中共2016《網絡安全法》對網路空間建構能力之影響

作者簡介

王清安中校，中正理工學院88年班、通資電正規班175期、陸院98年班、戰院暨戰研所107年班；曾任排長、連長、營長、通資組長，現任職於馬防部。

提　要

一、網路戰攻、防平衡點，在於敵、我通資系統內的應用程式密鑰攻、防對決。中共於2016年底頒布《中華人民共和國網絡安全法》，使公安部門及「國家廣播電影電視總局」(以下稱廣電總局)等相關部門，得以合法監控數據流動。此舉將有助於中共掌握數據安全的主動權。

二、中共《網安法》頒布後，其網路安全戰略將從「被動防禦」轉向為「主動防禦」，其所造成影響，將可強化國家境內網路安全防禦作為，提升網路空間整體戰力，並增加區域安全影響力。

三、總體而言，因應中共網路空間戰力的提升，本文建議我陸軍應提升網路空間聯合作戰反制能力、強化通資系統密鑰程式自主發展，及增編我陸軍網路部隊等，俾利我陸軍指管通資系統暢通。

關鍵詞：網絡安全法、網路空間、網路防禦、程式密鑰

前　言

自網路戰發展以來，運用電腦駭客或植入病毒，癱瘓敵國政、經中樞，與軍事指管系統，已成為奪取網路空間制高點的重要手段。然而，決定網路攻擊成功與否，關鍵在於攻、守雙方誰掌握數據安全的主動權，誰就擁有網路戰的主導權。2016年底，中共頒布《中華人民共和國網絡安全法》(簡稱網安法)，其第一條開宗明義表示：「為了保障網絡安全，維護網絡空間主權和國家安全、社會公共利益，保護公民、法人和其他組織的合法權益，促進經濟社會信息化健康發展，制定本法。」[1]其目的即為奪取網路空間的制高點。然而，回顧近年來中共遭西方媒體揭露，運用網路駭客竊取他國重要機密，其目的為提升軍事或經濟競爭力。根據2016年3月26日，美國司法部公告資料證實：1位名為蘇斌(Su Bin,或Stephen Subin)的中國籍網路駭客於加利福尼亞州中區地區法院承認，自2008年10月～2014年3月間，與另外兩名中國網路駭客，入侵加利福尼亞州奧蘭治縣的波音公司；其目標為獲取C-17戰略運輸機的數據軍事機密資訊。[2]不僅如此，2017年《美國國家安全戰略》(National Security Strategy of the United States of America)更明確指出：中共和俄羅斯控制網路數據的行為，支持發展國防武力，已損及到美國維護世界安全與繁榮的戰略目標。[3]雖然，中共官方始終否認他國網路行為的指控，但中共的網路科技已跳躍式的提升，卻是不爭的事實。因此，中共《網安法》頒布後，使數據呈現在地化管理，將有助於中共網路空間整體戰力的提升。

因應中共網路戰的威脅，我國雖然已於2017年成立「資通電軍指揮部」，以強化網路安全防禦作為。但由於我陸軍通資系統的數位化發展，其指管系統所面臨的威脅也隨之提升。鑒此，瞭解中共網路空間能力的虛、實，就更顯重要。惟國內研究中共網路戰不計其數，但真正探討其網路戰力卻是寥寥無幾。故本文將採「文

1　〈中華人民共和國網絡安全法〉《人大新聞網》，http：//www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm，2016年11月7日。

2　Department of Justice Office of Public Affairs," Chinese National Pleads Guilty To Conspiring To Hack Into U.S. Defense Contractors' Systems To Steal Sensitive Military Information", Department of Justice Office of Public Affairs, https：//www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive, March 23, 2016

3　The White House Washington, DC, National Security Strategy of the United States of America (Washington：The White House Washington, December ,2017), pp.2-3.

獻分析法」，透由簡析中共《網安法》緣起與發展。進而探討《網安法》對其網路戰力之影響。最後，據以評估對我陸軍資電防護威脅，並提出策進之道。

簡析中共《網絡安全法》之緣起與發展

因應網路攻擊威脅日益增加，《網安法》頒布後，將合法賦予中共各政府部門對個人及網路營運商實施管轄權。同時，透過監控數據，以強化網路安全防護。

一、緣起與目的

(一)緣起

沒有網路安全，就沒有國家安全。根據2014年2月27日中共總書記習近平首度主持《中共中央網路安全和信息化領導小組》表示：完善網際網路資訊內容管理，須立法制定規範，以保障資訊、通訊等關鍵基礎設施免受網路攻擊。同年，10月中國共產黨召開《第十八屆中央委員會第四次全體會議》。審議通過《中共中央關於全面推進依法治國若干重大問題的決定》；其決定內容為加強網際網路立法，及依法規範網路行為。[4]與此同時，中共因網路科技的落後，長期遭西方網路滲透、顛覆、竊密和監控活動，已對國家安全產生嚴重危害。[5]另外值得注意的是，根據2015年1月2日英國BBC報導：美國科技公司面臨在中共龐大的國營金融機構購買產品之前，須接受嚴格安全檢查的壓力，如思科及微軟；其主因為避免美國情報單位，利用網路產品的後門程式，竊取重要資訊。[6]由中共所面臨的網路安全威脅，已凸顯出無法掌握數據主動權，即無法確保網路安全。

(二)目的

法律的目的為實現公平正義，維護個人及公共安全。中共《網安法》，其目的為約束網路駭客行為，保障個人數據資料安全。根據2015年，中共《工業和信息化部電子科學技術情報研究所》所長洪京一表示：網路安全審查制度，其目的為維護國家網路安全、保障中國大陸境內用戶合法利益。同時，針對進入中國大陸市場的資訊產品實施審查，以防止資訊業者提供非法控制、干擾，及中斷用戶系統等不合法的行為。[7]此外，根據2016年中共

4 洪京一主編，世界網路安全發展報告(2015)－全球態勢與中國進展(香港：和平圖書有限公司，2015年12月)，頁139。

5 朱莉欣，〈「網路安全法(草案)」的解讀與建議〉，《中國資訊安全》，2015年8期，2015年8月，頁118。

6 Kevin Rawlinson," US tech firms ask China to postpone intrusive rules." BBC, 29 January 2015, http：//www.bbc.com/news/technology-31039227，2018年1月3日

7 同註4，頁138。

「國家資訊中心」處長呂欣表示：2015年7月6日，全國人大公布《中華人民共和國網絡安全法》，其目的為維護國家安全、促進經濟社會資訊化健康發展。同時，透過法律、組織、技術和教育等手段，以強化網路空間整體安全。[8]因此，網路空間的法治化，對中共維護國家利益、安全及主權，至關重要。

二、簡析《網絡安全法》[9]

《網安法》共計7章79條。明確規範國家監管機關權責、資訊用戶及網路營運商等義務與責任，與關鍵資訊基礎設施網路安全要求事項，簡析如後：

(一)國家監管機關權責

維護國家境內網路安全，須建構責任分明的政府部門。根據《網安法》指出：國家「網信部門」負責統籌網路安全、監督管理。國務院下轄之電信、公安部門，在各自職責範圍內監督、保護網路安全工作(第八條)。凡危害到國家境內網路安全之機構、組織或個人，公安部門和有關部門須依法採取制裁措施(第七十五條)。此外，國務院和省、自治區、直轄市人民政府，應支援企業、研究機構和大學參與國家網路安全技術創新專案，以提升網路技術產業研發、應用，並保護智慧財產權(第十六條)。不僅如此，各部門應經常性辦理網路安全宣傳教育(第十九條)。故在《網安法》頒布後，網路安全維護、監管、教育等責任已清楚劃分。同時，在國務院和省、自治區、直轄市等逐級，與企業、研究機構和大學等合作扶植網路科技研發，將建構更為安全的網路空間。

另外值得注意的是，中共網路空間安全核心主管部門，由「中華人民共和國國家互聯網信息辦公室」，統籌下轄的「工業和資訊化部(協調司)」、「公安部(網路安全保衛局)」負責。同時，指導「互聯網路信息中心(CNNIC)」、「國家互聯網應急中心」及「信息安全評測中心」等網路安全業務部門[10](如圖1)。

(二)資訊用戶

隨著網路攻擊日新月異，保護資訊用戶數據安全，已成為國家政府部門維護網路安全最重要的議題。根據《網安法》指出：具有收集使用者資訊功能的網路產品，網路營運商應向用戶說明，並取得同意(第廿二條)。營運商應遵循合法、正當、必要的原則收集使用個人資訊(第四十一條)。任何人、組織不得竊取或非法

8 呂欣，〈構建網路空間安全戰略體系的思考〉，《中國國際安全研究報告(2016)》(北京)，社會科學研究出版社，2016年7月，頁72～80。

9 同註1。

10 惠志彬，《全球網路空間信息安全戰略研究》(上海：上海世界圖書出版公司，2013年9月)，頁146、147。

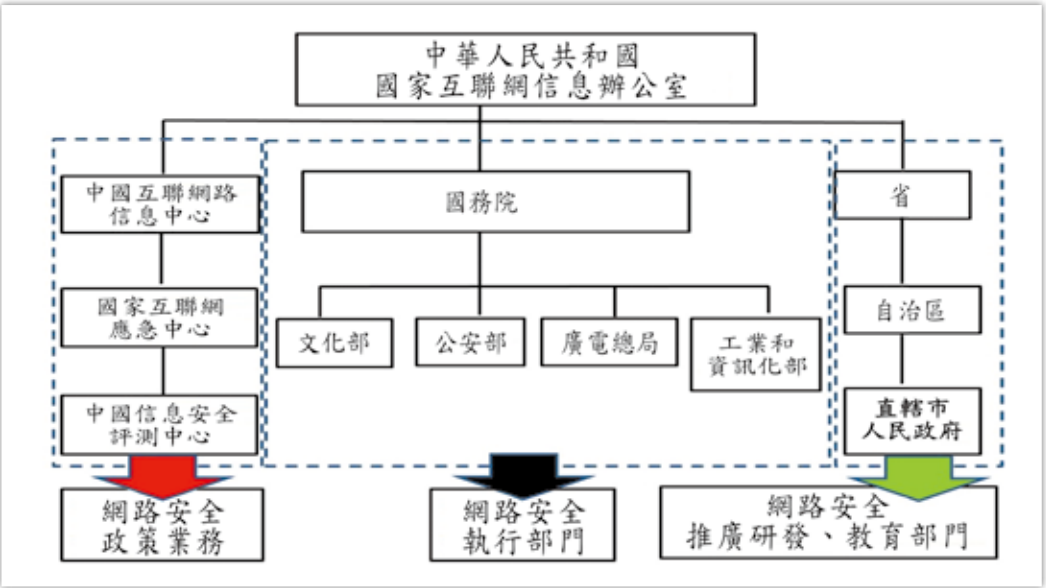

圖1　中共遂行網路空間安全管理組織圖

資料來源：惠志彬，《全球網路空間信息安全戰略研究》(上海：上海世界圖書出版公司，2013年9月)，頁146、147；中華人民共和國網絡安全法，中國人大網，2016年11月7日http：//www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm

知用戶，並向有關主管部門報告(廿二條)。此外，營運商發現用戶傳播危害網路安全資訊時，應即採取刪除等處置措施，防止不良資訊擴散(第四十條)。因此，在《網安法》頒行後，將使數據資料(含用戶在網路上的言論)在中國大陸境內受到監控與管理。同時還賦予營運商刪除責任。

使用個人資訊(第四十四條)。另外值得注意的是，用戶人電子帳戶，須結合自然人的姓名、出生日期、身份證件號碼、個人生物識別資訊、住址、電話號碼等(第七十六條)。故《網安法》頒布後，個人數據安全得到保護。換句話說，網路營運商將無法再任意收集和使用個人資訊。

(三)網路營運商

監控、掌握國家境內的數據流動，即能降低遭網路駭客攻擊風險。同時，亦嚇阻有心人士的非法網路攻擊。根據《網安法》指出：營運商須監測、記錄網路運行狀態，並按照規定留存相關的網路日誌不少於六個月(廿一條)。另外，提供網路產品的營運商，不得設置惡意程式；發現其漏洞程式，應採取補救措施，及時告

(四)關鍵資訊基礎設施網路安全

隨著國家工業用的關鍵基礎設施朝向數位化發展，誰能控制數據資料，誰就能掌握網路戰的主動權。根據《網安法》指出：對於公共通信和資訊服務、能源、交通、水利、金融、公共服務、電子政務等重要關鍵資訊基礎設施，實行重點保護(第三十一條)。另外，關鍵資訊基礎設施之網路產品和服務，應通過國家網信部門會同國務院有關部門組織的國家安全審查(第三十五條)。故在《網安法》頒行後，其關鍵資訊基礎設施所需的網路商品，再複式審查、稽核執行，將有助於網路安

全的管理。

總之，中共《網安法》頒行後，將使自由、開放的網路空間，在中國大陸境內呈現數據在地化的管理。該法規範的重點，首先，明確律定網路安全維護、監控責任。其次，確保資訊用戶數據資料的完整性。第三，規範網路營運商須主動採取網路防護作為。最後，律定關鍵資訊基礎設施之網路產品審查權責，以防杜後門程式遭他國網路監控、入侵。簡言之，中共《網安法》頒行後，網路空間防護責任，將從個人－政府，擴及到個人－企業－政府。同時，亦使中共網路空間成為一個內部的網路空間與世界網際網路隔離，其境內的網路行為均受到中共政府的監控(如表1)。

評估中共《網絡安全法》對建構網路空間能力之影響

中共《網安法》頒布後，其數據在地化有利於網路科技整體實力提升。同時，將挑戰現行的網路秩序。

一、特點

(一)強化網路安全防禦作為

無法監控、掌握數據資訊的流動，即無法確保網路安全；數據資料在地化的管理，將可提升網路空間防護能力。根據2017年，中國電腦學會計算安全專業委員會委員蔣天發表示：透由法律規範結合到網路空間安全議題，可強化網路空間資訊安全使用；其網路安全防護也從「被動防禦」轉向為「主動防禦」。[11]另外，根據2015年曾任澳大利亞移民和公民事務部門(Australian Government's Department of Immigration and Citizenship)在中國北京外交職務的Nicholas Dynon表示：中共《網安法》為提供國內司法行使的依據，管轄對象為數據中心、網路服務提供商、海底電纜和國際標準制定機構；其原則為只要在中國大陸境內使用的通、資產品，都須符合中共法律規範。[12]另外值得注意的是，根據2018年蘭德公司的報告揭露出：中國大陸網路空間的資訊操作系統，已成為一個內部局部網路空間與世界網際網路隔離；其能力預估以可防止網路空間邊界遭突破，包括防範病毒攻擊、反駭客攻擊，及網路緊急處理恢復。[13]因此，在中共《網安法》頒布後，政府部門可以依法監控，用戶數據資料流動，其網路安全防禦能力也隨之提升。簡言之，中共網路空間的

11 蔣天發、蘇永紅，《網路空間資訊安全》(北京：電子工業出版社，2017年2月)，頁8。

12 Nicholas Dynon," The Future of Cyber Conflict： Beijing Rewrites Internet Sovereignty Along Territorial Lines,"" China Brief. Volume： 15 Issue： 17, September 4, 2015〈https：//jamestown.org/program/the-future-of-cyber-conflict-beijing-rewrites-internet-sovereignty-along-territorial-lines/〉，2018年1月3日

13 於下頁。

表1　中共《網絡安全法》要求重點歸納表

區分 / 對象	條文	要求重點
國家監管機關	國家《網信部門》負責統籌網路安全、監督管理。國務院下轄電信、公安部門，負責網路安全保護和監督管理工作(第八條)。	合法賦予政府部門監控數據權利。同時，整合產、學、研等資源提升網路科技能量。
	公安部門和有關部門對機構、組織與個人，依法採取制裁措施(第七十五條)。	
	國務院和省、自治區、直轄市人民政府，支援企業、研究機構和大學，參與國家網路安全技術創新專案(第十六條)。	
	各部門辦理網路安全宣傳教育(第十九條)。	
資訊用戶	收集使用者的網路產品，網路營運商應向用戶說明，並取得同意(第廿二條)。	個人數據安全得到重視。
	營運商應遵循合法、正當、必要的原則，收集資訊用戶數據資料(第四十一條)。	
	任何人不得竊取個人資訊(第四十四條)。	
網路營運商	營運商須監測、記錄網路運行狀態，網路日誌不少於六個月(廿一條)。	將使數據資料(含用戶在網路上的言論)在中國大陸境內受到監控與管理。同時，賦予營運商刪除責任。
	網路產品的營運商，不得設置惡意程式；發現其漏洞程式，應採取補救措施，同時告知用戶、有關主管部門報告(廿二條)。	
	網路營運商發現用戶傳播危害網路安全資訊，應採取刪除措施(第四十條)。	
關鍵資訊基礎設施網路安全	公共通信和資訊服務、能源、交通、水利、金融、公共服務等重要關鍵資訊基礎設施，實行重點保護(第三十一條)。	透由複式審查方式，強化網路安全防禦作為。
	關鍵資訊基礎設施之網路產品，應通過國家網信部門，會同國務院有關部門組織的國家安全審查(第三十五條)。	

資料來源：作者自行整理

戰鬥警戒哨，已在無形的網路空間中被勾勒出來。

(二)提升網路空間整體戰力

沒有資訊技術發展，就沒有現代化發展。未來網路戰將是密鑰的攻防戰。根據2017年任職於美國海軍學院Dorothy Denning教授表示：中共為實現網路強國的戰略目標，利用網路駭客竊取其他國家網路公司的商業秘密，如谷歌(Google)的程式密鑰，或是美國武器系統重要機密資訊。同時，還利用網路長城的防火牆，使中國的網路用戶無法連接其外國網站，如西藏自治區已被其網路長城隔離於網際網路。[14]此外，根據2016年英國埃克塞特大

13　Jeffrey Engstrom, Systems Confrontation and System Destruction Warfare： How the Chinese People's Liberation Army Seeks to Wage Modern Warfare(California RAND Corporation, 2018).pp115-116.

14　於下頁。

學擔任法律講師的(Law School University of Exeter Exeter)Kubo Mačák表示：在沒有國際法可約束各國網路行為的前提下，資訊、通訊等科技一旦被國家納為所用後，可作為國家運用軍事行動的一部份。[15]另外值得注意的是，2017年美國蘋果電腦被迫繳出程式密碼後，同年7月宣布投資達到10億美元，在中國大陸貴州省貴安區，成立蘋果公司在海外第一個iCloud數據中心。[16]然而，中共為獲取蘋果電腦程式密鑰，早已不是秘密。根據2014年7月11日美國路透社報導：中共官方對外宣稱蘋果公司所研發的iPhone手機，能向美國情報機構提供用戶數據，迫使該公司繳出程式密鑰。[17]故中共《網安法》頒布後，外國網路科技廠商要進入中國大陸市場，須依法繳出程式密鑰，此舉有助於中共獲取數據安全的主動權。換言之，中共《網安法》頒布後，將可強化網路空間整體戰力。此舉也解釋2017年11月底，印度要求駐紮在印「中」部隊，其智慧型手機中安裝微信(WeChat)、微博(weibo)等應用軟體刪除；其原因為中共所研發之軟體，極可能已安裝間諜軟體或其他惡意程式。[18]

(三)增加區域安全影響力

《網安法》頒布後，賦予中共政府可依其國家利益，有權要求它國改變行為。根據2013年中共《國防科技大學》社會科學學院副教授劉楊鉞表示，《網安法》制定，對內可約束虛擬網路空間內的社會行為；對外可強化網路部隊捍衛網路空間利益與安全的話語權。[19]另外，根據2016年Frank Zhao and Jesse Heatley表示：中共《網安法》其主要目的之一

14 Dorothy Denning,"Cyberwar： How Chinese Hackers Became a Major Threat to The U.S.,", http：//www.newsweek.com/chinese-hackers-cyberwar-us-cybersecurity-threat-678378, oct.5,2017 .

15 Kubo Mačák ,"Is the International Law of Cyber Security in Crisis?," paper presented at the 2016 8th International Conference on Cyber Conflict (Tallinn： NATO CCD COE, 2016), p.131

16 dipayan ghosh,"Apple's Dangerous Market Grab in China," The New York Times' , https：//www.nytimes.com/2017/07/18/opinion/apple-china-regulation.html?_ga=2.202164376.86094706.1500900338-1159746865.1483843645，2018年1月3日

17 Jason Lee," Apple iPhone a danger to China national security： state media,"Reuters Staff, http：//www.bbc.com/news/technology-27712908，2018年1月3日

18 Manu Pubby," Indian troops on China border told to format smartphones, delete 42 apps," The Print, https：//theprint.in/2017/11/28/troops-told-to-format-smartphones-delete-42-apps-after-chinese-spyware-threat/，2018年1月3日

19 劉楊鉞、楊一心，〈網路空間再主權化與國際網路治理的未來〉《國際論壇》(北京)，第15卷第6期，外語教學與研究出版社，2013年11月，頁1。

，為阻礙外國網路公司在中國大陸境內的競爭力。[20]事實上，根據2012年Scott D. Applegate研究指出：中共用網路間諜，竊取美國公司機密，以幫助其國內企業跨越美國和其他外國競爭對手，最終目的成為世界最大經濟體。[21]此外，根據2016年Frederic Martel指出，中共有系統的補助其網路、電信產業和私營設備供應商發展；其目的為提升經濟發展與政治影響力，如2009年的Facebook、Twitter被禁止進入中國大陸市場為例，時間點比新浪微博推出的時間稍早一點。[22]隨著中共自主研發的網路設備，如路由器、交換機等產品技術突破，華為、阿里巴巴、騰訊等網路科技公司，已成功搶占國際市場占有率。[23]故《網安法》頒行後，將有助於提升中共國內網路科技全球競爭力，推動其數位經濟發展。同時，間接提升其國際話語權的影響力。

二、弱點

中共《網安法》頒布，已衝擊到現行網路空間秩序管理。一方面為衝擊個人隱私權，另一方面造成經貿非公平競爭。

(一)衝擊個人隱私權

自由、開放的網路空間，有利於政治民主化發展；反之，封閉的網路空間，極易造成政府專政，不利於內部政權穩定。根據2014年時任美國前國土安全部長Michael Chertoff(2005～2009)曾表示：中共與俄羅斯企圖宣告以國家行為者擁有網路主權，以保護國內網路關鍵基礎設施資訊安全，將不利於自由、民主的推展。[24]另外，2016年Elizabeth Goitein更指出，《網安法》對改善網路安全沒有什麼作用；相反，使政府藉由網路安全議題，擴大其行政權力。[25]另外值得注意的是，根據2018年1月《紐約時報》報導：中共「支付寶」因幫用戶預設隱私選項，已引起民眾盛怒，廣泛的網路詐騙和個人資

20 Frank Zhao and Jesse Heatley," China's Master Plan for IT Dominance," The Diplomat , https：//thediplomat.com/2016/08/chinas-master-plan-for-it-dominance/, August 11, 2016.

21 Scott D. Applegate, "The Principle of Maneuver in CyberOperations," paper presented at the2012 4th International Conference on Cyber Conflict (Tallinn： NATO CCD COE, 2012), pp.188-189.

22 Frederic Martel著，林幼嵐譯，《全球網路戰爭：全球化vs在地化》(SMART. Enquete sur les internets)(新臺市：稻田出版有限公司，2016 年)，頁60。

23 魏亮、魏薇等編著，2016年1月。《網路空間安全》北京：電子工業出版社，頁19。

24 Michael Chertoff," The Strategic Significance of the Internet Commons," Strategic Studies Quarterly, Summer 2014,pp.13-14.

25 Elizabeth Goitein, "Why Surveillance Won't Prevent Cyber Attacks," The American Prospect, July 10, 2015, 〈http：//prospect.org/article/why-surveillance-wont-prevent-cyber-attacks〉.

訊被盜現象，推動中共民眾隱私意識的崛起。[26]故《網安法》雖然賦予政府部門監控民眾的數據(含言論)自由，但已衝擊到個人隱私問題，此舉不利於內部政權穩定。

(二)不利經貿發展

開放、自由的市場有利於進行經貿往來；反之，限制數據跨境傳輸，將不利於經濟發展。根據2016年南華大學傳播系系主任張裕亮表示：中共實施網路封鎖，對其電子郵件和網路流量進行過度控制，將阻礙經濟需要的創新和生產力。[27]另外，《網安法》加強了對中共媒體和網路基礎設施的控制，其數據在地化的要求，將增加跨國公司網路安全管控成本。[28]此外，2017年美國《金融時報》報導：美國蘋果公司被迫從中國App Store中刪除應用程序，美國和歐洲應考慮中國網路公司不受限制地進入本國市場是否明智。[29]故中共《網安法》所形塑出的經貿保護主義，將限縮中共進入全球化市場，不利於經貿發展。

總體而言，中共《網安法》頒布後，對網路空間安全防護戰略，將從被動防禦轉向主動防禦。然而，回顧《網安法》頒布前，根據2013年香港大學新聞傳媒研究中心副教授傅景華(King-wa Fu)表示：中共已建立世界最大網路過濾系統；在封閉的網路空間中，敏感的用語將被過濾，且無法連線至Facebook，Twitter和YouTube等西方網站。同時，國內網路、資訊等公司必須審查內容，以屏蔽客戶資訊或禁用帳戶。另外，政府部門還設立創建和恢復系統(Rescue and Recovery, RnR)，以自動過濾不利政府言論的文章。[30]此外，根據2015年Angela Xiao Wu研究指出，中共為確保網路空間政治意識形態安全，2001年所設立中國金盾(現稱為網路長城,GFW)，其管轄對象為公民，新聞記者和非政府組織，使中共網路空間隔絕於全

26 Paul Mozur, "Internet Users in China Expect to Be Tracked. Now, They Want Privacy,"The New York Times,https：//www.nytimes.com/2018/01/04/business/china-alibaba-privacy.html?_ga=2.135812849.1113268427.1515288746-250413717.1505435301, Jan. 4, 2018 .

27 張裕亮，〈第二屆世界互聯網大會評析〉，《展望與探索》，第14卷第1期，2016年1月，頁22、23。

28 Jun Wei ,Roy Zou ,Liang Xu, China passes controversial Cyber Security Law Hogan lovells, https：//www.hoganlovells.com/～/media/hogan-lovells/pdf/publication/2016/beilib0185898v120161110chinapassescontroversialcybersecuritylaw.pdf, November 2016,pp.3 .

29 "The dangers in Beijing's bid for cyber sovereignty," Financial Times, https：//www.ft.com/content/52d5880c-7607-11e7-a3e8-60495fe6ca71，2018年1月3日

30 King-wa Fu," Assessing Censorship on Microblogs in China： Discriminatory Keyword Analysis and the Real-Name Registration Policy," IEEE Internet Computing, Vol. 17, No. 3, 11 February 2013, p.43.

球網際網路，成為一個內部網路。[31]因此，中共《網安法》頒布後，已形塑出以中國大陸境內的內部網路，對其網路空間建構能力之影響；首先，賦予政府部門更多監管權責，管轄對象從個人用戶資料，擴及到中國境內國內、外資訊、通信營運商的責任，且網站、App、博客和社群媒體等申請帳號，採實名制，且須獲政府許可才能上網發布，將可強化其國家境內的網路安全防禦作為。其次，以網路安全為由，迫使外國網路科技廠商，須繳出程式密鑰，供政府部門監管，提升網路空間整體戰力。最後，有助於提升中共國內網路科技全球競爭力，推動其數位經濟發展，增加對區域安全的影響力(如表2)。

對我陸軍資電防護能力威脅評估及建議具體作為

隨著中共網路空間整體戰力提升，對我陸軍數位化指管通資系統，將產生更大的風險。為此，評估我陸軍資電防護能力，據以提供策進之道。

一、對我陸軍資電防護能力之威脅評估

(一)通資系統數據鏈路易遭敵破壞

網路戰的攻防戰，即為敵、我雙方密鑰技術的對抗。隨著網狀化作戰發展，各載台、用戶資料鏈結所形成的資料庫，已成為影響作戰成敗的關鍵。根據我國(民106)《國防報告書》指出：中共對臺軍事能力，已具有電磁參數監偵，與指管系統偵蒐、阻斷與干擾等電子軟、硬殺能力。[32]事實上，通資系統的脆弱性，已是維護網路安全的重要議題。根據2017年10月5日美國陸軍網路主任(Cyber Director at Army G-3/5/7 Office)弗羅斯特少將(Maj. Gen. Patricia Frost)表示：2018年網路安全重點工作之一，就是評估武器平台與通資系統安全性和彈性。[33]因此，在中共積極掌握網路科技程式密鑰的同時，已對我陸軍資電防護能力造成極大之威脅；其原因為我陸軍通資裝備，無論是我國自製研發，或是採購美國系統，其共同因素為未定期提升作業系統。故在中共積極發展人工智慧，打造大數據的時代，若將數據資訊提供其自行研發的無人機，對我陸軍重要通資節點攻擊，後果將不堪設想。

(二)輿情資料易遭敵掌握

31 Angela Xiao Wu.," Historicizing Internet Use in China and the Problem of the User Figure," IEEE Annals of the History of Computing, Vol. 37, No. 4, Oct.-Dec 2015, pp.2-3.

32 國防部《中華民國106年國防報告書》(臺北：中華民國106年國防報告書編纂委員會，民國106年12月)，頁44。

33 Kathleen Curthoys," Two-star： Every soldier must be a cyber defender," army times, https：//www.armytimes.com/news/your-army/2017/10/22/two-star-every-soldier-must-be-a-cyber-defender/，2018年1月3日。

表2　中共實施網安法後網路空間管理前、後對照

區分 / 類別		2016年網安法頒布前	2016年網安法頒布後
管轄對象		運用行政規章，約束用戶、國內網路科技營運商、媒體(新聞記者)和非政府組織。	立法要求用戶、國內、外網路科技營運商(只管公司不管地域)、媒體(新聞記者)和非政府組織。新增實名制，要求申請帳戶須先審後用，杜絕錯誤資訊傳播。
手段		編組網路警察(公安系統)，透由網路輿情師、五毛黨實施網路文字審查。同時，以國家安全為由逼迫外國廠商繳出程式密鑰，未配合廠商，阻封進入中國市場，如2011年，Google、facebook。	直接立法，要求在中國大陸資訊、通訊科技廠商繳出密鑰，未依法要求實施罰款。 同時，賦予公安部、文化部、廣電總局實施管轄的權利。
影響	強化網路安全防禦作為		法律賦予各部門管轄權，使中共網路空間成為以中國大陸境內為核心的內部網路，確保用戶數據安全。
	提升網路空間整體戰力		獲得程式密鑰後，有利於政府部門掌握跨境網路數據的偵蒐與攻擊來源，有利於提升網路空間攻、防及偵察整體戰力。
	增加區域安全影響力		保護用戶數據安全為由，要求進入中共境內網路科技廠商，須增設數據中心(增加外資成本)。間接，提升國內網路產業競爭力，與區域安全影響力。

資料來源：作者自行整理

由於我國資安環境無法比照中共《網安法》，要求網路營運商提供網路安全防護。與此同時，隨著我陸軍營區開放智慧型手機，在資安防護能力不足，將影響我陸軍戰力發揮；其主要理由為，一旦敵人掌握程式密鑰，於平時透由監控電子郵件，即可掌握我陸軍重要人物情資。戰時，透過散布假訊息，將影響關鍵決策。根據2017年中共《國防科技信息中心》所出版的一篇研究指出：網路空間提供獲取戰爭主動權的絕佳戰場。和平時期，運用網路滲透潛伏他國資訊系統，以偵察獲取情報；戰時，實施全面攻防，其作戰目標為軍方人員與指管通資系統。[34]另外值得注意的是，2018年我陸軍○部黃姓連長，因未按資安規定安裝手機管制軟體，並翻攝一般公務文件，上傳通訊軟體群組。[35]雖未造成洩密情事，但已凸顯出資安防護不足的問題。故在無資安法規範網路營運商提供網路安全前提下，及部分幹部資安

34　陳森，〈廓清網路安全殘缺認知，務實推進網路國防建設〉，《現代軍事》，480期2017年1月，中國國防科技信息中心，頁48、49。

35　〈6軍團：依規定嚴懲強化資安教育〉，《青年日報》，2018年3月4日，版3。

防護觀念不足，將影響我陸軍整體戰力發揮。

二、策進之道

(一)提升網路空間聯合作戰反制能力

奠定聯合作戰成功基礎，在於統合戰力的發揮。取得資電作戰優勢，對於未來遂行臺、澎防作戰極為重要。基此，2018年我陸軍除持續運用部署於各作戰區(防衛部)的資通電軍，配合漢光、聯勇等時機，與我陸軍聯兵旅通資部隊共同演訓外。同時，應選擇適當時機，由資通電軍擔任假想敵，對作戰區某旅實施資電攻防演練。此外，借鏡參考《美陸軍2018年所提出的網路戰精進作法》：美陸軍計畫擴大網路培訓計畫，引入新的網路訓練環境，以強化網路部隊訓練。透由新的虛擬環境，強化網路空間聯合作戰能力，以填補現在可用的網絡訓練平台的空白。同時，還預劃於2018年二月份在亞利桑那州的華楚卡堡(Fort Huachuca, Arizona)，進行陸軍及陸戰隊聯合網路演習，使陸軍參演官兵，透由演習中與海軍陸戰隊互動，進一步瞭解戰術環境中所需的資訊分享、電子戰威脅等。[36]因此，勇於創新、不斷革新，才是提升資電防護最好方式。以往傳統按想定計畫實施資電作戰攻防，如聯電操演，將不再符合未來作戰場景需求。唯有強化實戰演練，增加跨軍種網路對抗演習，才能提高我陸軍資電防護能力。

(二)強化通資系統密鑰程式自主發展

隨著網路戰爭型態的轉變，平時運用網路偵察掌握敵國重要人物資訊，如電子郵件。戰時，透由大數據分析以策劃發動網路宣傳戰，已成為中共解放軍攻臺戰役重要手段。在中共《網安法》迫使美國網路科技營運商，繳出程式密鑰後，已威脅到美國網路科技優勢。根據2017年《美國國防戰略》指出：在情報需求方面，應防止敏感資訊遭竊取。同時，提高檢測和打擊敵網路間諜活動能力，確保美國在使用前不會受到損害。[37]雖然，我國(民106年)《國防報告書》指出：國防資源及科技能力應集中在關鍵戰力；其建軍方向之一為籌建資通電反制裝備，形塑戰場資電優勢。[38]然而，在忽略程式密鑰為網路攻、防重要守門員下，我陸軍應建立一套通資系統定時更新週期，

36 Kathleen Curthoys,"New in 2018： Army cyber expands training, gains EW soldiers," Army Times，https：//www.armytimes.com/news/your-army/2017/12/29/new-in-2018-army-cyber-expands-training-gains-ew-soldiers/，Dec.29,2017.

37 The White House Washington, DC, National Security Strategy of the United States of America (Washington：The White House Washington, December ,2017), p. 32.

38 同註32，頁74。

透由定期檢測、更新，以提升我陸軍網路安全整體防護能力。同時，我陸軍應建議國防部，整合國安局、中科院研發我陸軍所需的通資訊系統。但不可諱言，中科院所研發的Juiker系統為例，推行迄今，使用率不高；究其原因方便性無法與Line相比，這點值得我陸軍發展自主化重視的議題。

(三)增編我陸軍網路部隊

不戰而屈人之兵，是用兵最高指導。根據網路戰發展趨勢，未來臺海戰役中，中共解放軍極可能運用網路戰，以影響社會民眾反戰爭行動，進而瓦解全民國防戰力。同時，運用網路攻擊，癱瘓我國指管通資系統，將我國隔離於網際網路外，使我國喪失國際說話權。由於網路謠言散布屬司法案件，須協調警政署的電信總監處理。在我國不像俄羅斯、中共設有網路警察、電腦系統可全時監控不實言論，且系統可自行審查、依法懲治下，建議我陸軍應成立適切的網路部隊，以強化網路空間監控能力。另外，建議國防部與國安局、警政署完成支援協定，以建構聯合網路空間防護體系。

結　　語

由於網路空間是個虛擬、自由的網路空間，中共《網安法》實行，意味著在網路空間中將形塑出網路國防長城。透過隔離數據資料的流動，將使中共國家境內成為有別世界網際網路的內部網路。事實上，要強化網路空間安全防護，須從網路科技、網路空間管理規範及網路安全教育著手。在2016年底中共《網安法》公布後，其網路空間整體戰力得到相當大的提升。令人驚訝的是，數據在地化的管理，使中共網路空間管轄的對象，從個人－政府擴及到個人－企業－政府；其值得注意的是，網路安全作業系統漏洞程式，網路營運商須主動修復且主動報告用戶及政府部門。不可諱言，自由網路空間的邊界，須在國際體系中得到國與國的認可下建構，單方面由中共透由國內立法《網安法》頒布，限制數據自由流動，勢必挑戰到現行網路空間秩序。同時，對區域安全穩定造成影響。總而言之，中共網路空間整體戰力，在其政府部門主導《網安法》頒布後，已得到相當程度的提升。為此，我陸軍須加強聯合網路空間演訓、建構國防自主所需密鑰及增編網路部隊，俾利肆應未來網路戰之挑戰。