繁的國家，勝過美國、中國大陸，主因是「多數駭客來自中共」。《聯合報》並表示，對於部分行政機關、駐外單位都曾「淪陷」，府院高層大感震警。我國資安官員也指出，組織型駭客對國安、兩岸、金融稅務資料最感興趣，但總統府、國安會、陸委會、財產部的資安是最高防密等級，駭客多採取「迂迴突破」攻擊駐外使館、地方政府，學校等「脆弱點」。[474]同年 4 月，我國國安局副局長張光遠於接立法院表示，中共為全面掌握我國防、政治、外交、兩岸等發展動態，對我發動網攻擊竊密對象，已由政府機關、駐外館處，轉向民間智庫、電信業者、委外廠商等，並轉變思維攻擊我較疏於防護網路節點設施或車量交通誌儀設備、寬頻路由器、工業微電腦控制器、網路停存系統等嵌入式系統裝備，未來恐將擴及我國關鍵基設施與個人，並逐步蒐集民間政黨規劃、經貿分析、學術著作，以及電信網路、關鍵基礎設施系統等隱性資訊或是透由網路攻擊癱瘓我國運作。[475]

版 12。

[470]劉台平，《島計畫-2008 年中共發動對台割喉戰》，北京:時英出版社，2004 年，頁 25。

[471]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 240-27。

[472]林宗達，〈中共信息戰之「網軍」作戰初探〉，《展望與探索》，第 5 卷，第 9 期，2007 年 9 月，頁 84。

[473]載政龍，〈中共網軍發展與網路攻防:兼論我國資通安全之政策規劃〉，《戰略評估》，第四卷，第四期，2012 年冬季，頁 112。

[474]林政忠，〈駭客攻擊對象 台灣居世界之冠〉，《聯合報》，2013 年 3 月 25 日， 版 8。

[475]〈 立法院第 8 屆第 3 會期外交及國防委員會第 20 次全體委員會議記錄〉，《 立法院公報》，第

(二)病毒

我國近來也頻傳遭受中共「網軍」入侵事件，如 1999 年「兩國論」後，中共的駭客族，在 1999 年 8 月間，就對台灣發動了高達 72,000 次的攻擊，其中有 165 次成功。同時國安局網站一個月內也遭受中共駭客有計畫的從 165 個網站發起的 7,238 次的攻擊。在 2003 年 7 月的 1 個月內，我政府機構、企業、大專院多達 58 個單位的電腦系統，先後遭致 23 種攻擊程式入侵，這些惡意攻擊均源自於中國大陸的湖北與福建。依據全球知名網路安全賽克鐵門公司(Symantec)的統計，以上網人數與惡意活動數量比較，台灣是全球惡意活動密度第二高地區，其排名僅次於以色列。另據報全台有 984 個網站被植入惡意程式碼，其包含木馬程式、後門程式、間諜軟體、病毒軟體等，上述的網路入侵活動，據「國家通資會報」研判不排除中共「網軍」的作為。[476]

2009 年 3 月多倫多的蒙克國際研究中心(Munk Center for International Studies)研究發現，全球 103 國至少有 1295 部政府和民間機構電腦曾遭電子間諜滲透，許多政府機構的機密文件遭竊取。這些滲透所使用的手法為社交工程[477]，藉由寄發引人注目標題之信件，誘使特定對象開啓信件附件或 URL 連結。受此手法入侵之電腦，會下載「ghost RAT」木馬程式，竊取文件，加拿大研究人員稱其為「鬼網」，其目的係為部署電子間諜於全球網路以搜取世界情報，而幕後主控當局則是中共當局。[478]根據「Tracking GhostNet:Investigating a Cyber Espionage Network」研究報告顯示，鬼網的 4 部電腦有 3 部在中國的海南島、廣東和四川，第 4 部則在美國加州南部，感染 103 個國家 1295 台電腦，其中有三分之一屬「高價值」目標，包括外交部、領事局、大使館、國際組織及非國際組織、新聞媒體，並指出，台灣被感染之電腦數量為最高，可見台灣為其主要針對性主要目標。[479]

據美國安全軟體公司「邁克菲」(McAfee)2010 年對「極光行動」(Operation Aurora)的調查報告，谷哥和其它 30 多家美國公司遭先進而持續的網路攻擊，是利用社交工程連結到有惡意病毒碼的網站所造成的，追縱電腦病毒來源，是來自台灣遭中共病毒入侵的伺服器所造成，其證據為本案病毒碼片段，符合一篇有關數學演算法的中文論文所提及樣本。此外，2011 年 8 月，一個名為「隱蔽遠端存取木馬程式行動」(Operation Shady RAT)的國際駭客活動，遭滲透計有加拿

---

102 卷第 29 期， http://lis.ly.gov.tw/lgqrc/lgqrkm1?4^850847759^15^^^1022902^1-62^102 卷 29 期 ^@@14047(2014 年二月 9 日)

[476]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 22-23。

[477]就網路應用的實務而言，「社交工程」式的網路攻擊的確是最前最常見、也最難防範的攻擊方式。在受攻擊者瀏覽或開啟附加檔案後，即同時被安裝惡意程式，接著就可能遭到遠端入侵、攔截、追蹤、監聽或成為另一個攻擊行動的跳格。由於「社交工程」的對象難以捉摸，因此，舉凡政治、金融、科技、商業、通訊、工業、國防等各領域，以至個人隱私，可有可能暴露在「網軍」攻擊的範圍中，其影響是全面的，而且損害難以評估。

[478]鬼網(GhostNet)，RAT 是 Remote Adminstration Tool 縮寫，此工具為遠端管理工具程式，但並不漫無目標寄送惡意電子郵件竊取使用者電腦資料，而是有特定目標採取蠶食鯨吞的手段滲透，其攻擊行為由攻擊者一開始捏造之電子郵件帳號發出信件至特定對象之電子郵件信箱，並於信件內夾帶一個 word 文件藏有惡意程式之 URL 連結，引誘使用者開啓檔案，當使用者開啓檔案或點選連結之後，被感染之電腦將下載一個稱 ghost RAT 的木馬程式，此允許攻擊者取得完整存取權限，自動連結至主要的控制電腦，也可開啓受感染電腦之 web cam 進行視訊監控。

[479]陳漢強、蘇文德，〈中共信息戰之網路攻擊型態研究〉，《新新季刊》，第四十卷，第二期，2012 年 4 月，頁 236-237。

大、印度、臺灣，還包括建築、鋼鐵、能源、科技、電信和媒體等公司，其入侵者可操控指管伺服器公開入侵對象的標準程序，此伺服器位於北京和上海。[480]

據報導，號稱「世界第一間諜」的中共新型監控軟體，已被引進台灣，且有不肖徵信業者用來為客監控目標。此套軟體只須一分鐘控檔，就能將監控軟體快速植入被害人手機，且無須被害人點閱，就能連線監機主的行蹤，市面上九成以上的智慧型手機都能安裝，iphone、三星手機等大廠也未能倖免。一旦遭此軟體鎖定，不論是通話內容、傳送圖檔、簡訊，統統無所遁形。[481]

除此之外，據 2011 年 12 月 9 日《聯合報》的報導，美國國防部將台灣遭中共封鎖納入兵棋推演項目內，其想定事項為中共借對台出兵轉移內部接腫而來的危機壓力，且美國行政部門忙著對激進派伊斯蘭教國家和團體，又享受與中國做生意帶來的短期利益，未能洞燭機先。屆時由中共潛艦上裝設了切斷海底光纖電纜的機具，一方面造成美國國防部與部隊補給線失聯，另一面擾亂紐約證交所，造成「美股停止交易近兩天」。[482]若加上 2009 年，一名號稱中國科技公司董事長的馬中飛，參訪位於基隆路、和平東路口的國軍人才招募中心時，竟非法闖入後方的通資部營區，還到處拍照，後被以「不法侵入或留滯軍用處所罪」移送高檢署偵辦。[483]從上述種種中共企圖以網路戰優勢，以癱瘓、摧毀我國政、經、軍、心的種種行為，均證明網路戰是攻台最佳作戰方式。

[480]童光復譯，Scott Jasper，〈美國與中共的網路戰爭〉(Are US and Chinese Cyber Intrusions So Different)，《國防譯粹》，第 40 卷，第 12 期，2013 年 12 月，頁 79。
[481]陳文嬋，〈手機間碟軟體 傳通簡訊就監控〉，《自由時報》，2012 年 12 月 20 日， 版 5。
[482]馮克芸，〈美兵推模擬..台遭中共封銷〉，《聯合報》，2011 年 12 月 9 日， 版 19。
[483]吳明杰、邱燕玲，〈我神秘網軍 首度秀戰力》，《自由時報》
http://www.libertytimes.com.tw/2013/new/may/31/today-fo1.htm (2014 年 3 月 21 日)

第二節　我國網路戰力評估

一、組織及預算

(一)行政組織多頭馬車

我國「國家資通安全會報」自2001年1月成立以來，早期是由前行政院科技顧問組兼辦幕僚作業(總召集為行政院副院長兼任，副總召集人由行政院主管科技之政務委員及研究發展考核委貝會主任委員兼任,執行長由行政院科技顧問組執行秘書兼任，副執行長分別由行政院主計處電子處理資料中心主任、國防部派員及行政研究發展考核委員會資管處處長兼任)。[484]

我國網路情報蒐集單位包括內政部警政署、法務部調查局、國安會國安局與國防部情報局，然而各單位仍傾向獨立操作，彼此的資料交換與整合分析仍嫌不足。且目前資安攻擊速度太快，應將產、官、學、研、軍整合一起，由國防部、國安全、研考會或資通安全會報，給合其相關單位設立研發管理單位，公開拋出議題，提供經費提供研究工作，如自由軟體與電腦作業系統。[485]

2011年3月，行政院修正「行政院國家資通安全會報設置要點」，成立「行政院資通安全辦公室」，期強化國家資安政策規劃、提升資安通報應變效率及加速重大資安計畫推動。配合2012年1月1日行政院院本部組織再造後，「行政院資通安全辦公室」成為行政院常設任務編組。[486]2011年4月6日，國家安全會議訂定發布「國家資通安全指導小組設置要點」，在國家安全會議置「國家資通安全辦公室」，並設置「網際防禦(國防部)」「外館防禦(外交部)」、「網情蒐集(國家安全局)」等3個體系[487]與行政院「國家資通安全會報」、「資通安全」，受總統指揮。編組架構圖如圖5-1

雖然政府相關部門日益重視資訊安全，但 2013 年 4 月 30 日《台灣醒報》報導指出，我國資訊安全漏洞百出，資安單位層級應提升。有立委建議，我國資安管理由行政院下的國土安全辦公室和資通安全辦室負責，為能快速反應突發狀況，應將其組織整併，否則兩個預算不夠，沒有法源權力，無法確實保護國家安全。前陸軍司令陳鎮湘委員指出，『資訊安全管理防護雜亂，看不出來是誰主導!』。2013 年 3 月 21 日行政院在推行全國政府機關進行有系統地分析和管理資訊安全風險的方法(Information Security Management System,ISMS)資安驗證，只有行政院本部和農委會通過驗證。[488]

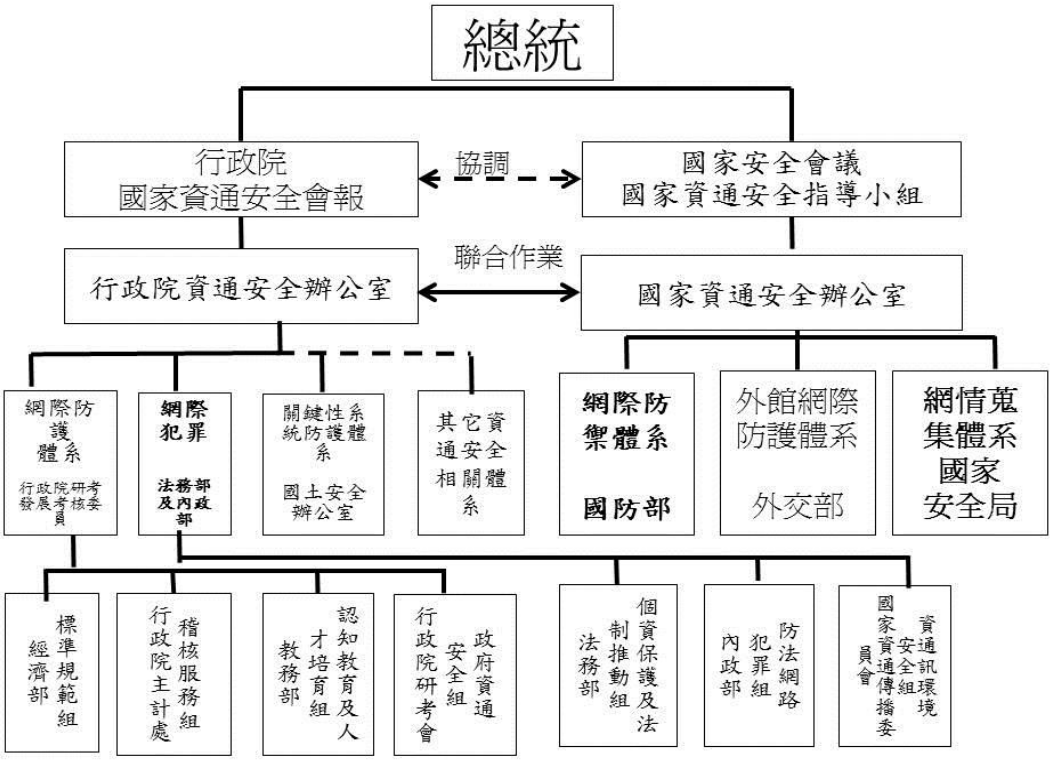
根據《中國時報》的報導，台灣號稱資訊大國，而且長久以來面臨中國的軍事威脅，但是政府對於自身資訊系統的處埋方式卻還停留在工業時代。主事者以最低標招標的方式，採購涵蓋全民重要個資的戶政資訊系統，在系統需求、軟硬體相容性及資訊安全均有欠考慮，雖然目前行政院已指定科技政委張善政擔任

[484]行政院研究發展考核委員會，《整合資通安全機制以強化國土安全之研究》，台北:五南文化出版，2005 年，頁 30。
[485]行政院研究發展考核委員會，《整合資通安全機制以強化國土安全之研究》，台北:五南文化出版，2005 年，頁 58-62。
[486]《國家資通訊安全發展方案》，《行政院國家資通安全會報》，2013 年 12 月 25 日，頁，8-9。
[487]立法院，《我國如何因應網軍與駭客攻擊並強化資訊安全措施》，《 立法院公報》，第 102 卷第 29 期，頁 7。
[488]楊智強，〈資安等級低 立委促成國土安全部〉，《台灣醒報》，2013 年 4 月 30 日， 版 2。

「資訊長」，建立政府資訊系統建置的標準作業流程，但此資訊長並非專職，未來究竟能發揮多少作用及相關政策的延續性，均有待觀察。[489]

2014 年，國安局局長蔡得勝局於立法院提報「國家情報工作暨國家安全局業務報告」時，有立委質詢，資拓宏宇公司不但承包新戶政系統，同時還承包台北市政府的消防局以及捷運局所有資訊軟體，而這公司又與大陸公司合作，讓台灣的整個資訊、資安讓中共可以在遠端搖控。蔡得勝表示，國安局已向國會機密報告，新戶政系統的資拓宏宇公司，把此軟體程序外包中國的網路公司，相關強化措施，國安局只能建議，須待行政院與國安會資通辦公室指示，才能辦理。[490]

圖 5-1:我國整體資通安全機制組織架構圖



資料來源: 立法院，《我國如何因應網軍與駭客攻擊並強化資訊安全措施》，《立法院公報》，第 102 卷第 29 期，頁 7。

(二)預算不足

2013 年 4 月 30 日《台灣醒報》引述國安局副局長張光遠補充的談話表示，目前無法完全推動資訊安全驗證，最重要的環節就是預算編列不足[491]同年 11 月 12 日，行政院政務委員張善政出席英國標準協會 BSI(British Standards Institution,BSI)資安年會指出，許多機關在資安管理和資安技術有極大的落差，有些單位妥善落實資安管理，但資安技術能力極差而難以因應資安事件，不均衡的發展讓行政院陷入高度的資安風險。此外，在管理面上最大的問題就是「承辦人」資安意識不足。雖然行政院許多 A 級和 B 級機關都被要求導入 ISO 27001

[489]李治安，〈駭客無任務〉，《自由時報》，2014 年 2 月 21 日， 版 21。
[490]楊舒媚，〈新戶政系統 轉包中國網路公司〉，《中國時報》，2014 年 3 月 11 日， 版 11。
[491]楊智強，〈資安等級低 立委促成國土安全部〉，《台灣醒報》，2013 年 4 月 30 日， 版 2。

資安驗證，但從資安稽核的結果發現，許多單位 ISO 27001 資安驗證的範圍多數侷限在資訊部門，但許多資安漏洞往往出現在業務單位的某個作業流程中，再者，有許多單位的資安經費是依據單位年度預算做調配，甚至是從編列的 IT 預算中，再挪出些許的資安經費，杯水車薪的資安預算對於各種資安業務需求，往往無法及時因應。行政院資安長趙培因並指出，包括資安驗證的範圍過小以及資安預算不足，都成為政府各機關在資安政策上面臨的主要缺失[492]。

2014 年 1 月 22 日，台、韓政府同步宣布第五代行動通訊（5G）[493]發展政策，雙方在 5G 市場上正面交鋒。政務委員張善政並表示，規劃未來六年我國將每年要投入至少 20 億元，累計逾 120 億元，扶植 5G 產業；南韓科學部則宣布要投入 1.6 兆韓元（相當於新台幣 450 億元），六年內落實 5G 飆網。根據行政院資料顯示，2012 年台灣宏達電投入研發費用 5.2 億美元、聯發科 4.4 億美元、鴻海 3.83 億美元、華碩約 2.9 億美元、宏碁約 1 億美元，相較之下，三星投入研發費用高達 103.5 億美元，是台灣這五家重要廠商的數倍之多。觀察雙方的智財權數量，全球 5G 智財權排行中，LG 達 438 件，排行第一，微軟 305 件，諾基亞 288 件，RIM 218 件，三星 203 件；全台包括工研院、聯發科、宏達電、資策會、交大及宏碁等，僅有 21 件，落後韓廠相當多。[494]上述數據顯示，無論在政府或民間部門，我國在資安與資科方面的經費支出，都遠不如南韓。

二、網路安全漏洞與缺失

(一)防護能力不足

網際網路已成為台灣社會的一個重要組成部份，正因如此，在資訊戰攻擊下，整個經濟、社會和軍事等將會大受影響，資訊網路技術的發達意味著國家在經濟、社會和軍事等諸方面依賴網路，當遭遇資訊戰攻擊即產生經濟損失和安全威脅。據研究指出，針對台灣地區駭客分析，報告發現，台灣金融、教育、政府等單位被駭客攻擊事件在亞洲地區，只僅次中國，更是亞洲四小龍之冠，台灣網路的不安全，不僅是經濟上的損失，更重要的是機敏機料的外洩。[495]

在 2008 年，我國好幾個政府部門-包括外交部-必須拆解電腦資料庫並加以重建，因其遭到中共的駭客人侵。[496]美國戰略專家費學禮(Richard D. Fisher Jr.)即警告說，中共對台灣遂行資訊戰和電腦網路攻擊，是要癱瘓台灣的民間基礎設施，以加速軍事戰役的勝利。我國學者徐佳也指出，逛一趟中國的駭客討論區，可以看到許多台灣一級政府單位的資訊直接被貼在上面，他並表示，面對網軍強勢攻擊，台灣的情資單位根本防不勝防。[497]

---

[492]〈行政院年度資安稽核結果首度公開》,《行政院國家資通安全會報技術服務中心》 http://www.icst.org.tw/NewsRSSDetail.aspx?seq=14672&lang=zh (2014 年 3 月 21 日)

[493] 5G 比現行的 4G 網路傳輸速度快約 1,000 倍，可讓用戶在一秒內下載 800MG 的電影檔案，比 4G 需時 40 秒更快，飆網速度快將有助南韓企業爭取海外生意。

[494]林安妮、黃晶琳、季晶晶，〈5G 投資 台灣大輸南韓〉,《聯合理財網》, http://udn.com/NEWS/FINANCE/FIN3/8444050.shtml>（2014 年 3 月 16 日）。

[495]陳憶綾，《解放軍資訊戰對台軍事安全影響之研究》，政治作戰學校政治研究所碩士論文，2006 年 6 月，頁 67。

[496]國防部史政編譯局譯，費學禮 (Richard D. Fisher Jr.)，《中共軍事發展-區域與全球勢力佈局》(China's Military Modernization-Building for Regional and Global Reach)，台北:國防部史政編譯局，2011 年，頁 204。

[497]徐佳，〈網軍來襲，新一代國防戰開打〉,《數位時代》，第 228 期，2013 年，5 月，頁 91-92。

台灣因資訊化普及，已成為惡意程式最佳攻擊測試平台。據國家高速網路與計算機中心監測分析，全球駭客每天平均對我國發動 340 萬次惡意攻擊，居世界之冠。全球新發現惡意程序中，每 10 集就有 1 集是台灣特有種率先在台灣出現，吸引各國駭客把新發展惡意程程拿到台灣測試，確認可以入侵後，再放全球作亂，使我國成為成為惡意程式跳板。國網中心過去 3 年測試分析發現，台灣每天平均受到 340 萬次惡意攻擊，俄羅斯是主要來源，研判是中共駭客以俄羅斯為跳板，對台發動攻擊。[498]

另外，根據 2013 年 12 月 24 日一名法國的安全系統工程師凡德肯(Eloi Vanderbeken)無意間發現路由器(Linksys)有後門，並在軟體專案共享網站(Github)公布其發現，隨後引起許多軟體工程師的興趣，進而挖掘出其他存有同樣漏洞的路由器，還包括 Linksys、Cisco 與 Netgear 等品牌的多款路由器。[499]根據 2014 年 1 月 3 日美國網路安全網站(Net-Security.org)指出，這些路由器均由台灣的專門代工網通設備的中磊電子(Sercomm)所製造，所以其他由中磊代工的 3Com、Aruba、Belkin 與 Watchguard 等品牌的產品也被懷疑含有同樣的後門。[500]

根據媒體的批露，我國國防部及民進黨黨部網站都曾遭植入木馬程式，只要利用 IE9 與 IE10 瀏覽器這些網站就可能中木馬病毒[501]。中毒後，民眾電腦不但會被遠端監視並控制，所有的資料包含信用卡資料甚至私密照版均可能外洩，我我國遭中共駭客攻擊統計，如表 5-1。[502]

表 5-1. 我國遭中共駭客攻擊統計表

1999 年 8 月	兩國論後中國網軍首次大規模發動攻擊，行政院、國安局、監察院等政府網站被植入木馬程式。
2003 年 8 月	威盛電子、中華電信、警政署、中選會、國防部等 88 個政府和民間單位電腦，陸續遭到中國湖北與福建網軍入侵，植入木馬程式。
2004 年 3 月	中國網軍利用總統大選期間大選入侵總統府、國安會內部網站取資料。
2004 年 6 月	民進黨官方網站與軍聞社被中國網軍入侵。
2005 年 6 月	外交部電腦被中國網軍入侵植入木馬程式
2006 年 3 月	台灣百餘外交使館網站遭到中國網軍入侵，外館資料密。

資料來源:陳憶綾，《解放軍資訊戰對台軍事安全影響之研究》，政治作戰學校政治研究所碩士論文，2006 年 6 月，頁 68。

[498]李宗祐，〈台灣 340 萬次/天網路攻擊〉，《中國時報》，2013 年 8 月 30 日， 版 8。
[499]〈Cisco、Linksys 與 Netgear 的無線路由器存有後門》，《行政院國家資通安全會報技術服務中心》http://www.icst.org.tw/NewsRSSDetail.aspx?seq=14698(2014 年 3 月 21 日)
[500] 同註 498。
[501]據全球最大防毒防體 360 發現，駭客利用 IE9 與 IE10 最新的 Oday 漏洞，在中國民國國防部及民進黨部網站入木馬病毒，此次 IE 漏洞編號為 CVE-2014-0322，駭客利用了 use-after-free 網站，結合 Flash 特性，繞過 IE 瀏覽器的 ASLR+DEP 防護，得到執行以後，惡意程式就會下載一個含有加密的攻擊程式 jpg,讓攻擊者可以遠端監視並控制中毒的電腦。
[502]鍾翠珠，〈國防部也受駭 網路安全陷危機〉，《民眾日報》，2014 年 3 月 3， 版 2。

(二)資訊警覺不夠

我國大力推動資訊發展，但相對地對資訊相關設備之依賴則日益加深，又因社會變遷，人民危安意識淡薄，使得現階段我國資訊戰的發展僅止於軍事層面，關係民生其鉅之各種金融、電信、電力與交通運輸及當前政府推動的網路化政府等計畫中各種資訊系統已成為中共之最佳攻擊目標而不自覺，儼然成為國家安全之嚴重隱憂。[503]

2012 年 10 月 18 日，中國網路軟體龍頭「騰訊」手機即時通訊軟體（APP）微信（WeChat），正式宣布來台擴展市場。資訊安全專家提醒，使用微信 App 需登錄手機號碼或電子郵件，且是透過騰訊伺服器實施訊息傳遞，只要熟知該軟體架構者，做到監聽並不困難，安裝微信等於自動納入中共的網路防火牆中。[504]相對而言，印度國家安全事務副顧問桑德胡建議印度情報局、內政部和電信部聯合商討封殺微信的方案，理由是微信威脅印度網絡安全。[505]

當歐、美、等均禁止採購中共「華為」製造的資通訊產品，在 2013 年，我國包括總統府在內竟有高達 46 個機關採購華為生產製造的通訊產品，如表 5-2。另外 4G 電信是台灣全新商機同時，中共「華為」已透過在台獨家總代理「訊崴公司」積極布局台灣 4G 市場。若台灣採用 TD-LTE 技術，就有可能像木馬屠城記中的特洛伊城，通訊安全門戶大開，未來中共網軍不必大費周章，就可直接在台監控所有通訊，屆時國安防線也將全面瓦解。因此，NCC 應該嚴格禁絕國內的電信業者採購華為，以維護國家安全。[506]

另外，國內電信業者希望在未來 4G 基地台，採購中國大陸品牌華為的電信設備，而首先提出申請採購「華為」基地台則鴻海旗下的國基電子。該報導表示，在電信 3G 服務時代，電信業不得採購陸資廠商的電信核心網路設備，但周邊的基地台、電話及網卡則不在此限。故國內電信業者幾乎均採購一定數量的陸資廠周邊設備。[507]據另一項報導披露，國內主管機關未明確將技術規格訂定清楚，致使產生資安漏洞疑慮。且因為未來 4G 基地台遍布各地，有心人士僅透過基地台植入木馬程式，就能攻擊其他基地台甚至核心設備。[508]

同樣令人關切的是，國防部據報導規劃自 2014 年起，將裁撤有三十四名總機暨「聯合查號台」話務人員，將總機話務委由民間公司承包。但有立委即指出，資電作戰指揮部聯合查號台，具有相當機敏性質，話務人員應屬作戰支援人員，掌握國軍電話資料庫都屬密級上，若貿然將機敏性工作委外，將衍生國防安全作業上難預測的。[509]上述資料顯示，當國內一味追求低成本的同時，網路安全卻已曝露在中共的威脅下。

---

[503]行政院研究發展考核委員會，《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》，台北:五南文化出版，2002 年，頁ⅤⅡ。

[504]王珮華，〈中國騰訊 APP 微信今登台 台灣即時通 中國可掌控》，《自由時報電子報》http://www.libertytimes.com.tw/2012/new/oct/18/today-fo1.htm (2014 年 3 月 23 日)

[505]〈借口網絡安全　印度或封殺中國微信》，《中國評論新聞網》http://hk.crntt.com/doc/1025/8/6/4/102586449.html?coluid=0&kindid=0&docid=102586449&mdate=0618105253 (2014 年 3 月 23 日)

[506]黃文玲，〈中國解放軍　監聽台灣政府〉，《台灣團結聯盟全球資訊網》，http://www.tsu.org.tw/?post_type=ly&p=5448 (2014 年 3 月 23 日)

[507]彭慧明，〈買陸資設備卡關〉，《聯合報》，2014 年 4 月 28 日， 版 10。

[508]彭慧明，〈4G 基地台 涉通訊、資料加解密〉，《聯合報》，2014 年 4 月 28 日， 版 10。

[509]羅添彬、曾韋禎，〈軍方總機外包喊卡〉，《自由時報》，2013 年 1 月 10 日， 版 4。

表 5-2:國內各政府機關採購華為通訊產品一覽表

機關名稱	手機	行動網卡		
	CHT8000	E169	E173	E800
法務部調查局	—	—	124	—
文化部	1	25	16	0
財政部關務署台中關	—	—	40	—
金管會	—	35	—	—
考選部	—	—	27	—
行政院	—	—	24	—
交通部	20	—	—	—
交通部港務局	—	—	20	—
衛生福利部台中醫院	—	4	11	—
總統府	—	—	6	—
原民會	—	5	—	—
原能會	—	—	5	—
教育部及轄下院校	—	3	6	1
內政部及其他單位	—	1	3	1
陸委會(調查後已立即停用)	—	—	1	—

資料來源: 羅添斌、施曉光、林嘉琪、林俊宏,〈華為產品 國安局禁用總統府照買〉,《自由時報》,2013 年 10 月 29 日,版 4。

根據 2013 年 8 月 16《自由時報》的報導，兩岸服貿協議引爆資安與國安危機，服務開放第二類電信業務及電腦相關服務業，形同現代 e 化版的木馬屠城條款，提供中共合法、安全且隱密的管首竊取所有資訊，對我國家安全及言論自由都都將受到威脅，但我國經濟部官員辯稱服貿只開放較不重要的第二類電信[510]。交大資工系教授林盈達亦表示，美國和印度都透國安審查機制，杜絕中國電信設備進入電信網路服務業者的機房，而我政府卻是在設備都仍有疑慮之下，竟還允許中共業者來台開店，林盈達擔心中共可能藉此方式，透過執照，在從現有台灣電信網路業者取得外包網路服務的機會，直接掌控用戶通訊，陷台灣人民於紅色警戒之中。此外，台科大資工系助理教授鄧惟中也揭露，開放電腦及相關服務，使公司和公私立機構，可能因與中資代理商簽訂維修合約，而維修工程師則是中共受原廠訓練的專家，因維修所需可遠端連線到電腦主機，不僅擁有管理員等級權限，甚至能夠實體接觸主機，等於提供中共合法，安全且隱密的連線通道。[511]

此外，2013 年 10 月 2 日立法院內政委員會第四場服務貿易協議公聽會即有立委指出，國家通訊傳播委員會(National Communications Commission,NCC)對這次開放項目的業務範圍到底有那些都說不清楚，而且對國安的影響，國安單位竟無相關評估，再加上兩岸貨品貨易協議簽訂後，增加開放硬體設備，國安將全面潰堤。[512]其結果可能如 2014 年元月初，我國行政部門機敏會議內容外洩，檢討原因為某位長官因為手機遭植入惡意程序，並於會議中利用電腦充電，該手機啟動錄音功能，所有會議內容都被錄音且對外傳送。[513]

[510](根據定義,第一類電信指提供實體電路的服務執造,包括中華電信.遠傳.台灣大等都屬此類電信服務提供者.第二類電信則必須向第一類電信者承租線路.提供網路服務.如 CNET.SoNET 等屬第二類)。

[511]林詩萍，〈學者:服貿開放網路電信.國安資訊都淪陷〉,《自由時報》，2013 年 8 月 16， 版 6。

[512]蘇芳禾，〈電信業開放 業者:像木馬屠城〉，《自由時報》，2013 年 10 月 3 日，版 5。

[513]黃彥棻，〈正視政府機關的資安危機，行政院年度資安稽核結果首度公開〉，《ithome》

根據 2014 年 2 月 20 日《自由時報》的報導，我國新戶政系統不穩定問題癥結，在於得標商資拓宏宇[514]為節省工程師人力成本，將部分系統轉包給中國資訊軟體業者撰寫程式，可能因國情與實務應用狀況不同，造成與國內既有系統不整合問題，也危承及且恐成為資安漏洞。戶政系統負責國民最重要的身分證，一旦資安出現問題，其影個人安全。也有台北市議會議員透露，目前我國採購法或北市府軟體採購的標準作業程序(SOP)，根本無法防範得標廠商轉包給國外，北市府也缺乏一套有效管控機制，防止外國間接控制個資或植入不明「後門軟體」。[515]

三、基礎設施

根據 2002 年行政院研究發展考核委員會的資料，台灣已逐漸成為國家通信基礎建設完整性的國家，而這樣的一個依賴國家資訊通信基礎建設的國家很容易遭到受攻擊而陷入危險。由於海外科技商品、技術陸續傳回國內，同時使用現成科技商品已成為常規。因此，台灣的國家資訊基礎建設的一些科技產品(如電腦軟體)皆以外國規格為主，很容易肇生資安洩密情事發生。[516]

美國學者毛文杰等人曾對我國提出警告，由於重要基礎設施的防護，一直是中華民國政府的低度優先項目，在面對類似俄羅斯 spetnaz 特戰部隊或第五縱隊時，更是不堪一擊。在民間電網方面，中華民國電信、電力與交通設施都極易遭受破壞。如 1999 年的 921 大地震與 2001 年 9 月的颱風，都使通信設施嚴重受創，間接暴露這方面問題。[517]

2013 年 2 月 25 日，全台八成網路使用者經歷了十年來第一次「網路黑色星期一」，因一棟掌握全台網路命脈的關鍵機房，位於內湖陽光街的麗源大樓，是 IDC 業者是方電訊總部[518]，進行年度地下室例行檢修 UPS 電池時，不慎引燒起火，因救火第一步驟要切斷電源，但是用來做備援電力的發電機同樣位於失火的地下室，致使近 20 小時服務中斷。經檢討後發現，原來係因台灣國際海纜、電信服務過度集中化的問題。[519]國安局張副局長因此表示，面對日益嚴峻的資安威脅與挑戰，除加強個人資安防護觀念與作為外，更需結合國內電信者力量，前進部署防護措施至電信體幹網路，故籲請國內各家電信業者不能僅考量自身商業利益，配合國家整體政策需求，強化並落實骨幹網路安全。[520]

---

http://www.ithome.com.tw/itadm/article.php?c=83953

[514]資拓宏宇同時負責北市消防局防災、工務局、捷運公司、資訊局台北地圖、市政雲軟體撰寫。

[515]陳慰慈、蔡亞樺、吳柏軒、甘芝美、陳慧萍、陳彥廷，〈新戶政程序轉包中國資安系統門戶大開〉，《自由時報》，2014 年 2 月 20 日， 版 7。

[516]行政院研究發展考核委員會，《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》，台北:五南文化出版，2002 年，頁 72。

[517]國防部史政編譯局譯，毛文杰(James C.Mulvenon)、譚睦瑞(Murray Scot Tanner)、蔡斯(Michael S. Chase)、傅里林格(David Frelinger)、龔培德(David C.Gompert)、李比奇(Martin C.Libicki)、包克文(Kevin L. Pollpeter)，《中共對美國軍事變革之反應》(Chinese Responses to U.S.Military Transformation and Implications for the Department of Defense)，台北:國防部史政編譯局，2010 年，頁 116

[518]2000 年網路起飛，是方電訊是最早投入專業 IDC 的業者，而麗源大樓的機電設計、空調、布線在當年是五星級規格，並且是唯一中立業者，當時吸引九成的國際海纜業者向是方承租，海纜進來，向其購買頻寬的國際和國內電信業者、固網也紛紛進駐，這裡同時是台北網路交換中心，所有國際知名網路服務供應服(ISP)都在此交換。簡言之，台灣對內、外網路服務都在此匯集。

[519]趙郁竹，〈一把火，燒出台灣網路建設隱憂〉，《數位時代》，第 228 期，2013 年，5 月，頁 114-115。

[520]立法院，《我國如何因應網軍與駭客攻擊並強化資訊安全措施》，《 立法院公報》，第 102 卷，第 29 期，頁 8。

第三節　我國因應中共網路戰之具體作法與建議

一、強化創新、不對稱作戰思維

2012 年，國防部在「國軍五年兵力整建計畫」中透露，國軍為發展不對稱作戰，將重點發展「區域效應武器」和「岸置機動遠程精準打擊火力」，而區域效應武器為非核電磁脈衝武器攻擊，造成敵軍大區域電路和網路中斷，進而指揮系統癱瘓。這些戰力平時可隱而不顯，戰時則能重擊敵軍戰略重心或癱瘓敵軍作戰能力，以創造局部優勢。[521]國防大學謝游麟上校認為，面對中共導彈威脅，我國尚無立即有效的對策時，應利用我國雄厚的資訊潛力或許可在中共採取導彈攻擊之際，對其 C4ISR 等系統進行網路戰攻擊，爭取資電優勢，另藉網路破壞、駭客入侵、植入病毒、邏輯炸彈等方式，入侵共軍相關網路，癱瘓指管機能，使用其無用武之地。因此，國軍應結合民間科技能量，研發關鍵技術，建構有效的資訊武器，例如電腦病毒、防毒防護軟體、網路監控軟體，以建立全軍資訊戰攻擊能量。[522]在 2013 年出版的《國防報告書》中，國防部再度強調，因應未來防衛作戰需求，國軍應針對作戰重心與關鍵要害，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。[523]

立法委員林郁方表示，2013 年我國國防預算計 3,145 億元，較 2012 年法定預算 3,172 億元，減少 27 億元，佔中央總預算的比例約 16.17%。而人員維持費為達成 2015 年 1 月 1 日實現「全募兵制」的政策目標，2013 及 2014 將各增增 1 萬 5 千名志願役官士兵，受志願役士兵員額大幅成長的影響，2013 年人員維持預算編列 1,575 億，較 2012 年增加 20 億，占國防預算的比例由百分之 49 至增至 50。若大環境持續不佳使整體財政政支出無法大幅提升，勢必對「作業維持」和「軍事投資」預算造成明顯的排擠效應。再加上對美軍購(AH-64E 攻擊直升機、UH-60 通用直升機、愛國者二型性能提升及新購愛國者三型防空彈、F-16A/B 性能提升)付款進入高峰期的影響，2013 年就需支付 480 億元，相對壓縮科學研究預算不到 30 億元(2012 年 60 億)，對國防科技能量的累積造成嚴重衝擊。[524]

根據我國學者王志鵬的研究，台灣的國防預算佔中央政府總預算的比例，從 1991 年的 30.34，降至 2006 年 16.06，年均下跌約 0.95%，2007 年調整至 19.4%，2008 年，調高為 20.6%。2008 年馬英九總統於選前政見即承諾國防預算維持 GDP 的 3%，但至今歷經五年仍從未能落實。未來台灣國防態勢仍將如此，且在此國防資源有限與募兵制產生經費排擠的情況下，實在不容許無用的浪費。[525]據報導，國軍目前正在研發「無人攻擊飛機」，但因國防部近兩年科研經費減半，致使研發單位中科院研發能量陷入瓶頸。[526]在受國內經濟不景氣影響下，國防預算又因募兵制所需人員維持費佔總金額一半，加上現代化的武器價格昂貴，當務之急，就是投資成本小、效益高的網路戰，才能符合最佳經濟效益，確保國家安全。

---

[521]吳明杰，〈癱敵網路 軍方擬研發脈衝武器〉，《中國時報》，2012 年 9 月 3 日， 版 4。
[522]謝游麟，〈國軍發展「不對稱」軍事思想之途徑與實踐〉，《國防雜誌》，第 27 卷第 4 期，2012 年 7 月，頁 59-60。
[523]國防部，《中華民國 102 年國防報告書》，台北:五南文化出版，2013 年，頁 72。
[524]林郁方，〈2013 年國防預算剖析〉，《亞太防務》，第 56 期，2012 年，12 月，頁 4-5。
[525]王志鵬著，〈面對中國大陸軍力成軍，台海空優成空憂!思維必須大轉變〉，《尖端科技》，第 347 期，2013 年 7 月，頁 13
[526]吳旻洲，〈我無人攻擊機 研發經費不足受阻〉，《大紀元電子日報》，http://www.epochtimes.com.tw/b5/14/01/23/81787.html >（2013 年 11 月 28 日）。

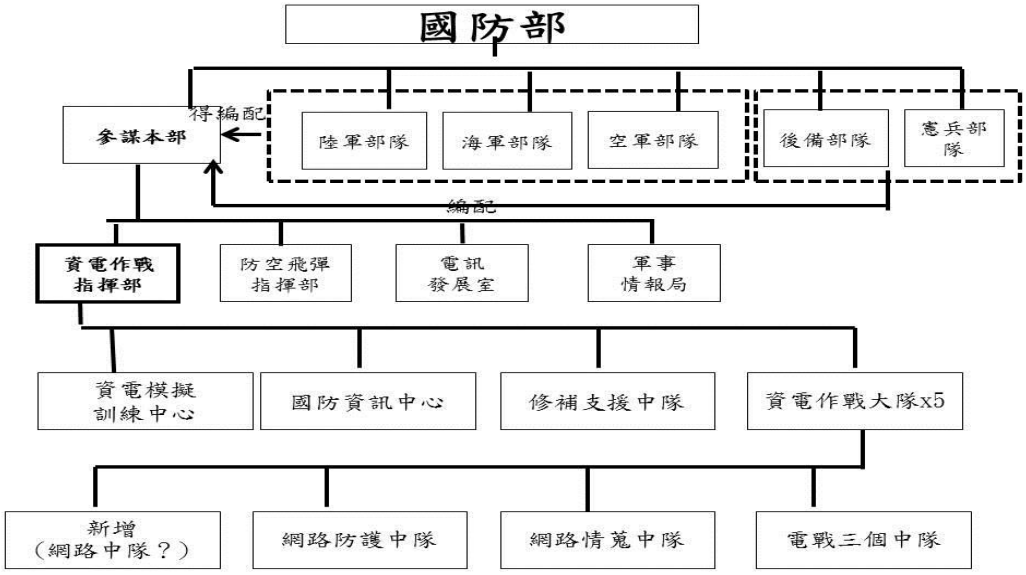
二、積極培育網軍人才與增加網軍預算

根據 2004 年《國防報告書》的資料，國軍資電作戰指揮部編組資電作戰大隊 x5、國防資訊中心、資電模擬訓練中心、修補支援中隊等單位，總員額 3 千餘員，武器裝備為資訊戰攻防裝備、電偵、電子戰裝備、全數位式交換機系統、數位微波通信系統、衛星通信系統、光纖通信系統。[527]這是國防部對於我國網軍編制所做的首次透露。

為強化資電作戰能力、反制中國網軍，在軍方各單位面臨縮併情形下，資電作戰部門則是反向擴充，除增加資電作戰指揮部作業部隊外，並根據國防部「一〇二年度預算規劃」，軍方將建構「仿網路戰作戰攻防驗測環境」，提升軍方資電作戰能力，執行網路戰任務。[528]

2013 年，國防部表示，國軍資訊組織及人力編配未來規劃，以執行資訊專業人員及訓練流路為基準，以強化資安應變處置能力。[529]同年 5 月 30 日，根據《自由時報》的報導，負責國軍網路作戰，為隸屬參謀本部資電作戰部的通資電大隊，下轄包括網路防護、網路情蒐和電戰三個中隊，編制約三百餘人，國防部已宣示將於七月再成立第四支網路部隊，以強化國軍網路作戰能量，其網軍編制架構，如圖 5-3。[530]同時，國防部表示在人才招募，未來則應更具彈性，才能號召藏身於民的網路高手，在待遇和制度都要有彈性空間，才能吸引優秀電腦高手，同時也要懂得創造網路英雄，讓民間人才因為愛國心願意投入國軍網路部隊。其實，已有立法委員指出，軍方應該擴大對外招募網路高手，如有制度需要修改和預算需要支持，像是調高專業加給等，朝野立委都會贊同。[531]

圖 5-3:我國網軍編制架構圖



[527]國防部，《中華民國 93 年國防報告書》，台北:五南文化出版，2004 年，頁 117。
[528]羅添斌，〈反制中國網軍我建構網路戰攻防驗測環境〉，《自由時報》，2012 年 9 月 2 日，版 6。
[529]國防部，中華民國一〇二年《四年期國防總檢討》(Quadrennial Defense Review)，台北:五南文化出版，2013 年，頁 39-40。
[530]吳明杰、邱燕玲，〈我神秘網軍 首度秀戰力》，《自由時報》
http://www.libertytimes.com.tw/2013/new/may/31/today-fo1.htm (2014 年 3 月 21 日)
[531]同上註。

作者整理
資料來源: 國防部,《中華民國 93 年國防報告書》,台北:五南文化出版,2004 年,頁 117-8;國防部,《中華民國 102 年國防報告書》,台北:五南文化出版,2013 年;立法院,《我國如何因應網軍與駭客攻擊並強化資訊安全措施》,《立法院公報》,第 102 卷第 29 期,頁 7;吳明杰、邱燕玲,〈我神秘網軍 首度秀戰力》,《自由時報》 http://www.libertytimes.com.tw/2013/new/may/31/today-fo1.htm

為強化網路攻防作為,國安局自 2013 年起,首度配合原僅由國防部軍事單位參與的「大學儲備軍官訓練團」制度中辦理甄選。(招生 2 位;總名額為 138 員)。[532]此外,2014 年國安局國家安全情報人員召考,新增「情報組」、「公職資訊師組」等 2 類,初任薪資含專業加給約 6 萬元。據報導指出,「公職資訊師組」則是為防止駭客入侵,以網羅網路、資訊等科技情報,維護資訊安全系統等相關人才為主,其應考資格,為 18 歲至 35 歲,須具有資訊技師證書,並且從事相關工作經驗 2 年以上。[533]目前,我國培養網路戰軍事院校,計有國防大學理工學院及管理學院,在其課程設計均有資訊戰理論及相關網路安全防護相關課程。[534]

據最近媒體的披露,為掌握輿論力量,警政署要求「人民保母」變身為「網軍」,分工監看反核輿情及反服貿等言論,並要求警察主動反制不利政府的言論,若有發現可疑情質立即回報,監控有功者,將可簽報敘獎,若疏於監看者,則檢討議處。此項要求,已於 2014 年 5 月 1 日由警方證實,是該部保二總隊行文所要求。[535]

其實,國內網路人才不餘匱乏。例如 2013 年 5 月 12 日深夜,我國漁民因遭菲律賓公務船開槍掃身亡,引發國際知名駭客團體「匿名者(Anonymous)」組織,對菲律賓政府的伺服器實施網路攻擊,此次網路攻擊準確打到菲國網路要害,造成很大的破壞,短期內想全面復原並不容易,最後導致菲國政府網站一個個癱瘓。過去,外界並不知台灣也有「匿名者」成員,此一戰,讓台灣駭客也了國際焦點。[536]據另項報導,國內一名高二生於兩個月內入侵一千兩百多個網站,讓自己在駭客網站的全球排名衝至第十九名,還開心打扮成 V 怪客在臉書自拍炫耀。此舉已觸犯《刑法》妨害電腦使用罪,侵入他人網站可處三年以下徒刑,刪除或變更網站內容可處五年以下徒刑。[537]

在民間學校方面,國內致理技術學院自 2006 年 2 月 1 日配合教育部推動技職教育證照制以來,已培育許多產業界所需人才。該校並與全球最大第三方國際認證機構 CompTIA 合作,獲得的 A+、NETWORK+等系列專業國際證照教學資源。據

[532]羅添斌,〈強化網攻 國安局招募大學生駭客〉,《自由時報》,2013 年 11 月 12 日, 版 6。
[533]董俞佳,〈國安特考增情報、公職資訊師 2 組〉,《聯合報》,2014 年 4 月 6 日, 版 A。
[534]〈課程設計〉,〈國防大學理工學院資訊工程學系〉http://csie.ccit.ndu.edu.tw/files/11-1011-322.php;〈教學設施〉,〈國防大學管理學院資訊管理學系〉 http://www.ndmc.ndu.edu.tw/editor_model/u_editor_v1.asp?id={BA343F8D-5D9D-4E6B-AAA3-8BFAF291A62A}(2014 年 4 月 20 日)
[535]黃欣柏、陳慧萍、余仁皓、王定傳、湯佳玲、洪美秀,〈警仿中國五毛黨 組網軍監控輿情〉,《自由時報》,2014 年 5 月 2 日, 版 4。
[536]蔡靚萱,〈癱瘓菲國網站 幕後神祕網軍揭祕〉,《商業周刊》,第 1330 期,2013 年 5 月 20-26 日,頁 88-90。
[537]黃楷棟,〈全球第 19 台 C 咖駭客侵千網高二生自認大咖 卻挑雞排店下手〉,《蘋果日報》 http://www.appledaily.com.tw/appledaily/article/headline/20131017/35369560/ (2014 年 3 月 23 日)

2012 年 12 月《經濟日報》的報導，致理技術學院已發出 700 多萬元獎勵金，資管系更是平均每位畢業生擁有 8 張證照。[538]

圖 5-4: 我國高二手入侵網頁成功圖

表 5-3:國內駭客入侵事件表

2013/09	19 歲大學肄業生向臉書反映安全漏洞未獲重視，刪除臉書創辦人薩克柏的數篇發文和分享，臉書回信坦承缺失
2013/07	景文科大一年級學生侵入學校網路，竄改成績，變成全系第 1 名，遭判緩刑 2 年
2007/09	大學生蘇柏榕及 17 歲林姓少年突破中華電信、批踢踢等網站，盜走藝人林志玲等 300 多人個資

資料來源: 資料來源:黃楷棟，〈全球第 19 台 C 咖駭客侵千網高二生自認大咖 卻挑雞排店下手〉，《蘋果日報》，http://www.appledaily.com.tw/appledaily/article/headline/20131017/35369560/

值得一提的是，當中共以國家資源支撐駭客鑽研技術，台灣社會卻普遍把駭客等同於犯罪，造成我國的資安圈人數偏低，將駭客這個名詞除罪化，乃是台灣發展資安人才的第一要務。[539]我國學者黃基禎也指出，未來戰爭中雙方將不遺餘力攻擊對方的資訊系統和保護自己的資訊優勢，以便在發揮主導戰場的作用，網路空間的特性已除去傳統的地理障礙和國與國之間的邊界限制，產生獨特的戰略價值。然而，對於這種戰爭是否可以成功達其政治目的，「網路戰士」的素質(例如在敬業精神和忠誠度方面)是要考慮的重要因素。[540]

三、加強網路科技研究

2002 年，行政院研究發展考核委員會表示，台灣未設有如美國國安局的網路監控預警電腦，一旦網路遭入侵，無法一時間反應。在缺乏預警系統情形下，大量網站將在極短時間內逐個被破壞或殲滅。台灣有所謂網路「八號分機」，但到目前為止未曾捕獲過任何一位境外入侵者，連調查局的網站都被攻破，多個政府網站在遭境外駭客入侵後 8-10 個小時方態恢復運作，這個時間足以下載九十六萬頁資料和破壞二千個網站。[541]

2005 年，行政院研究發展考核委員會認為，由於我國尚未針對網路攻擊與

[538]〈致理技術學院加入「CompTIA 教育學院」展現教學卓越活力與國際接軌〉，《Comp TIA》http://210.68.23.242/events/Default.aspx?view=content_atricle&articleid=527(2014 年 4 月 20 日)
[539]徐佳，〈網軍來襲，新一代國防戰開打〉，《數位時代》，第 228 期，2013 年，5 月，頁 92。
[540]黃基禎，〈中國大陸網路戰思維〉，《中共研究》，第 47 卷第 10 期，2013 年 10 月，頁 149-151。
[541]行政院研究發展考核委員會，《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》，台北:五南文化出版，2002 年，頁 52-61

中共對我實施網路戰的可能性做出明確的防護措施，防範網路威脅，確保資訊安全為當務之急。再加上我國與中共之間駭客之相互攻擊，政府機關更是攻擊之目標，因此，建立網路通訊監察偵測網，不僅可以偵查犯罪行為、蒐集情報外，還可以維護系統安全，確保系統可靠性。另因系統本身之易毀與脆弱性，重要的系統與資料均有必要備援。[542]

在網路戰中，防禦比進攻更難，因為由於軍隊的資訊系統廣泛依賴電腦技術和網路技術，使得資訊系統成為整個作戰系統中最易於暴露和難以防護的部位，資訊進攻所選擇的打擊目標往往只是若干個點，而防護則為整個面，面對資訊系統攻擊的日益多樣化和綜合化，資訊系統的防護與資訊戰力是目前亟需建立的能量。中共目前投入大量人力從事網路入侵、網路防火牆、資料保密等網路技術研究，面對中共積極投入發展網路技術，我應著重電腦安全防護系統之發展，並研製電腦網路攻擊、防護及軟、硬體設備等之研究發展。[543]

我國學者陳漢強及蘇文德兩位學者表示，國軍對資訊戰能量投入資源，除提供先進資訊軟硬體，以強化資訊運算效率，以不斷更新資安技術、知識以掌握最新的網路威脅、漏洞及防護之道。國軍資訊系統應將系統發展生命週期(System Devlopment Life Cycle ,SDLC)導入，以驗證流程(Certification & Accreditation)。系統設計須導入驗證(Authentication)及授權(Authorization)管控機制，如授權機制必須符合必要用權限原因(Principle of the Least Privilege ,POLP)，系統還原程式必須導入完整性檢測，防止系統損壞時資訊可用性遭破壞。在資訊資產採購時，考量學習美軍所採用現行的資安標準(Evaluation Assurance Levels, EALs)，本項標準有 7 個等級，等級愈高代表安全性愈有保障，國軍可以依據作業的機密等級，要求採購安全標準較高的資訊資產，而廠商產品資安標準的審認及賦予，可由國軍依據訂定之資安要求所認定。[544]

其實，我國國內民間長期累積的資訊科技能量(尤其是電腦病毒攻擊技術)是相當可觀，且居全球領先地位。[545]根據 2013 年 8 月 30 日，《中國時報》的報導，我國國網中心結合台灣大學及交通大學等 20 個學研機構，耗時 3 年在全台部署超過 6000 個網路位址，偵測誘捕從國內外入侵的惡意程式，抓到「惡意程式資料庫」[546]再分析攻擊特性及入侵散播途徑。「惡意程式資料庫」已累計誘捕超過 20 萬隻惡意程式，並以每月 1200 集增加中。[547]除此之外，據報導，國內網路安全軟體公司趨勢科技(Trend Micro)在 2013 年已成為全亞洲最大軟體公司。報導並指出，耗時 3 年的上線雲端代管安全服務的「Worry free」軟體在 2010 年

[542]行政院研究發展考核委員會，《整合資通安全機制以強化國土安全之研究》，台北:五南文化出版，2005 年，頁 56-57。
[543]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 27-8。
[544]陳漢強、蘇文德，〈中共信息戰之網路攻擊型態研究〉，《新新季刊》，第四十卷，第二期，2012 年 4 月，頁 239-240。
[545]行政院研究發展考核委員會，《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》，台北:五南文化出版，2002 年，頁ⅦⅡ。
[546]「惡意程式資料庫」已於 2013 年 8 月 29 日啟用，可監測全球攻擊來源，結合 google earth，可追縱惡意程式源頭。並透過比對追縱惡意資料庫中的惡意程式，掌握未來可能攻擊行為，即時通報相關資安與網管單位緊急應變，阻斷惡意程式與駭客攻擊，只要上網 owl.nchc.tw 線上申請加入會員，就可以使用惡意程式知識庫，據國網中心副研究員蔡一郎表示，只要「惡意程式資料庫」啟用後，僅須 5 分鐘就可以把自己電腦中的惡意程式殲滅。
[547]李宗祐，〈台灣 340 萬次/天網路攻擊〉，《中國時報》，2013 年 8 月 30 日， 版 8。

正式推出，並於 2013 年獲德國調查機構 Experton 評選，為全球整體雲站安全最佳企業。[548]另據報導證實，趨勢科技前瞻性威脅研究（FTR-Forward Looking Threat Research team）團隊曾幫助美國聯邦調查局（FBI）逮捕製造病毒感染了全球 140 萬台電腦的「SpyEye」駭客，並成功地加以定罪。[549]

在網路戰硬體方面，根據 2013 年 2 月，國泰投信中國股票投資部基金經理人蔡佩芬表示，NB 的整個供應鏈，中國還沒辦法複製，以連接器來說，中國廠商就表示它們還沒有辦法跟進台廠，因為 NB 連接器的技術比手機來得難，而平板這塊，中國廠商也需要向台廠請求協助，此台廠目前看來只有像聯詠這種 IC 廠是中國真的趕不上的，所以一定要有研發力的產品，才有競爭力。[550]在未來的世界中，通訊就像高速公路一樣，成為國家的基本建設，只要把路蓋好，產業自然會起飛。只當笨水管已經賺不到錢，電信業者下一步要找到好的內容服務和對的商模式，透過合作、拆帳、在新的平台上找到不同的獲利模式，每年投入幾百億建設的行動通訊平台，才能真正替自己帶來高端價值。[551]故在網路安全裡，基礎設施如同一樣重要防毒軟體一樣重要。

[548]林士蕙，〈防毒雲 1 套抵 10 套，單品營收破 30 億〉，《遠見》，第 331 期，2014 年 1 月，頁 150-152。
[549]〈趨勢科技協助 FBI 成功起訴 SpyEye 惡意軟體作者〉，《算與網路安全趨勢部落格》http://blog.trendmicro.com.tw/?p=7305(2014 年 4 月 17 日)
[550]楊欣霖，〈跟著新政策賺錢去〉，《數位時代》，第 22 期，2013 年，2 月，頁 49。
[551]趙郁竹，〈全球瘋 4G，台灣怎麼走〉，《數位時代》，第 222 期，2012 年，11 月，頁 168。

第四節　小結

近二十年來，中共國防預算以 2 位數快速成長，從 1991 年至 2011 年中共的國防預算已成長 3 倍之多，其軍事實力已於 2006 年超越我國。雖兩岸關係趨於和緩，但歷年共軍演習顯示，中共始終未放棄武力犯台，而且駭客攻擊數目不減反增。國內、外相關學者均指出，中共攻台戰略除以網路戰除對我軍事重要單位攻擊，將結合導彈及特工人員對我實施政、經、軍、心多方面的綜合攻擊，以求經濟實惠的戰爭勝利，此一方案也最能符合中共的非對稱作戰之戰略目標。

我國具有科技小島之稱，惟政府對資安防護未能採中集中管理。政府雖在 2011 年 3 月，成立「行政院資通安全辦公室」為常態編組，惟其編制乃以各部會自行發展，致使管理組織分散、預算不足，如網路情蒐，分由內政部、法務部、國安局、國防部軍情局，其次是政策以經濟考量，未落實為國家安全。如 2013 年服貿協議，協議將手機伺服器後端同意委由中共民間企業辦理，又如 2014 年我國戶政資訊系統委由資宏拓宏將軟體委由中共廠商。最後，在基礎設施方面，並未能分散部署，雖政府一直推廣雲端概念，想強化資訊安全，但在 2014 年一個內湖網路機房因施工不慎，造成網路大中斷，反映出基礎設不足。

為因應中共共網路之威脅，我國首先應以不對稱的作戰思維面對中共外，應採集中資源，發展出關鍵性的武器，才能確保國家安全。其次應擴大網軍編制與增加預算。此外，對網路人才的培育，也顯然不夠，另外未來網軍的培養應考量「網路戰士」的素質(例如在敬業精神和忠誠度方面)，才能將民力化為我力的提升網路戰力。最後我國應加強網路科技研究，提升整體競爭力。

第六章　結論

中共發展網路戰之研究始於 1991 年波灣戰爭，並以網電一體戰或信息化名詞普見於各項有關軍事之論叢。2003 年起，中共網軍陸續遭各國媒體披露，以竊取相關軍事、商業機密為主要攻擊手段。2013 年美國曼特公司明確指出，中共網軍是位於上海浦東之總參謀部的 61398 部隊。本研究即以中共軍方的相關論述為客體，旨在探討中共發展網軍之由來、優、弱點，以及我國如何因應中共網軍之威脅，茲將本研究之發現及建議陳述如下:

第一節　研究發現

一、網路戰已成為當今最重要的戰場領域

每一個戰場空間的武器創新，訴說著將改變作戰方式及新軍種的成立，網路戰應是繼陸、海、空、天等領域後，最新一種的戰場領域空間。而隨著資訊科技及網際網路的高速發展，網路已成為每個人生活、工作必要的工具。網路不僅提升軍事指管系統，並融入政治、經濟及交通各方面領域，故網路戰已躍升成為國家安全的重要議題。再者，在現今高科技武器下，各項軍費均節節上升，而網路戰卻是相對便宜，且又不會造生人員傷亡的戰爭，故最符合不對稱作戰方式。其次，是網路戰的關鍵不再於你有多少人，擁有多少強大的武器，而是誰具有一支有組織、有紀律的高素質網路高手部隊，故網路戰已成戰場的新尖兵。在 2009 年，由美國成為全球第一個對外公佈擁有網軍部隊的國家，美國並於 2011 年，召集北約相關國家，策頒網路戰條款。同年美國國會並立法通過，可由美國國防部依總統命令，對任何一個國家發動網路攻擊。上述種種，已將網路戰正式推向國際舞台。因此，世界各國也相繼成立網軍及編組網軍所需預算，期能在未來戰場獲得先制勝利，截至 2013 年 5 月止，聯合國裁軍研究所報告，全球已有 46 個國軍成立網軍。最後，隨時資訊科技的進步，網路戰作戰方法也隨之提升，2010 年的震網病毒，是網路戰一個重要的分水嶺，以往的病毒，是以竊取、情蒐為主要目標，但震網病毒的出現，卻是一個可直接癱瘓敵人重要工業基礎設施，如核能發電廠的離心機，故網路戰的重要性已愈來愈獲重視。

二、中共積極投入網路戰發展

自 1991 年美伊波灣戰爭以來，中共已體會到資訊化時代作戰勝利的關鍵，勢必與以往不同，人海戰爭的總體戰爭將不在適合未來戰爭需求。中共也同時體會到短時間在軍事科技是無法迎頭趕上歐、美軍事強國，故自 1999 年，中共兩位學者提出「超限戰」理論後，打贏信息戰、網路戰的不對稱的作戰思維，如雨後春筍般相繼提出。2004 年，中共國防白皮書將打贏高科技下的局部戰爭修訂為打贏信息化條件下的局部戰爭，就可證實中共是愈來愈重視網路戰。此外，為能爭取資訊優勢，中共自 1991 年起，陸續組成網路部隊，其大部份為納編民間團體組織，至 2007 年，才由美國學者提出，中共已培育一支網路部隊對美國民間、軍事進行竊取等行動，其損失達上億美金。2013 年 2 月，中共網軍(61389 部隊)已成軍，並為直屬總參謀部第三部。另外，中共為確保網路安全，自 2001 年起成立中國信息安全產品測評認證中心，並於 2014 年 2 月宣布成立「信息化和互聯網信息安全領導小組」並由中共國家主席習近平擔任小組長，企圖從政治、經濟、資訊技術以確保網路安全。

三、中共網軍的作戰能力及特、弱點

中共網路戰的戰略構想，仍依循以往的人海戰術思想，並在國防政策積極防禦指導下，中共網路戰的作戰構想就是優先以癱瘓敵政、經、軍、交通(如高鐵、航管)為目標，以達損小、效高的戰爭勝利。對內，則是利用網路監控軟體，嚴控各項輿論衝突，以確保國家安全。中共網軍編組，除依眾所皆知的總參部三局61398部隊，及7大軍區之通信部隊、電戰部隊及國防科研機關與各級院校，也應包含特戰人力以及2012年成立的「預備役頻譜管制中心」等單位，其中共網軍人數預估約為6萬餘人。另外，中共在2013年投資網路戰資料推估約為1920.35億人民幣，與美國相差約370億人民億。

中共雖積極投入網路戰，且具有龐大的人口擁有電腦及手機，使得戰爭潛力向上提升，並拜世界經濟不景氣，中國政府企圖以花大錢，吸引世界各國網路人材，至中國大陸電子產業服務，並以相關政策，研發各項軟體，拒止外國企進入，以期提供一個實體隔離，確保純淨的網路空間，但中共受限制核心科技現階段仍以美國廠商為主，且網路通訊標準制定、網域、IP等都由美國律定規則，故中共網路戰攻、防能力，僅能以網路削弱及竊取為主要手段，尚未達到可以用網路病毒直接癱瘓敵人網站，其網路戰實力應仍落後歐、美軍事強國。

四、我國網路戰能力評估

我國具有科技小島之稱，尤其在資訊產業核心技術更是領先中共，惟政府對資安防護未能集中管理，雖在2011年3月，成立「行政院資通安全辦公室」，為常態編組，但成效有限，而管理組織分散與預算不足，則是更嚴重問題。例如網路情蒐，分由內政部、法務部、國安局、國防部軍情局致使無法有效掌握，其次是政策以經濟考量，未落實為國家安全。例如2013年服貿協議，協議將手機伺服器後端同意委由中共民間，及2014年我國戶政資訊系統委由資宏拓宏將軟體委由中共廠商，均說明政府在網路安全未能重視。最後，在基礎設施方面，又未能分散部署，雖政府一直推廣雲端概念，想強化資訊安全，而在2014年一個內湖網路機房因施工不慎，造成網路大停擺，反映出基礎設不足。

第二節　研究建議

一、發揮不對稱作戰思維

不對稱作戰思維，不能僅僅是口號形式，而是必須落實在各項戰術戰法上及建軍備戰發展上。在我國各項硬體設備投資及兵力規模均不及中共同時，想要贏得戰爭勝利，確保中共不以武力進犯，發揮不對稱作戰思維更顯重要。如何有效嚇阻、拒止發生戰爭，是當今國家安全必須納入至為重要的思考問題。在當今世界軍事發展上，網路戰被認為最符合損小、效高的作戰模式，因此，我們更應積極投入研究。另者，網路戰跨越領域已涵蓋政治、經濟、交通、能源，當務之急，應將負責單位向上提升，且戰略地位不可侷限於防禦為主。須知網路戰未能先發制勝，戰爭即宣告結束，故網路戰因由國安會主導，國防部為負責單位，並由國安會召集跨部會實施研討，律定未來發展網路戰的攻守模式，而國防部則依循研討結果，完成網路戰攻、防教戰守冊，以作為網軍編組及算獲撥的依據。

二、積極培養網軍人材及增加預算

面對網路戰的挑戰，關鍵因素在於資訊科技及網際網路的核心技術，而技術的發展則在於人力素質，單純成立一支網軍是無法面對現今世網路戰科技挑戰。網軍成員若未經挑選，僅因員額補充而所成立，其戰力將大打折扣。故在網軍人材方面，首先必須向下札根，由國防部主導與教育部合作，結合全民國防教育，藉由各項競賽，深根於高中、職學校，以厚植國內網路戰人材。其次，與國安局、產、官學界合作共同出資，提供國防獎學金，比照 ROTC 模式，鼓勵高中、職競賽得名團隊或個人考取民間頂尖大學接受轉輔，除寒、暑外接受軍事及思想教育，餘均在民間大學學習。畢業後，進入網軍部隊實習及服務。另結合建教合作，以責任區域為劃分，與地區頂尖大學資工、資管系所及軟體公司成立網軍後備部隊。最後，對於網軍人材的待遇必須提高，以留住高科技產業人材，提升整體網路攻防能力。當然，操作網路戰武器的隊員必須絕對忠誠，防止洩露秘密計畫或網路漏洞。此外，網路戰士必須具有不斷提高他們技術熟練程度的強烈願望，來滿足快速變化的技術、程式和作戰限制等方面的具體需求。

另外，我們必須成立網路戰兵科。現行國軍通資電兵科的通識教育，其專業領域無法滿足未來網路戰任務需求。如果能整合各方面資源，再加上現有「國防大學」資訊課程，相信在未來我國網路戰的人才培養上，應可以趕上歐美各軍事強國對網軍的投入。

三、加強網路科技研究

網路戰除人材培育外，研發部門是否可提供高科技的的關技核心，亦至為重要。網路戰已不再是病毒及駭客等手段，很多的關鍵武器如美國的無線電的量子注入，單單一部造價就一千萬美元。故投入充裕的經費，加強網路科技研究也是不可缺。

四、提升網路安全管理層級

此外，資訊、網路安全絕非任何一個部門可以勝任，且不可以多頭馬車，現今美國與中共資安小組的組長均由總統兼任，因此我國在管理階層不能再由行政院部門負責，應提升由總統負責，以確保資安防護。

參考書目

一、中文部份

(一)官方出版品

立法院,《我國如何因應網軍與駭客攻擊並強化資訊安全措施》,《立法院公報》,第 102 卷第 29 期。

行政院研究發展考核委員會,《中共發展「信息戰」及對我國建立資訊安全制度影響之研究》,台北:五南文化出版,2002 年。

行政院研究發展考核委員會,《整合資通安全機制以強化國土安全之研究》,台北:五南文化出版,2005 年。

行政院科技顧問組,《2010 年資安政策白皮書》,(台北:五南文化出版),2010 年。

國防部,中華民國 102 年《四年期國防總檢討》(Quadrennial Defense Review),台北:五南文化出版,2013 年。

國防部,中華民國 93 年《國防報告書》,台北:五南文化出版,2004 年。

國防部,中華民國 102 年《國防報告書》,台北:五南文化出版,2013 年。

(二)專書

丁志宏,《陸軍數字化部隊建設研究》,北京:國防大學出版社,2003 年。

王正德,《決勝賽柏空間-網路軍事技術及其運用》,北京:軍事科學出版社,2003 年。

王保存,《外國軍隊信息化建設的理論與實踐》北京:解放軍出版社,2008 年。

田文輝主編,《韜略談兵-現代戰爭及安全情勢新思維》,台北:青年日報社,2007 年。

江澤民,《江澤民文選一第 3 卷》,北京:人民出版社,2006 年。

李健、嚴美譯,Larry K.wentz、Charles L.Barry、Stuart H. Star,《網路戰美軍稱霸世界的第五戰場》(Military Perspectives on Cyberpower),香港:新點出版公司,2010 年。

李曉、陳乘風、郭鑄文,《鍵與屏的博殺-網路戰掃描》,湖北:科學技術出版社,2003 年。

沈偉光主編,《中國信息戰:知名學者聚焦信息戰權威專家解讀信息化》,北京:新華出版社,2005 年。

沈偉光主編,《信息邊彊-無影無形的第五邊彊》,北京:新華出版社,2003 年。

沈偉光主編,《電子軍務-敲開未來戰爭之門》北京:新華出版社,2003 年。

沈偉光、解璋、馬亞西,《信息化軍隊-未來戰爭的主角》,北京:新華出版社,2003 年。

吳漢平主編,Edward Walts,《信息戰原理與實戰》(Information Warfare: Principles and Operations),北京:電子工業出版社,2004 年。

周宏仁主編、徐愈副主編,《中國信息化形勢分析與預測》,北京:社會科會文獻出版社,2010 年。

林宗達,《中共軍事革新之信息戰與太空戰》,台北:全球防衛雜誌社,2002 年。

東鳥,《中國輸不起的網路戰爭》,北京:中南出版傳媒集團,2010 年。

東鳥,《網路戰爭:互聯網改變世界簡史》,北京:九洲出版社,2009 年。

馬亞西、成冀、王漢水,《網路戰-地球村時代的戰爭》,北京:國防出版社,1999 年。
國防部史政編譯局譯,《2010 美國四年期國防總檢討報告》(Quadrennial Defense Report,QDR),台北:國防部史政編譯局,2010 年。
國防部史政編譯局譯,毛文杰(James C.Mulvenon)、譚睦瑞(Murray Scot Tanner)、蔡斯(Michael S. Chase)、傅里林格(David Frelinger)、龔培德(David C.Gompert)、李比奇(Martin C.Libicki)、包克文(Kevin L. Pollpeter),《中共對美國軍事變革之反應》(Chinese Responses to U.S.Military Transformation and Implications for the Department of Defense),台北:國防部史政編譯局,2010 年。
國防部史政編譯局譯,《中共崛起構成的挑戰-亞洲觀點》(Asian Perspec -tives on the Challenges of China),台北:國防部史政編譯局,2001 年。
國防部史政編譯局譯,史利芙爾(Frank J.Cilluffo),《網路威脅與資訊安全》(Cyber Threats and Information Security),台北:國防部史政編譯局,2002 年。
國防部史政編譯局譯,布里特(Thomas W.Britt)、安德魯(Carl Andrew Castro)、艾德樂(Army B.Adler)《軍事成效》(Military Performance),台北:國防部史政編譯局,2009 年。
國防部史政編譯局譯,甘浩森(Roy Kamphausen),施道安(Andrew Scobell)著,《解讀共軍兵力規模》(Right-Sizing the people'Sliberation Army),台北:國防部史政編譯局,2010 年。
國防部史政編譯局譯,多伊爾(Michase W. Doyle),《第一擊-國際衝突的先制與預防》(Striking First-Preemption and Prevention in International comflict),台北:國防部史政編譯局,2011 年。
國防部史政編譯局譯,艾利諾.史龍(Elinor Sloan),《軍事轉型與當代戰爭》(Military Transformation And Modern Warfare),台北:國防部史政編譯局,2010 年。
國防部史政編譯局譯,佛蘭納根(Stephen J Flanagan)、馬提(Michael E. Marti),《人民解放軍與變動的中國》(The peple's Liberation Army and China in transition),台北:國防部史政編譯局,2005 年。
國防部史政編譯局譯,克里夫(Roger Cliff),《中共商用科技的軍事潛力》(The Military Potential of China's Commercial Technology),台北:國防部史政編譯局,2001 年。
國防部史政編譯局譯,辛巴拉(Stephen J.Cimbala),《美國國家安全》(U.S.National Security),台北:國防部史政編譯局,2005 年。
國防部史政編譯局譯,阿里斯德(Leigh Armistead),國防部史政編譯局譯,《資訊作戰》(Information Operation Matters),台北:國防部史政編譯室,2012 年。
國防部史政編譯局譯,阿里斯德(Leigh Armistead),國防部史政編譯局譯,《資訊作戰-以柔克剛的戰爭》(Information Operations Warfare and the Hard Reality of Soft Power),台北:國防部史政編譯室,2008 年。
國防部史政編譯局譯,阿瑞(Guy Ben-Ari)、趙(Pierre A.Chao),《因應複雜的世界-發展明日國防與網狀化系統》(Organizing for a Complex World –Developing Tomorrow's Defense and Net-Centric systems),台

北:國防部史政編譯局，2010 年。
國防部史政編譯局譯，哈特(Gary Hart)，《第四種國力-美國廿一世紀的大戰略》(The Fourth Power-A Grand Strategy for the United States in the twenty-first Century)，台北:國防部史政編譯局，2008 年。
國防部史政編譯局譯，奎斯特(George H.Quester)，《國際體系的攻擊與防禦》(Offense and Defense in the International System)，台北:國防部史政編譯局，2004 年。
國防部史政編譯局譯，科普蘭(Thomas E.Copeland)，《資訊革命與國家安全》(Information Revolution and Natonal Security)，台北:國防部史政編譯局，2001 年。
國防部史政編譯局譯，約翰.阿爾吉拉(John Arquila)、大衛.朗斐德(David Ronfeldt)，《網路及網路戰》(Networks and Netars:The Future of Terror,Crime,And Militancy)，台北:國防部史政編譯局，2003 年。
國防部史政編譯局譯，麥艾文(Evan S Medeiros)，《中共的國際行為》(China's International Behavior)，台北:國防部史政編譯局，2011 年。
國防部史政編譯局譯，費根保 (Evan A. Feigenbaum)，《中共科技先驅:從核子時代到資訊時代的國家安全與戰略競爭》(China's Techno-warriors National Security and Strategic Competition from the Nuclear to the Information age)，台北:國防部史政編譯局，2006 年。
國防部史政編譯局譯，費學禮 (Richard D. Fisher Jr.)，《中共軍事發展-區域與全球勢力佈局》(China's Military Modernization- Building for Regional and Global Reach)，台北:國防部史政編譯局，2011 年。
國防部史政編譯局譯，賈斯伯 (Scott Jasper)，《國防能力轉型-國防安全新策略》(Transforming Defense Capabilities)，台北:國防部史政編譯局，2012 年。
國防部史政編譯局譯，盧福偉(Bernard Loo)，《軍事轉型與戰略》(Military Transformation and Strategy)，台北:國防部史政編譯局，2011 年。
國防部史政編譯局譯，韓力(Eric L.Haney)、湯姆生(Brian M.Thomsen)《論 21 世紀戰爭超越震撼與威懾》(Beyond Shock and Awe: Warfare in the 21st Century)，台北:國防部史政編譯局，2010 年。
崔國平主編，《國防信息安全戰略》，北京:金城出版社，2000 年。
張春江、倪健民主編，《國家信息安全報告》，北京:人民出版社，2000 年。
張軍主編，《IT 戰爭》，北京:科學出版社，2000 年。
張蜀平、禚法寶、王祖文，《直面信息化戰爭》，北京:國防工業出版社，2007 年。
張黎，《構建信息化軍隊的組織體制》，北京:解放軍出版社，2004 年。
曹正榮、吳潤波、孫建軍，《信息化聯合作戰》，北京:解放軍出版社，2006 年。
曹峻、楊慧、楊麗娟，《全球化與中國國家安全》北京:社會科學文獻出版社，2008 年。
曹雄源，《美國國防暨軍事戰略》，桃園:國防大學，2008 年。
曹雄源，《戰略透視:冷戰後美國層級戰略體系》，台北:五南圖書出版社，2013 年。
曹雄源，《戰略解碼:美國國家安全戰略的佈局》，台北:五南出版社，2013

年。
曹雄源、廖舜石譯,《布希政府時期國家安全戰略》(The National Security Strategy of The United States of America,2002、2006),桃園:國防大學,2008 年。
曹雄源、廖舜石譯,《全球戰略觀察》,桃園:國防大學戰略研究所,2008 年。
曹雄源、廖舜石譯,《柯林頓政府時期:全球時代的國家安全戰略》(A National Security Strategy for A Global Age,2000),桃園:國防大學,2008 年
曹雄源、廖舜石譯,《柯林頓政府時期:接觸與擴大的國家安全戰略》(A National Security Strategy of Engagement and Enlargement 1995、1996),桃園:國防大學,2008 年。
曹雄源、廖舜石譯,《柯林頓政府時期:新世紀的國家安全戰略》(A National Security Strategy for New Century 1997、1998、1999),桃園:國防大學,2008 年。
喬良、王湘穗,《超限戰》,台北:左岸文化出版社,2004 年。
楊世松,《軍事信息能力論論》,北京:軍事科學出版社,2007 年。
載清民,《直面信息戰》,北京:國防大學出版社,2002 年。
劉天竺,《中共正在輸掉的戰爭》,北京:明鏡出版社,2010 年。
劉台平,《島計畫-2008 年中共發動對台割喉戰》,北京:時英出版社,2004 年。
劉俊英主編,《中共研究》(China Studies)彙編,台北:國防部部長辦公室,2006 年。
劉威麟,《網路紅事件》,台北:大塊文化出版社,2009 年。
劉偉,《信息化戰爭作戰指揮研究》,北京:國防大學出版社,2009 年。
劉慶元,《解析中共國家安全戰略》,台北:揚智文化出版社,2003 年。
潘小剛、周亞明、肖琳子,《中國信息安全報告-預警與風險化解》,北京:紅旗出版社,2009 年。
蔡翼主編,《崛起東亞-聚焦新世紀解放軍》,台北:勒巴克顧問出版社,2009 年。
戴旭,《2030 肢解中國?美國的全球戰略和中國的危機》,香港:新點出版公司,2010 年。

(三)期刊論文

王文勇譯,亞歷山大(David Alexander),〈網路防衛戰略方案〉(A SDI for Cyberspace),《國防譯粹》,第 40 卷,第 9 期,2013 年 9 月,頁 53-57。
左少雄,〈中共信息戰與我國通資安全應變機制之研究〉,《陸軍學術月刊》,第 40 卷,第 461 期,2004 年 1 月,頁 32-42。
余忠勇譯,杜迪克(Charles E. Dudik),波爾格(Jesse Bourque),〈電子戰與網路作戰:未來聯合兵種〉(Electronic Warfare and Cyber Operations),《國防譯粹》,第 40 卷,第 11 期,2013 年 11 月,頁 23-27。
余忠勇譯,奧本海默(Andy Oppenheimer),〈網路戰-對抗無聲的大規模毀滅性武器〉(Fighting the Quiet WMD-Cyber-Warfare),《國防譯粹》,第 39 卷,第 8 期,2012 年 8 月,頁 26-32。
李永悌,蘭貝斯(Benjamin S.Lambeth),〈空權、太空權與網路權〉

（Airpower、Spacepower,and cyberpower），《國防譯粹》，第 38 卷，第 4 期，2011 年 4 月，頁 12-31。
李育慈譯，克勒(Mara Koehler)，〈得不償失:九一一事件對中共戰略環境的衝擊〉（The Effects of 9/11 on China's Strategic Environment:lllusive Gains and Tangible Setbacks），《國防譯粹》，第 40 卷，第 10 期，2013 年 10 月，頁 4-15。
李育慈譯，哈姆斯(T.X.Hammes)，〈近海管制:因應中(共〉可能衝突的遠慮深計〉（Offshore Control:A Proposed Strategy for an Unlikely Conflict），《國防譯粹》，第 39 卷，第 10 期，2012 年 10 月，頁 7-23。
李泇鋐譯，高井(Teri Takai)，〈更靈活的國防資訊能力〉（Creating a More Agile Defense Department info-Tech Enterprise），《國防譯粹》，第 39 卷，第 8 期，2012 年 8 月，頁 36-38。
辛毅，〈電子信息裝備軍民融合式發展的思考〉，《國防》，第 3 期，2013 年，頁 10-13。
周敦彥譯，布姆加納(John Bumgarner)，〈確保網路安全:重新思考新防禦時代之軍事準則〉（Securing the Cyber Sphere: Rethinking Military Doctrine for A New Defense Era），《國防譯粹》，第 39 卷，第 8 期，2012 年 8 月，頁 33-35。
周敦彥譯，湯馬斯(Thomas Henderschedt)，〈共軍資訊化作戰之借鏡〉（Learn from the PLA)，《國防譯粹》，第 39 卷，第 10 期，2012 年 10 月，頁 29-35。
林宗達，〈中共信息戰之「網軍」作戰初探〉，《展望與探索》，第 5 卷，第 9 期，2007 年 9 月，頁 60-84。
林宗達，〈中共信息戰發展之評估〉，《中共研究》，第 36 卷，第 7 期，2002 年 7 月，頁 43-59。
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 27 卷，第 4 期，2012 年 7 月，頁 87-101。
林穎佑，〈大陸網軍與 APT 攻擊〉，《展望與探索》，第 11 卷，第 3 期，2013 年 3 月，頁 95-110。
昌業庭，〈以十八大精神為指導 在新的起點上推進國防動員建設科學發展〉，《國防》，第 2 期，2013 年，頁 12-15。
高一中，成斌(Dean Cheng)，〈中共對嚇阻的觀點〉（Chinses Views on Deterrence），《國防譯粹》，第 38 卷，第 4 期，2011 年 4 月，頁 50-55。
高一中譯，巴坎(Kris E.Barcomb)，〈從海權到網權:以史為鑑勾革未來的戰略〉（From Sea Power to Cyber Power: Learning from the Past to Craft a Strategy for the Future），《國防譯粹》，第 41 卷，第 2 期，2014 年 2 月，頁 29-37。
高一中譯，帕克(G.Stavridis and Elton C.Parker)，〈航向網路之海〉(Sailing the Cyber Sea)，《國防譯粹》，第 39 卷，第 8 期，2012 年 8 月，頁 4-14。
高一中譯，馬格努森(Stew Magnuson)，〈阻絕中共駭客狂襲〉(Stopping the Chinese Hacking Onslaught)，《國防譯粹》，第 40 卷，第 2 期，2013 年 2 月，頁 73-78。
高一中譯，奧爾森(Soren Olson)，〈檯面下較勁:網路戰與戰略經濟攻擊〉(Shadow Boxing: Cyber Warfare and Strategic Economic Attack)，《國防

譯粹》，第 39 卷，第 12 期，2012 年 12 月，頁 42-49。
高光耀、鄭從卓，〈我國光網城市建設的主要問題及對策研究〉，《未來與發展》，第 4 期，2013 年，頁 2-6。
洪志安、王官德，〈轉型中之中共陸軍〉，《陸軍學術雙月刊》，第 532 期，2013 年 12 月，頁 44-61。
范宏武，〈從中共信息戰發展概況論第三波戰爭概念建構及發展之重要性〉，《大直高中學報》，第 4 期，2007 年 6 月，頁 123-158。
唐仁俊，〈中共信息戰之發展與限制〉，《空軍學術雙月刊》，第 619 期，2010 年 10 月，頁 26-40。
孫國祥，〈具有中國特色社會主義的複雜訊息〉，《中共研究》，第四十七卷，第八期，2013 年 7 月，頁 4-18。
袁平譯，南麗(Nan Li)，〈中共擴張海權之企圖〉(Scanning the Horizon for "New Historical Missions")，《國防譯粹》，第 37 卷，第 12 期，2010 年 12 月，頁 85-92。
張淑中，「中國大陸軍事及科技發展的全球戰略意涵分析」，《中共研究》，第 47 卷第 10 期，2013 年 10 月，頁 101-116。
戚魯江，〈美國國會網路安全立法探析〉，《中國人大》，第 340 期，2013 年 8 月，頁 51-52。
梁正綱譯，哈米迪(Ahmad Zahid Hamidi)，〈新戰爭型態:網路結合無人飛行載具與新興威脅〉(New Forms of Warfare: Cyber, UAVs and Emerging Threats)，《國防譯粹》，第 40 卷第 11 期，2013 年 11 月，頁 42-45。
陳嘉容譯，埃爾南德斯(Rhett A.Hernandez)，〈美陸軍在網際空間的全方位策略〉(Preparing the Army to Prevent,Shape and Win in Cyberspace)，《國防譯粹》，第 41 卷，第 1 期，2014 年 1 月，頁 4-8。
陳漢強、蘇文德，〈中共信息戰之網路攻擊型態研究〉，《新新季刊》，第四十卷，第二期，2012 年 4 月，頁 235-240。
章昌文譯，巴雷特(Danelle Barrett)、卡斯蒂略(Jesse Castillo)，〈訓練官兵網路戰力〉(Creating Cyber Warriors)，《國防譯粹》，第 40 卷，第 4 期，2013 年 4 月，頁 47-51。
章昌文譯，法加迪(David Faggard)，〈風起雲湧的社會運動:不對稱衝突的隱憂〉(Social Swarming: Asymmetric Effects on Public Discourse in Future Conflict)，《國防譯粹》，第 40 卷，第 10 期，2013 年 10 月，頁 43-55。
章昌文譯，紐美勒(Kevin P.Newmeyer)，〈誰該主導美國的網路安全作為〉(Who Should Lead U.S Cybersecurity Efforts？)，《國防譯粹》，第 39 卷，第 8 期，2012 年 8 月，頁 15-25。
章昌文譯，菲利普斯(Kyle Genaro Phillips)，〈武裝衝突法足以適用網路戰爭〉(Unpacking Cyberwar:The Sufficiency of the Law of Armed Conflict in the Cyber domain)，《國防譯粹》，第 41 卷，第 1 期，2014 年 1 月，頁 21-28。
章昌文譯，歐文(Sandra I.Erwin)，〈國家安全未來五大威脅〉(The Five Treats To National Security in the Coming Decade)，《國防譯粹》，第 40 卷，第 2 期，2013 年 2 月，頁 42-54。

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 526 期，2012 年 12 月，頁 4-20。
童光復譯，賈斯伯(Scott Jasper)，〈美國與中共的網路戰爭〉(Are US and Chinese Cyber Intrusions So Different)，《國防譯粹》，第 40 卷，第 12 期，2013 年 12 月，頁 76-81。
黃文啟，克拉克(Balne R.Clark)，〈以資訊戰做為武裝衝突嚇阻手段〉(Information Operations as a Deterrent to Armed Conflict)，《國防譯粹》，第 37 卷，第 12 期，2010 年 12 月，頁 4-13。
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 17-28。
黃基禎，〈中國大陸網路戰思維〉，《中共研究》，第 47 卷，第 10 期，2013 年 10 月，頁 147-151。
黃淑芬譯，成斌(Dean Cheng)，〈共軍特種作戰〉(The Chinese People's Liberation Army and Special Operations)，《國防譯粹》，第 39 卷，第 12 期，2012 年 12 月，頁 87-92。
楊黎中譯，格蘭特(Rebecca Grant)，〈鑑往知來的網路安全與發展〉(Old Lessons,"New"Domain:The Air Force Can Learn A Lot from What It Has Already Seen in Cyberspace)，《國防譯粹》，第 41 卷，第 1 期，2014 年 1 月，頁 48-55。
謝台喜，〈中共太空發展對我之威脅與因應作為〉，《陸軍學術雙月刊》，第 526 期，2012 年 12 月，頁 21-34。
謝游麟，〈國軍發展「不對稱」軍事思想之途徑與實踐〉，《國防雜誌》，第 27 卷第 4 期，2012 年 7 月，頁 51-64。
龐小寧，〈政府危機管理中的網路謠言控制研究〉，《未來與發展》，第 4 期，2013 年，頁 12-15。

(四)碩博士論文

李承瑀，《中共高技術條件下信息戰之研究》，政治作戰學校政治研究所碩士論文，2000 年 6 月。
陳憶綾，《解放軍資訊戰對台軍事安全影響之研究》，政治作戰學校政治研究所碩士論文，2006 年 6 月。
黃鈴，《「信息化戰爭條件」下之共軍對台戰略》，政治作戰學校政治研究所碩士論文，2005 年 6 月。

(五)週刊、雜誌

山本進一、平可夫，〈中國陸軍數據鏈 使用更多加固式電腦〉，《漢和防務評論》，第 101 期，2013 年 3 月，頁 49。
于揚，〈中國裝力量的多樣化運用白皮書 vs 中國軍力報告〉，《亞太防務》，第 63 期，2013 年 1 月，頁 30-35。
史可夫，〈中國在西藏建設監聽站〉，《漢和防衛》，第 93 期，2012 年 7 月，頁 36-37。
史可夫，〈中國建設監聽站〉，《漢和防務評論》，第 93 期，2012 年 7 月，頁 45-48。
史可夫，〈中國軍事力量的世界延伸範圍〉，《漢和防務評論》，第 96 期，2012 年 10 月，頁 47-48。
史可夫，〈中國軍隊正式成立駭客部隊〉，《漢和防務評論》，第 87 期，2012

年 1 月，頁 23-25。
毛峰，〈日本創建網軍聯美反制中國〉，《亞洲週刊》，第 27 卷第 21 期，2013 年，6 月，頁 36-37。
毛峰，〈日美軍事同盟遏制中國崛起〉，《亞洲週刊》，第 27 卷第 41 期，2013 年，10 月，頁 32-33。
李少弘，〈從美國軍力發展看 2013-2023 中共軍事能力〉，《尖端科技》，第 352 期，2013 年，12 月，頁 34-41。
李建，〈美國實施網路威攝戰略試圖遏制中國大陸網戰力量〉，《尖端科技》，第 344 期， 2013 年 4 月，頁 26-27。
李貴發，〈2023 年東亞軍事情勢分析之二〉，《尖端科技》，第 351 期，2013 年，11 月，頁 14-20。
沙沙，〈美軍亟思壓制「解放軍之眼」〉，《亞太防務》，第 56 期，2012 年，12 月，頁 34-35。
沙沙，〈網路版朝鮮戰爭爆發-兩韓網路戰對抗升級〉，《亞太防務》，第 61 期，2013 年 3 月，頁 22-27。
余揚，〈中國戰術導彈威懾美日〉，《遠望》，第 292 期，2013 年 1 月，頁 47-51。
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》，第 311 期，2010 年 7 月，頁 90-92。
林郁方，〈2013 年國防預算剖析〉，《亞太防務》，第 56 期，2012 年，12 月，頁 4-5。
昊銘，〈”.CN”攻擊疑犯已從國外帶回〉，《瞭望東方周刊》，第 2 期，2014 年 1 月 9 日，頁 37。
昊銘，〈黑客關注中國 600 個網站〉，《視野》，16 期，2013 年 8 月，頁 17-18。
昊銘，〈境外對華網路攻擊報告〉，《瞭望東方周刊》，第 30 期，2013 年 8 月 8 日，頁 17。
約翰(Juhn chang)，〈中國信息安全發展現況〉，《漢和防衛》，2013 年 9 月，頁 44-45。
倪耿，〈台式不對稱作戰與戰力組合〉，《亞太防務》，第 63 期，2013 年 1 月，頁 36-41。
倪耿，〈追求台海軍事穩定台式不對稱與戰力組合〉，《亞太防務》，第 2 期，2012 年 1 月，頁 37-40。
徐佳，〈網軍來襲，新一代國防戰開打〉，《數位時代》，第 228 期，2013 年，5 月，頁 91-92。
徐海濤、鮑曉菁，〈我國首台基於龍芯 3B 的萬億次高性能電腦研制成功〉，《遠望》，第 293 期，2013 年 2 月，頁 3。
柴惠珍譯，Shame Harris 著，〈中共網軍〉，《陸軍軍事譯粹選輯》，第十八輯，2008 年 5 月，頁 726-725
張雯、姚曉天，〈美國電子監控細節曝光〉，《亞洲週刊》，第 27 卷第 25 期，2013 年，6 月，頁 32。
梁華傑，〈資訊時代戰場如何優劣轉換及以小搏大〉，《尖端科技》，第 352 期，2013 年，12 月，頁 93-97。
梁華傑，〈奪取制網路權 搶先制定網路戰規則〉，《尖端科技》，第 351 期，2013 年，11 月，頁 51-55。

畢誠斌，〈史諾登洩密案有如網路戰 911〉，《尖端科技》，347 期，2013 年 4 月，頁 4-5。
莆勛、區肇威，〈美國在亞太區域的不對稱作戰〉，《軍事連線》，第 52 期，2012 年，12 月，頁 61-68。
新華網，〈習近平:科技是國家強盛之基〉，《遠望》，第 299 期，2013 年 8 月，頁 4。
楊欣霖，〈跟著新政策賺錢去〉，《數位時代》，第 22 期，2013 年，2 月，頁 48-49。
載政龍，〈中共網軍發展與網路攻防:兼論我國資通安全之政策規劃〉，《戰略評估》，第四卷第四期，2012 年冬季，頁 97-120。
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 11 月，頁 1-5。
趙郁竹，〈一把火，燒出台灣網路建設隱憂〉，《數位時代》，第 228 期，2013 年，5 月，頁 114-115。
趙郁竹，〈全球瘋 4G，台灣怎麼走〉，《數位時代》，第 222 期，2012 年，11 月，頁 166-168。
齊先予，〈大陸網癱「秦始皇」賊喊捉賊〉，《新紀元》，第 363 期，2014 年 1 月 30 日，頁 46-48。
編輯部，〈中國軍隊在西藏的部署與軍事訓練〉，《漢和防衛》，第 103 期，2013 年 5 月，頁 56-62。
編輯部，〈中國對印度、阿富汗的作戰準備南疆軍區兵力部署〉，《漢和防衛》，第 103 期，2013 年 5 月，頁 51-55。
鄭文浩、楊雷，〈網路戰比核彈威脅更大〉，《瞭望東方周刊》，第 47 期，2013 年 12 月 12 日，頁 39-43。
鄭宇欽，〈北約未來的軍事重心:網路、核生化與能源安全〉，《尖端科技》，第 340 期，2012 年 12 月，頁 35-39。
蘇武，〈強龍利爪 不可低估的中國軍事力量〉(China's Military Forces)，《亞太防務》，第 56 期，2012 年，12 月，頁 36-41。

（六）報紙

〈Twiiter 也遇駭 25 萬用戶資料遭竊〉，《中國時報》，2013 年 2 月 3 日，版 11
中央社紐約，〈避免誤解 傳美曾對中共說明網攻計畫〉，《青年日報》，2014 年 4 月 8 日，版 5。
王光慈，〈國防部第 4 支網路中隊成軍〉，《聯合報》，2013 年 4 月 30 日，版 11。
王光磊，〈美軍與塔利班新戰場-社群網站〉，《青年日報》，2012 年 9 月 5 日，版 6。
王光磊，〈美智庫預算兵推 航艦、陸軍優歌〉，《青年日報》，2013 年 2 月 18 日，版 5。
王光磊，〈美網路戰預算倍增〉，《青年日報》，2011 年 11 月 9 日，版 5。
王光磊，〈駭客攻擊雷達網路 抗駭新時代國防要務〉，《青年日報》，2013 年 2 月 29 日，版 5。
王超群，〈中美網路軍演 資安全作又較勁〉，《旺報》，2012 年 4 月 19 日，版 8。

王銘義，〈美隨時可以把陸打回石器時代〉，《中國時報》，2014 年 1 月 23 日，版 13。
尹曉春，〈磋商網安議題 中美取得共識〉，《台灣醒報》，2013 年 4 月 25 日，版 3。
〈共軍網頻繁 美網戰單位擬升級〉，《青年日報》，2012 年 9 月 30 日，版 5。
〈全球網路監控 敘中最嚴重〉，《青年日報》，2013 年 3 月 13 日，版 5。
白德華，〈習近平領軍 網路安全成國家戰略〉，《中國時報》，2014 年 2 月 28 日，版 22。
朱建陵，〈紐時:美國安局駭進華為竊密〉，《中國時報》，2014 年 3 月 25 日，版 13。
李治安，〈駭客無任務〉，《自由時報》，2014 年 2 月 21 日，版 21。
李宗祐，〈台灣 340 萬次/天網路攻擊〉，《中國時報》，2013 年 8 月 30 日，版 8。
李奕明、劉時均、鄧桂芬，〈詐團吸收同袍 LINE 拍圖傳軍情〉，《聯合報》，2014 年 5 月 9，版 12。
李登科，〈網路攻擊威脅日增 慎防無聲戰爭〉，《青年日報》，2012 年 4 月 14 日，版 2。
吳明杰，〈癱敵網路 軍方擬研發脈衝武器〉，《中國時報》，2012 年 9 月 3 日，版 4。
林克倫、賴錦宏、李春，〈大陸維穩預算 連 3 年高出軍費〉，《聯合報》，2013 年 3 月 6 日，版 13。
林秉學，〈專家警告 智慧網路武器將興起〉，《青年日報》，2012 年 6 月 9 日，版 5。
林政忠，〈駭客攻擊對象 台灣居世界之冠〉，《聯合報》，2013 年 3 月 25 日，版 8。
林詩萍，〈學者:服貿開放網路電信.國安資訊都淪陷〉，《自由時報》，2013 年 8 月 16，版 6。
林翠儀，〈攔截中國情資？日拒美監亞太海底光纜〉，《自由時報》，2013 年 10 月 28 日，版 10。
邱燕玲，〈網路戰爭時代 陳撥促部會警覺〉，《自由時報》，2012 年 12 月 21 日，版 6。
俞智敏，〈伊朗網路劫機？陰謀論 滿天飛〉，《自由時報》，2014 年 3 月 18 日，版 8。
俞智敏，〈監控九萬留澳生 中國廣布情報網〉，《自由時報》，2014 年 4 月 22 日，版 13。
洪健元，〈軍費投注不對稱戰爭、電磁武器、網路戰〉，《青年日報》，2014 年 3 月 21 日，版 5。
姜翔、羅添斌，〈治安國安隱憂 784 中國人非法滯台〉，《自由時報》，2014 年 3 月 3，版 1。
胡蔥寧，〈無疆界記者:美英網路監控 不輸中俄〉，《自由時報》，2014 年 3 月 13 日，版 10。
崔敬熙，〈防網攻 美網軍 2016 年擴編至 6 千人〉，《青年日報》，2014 年 3 月 30 日，版 5。

張佑生，〈美聯社遭駭 美股2分鐘跌144點〉，《聯合報》，2013年4月25日，版17。
張沛元，〈上海交大遭爆與解放軍駭客部隊合作〉，《自中時報》，2013年3月25日，版12。
張玲玲，〈中共管控網際網路 對內維穩對外情蒐〉，《青年日報》，2014年3月9日，版7。
〈習近平對天河二號超級電腦系統研制成功作出重要批示〉，《解放軍報》（北京），2013年6月19日，版1。
曹郁芬、林翠儀譯，〈美國防部:中國軍事力及意圖不透明〉，《自由時報》，2014年3月6日，版3。
曹郁芬，〈美官員:解放軍抗美 信心大增〉，《自由時報》，2014年2月1日，版6。
陳文嬋，〈手機間碟軟體 傳通簡訊就監控〉，《自由時報》，2012年12月20日，版5。
陳伃軒、林翠儀，〈威脅四鄰 中國擴武 軍費4兆〉，《中國時報》，2014年3月6日，版13。
陳伃軒，〈烏克蘭實彈鎮壓 死傷逾600人〉，《自由時報》，2014年2月21日，版18。
陳思豪，〈共軍轉型要裁80萬人〉，《聯合報》，2011年4月23日，版15。
陳柏廷，〈封殺美產品 陸際出網安審查〉，《中國時報》，2014年5月23日，版22。
陳家倫，〈陸首支資訊化旅〉，《旺報》，2014年3月18日，版6。
陳曼濃，〈軍事革命浪潮 生化戰將登場〉，《旺報》，2014年1月14日，版8。
陳清泉，〈網路冷戰下的資訊安全戰略〉，《蘋果日報》，2013年3月25日，版15。
陳維真，〈中國數位人民戰爭 全民抗美〉，《自由時報》，2013年8月1日，版AA2。
陳慰慈、蔡亞樺、吳柏軒、甘芝美、陳慧萍、陳彥廷，〈新戶政程序轉包中國資安系統門戶大開〉，《自由時報》，2014年2月20日，版7。
許博淳，〈國軍落實資安維護 確保國防安全〉，《青年日報》，2012年12月23日，版4。
黃一翔，〈政院研擬組織型網駭攻擊因應方案〉，《青年日報》，2012年12月23日，版4。
黃一翔，〈面對網路戰爭陳揆指示速擬對策〉，《青年日報》，2012年12月20日，版1。
黃文正，〈你的手機可能正被美追縱〉，《中國時報》，2013年12月6日，版22。
黃文正，〈美國安局研發量子電腦 破解加密〉，《中國時報》，2014年元月4日，版19。
黃德潔，〈中共持續關注 美日亞太軍力發展〉，《青年日報》，2014年1月2日，版5。
馮克芸，〈美兵推模擬 台遭中共封銷〉，《聯合報》，2011年12月9日，版19。

馮克芸，〈美軍網路武器 總統才能發動〉，《聯合報》，2013 年 2 月 6 日，版 14。
彭顯均，〈馬坦承:對中開放 駭台更多〉，《自由時報》，2013 年 4 月 2 日，版 4。
曾復生，〈習近平的戰略時間表〉，《中國時報》，2014 年 1 月 25 日，版 16。
楊智強，〈資安等級低 立委促成國土安全部〉，《台灣醒報》，2013 年 4 月 30 日，版 2。
楊湘鈞、蘇瓊璇、陳乃綾，〈張善政:攻擊屬「非常嚴重」〉，《聯合報》，2014 年元月 10 日，版 6。
楊舒媚，〈新戶政系統 轉包中國網路公司〉，《中國時報》，2014 年 3 月 11 日，版 11。
湯雅雯，〈台灣首枚太空 GPS 2018 年升空〉，《中國時報》，2014 年 2 月 26，版 6。
管淑平，〈美起訴解放軍 中國暫停網路合作〉，《自由時報》，2014 年 5 月 21 日，版 10。
管淑平，〈無線電波植間碟美滲透 10 萬電腦〉，《自由時報》，2014 年元月 16 日，版 9。
管淑平，〈華為替南韓建 4G 美憂情資外洩〉，《自由時報》，2013 年 12 月 5 日，版 15。
劉屏、朱建陵，〈美政府告解放軍 5 軍官〉，《中國時報》，2014 年 5 月 20 日，版 1。
劉榮，〈嚴密管控機制反制網軍入侵〉，《青年日報》，2007 年 10 月 22 日，版 3。
編譯組，〈俄軍入侵 克里米亞遭網攻〉，《青年日報》，2014 年 3 月 6 日，版 6。
編譯組，〈美韓機密通訊〉，《青年日報》，2014 年 2 月 23 日，版 5。
蔡筱雯，〈谷歌董座批中國老練駭客〉，《蘋果日報》，2013 年 2 月 3 日，版 23。
鄭光華，〈強化網路防衛體系有效反制中共網軍攻勢〉，《青年日報》，2007 年 12 月 21 日，版 3。
鄭德麟，〈我應積極建立總體防衛體系〉，《青年日報》，2008 月 11 月 22 日，版 3。
鄧智原，〈強化資訊安全保障國土防衛〉，《青年日報》，2008 年 9 月 17 日，版 3。
〈鞏固第 5 戰場 美日將聯手防駭〉，《青年日報》，2014 年 1 月 28 日，版 5。
盧永山，〈去年駭客網攻三成中國幹的〉，《自由時報》，2013 年 4 月 25 日，版 5。
盧素梅，〈陸聯戰指揮改革估 2020 年完成〉，《旺報》，2014 年 1 月 7 日，版 6。
蕭示恩，〈符合戰略需求提升國家競爭力長役期發揮戰力-裨益國家發展需求〉，《青年日報》，2012 年 1 月 9 日，版 1。
賴昭穎，〈2015 年前美將組 40 支網路部隊〉，《聯合報》，2013 年 3 月 25

日，版 8。
賴昭穎，〈中共政治作戰 台灣是首要目標〉，《聯合報》，2013 年 10 月 23 日，版 13。
賴錦宏，〈央視畫面 驚見對台作戰地圖〉，《聯合報》，2013 年 10 月 14 日，版 13。
鍾翠珠，〈國防部也受駭 網路安全陷危機〉，《民眾日報》，2014 年 3 月 3，版 2。
簡竹君，〈美爆史上最大監控每天蒐 50 億筆手機資訊〉，《蘋果日報》，2013 年 12 月 6 日，版 28。
藍孝威，〈習領軍信息化小組 因應資訊戰〉，《中國時報》，2014 年 1 月 23 日，版 13。
魏國金，〈反擊中國駭客 美將先發制人〉，《自由時報》，2013 年 2 月 6 日，版 10。
魏國金，〈美海軍網路司令 將掌國安局〉，《自由時報》，2014 年 2 月 1 日，版 10。
魏國金，〈美國安局日蒐 50 億筆手機位置資料〉，《自由時報》，2013 年 12 月 6 日，版 29。
羅印沖、陳秀蘭、黃淑嫆，〈軍費近 4 兆 陸強化海空二炮〉，《旺報》，2014 年 3 月 6 日，版 C1。
蘇芳禾，〈電信業開放 業者:像木馬屠城〉，《自由時報》，2013 年 10 月 3 日，版 5。
羅添斌，〈中對台導彈民進黨評估 2025 年增至 1850 枚〉，《自由時報》，2014 年 3 月 3，版 4。
羅添斌，〈反制中國網軍我建構網路戰攻防驗測環境〉，《自由時報》，2012 年 9 月 2 日，版 6。
羅添彬，〈反制中國 軍方發展無人攻擊機〉，《自由時報》，2012 年 9 月 3 日，版 1。
羅添斌，〈防紅色駭客美禁官方買中國網通產品〉，《自由時報》，2013 年 4 月 28 日，版 2。
羅添彬，〈國防科技研發預算低 奢談發展不對稱戰力〉，《自由時報》，2012 年 9 月 3 日，版 2。
羅添斌，〈強化網攻 國安局招募大學生駭客〉，《自由時報》，2013 年 11 月 12 日，版 6。
羅添彬、曾韋禎，〈軍方總機外包喊卡〉，《自由時報》，2013 年 1 月 10 日，版 4。

（七）網路資料

〈中共中央軍委主席江澤民、中央軍委副主席胡錦濤參加十屆全國人大二次會議解放軍代表團全體會議發表講話內容〉，《解放軍報》，http:big5.xinhuanet.com/gate/big5/news.xinhuanet.com/newscenter/2004-03/11/content_1360725.htm(2014 年 2 月 11 日)。
〈中國政府疑似於十八大期間封鎖境內 Google 服務〉，《行政院國家資通安全會報技術服務中心》，http://www.icst.org.tw/NewsRSSDetail.aspx?seq=14276(2013 年 11 月 10 日)。

中華人民共和國國務院新聞辦公室，〈2006 年中國的國防〉白皮書，《中華人民共和國國防部》，http://www.mod.gov.cn/affair/2011-01/06/content_4249948_6.htm(2014 月 1 月 10 日)。

中華人民共和國國務院新聞辦公室，〈2008 年中國的國防〉白皮書，《中華人民共和國國防部》，http://www.mod.gov.cn/affair/2011-01/06/content_4249949.htm(2014 年 1 月 10 日)。

中華人民共和國國務院新聞辦公室，〈2010 年中國的國防〉白皮書，《中華人民共和國國防部》，http://www.mod.gov.cn/reports/201101/bpsz/2011-03/31/content_4235224.htm>(2014 年 1 月 10 日)。

中華人民共和國國務院新聞辦公室，〈中國武裝力量的多樣化運用〉，《中華人民共和國國防部》，http://www.mod.gov.cn/affair/2013-04/16/content_4442839_4.htm(2014 年 1 月 10 日)。

中華人民共和國國務院新聞辦公室，〈中國統計年鑑 2013〉，《中華人民共和國國家統計局》，http://www.stats.gov.cn/tjsj/ndsj/2013/indexch.htm> (2014 年 3 月 21 日)。

王珮華，〈中國騰訊 APP 微信今登台 台灣即時通中國可掌控〉，《自由時報電子報》http://www.libertytimes.com.tw/2012/new/oct/18/today-fo1.htm(2014 年 3 月 21 日)。

〈以色列成立駭客學校：推崇真刀真槍〉，《中國安全網》(securitycn)，http://www.securitycn.net/html/news/colligation/8691.html(2014 年 3 月 10 日)。

〈行政院年度資安稽核結果首度公開〉，《行政院國家資通安全會報技術服務中心》http://www.icst.org.tw/NewsRSSDetail.aspx?seq=14672&lang=zh(2014 年 3 月 21 日)。

技術服務中心整理，〈Cisco、Linksys 與 Netgear 的無線路由器存有後門〉，《行政院國家資通安全會報技術服務中心》，http://www.icst.org.tw/NewsRSSDetail.aspx?seq=14698(2014 年 3 月 21 日)。

余采霏，〈資安人才難覓 台灣應急起直追〉，《網管人》，http://www.netadmin.com.tw/article_content.aspx?sn=1005200015(2014年3月20日)。

吳明杰、邱燕玲，〈我神秘網軍 首度秀戰力〉，《自由時報》http://www.libertytimes.com.tw/2013/new/may/31/today-fo1.htm (2014 年 3 月 21 日)。

林頂杜(Dindo Lin)，〈卡巴斯基 CEO 爆料:俄國太空站與核電廠曾遭病毒入侵〉，《科技新報》，http://technews.tw/2013/11/14/kaspersky-ceo-stuxnet- iss -nuclear-plant/(2014 年 2 月 14 日)。

胡光曲，〈全軍預備役電磁頻譜管理中心打造高技術尖兵〉，《華夏經緯網》http://hk.huaxia.com/thjq/jsxw/dl/2013/10/3573880.html(2014 年 3 月 20 日)。

〈科技計畫中央財政撥款綜合情況〉，《中國主要科技指標數據庫》，http://www.sts.org.cn/kjnew/maintitle/MainMod.asp?Mainq=2&Subq=1(2014 年 3 月 21 日)。

〈借口網絡安全 印度或封殺中國微信〉，《中國評論新聞網》http://hk.crntt.com/doc/1025/8/6/4/102586449.html?coluid=0&kindid=0&docid=102586449&mdate=0618105253(2014 年 2 月 11 日)。

〈國防部因應「終統」中共可能採取之威懾武嚇研判及我因應作為專案報告〉，《部會報告》，http://npl.ly.gov.tw/npl/report/950315/19.pdf。(2014 年 1 月 10 日) 。

〈國家資通訊安全發展方案〉，《行政院國家資通安全會報》，http://www.nicst.ey.gov.tw/News_Content3.aspx?n=F7DE3E86444BC9A8&sms=FB4DC0329B2277CF&s=1ACE1B808B9444DF。(2014 年 2 月 10 日)。

陳祐欣，〈現代版木馬屠城 中共以網向全球開戰〉，《看雜誌》http://www.watchinese.com/%E7%9C%8B%E4%B8%AD%E5%9C%8B/2008/280(2014 年 1 月 10 日)

陳曉莉，〈美國國安局以惡意程式滲透全球 5 萬個網路〉，《iThome》，<http://www.ithome.com.tw/itadm/article.php?c=83941>。(2014 年 3 月 10 日)。

曹乙帆，〈小心！目標式網路誤導攻擊增溫〉，《網路資訊》，http://news.networkmagazine.com.tw/classification/security/2013/11/21/60342/>(2014 年 2 月 20 日)。

曾復生，〈美中俄日太空爭霸〉，《旺報》，http://tw.news.yahoo.com/%E7%BE%8E%E4%B8%AD%E4%BF%84%E6%97%A5%E5%A4%AA%E7%A9%BA%E7%88%AD%E9%9C%B8-213000573.html(2014 年 2 月 10 日)。

曾復生，〈美中網路戰略七大高地〉，《財團法人國家政策研究基金會》，http://www.npf.org.tw/post/3/13321(2014年2月10日)。

曾復生著，〈國際網路安全競合情勢剖析〉，《國家政策研究基金會》，<http://www.npf.org.tw/post/2/12290(2014 年 2 月 10 日)。

蔡和穎，〈共軍演訓動態 國防部全程掌握〉，《中央社新聞網》，http://tw.news.yahoo.com/%E5%85%B1%E8%BB%8D%E6%BC%94%E8%A8%93%E5%8B%95%E6%85%8B-%E5%9C%8B%E9%98%B2%E9%83%A8%E5%85%A8%E7%A8%8B%E6%8E%8C%E6%8F%A1-143211709.html(2014年2月10日)。

鄭文浩、王玉山，〈院士：我國網絡基本算不設防 成網絡攻擊最大受害國之一〉，《人民網》http://military.people.com.cn/BIG5/n/2014/0107/c1011-24045169.html (2014 年 3 月 23 日)。

戴定國，〈新新人類戰爭 網軍納入正規部隊〉，《人間福報》，http://www.merit-time.com.tw//NewsPage.asp?unid=306788(2014年3月10日)。

二、英文部份

(一)期刊

Murray, Williamson & Leary,Thomas,"Military Transformation and Legacy forces,"*Joint Force Quarterly*,No.30.Spr. 2002,pp.20～27.

Rid,Thomas,"Cyberwar and Peace,"*FOREIGN AFFAIRS*,No.56.Nov/Dec. 2013,pp.77-85.

(二)網路資料

Cenciotti David,"DISA PARTICIPATES IN ANNUAL EXERCISE FOCUSED ON CYBER OPERATIONS AND DEFENSE",*DISA*,< http://www.disa.mil/News/Stories/2013/Cyber-Flag-Exercise>(2014 年 4 月 20 日).

Cenciotti David,"Third Prototype of China's Stealth Jet Makes Maiden Flight and Shows Improvements",*The Avaitionist*，<http://theaviationist.com/2014/03/02/j-20-3rd-prototype-comparison/>(2014 年 4 月 20 日).

Cheryl Pellerin,"DOD at Work on New Cyber Strategy, Senior Military Advisor Says",*defense*, <hhttp://www.defense.gov/news/newsarticle.aspx?id=120397>。(2014 年 3 月 21 日).

Don Eijndhoven,"The Chilling State of Cyber Affairs", *infosecisland*, <http://www.infosecisland.com/blogview/23248-The-Chilling-State-of-Cyber-Affairs-US-DoD-Report.html>(2014 年 3 月 21 日).

Department of Defense Chief Information Officer, "DoD 8570.01- M:Information Assurance Workforce Improvement Program," *Washington. DC*, 〈http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf〉(2014 年 3 月 20 日).

Department of Defense, "Quadrennlal Defenes Review 2014", *Washington. DC*,〈http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf〉(2014 年 4 月 16).

Jarno **Limnéll,** "Resilience - The way to Survive a Cyber Attack", *infosecisland*, <http://www.infosecisland.com/blogview/23137-Resilience--The-way-to-Survive-a-Cyber-Attack.html>(2014 年 3 月 21 日).

"New Chinese stealth jet built with stolen F-35 component designs",*RT*, < http://rt.com/news/chinese-jet-cyber-espionage-stolen- 718/>（2014 年 4 月 21 日）

PAUL KALLENDER-UMEZU,"Experts:Japan's New Cyber Unit Understaffed, Lacks Skills",*defense*, < http://www.defensenews.com/article/20130709/DEFREG03/307090007/Experts-Japan-s-New-Cyber-Unit-Understaffed-Lacks-Skills>(2014 年 4 月 2 日).

Pierluigi Paganini,"The cyber capabilities of Iran can hit US", *Security Affairs*, <http://securityaffairs.co/wordpress/17064/cyber-warfare-2/the-cyber-c

apabilities-of-iran-can-hit-us.html > (2014 年 2 月 20 日).
" 'Spying Birds': Hackers deface Angry Birds website following NSA revelations",*RT*, < http://rt.com/news/angry-birds-nsa-hackers-374/>2014 年 3 月 16 日）。
"US report:China's cyberwar skills a risk to military",*bbc*, http://www.bbc.co.uk/news/world-asia-china-17308921&prev=/search%3Fq%3Dchina%2Bcyber%2Bability%26biw%3D1229%26bih%3D562(2014 年 3 月 20 日).
Zachary Fryer-Biggs,"Hesitancy Over Cyber Strike on Syrian Air Defense",*defensenews*, <http://www.defensenews.com/article/20130830/DEFREG02/308300017/Cyber-Likely-Afterthought-Syria-Intervention-Plans>（2013 年 12 月 8 日）.

附錄:國內中共網路戰研究出版品統計表,2002-2014

項次	研究題目	著作	出版期刊	發表日期	頁數
1	大陸網軍與APT攻擊	林穎佑	展望與探索	2013.03	頁 95-100
2	中共信息戰之網路攻擊形態研究	陳漢強 蘇文德	新新季刊	2012.04	頁 234-240
3	中共信息戰之發展與限制	唐仁俊	空軍學術雙月刊	2010.12	頁 26-40
4	中共信息戰應用後備動員之研究	王志民	後備動員軍事雜誌	2008.10	頁 49-54
5	中共信息戰之「網軍」作戰初探 The Operation of the Internet Forces on PRC's Information Warfare	林宗達	展望與探索	2007.09	頁 60-84
6	中共信息戰與網路戰結合未來網軍發展之研究	黃俊麟	聯合後勤季刊	2007.8	頁 17-28
7	從中共信息戰發展概況論第三波戰爭概念建構及發展之重要性	范宏武	大直高中學報	2007.06	頁 123-158
8	中共信息戰之人民動員戰力概論	林宗達	中共研究	2006.05	頁 83-103
9	以弱勝強的考量剖析中共信息戰之不對稱戰的戰略考量	林宗達	全球防衛雜誌	2005.8	頁 104-111
10	以弱勝強的考量剖析中共信息戰之不對稱戰的戰略考量	林宗達	全球防衛雜誌	2005.07	頁 94-101
11	2005解放軍圓桌論壇中共信息戰(林宗達)	林宗達	全球防衛雜誌	2005.05	頁 90-93
12	中共信息戰與我國通資安全應變機制之研究	左少雄	陸軍學術月刊	2004.01	頁 32-42
13	中共信息戰略與戰術運用	林宗達	中華戰略學刊	2003.04	頁 97-134

14	試論中共信息戰之發展與我因應作為	陳偉寬	空軍學術月刊	2002.10	頁 3-14
15	中共信息戰發展之評估	林宗達	中共研究	2002.07	頁 43-59
16	中共信息戰的戰略理論=The Strategic Theory of PLA's Information Warfare	林宗達	全球防衛雜誌	2002.05	頁 82-89
17	中共信息戰與太空戰的發展對臺灣的衝擊=The Impact of PRC Electric Warfare	林宗達	全球防衛雜誌	2002.04	頁 45-53
18	中共信息戰之戰略概論=Strategic Concept of Information Warfare	林宗達	中共研究	2002.02	頁 14-132
19	中共信息戰略武力之發展=The Development of Strategy and Force of PRC's Information Warfare	林宗達	中國事務	2002.01	頁 97-137
20	中共信息戰之發展與戰術概論	林宗達	共黨問題研究	2002.01	頁 63-79
21	強化資訊安全以因應中共信息戰之威脅	李俊成	陸軍學術月刊	2001.10	頁 4-15
	中共信息戰發展及我因應之道	趙介一	陸軍學術月刊	2000.01	頁 36-43

項次	出版年	發表次數
1	2002	(7 筆)
2	2005	(3 筆)
3	2007	(3 筆)
4	2000	(1 筆)
5	2001	(1 筆)
6	2003	(1 筆)
7	2004	(1 筆)
8	2006	(1 筆)
9	2008	(1 筆)
10	2010	(1 筆)
11	2012	(1 筆)