中共網軍發展對本軍威脅評估之研究

作者／王清安中校

提要

一、 中共網軍，自2013年被美國媒體揭露後，其後迄今，中共網軍所發動攻擊行為便陸續被報導出來，其網軍部隊人數多少？能力為何？一直都倍受矚目。此外，中共為因應未來作戰趨勢，於2016年元月成立「戰略支援部隊」，據報導指出，此舉是中共為打贏網路戰所做的組織調整。故中共網軍是否因此而擴軍、網路作戰運用方式因此改變？便是本文研究重點之一。

二、 兩岸關係雖趨於和緩，然就軍事層面來說，中共犯我意圖未曾稍減。據國安局統計資料指出，我國每年平均遭中共網路戰攻擊就高達377萬次，故在未來台海戰役中，中共將如何運用網軍對本軍實施網路戰攻擊？便是本文研究重點之二。

三、 本文將藉由探討、分析中共網軍編組、能力及攻臺網路戰模式，進而評估中共網路戰對本軍之威脅，據以策進本軍相對應處置作為，俾利確保遂行國土防護作戰之任務遂行。

關鍵詞：網軍、網路戰、網路戰攻擊、網路戰防禦。

前言

2014年，美國防部長副部長肯德爾(Frank Kendall)曾表示，美軍技術優勢正遭受數十年來前所未見的挑戰，尤其在亞太地區；副部長亦指出，中共推動現代化計畫，絕對不是一個未來問題，而是一個當前問題。[1]此外，美國軍陸軍訓練暨準則指揮部(TRADOC)指揮官麥克馬斯(Herbert R. McMaster Jr.)中將強調，面對俄、中日益強大的網路戰攻擊能力，對於仰賴無線網路通信的美陸軍而言，將更加致命。[2]由上述資料顯示，中共網軍實力已是日益強大，不容本軍小覷。

根據2015年美國國防部公布《中共軍力報告》指出，中共對臺軍事部署方面，未因兩岸關係和緩而有所放鬆。該報告並透露，中共犯臺除採取傳統封鎖、空中或飛彈攻擊與兩棲登陸等方式之外，還可能採取小規模有限度的傳統或非傳統軍事行動。而

[1] 童光復譯，HB Warimann，〈中共軍事現代化〉《國防譯粹》(台北)，第 41 卷第 11 期，國防部，2014 年 11 月，頁 70。
[2] 王光磊，〈美陸軍恐將寡不敵衆〉《青年日報》，2016 年 4 月 8 日，版 4。

其中一項的軍事手段，是中共透過網軍對臺發動網路戰攻擊，或併同運用特戰部隊以打擊我政治、軍事與經濟方面的基礎建設，其背後企圖為引發臺灣內部當局恐慌。[3]

除此之外，我國104年國防報告書更證實，中共網軍近年來透過社交工程、遠端滲透、病毒（惡意程式碼）感染、竊取或監控等方式，企圖影響本軍指管資訊系統運作及遲滯應變能力。[4]綜合上述各項資料，未來中共犯臺軍事手段，將可能運用網軍對臺實施網路戰攻擊，以獲取軍事勝利。

網路戰概述

一、 網路戰定義

(一)美國

2001年，美國阿爾吉拉(Arquilla)及朗斐德(Ronfeldt)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」及認識論。[5]2004年，美國另一位學者指出，網路戰為擾亂、阻絕或摧毀電腦與電腦網路中的資訊或電腦與網路本身；而資訊作戰則為影響敵方觀察、指導及認知，促使敵方決定採取有利於指揮官軍事目標。[6]2014年，美軍JP3-13(Joint Publication 3-13)準則指出，資訊作戰應包含戰略溝通、跨部會整合、公共事務、軍文關係、網路戰等。換言之，網路戰為資訊作戰其中一環。[7]

(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》指出，網路戰屬於資訊作戰範疇(中共信息戰於國內稱為資訊作戰)，而資訊作戰又分為戰略資訊作戰和戰術資訊作戰。所謂戰略資訊作戰稱為戰場外之資訊作戰，通過破壞或操作電腦的資訊，對敵人的電話網、電子網及各種銀行帳系等實施破壞。而戰術資訊作戰，為運用資訊技術和資訊化作戰平台，在偵察採測預警、信息處理與作戰指揮、控制、偽裝、欺騙與干擾的對抗與戰鬥。[8]

綜合上述，筆者認為中共網路戰為運用網路傳輸手段(有、無線電)，對敵人網路節點、資訊系統及儲存資料實施攻擊，以獲取或竄改情報，使敵人無法即時產生正確重要決策，進而癱瘓敵國重要基礎設施，造成人民恐慌，影響政府運作機制，達到不

---

[3] 王光磊，〈美公布中共軍力報告聚焦臺海戰力部署〉《青年日報》，2015 年 5 月 10 日，版 4。
[4] 國防部「國防報告書」編纂委員會，《中華民國 104 年國防報告書》(台北：五南文化廣場，2015 年)，頁 60。
[5] 國防部史政編譯室、約翰・阿爾吉拉(John Arquilla)，《網路及網路戰》(台北：五南文化廣場，2003 年 8 年)，頁 5-6。
[6] 國防部史政編譯室、艾利諾・史龍(Elinor Sloan)，《資訊作戰以柔克剛的戰爭》(台北：五南文化廣場，2008 年8年)，頁146-147。
[7]〈Joint Publication 3-13 :Information Operations〉，http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf，2015/8/27.
[8] 張召忠，《網路戰爭》(北京:解放軍出版社，2001 年 1 月)，頁 87-90。

戰而屈人之目標，同時保護己方資訊系統，不受敵人影響。

二、網路戰與作戰之關係

首次將網路戰攻擊引入戰爭是1991年波灣戰爭。戰爭前，美國中央情報局特工人員到伊拉克，將伊拉克從法國購買的防空系統印表機換上染有電腦病毒的晶片，進而使防空系統電腦程序錯誤，達到指揮失靈。[9]2007年，俄羅斯以網路戰攻擊愛沙尼亞政府和金融機構，意圖要瓦解並阻絕其正常運作。2008年，俄羅斯入侵喬治亞共和國，地面行動伴隨網路攻擊，其目的在瓦解喬治亞的指揮管制功能。[10]2010年，伊朗核電廠因遭電腦病毒震網(Stuxnet)入侵，導致核電廠停擺數小時。[11]由上述資料可知，在2010年前的網路戰，其作戰對象為敵國網路系統，差別之處在於原軍事安全層級提升至國家安全層級。

然而，隨著智慧型手機普及，網路戰的作戰模式也隨之改變。據2016年美國學者表示，由於網際空間不明確的屬性，未來網路政擊將會是國家政府與非國家團體緊密結盟。[12]網際網路和社群媒體已讓所有人都可以運用資訊發揮自身力量，不論是個人、團體或社群，均可影響到外交、資訊、軍事與經濟等相關權力，其影響程度和過去各國政府戰略溝通訊息等同。[13]同年，美網路司令部羅傑斯(Michael Rogers)上將更明確表示，美軍將大幅提升對IS(Israel Stinson)的網路戰攻擊，並透過網路與社交媒體傳播極端思想的能力來反制IS對抗能力。[14]由此可知，未來網路戰對作戰影響攻擊對象將由過去攻擊敵方網路系統或節點，改變至擁有智慧型手機的每個人，故其作戰效益將會更快速，影響層面會更廣大。

故網路戰與未來作戰關係，將會是聯合作戰型態。作戰初期由正規網軍或潛伏敵國人群中，透過各種網路傳播媒體(例如，臉書(Facebook))，發布各種不利執政當局等言論，期以瓦解敵國人民心防與抵抗意志，進而爭取各國認同其出兵作戰之合理性，以達到孫子兵法所說：「不戰而屈人之兵的理想」。爾後隨作戰進展，藉網路掌握敵軍指揮部與主力部隊位置，配合兵、火力對敵實施攻擊，以爭取時效，達到作戰勝利。（如表一）

---

[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。

[10] 鄧炘傑，〈網路公共領域的戰略意義〉《陸軍學術雙月刊》(桃園)，第51卷第542期，陸軍司令部，2015年8月，頁143。

[11] 震网（Stuxnet），https://zh.wikipedia.org/zh-hant/%E9%9C%87%E7%BD%91，2016 年 8 月 30 日。

[12] 章昌文譯，Andrea Little Limbago，〈網路治國的多面向本質〉《國防譯粹》(台北)，第43卷第2期，國防部，2016年2月，頁14。

[13] 黃文啟譯，Bryan Leese，〈從社群媒體獲取軍事情報〉《國防譯粹》(台北)，第43卷第2期，國防部，2016年2月，頁53。

[14] 王光磊，〈美打擊 IS 展開史上首次網路戰〉《青年日報》，2016 年 4 月 7 日，版 1。

表一 網路戰與機械化戰爭區分

區分 / 對象	機械化戰爭	網路戰
作戰型態	線性作戰方式(制空、制海、反登陸作戰)	非對稱型態(直接攻擊)。
主要作戰方式	集中兵力、火力突擊，戰場對抗決定勝利。	分散兵力，火力打擊重要資訊系統，或由網路病毒控制資訊、癱瘓敵國網路系統，並運用即時媒體或臉書傳播，爭取國際輿論支持，影響敵國人民抗敵意志。
戰場主要力量	機械化的陸海空軍聯合作戰部隊。	網狀化作戰單位為主。
戰場主要目的	打擊敵人軍隊和重要軍事或政治。	打擊敵人重要軍事、政治目標，必要時轉以粉碎敵人經濟潛力為目標。隨著web2.0攻擊對象，以朝向全民手機，以顛覆政府政權。
戰爭軍事目標	打垮敵國、消滅敵軍為主。	癱瘓敵國、打敗敵軍為主。
作戰效能	贏得軍事勝利。	贏得軍事勝利外，確保國家政治、經濟等安全。
參演兵力	聯合作戰型態。	聯合作戰與聯合行動(此意，即為增加民間駭客、科技實施)。
攻擊來源	容易定位。	難以定位。
成本	取決於武器成本。	用於電腦及軟體。
攻擊指標	可以探測。	難以探測。
作戰效能	戰爭進展緩慢，時間較久、進程難以控制。	進展迅速、時間短暫，進程易於控制。

資料來源：整理自1.謝游麟，〈中共陸軍「作戰理論」轉型之研究〉《國防雜誌》(桃園)，第30卷第3期，國防大學，2015年5月，頁9。2.黃文啟譯，Bryan Leese，〈從社群媒體獲取軍事情報〉《國防譯粹》(台北)，第43卷第2期，國防部，2016年2月，頁53。3.謝游麟，〈美陸軍網狀化作戰之檢討與展望〉《陸軍學術雙月刊》(桃園)，第48卷第526期，陸軍司令部，2012年12月，頁8-9。

中共網軍發展背景與經過

一、中共網軍發展背景

受 1991 年第一次波灣戰爭啟發，中共解放軍於 1993 年提出「打贏高科技條件下的局部戰爭」戰略構想，以作為新時期軍事戰略方針下的軍事鬥爭準備基點，其目的為癱瘓敵軍指管通資系統。[15]到 1999 年，「被譽為中共航天之父」的錢學森指出，為打贏高技術條件下的戰爭型態，中共必須注意研究資訊戰爭，其內容包括電子戰、網

[15] 戴政龍，〈對《中國的軍事戰略》白皮書之評析〉《展望與探索》，第13卷第7期，2015年7月，頁30。

路戰及心理戰等。[16]此時，中共已注意到網路戰在高技術條件下局部戰爭的重要性。

2004年6月，中共國務院出版《中國的軍事戰略》更首度公開指出，21世紀戰爭型態將是資訊化戰爭，必須明確地把軍事鬥爭準備的基點放到「打贏資訊化條件下的局部戰爭上。[17]2006年，中共軍事戰略為達成以弱擊強的目標，便積極研究各種軍事手段之「殺手鐧」，以達到嚇阻及癱瘓敵人。而其主要手段便是運用網路戰對敵人資訊系統中「資訊的來源」、「資訊管道」及「資訊處理中心」等實施攻擊，以癱瘓敵軍使其不戰而潰。[18]2007年，具有中共解放軍資訊背景的載清民少將，提出「網電一體戰」理論，運用網路戰以擾亂敵人處理與運用資訊的能力，並整合電子戰與電腦網路戰形成整體戰力，進而癱瘓敵人之資訊系統。[19]此階段的網路戰，中共希藉由網路戰攻擊，達到癱瘓敵人資訊系統。

2013 年，中共國務院發表《中國武裝力量的多樣化運用》一文指出，面對複雜多變的安全環境，要打贏資訊化條件下的局部戰爭，中共必須搶占太空、網路空間等國際競爭戰略制高點，並拓展國家安全戰略和軍事戰略視野。[20]隨後在 2015 年，中共國務院發布《中國的軍事戰略》，將「打贏信息化條件下的局部戰爭」中的「條件下的」刪除，其所意涵即為以積極防禦的戰略思維應用在資訊化的環境中，其目的在追求成為網路戰的最終勝利者。[21]中共為加強網路戰略嚇阻要域，確保國家利益拓展，必須組建資訊化部隊，以推動中共戰略轉型。[22]由上述得知，中共網路戰已不是以往採取網路戰防護的消極作為，進而認知到在未來作戰領域中，誰在網路戰場搶得到制高點，誰就能控制戰場主導權。

二、中共網軍發展經過

中共「網軍」乙詞，最早於1999年解放軍報出現；同年成立「解放軍理工大學」，著重培養網路人才，並設立獎學金招收民間資訊高手。[23]2001年，依中共「863計畫」將完成駭客部隊編組，成員以中共科學院為主的團體。這支部隊是中共最早啟動及規模較大的一支駭客部隊，雖只有50員，但最差是碩士研究生;另外，並啟動「973計畫」，以發展出「資訊的獲取與網路監控」。[24]

---

[16] 張明睿，《中共國防戰略發展：跨世紀軍事革命浪潮跟尖者》(台北：紅葉文化，1998 年 5 月)，頁 32

[17] 謝游麟，〈中共陸軍「作戰理論」轉型之研究〉《國防雜誌》(桃園)，第30卷第3期，國防大學，2015年5月，頁9。

[18] 國防部史政編譯室、施道安(Andrew Scobell)、伍爾澤(Larry M.Wortzel)，《中共軍文變化》（台北：五南文化廣場，2006年4月），頁414-415。

[19] 載清民，《直面信息戰》(北京:國防大學出版社，2002 年 7 月)，頁 57-60。

[20] 謝奕旭，〈由習近平宣示裁軍談大陸的國防現代化〉《展望與探索》，第 13 卷第 10 期，2015 年 10 月，頁 20-21。

[21] 同註 13。

[22] 宋吉峰，〈中共崛起的途徑「整合式戰略嚇阻」上〉《青年日報》，2016年5月24日，版7。

[23] 國防部史政編譯室、伊凡.費根堡(Evan A.Feigenbaum)，《中共科技先驗-從杠子時代到資訊時代的國家安全與戰略競爭》(台北：五南文化廣場，2006年5月)，頁245。

[24] 沈方祥，《新世代解放軍》(台北：黎明文化，2003 年 4 月)，頁 240-241。

2002年組建「科研實驗部隊」，2003至2005年，結合民間網路高手(駭客)成立「國防信息民兵隊」。綜觀中共組建信息戰力的具體作為，已朝「全民皆兵、平戰結合、軍民兩用」目標發展。[25]2002至2005年期間，中共7個軍區中有6個軍區設立「特種技術偵察部隊」，遂行守勢和攻勢網路作戰。因此，中共可能在「特種技術偵察部隊」和比較不正式的後備和民兵單位之間，擁有一支數千人組成的網軍。[26]2007年，美國學者哈里斯(Shame Harris)亦表示，美國政府與企業電腦網路攻擊來自中共。該學者並指出，中共已建立網軍，發展病毒，以攻擊敵人之電腦系統與網路。[27]從2002年至2007年，相關學者研究報導，中共確實已組建具備有網路戰能力的部隊。

2013年，美國迪安網路安全公司(Madiant Corporation)公布一份名為「APT:揭露中國大陸網路間諜單位」的報告，在該報告附加一份超過三千餘筆技術資料證明，美國遭網路戰攻擊，是來自中共代號為APT1(Advanced Persistent Threat 1)的攻擊行動，並隸屬於中共總參謀部指揮。[28]2013年，我國《中華民國102年四年期國防總檢討》亦首度證實，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。[29]由上述得知，中共解放軍已具有一支網軍部隊，並可執行網路戰攻擊能力。

2015年，中共近年來利用網路科技，大量招募專業技術人員組成「網軍」，人才來自學者與企業界，執行網路戰攻擊和防禦。[30]2016年元月，中共解放軍新編成一支「戰略支援部隊」，專職從事網路戰攻擊與防護。該部隊成立後，將使駭客部隊得到更集中的管理。[31]此外，最新報導指出，2016年中共「國家」網信辦公室發布「國家信息化發展戰略綱要」，內容包括要建設網路強國及培養資訊化作戰。該報導強調，中共將要積極培養資訊化作戰指揮、技術專業等作戰人才。[32]中共已意識到網路戰已不再只是軍事戰層級，而是提升至國家安全戰略層級，統一管制運用，以提升網路戰效能。此外，中共並意識到未來作戰型態，網路人才將攸關網路戰勝負關鍵，故積極籌獲網路人才。

中共網軍編組與能力

[25] 同註23，頁244。
[26] 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〉(台北:國防部，2011年)，頁 201。
[27] 柴惠珍譯，Shame Harris著，〈中共網軍〉《陸軍軍事譯粹選輯》，第18期，2008年5月，頁748。
[28] 載政龍，〈中共網軍發展與網路攻防:論我國資通安全之政策規劃〉《戰略評估》，第 4 卷第 4 期，2012 年，頁 112。
[29] 國防部「國防報告書」編纂委員會著，《中華民國102年四年期國防總檢討》(台北:五南文化廣場，2013年)，頁18。
[30] 陳育正，〈美國網路安全防護經驗-對我國網路安全情勢之啟示〉《國防雜誌》(桃園)，第30卷第3期，國防大學，2015年5月，頁78。
[31] 陳家倫，〈中共五戰區平可夫：軍改速度快阻力多〉《中央社》，2016年2月3日。
[32] 吳佰璋，〈中共發布「信息化發展戰略綱要」〉《青年日報》，2016 年 7 月 28 日，版 6。

一、 中共網軍編組

(一) 軍方體系

1999年，中共成立網軍，主要作為敵網路資料的竊取及破壞網路系統。另一方面為負責內部網路安全防護工作，並由國防動員委員會新設「信息動員辦公室」，除納編解放軍外，並廣納民間從事電子及網路相關人員，編成電子戰分隊、網路戰分隊、駭客分隊及信息救護分隊，從事網路入侵、破壞等工作。[33]

自2006年起，美國115大企業的商業機密遭竊取，損失金額預估約3000億美元，是由解放軍代號61398網路部隊所造成。自2007年起，西方國家政府和國防事務承包商資訊系統遭網路攻擊，是由中共另一支網路部隊代號61486所為。該報導還發現，中共61486部隊與61398部隊，經常共享電腦資訊、相互通訊。[34]此外，據報導，中共上海交大信息安全工程學院除提供61486部隊技術支援外，其校內學者已與61398部隊有密切合作關係。[35]

2010年7月，我國學者呂炯昌引用美國聯邦調查局(FBI)的一份機密報告指出，中共已經組一支超過18萬人的網軍，其中3萬人為網路特工，15萬為民間駭客，目標在2020年建立全球第一支「資訊化武裝的部隊」。[36]中共網軍正式國防編制，各省份都有完整組織體系、分析。據美國聯邦調查局估計，中共網軍人數高達近20萬，主要從事各種網路偵察技術、網路戰攻擊截取各國國防機密。[37]

2014年，據報導揭露，中共還有一支61419網路部隊，總部位於山東青島，專司對日本網路攻擊。該報導指出，該支部隊中共網軍具有數千至1萬名網路士兵及800萬網路民兵，並隸屬總參謀部。[38]2015年，據另一項報導，中共網軍還包含有成都軍區78020部隊，該組織已滲透至越南、菲律賓和東南亞許多國家的政府、軍事、媒體和能源公司的網路。此外，該報導還引述美國智庫「Project 2049 Institute」執行主任斯托克斯（Mark Stokes）表示，解放軍共有20多個類似78020部隊的編制，功能為情報收集、分析和電腦網絡防禦與攻擊。[39]

中共大陸網軍主要受總參謀部的指揮，據美國所多資安公司的分析報告指出，總參三部及下屬61398及61486部隊為中共網軍的主要來源，但可能來自IP位置追縱下線，若配合中共情報組織的分工推論，總參二部可能才是真正指揮的中樞。[40]總參謀部第

---

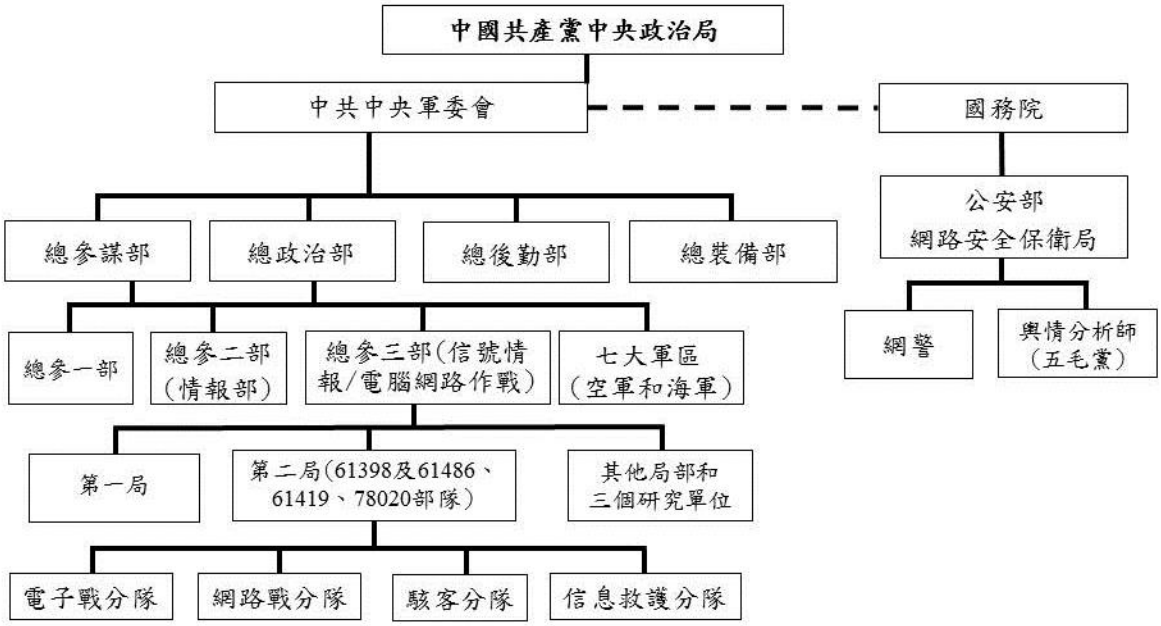
[33] 謝茂淞，《亢龍有悔-中共反介入戰略之研究》，(台北:高手專業出版社)，2010 年 3 月，頁 109。
[34] 王文勇，David Alexander〈網路防衛戰略方案〉《國防譯粹》(台北)，第 40 卷第 9 期，國防部，2013 年 9 月，頁 53。
[35] 張沛元，〈上海交大遭爆與解放軍駭客部隊合作〉《自由時報》，2013 年 3 月 25 日，版 12。
[36] 呂炯昌〈美印組成網路聯合部隊對抗中國大陸網軍〉《尖端科技》，第311期，2010年7月，頁87。
[37] 徐佳〈網軍來襲，新一代國防戰開打〉《數位時代》，第 288 期，2013 年 5 月，頁 91-92。
[38] 楊家鑫，〈青島網軍曝光專司攻擊日本〉《中國時報》，2014 年 8 月 23 日，版 16。
[39] 大陸中心，〈美給臉色再揭陸網軍竊資〉《蘋果日報》，2015年9月29日，版7。
[40] 林穎佑，〈2014年中國大陸軍事情勢總結及未來發展趨勢〉《中共研究》，第49卷第1期，2015年6月，頁126-133。

三部為共軍信號情報(SIGINT)的蒐集機構，主要任務為對無線電通信實施監聽、各種密碼破譯等工作，在網路方面，負責網路安全維護及網路間諜防制。另總參謀部第四部，主要任務為電子情報蒐集、分析、反雷達干擾等，以及資訊與電子戰之研究、電腦網路攻擊之反擊。[41]

我國《中華民國104年國防報告書》首度證實中網軍佈署於各總部、五大戰區、國防科研機關、國防動員信息及民兵等軍事部門，組成網路攻擊、防禦的基本戰力。[42]另據一項研究揭露，共軍大約有16個(信號情報)技術偵察單位和局處，和至少7個電子作戰/電子反制單位，中共五大戰區，均各自編配了一個電子反制團，且二砲部隊應該也有其電子支援單位。這些組織的任務，就是進行網路滲透、網路諜報及電子作戰。[43]

另外值得一提，中共為推展「資訊心理戰」，在其總參謀部下建立心理戰指揮中心，遂行資訊心理戰的任務，包括組織部隊、院校和科研機構進行資訊心理戰理論的研究，制定共軍資訊心理戰的發展規劃等。[44](如圖一)

圖一 2015年中共網軍編組圖



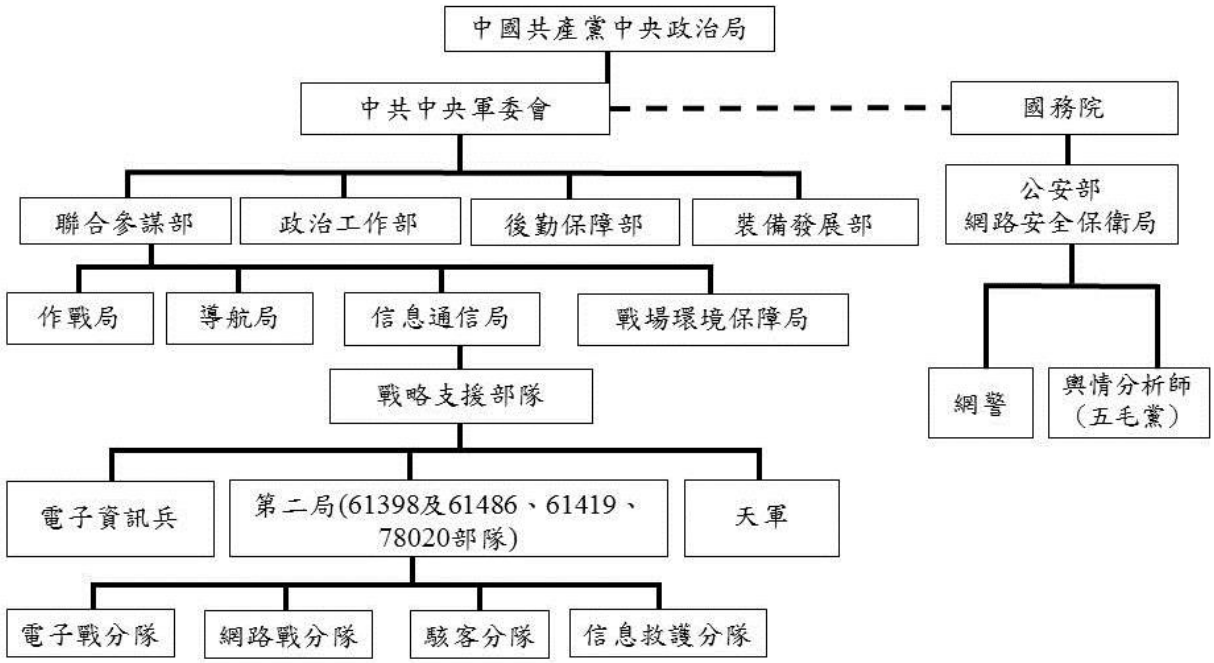
資料來源：整理自1.陳育正，〈美國網路安全防護經驗-對我國網路安全情勢之啟示〉《國防雜誌》，第30卷第3期，2015年5月，頁78。2.林穎佑，〈2014年中國大陸軍事情勢總結及未來發展趨勢〉《中共研究》，第49卷第1期，2015年6月，頁126-133。3.王政，〈大陸「國家安全法(草案)」中有關國家安全制度之評析〉《展望與探索》，第13卷第6期，2015年6月，頁30-31。4.國防部「國防報告書」編纂委員會，《中華民國104年國防報告書》(台北：五南文化廣場，2015年)，頁56。

[41] 王政，〈大陸《國家安全法》(草案)中有關國家安全制度之評析〉《展望與探索》，第13卷第6期，2015年6月，頁30-31。
[42] 同註4，頁56。
[43] 鄧炘傑，〈中共軍事現代化及網路作為〉《陸軍學術雙月刊》(桃園)，第52卷第545期，陸軍司令部，2016年2月，頁139。
[44] 蔡國堂，〈共軍資訊心理戰之研究〉《國防雜誌》(桃園)，第27卷第2期，國防大學，2012年3月，頁60-61。

2016年元月，中共為縮減指戰層級，適應現代戰爭的需求，其軍改重點為新增陸軍及火箭軍(原二砲提升為火箭軍)及1支戰略支援部隊，其軍委、總部體制改方向為「軍委管總、戰區主戰、軍種主建」的格局。[45]「戰略支援部隊」將整合過去負責無線電監聽、偵查的總參謀部技術偵察部(總參三部)、負責雷達系統的總參謀部電子對抗部(總參四部)，以及總參謀部訊息化部(總參五部)。[46]

中共聯合參謀部下設有4大局，分別是信息通信局、導航局、作戰局、戰場環境保障局。[47]聯合參謀部內部設立「信息通信局」，負責網路戰進攻與防護。其中，名為「總部直屬信息作戰力量」的部門集結共軍最優秀的駭客專家，專門研製各種病毒，用於網路攻擊。據報導指出，這個部門至少擁有7個工廠、1個研究所、1個保障基地，負責研製、生產資訊病毒。此外，中共解放軍也在陸軍的軍級單位成立信息化辦公室及下屬「信息戰分隊」，專門負責駭客部隊的網路攻擊。[48](如圖二)

圖二 2016年中共網軍編組圖



資料來源：整理自1.陳君碩，〈戰略支援部隊打網戰經費提高30%〉《旺報》，2016年1月30日，版6。2.陳建瑜，〈軍委聯參部神祕4大局曝光〉《旺報》，2016年4月17，版6。

(二)非軍方體系

2012年底，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軍事實力相結合，並強調網路戰不限軍事人員，所有擁有資訊系統特殊知識與技

[45] 鄒文豐，〈淺析中共改編戰區之聯戰意涵與影響〉《青年日報》，2016年3月6日，版7。
[46] 〈戰略支援部隊作用中共黨媒：致勝關鍵〉《中央通訊社》，2016 年 1 月 25 日。
[47] 陳建瑜，〈軍委聯參部神祕4大局曝光〉《旺報》，2016年4月17，版6。
[48] 尹俊傑，〈網路戰漢和：共軍駭客部隊增加〉《中央社》，2016年1月5日。

能的人，都能參與網路戰。[49]2013年，中共前寧夏軍區司令員昌業庭少將亦表示，國防後備體系，應積極推動向新一代網路技術研改，編組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，以加強網路防護能力，並儲備網路專業人才，達到不求所有，只求所用。[50]

為掌握全國網路安全，中共公安部所屬「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)下設立的「網監處」，負責轄區內的網路信息安全監察和違法查處工作。據2004年非正式統計，公安部負責網路保密、偵防的網路警察和網路安全人員，已多達23萬人。另外，還有4萬人各相關單位的網路科研機關人員，總計27萬人員。[51]自2015年起，中共警方招募志願者，成立「網警志願者」，俗稱第6支的「王牌群眾力量」，該部隊3,000員遍布中共全境，各行各業，且80、90年代後的年輕人佔約8成。[52]

中共為落實對網路線上監控、宣傳，則由政府雇用線上評論人員(俗稱的五毛黨)[53]，他們拿錢加入線上社群，對反對共產黨的內容、宣揚黨的重大工作，或是制止敏感內容實施過濾。[54]據國內學者研究指出，其中共網路評論人員預估人數高達五萬人，其工作內容為不僅形塑對中共友善的國際氛圍，甚至創造出有利軍事行動的條件。[55]在2013年10月，中共首次舉行輿情分析師培訓，預估從事輿情分析師約200萬人，這些人多半分布在黨政宣傳部門與入口網站。[56]

另外，須注意到中共隱藏而無法估計的網路駭客人員(中共俗稱黑客)。據報導指出，中共近年來陸續規劃、建置及投資網路建設，甚至舉辦所謂「駭客擂台」藉以吸收民間技術精湛之駭客，將其納入至網軍中，並視其專長編組及任務需求，入侵各國網路，伺機截取機敏資料。[57]

綜合上述各項資料，2016年中共新成立的「戰略支援部隊」預估約4萬人員(將原編制於總參謀部二、三局61398、61486、61419、78020的網路部隊及隸屬合作關係的大學研究者)，另應包含在各軍區的通信、電戰等部隊的網路人才，預估中共網軍正規軍約7萬等。此外，若加上隱含看不見的隱匿在各大學、民間等網路高手15萬，預估中共網軍將達22萬之多(如表二)。這數字略大於2015年，當時國安局李翔宙先生於立法

---

[49] 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。
[50] 昌庭，〈以十八大精神為指導在新的起點上推動國防動員建設科學發展〉《國防》，第二期，2013 年 3 月，頁 14。
[51] 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。
[52] 謝璿，〈中共網路維穩打手 年刪50萬筆貼文〉《青年日報》，2016年1月18日，版6。
[53] 五毛黨 50-cent party，譯註:意指每貼一則正面訊息就可得人民幣五毛錢酬勞的那些人。
[54] 楊黎中譯，Shannon Knight，〈中共獨特的網際空間〉《國防譯粹》(台北)，第42卷第10期，國防部，2015年10月，頁13。
[55] 謝茂淞，《亢龍有悔-中共反介入戰略之研究》，(台北:高手專業出版社)，2010 年 3 月，頁 111。
[56] 〈監控網路培訓腦大軍〉《蘋果日報》，2013 年 10 月 6 日，版 26。
[57] 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 40 卷第 2 期，2012 年 4 月，頁 236。

院會質詢表示，中共網軍人數約18萬人。[58]

表二 中共網軍人數概算統計

區分	項次	部隊	預估人數	總計	備註
軍事部隊	1	總參第三部網軍－部分單位藏身於北京、上海、青島及武漢等地區大學，以研究中心及通訊實驗室存在（61398及61486、61419、78020）	4萬	7萬	執行網路戰攻擊為主
	2	總參第四部－通信部隊(信息化部隊)	1萬5千人員		
	3	總參第四部－電戰部隊	1萬5千人員		
非軍事部隊	4	約僱駭客	約15萬人。		
	5	公安部	27萬人員		執行網路戰防護為主
	6	輿情分析師	二百多萬人		

資料來源：整理自1.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。2.楊家鑫，〈青島網軍曝光專司攻擊日本〉《中國時報》，2014年8月23日，版16。3.鄧炘傑，〈中共軍事現代化及網路作為〉《陸軍學術雙月刊》(桃園)，第52卷第545期，陸軍司令部，2016年2月，頁139。4.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。5.〈監控網路培訓腦大軍〉《蘋果日報》，2013年10月6日，版26。6.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》(台北:國防部，2010年)，頁261-282。

二、中共網路戰能力

(一) 攻擊能力

1.駭客能力

根據美國學者蘭柏司(Benjamin S.Lambeth)研究，中共網路戰攻擊的能力有長足的進步，且有足夠證據顯示，中共早已對美國非保密資料傳輸遂行網路戰攻擊。[59]中共對網軍的投入程度，已積極超過熱兵器對抗，其網軍已非過去單純的竊取情資，而是提升為經常主動出擊，透過癱瘓、破壞來完成戰略目標。該研究並指出，2014年5月底，美國司令部以網路間諜罪起訴5名中共軍官指控涉嫌入侵美國公司竊取機密及對媒體網站進行DDOS攻擊癱瘓網路運作。[60]

2015年，中共網軍已非單純的民間駭客，而為有組織具計畫性的針對式攻擊。此外，中共網軍還慣用「進階持續性滲透攻擊」(Advanced Persistent Threat, APT)[61]，

[58] 呂昭隆，〈國安局網路部隊5月1日成軍〉《中國時報》，2015年3月16日，版A2。
[59] 李永悌， Benjamin S.Lambeth，〈空權、太空權與網路權〉《國防譯粹》(台北)，第 38 卷第 4 期，國防部，2011 年 4 月，頁 26。
[60] 同註40，頁131。
[61] 中共APT攻擊主要是結合程式上的漏洞，以及社交工程(Social Engineering)來攻破安全防護系統，並搭配「零時攻擊」(Zero-Day)，對尚未修補的漏洞進行入侵。許多攻擊目標其主要的收信匣可能會選擇架設在外部的儲存空間，有問題的信件可能在外部就已遭受系統服務的攔截。APT經過特別的設計，俾能利用在目標系統中獨一

除重視攻擊技術外，更重要的是瞭解攻擊目標的愛好，以引誘受害者打開含有惡意程式的文件。而攻擊的對象也不直接朝最終目標攻擊，而是由目標的外圍進行攻擊。[62]據另一項報導亦表示，在2015年，有駭客組織使用來自中共的軟體，入侵東南亞和印度政府、企業的資訊系統，其攻擊手段也是運用寄送Email及流利的當地語言書寫，誘使目標打開已安裝惡意軟體的檔案。[63]

中共網路戰能力將可以協助中共解放軍，更有效的蒐集情報或進行網路攻擊的行動。這樣的網路戰攻擊，可用來約束對手的行動，透過網路的運用來減低對手反應的時間。該研究還指出，中共網路戰還可以阻斷敵方運用網路和資訊系統的能力。[64]2016年，中共針對美國政府和國防工業設施進行網路間諜活動，對美國的軍事行動、美軍人員的安全福祉、裝備效能與作戰整備等，都已形成威脅。[65](如表三)

表三　中共網軍駭客攻擊行動統計

項次	時間	攻擊行動
1	2005 年	美國網路安全公司 FireEye 研究人員表示，過去 10 年來，中共網路駭客，一直在刺探東南亞和印度等國政府和企業情報，從未間斷過。
2	2008 年至 2014 年	中共利用民間商業往來過程，例如中共商人蘇斌(Su Bin)，伺機竊取美國先進科技技術，取得 F-22、F-35 戰機等機敏資料，以轉售中共國營企業，最後遭受美國加州聯邦法院起訴。
3	2013 年	日本民營網路安全公司「趨勢科技」(Trend Micro)的一位威脅員宣稱，透過他偽裝自美國一家自來水工廠的控制系統，設下的陷阱，發現從 2012 年 12 起，中共進行入侵。
4	2014 年	美國司法部控告一名中國商人與駭客聯手侵入波音等數家美國公司，竊取軍機資料轉賣中國國企。
5	2014 年	美國國家安全局（NSA）前局長麥克康納爾人表示：「中共網軍已入侵美國國會國防部、重要公司，並竊取資訊。」
6	2015 年	美國司法部 5 月 19 日起訴六名中國公民以「商業間諜」名義，其中包括三名天津大學教授。
7	2015 年	美國知名程式碼代管網站 GitHub 於 6 月初起遭 87 小時的駭客攻擊，GitHub 緊急轉移試圖癱瘓網站的流量後，才恢復運作。
8	2015 年	6 月初，美國人事管理局 400 萬現職及離職政府職員的個資遭到駭客入侵竊取，被一種稱為「Sakula」的罕見程式來遙控遠端電腦。

無二的缺陷，同時還能保持不受作業系統更新和安全修補程序的影響。其目標在網路安全的防護作為下低調運作，直至預定攻擊的時刻到來，且要繼續不被察覺，達成前述目標，惟有民族國家有能力設計和部署。

[62] 林穎佑，〈看不見的網路大戰台灣如何接招〉《聯合報》，2015年2月10日，版A15。

[63] 謝璿，〈火眼控中共駭客襲印、東南亞達 10 年〉《青年日報》，2015 年 4 月 15 日，版 6。

[64] 同註52，頁13。

[65] 同註40，頁140。

9	2015 年	中共相關部門利用 IMSI-catchers 技術監視 4 家航空公司，在機上乘客試圖連接互聯網時，該設備能夠入侵手機，藉閱讀手機中的電子郵件等，將數據發送回中共。

資料來源：整理自1.〈美控6陸人竊商業機密涉用軍用科技〉《青年日報》，2015年5月21日，版4。2.陳育正，〈美國網路安全防護經驗-對我國網路安全情勢之啟示〉《國防雜誌》，第30卷第3期，2015年5月，頁79。3.鄧炘傑，〈中共軍事現代化及網路作為〉《陸軍學術雙月刊》，第52卷第545期，2016年2月，頁140。4.〈中共「大砲」監控網路擴及境外〉《青年日報》，2015年4月12日，版6。

2.病毒

據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」，並有能力加以使用。本武器還包括「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。[66]2012年中共的研究機構針對「聯合戰術偵報分發(傳送)系統」(Joint Tactical Information Distribution System, JTIDS)數據鏈路系統，研發反制措施。該報告指出該機構正針對系統的指管節點與網路，研發網路攻擊工具，以利中共網軍發動全面的網路戰攻擊。[67]

另外，在2015年中共已研發出一種俗稱「大砲」的網路戰攻擊武器。當外國資訊流向中共網站後，該項系統即攔截並注入惡意代碼，再發送回給打擊目標。[68]此外，根據2016年一份最新資料透露，中共為建設網路強國，預估到2020年，其網路核心關鍵技術部分將達到國際先進水平，到2025年，將改變核心關鍵技術受制於人的局面。[69]

由上述中共網路戰攻擊能力得知，中共發展網路戰，已不再只是從事竊取，而是積極研究各項網路戰攻擊手段，以提升網路戰能力。此外，中共積極在網路技術發展上朝向自行研發，以確保網路戰優勢。

(二) 防禦能力

1. 對內防禦

2001年中共為與法輪功學員組成的反網路封鎖力量展開一場網路戰，投入逾10億美元建設網控金盾工程「防火長城」，其審查的主要目標為防範社會動員，聚焦在限制反政府的修辭。[70]另外，中共為掌握官員上網情形，已由北京市平谷區紀委開發出電子監察系統。該瀏覽監控軟體通過關鍵字、事項即可找到違規人員的網路IP位址，並馬上進行封鎖單位及犯規員工。[71]

---

66 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〉(台北:國防部，2011年)，頁 200。

67 劉慶順譯，John M.Dahm，〈美軍「聯合資訊環境」的挑戰未來〉《國防譯粹》(台北)，第43卷第2期，國防部，2016年2月，頁16-24。

68 〈中共「大砲」監控網路擴及境外〉《青年日報》，2015年4月12日，版6。

69 吳佰璋，〈中共發布「信息化發展戰略綱要」〉《青年日報》，2016 年 7 月 28 日，版 6。

70 同註23，頁13。

71 〈上班點擊千次色情網站陸官員被舉報〉《青年日報》，2015年9月16日，版6。

2015年，中共《國家安全法草案》網路與訊息安全中，新增「維護國家網路空間主權」規定，其內容最值得觀切為中共確保國安戰略，將建立準確高效的情報訊息收集、研判和使用制度等。[72]同年，中共為加強網路安全管制作為，於互聯網信息辦公室制定「互聯網用戶帳號名稱管理規定」，針對網路訊息服務中心註冊或使用的帳號名稱中，若有違法和不良訊息，則予不能註冊。[73]

中共已將網路空間視為中共整體國力與美國戰略競逐要項的重要一環，而中共領導階層也忌憚開放的網際空間和網路，威脅到共產黨統治的正當性。[74]2015年，中共首次把新媒體從業人員系統性的納入「中央」統戰部培訓體系，名單則由中共「中央」網路安全與信息化領導小組辦公室擬定。該報導亦指出，中共未來可能持續藉由收緊網路言論自由力道，進一步影響全世界。[75]

2016年中共國務院制定網路新聞資訊管理新規定，嚴控網路新聞資訊。據新規定指出，中共網路資訊的監管部門，變更為「網信辦」，作為建立信用檔案和約談制度。[76]同年，中共國家主席習近平視導「新華社」時，要求媒體牢牢堅持「黨性原則」、「正確輿論導向」、「正面宣傳為主」等，並要求加強網路監管、廣儲五毛黨員、升級長城防火牆及大砲等網路安全工作，並落實禁止外企及中外合資公司從事網路訊息服務。[77]

除此之外，美國洛杉磯的網域註冊公司XYZ.com與中國政府達成協議，同意在其經營的網址實施北京的審查制度，讓中共「自由」、「民主」或任何指涉天安門大屠殺等一萬兩千個「黑名單」字彙，封鎖全球各地網名。[78]此外，2016年，據美國貿易代表辦公室（Office of the United States Trade Representative）發布報告證實，在2014年裡，全球25個人氣最高的網站中，有8個在遭中共封鎖，例如谷歌（Google）、臉書和推特（Twitter）等。[79]

2. 對外防禦

中共正採取一些措施以建立網路的防禦工事並阻擋外界入侵其網路。同時，中共也把網路領域當作一個能在其中獲得優勢，凌架敵人的數位戰場。據研究表示，中共正準備實施其所謂的網路「核武」方案，亦即將中共自全球網路中抽離，作為其防衛手段，故其軍方的內部電腦網路實際上已與其他網路隔離。[80]中共與俄羅斯政府主張，國家必須保護與控制網路，呼籲各國重新思考網路管制思題，並提議納入聯合國

[72] 謝璿，〈陸「國安法」二審稿堅持共黨專攻〉《青年日報》，2015年4月21日，版A6。
[73] 蘇家慶，〈網管新制上路刪逾6萬個帳號〉《青年日報》，2015年3月1日，版6。
[74] 楊黎中譯，Shannon Knight，〈中共獨特的網際空間〉《國防譯粹》(台北)，第42卷第10期，國防部，2015年10月，頁138。
[75] 謝璿，〈網路媒體人遭中共收編輪訓〉《青年日報》，2015年5月24日，版6。
[76] 汪莉絹、林克倫〈轉載發布網路新聞陸管制變嚴〉《聯合報》，2016年1月14日，版A12。
[77] 鍾承翰，〈「媒體姓黨」是中共新一波造神運動的起點〉《青年日報》，2016年4月3日，版7。
[78] 魏國金，〈美網域商屈服中國封殺敏感字〉《自由時報》，2015年11月6日，版6。
[79] 黃忠榮，〈中美網戰升級防火長城成貿易壁壘〉《旺報》，2016年4月9日，版6。
[80] 同註52，頁22。

國際通信聯盟(ITU)管轄。此外，伊朗在中共技術援助下，境內建立許多設施，包含全國性網際網路，透過數位通路的嚴密管制和區分，以降低西方對伊朗的網路攻擊。[81]

2015年，中共為加強主幹網路品質監管，建立完善行動網路應用程序安全管理機制，藉控制海底光纜接口，以擴大控制網路實體層面。各網路運營商（電信企業）須將連網的IP，改成只能獲取運營商設置的虛擬局域網IP，再透過公網IP實施上網，如果使用的DNS不是認可，將無法連結上網。[82]同年，中共當局避免網路革命，要求境內所用連網用戶，須透過虛擬專用網路技術－翻牆(VPN)技術連接國際網站。該報導並透露，至少3家VPN技術國際供應商已證實，在中共境內使用者的活動，已完全不能通過翻牆使用。[83]

除此之外，2015年，中共以維護網路安全為由，迫使為中共各銀行提供電腦設備的外國供應商交出機密原始碼（中國稱「源代碼」），並採取中共的加密演算法，接受侵入性檢查，在軟硬體產品中建立所謂的「後門」。[84]

不可諱言，智慧型手機的通資安全監控，對中共而言，是很重要的一環。故在2013年8月31日，中共當局要求所有手機用戶嚴格實施手機卡實名制，否則將對用戶「半停機」處理，即不能打電話、發簡訊及上網，只能接電話和收簡訊。[85]不僅如此，於2016年8月，中共「互聯網信搜索服務管理規定」，要求所用手機APP，採「後台實名、前台自願」原則，註冊用戶進行認證，不得從事「危害國家安全與擾亂社會秩序」活動。對違者，將限制功能甚至關閉功能。[86]

中共網路戰對我軍威脅評估

一、中共網路戰對我軍之可能行動

(一) 正規作戰

根據國內學者林中斌《核霸》一書指出，中共若以海、空軍及導彈攻擊等硬殺器，應可順利占領臺灣，惟一切基礎設施均毀於戰火且耗時費日，並會引起國際干預與制裁，若用網路戰此無顧慮，可達速戰速決之目標。[87]另外，據國內學者研究表示，未來中共攻臺戰役中，中共解放軍極可能放棄傳統大規模的灘岸登陸方式犯臺，而採「高速、多點、立體登陸」方式遂行非線性作戰，直接威脅地面作戰。其模式將綜合運用網路資訊、電磁脈衝、導彈攻擊、島內策應、特戰襲擊，直接指向本島海空基地

81 同註8，頁142-145。
82 同註40，頁139。
83 謝璿，〈中共封銷對外網路「翻牆」失效〉《青年日報》，2015 年 1 月 25 日，版 6。
84 張沛元、盧永山，〈中國設網安「後門」迫美商交出原始碼〉《自由時報》，2015年1月30日，版6。
85 大陸新聞中心，〈陸加強網路管控翻牆更難了〉《聯合報》，2015年5月21日，版A12。
86 謝璿，〈陸 8 月多項新規上路網管趨嚴〉《青年日報》，2016 年 7 月 31 日，版 6。
87 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。

及政經要害，摧毀或癱瘓國軍防衛體系，迫使我軍無條件屈服。[88]

此外，美國智庫德公司表示，若台海發生衝突，中共可能運用網路戰，以阻止美軍協防臺灣。當前中共以經濟發展作為國家戰略主軸下，運用網路戰攻台，在各方面的風險成本評估中，最為經濟又能兼顧戰略效果。[89]據美國網路安全曼迪亞公司研究證明，中共61398部隊曾有6部伺服器擁有臺灣IP位址，並利用臺灣當做駭客跳板。[90]據2016年最新報導指出，中共將積極建設網路強國，除持續做好網路戰防護工作「防」(網路長城)，更要發展網路戰攻擊的領域，其攻擊對象包含美國、日本及臺灣。[91]

除此之外，中共解放軍在香港各軍營建設無線電訊號監聽天線，能攔截香港民用手機基地台的收發訊號，讀取香港民眾Wi-Fi 通訊、手機語音通訊資料。報導並指出，中共解放軍在香港大帽山建設相當大的無線電監聽站，可將在香港各駐軍基地的無線電截獲數據，實施分析處理。[92]此舉，若配合島內特工人員，對於現階段本軍智慧型手機開放，將造成嚴重威脅。

綜合上述，在未來中共攻臺戰役中，中共解放軍除可能發動大規模兩棲登陸奪下臺灣外，極可能運用網軍，並配合島內特工人員對本軍指管通資系統實施竊取、破壞，以迅速獲取戰爭勝利。

(二) 非正規作戰

1.駭客能力

當前中共「網軍」為突破本軍資通安全防禦機制，大量利用「社交工程」方法，藉機敏機關或重要人士周邊關係，「由近而遠」及「由疏而密」等迂迴方式對本軍發動突穿、滲透等駭客攻擊，以獲取遭駭單位內部網路最大控制權限後，大肆行盜、偽造或癱瘓網路等。[93]2013年4月，我國國安局前副局長張光遠於立法院表示，中共為全面掌握國防、政治、外交等動態，對我發動網路戰攻擊，已由政府機關、駐外館處，轉向民間智庫、電信者及委外廠商，並轉思維攻擊較疏於防護網路節點設施或寬頻路由器及網路停存系統等崁入式系統裝備，未來將擴及我國關鍵基礎設施等隱性資料或是透過網路戰攻擊癱瘓運作。[94]

行政院前副院長張善政指出，從2009年1月到2014年10月進階持續威脅（APT）攻擊分析，中國駭客會配合節慶、政經事件，吸引使用者開啟信件，並對總統府、行

---

[88] 同註17，頁16。
[89] 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。
[90] 〈破天荒美跨海通緝解放軍網諜〉《蘋果日報》，2014 年 5 月 20 日，版 17。
[91] 吳佰璋，〈中共發布「信息化發展戰略綱要」〉《青年日報》，2016 年 7 月 28 日，版 6。
[92] 〈漢和：共軍在港監聽手機全都露〉《中央通訊社》，2015 年 1 月 28 日，
[93] 載政龍，〈中共網軍發展與網路攻防:論我國資通安全之政策規劃〉《戰略評估》，第4卷第4期，2012年，頁112。
[94] 〈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^@@14047，2016年9月9日。

政院、外交部、經濟部和國發會等單位實施網路戰攻擊。[95]2015年，前國安局長李翔宙曾在立院備詢證實，國安局已成中共網軍及駭客長期鎖定目標，國安局公開網站，每年平均遭侵擾事件達377萬次。其中，惡意侵擾有12萬次。[96]同年，民進黨立委蕭美琴在立法院外交國防委員會爆料指出，2015年3月24日，民進黨中央的網站，僅上午5分鐘，就遭到中共網軍10萬次以上的惡意攻擊，民進黨中央黨部網站遭網攻，主要就是遭受DDOS(Distributed Denial of Services)就是「阻斷服務攻擊」，就是平常植入在電腦中的程式同時間啟動，讓服務中斷。[97](如表四)

表四 中共網軍近年來對我攻擊行動

項次	年度	攻擊行動
1	1999 年	兩國論發表後，中共「網軍」首次對我發動了大規模攻擊，行政院、國安局、監察院等政府網站都曾被植入木馬程式。
2	2004 年	總統大選期間，中共「網軍」曾入侵總統府、國安會內部網站竊取資料。此外，據 2006 年法務部調查局資訊室錢世傑研究指出，囿於兩岸關係緊繃，雖查覺 IP 來源來自中共時，但因對入侵駭客之身分無法確認，僅採取消極防範。
3	2008 年	中共網軍針對臺灣關鍵基礎建設進行監控(如醫療院所、重要交通建設及核電廠)。
4	2013 年	國安局報告指出，中共為全面掌握我國防、外交動態，已由政府機關、駐外館處，轉向民間智庫、電信業者，並攻擊我較疏於防護的交通號誌儀控設備。
5	2015 年	當時國安局李翔宙上將在立院備詢指出，國安局已成中共網軍及駭客長期鎖定目標，國安局公開網站，每年平均遭侵擾事件達 377 萬次。其中，惡意侵擾有 12 萬次。
6	2015 年	全台有 15 家據點的歐悅國際連鎖精品旅館集團(OHYA CHAIN BOUTIQUE MOTEL）遭駭長達 10 個月，去年被發現有五千筆會員和住宿客戶個資遭中國網軍張貼在 Pastebin 駭客網站上，流出的個資包括姓名、聯絡電話等，連訂房型式、房間都一覽無遺。
7	2015 年	臺灣大選將至，美國媒體「彭博」昨報導，中國國家支持的網軍近期對臺灣媒體與民進黨發動攻擊，欲竊取民進黨的政策演說內容或不為人知的資訊，破壞其勝選機會。民進黨稱有 50 名黨工成攻擊對象，有核心幕僚的電郵被駭。美國資訊公司「火眼」發言人波蘭德昨向《蘋果》表示，這次網攻是為取得民進黨的相關訊息。

資料來源：整理自1.劉慶侯、詹士弘，〈歐悅旅館被駭萬筆個資外洩〉《自由時報》，2015年9月29日，版7。2.〈綜合報導－彭博：中國網攻綠營竊密阻勝選〉《蘋果日報》，2015年12月22日，版A12。

[95] 鍾麗華，〈張善政：中國將台灣當網攻試驗場「自己的資安自己救」〉《自由時報》，2015年1月23日，版A9。
[96] 同註52。
[97] 王炯華，《民進黨官網遭駭李翔宙證實是DDOS攻擊〉《蘋果時報》，2015年3月27日，版7。

2.病毒

據2010年，美國安全軟體公司(邁克菲)(McAfee)對「極光行動」(Operation Aurora)的調查報告，美國約30多家公司遭網路攻擊，是利用社交工程連結到有惡意病毒碼的網站所造成，追縱電腦病毒來源，是來自臺灣遭中共病毒入侵的伺服器所造成。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，遭滲透計有加拿大、臺灣，包括科技及電信等公司，其入侵者指管伺服器公開入侵對象的標準程序，此伺服器位於中共的北京和上海。[98]

中共網軍不斷對臺發動網路攻擊，潛藏中國特定程式的數據通訊產品也已大量來台銷售，政府網路遭攻擊癱瘓發生的機率也將大幅提高。中國網軍人數龐大，對臺進行有系統、針對性的密集攻擊，政府部門、軍事及情報、國安單位，以及水力、電力、電信等國家關鍵性基礎建設，更是中國網軍的頭號攻擊目標。[99]據報導，號稱「世界第一間諜」的中共新型監控軟體，已被引進臺灣，且有不肖徵信者用來為客監控目標。此套軟體只需一分鐘空檔，就能將監控軟體快速植入被害人手機，且無需被害人點閱，市面上智慧型手機都能安裝，三星及Iphone等大廠也未能倖免。一旦遭此軟體鎖定，不論是通話內容、傳送圖檔均無所遁形。[100]

二、我軍網路戰力評估

(一)外在環境

2006年，在臺灣西南海岸外的7級地震，使8條海底電纜產生了18處斷裂，使整個亞洲發生為期數週的網路中斷。海底電纜網路若遭受到針對性的攻擊，尤其是「制扼點」(Choke Point)或島嶼電纜陸地站臺等，其後果將非常嚴重。[101]另外，2015年，在南部左營軍區中山堂高壓變電室等處，有民人剪走近百公斤電纜銅線，造成左營軍區、亞太機電的營運停擺。[102]由此可知，網路戰防護第一層便是實體安全的確保，不管是天災或是人為，其影響將難以估計。

(二)防護能力不足

2015年，臺灣已成為中國駭客試驗場域。該報導並表示，臺灣高科技企業一年有346天遭駭客入侵，是全球平均220的1.5倍，且長達8.5個月才被政府發現。[103]此外，數據顯示，在新一波感染行動裝置，遭駭客攻擊事件中，受影響最大的國家與地區，分別是臺灣、美國和法國。而我國受影響使用者占全球27.41%，高居被駭客竊取網路

[98] 童光復譯、Scott Jasper，〈美國與中共的網路戰爭〉《國防譯粹》(台北)，第 40 卷第 12 期，國防部，2013 年 12 月，頁 79。
[99] 羅添斌，〈反駭要務禁絕中國通訊產品進口〉《自由時報》，2015年9月7日，A8版。
[100] 陳文嬋，〈手機間軟體傳通訊就監控〉《自由時報》，2012年12月20日，版5。
[101] 章昌文譯，Andrea Little Limbago，〈網路治國的多面向本質〉《國防譯粹》(台北)，第43卷第2期，國防部，2016年2月，頁22。
[102] 呂素麗，《竊盜集團偽裝工程人員專偷電纜線》《中時電子報》，2015年4月18日，版A7。
[103] 湯佳玲，〈中國18萬網軍威脅我將分級聯防〉《自由時報》，2015年1月13日，版A8。

憑證第一。[104]由於國情不同，我國在網路安全防護作為上與中共相比較(例如防火長城、輿情分析師)確實略顯不足，若再加上本軍已將智慧型手機開放使用，勢必造成網路安全防護某種程度上的影響。

(三)資訊警覺不夠

2013-14年，中共北京樂視租用遠傳內湖機房安裝高端伺服器設備，在機房直通、遠端遙控下，中共將可超高速且不著痕跡地進行直播串流。[105]2014年，中國人士吳昕去年10月違反法令擅入中華電信台北營運處南四機房，還拍照po網炫耀自稱是「第一個進入臺灣軍事重地的中國人。[106]網路安全除了資訊環境（有、無線電）外，另外重要的便是資訊設備，由於現階段資訊流通均走向雲端技術，如果未做好把關，相信這對網路安全也將造成相關防護上的漏洞。

三、中共網路戰對我最大可能行動

承上述綜合得知，中共對我網路戰攻擊可能行動如后：

(一)平時

藉由網路資源大量竊取個人隱私資料，影響電子商務與金融正常運作。平時藉較低廉價格輸出含後門程式之網通設備至其他國家，後續可為其所用。平時透過社交工程或程式漏洞、網頁附掛程式等方式，針對國軍官兵家用或個人電腦植入惡意程式，進而等待時機，當公務家辦時一舉取得軍事資料。

(二)戰時

兩岸局勢不穩時，透過開放系統與網際網路，實體破壞基礎關鍵設施(如供水及電力系統、交通控制系統等)，恫嚇全體國民。戰時運用現有龐大編組網軍分別對我政治、經濟、金融及軍事設施採分散式阻斷攻擊及先前植入之木馬程式等方式，癱瘓國家網路運作。(如表五)

表五 中共對臺網路戰可能行動要項表

行動作為	企圖
聯合軍事威攝	除運用正規部隊犯臺外，運用中共強大的網民，對本軍發動網路戰攻擊，並經傳媒渲染臺海危險，以引發本軍幹部心理恐慌，打擊本軍民心士氣；另外，藉由島內特工、潛伏人員，針對預先規劃本軍機房或對外實體線路，實施破壞，使本軍無網路可用。
聯合封鎖作戰	配合火箭軍或海、空軍，對我本、外島重要港口、對外航道等實施局部封鎖作戰時；中共網軍，趁本軍實體線路尚未修復前，運用無線電干擾本軍備援系統。

104 〈社論：物聯網便利化資安防護需求殷切〉《青年日報》，2016年4月29日，版2。
105 〈綠委爆中國「樂視網」租遠傳機房 恐有資安疑慮〉，http://www.appledaily.com.tw/realtimenews/article/new/20141215/524435/，2016/9/9。
106 羅添斌、邱燕玲，〈監院調查：中客擅入機房中華電信管制鬆散〉《青年日報》，2015年3月16日，版A2。

聯合火力打擊	運用火箭軍及攻陸飛彈等，優先攻擊本軍營區重要電源設備，使本軍資訊訊備無法使用。
聯合登島作戰	運用特戰人員攜帶網路遮罩器，對本軍重要指揮所實施干擾，並持續運用網路戰發布不利消息，以解本軍抗敵意志。

資料來源：作者整理。

本軍因應之道

一、 研擬新軍事戰略，調整作戰思維

未來網路戰戰法，勢必將先聲奪人。以現今臺、澎防衛軍事戰略構想，「有效嚇阻、防衛固守」，將無法適應於未來網路作戰進程。須知網路空間戰略高地，乃是兵家必爭之地，誰先佔領，誰就得到較大成功勝算。當今，中共當局網路戰罩門，乃是敵國運用網路戰，搧動民眾反中，如果借鏡2013年，俄羅斯出兵佔領克里米亞，能順利得到軍事勝利，便是俄羅斯巧妙運用網路戰先發制人。鑒此，應建議國防部積極調整、研擬新軍事戰略，俾利本軍執行作戰任務。

二、 培育網育人才，整合軍、民科技

誠如上段所述，中共現階段最不想所遭遇的便是敵方運用網路戰顛覆其政權。然而，現階段發展網軍的困境，便是本軍網路人才缺乏，以筆者103-105年曾任本軍資電群營長為例，本營志願役幹部留營率僅達46%，相較於戰鬥部隊而言，略顯過低。究其原因，為本軍現階段志願役資訊加給約3,200元至2,700元不等，與戰鬥加給5,000元相比，此等條件實在無法留住本軍網路人才。建議參照美國陸軍擇優網路人才，設立續服鼓勵金，每月最高可領500美元。[107]相信，此等優渥條件，才能為本軍留住網路人才。

三、 編列教育訓練經費，從教育根本著手

一個資訊系統安全通常包括三部分：硬體、軟體及通信，只要任何一個部分出現漏洞，就可能威脅到整個系統的安全。就本軍現階段而言，因採實體隔離，故就硬體與通信防護不屬問題。然而，在網路工作人員技術方面，目前資訊專長僅一般資訊相關科系畢業，如能從教育著手或由院校證照班納入，將可大幅提升人員素質。以現在業界大型企業任職網路系統工程師(IT)至少須具備下列二項：思科網路管理(CCNA)、微軟系統認證(MCSE)及LINUX網路管理之RHCE、NCLP證照，進階者可進修駭客殺手(CHE)課程。(如表六)此外，可參照美軍作法，在協助網路基層操作人員取得相關軍事技能及晉階所需的認證，並且設立不同軍職專長，如網路密碼戰專業人員(35Q)任務為利用各種技術參數來分析資訊；網路防禦人員(25D)任務為維護基礎設施支援、分析

[107] 同註97。

網路防禦資訊、對事故和網路損壞做出回應。[108]

表六「網路工程師」應具備基本證照一覽表

項次	證照類別	具備能力
1	思科網路管理CCNA(入門)、CCNP專業)及CCIE(高階)	建置與維護網路環境、基本故障排除
2	微軟認證技術專家MCSE、微軟認證IT開發專家MCTS	WINDOWS伺服器架設管理、系統開發
3	Novell系統管理CNA、CNE	網路認證管理與規劃、組裝、設定組態與各式疑難排解
4	Oracle OCADBA	各式參數、資料庫管理

資料來源：作者整理自〈Cisco CCNP課程-「網」上加薪的秘密武器，挑戰薪水60K不是夢〉，http://www.geego.com.tw/cisco%E8%AA%B2%E7%A8%8B%E8%B3%87%E8%A8%8A/cisco-ccnp%E8%AA%B2%E7%A8%8B，2016年9月5日。

四、 辦理網路戰攻、防演練，強化資安警覺

囿於網路安全威脅不斷提升，於2015年，在國安會主導下，已將網路戰納入「漢光31號電腦輔助兵棋推演」演練課目，雖然因外在環境限制下，無法藉由實兵驗證計畫之可行性，故研擬敵網路攻擊方案之真實性就變得更為重要。在驗證方面，希藉由封閉網路，由國防部主導以驗證其處置程序是否周延，藉由不斷的評估、檢討、驗證，以找到最佳防禦作為。此外，更應採不定期資安演練(包含以電子郵件實施社交工程演練、弱密碼攻擊)，凡遭攻擊成功者，定期召開檢討會，辦理資安講習(或再教育)，將資安警覺確切落實至官兵個人。

五、 指管電路受損，緊急查搶應變

根據2016年，〈美軍聯合資訊環境的挑戰與未來〉一文指出，僅打擊敵最弱的鏈路－傳輸層，將能造成聯合資訊環境的破壞，使敵方網路能力受影響。[109]檢視本軍實體網路，將可發現營區內機房與各兵舍間線路，仍有部分線路均暴露在外，其所影響非但易遭外在環境所破壞，亦可成為敵人攻擊之目標。基此，本軍通資部隊應妥善編組人員(有線及資訊專長)，藉由每日巡管，確維線路維護。此外，因應營區對外管道，各級重要電路均屬專網專用，由各作戰區群網傳連區分各排管轄範圍，平戰時任務為電路查搶修作業，業經司令部、基地訓練及本部驗證，均可於時效內完成查搶修作業。此外，若能在作戰區統一主導下，適當指導資電部通信指管大隊共同配合實作演練，相信更能維護資訊優勢。

---

[108] 楊黎中譯，Ferdinand H.Thomas，〈美陸軍網路部隊人才留用(Retaining Soldiers on a New Battlefield:An Army Plugged into Cyber Needs Talented Specialists)〉《國防譯粹》(台北)，第43卷第2期，國防部，2016年2月，頁60-61。

[109] 同註53，頁17-18。

六、 貫徹實體隔離，建立安全環境

通資安全防護手段，在現今各國所採取的手段均為實體隔離，然而如何落實執行？才是影響問題關鍵所在。本軍網路實體隔離政策已施行多年，雖然是封閉性網路，可降低風險及外來威脅，與現行網際網路開放之複雜性有極大區別，管理只需投入相當資源，即可強化自我網路安全防護能力。但回顧這幾年來的資安違規事件，大部分的原因還是人為疏失所造成，其實這不僅是我國普遍存在的問題，其實就美軍而言，其資安違規事件，人員問題就佔70%。故資安防護基本應處作為，應該是不分各軍種、兵科，惟有逐級建立資訊安全觀念（杜絕外來威脅），當可建構國軍整體通資安全服務環境，防範網路攻擊危害，維護國軍通資安全。

結論

根據美國陸軍網路司令部司令卡敦(Edward C.Cardon)中將表示：「未來無論陸軍所面臨的挑戰是什麼，都會有網路的成分在內，陸軍必須要對此做好準備。」[110]總之，網路戰爭是一場別具意義的「民間戰爭」，面對一個不斷強大的中共網軍，不論編制、數量及挹注科技研發經費均大幅成長，確實對我網路安全防護形成重大影響。故平時就必須不分任何兵科，建立「資訊安全、人人有責」的務實態度與良好習慣，並藉由綿密的教育宣導及標準化作業程序，使用網際網路及資訊媒體設備，以確保資訊及相關系統之機敏性、完整性與可用性。未來在面對資訊戰、電子戰的戰場時，方能憑藉堅固的資安防護網，確保國防與資訊安全。

參考文獻

一、 國防部「國防報告書」編纂委員會，《中華民國102年四年期國防總檢討》，(台北：五南文化廣場，2013年)。

二、 國防部史政編譯室、約翰・阿爾吉拉(John Arquilla)，《網路及網路戰》（台北：五南文化廣場，2003年8年）。

三、 國防部史政編譯室、艾利諾・史龍(Elinor Sloan)，《資訊作戰以柔克剛的戰爭》（台北：五南文化廣場，2008年8年）。

四、 國防部史政編譯室、施道安(Andrew Scobell)、伍爾澤(Larry M.Wortzel)，《中共軍文變化》（台北：五南文化廣場，2006年4月）。

五、 國防部史政編譯室、伊凡・費根堡(Evan A.Feigenbaum)，《中共科技先驗－從杘子時代到資訊時代的國家安全與戰略競爭》(台北：五南文化廣場，2006年5月)。

[110] 同註97，頁57。

六、沈方祥，《新世代解放軍》（台北：黎明文化，2003年4月）。
七、張召忠，《網路戰爭》(北京：解放軍出版社，2001年1月)。
八、載清民，《直面信息戰》(北京：國防大學出版社，2002年7月)。
九、東鳥，〈中國輸不起的網路戰爭〉(北京：中南出版傳媒集團)，2010年。
十、蔡國堂，〈共軍資訊心理戰之研究〉《國防雜誌》(桃園)，第27卷第2期，國防大學，2012年3月。
十一、戴政龍，〈對《中國的軍事戰略》白皮書之評析〉《展望與探索》，第13卷第7期，2015年7月。
十二、謝奕旭，〈由習近平宣示裁軍談大陸的國防現代化〉《展望與探索》，第13卷第10期，2015年10月。
十三、鄧炘傑，〈網路公共領域的戰略意義〉《陸軍學術雙月刊》(桃園)，第51卷第542期，陸軍司令部，2015年8月。
十四、章昌文譯，Andrea Little Limbago，〈網路治國的多面向本質〉《國防譯粹》(台北)，第43卷第2期，國防部，2016年2月。
十五、劉慶順譯，John M.Dahm，〈美軍「聯合資訊環境」的挑戰未來〉《國防譯粹》(台北)，第43卷第2期，國防部，2016年2月。
十六、周茂林譯，Jeffrey B Hunter，〈提升美軍聯合資訊環境〉《國防譯粹》(台北)，第43卷第2期，國防部，2016年2月。
十七、楊黎中譯，Ferdinand H.Thomas，〈美陸軍網路部隊人才留用〉《國防譯粹》(台北)，第43卷第2期，國防部，2016年2月。
十八、楊雅棋譯，Alexander Sullivan and Andrew S.Erickson，〈中共軍事戰略的背後意圖〉《國防譯粹》(台北)，第42卷第10期，國防部，2015年10月。
十九、楊黎中譯，Shannon Knight，〈中共獨特的網際空間〉《國防譯粹》(台北)，第42卷第10期，國防部，2015年10月。
二十、陳嘉生譯，Stephanie Meloni and Lloyd McCoy Jr，〈大數據：國防資訊須從雲端發展著手〉《國防譯粹》(台北)，第42卷第7期，國防部，2015年10月。
二十一、劉慶順譯，Robert Haddick，〈美國西太平洋的新戰略〉《國防譯粹》，第42卷第7期，國防部，2015年10月。

作者簡介

王清安中校，中正理工學院88年班、陸軍通信電子資訊學校正規班175期、國防大學陸軍學院98年班，曾任排長、連長、通參官、營長，現任國防大學戰爭學院學員。