中共網路發展暨威脅之研究

作者　國防大學戰爭學院　江國顯中校・于成森上校

提　要

一、自1985年起，中共積極從事「信息戰」發展，從近期美國政府安全部門聲明、國內外新聞媒播或軍事專家研究報告中，可探知中共網路科技不斷地進步，不容小覷。

二、網路運用範疇廣泛，可藉由駭客或電腦病毒等手段，實施干擾、竊取、摧毀等多樣式攻擊作為，進而破壞資訊基礎結構，製造假資訊、癱瘓指揮決策能力，因而導致喪失反擊能力，若不加以有效防範，將成為我國防資訊安全的一大隱憂。

三、國軍未來建軍發展應朝向發展數位及各項預警防護機制，並落實全民國防強化網路資訊安全觀念，培訓專業人才，確保國家與軍隊安全。

關鍵詞：網際網路、駭客、電腦病毒、網路戰

前　言

「不戰而屈人之兵」係孫子兵法對戰爭指導的最高境界，然「先勝後戰、避實擊虛及因敵制勝」的作戰原則，進而追求「致人而不致於人」的戰略優勢，是中華民族所追崇的戰略思維。伴隨著科技發展與作戰思想改變，現代戰爭型態已漸由傳統的殲滅戰、消耗戰朝向癱瘓戰的模式發展。2014年2月27日，中共國家主席習近平主持「中央網絡安全和信息化領導小組第一次會議」，強調統籌布局各方創新發展，努力將中國大陸建設成為網路強國。[1]由此可見，中共在其國力崛起後企

1　於下頁。

圖在「網路世界」躍升為「霸權」的具體實踐。

網際網路緣起與基礎概念

一、緣起

美軍為滿足作戰實需，美國國防部成立先進研究計畫署，積極建構發展網際網路，1960年美國學術界在國防部專案經費資助下，開啟網際網路發展的新紀元。1974年，瑟夫與康恩提出TCP(Transmission Control Protocol)及IP(Internet Protocol)通訊協定，[2]使得不同系統的電腦，能透過規範的格式實施資料傳輸與連結。1990～1993年，隨著全球資訊網(WWW,World Wide Web)瀏覽器的發展，網際網路不再僅限於收發電子郵件及資料傳輸，更增添圖片登錄及提供瀏覽等功能；[3]另外網際網路也廣泛運用在軍事、學術及日常生活上，使得使用者運用更多元及便利化(如表一)。

二、網際網路基礎概念

(一)網際網路重要性

網際網路(Internet)並不是真正的網路，乃是由數臺電腦乃至於數百臺、數千臺電腦，透過不同的傳輸媒介與設備，彼此相連接起來之謂。網路不僅可使資料共享、大幅降低傳輸成本及加快傳輸速度，最重要的是提供多元化的人際溝通管道及多媒體的互動式娛樂。

(二)網際網路特色

基於網際網路「封包交換」、「TCP/IP通訊協定」及「主從式運算」等基本運作，[4]以及WWW(World Wide Web)連結技術，使得網際網路具有下列特色：[5]

1.無時空限制的全球連線

TCP/IP開放式的通訊協定及伴隨智慧型手機盛行，任何人皆可輕易連結上網，使得網路成為一個無遠弗屆、沒有任何時間限制的連線環境。

2.豐富的資訊資源

無所不在的便利是網際網路的特色，全世界的各種資料因此而得以串連起來，創造了豐富的資訊資源，任何人都可以是內容創造者與提供者，也可以輕易地在網路上分享各種資訊，例如政府機關公開資訊、圖書、應徵求才或高科技等資料庫。

3.超連結簡單便捷

透過Web(Web-browser)網頁瀏覽器及HTTP(Hyper Text Transfer Protocol)超文字傳輸協定，使用者可以超連結方式，連結網頁中各種不同的多元化資料，透過

1 新華社，〈中央網絡安全和信息化領導小組第一次會議召開〉，http://big5.gov.cn/gate/big5/www.gov.cn/ldhd/2014-02/27/content_2625036.htm，檢索日期104年5月14日。

2 吳顯東、張文鐘，〈網際網路的誕生：科學月刊全文資料庫〉，http://campus2.chgsh.chc.edu.tw/science/content/1998/00060342/0005 htm，檢索日期104年01月05日。

3 毛慶禎，〈網際網路簡史〉，http://blue.lins.fju.edu.tw/mao/internet/history.htm，檢索時間：104年1月13日。

4 〈電腦網路的基本知識〉，http://webftp.cogsh.tp.edu.tw/cti573/bcc2012/handout/unit5.htm，檢索時間：104年1月13日。

5 賴香菊，《網路行銷：電子商務理論與實務》(臺北：華泰文化，西元2000年)。

表一　網際網路發展簡史

年代(西元／年)	重大事件摘列
1960年	建構網際網路發展思維。
1974年	建立TCP/IP通訊協定。
1990年	廣泛運用於軍事及學術上。
1991年	WWW全球資訊網及網頁瀏覽器發明，網路功能提升。
1993年	美國推動NII國家資訊基礎行動網領(National Information Infrastructure)建構資訊高速公路。
1995年	提出網路光世代概念，建構高速傳輸技術FTTx(Fiber To The x)。
1999年	無線網路技術發明。
2011年	光纖技術普及。

資料來源：1.王佳煌，《資訊社會學》(臺北：學富文化，西元2000年)。
2.周獻彬，〈中央研究院FTTx光世代服務簡介：中央研究院計算中心通訊電子報〉，http://newsletter.ascc.sinica.edu.tw/news/read_news.php?nid=1803，檢索時間：104年1月13日。
3.作者自行整理。

Web瀏覽器加上主從式運算及封包交換的運作，網路資源獲得不僅容易，也非常迅速、便捷。

4.遠程終端服務(Telnet)

透過網路連線至遠方主機，進行即時線上作業，即可使用其主機上之資源、互相傳送或擷取檔案。在Internet上提供相當多此類資訊系統，包括圖書館線上目錄、資訊系統、檔案。

網際網路威脅概念

一、網路威脅概念

現今網路安全已是全球性的問題，世界各國對資訊基礎建設的依賴越來越重，伴隨網路興起使得網路資安事件不斷發生，然漏洞百出的系統讓有心人士很容易入侵進行破壞。[6]從近年來網路遭到入侵相關報導中，網路各種類型的攻擊與破壞行為與日俱增，駭客技術不斷精進，手法越來越多元，導致世界各地的電腦網路系統遭到破壞，造成的經濟損失達數百億美元。

二、常見入侵手法

(一)近期網路入侵案例

隨著網際網路普及與便利，上網幾乎已成為人類生活上不可或缺的行為，也造成不肖人士藉由網路工具破壞政府及企業重要基礎設施，造成生活或經濟上相當程度的損失。近期網路入侵案例如下：

1.2014年5月20日，中共5名軍官入侵美國鋁業、阿勒格尼技術、太陽能、鋼鐵、西屋電氣及航太科技，遭美國司法院起訴。[7]

2.2014年7月11日，中共駭客入侵美

6　彭錦珍，〈資訊時代中共國防現代化之研究 ── 解放軍資訊戰發展及其對臺海安全之衝擊〉，收錄《復興崗學報》(臺北)，國防大學政治作戰學院，西元2004年，頁187～218。

7　於下頁。

國聯邦政府人事管理辦公室電腦系統，竊取美聯邦雇員個資。[8]

3.2014年10月20日，中共駭客侵入美國金融業，盜取重要信息，來自中共的網路犯罪對美國安全和經濟，產生不利影響。[9]

4.2014年11月14日，中共駭客入侵美國氣象系統和衛星網路，迫使網路安全小組封閉了災害規劃、航空、航運的關鍵數據，以及幾十個其他重要用途的數據。[10]

5.2014年11月17日，駭客入侵美國務院網路系統，影響電子郵件流量和進入公用網站作業。[11]

6.2014年12月19日，索尼影視內部網路遭北韓駭客入侵，多部電影遭竊，重要機密外洩，美國白宮定調為國安事件。[12]

7.2015年1月13日，伊斯蘭聖戰組織IS駭客，入侵美軍司令部滲透取得帳號，竄改多家媒體網頁，並宣傳宗教聖戰。[13]

(二)常見入侵手法

只要懂得如何使用工具，就可以輕易發動網路入侵或攻擊，近年來，從媒播報導中得知，企業組織及重大關鍵設施遭駭客入侵事件頻傳，常見入侵手法如表二。

綜合以上歸納得知，隨著科技日新月異，戰場型態也快速轉變，以往肉搏相對、兵戎相接的傳統戰場均不復見。由於人類對資訊與數位的依賴，在未來的軍事整備上，「網路戰」或「資訊作戰」的戰爭整備，仍然是耗費龐大，甚至超越任何實體武器，憑藉網路高科技技術打擊或癱

7 Taiwan news,"美國起訴5名中國網軍中國憤怒回應,"http://taiwannews.com.tw/etn/news_content.php?id=2485950，檢索時間：104年1月19日。

8 自由時報，〈中國駭客 竊取美聯邦雇員個資〉，https://tw.news.yahoo.com/%E4%B8%AD%E5%9C%8B%E9%A7%AD%E5%AE%A2-%E7%AB%8A%E5%8F%96%E7%BE%8E%E8%81%AF%E9%82%A6%E9%9B%87%E5%93%A1%E5%80%8B%E8%B3%87-221022243.html，檢索時間：104年1月19日。

9 Taiwan news，〈美國起訴5名中國網軍中國憤怒回應〉，http://taiwannews.com.tw/etn/news_content.php?id=2485950，檢索時間：104年1月19日。

10 華盛頓郵報，〈中共駭客入侵美國氣象系統和衛星網絡〉，http://www.epochtimes.com/b5/14/11/14/n4295518.htm，檢索時間：104年1月19日。

11 自由時報，〈俄駭客攻白宮美嗆反擊〉，https://tw.news.yahoo.com/%E4%BF%84%E9%A7%AD%E5%AE%A2%E6%94%BB%E7%99%BD%E5%AE%AE-%E7%BE%8E%E5%97%86%E5%8F%8D%E6%93%8A-221036166.htmll，檢索時間：104年1月19日。

12 TVBS，〈索尼被駭北韓搞鬼白宮定調國安事件〉，https://tw.news.yahoo.com/%E7%B4%A2%E5%B0%BC%E8%A2%AB%E9%A7%AD%E5%8C%97%E9%9F%93%E6%90%9E%E9%AC%BC-%E7%99%BD%E5%AE%AE%E5%AE%9A%E8%AA%BF%E5%9C%8B%E5%AE%89%E4%BA%8B%E4%BB%B6-094200846.html，檢索時間：104年1月19日。

13 民視新聞網，〈網路聖戰IS駭客入侵美軍司令部〉，https://tw.news.yahoo.com/%E7%B6%B2%E8%B7%AF%E8%81%96%E6%88%B0-is%E9%A7%AD%E5%AE%A2%E5%85%A5%E4%BE%B5%E7%BE%8E%E8%BB%8D%E5%8F%B8%E4%BB%A4%E9%83%A8-030040785.html，檢索時間：104年1月19日。

表二　常見入侵手法一覽表

入侵型態	破壞方式
暴力密碼攻擊	輸入admin(意旨管理員)使用名稱，嘗試輸入數千種密碼或是利用數萬台的殭屍電腦企圖登入系統。
傀儡(殭屍)系統程式	利用奴隸傀儡程式，大量複製訊息，使網站瞬間湧入大量資訊，導致系統功能癱瘓。
擷取網路封包	擷取主機所傳送的封包，並解碼以獲取重要資料。
利用作業系統漏洞入侵系統	藉由作業系統程式設計的漏洞，使網路駭客可經由這些漏洞入侵系統。
特洛依木馬程式	暗藏隱含潛伏電腦病毒的程式碼，藉由Active X & Java Applet技術，輸入病毒，達成入侵破壞目的。
冒充系統內網路的位置	入侵者把自己偽裝成其他的系統，同時偽裝資料封包的發送地址，將封包透過網際網路傳輸給另一系統。
盜用使用者密碼	竊取使用者或系統管理者帳號、密碼，以取得特殊權限，為所欲為。
植入破壞晶片裝置	將上述幾類病毒程式，直接壓(燒)製於電腦晶片中，藏匿於硬體可連接網路或利用無線電子方式來釋放病毒或傳輸資料至指定地區。
電腦病毒	指編製或在電腦程式中植入可破壞干擾電腦功能藉以毀壞數據，以影響電腦使用，常見惡意程式計有寄生蠕蟲、邏輯炸彈、間諜軟體、垃圾郵件軟體等。

資料來源：1.朱延智，《臺灣安全》(臺北：幼獅出版社，西元2000年)，頁136。
2.作者自行整理。

癱敵方致命要害，便可收不戰而破之效，資訊安全的威脅，將會是日後最大的挑戰，故網路作戰在未來戰爭中將扮演重要角色。

中共網路發展思維及階段

一、網路發展思維

自1985年起中共已高度重視網路作戰，從最近幾次演訓狀況及國內、外軍事專家的研究報告顯示，中共在網路發展方面已有相當成就，其網路發展思維如次：

(一)第一次波灣戰爭促使網路發展

1991年第一次波灣戰爭，美軍藉由高科技電子設備，竟能運籌帷幄、指揮調動自如，除有效掌握戰場的變化，又能壓制伊拉克的電子及癱瘓網際網路等設備，徹底掌控戰場，打一場絕對優勢的高科技戰爭。[14]第一次波灣戰爭顛覆了中共傳統戰略思維，開啟了資訊化的戰爭軍事事務革命。

(二)打贏高技術條件下的局部戰爭之戰略指導

1991年第一次波灣戰爭促使中共展開對高技術戰爭的研究，前中共國家主席江澤民指出：「第一次波灣戰爭是場典型的高技術戰爭」，這也讓解放軍明瞭，不論在武器裝備及高技術科技上與西方國家的差距正逐漸拉大，所以必須全面精進資訊網路技術、海空軍戰略武器、戰略決

14　蕭朝琴，〈中共發展高技術資訊戰爭對臺安全之威脅〉《共黨問題研究》，25 卷6期(1999年6月)，頁56。

策及指導的改革。[15]2004年12月中共公布「2004年中共國防白皮書」指出：「人民解放軍須立足打贏信息化條件下局部戰爭，依建設信息化軍隊、打贏信息化戰爭的目標，深化改革，銳意創新，加強質量建設，積極推進以信息化為核心的中國特色軍事變革」，[16]中共在新軍事戰略方針指導及前瞻新穎之戰爭型態，除參考美軍等先進國家的資訊作戰理論，擷取適用的內容作為發展與實踐之依據；另根據作戰任務與部隊實況，發展適合共軍剋敵制勝資訊作戰之理論基礎，並積極從事網路發展之研究。[17]

(三)發揮「網電一體戰」作戰優勢

中共積極發展「網電一體戰」主要係不強調大規模殺傷，進而重視癱瘓作為；其交戰方式由接觸轉向非接觸作戰；行動模式從線性向非線性轉變；作戰指揮從預先計畫變成同步指揮。這種作戰方式，基本上是貫徹「不戰而屈人之兵」的用兵思想，以「非對稱性戰略」創造有利的戰略態勢，減少附帶傷亡的數量，並迫使對手快速進入政治談判階段。[18]

(四)提升國家經濟競爭實力

網際網路是國家建設之基礎設施，也是推動經濟發展和社會進步的重要支撐。藉由網路發展，加快產業的增值服務、現代物流、專業諮詢服務等，網際網路發展與技術研發戰略，將提升國家經濟競爭實力。

(五)有利意識形態的政治操作

中共是世界上僅存的幾個實行社會主義及一黨專政制度的國家，基於維護社會政治穩定，以及政治不受外國各方不同勢力影響，凡危及國家和社會穩定的不利資訊，中共均主動實施網路、輿論控制等政治操控，以防止進一步轉化為社會與政治危機。

二、中共網際網路發展階段

中共網際網路建設可區分準備、基礎設施建設、建設發展及全面展開等四個階段，分述如次：

(一)第一階段：網際網路準備階段

1984年鄧小平提出：「開發信息資源，服務四化建設」，成為提升經濟產業發展重要依據；1986年中共推動「國家高技術研究發展計畫」；[19]1987年中共建立網際網路電子郵件節點；1989年中共推動「國家電腦與網路設施計畫」，建立北京、清華大學校園與中共科學院網路的高速網際網路與計算中心，以作為學術網路之基礎，開啟中共網路建設啟端。[20]

15 江澤民，〈關於軍事戰略方針和國防科技問題〉，中共中央文獻編輯委員會編輯《江澤民文選輯第一卷》〈北京：人民出版社，2006年)，頁142～147。

16 中共國務院新聞辦公室，〈2004年中國的國防〉《新華網》，http://news.xinhuanet.com，檢索時間：104年7月17日。

17 平松茂雄原著，楊鴻儒編譯，《江澤民與中國共軍》(臺北：凱侖出版社，西元1999 年8月)，頁20。

18 曾復生，〈中共國防戰略新思維的特質：財團法人國家政策研究基金會〉 http://www.npf.org.tw/post/3/9104，檢索時間：104年1月20日。

19 劉延章，〈我國資訊化建設及資訊服務和開發問題研究〉《信息科學》，第11期，西元2003年。

20 於下頁。

(二)第二階段：基礎設施建設階段

1993年中共藉由網路科技發展大力推動資訊化產業基礎和各類資訊系統建設；1994年中共透過美國Sprint公司[21]協助，啟動TCP/IP[22]協議的連結接入Internet，成為國際網路的第71個國家，啟動網際網路的服務，並陸續完成科學技術、教育、科技研發及公用電腦等網路建設；1995年籌建八縱八橫光纜及數位化網路建設。

(三)第三階段：建設發展階段

1996年中共成立國務院資訊化工作領導小組，組建全國性網路提供網際網路聯網服務；1997～2000年，陸續將科學技術、教育、科技研發、公用電腦與產業網路加以連結，[23]並完成八縱八橫光纜及數位化網路建設，以奠定經濟競爭實力基礎，滿足網路使用需求。[24]

(四)第四階段：全面展開階段

由於光纜建設涵蓋中國大陸計31個省市、659個城市、2,070個縣(區)、61.5萬個行政村，[25]連接日、美及歐洲等多個國家陸地和海底光纜，透過寬頻高速網路基礎建設，開展跨境電子商務合作，積極活絡全球網路經濟的繁榮發展。

三、中共國家基礎建設(NII)[26]及國防基礎建設(DII)[27]建設發展

(一)國家基礎建設(NII)發展

中共自1978年經濟改革開放以來，社會經濟型態漸漸在轉變，為促進經濟發展與縮短各國網際網路之差異，1993年提出「三金工程」[28]積極推動國家資訊基礎建設計畫，將衛星、光纖、微波、無線等傳播系統整合成資訊平臺，建設網路資訊高速公路，並訂定信息化政策及建立法律規範，如電信安全、資源分配、機構與管理規範等；1996年1月成立國務院資訊化工作領導小組；1997年3月成立互聯網；1998年3月成立信息產業部。就發展歷程言，中共國家基礎建設發展，主要是

20 王雅慧，〈中共管制網際網路之研究 ── 以政治向度探討〉(中國文化大學中國大陸研究所，碩士論文，2002年)，頁51。

21 美國Sprint公司成立於1938年，前身是1899年創辦的Brown電話公司，當時是堪薩斯州的一家小型地方電話公司，目前Sprint公司已成為全球性的通信公司，在美國主要提供長途通信和移動通信業務。

22 TCP/IP：Transmission Control Protocol/Internet Protocol，中譯傳輸控制協議/因特網互聯協議，簡稱網絡通訊協議。

23 楊家誠，〈網際網路對中共統治之影響〉《共黨問題研究》(臺北)，第27卷10期，西元2001年10月，頁86。

24 王立德，〈中國大陸知識經濟概念探討以電信與網際網路整合為例〉(東華大學大陸研究所，碩士論文，2000年)，頁87。

25 吳慰慈，〈我國信息化建設的進展和挑戰〉《G9圖書館學、信息》，第3期，西元2004年，頁21～28。

26 NII, National Information Infrastructure,國家基礎建設。

27 DII, Defense Information Infrastructure,國防基礎建設。

28 「三金工程」，即意指金橋工程、金關工程和金卡工程，其目的係建設中共「信息準高速國道」，如同臺灣「資訊高速公路」謂之。

為促進國家經濟利益、科學教育人才培育及網路空間技術發展，藉由政府力量推動資訊基礎建設，以提升國家實力及競爭力。

(二)國防基礎建設(DII)發展

中共自從「八五」計畫[29]即提出以光纖傳輸為主的國防資訊基礎建設，籌建指揮管制系統及二砲部隊指揮中心，並在西山籌建指揮所，作為全國性作戰指揮中樞；1989年完成「八縱八橫」，[30]共計16條骨幹光纖網路連接各軍區，並於「九五」計畫[31]繼續興建長途與區域光纖網路，[32]並尋求C4ISR關鍵技術突破，開發具戰略層次智能網，積極研發聯合指揮自動化及戰略預警系統使得各種武器系統連結為一有機體系，邁向科技化、自動化及智能化之趨勢，提升遠程攻擊能力，打擊精度提高，保持絕對優勢戰力，期達到「決勝千里之外」之目標。

中共網際網路發展現況

一、就使用普及率言

依中共互聯網信息中心數據顯示，2014年中國上網人口已達6.32億，[33]較2013年增加1,442萬人，成長率為1.1%，網路普及率為46.9%。其中利用手機上網為83.4%，主要應用於電子商務、休閒娛樂、新聞資訊、即時通訊等範圍，預判未來上網人數仍會持續攀升。[34]

二、就應用層面言

因網路的快速發展，已影響民眾的日常生活行為，截至2014年12月，中共網路零售市場交易規模達12,205億元，較2013年同時期增長64.7%，預判2015年

29 「八五」計畫，指中共所制定從1991～1995年，第八個五年計畫，其計畫主要是以國民經濟發展為主，主要的內涵以提升國民生產總值與進出口總額獲利、廣播、電視及網路系統建設、興建鐵、公路與鐵路電氣化，以及改善貧困等。

30 「八縱八橫」採取橫向與縱向交錯之網狀建設；「八縱」是指1.自牡丹江經大連、煙臺、青島、杭州、福州至廣州；2.自齊齊哈爾經白城、承德、北平、石家莊、鄭州、武漢、長沙、廣州、海口至三亞；3.自哈爾濱經長春、瀋陽、天津、濟南、合肥、南京至上海；4.自北平經衡水、九江、南昌至廣州；5.自呼和浩特經太原、襄樊、南寧至北海；6. 自呼和浩特經百安、成都至昆明 ；7.自蘭州經格爾木至拉薩；8.自蘭州經成都、貴陽至南寧。「八橫」是指1.自天津北平經呼和浩特、銀川至蘭州；2.自青島經濟南、石家莊、太原至銀川；3.自上海經南京、合肥、信陽、南陽至西安；4.自連雲港經徐州、鄭州、西安、蘭州、烏魯木齊至伊寧；5.自上海經南京、武漢至重慶；6.自杭州、福州經南昌、長沙、貴陽至成都、重慶；7.自廣州經南寧至昆明；8.自上海經南平、廣州、北海至昆明。

31 「九五」計畫，指中共所制定從1996～2000年底，第九個五年計畫，其計畫主要是以國民經濟和社會發展為主，主要的內涵為消滅赤貧現象、中西部地區平衡發展、培育優質農林牧漁及研發信息電腦技術。

32 湯添福，〈中共信息戰之研究〉(國立中山大學中國與亞太區域研究所，碩士論文，2009年)，頁114。

33 iThome新聞，林妍溱，〈中國上網人口達6.32億手機首度超越PC〉，http://www.ithome.com.tw/news/89545，檢索時間：104年5月14日。

34 同註24。

可達到17,155億；另政府和公益性資訊資源開發，使得電子商務管理機制快速推進。

三、就政治層面言

(一)隨著網路成熟發展，已逐步觸及重大公共性敏感議題，如兩岸敏感問題、2014年11月臺灣「九合一地方公職人員選舉」、「九二共識議題」等，[35]中共不再全面封鎖或迴避，但許多網站所發布的消息或資訊都經過修飾，[36]若想使用如「臉書」、「Youtube」等熱門網站，依中共網路審查機制這些有問題的網站就會進行「網路監控」，如果百姓想要進入這些被封鎖的網站，只能利用各種管道進行所謂「翻牆」。[37]

(二)2015年2月28日，在人民網及優酷網播出由前央視記者柴靜小姐籌備一年時間拍攝的「穹頂之下」霧霾調查紀錄片，短短幾天便獲得大約兩億點擊率，影片直接反映出目前大陸霧霾、產業污染、政策和執法等層面問題，掀起民眾強烈關注。此舉中共當局如不積極制止，就有可能會導致社會結構動盪，甚至影響中共政權，種種考量在中共「兩會」(中華人民共和國全國及地方各級人民代表大會、中國人民政治協商會議之簡稱)舉行期間，中共當局已全面封殺影片，目前在大陸主流網站，如騰訊、優酷及搜狐等已經找不到這部紀錄片。

(三)由此顯示，中共欲藉由「互聯網」新興傳播媒體宣達國家進步及強化政治掌控；但同時必須面對「互聯網」的新興公共輿論與自由表述空間，肇生中國社會型態改變、人民思想解放，以及對其政權所形成的威脅，因此，網際網路發展對於中共領導當局而言，雖可富國強兵，但亦會動搖其政治統治基礎，對其政治生態將產生相當程度的影響。

四、就經濟層面言

習近平主席在2014年11月世界網際網路大會開幕式中提出：「願與世界各國實施網路合作，構建網路空間及國際網際網路治理體系」。然事實上，中國大陸利用網路宣傳，開啟與世界溝通，以及建立對外貿易經濟合作的窗口，並積極加速經濟現代化進程，提倡經濟信息化、金融電子化及對外經貿自動化之目標，目前中共致力亞洲基礎設施投資銀行、絲路基金的籌建，網路設施建設將是未來投資重點之一。[38]

五、就軍事層面言

(一)網際網路的進步，相對的影響中共戰略及用兵思維，網際網路亦是不對稱作戰及爭奪先制權的重要憑藉，網際網路

35 人民日報，〈臺灣九合一選舉結果〉，http://www.bbc.co.uk/zhongwen/trad/china/2014/12/141202_taiwan_election_onlinecomments，檢索時間：104年1月21日。

36 Peopo公民新聞，張亦尚、賴冠廷、林羿岑、陳沛吟，〈兩岸上網限制差異大陸需「翻牆」才能享網路自由〉，http://www.peopo.org/news/113177，檢索時間：104年1月22日。

37 「翻牆」一詞是指突破網路審查或突破網路封鎖，是指對網際網路審查封鎖的限制，繞過相應的IP封鎖、埠封鎖、內容過濾、域名劫持等，實作對網路內容的存取。

38 國際在線新聞，韓基韜，〈網路基礎設施建設將成為重點投資領域〉，http://big5.cri.cn/gate/big5/gb.cri.cn/42071/2014/11/19/5311s4772382.htm，檢索時間：104年1月20日。

運用時機不分平戰時期，亦是中共蒐集情報的工具，使用的範圍及手段非常廣泛，舉凡政治、經濟、民意輿情掌握或高科技軍事工業等都是主要蒐集項目。對於依賴網路科技的國家，不論在政治、軍事、經濟、心理及社會上將形成另一個隱憂，其可運用的範圍包含戰場監偵管制、部署運用、定位管制、精準攻擊、反制等。

(二)目前負責網路戰的單位包括解放軍總參謀部、7大軍區、國防科研機關、各級軍事院校等，平時係以負責網路竊密滲透，戰時則實施網路攻擊，中共並暗中扶植民間駭客組織，從旁協助網路間諜活動，據「美中經濟委員會」報告評估，中共「網軍」[39]多達18萬人(如表三)；另成立「中央網路安全及信息化領導小組」，統合相關部會職能，藉由頂層設計、統籌規劃、創新發展等，企圖建設網路強國。[40]

(三)解放軍7大軍區所轄之電抗團(營)，可採任務編組方式或廣納民間IT產、官、學界、省屬縣市及鄉鎮之民兵共同組成，配合各項軍演實施網路作戰。其組織編組模式如下：[41]

1.電子戰分隊

以連為單位或由民間電子行業抽調人員編成，負責偽冒、電子干擾、反干擾、欺騙及攻擊目標國之電子系統。

2.網路戰分隊

以連為單位或由民間相關高等院校、科研單位抽調專業人員組成，除負責設置自我防衛保護己方網路安全外，大量製造或複製電子垃圾，阻塞目標國之網站，導致系統功能癱瘓。

3.救護分隊

以連為單位或由民間相關行業中抽調專業人員訓練編成，負責網路系統硬軟體維修和復原工作。

4.駭客分隊

以排為單位，吸收學校資訊科系、社會熱中於程式設計的人士或從事網際科技公民機構等各階層為主，具有相關專長之人才組成，以入侵目標國網路為目標，並負責蒐集情報或植入後門、病毒程式進行竄改、銷毀及破壞。

5.網路民兵組織

由北京、清華、交通及復旦等著名院校資訊科系、研究所成立網路民兵分隊，其組織規模概等於營級編制，轄不同專業之連、排、班；運用上，可適時抽調相關人員實施彈性編組，主要負責軟、硬體系統維修、應用理論研究、科研技術發展等。

綜合以上歸納得知，近年來中共經濟

39 所謂「網軍」首次出現是在1999年中共軍報，其任務在於有效進行網路戰攻擊及防禦。此為中共為了因應超限戰，建軍方向朝向陸、海、空、天、電、網一體化的作戰方式而發展。

40 Yahoo奇摩新聞，謝莉慧，〈國安局證實 中共「網軍」多達18萬人〉，https://tw.news.yahoo.com/%E5%9C%8B%E5%AE%89%E5%B1%80%E8%AD%89%E5%AF%A6-%E4%B8%AD%E5%85%B1-%E7%B6%B2%E8%BB%8D-%E5%A4%9A%E9%81%9418%E8%90%AC%E4%BA%BA-063307540.html，檢索時間：104年1月20日

41 廖文中，〈中國網軍：國安、公安與解放軍〉《全球防衛雜誌》(臺北)，第271期，西元2007年11月，頁3。

蓬勃發展，中共與美國達成加入WTO的協議後，已逐漸放寬網際網路市場的限制，使得網際網路成為中國大陸下一波的工業革命，然而一個國家的資訊科技技術與網際網路發展，也是評估網路作戰能力的重要關鍵因素之一，目前中共採用的網路戰策略，其目標不僅針對國家、政府及商業基礎設施和網路，甚至破壞目標國的軍事系統運作或毀損其軍事防禦及攻擊能力，一旦攻擊得逞，就會導致系統操作失靈，進而降低指揮自動化系統、武器性能及軍隊後勤之運作。然而中共積極尋求軍民技術的結合，有計畫的推廣網際網路的應用，從近期媒播幾則有關網路駭客入侵的報導中不難發現，中共網路科技尤其是網路戰的能力不斷增長，甚至縮短與先進歐

表三　中共網軍部隊一覽表

區分	運用範圍
國防動員委員會 信息動員辦公室	負責吸收與培訓民間資訊科技人才。[42]
南京軍區 信息戰情報研究中心	負責對臺通訊打擊、辨識與選定竊取的情報。
61398部隊	隸屬解放軍總參謀部技術偵察部第三部第二局，主要從事網路安全、網路攻擊訓練。[43]
61419部隊	為高科技軍事科研部隊，隸屬總參謀部，主要從事對各國政府、軍事承包商與研究機構發動駭客任務，竊取機密。
61486部隊	位於上海閘北區，支援中共太空監測網路，主要從事盜取美國的航天及衛星技術、網路情蒐與駭客入侵。[44]
華為技術公司 中興通訊	設有黨務組織與官職，可提供中共網路戰部隊所需之資訊服務。
武漢大學 藍翔技校 交通大學 信息工程大學	與民間大學院校合作，培育未來共軍資訊科技人才。
紅客聯盟 網路水軍 五毛黨	屬駭客集團，主要以入侵攻擊或竊取資料，以及嘗試癱瘓目標國關鍵基礎設施運作。

資料來源：1.林穎佑，〈大陸網軍與APT攻擊〉《展望與探索》，第11卷3期，西元2013年3月，頁95～110。
2.蘋果即時報，呂一銘，〈中共網軍終於露出猙獰面目了〉，http://www.appledaily.com.tw/realtimenews/article/new/20140620/420118/，檢索時間：104年1月29日。
3.大紀元，秦雨霏，〈紐時：第二支中共部隊捲入網絡間諜醜聞〉，http://www.epochtimes.com/b5/14/6/11/n4175456.htm，檢索時間：104年1月29日。
4.作者自行整理。

42　林穎佑，〈大陸網軍與APT攻擊〉《展望與探索》，第11卷3期，西元2013年3月，頁95～110。

43　蘋果即時報，呂一銘，〈中共網軍終於露出猙獰面目了〉，http://www.appledaily.com.tw/realtimenews/article/new/20140620/420118/，檢索時間：104年1月29日。

44　大紀元，秦雨霏，〈紐時：第二支中共部隊捲入網絡間諜醜聞〉，http://www.epochtimes.com/b5/14/6/11/n4175456.htm，檢索時間：104年1月29日。

美國家間的差距。網路科技是21世紀時代的必然產物，是未來軍事事務革命的核心，也是繼核武器發展後，中共必須再次投入大量精力去研發及運用，才能真正在未來戰場上實現高技術條件下局部戰爭，達到孫子兵法所述「不戰而屈人之兵」的目標，秉持「科技強軍」的原則，面對美國強大的軍事科技，中共唯有積極發展網際網路，研擬避實擊虛的不對稱思維，才能化被動為主動，進行抗衡。

中共網際網路發展特、弱點及對我國的影響

一、中共網際網路發展特、弱點

中共國家主席習近平及中共國務院總理李克強先生自上任以來，積極推動深化改革，藉以提升中國大陸的發展，尤其置重點於第四代移動通訊、建設光纖高速網路縮短城鄉差距、電子商務的創新及物流產業建設等，經過20多年發展，中國大陸已全面進入Web2.0時代，涵蓋政治、經濟、文化、醫療、教育及軍事等領域，若遭意圖不軌人士運用，就會成為另一種新隱憂及威脅，其特、弱點如次：

(一)特點

1.網際網路改變人們的生活形態，也帶動新的軍事事務革命，[45]並可強化其指、管、通、資、情、監、偵等能力。

2.網際網路可依情資蒐集、心理控制、資訊威懾、先制等不同層面需求，適時調整或轉換其形式，如駭客戰、網路戰、心理戰等。

3.運用目標範圍廣、多元及低強度的特徵，且無明顯之交火作為，可使網路衝突事件層出不窮，並可於短時間內控制或癱瘓各類指揮機構、運輸、水源及電力系統等，除造成政治、社會、經濟、軍事等全面或局部性傷害，亦會引發社會大眾恐慌。

4.網路無遠弗屆，無法精確掌握、偵測、預警或防範，可收連續無限制性猝然、突襲之效果。

(二)弱點

1.網路的便利，使得中共國家基礎建設與軍隊的資訊系統非常依賴網際網路，潛在的敵人可能利用電腦、網路或定向能武器對此實施攻擊及破壞，成為致命的弱點。

2.網路系統為複雜且龐大的高科技實體，亦可連結個人、企業、社會及國家成為一個整體網路，任何一個環節受到攻擊或破壞，都可能牽一髮而動全身，影響整個運作，進而危及國家安全。

3.駭客組織不易掌握，網路入侵行為日益嚴重，若自我防護能力不足，除會造成資安隱憂，亦有可能掀起全國性的網路大戰。

4.網際網路發展影響人類的文化層面非常廣泛，舉凡政治、經濟、社會、人文，無不與其產生互動，正因傳播力量迅速、網路論壇交流範圍擴大、大量網民人氣滙聚，群眾監督輿論、間接催化民主意識等，為中共政權帶來隱憂。

二、中共網際網路發展對我國之影響

隨著網際網路日益快速發展，新網路時代顛覆中共政府的傳統架構，社會價值

45 蕭朝琴，〈中共發展高技術資訊戰爭對臺安全之威脅〉《共黨問題研究》(臺北)，第25卷6期，西元1999年6月，頁58。

體系也產生巨大影響，透過網路快速流通，在多元的環境中衍生不少問題。然網路運用可循多渠道、多形式的發展，如網路戰或網路威懾等，所針對的目標已非限定於軍事層面，亦可於短時間內或一次微不起眼的小型攻擊行動中，威脅或癱瘓目標國之政治宣傳、經濟財政、指揮管制、科技建設、民生設施等系統，乃至國民精神、觀念或心理，造成全面或局部性之傷害。本文僅就中共網際網路發展對我國政治、經濟、軍事、心理等領域影響析論如次：

(一)就政治言

1.自由民主政治成就是我國最寶貴的普世價值，倘若中共利用網路或國內、外各類傳媒系統，利用各種文攻手段對我政權(策)作為實施操弄或破壞，[46]那麼我們引以為傲的自由民主政治，將會產生重大影響。

2.現代戰爭之平、戰時劃分已漸趨模糊，作戰型態已非僅限於戰車、戰機、軍艦、甚至核武飛彈等有形戰力的較量，而是利用網際網路實施無形博弈。中共一直希望能透過雙方的政治談判解決兩岸問題，倘若中共決心以武力犯臺，必須花費龐大軍費，且美國為維護其在亞太地區的國家利益，將極可能介入。網路作戰包含攻勢與守勢兩種形態，主要的目的是設法影響目標國決策系統，因此發展網路作戰能力，就是為了未來武力犯臺做反制準備。

(二)就經濟言

1.網際網路可打破空間及距離的藩籬，可即時掌握全球市場經濟與各種商業契機，網際網路的發展開啟邁入國際化契機，造就新的就業機會，成為經濟創新的催化劑，以及降低企業、供應商和承包商之間的溝通成本，是故也改變傳統商業、交易(如實體店面、賣場)的經濟模式。

2.美國中央情報局局長麥克爾．海登(Michael Hayden)明確指控，中共網路發展對美國傷害最深的，就是在經濟領域上的網路間諜活動，包括竊取國家機密、公、私企業商業機密、盜取知識財產權、工業技術機密及竊取談判策略等。[47]

3.近年來我國許多企業組織或重大關鍵設施疑似遭中共駭客入侵，利用木馬、後門、病毒或間諜程式等，企圖破壞或攻擊金融機構主機，竊取主機內的帳戶資料、散布虛假消息或惡意買賣貨幣造成經濟危機，企圖使我經濟陷入混亂(如表四)。[48]

表四　中共利用網路破壞我經濟案例

時間(年／月／日)	入侵案例
2014年11月20日	中共研製各類惡意行動App應用程式，駭侵個人行動裝置，竊取特定目標的電郵帳密、通聯以及通話內容等敏感資訊，並駭侵各機關委外廠商、軟體開發或服務供應商，盜用廠商維管人員遠端管理權限，遂行網路滲透陰謀。[49]

46　孫以清，〈資訊戰與戰爭：資訊戰能否達到戰爭目的〉，收錄於《佛光大學政治與資訊研討會論文集》，頁4頁。

47　中央日報網路報，〈中共網路安全戰略發展趨勢〉，http://www.cdnews.com.tw/cdnews_site/docDetail.jsp?coluid=110&docid=103108775&page=2，檢索時間：104年3月12日。

48、49　於下頁。

2014年11月26日	調查局資通安全處副處長藍元鳴表示，我國已經成為殭屍病毒的中繼站，利用惡意及間諜程式，廣泛入侵全球政府機構及企業，造成美國經濟每年高達1,400億美元損失。[50]
2015年01月13日	行政院資通安全辦公室主任蕭秀琴小姐表示，我國已成為中共駭客試驗場域，依趨勢科技調查，我國高科技企業一年有346天遭駭客入侵，是全球平均數的1.5倍。[51]
2015年01月22日	行政院副院長張善政表示，中共持續以駭客針對我國經濟部、簽署ECFA、服貿協議、遠通電收實施入侵，[52]企圖蒐集相關情報資料。

資料來源：1.Yahoo奇摩新聞，朱明，〈國安局示警中國網軍攻擊重點轉向智慧手機〉，https://tw.news.yahoo.com/%E5%9C%8B%E5%AE%89%E5%B1%80%E7%A4%BA%E8%AD%A6-%E4%B8%AD%E5%9C%8B%E7%B6%B2%E8%BB%8D%E6%94%BB%E6%93%8A%E9%87%8D%E9%BB%9E%E8%BD%89%E5%90%91%E6%99%BA%E6%85%A7%E6%89%8B%E6%A9%9F-%E9%A2%A8%E5%82%B3%E5%AA%92-015900601.html，檢索時間：104年1月29日。
2.中時電子報，康文柔，〈愛用盜版臺灣成駭客溫床〉，http://money.chinatimes.com/news/news-content.aspx?id=20141126000690&cid=1206，檢索時間：104年1月29日。
3.自由時報，湯佳玲，〈中國18萬網軍威脅我將分級聯防〉，http://news.ltn.com.tw/news/politics/paper/847002，檢索時間：104年1月29日。
4.中時電子報，呂雪慧，〈防陸駭客網攻張善政：自己資安自己救〉，http://www.chinatimes.com/realtimenews/20150122004457-260412，檢索時間：104年1月29日。
5.作者自行整理。

(三)就軍事言

1.我國各項軍事科技及設施部分與民間科技共享或通用，如電力、自來水系統、作業軟(硬)體、中華電信軍租網路設備(施)等，[53]易遭敵方攻擊或破壞，國家整體秩序與運作能力必將遭到全面性癱瘓。

2.中共若對我國採取軍事威脅，可藉由網路駭客、電腦病毒入侵等手段，採縮小影響範圍、精準打擊方式，將原本的大量武力封鎖、癱瘓我政經軍心的作戰方式，轉變成精準打擊，進而癱瘓我國的指管通情，達到不戰而屈人之兵，且其入侵手

48 國防部史政編譯局編，《共軍「信息戰」研究專輯》(臺北)，國防部史政編譯局，西元1997年，頁254～256。

49 Yahoo奇摩新聞，朱明，〈國安局示警中國網軍攻擊重點轉向智慧手機〉，https://tw.news.yahoo.com/%E5%9C%8B%E5%AE%89%E5%B1%80%E7%A4%BA%E8%AD%A6-%E4%B8%AD%E5%9C%8B%E7%B6%B2%E8%BB%8D%E6%94%BB%E6%93%8A%E9%87%8D%E9%BB%9E%E8%BD%89%E5%90%91%E6%99%BA%E6%85%A7%E6%89%8B%E6%A9%9F-%E9%A2%A8%E5%82%B3%E5%AA%92-015900601.html，檢索時間：104年1月29日。

50 中時電子報，康文柔，〈愛用盜版臺灣成駭客溫床〉，http://money.chinatimes.com/news/news-content.aspx?id=20141126000690&cid=1206，檢索時間：104年1月29日。

51 自由時報，湯佳玲，〈中國18萬網軍威脅我將分級聯防〉，http://news.ltn.com.tw/news/politics/paper/847002，檢索時間：104年1月29日。

52 中時電子報，呂雪慧，〈防陸駭客網攻張善政：自己資安自己救〉，http://www.chinatimes.com/realtimenews/20150122004457-260412，檢索時間：104年1月29日。

53 曹邦全，〈中共信息戰之研究〉，國立中山大學研究所，碩士論文，2001年。

段，無法讓我方有預警和準備的機會，其威脅來源可來自軍事機構或某些非政府組織的駭客，對我方機要資訊網路實施入侵、攻擊、破壞等。如此情況複雜，真偽難辨，難以掌控攻擊效程，顛覆我對於傳統慣用戰(術)法的認知。

(四)就心理言

1.我國自大陸播遷來臺，經濟持續成長，國人已習慣安逸生活，新生代長期處於安定、富裕生活，普遍缺乏憂患意識，兩岸交流互動後，一般人都以為臺海無戰事，一旦中共以任何形式對我實施進犯，將使國人在心理上失去平衡，導致人心浮動不安，造成社會混亂。

2.我國社會的網路資訊科技發達，網際網路的應用，更涉及政、經、軍、科技、文化及日常生活等領域，若中共利用網路對我各項基礎設施任一環節實施入侵、癱瘓、破壞或攻擊，都會造成連鎖效應及損害；另網路運用的手段多元且日益翻新，從以往的替換政府機關網頁，到入侵電子金融市場，造成敵方股市混亂、金融失序，這都是網路戰應用發展的特點，如此除迫使我社會金融失序，更造成民心士氣分化，產生震撼與威懾效應，屈從於己方的意志，達不戰而屈人之兵，進而完成戰爭的政治目的。

綜合以上歸納得知，「網路」是繼物資、能源之後的一種新戰略資源，它不僅決定爾後世界的經濟、社會、政治、文化發展的關鍵因素，更是影響戰爭勝負的第一要素。[54]回顧20年來中共網際網路應用及發展建設，不論在產業發展或國際競爭力的提升，已創造成就非凡的奇蹟。孫子兵法：「故善用兵者，屈人之兵，而非戰也；拔人之城，而非攻也；毀人之國，而非久也」。我國各項建設如電信、水電、飛航、金融及政府服務等運作皆已高度資訊化及網路化，隨著政府、企業、軍事、社會及個人依賴資訊網路系統的程度日深，面對中共全力發展網路戰之威脅，資訊及安全維護上已成為國家安全最迫切課題。

中共網際網路發展戰略企圖

一、積極爭取第五空間，實踐世界霸權

「不戰而屈人之兵」係孫子兵法倡導戰爭最高境界，從「先勝而後求戰、避實擊虛及因敵制勝」的作戰原則，進而致力於追求「致人而不致於人」的戰略優勢，就是我中華民族所追崇的戰略思維。伴隨著科技發展與作戰思想改變，現代戰爭型態已漸由傳統的殲滅戰、消耗戰朝向癱瘓戰的模式發展。1992年起，中共提倡「互聯網」計畫，之後陸續成立「信息民兵」、「信息保障基地」等各類官方或軍方組織；2014年中共國家主席習近平指示須全力具體實踐「網路強國的戰略部署」，以成為網路世界霸權為目的。[55]

二、以國家戰略角度主導網際網路發展

2014年5月20日，美國司法部對中共61398部隊王東、孫凱亮、溫新宇、黃振宇及顧春暉(以上均為音譯)等5名共軍軍官提起告訴，主要的起訴原因係渠等以駭

54 林勤經，〈中共發展信息作戰軍事運用之探討〉，《中共對信息戰之研發與影響研討會論文集》，臺灣綜合研究院戰略研究所主辦，2000年2月19日。

55 自由時報，曹伯晏，〈學者示警：中國已成網路霸權〉，http://news.ltn.com.tw/news/politics/paper/794109，檢索時間：104年2月2日。

客行為，入侵美國核能、鋼鐵、太陽能及航太科技等重點企業；這也是美國政府首次對具有外國官方背景的人士，對於境外國家動用軍方和情報界的資源、工具，來對付美國企業以及業界人士、獲取行業機密或敏感的商業信息所提出的告訴」。[56]由此可見，渠等事件並非偶發，而是中共以國家戰略的角度主導軍事戰略，也就是授權解放軍網軍部隊有計畫執行網攻，主要目標仍鎖定英、美等先進國家之軍事科技研發、衛星通訊與能源為主；隨著資訊科技發展，中共仍積極致力建構網際網路，拉近與美國軍事武力上之差異。

三、嚴密思想控制，鞏固共黨政權

槍桿子和筆桿子是共產主義統治主要的利器，熟知操弄人性的中共就是充分利用意識形態，統治民族文化與傳統價值觀，尤其擅長使用溫水煮青蛙的效應，對百姓灌輸一套有利於共產黨操作的思維模式—「一黨文化」，然「媒體、網路、新聞、電影(視)、防止低俗及色情文化」的審查與掌控，為了穩固政權、端正社會視聽，不惜花費鉅資打造「長城防火牆」，以便偵控網路，封殺異己言論，阻止民眾瞭解自由世界的真實資訊，監控新聞、言論及異議分子就是中共網軍部隊主要任務之一。2014年香港佔中事件，中共利用駭客部隊攻擊壹傳媒，除導致該網站癱瘓外，並竊取合約、貸款紀錄及該集團主席黎智英個人向香港民主黨人士或機構捐款單據等，以利後續據以發動抹黑。另外中共網軍部隊可主動封鎖如「人權」、「法輪功」、「西藏」或「自由民主」等網站檢索，透過監控軟體，監視政治異議分子的批評活動，並追蹤他們的網路使用紀錄，而這些提倡政治改革者，大部分會因為透過網路發表其政治觀點，遭到中共當局以國家安全為理由，予以拘禁、逮捕或判以長期監禁，這意味著中共當局雖一面讚揚網際網路發展所帶來的經濟利益，卻又封鎖宣揚反對共產黨思想的異議網站，間接凸顯中共領導階層對網際網路發展的矛盾心態。

四、網路戰易使美中關係惡化

近年來，美、中之間的網路危機持續升級，2015年迄今，美國遭受來自中共的網路攻擊持續不斷發生，尤其中共官方支持網路入侵行為已成為外界關注焦點。[57]美國全球軍力雖然遠超越中共，若發生軍事衝突或危機，中共極有可能利用網路戰先發制人，以削弱美國軍事力量。2014年11月，亞太經合組織峰會(APEC)期間，美國總統歐巴馬要求中共立即停止由官方和軍方支持的網路間諜行為，禁止中共繼續以違反國際規範的行為獲取競爭優勢，如此可見，不論哪一方挑起網路戰，必將導致美中關係更加惡化。

因應作為與建議

一、落實保防及網路安全教育

當網路安全防禦達到一定程度後，駭客就比較難以完成攻擊，尤其是架設嚴密的防火牆，定期修補系統安全漏洞後，入侵者如果單純想從遠端利用系統漏洞占領

56 大紀元，燕青，〈美國對中共軍方駭客提出起訴的背後〉，http://www.epochtimes.com/b5/14/5/20/n4160098.htm，檢索時間：104年2月2日。

57 大紀元，何伊，〈蘭德公司：美中一旦開戰中方首攻網絡〉，http://www.epochtimes.com/b5/14/11/18/n4298388.htm，檢索時間：104年2月2日。

主機，幾乎是不可能的。這時駭客可以利用的方式，就是竊取使用者密碼。各單位人員如果保密警覺不夠，很容易就被入侵者利用取得重要資訊，藉以入侵攻擊。因此，如何有效教育國軍官兵安全妥善使用網路，才是刻不容緩的議題。

二、培育優秀資訊網路人才

為防範網路駭客大規模入侵，越來越多國家開始注重網路安全。美、法、日與俄羅斯等國家均與民間企業及大學資訊相關科系實施網路資訊交流合作，合作項目如網路管理、資訊安全、技術維修及駭客培訓等。我國不但是全球資訊產業重要代工基地，同時擁有眾多軟體研發人才，政府若能統籌各部會結合民間資訊產業人士，培訓優秀資訊網路人才，對於我國未來發展反制中共網路戰作為，將更有利。

三、防範網路威脅納入重點建軍項目

在資訊化及全球化時代，網際網路與日常生活之關係已密不可分，因應未來中共可能運用網路發動局部或全面性癱瘓戰，資安防護(範)應列為我建軍備戰之重點。然我資電部隊應著重危機處理及緊急應處，並研判敵可能遂行之網路戰攻擊方式，據以研擬各項因應作為，以確保我指管通資情監系統與神經中樞運作安全無虞。

四、研究網路攻擊方式

網路攻擊方式日新月異，可由國防部資電作戰指揮部專責成立研究小組，瞭解各種系統最新被公開的漏洞、新發現的病毒，並提供最新修補方案。不定期從事假想敵攻擊演練，嘗試突破國內各軍事或民間網路安全防禦系統，以監督各級網路未完備之處，如有發現弱點，立即要求改進。

五、以全民國防理念推動全民網路戰教育

為增進全民國防知識及全民防衛國家意識，廣泛運用全民國防教育日，針對政府、學校及公司民營等機關團體實施網路知識宣導，並透過全民國防教育法的推動，明析中共網路戰的手段及可能造成的影響，並藉以灌輸我主動防範及反制之道，期能降低網路戰對我造成之破壞與奇襲效應。

結　論

資訊安全是現今國防安全概念中重要一環，然網路科技領域，早已成為國家領土的一部分，是不容忽視與侵犯的。因此應特別加強網路安全層面防範。中共現今網際網路技術，足可對我方進行截聽、監視或操控，甚至可能藉由網路入侵危及我國國防安全，故我國應針對政治、經濟、金融、心理、基礎民生及軍事設施等，以全方位角度檢討因應對策，並在國防預算內增列相關研發經費，以深化網路理論基礎研究，強化各項防護作為。

科技是國家社會進步的動力，然軍事科技的發展則是成就軍事現代化最主要關鍵。我國應思考如何承勢轉化，基於「防衛固守、有效嚇阻」戰略指導及「預防戰爭」、「國土防衛」、「反恐制變」基本目標，本著「料敵從寬、備敵從嚴」的原則，因應戰略環境及防衛作戰需要，秉持「勿恃敵之不來，恃吾有以待之」心態、遵循軍事事務革新思維理念、前瞻尖端科技研發，藉「循序漸進」及「務實興革」之方法，結合國內產、官、學、研界技術能量，致力網際網路尖端及關鍵國防科技研發，以己之長發展適合我方之網路作戰策略，擘建立於不敗的戰略制高點，爭取資電優勢，令敵人投鼠忌器，不敢輕舉妄動，有鑑於此，吾人須認知網際網路對國家安全之影響，並發揮不對稱的優勢與潛力，開創以小搏大的轉機與契機！