國防大學政治作戰學院中共軍事事務研究所

碩士論文

中國大陸網路空間戰略發展：影響國際網路規則為例

The Research on the Development of PRC's Cyberspace Strategy: The Influence to International Cyberspace Institution.

研究生：毛允辰 撰

指導教授：陳育正 博士

中華民國一〇九年六月

國防大學政治作戰學院中共軍事事務研究所碩士學位論文

口試委員會審定書

中國大陸網路空間戰略發展：影響國際網路規則為例

The Research on the Development of PRC's Cyberspace Strategy: A Case Study: The Influence to International Cyberspace Institution

本論文係毛允辰（學號 1090720214）在國防大學政治作戰學院中共軍事事務研究所完成之碩士學位論文，於民國 109 年 6 月 4 日承下列考試委員審查通過及口試及格，特此證明

委員兼召集人 彭育仁

指導教授 馮育正

委員 林穎昌

所長 馬振坤

中華民國 109 年 6 月 4 日

國防大學
National Defense University

謝辭

論文終於寫完了，首先要感謝陳育正老師花費青春克盡心力的用心指導，不僅不棄學生不才，且在寫作過程中細心指引，透過多方面的討論引領我思考，並教會我許多寫作的敘述鋪陳的技巧及上下文邏輯連貫的組織方式，每篇都要圍繞著主軸，不要偏離題目跟研究途徑，在寫作的道路上就算跌跌撞撞，最後也還是能再度站起來繼續向前走。師恩浩蕩，感謝老師對學生的諄諄教誨，這樣的思考模式和寫作方式將使我一生受益無窮。

其次，感謝中軍所馬振坤所長、劉翰宇、王珍一、王惠民、丁樹範、李亞明、董慧明老師等傳道、授業、解惑，引領我進入博學的學術領域，並在兩年碩士生涯期間迅速累積相關學識，使我獲益良多。也感謝 109 年班的學長姐們，同窗兩年的學習過程中，一路上有家銘、復建和文傑學長們的協助與支持，使我在學習的道路上不孤單。同時也感謝中軍所最認真的明逸助教，在學期上許多的協助。

最後，感謝在我身後默默支持我的家人媽媽、妹妹、弟弟、先生和即將在六月底出世的女兒小安安，謝謝你們在我心情最低落的時候，成為我的溫暖的避風港；在我感到徬徨的時候，擔任我的後盾，為我出謀劃策，使我能夠在課業上無後顧之憂的全力以赴。

毛允辰　謹識

北投復興崗

2020 年 6 月 1 日

國防大學
National Defense University

摘要

本研究以攻勢現實主義作為研究途徑，探討中國大陸在面臨網路安全威脅的情況下，為追求權力及安全極大化的目標，持續建制網路空間戰略。首先，中共於 2014 年成立「中央網絡安全和資訊化領導小組」，突顯出中國大陸把網路安全上升為國家戰略，而發揮集中指揮和統一領導的作用。其次，建構國家網路空間安全的法律制度，在 2015 年和 2016 年前後通過《國家安全法》 和《網絡安全法》突顯出透過立法手段加強對境內網路空間絕對控制。最後，提出捍衛網路空間的戰略架構於先後發布《國家網絡空安全戰略》和《網絡空間國際合作戰略》。彰顯中國大陸對網路主權的維護是不容他國介入與干擾，並在國家主權的基礎上參與多邊建構網際網路全球治理的平臺。

中國大陸積極參與國際事務的意向從內部主導的「世界互聯網大會」和「數位絲綢之路」宣揚網路主權的概念，並與「一帶一路」沿線開發中國家建設網路基礎設施，藉此深化與區域間國家的互賴關係，並擴大中國大陸在區域的影響力。至於國際事務，參與聯合國組織及其網路治理平台、北大西洋公約組織、東南亞國協和上海合作組織等區域性國際組織，期望藉由商業利益與積極拉攏開發中國家，並逐步擴大在全球網路治理體系中

的影響力，甚至改變由美國等西方國家主導的全球網路治理體系，確立中國大陸在網路領域中能與美國抗衡的強權地位。

關鍵字：網絡空間國際戰略、中央網絡安全和資訊化領導小組、國家安全法、網絡安全法、世界互聯網大會、數位絲綢之路

Abstract

The concealment and transnational nature of cyberspace have caused various conflicts in cyberspace. As far as the internal situation in mainland China is concerned, acts of using cybercrime often occur. As far as the international situation is concerned, in July 2010, the Iranian nuclear power plant centrifuge was attacked by the Stuxnet virus attack and the 2013 U.S. PRISM program, which affected the national security and development of mainland China.

This research uses offensive realism as a research approach to explore the CCP’s strategy of continuously building cyberspace in pursuit of the goal of maximizing security in the face of cybersecurity threats. First, the Chinese Communist Party(CCP) established the “Central Cyber Security and Informatization Leading Group” in 2014, highlighting China's promotion of cyber security as a national strategy and its role of centralized command and unified leadership. Second, the establishment of a national cyberspace security legal system. The adoption of the National Security Law in 2015 and the Cybersecurity Law in November 2016 highlight the strengthening of absolute control over domestic cyberspace through legislative means. Finally, it is proposed that the strategic framework for defending cyberspace be published on December 27, 2016, "National Cyberspace Security Strategy" and March 1, 2017, "Cyberspace International Cooperation Strategy." To demonstrate that the maintenance of cyber sovereignty in mainland China is tolerant of interference and interference by other countries, and to participate in the multilateral construction of a global Internet governance platform on the basis of national sovereignty.

Mainland China's intention to actively participate in international affairs promotes the concept of cyber sovereignty from the "World Internet Conference" and "Digital Silk Road" led internally, and builds a network foundation with developing countries along the "Belt and Road" facilities to deepen the relationship of interdependence with countries in the region and expand the influence of mainland China in the region. As for international affairs, participating in the United Nations, affiliated organizations, and international organizations expects to gain substantial benefits from technology and technology and attract developing countries, and gradually expand its influence in the global network governance system. The state-led global network governance system has established China's powerful position in the network field to compete with the United States.

Keywords: Central Cyber Security and Informatization Leading Group, National Security Law, Cybersecurity Law, World Internet Conference, Digital Silk Road

論文目錄

圖目錄

表目錄

第一章 緒論

第一節 研究動機與目的

壹、研究動機

全球網際網路誕生於美國 1960 年代，是美國國防高等研究計劃署網路（Advanced Research Projects Agency Network, ARPAN）開發的世界上第一個運營的封包交換（packet switching）網路，是全球網際網路（Internet）的始祖。[1]它以深刻的影響著世界經濟、政治、文化和社會發展，促進社會經濟的繁榮與資訊傳播的變革。

中國大陸於 1994 年 4 月 20 日在北京中關村地區教育與科技研究示範網接入全球網際網路的專線開通後，正式接入全球網際網路。中國大陸把發展網際網路作為推進改革開放和現代化建設的重大機會，先後制定一系列的政策規劃，明確訂出階段性發展的重點。[2]中國大陸於 1993 年成立國家經濟資訊化聯席會議，負責領導國家公用經濟資訊通信網建設。並且在 2005 年 11 月，制定《國家資訊化發展戰略（2006-2020 年）》，進一步明確網際網路發展的重點，提出調整經濟結構和經濟轉型方式，推進經濟資訊化、推行電子政務、推展社會資訊化等。[3]

網際網路等基礎設施的建設和完善，促進網際網路的普及和應用，截至 2018 年 12 月底，由中國大陸互聯網路資訊中心發佈的第 43 次《中國互聯網路發展狀況統計報告》顯示中國大陸上網人數規模達 8.29 億，手機使用網路人數規模達 8.17 億，已成為使用網際網路人數的世界大國。[4]而經濟

[1] 網路在中國大陸稱為網絡，網際網路在大陸稱為互聯網。為了行文和閱讀的方便，除非文章必要維持之外，均以台灣用語網路一詞表示。沈逸，〈全球網絡空間治理需要國際視野〉，《中國資訊安全》，2013 年 10 月，頁 36。

[2] 國務院新聞辦公室，〈中國互聯網狀況〉，《政府之聲》，頁 1。

[3] 資訊一詞在中國大陸稱為信息，為了行文和閱讀的方便，文章均以資訊一詞表示。

[4] 中國互聯網路資訊中心，〈2019 年中國互聯網路發展狀況統計報告〉，《中國網信網》，2019 年 8 月。

方面，網際網路對中國大陸經濟成長也做出重要貢獻，網路與實體店面的結合，使得中國大陸的工業設計、生產設備資訊化、經營管理網路化，帶動產業結構的調整和產業製造的能力提升。

隨著經濟社會的不斷發展與進步，網路已成為當今社會發展不可或缺的重要組成部分，由於網路空間的特殊性和跨國性，使得網路空間衍生出各種衝突。就中國大陸內部情勢而言，借助網路犯罪的行為時常發生，個人隱私洩漏和侵犯、網路詐騙、網路暴力和利用網路進行散播不實消息，破壞社會秩序等犯罪行為層出不窮。就國際情勢而言，2010 年 7 月伊朗核電廠離心機遭受到震網病毒(Stuxnet)攻擊和 2013 年美國稜鏡事件(PRISM)，這些事件影響著中國大陸的國家安全與發展。

有鑑於此，中國大陸建構網路空間戰略，必須圍繞在政治、法律制度和戰略等各層面。首先，中共於 2014 年成立「中央網絡安全和信息化領導小組」，突顯出中國大陸把網路安全上升為國家戰略，而要發揮集中指揮和統一領導的作用。

其次，建構國家網路空間安全的法律制度，在 2015 年通過《國家安全法》[5]和 2016 年 11 月通過《網絡安全法》突顯出確保對境內網路空間絕對控制外，擔心美國的網路技術能突破其封鎖，輸入西方意識形態，危害其對網路空間言論的絕對掌握，透過立法手段，藉由法律來加強對中國大陸內部的網路言論的控制，避免造成國家安全危害之局面。[6]

〈http://www.cac.gov.cn/2019-02/28/c_1124175677.htm〉。(檢索日期 2019 年 10 月 1 日)。

[5] 《中華人民共和國國家安全法》係 2015 年 7 月 1 日為第 12 屆全國人民代表大會常務委員會第 15 次會議通過，該法共分為七章、84 條。全文請見〈中華人民共和國國家安全法〉，《人大新聞網》，2015 年 7 月 10 日，〈http://npc.people.com.cn/BIG5/n/2015/0710/c14576-27285049.html〉。(檢索日期 2019 年 11 月 1 日)。

[6] 〈中華人民共和國網絡安全法〉，《新華網》，2016 年 11 月 7 日。〈http://www.xinhuanet.com/politics/2016-11/07/c_1119867015.htm〉。(檢索日期 2019 年 11 月 1 日)。

最後，提出捍衛網路空間的戰略架構。2016 年 12 月 27 日發布《國家網絡空安全戰略》和 2017 年 3 月 1 日發布《網絡空間國際合作戰略》。彰顯中國大陸對網路主權與維護是不容他國介入與干擾，藉以強調各國應在相互尊重自主的網路管理模式、選擇網路發展道路，並在國家主權的基礎上建構國際合作平臺，共同建構多邊、透明的全球網際網路治理體系，實現資源分享、責任共擔、合作共治。[7]

自網路空間治理問題成為一項全球治理的新議題以來，中國大陸展現出積極參與國際事務的意向，從內部主導的世界互聯網大會和「數字絲綢之路」（Digital Silk Road）[8]在世界互聯網大會宣揚網路主權（internet sovereignty）的概念，並與沿線開發中國家的建設網路基礎設施，藉此深化與區域間國家的互賴關係，並擴大中國大陸在區域的影響力。至於國際事務，參與聯合國大會和國際電信聯盟（International Telecommunication Union，以下簡稱 ITU）。運用聯合國架構下的網路治理平台，期望藉由獲得科技與技術上的實質收益，並逐步擴大在全球網路治理體系中的影響力，甚至在重塑由美國等西方國家主導的全球網路治理體系，確立中國大陸在網路領域中能與美國抗衡的強權地位。[9]

近年，中國大陸積極參與全球網路治理事務，試圖將政治理念導入國際建制的規範中，突顯中國大陸積極參與網路空間規則制定是何其重要，然而現有研究大多聚焦於網路空間議題探討，或網路安全等議題，但對於中國大陸積極參與網路空間的國際事務等面向之研究，尚有不足。這樣的

[7] 中央網絡安全和資訊化領導小組，〈《網絡空間國際合作戰略》(全文)〉，《新華網》，2017 年 3 月 1 日。〈http://www.xinhuanet.com/politics/2017-03/01/c_1120552767.htm〉。(檢索日期 2019 年 11 月 11 日)。

[8] 數位絲綢之路在大陸稱為數字絲綢之路，為了行文和閱讀的方便，除非文章必要維持之外，均以數位絲綢之路一詞表示。。

[9] 左志，〈國際電信聯盟與中國崛起-以中國電信政策研究為視角〉，《新聞大學學報》，第 3 期，2016 年，頁 16-17。

問題意識建構出本文的研究動機，筆者希冀能夠透過客觀及系統化的角度，分析中國大陸網路空間戰略發展特點，在聯合國及區域性國際組織探討網路空間國際規則制定等相關行動，期許能對我國學界與政府提供建議與參考。補述，本文在接下來有關中國大陸用之「網絡」、「互聯網」、「數字」、「信息」等用語，統一以「網路」、「網際網路」、「數位」、「資訊」稱之。

貳、研究目的

網路空間現已成為陸地、海洋、空中和太空之外的第五空間，是國家主權延伸的新疆域，網路空間的規則制定，所帶來的衝擊，考驗著美、中、俄等國的立場，網路空間規則的制定仍是進行式，未來勢必成為新戰場。[10]

研究網路空間規則制定，所衍生的爭端可以從政治、外交、軍事、經濟等不同面向予以探討，但由於中國大陸的崛起，以攻勢現實主義來探討中國大陸網路空間戰略等研究略顯不足，筆者將嘗試以中國大陸網路空間戰略的發展模式做為分析對象。有關網路強國已有許多研究，對於中國網路戰略發展模式在國際關係理論上的意義，和中國大陸國家行為之間的關係，以及未來可能走向，則缺乏有系統的分析。因此，筆者從中國大陸政府對外的官方資料及新聞來研究，從中國大陸積極參與國際事務的立場來推斷中國大陸網路空間戰略發展，藉以提升中國大陸在國際上的影響力，與爭奪網路空間的話語權，是否符合攻勢現實主義的基本假設，而此措施有以下項目可供探究：

(一)探討中國大陸網路空間戰略的發展特點。

(二)檢視中國大陸如何影響國際網路空間規則制定。

[10] 方興東、胡懷亮，《網絡強國：中美網絡空間大博弈》，（北京：電子工業出版社，2014 年），頁 7。

第二節 文獻探討

文獻回顧的目的討論整個領域，所累積的學術與知識的研究成果，因此必須站在前人的肩膀上，才能夠看得更高更遠，避免重複與前人已做過相同的研究。文獻回顧絕非是心得閱讀報告，是要經過自己的消化整理的過程，所做具有邏輯的論述，需具有綜合、分析、批判的能力，並指出目前文獻的優缺點及不足處，並藉由不足之處，來發展出自身研究者的理論方向與命題。

文獻探討主要在確認自身的研究重心，蒐集國內、外各類書籍文獻中與本論文相互呼應的陳述，以不同角度顯現論文所表達的內涵及架構，在此基礎上汲取前人研究成果及經驗作為參考運用，依據歸類、摘要、批判及建議等四個步驟，[11]說明文獻與研究問題之關聯，進行系統化的分析，協助研究者觀念整理與分類，型塑有力的論證基礎，確保研究架構與思維邏輯有緊密結合。本研究透過文獻探討，整理中國大陸網路空間戰略等相關研究，在現有學術領域成果中梳理問題意識，提供未來研究方向與建議。

文獻探討區分為「中美雙方於網路空間之競爭」、「中國大陸網路空間戰略之探討」、「國際網路規則制定之影響」等三部分，於本文檢視相關之研究。筆者試圖歸納出重點與不足處，作為本文之參考，以下綜整及歸納各領域中指標及代表性文獻。

壹、美國與中國大陸在網路空間之競爭

近年來，中國大陸與美國在多個領域圍繞著網路安全問題展開競爭，2010 年至 2015 年是中國大陸與美國網路安全競爭張力大幅上升的五年，筆

[11] 孫本初，〈如何寫好一篇優質碩博士論文〉，曾於臺北大學「撰寫碩博士論文與投稿學術期刊」論壇發表，2005 年，頁 94。

者通過回顧這五年中國大陸與美國網路安全競爭的內在的原因，來源區分為三部分：

一、中美雙方意識形態領域分歧

美國政府對全球網際網路自由的問題非常重視，美國前國務卿希拉蕊（Hillary Clinton）分別於2010年1月和2011年2月發表「網路自由」（Internet Freedom）的演說，[12]運用網際網路等資訊技術，在全球推廣「網路自由」是作為美國二十一世紀的外交政策的首要任務。希拉蕊批評中國大陸對網際網路的審查，限制自由獲取資訊或侵犯網際網路用戶基本權利的國家，面臨著使自己與下一個世紀的進步隔絕的風險。前總統歐巴馬（Barack Obama），於 2011 年 5 月，公佈新的《網路空間國際戰略》（International Strategy for Cyberspace）指出：「網路自由如同言論和結社自由是美國核心理念」。[13]批評中國大陸和伊朗等政府管控網際網路等事件，阻礙全球網際網路的自由連通。

針對網際網路領域中美雙方意識形態分歧，中國共產黨在第十八屆中央委員會第三次全體會議通過《中共中央關於全面深化改革若干重大問題的決定》提出「加大依法管理網絡力度，加快完善互聯網管理領導體制，確保國家網絡和信息安全。」[14]中央網路安全和資訊化領導小組成立，習近平擔任組長。中國大陸此舉是從戰略層面防堵美國利用網路自由等名義，通過網路自由承載著美式自由、民主等價值觀，煽動政治運動，培植親美

[12] 〈美國國務卿希拉蕊柯林頓關於網際網路自由的演說 華盛頓新聞博物館〉，《美國在台協會》，2010 年 1 月 21 日。〈http://ait.org.tw/zh/news/officialtext〉，檢索日期：2019 年 10 月 15 日。

[13] "International Strategy for Cyberspace," *The White House*, May, 2011. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf >.(Accessed 2020/1/26).

[14] 新華社，〈中共中央關於全面深化改革若干重大問題的決定〉，《中華人民共和國人民府網》，2013 年 11 月 12 日。〈http://www.gov.cn/jrzg/2013-11/15/content_2528179.htm〉，（檢索日期：2019 年 10 月 14 日。）

勢力，實現政權更替，這與中國大陸所維護國家主權及領土完整的核心利益有所違背。[15]

中美雙方在網路安全問題，根本原因在於對網路空間認知的差異：美國試圖確保關鍵基礎設施安全、商業技術機密維護和網路自由的之餘，亦可持續對國際網路空間有控制權。反之，中國大陸重視的是網路空間是國家主權延續和政權的穩定，雙方所關注的網路安全亦有不同。

二、中美雙方於網路安全領域競爭

中美雙方於網路安全領域競爭從政策面都有顯著區別。首先，從美國學者詹森（Thomas Johnson）所編著的《網路安全：捍衛網路戰時代中的關鍵基礎設施》（Cybersecurity: Protecting Critical Infrastructures from Cyber and Cyber Warfare ）著作中，詳細和綜整美國網路安全的威脅，「關鍵基礎設施的防護」、「網路情報」、「網路衝突」與「網路戰」，對於研究網路安全等議題具有顯著之貢獻。尤其關鍵基礎設施之防護至關重要，美國瞭解網路安全涵蓋軍事、經濟、民生等各個領域。美國前總統小布希（George W. Bush）於 2003 年執政期間公佈《確保網路空間的國家戰略》（The National Strategy to Secure Cyberspace），第一次將「網路空間」設定為國家安全戰略報告，內容指出：「關鍵基礎設施依賴網路科技進行運作，將國防工業、通訊、資訊技術等 18 項基礎設施部門列為關鍵基礎設施，並且將核電廠、政府設施等 5 項列為重要資產，透過制定防護措施，保護資訊基礎設施免於遭受破壞、干擾，進而維護美國經濟發展，達成國家安全之目的」。[16]然而報告重

[15] 闞道遠，〈美國網路自由戰略評析〉，《現代國際關係》，第 8 期，2011 年，頁 22-23。

[16] "The National Strategy to Secure Cyberspace", *The White House*, February, 2003 < ttps://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf>.(Accessed 2020/1/26).

點在於政府已開始制定相關防護措施，避免關鍵基礎設施遭受破壞。由此可知，網路空間安全與否將牽動國家持續和平及繁榮發展的關鍵因素。

其次，中國大陸對網路安全領域的憂心，從美國企業掌握中國大陸關鍵基礎設施為例，在思科（Cisco）、微軟（Microsoft）、IBM、谷歌（Google）、高通（Qualcomm）、英特爾（Intel）、蘋果（Apple）、甲骨文（Oracle）等八大企業，已深入中國大陸各種不同領域。以思科為例，更是在「中國大陸電信」六大骨幹網路、國家銀行、海關、公安、武警、工商、教育等政府機構，以及鐵路、航空、港口、石油、傳播媒體等各領域，佔有相當優勢，亦可是全面滲透到中國大陸電信、金融、石油、化工等關係到國計民生的關鍵資訊基礎設施，危及中國大陸國家安全。[17]

最後，沒有網路安全就沒有國家安全，沒有資訊化就沒有現代化。習近平於 2014 年 2 月 27 日召開「中共中央網絡安全和資訊化領導小組」首次會議時所強調網路安全和資訊化，係攸關國家安全與國家發展之重大戰略問題，中國大陸雖已成為網路大國，但沒有網路安全就沒有國家安全，沒有資訊化就沒有現代化，其重視程度不容忽視。顯見維護網路安全是中國大陸國家經濟發展的前提和基礎。

三、中美雙方於外交領域競爭

中美雙方就網路空間屢次在外交領域競爭。首先，美國前總統歐巴馬公佈《網路空間國際戰略》指出：「美國將與各國或國際組織通過多邊和雙邊合作確立新的國際行為準則，加強網路防禦能力，減少針對美國政府、企業，尤其是對軍方網路的入侵」。[18]網路攻擊如果威脅到美國及同盟國國

[17] 朱志平、梁德昭，〈習近平時期美中網路安全競逐〉，《遠景基金會季刊》，2016 年，第 27 第 2 期，頁 11-12。

[18] " International Strategy for Cyberspace," *The White House* , May, 2011. <https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf >.(Accessed 2020/1/26).

家安全，美國將不惜動用軍事力量進行報復。2011 年 7 月 14 日，美國國防部發佈《網路空間行動戰略》（Strategy for Operating in Cyberspace），提出提升美軍網路空間作戰的「五大支柱」。分別是，一是把網路空間列入美軍行動領域。二是主動防禦。三是保護關鍵基礎設施。四是美軍將加強與北大西洋公約組織（North Atlantic Treaty Organization, NATO）和合作夥伴在網路空間的國際合作。五是人才培訓和技術指導。[19]美國政府和軍方在不到 2 個月裡連續推出 2 大網路戰戰略，是在網路空間積極「佈勢」舉動，可以清楚發現美國運用外交，通過與同盟國之間以及北大西洋公約組織等雙邊和多邊方式，宣傳與推進美國全球網際網路戰略，設置有關國際網際網路發展、治理、安全與防禦等全球議題，掌握全球網際網路發展與規則制定的主導權。[20]

其次，中國大陸面對美國在外交領域的攻勢下，中國大陸一直對美國利用「網路自由」的思想，進行和平演變十分警惕，認為首要目標是保護國家主權和安全，在網際網路的領域也不例外。因此，對於內部網際網路屬於一國主權管轄範圍之內，主張依據中國大陸法律進行管理，設置內容審查及防火牆，對非法及敏感資訊進行過濾。對於外部而言，習近平在 2015 年「世界互聯網大會」上提出「網路安全是全球性挑戰，沒有哪個國家能夠置身事外，獨善其身」，中國大陸參與網路安全的國際合作可以讓中國大陸更深入參與國際網路規則的制定，並從根本上維護網路主權。[21]

從 2010 年中國大陸、俄羅斯、塔吉克和烏茲別克於「上海合作組織」通過多邊國際論壇推廣其價值，共同起草的《資訊安全國際行為準則》，提

[19] "The U.S. Department of Defense Strategy for Operating in Cyberspace," *The U.S. Department of Defense*, July,2011.<https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf >.(Accessed 2020/1/26).

[20] 王翔，〈中美網路安全領域博弈機裡分析及未來展望〉，《中國與國際關係學刊》，2016 年，第 2 期，頁 41-42。

[21] 王翔，〈中美網路安全領域博弈機裡分析及未來展望〉，頁 44。

出可使網路空間規則的制定有別於西方主流價值觀，更能展現其多元化，中國大陸透過雙邊與多邊等方式表達自身觀點，進而影響國際立法，達到維護國家主權和提升國際地位的雙重目標。[22]

上述所強調的突顯出網路安全就是國家安全，中國大陸亟欲發展自己的國有企業，好擺脫美國掌握中國大陸內部的網路關鍵基礎設施，然而在國際上中國大陸要運用自身建立的影響力，在聯合國及區域性國際組織等平臺，把中國大陸所提倡的尊重各國的網路主權的理念推展開來。而國內學者只針對中國大陸「網路強國」有所研究，尚未對中國大陸利用雙邊多邊等外交手段影響國際網路規則制定，是以筆者想以中國大陸網路空間戰略為主軸檢視中國大陸影響國際網路規則背後的動機與目的，以利提升國際地位跟增加網路空間的話語權與影響力。

貳、中國大陸網路空間戰略之探討

中國大陸於 1994 年正式接入全球網際網路以來，已經進入全新的網際網路迅速發展時期，截至 2018 年 12 月底，由中國大陸互聯網路資訊中心發佈的第 43 次《中國互聯網路發展狀況統計報告》顯示中國大陸上網人數規模達 8.29 億，手機使用網路人數規模達 8.17 億，已成為使用網際網路的世界大國。如今，網際網路正以開放、包容、共用等特點，滲透到經濟、文化、生活等領域，重塑新的價值觀和生活方式，但也造成文化和政治上的衝突。[23]有鑑於此，習近平於中國共產黨第十八次全國代表大會以來，發表多次涉及網路戰略的系列講話。在此，筆者綜整中國大陸網路空間戰略的主要內容。

[22] 蘇金遠，〈《資訊安全國際行為準則》草案簡評〉，《中國資訊安全》，2013 年 8 月，頁 92。
[23] 中國互聯網路資訊中心，〈2019 年中國互聯網路發展狀況統計報告〉，《中國網信網》，2019 年 8 月。〈http://www.cac.gov.cn/2019-02/28/c_1124175677.htm〉。(檢索日期 2019 年 10 月 1 日)。

隨著經濟社會的不斷發展與進步，網路已成為當今社會發展不可或缺的重要組成部分，中國大陸的網路發展也進入全新領域，由於網路空間的特殊性和跨國性，使得網路空間衍生出各種衝突。就中國大陸內部情勢而言，借助網路犯罪的行為時常發生，個人隱私洩漏和侵犯、網路詐騙、網路暴力和利用網路進行散播不實消息,破壞社會秩序等犯罪行為層出不窮。就國際情勢而言，2010 年 7 月伊朗核電廠離心機遭受到震網病毒攻擊和 2013 年美國稜鏡事件，這些事件影響著中國大陸的國家安全與發展。

中國大陸面臨的網路安全威脅可歸納為三個面向。首先，從國家意識形態層面。美國及其盟國標誌「網路自由」，對中國大陸進行政治和意識形態的滲透，傳播不實資訊，挑戰中國共產黨執政合法性，甚至是支持和鼓吹分裂主義，試圖顛覆中國大陸政府的執政權，這與中國大陸所維護國家主權及領土完整的核心利益有所違背。

其次，從經濟和社會層面。中國大陸的網路關鍵基礎設施和資訊系統發展較晚和整體技術落後；應對網路駭客等攻擊，防禦能力落後，在出現類似伊朗震網病毒式的侵襲，這些關鍵基礎資訊系統一旦崩潰，不僅影響到社會和經濟帶來重大損失，甚至會危害國家安全。

最後，從軍事層面。資訊化的進程，使軍事對抗和戰爭已愈來愈依賴網路，直接改變戰爭型態，而衍生的是中、美兩國在軍事上的競爭。[24]美國在歐巴馬總統上任後，加速推動網路部隊的發展，並繼續維持在網路領域的領先地位。從 2009 年開始，不僅設立網路司令部，並在各軍種成立網路司令部，充分運用網路與軍事優勢相結合，進一步確保美國的國家安全。2013 年習近平接任中國大陸國家主席後，美國積極建立網路部隊，於 2016 年時已成立 123 支網路作戰部隊，總人數 4900 人，由三大部分組成，27 支

[24] 丁藝，〈網絡安全視角下的網絡空間安全戰略構建〉，《電子政務》，第 7 期，2014 年，頁 4。

執行進攻任務的作戰部隊，68 支保護國防部內部網路的網路部隊，13 支是國家任務部隊，主要保護美國國內重要關鍵基礎設施，另外支援部隊 25 支，已具備初步作戰能力。[25]

反觀中國大陸，根據美國智庫「2049 計畫研究所」(Project 2049 Institute)研究指出，隸屬於共軍總參謀部第三部第二局的 61398 部隊是以美國和加拿大為目標，不僅竊取情報，還有操縱美國電網和其他公用事業設施等關鍵基礎設施的能力。[26]習近平擔任中共中央軍委主席後於 2013 年 11 月中共十八屆三中全會提出「深化軍隊體制編制調整改革，推進軍隊政策制度調整改革，推動軍民融合深度發展」，[27]並於 2015 年 12 月 30 日新組建戰略支援部隊，將原本隸屬於總參謀部技術偵察部和電子對抗部，整併後納入新成立戰略支援部隊網絡系統部。[28]

面對中國大陸在軍事領域積極發展網路能力抗衡美國，雖然美國全球軍力遠勝中國大陸，但中國大陸可利用網路戰先發制人，可針對美國政府及商業重要基礎設施和網路資訊系統，進行破壞對方的軍事防禦能力和軍事指揮系統的運作，以達到削弱美軍作戰的能力。[29]

綜上所述，中國大陸面臨「意識形態」、「經濟和社會層面」和「軍事層面」之威脅，因此建構網路空間戰略，必須圍繞在政治、法律制度和戰略等各層面。首先，重視網路空間戰略的頂層建制。中共於 2014 年成立中

[25] 朱治平、梁德昭，〈習近平時期美中網路安全競逐〉，《遠景基金會季刊》，第 17 期第 2 期，2016 年 4 月，頁 28-31。

[26] David E. Sanger, David Barboza, & Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking against U.S.," *New York Times*, February 18, 2013, <http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seenas-tied-to-hacking-against-us.html?_r=0>.

[27] 〈全會公報十大看點：明確全面深化改革總目標〉，《新浪網》，2013 年 11 月 13 日。〈http://news.sina.com.cn/c/2013-11-13/025928692758.shtml〉。(檢索日期 2019 年 10 月 1 日)。

[28] 林穎佑，〈中共戰略支援部隊任務與規模〉，《展望與探索》，第 15 卷第 10 期，2017 年 10 月，頁 112。

[29] David C. Gompert & Martin Libicki, "Cyber Warfare and Sino-American Crisis Instability,"*Survival*, Vol. 56, No. 4, August-September 2014, pp.7-22, <http://www.iiss.org/en/publications/survival/sections/2014-4667/survival--global-politics-and-strategy-august-september-2014-838b/56-4-02-gompert-and-libicki-04fc>.

央網絡安全和資訊化領導小組，突顯出中國大陸把網路安全上升為國家戰略，而要發揮集中指揮和統一領導的作用，並須統籌及協調各地區、各部會和各領域的網路和資訊安全等重大議題，並能進一步明確管理職責，整合資源並建立機制，全面提升中國大陸網路安全的組織體系。[30]

其次，建構國家網路空間安全的法律制度。自習近平擔任國家領導人後，對特別是美、中兩國在網際網路領域中的競爭逐漸加劇之際，習近平加強對網路的關注。習近平在 2013 年中共十八屆三中全會強調，網路和資訊安全牽涉國家安全和社會穩定，是中國大陸面臨綜合性挑戰；如何加強網路法制建設和輿論導向，確保資訊傳播秩序和國家安全，已成為中國大陸所面臨到的挑戰。[31]除透過技術層面管控網路言論之外，中國大陸亦透過立法手段對網路言論進行控制。

中國大陸在 2015 年通過《國家安全法》，第 25 條規定「國家建設網絡與資訊安全保障體系，加強網絡管理，防範、制止和懲治網絡攻擊、網絡入侵、網路竊密、散播違法有害信息等網絡違法行為，維護國家網絡空間主權、安全和發展利益。」[32]明確呼應習近平所說，沒有網路安全就沒有國家安全。[33]

中國大陸於 2016 年 11 月召開第十二屆全國人民代表大會常務委員會第二十四次會議通過《網絡安全法》，其目的是「保障網絡安全，維護網絡

[30] 余俊傑、白瀛，〈在通向網絡強國的征程上穩步前進-寫在中央網絡安全和資訊畫委員會成立一周年之際〉，《新華網》，2019 年 3 月 20 日。〈http://www.xinhuanet.com/2019-03/20/c_1124261185.htm〉。(檢索日期 2019 年 11 月 1 日)。

[31] 習近平，〈關於《中共中央關於全面深化改革若干重大問題的決定》的說明〉，《中國共產黨新聞網》，2015 年 7 月 20 日，〈http://cpc.people.com.cn/xuexi/n/2015/0720/c397563-27331312.html〉。

[32] 《中華人民共和國國家安全法》係 2015 年 7 月 1 日為第 12 屆全國人民代表大會常務委員會第 15 次會議通過，該法共分為七章、84 條。全文請見〈中華人民共和國國家安全法〉，《人大新聞網》，2015 年 7 月 10 日，〈http://npc.people.com.cn/BIG5/n/2015/0710/c14576-27285049.html〉。(檢索日期 2019 年 11 月 1 日)。

[33] 中國國家互聯網信息辦公室，〈習近平：沒有網絡安全就沒有國家安全〉，《中國國家互聯網信息辦公室網站》，2018 年 12 月 27 日。〈http://www.cac.gov.cn/2018-12/27/c_1123907720.htm〉。(檢索日期 2019 年 11 月 1 日)。

空間主權和國家安全、社會公共利益，保護公民和組織的合法權益，促進社會經濟資訊化的健康發展」。[34]從中國大陸對「網路主權」的強調，不僅突顯出欲確保對境內網路空間絕對控制外，特別在於前美國國家安全局（National Security Agency, NSA）外包技術員史諾登（Edward Snowden）於2013 年 6 月在香港將美國國家安全局關於稜鏡計畫揭露給英國《衛報》(The Guardian）和美國《華盛頓郵報》（The Washington Post）後，[35]亦擔心美國的網路技術能突破其封鎖，輸入西方意識形態，危害其對網路空間言論的絕對掌握，透過立法手段，藉由法律來加強對中國大陸內部的網路言論的控制，避免造成國家安全危害之局面。

最後，規劃網路空間的戰略架構。中國大陸互聯網信息辦公室於 2016 年 12 月 27 日發布《國家網絡空安全戰略》和 2017 年 3 月 1 日互聯網資訊辦公室和外交部共同發布《網絡空間國際合作戰略》。前者明確指示「捍衛網路主權，維護國家安全，保護關鍵基礎設施，加強網絡文化建設，打擊網絡恐怖和違法犯罪，完善網絡治理體系，夯實網絡安全基礎，提升網絡空間防護能力，強化網絡空間國際合作」等九項任務。[36]

中國大陸首次以國家戰略文件的形式，要從中國大陸內部和國際等層面，提出推進和平、安全、開放、合作和秩序等五項具體目標。其中，和平與合作是著眼於國際，目的是有效遏止資訊技術的濫用，反對網路空間軍備競賽，有效防範網路空間衝突，逕而加強資訊技術交流、打擊網路恐

[34]〈中華人民共和國網絡安全法〉，《新華網》，2016 年 11 月 7 日。〈http://www.xinhuanet.com/politics/2016-11/07/c_1119867015.htm〉。(檢索日期 2019 年 11 月 1 日)。

[35] Te-Ping Chen，〈美國家安全局洩密案主角仍在香港〉，《華爾街日報中文網》，2013 年 6 月 13 日。〈 https://web.archive.org/web/20130616065036/http://cn.wsj.com/gb/20130613/bus095630.asp?source=whatnews2〉。(檢索日期 2019 年 11 月 1 日)。

[36] 中國國家互聯網資訊辦公室，〈國家網絡空安全戰略〉，《中國國家互聯網信息辦公室網站》，2018 年 12 月 27 日。〈http://www.cac.gov.cn/2016-12/27/c_1120195878.htm〉。(檢索日期 2019 年 11 月 11 日)。

怖組織和犯罪等合作，建立完善多邊、民主和透明機制的全球網際網路治理體系。中國大陸內部則側重於安全與開放。安全目標具體在掌握核心技術裝備，穩定網路和資訊系統技術和滿足網路安全人才的需求，提升網路安全意識和基本防護能力。[37]

後者，《網絡空間國際合作戰略》，提出應在「和平、主權、共治、惠普等四項基礎上，推動網路空間國際合作和宣導各國遵守《聯合國憲章》（Charter of the United Nations）的宗旨，確保網路空間的和平與安全；堅持主權平等，不搞網路霸權，不干涉他國內政等網路主權聲明；並主張各國應共同制定網路空間國際規則，彌平數字鴻溝，以確保安全分享和使用發展的成果。」[38]

然而，美國與中國大陸以在國家安全戰略下，將網路空間視為新的戰場，彼此競爭，相互指責，但對於中國大陸網路空間的穩定攸關著中國大陸主權的伸張，從國家安全和經濟發展下，中國大陸適時提出《網絡空間國際合作戰略》，彰顯中國大陸對網路主權與維護是不容他國介入與干擾，所以強調各國應在相互尊重自主的網路管理模式、選擇網路發展道路，並在國家主權的基礎上建構國際合作平臺，共同建構多邊、透明的全球網際網路治理體系，實現資源分享、責任共擔、合作共治。[39]

隨著資訊社會的快速發展，政治、社會、經濟、軍事等安全均建立在網路安全上，顯而易見，在資訊安全時代，誰能掌握網路安全，誰就佔據網路安全的制高點，然而國內學者只針對網路安全有所研究，而尚未對中

[37] 朱莉欣、韓曉陽，〈基於機遇和挑戰，謀求發展和安全-比較中解讀《國家網絡空安全戰略》〉，《資訊安全與通信保密》，2017 年 2 月，頁 28-31。

[38] 中央網絡安全和資訊化領導小組，〈《網絡空間國際合作戰略》(全文)〉，《新華網》，2017 年 3 月 1 日。〈http://www.xinhuanet.com/politics/2017-03/01/c_1120552767.htm〉。(檢索日期 2019 年 11 月 11 日)。

[39] 潘兆民，〈中國大陸發布《網絡空間國際合作戰略》政策意涵之評析〉，《展望與探索》，第 15 卷第 5 期，2017 年 5 月，頁 30-34。

國大陸發布《國家網絡空安全戰略》和《網絡空間國際合作戰略》兩大戰略指導下，以建設網路強國為目標，不僅要維護主權，要有先進的技術，必且彙聚人才資源以建設政治強、質量精、作風優良的強大隊伍，而領導小組要能發揮統一集中的領導作為，制定國家網路安全和資訊化發展的宏觀戰略和政策，並積極影響全球網路規則制定，取得全球網路治理的話語權，進而達到中華民族偉大復興的戰略目標。[40]

參、影響國際網路規則制定

中、美兩國在網路空間的矛盾與衝突和美國前國安局雇員史諾登揭露稜鏡事件，使得中國大陸日益重視建構全球網路空間治理的新秩序，在參與推動建設全球網路空間秩序的過程中，筆者整理中國大陸在參與國際網路空間的國際規則制定模式，分別為「國際參與」與「內部掌控」。

一、國際參與

自網路空間治理問題成為一項全球治理的新議題以來，聯合國就在其中扮演著重要的角色。尤其面對開發中國家與已開發國家的網路能力和話語權不平衡的狀況下，聯合國成為開發中國家參與治理的最佳途徑。

首先，以聯合國涉及網路空間治理領域的相關組織或平台，主要有資訊社會世界峰會（World Summit on the Information Society，以下簡稱 WSIS）和國際電信聯盟（International Telecommunication Union，以下簡稱 ITU）等兩部分。

(一)資訊社會世界峰會

[40] 中央網絡安全和資訊化領導小組，〈中央網絡安全和資訊化領導小組成立：從網絡大國邁向強國〉，《中國共產黨新聞網》，2014 年 2 月 27 日。〈http://cpc.people.com.cn/BIG5/n/2014/0227/c64094-24486382.html〉。(檢索日期 2019 年 11 月 11 日)。

其主旨是為全球範圍內資訊社會的協調發展的規制定，利用資訊技術推動聯合國發展目標，及各國經濟社會持續發展，促進全人類的進步。WSIS的歷史發展過程大致分為兩大階段，第一階段是峰會階段，第二階段為論壇階段。首先，峰會階段是以 2002 年至 2005 年分別舉行日內瓦峰會和突尼斯峰會。其中，日內瓦峰會通過《原則宣言》（Declaration of Principles）和《行動計畫》（Plan of Action）。

《原則宣言》界定資訊通信技術對未來社會、經濟和文化發展產生巨大影響，提出建設資訊社會的 11 條基本原則，並對未來全球資訊通信的發展，提出原則性指導。而《行動計畫》則將《原則宣言》化為舉體的行動方針，已通過廣泛運用資訊通信技術的網路、服務和應用來實現全球資訊發展的目標。[41]

其次，突尼斯峰會探討是如何縮小「數位鴻溝」[42]等全球網際網路治理與發展等議題，最後通過《突尼斯承諾》（Tunis Commitment）和《突尼斯議程》（Tunis Agenda for the Information Society）。《突尼斯承諾》重申日內瓦峰會《原則宣言》，強調彌平數位鴻溝，促進各國資訊技術交流。而《突尼斯議程》重點放置在建立數位鴻溝的融資機制和網際網路治理等相關議題。

然而，這兩次峰會衍生出美國等西方的已開發國家和中國大陸等開發中國家對於資訊社會等議題，產生嚴重分歧，主要在兩大爭議性問題。第一，關於消除數位鴻溝的問題。由於網路關鍵基礎設施的差異，貿易上的

[41] "Declaration of Principles," *World Summit on the Information Society*, December 12,2003 < https://www.itu.int/net/wsis/docs/geneva/official/dop.html >.

[42] 數位鴻溝在中國大陸稱為數字鴻溝。為了行文和閱讀的方便，除非文章必要維持之外，均以台灣用語數位鴻溝一詞表示。數位鴻溝是指在全球數位化進程中，不同國家、地區、行業、企業、社區之間，由於對資訊、網路技術的擁有程度、應用程度以及創新能力的差別而造成的資訊落差及貧富差異，進一步兩極分化的趨勢。劉俊、張蕾、俞立平，〈中國數位鴻溝評估研究：基於移動通信工具視角〉，《統計與決策》，2019年字第 5 期，頁 32。

鴻溝，中國大陸等開發中國家和已開發國家存在著基礎設施和技術發展上的差異。已開發國家將網際網路的關鍵基礎設施認定為智慧財產權保護的對象，而中國大陸等開發中國家認為正是因已開發國家對資訊技術和智慧財產權的壟斷，才導致資訊通訊技術應用的差距擴大，因此中國大陸等開發中國家提出建立專門基金，如團結基金（Solidarity Fund）來幫助開發中國家開發資訊技術，但卻遭美國等已開發國家反對。

第二，全球網際網路管理權歸屬問題。中國大陸等開發中國家認為網際網路的管理應納入聯合國領導框架下，各政府機構可參與協作，而美國堅持以商業利潤為原則。中國大陸和巴西等代表提出要把網際網路功能變數名稱和 IP 地址管理組織（Internet Corporation for Assigned Names and Numbers, 以下簡稱 ICANN）的業務交由國際電信聯盟管理，而美國、歐洲等已開發國家仍堅持由網際網路名稱與數字位址分配機構負責管理。[43]

最後，自日內瓦和突尼斯峰會之後，WSIS 進入論壇階段。自 2009 年開始正式定名為資訊社會世界論壇，從 2009 年至 2016 年發展特徵，主要是注重資訊技術發展議題，包括通過建設資訊基礎設施、拓寬資訊通信技術的應用，加大資訊和智慧財產權的獲取，以促進世界各國資訊技術的發展。WSIS 作為聯合國領導下最主要網路治理機制之一，對網際網路的發展和治理產生深遠的影響，但是各國對網路治理的主權歸屬問題爭執不斷。美國為首等西方國家認為要建立一個與網路組織合作的論壇；而中國大陸等開方中國家認為聯合國機構應有的接管網際網路的控制。WSIS 表面上為各國政府之間的鬥爭，實質上是美國與中國大陸等國家就全球網際網路的控制權展開的競爭，相較於美國主導的 ICANN 平臺，WSIS 更平衡開發中

[43] 許瑋陰，陳帥，方興東，〈資訊社會世界峰會的演進歷程和發展現狀〉，《汕頭大學學報》，第 33 卷第 7 期，2017 年，頁 30。

國家在國際網路治理參與程度，而中國大陸已成為網路大國，一直積極找尋自己的定位，從中國大陸在內部削減數位鴻溝，加大資訊基礎設施，網路經濟和創新等議題，都全層參與，積極發聲，一路朝著網路強國的目標邁進。[44]

(二)國際電信聯盟

20 世紀末，通訊和資訊技術飛速發展，以全球網際網路和移動通訊改變人們的生活方式，推動社會、經濟、文化和科技等各領域的發展，人們預測 21 世紀將是「資訊世紀」，有效的國際合作顯然是關鍵性，誕生於 1865 年的國際電報聯盟（International Telegraph Union, ITU），1932 年改稱為國際通訊聯盟，1947 年聯合國成立時將其設立為下設機構，是國際間最早成立的國際組織。其宗旨是促進各種電信業務的研發和國際合作；提高電信服務的效率，增加使用率和達到大眾化和普遍化；協調各國電信標準化、無線通訊規範和通訊發展的目的。[45]

中國大陸近代電報發展於 1870 年代，當時是電報是由外國殖民者營運，清政府迫於外國侵略的刺激下，開始創辦電話和無線電報於 1906 年以觀察員的身分參加柏林召開的無線電大會。辛亥革命後，中國大陸進入長達 38 年的戰亂，在此背景下，電信業發展極為緩慢。1949 年，中國大陸建政後，經中國大陸人民革命軍事委員會批准，電信總局成立，到 1957 年底已建成國內長途有限通訊網路。1971 年因聯合國《2758 號決議，承認中華人民共和國為中國大陸的合法政府，加入國際電信聯盟。改革開放後，鄧小平重視通訊發展「中國發展經濟，搞現代化，要從交通、通信入手，這是經濟

[44] 許瑋陰，陳帥，方興東，〈資訊社會世界峰會的演進歷程和發展現狀〉，《汕頭大學學報》，頁 30-34。
[45] 陳陽，〈國際電信聯盟簡介〉，《現代通信》，第 8 期，1998 年，頁 2。

發展的起點」，[46]這一時期的電信業發展與工業化發展密切，直到中國電信營運商壯大後，中國大陸政府才慢慢放寬外資准入。

改革開放迄今，中國大陸電信業已獨立自主，已成為中國大陸「走出去」的重要戰略目標，在中國大陸政府的鼓勵下，中國移動及中國電信等電信產業也紛紛走向世界，以中興、華為等晶片製造業也至海外拓點，中國大陸政府制定的電訊政策與國際通訊聯盟的政策大體一致，中國大陸不僅需要參與國際通訊領域的治理，而且要在通訊領域的話語權得利。

國際通訊聯盟的誕生在於制定通訊技術的統一標準，而國際標準制定不僅直接讓製造商獲利並能提升製造商所在國家在通訊領域的影響力與話語權。因此，中國大陸於 1998 年積極參與國際通訊聯盟三大組織之一標準局局長改選，由中國大陸所推薦的趙厚麟獲選。中國大陸政府透過參與國際通訊標準化局組織改選下，有利推動中國大陸製造業在國際市場上發展，使中國自主研發的標準通行於全世界。

國際通訊聯盟於 2014 年第 19 次全權代表大會舉行秘書長選舉，由中國大陸趙厚麟當選秘書長，改變一直由西方已開發國家擔任秘書長的格局。[47]之後，中國大陸代表團於 2019 年由中國大陸資訊通信研究院、華為、中興、中國信科、中國移動等單位向國際通訊聯盟「WP 5D」提交 IMT-2020（5G）技術方案，並已獲得國際電信聯盟的正式接收確認函。[48]

中國大陸政府與通訊產業積極參與國際通信標準化，有利推動中國大陸從電信大國邁向電信強國，使得中國大陸製造業在國際市場能見度大增。

[46] 資訊產業部辦公廳〈我國電信領域改革開放大事記〉，《中國資訊產業網》，2001 年 2 月 27 日。〈http://www.cnii.com.cn/20020808/ca79451.htm〉。(檢索日期 2019 年 11 月 11 日)。

[47] 〈趙厚麟成國際電信聯盟 150 年來首位中國籍秘書長〉，《人民網》，2014 年 10 月 24 日。〈http://ip.people.com.cn/BIG5/n/2014/1024/c136655-25900794.html〉。(檢索日期 2019 年 11 月 12 日)。

[48] 中國信通院〈中國完成面向國際電信聯盟的 5G 候選技術方案提交〉，《新浪科技網》，2019 年 7 月 18 日。〈https://tech.sina.com.cn/5g/i/2019-07-18/doc-ihytcerm4459560.shtml〉。(檢索日期 2019 年 11 月 12 日)。

在華為、中興等科技公司崛起，致力於通過國際通訊聯盟標準制定，使中國大陸自主研發的標準通行於全世界，並擴大在國際通訊領域的話語權。[49]

二、內部主導

中國大陸政府近年來致力於積極參與聯合國與國際組織，試圖將「網絡主權」（Cyber Sovereignty）等理念傳達至其中，而在中國大陸政府主導的世界互聯網大會等網路相關會議，這些作為不僅展現中國大陸在參與國際網路治理的影響力與日俱增，也間接重塑國際網路運行規則，挑戰美國等西方國家的主導地位。

首先，中國大陸政府將《網絡空間國際合作戰略》的戰略構想融入當前積極推行的「一帶一路」倡議（One Belt One Road, OBOR）之中，陸續在 2017 年推出「數字絲綢之路」（Digital Silk Road）等戰略構想，提倡在沿線開發中國家的網路基礎建設，加強數位元經濟、人工智慧、大數據、雲端計算和智慧城市，[50]藉此深化與區域間國家的互賴關係，並擴大中國大陸在區域的影響力。

再者，中國大陸政府透過 2014 年在浙江烏鎮舉辦「世界互聯網大會」（World Internet Conference）的常態性會議平臺，廣邀世界各國的網路事務主管、資訊企業領袖與網路安全技術專家與會交流，藉此擴大和各開發中國家及資訊產業等在數位經濟發展方面的合作，同時也向國際社會宣示中國大陸網路科技實力與宣揚「網路主權」的政治理念。[51]

[49] 左志，〈國際電信聯盟與中國崛起-以中國電信政策研究為視角〉，《新聞大學學報》，第 3 期，2016 年，頁 16-17。

[50] 〈習近平在“一帶一路”國際合作高峰論壇開幕式上的演講〉，《“一帶一路”國際合作高峰論壇官方網站》，2017 年 05 月 14 日。〈http://www.beltandroadforum.org/BIG5/n100/2017/0514/c24-407.html〉。(檢索日期 2019 年 11 月 15 日)。

[51] 〈烏鎮倡議〉，《新華網》，2015 年 12 月 18 日。〈http://www.xinhuanet.com/politics/2015-12/18/c_1117512543.htm〉。(檢索日期 2019 年 11 月 15 日)。

最後，中國大陸近年積極參與全球網路治理事務，在聯合國或是中國大陸主導的世界互聯網大會推行「網路主權」的概念，強調網路空間和現實空間一樣，既要提倡自由，也要保持秩序，在中國大陸境內的網路設備與訊息內容，都要遵守中國大陸的法律，就如同領土、領海、領空依樣，在虛擬的網路空間中，國家依然保有主權。此番舉措，試圖將「網路主權」的理念，導入全球網路治理的規範之中，進而重塑國際法體系，向美國等西方國家主張的「網路自由」理念提出挑戰。

整體而言，中國大陸政府當前積極推動網路戰略，對內部從黨組織成立中央網絡資訊領導小組，從法制層面著手，頒布《國家安全法》和《網絡安全法》，將網路安全視為國家安全。對國際，則強調與其他國家的合作交流，期望藉此獲得科技與技術上的實質收益，並逐步擴大在全球網路治理體系中的影響力，甚至爭取聯合國下轄組織領導人的意向，其目的在重塑由美國等西方國家主導的全球網路治理體系，確立中國大陸在網路領域中能與美國抗衡的強權地位。

第三節 研究途徑與研究方法

壹、研究途徑

依據方法論區分為研究途徑與研究方法，研究者須先確定研究途徑，而所謂研究途徑係指研究者對研究對象，是從哪一層次為出發點、著眼點、入手處，去進行觀察、歸納、分類與分析。[52]本文研究主旨為中國大陸網路空間戰略，必須先瞭解網路戰略的政策源起、演變與發展，始能深入問題核心，因此將採「攻勢現實主義」為本文研究取向。

[52] 朱浤源主編，《撰寫博碩士論文實戰手冊》，（臺北：正中書局，1999 年），頁 182。

後冷戰時期，國際格局的改變，傳統的現實主義以顯然不適合新型式的需要，攻勢現實主義（Offensive Realism）提供一個理論基礎。代表人物是米爾斯海默(John Measrsheimer)，《大國政治的悲劇》（the Tragedy of Great Power Politics）一書中提出，該理論主要承襲古典現實主義「無政府狀態」（anarchy）及「權力最大化」等基礎和瓦茲（Kenneth Waltz）的新現實主義認為國際體系結構導致國家追求自身權力最大化終極目標是成為霸權。[53] 攻勢現實主義的理論架構可歸納為國際政治的「基本假設」來確保權力最大化：一是國際體系處於無政府狀態，而國家無法保證其他國的意圖，因此國家必須採取自助。二是透過攻勢獲取權力。三是大國想要「改變現狀」。四是大國的終極目標是成為區域霸權。[54]

綜上所述，攻勢現實主義從當前的國際現勢分析，強調國家在無政府狀態下，國家並非追求最大權力，而是更關注生存與安全的問題。後冷戰時期，由於國際格局的變化以及中國大陸在國際社會影響力日漸增，中國大陸更關注生存與安全的問題。在網際網路時代，全球形成一個沒有疆界的網路世界，在此領域各種行為和言論通過網路迅速傳播，並產生足以影響整個世界動態的力量。

筆者自權力競爭的角度觀之，可知國際上的權力競爭已從傳統的軍事領域延到非傳統安全領域，網路空間被應用於戰爭的事件層出不窮，如伊朗於 2010 年 9 月遭受震網病毒攻擊，此類新型的網路犯罪行動，迫使許多國家投入網路治理等相關工作。但當前網路空間仍處於無政府狀態，因此，中國大陸無法掌握他國的意圖必須採取自助，從政策、立法、組織等層面

[53] 張訓譯，〈習近平的「中國夢之一帶一路」：從攻勢現實主義的觀點分析〉，《樹德科技大學學報》第 21 卷第 2 期，2019 年，頁 182。

[54] 張國城，〈中國航母的發展模式：攻勢現實主義的觀點〉，《遠景基金會季刊第十八卷第三期 2017 年 7 月》第 18 卷第 3 期，2017 年 7 月，頁 86-87。

建構網路空間戰略，和運用國際組織或是自身主導的場合宣揚網路主權的理念，以達到生存與安全的需求。本論文將以攻勢現實主義理論檢視具有中國大陸網路空間戰略的發展特點，以及國際參與所帶來影響與評估。

貳、研究方法

將採用「文獻分析法」，以宏觀角度下檢視中國共產黨和中國大陸國務院所發布之國家外交及網路空間國際戰略等政策、檔案、領導人有關發言進行縱向整理；其次再以美國政府及智庫出版書籍對參與國際組織等議題來釐清中國大陸網路空間戰略佈局，期待能全面完整描繪出 完整樣貌，研究者將文獻分析後，產生的歷史演變之因果關係與辯證，也是一種因果推論的研究方法，[55]而文獻分析的主要來源與途徑，可概略區分為以下三種

表 1-1 文獻種類區分

第一手來源 (Primary)	第一手資料是以其原始格式提供資訊，包括檔案、官書、歷史遺物、遺址、文件、數據(data)、訪談(interviews)、日記(diaries)、相片(photographs)。
第二手來源 (Secondary)	第二手資料來源是指對於第一手資料解釋與提出判斷的成品，包括期刊文章(journal articles)、專書(books)、翻譯(translations)。
第三手來源 (Bibliographic Instrument)	書目性工具是那些將相關性資訊加以組織的工具，包括百科全書(encyclopedia)、字典(dictionaries)、年刊(yearbooks)、書目(bibliographies)、索引(indexes)、摘要(abstracts)、電子索引(electronic indexes)。

資料來源：朱浤源編，《撰寫碩博士論文實戰手冊》（臺北：正中書局，2006），頁 103。

[55] 陳偉華，《軍事研究方法論》（臺北：國防大學，2003 年 7 月），頁 143。

參、研究架構

研究架構係指研究問題的步驟與程式，本文首先探討中國大陸網路戰略之意涵與特點，其中在以特點去劃分為「立法層面」、「戰略層面」和「組織層面」，再藉由「網路空間國際戰略」的脈絡去整理出中國大陸在參與國際組織的立場與後續影響，由中國大陸主導國際會議 G20 元首峰會、金磚五國元首高峰會和浙江省烏鎮所舉辦的「世界互聯網大會」所傳達的網路主權理念，以及參與北大西洋公約組織、上海合作組織和東南亞國協等區域性組織和聯合國組織及網路治理平台，以參與國際規則的研擬等方式，逐步影響世界各國對網路規則制定的看法，逕而影響全球網路規則制定做全面性說明，本文以總結進行檢討及建議；本篇論文研究架構如下圖 1-1 所示：

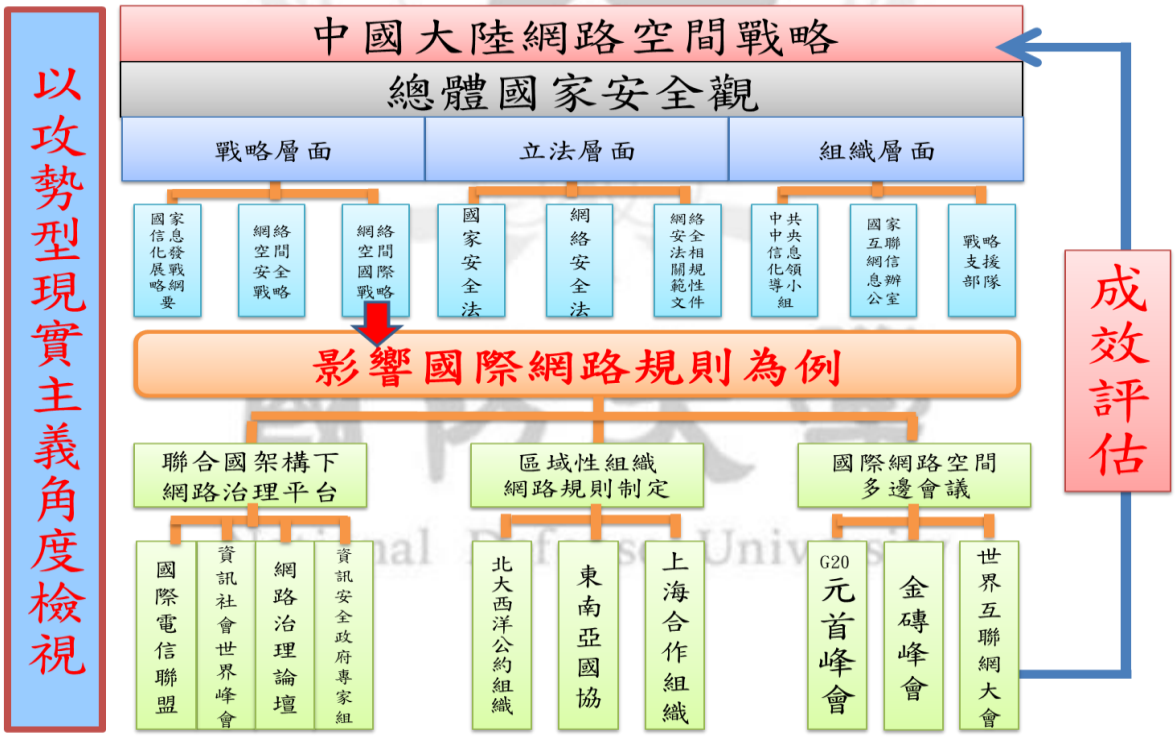

圖 1-1 分析架構

資料來源：筆者研究繪製

第四節 研究範圍與限制

壹、研究範圍

一、時間界定

以中國大陸國務院新聞辦公室發布的 2010 年《中國互聯網狀況》白皮書，內容指出，中國大陸積極運用外交手段參與全球網際網路的國際交流與合作並支持在聯合國框架下，產生網際網路的國際管理機構，這些都可檢視中國大陸網路空間國際戰略。本文以 2010 年為研究起點迄 2019 年 12 月 30 日止，檢視中國大陸的網路空間國際戰略及影響國際網路規則為時間範疇。

二、研究資料

中國大陸網路戰略雖有機敏性，但所幸中、英文等文獻近年來大量出現，有關相關主題文獻若涉及於網路戰、網路所屬部隊、裝備、機密等檔，均不列入本文研究資料。本文資料蒐整均採用公開資訊，以中國大陸官方機構所發布的公開資訊或出版著作以及外文文獻，可使本研究達到客觀及中立的立場。

三、研究對象

本研究以「國際網路空間治理」為主要研究範圍，並特別著重在「聯合國組織及其架構下的網路治理平台」、「區域性國際組織國際網路規則制定」和「網路空間多邊會議」之討論面。試將研究對象說明如下：因受限於時間及資料蒐集的限制，無法一一對每個聯合國組織、區域性國際組織和多邊會議之網路空間治理均進行研究。因此本文主要以聯合國下轄組織國際電信聯盟為代表，並帶入聯合國架構下網路治理平台以「資訊社會世界峰會」、「網際網路治理論壇」與「資訊安全政府專家組」為研究對象。

區域性國際組織則選擇以制定網路戰國際法手冊為代表性的「北大西洋公約組織」。中國大陸積極推動帶路倡議和數位絲綢之路，需要沿線國家在網路空間合作上多邊的區域性國際組織以「上海合作組織」和「東南亞國協」為研究所在。網路空間多邊會議則以中國大陸輪值主辦的二十國峰會和金磚峰會倡導網路主權概念為例，並著重在中國大陸主導的世界互聯網大會，邀請開發中國家研議網路空間議題，並舉辦論壇。其餘聯合國組織、區域性組織及其他國際會議不在本文研究所指範圍內。

貳、研究限制

由於以中國大陸外交手段切入網路戰略議題為新領域的研究方向，尤其是網路安全、網路攻擊及網路戰，其各國資料與文獻頗具豐碩，筆者置重點於中國大陸參與國際事務等層面切入，對於中國大陸網路空間戰略之發展與運用作綜合析論。

然而中國大陸屬於一黨專政的政權，所有宣傳媒體皆由國家統籌，對於相關敏感資訊有所監控，對外發布資訊必須符合官方政策及形象，且實地田野調查及取得第一手資訊等方式不易，所以引用公開資訊為主，任何涉及機密資料均不採用，雖然有這方面限制，但本次研究文獻來源，力求具代表性與有效性。

國防大學
National Defense University

第二章 攻勢現實主義理論與探討

在國際政治學領域中現實主義被認為是國際關係中主導地位的理論，雖然歷經二次世界大戰及冷戰後世界格局的變動，刺激著國際政治理論的創新。現實主義學派分為「古典現實主義」(Classical Realism)、「結構現實主義」(Structural Realism)或稱「新現實主義」(Neo-Realism)和「攻勢現實主義」(Offensive Realism)對權力的定義、手段、目的的詮釋有所異同，但是「權力政治」始終是主軸。

「攻勢現實主義」延續著「古典現實主義」和「新現實主義」架構而來。兩者區別歸納出兩點：首先，古典現實主義者認為，國家就是要不斷地謀求擴大自身的權力，權力被視為目的本身，對權力的追求根植於人性中。然而新現實主義者認為，權力故然重要，但卻是一種手段，國家最終所關心的並不是權力，而是安全。

其次，古典現實主義重視國家之間的差異，主要通過單元層次的分析來解釋國際政治下的後果；新現實主義者認為主要從結構層次入手，認為國際政治後果主要從無政府狀態和權力分佈來解釋。而攻勢現實主義則結合摩根索（Hans Morgenthau）的「權力政治」和瓦茲（Kenneth Waltz）的新現實主義，認為國際體系結構導致國家追求自身相對權力的最大化，以及國家間的權力鬥爭是無可避免的，終極目標是成為霸權國。

本研究是採用美國政治學者米爾斯海默的攻勢現實主義作為理論分析的基礎，主張國際體系是無政府狀態的，雖然權力並不一定是國家行為的目的，但國家最終目的亦是生存與安全，必須追求權力極大化，以上述觀點檢視中國大陸網路空間戰略，以參與國際事務案例，是否符合攻勢現實主義認為中國大陸將權力與安全置於首位,且在面對不確定的網路空間中，國家所要爭取的就是自身權力和成為區域霸權之推論。至此，本章區分三節「現實主義緣起」、「攻勢現實主義內涵」和「中國大陸在國際網路空間戰略應用」做一整體性的說明。

第一節　現實主義的源起

國際關係中的現實主義學派於 30 年代形成，於 40 年代發展至 50 年代以後成為國際關係學界中的主流理論。現實主義不是新興學科，是承襲歷史悠久的權力政治思想，可追溯到西元前 500 多年，希臘是眾多城邦構成的國際體系，許多國際政治的基本原則在此得到驗證。古希臘歷史學家修昔底德（Thucydides）編著《伯羅奔尼撒戰爭史》（History of the Peloponnesian War）對於雅典與斯巴達戰爭有著精闢分析，提出下列意見：國家之間的對立與仇恨是各國獨立的基本條件，也是各國尋求同盟的原因。當國家必須

永遠掌握權力和利益，否則無法生存。這以國家利益為前提，對現實主義學派具有啟示作用。[1]

15 世紀馬基維利（Niccalo Machiavelli）的《君王論》（The Prince）是現代主義學派對權力現實分析的先驅，[2]其理論建立在三項論點上：其一，歷史是一連串的因果序列，不能用想像或幻想，只能用知識去分析和理解。其二，理論不能創造實踐，唯有不斷的實驗，才能解決問題。其三，政治不能與一般倫理觀念混為一談，有其自身的運作原則，必要時，可以合理化手段。[3]馬基維利由此推斷出強調外交、軍事以及專制的對內與對外策略。並由法律和武力兩種方式，統治者才能得勝，唯有持續擴張才能保有社會安定和國家安全，統治者可以為國家，不遵守一般道德規範和法律，只為達到保護全體國民的利益。馬基維利的君王論成為後來國際政治理論家的思想和理論的基礎。[4]

從馬克維裡權力現實的分析到霍布斯（Thomas Hobbesl）在《巨靈》（Leviathan）一書中說明「無政府的狀態」，此概念對後來的現實主義學者影響深遠，加上近代的威特（Martin Wight）現實主義成為國際關係最主要的理論，往後的學者只是加以整理和闡述而以，而集大成者摩根索成為代表者，其著作正好和第二次世界大戰後美國成為世界超強一同問世。

[1] 林碧炤，《國際政治與外交政策》，（台北：五南，2006 年），頁 39-40。
[2] 吳東林，《巨變中的強權政治-體系變遷與美中台》，（台北：時英，2002 年），頁 53。
[3] 林碧炤，《國際政治與外交政策》，頁 40。
[4] 王逸舟，《國際政治學-歷史與理論》，（台北：五南，1999 年），頁 11。

作為國際關係的主流，被視為古典現實主義學者有摩根索和吉爾平（Robert Gilpin）等。各時期的現實主義從各個角度對國際政治的性質以及主要原則做出諸多精闢的論述。而筆者將現實主義者的論述區分為三部分，加以整理，歸納出現實主義的核心基本假設。

首先，摩根索，他不但是現實主義學派的奠基宗師，是迄今為止最具影響力的國際關係學家之一。[5]摩根索總結之前的現實主義學者的觀點與思想，並加以歸納整理，同時也提出自身的觀點，建立系統化的現實主義國際關係理論。

摩根索於 1948 年出版的《國家間政治》（Politics Among Nations）在此書中提出人的本性是利已的，人為自身的安全要追求權力；國家的本性同人的本性一樣，國家為本國的利益也要追求權力。他從國家追求強權和強權政治的邏輯出發，直接導引出「均勢論」（The balance of power）。幾個國家尋求權力，或試圖維持現狀和推翻現狀，這種情況必然將導致幾個權力對峙的形勢發生，這種形勢稱為「權力平衡」，也將使各國採取政策以維持「權力平衡」。

權力平衡的概念指在若干穩定的自主力量體系在任何時候，受到外力或因內部組成份子的變化而遭受到干擾時，體系顯示要重建其原有平衡，

[5] 王逸舟，《西方國際政治學：歷史與理論》，（上海：上海人民出版社，2006 年），頁 93。

或建立新的平衡機制。這些平衡的目的就是要保持體系的穩定，阻止任何成員權力優勢壓過其他成員地位，確保體系內部成員的存續。[6]他說若干嚮往強權的國家，各自試圖維持現狀或推翻現狀，最後必然會導致一種稱為均勢的格局及只在維持這種結構的政策。[7]

摩根索依據對近代歷史的分析，強調均勢平衡者或支配者是佔有關鍵地位和決定性的一方，是與任何一國或集團的政策是維持均勢，所以會把自身的優勢加到弱勢一方，使國家不可能凌駕於其他國家之上的優勢，是國際政治最具方法的重要因素。[8]

其次，吉爾平認為不論哪時期的現實主義，他們理論基礎都未改變，均有共同假設。其一，強調衝突集團的重要性。從歷史上集團曾出現多種形式，如部落、城邦和帝國等。而現代衝突集團的表現形式是民族國家。其二，國家利益的重要性。國家行為主要是受到國家利益所驅使，利益可分為經濟和領土等。儘管國家利益本身受到主、客觀因素影響，但維護國家利益仍是國家的首要任務。其三，權力的重要性。在一個無政府狀態和利益衝突為特徵的世界，權力和大國關係將是國際事務的主要特點，現實主義者重視經濟力量並視軍事力量為政治的最終決定力量。[9]

---

[6] 林碧炤，〈國際關係的典範發展〉，《國際關係學報》，第 29 期，2010 年，頁 17-19。

[7] Thomas Hobbes, *Leviathan*, ed. and with an introduction by Michael Oakeshott（Oxford, England: Basil Blackwell, 1946）, p. 64.

[8] Hans J. Morgenthau, A Realist Theory of International Politics, Essential Readings in World Politics (New York: W. W. Norton & Company, 2001), pp. 48-53.

[9] Robert Gilpin, "The Richness of the Tradition of Political Realism", *International Organization*, Vol. 38, No. 2, Spring 1984, pp. 287-304.

最後，古典現實主義的共同假設從人性（human nature）的角度分析國家對於權力的追求。每一個行為體的主要行為動機，就是要取得一個使自己安全的地位。按照權力分配方式的不同，國際秩序可以劃分為世界政府型、霸權型、權力均衡型、參與型和國際組織型五種類型。現實主義者認為權力均勢是主權國家體系中維持國際秩序穩定的理想模式。其實不論古典或新現實主義，他們理論基礎具有下列共識。

第一，以國家為中心，國家是國際政治的行為體，更注重解釋國家的行為，而對於個人或國際組織的行為體不甚重視。

第二，現實主義將無政府狀態是為國際社會的主要特點，由於國際社會中不存在權威來保證協議付諸實行並提供安全保障，所以各國必須依靠自身的力量來維護自身的利益。現實主義者雖不否認國家之間合作的可能性以及國際制度規範的作用，但認為對國家間有侷限性跟拘束性。

第三，國家謀求自身安全或權力的最大化。

第四，國家在追求權力或安全實奉行理性政策。

第五，重視武力，國家依靠使用或威脅使用武力來維護自身的利益和加強自身的安全。[10]

現實主義主要是強調富國強兵的重要性，對於戰爭的正當性與合法性是採支持的態度。[11]連帶對於國家安全、軍事擴張、國家利益和聯盟體系採

[10] 包宗和主編，《國際關係理論》(臺北，五南出版社，2011 年 5 月)，頁 5。

一樣重視，政治優於法律，而經濟要為政治服務。這樣的主張在 19 世紀的歐洲盛行，幾乎整個歐洲對帝國主義的擴張，海外殖民地的掠取、經濟的剝削和政治壓迫都是從這主張找到理論根據。但冷戰結束之前，現實主義受到諸多挑戰，其中最主要原因是經濟因素的提升、權力的性質多樣，無政府的國際社會已有國際組織發揮功能，於是古典現實主義所主張的權力之爭，以無法解釋冷戰時期而被批評，而後發展出新現實主義。[12]

第二節　攻勢現實主義內涵

古典現實主義在第二次世界後成為國際關係中的主流，但無法預測冷戰的結束而遭受到強烈的批評，開始質疑現實主義的主張。西方國家的國際關係學者經過長時間的辯論及實際政治的檢驗，在學術上強調社會科學化的國際關係已成為學界的共識。其次，在國際政治上，發生越戰、美蘇和解、美中關係正常化和歐洲整合使得現實主義的傳統理論的適用性受到質疑。

新現實主義理論者瓦茲，繼承摩根索的無政府狀態的大架構下去思索新現實主義。其一，擺脫摩根索運用歷史事實的研究方式，以說理和演繹的方法去推論出國際政治理論。其二，引用社會科學的實證主義，參考自然科學的方法，透過簡化而成的通則，針對國際事件沒有探討戰爭的起因、

[11] Hans Morgenthau&Stephen Walt, *The Origins of Alliances,* (Ithaca, New York: Cornell University Press, 1987) .pp. 120-122.

[12] 林碧炤，〈國際關係的典範發展〉，《國際關係學報》，頁 18。

結果和影響，可說是革命性的專書，對往後的學者造成影響。其三，採用經濟學和一般體系理論來說明國家在國際社會中如何自保。其四，推崇二元體系理論，國家間不易發生衝突，較容易掌控及處理。其五，使用結構和單元分析國家在國際政治中如何去保護自己，爭取最大利益。[13]

瓦茲的《國際政治理論》（Theory of International Politics）出版後，被認為是新現實主義的先驅，從古典現實主義的窠臼中跳脫出來，走向科學化的方向，以下針對瓦茲《國際政治理論》的論點，歸納四點予以說明。

第一，瓦茲認為在一個無政府狀態結構下，國家只能自助來求取生存，正因為安全沒有保障，故國家不免視他國為國家威脅對象，這種不信任及恐懼導致安全困境，使得國與國之間無法合作。在自助體系下，不僅在意自己獲得多少利益，也關心他國獲得多少利益，因他國既然為自己的潛在威脅，任何力量的增長，均會增長他國的不信任感，特別當任何一個國家都無法確定其他國家未來的意圖，國家彼此間對任何獲益都相對敏感，相互合作也略顯困難，所以瓦茲認為國際體系不能由內向外解釋，而須從國際體系分析著手。[14]

第二，瓦茲認為權力不是目的，而是實現國家目標的手段，然而國際體系是無政府狀態，並鼓勵國家追求安全極大化，而非權力極大化，國家

[13] 林碧炤，〈國際關係的典範發展〉，《國際關係學報》，頁 36。
[14] 林碧炤，〈國際關係的典範發展〉，《國際關係學報》，頁 18。

在乎的是維持其在體系中的地位。在相對得利的思考下，國家尋求的是權力平衡。國家若追求權力則會加入強勢一方，因而造就霸權，但就保障自身安全，強勢一方終究會對自己造成威脅，故應加入弱勢一方，以確保權力平衡。

反之，在一個階層體系下採取扈從策略是可以理解的因為失去平衡不會危及自身安全。故從某個角度而言，平衡策略與扈從策略均可作為生存之道，端視在何種體系架構下而定。此亦為體系結構決定國家行為的一項推論性佐證。[15]對新現實主義者而言，最穩定的權力分配體系是兩極體系。二元之優多元，依據瓦茲觀點，在於兩極體系下方警覺性提升，特別是過度反應。多元架構之下行為者較不具責任感，對危險具有不確定性，重大利益也較不明確。[16]

第三，新現實主義者認為安全為國家首要關注，但同時也強調經濟利益的重要性。瓦茲就指出所謂安全乃是國家會不斷追求其政治與經濟獨立性並抵禦他國的潛在威脅。[17]而其他新現實主義學者更強調經濟利益在當前國際政治的重要性，經濟實力往往是政治以及軍事實力的重要基礎。[18]

第四，瓦茲於 1979 年提出新現實主義，不僅對於古典現實主義的諸多內涵有所批評與修正，更加入系統理論以求更完整的解釋以更為完整的詮

[15] Jack Donnelly, *Realism and International Relations* (New York: Cambridge University Press, 2000), p. 18.
[16] 林碧炤，〈國際關係的典範發展〉，《國際關係學報》，頁 29。
[17] 羅伯特吉爾平著、楊宇光、楊炯譯，《全球資本主義的挑戰-21 世紀的世界經濟》(上海：上海人民出版社，2001 年)，頁 19-22。
[18] David Baldwin, *Key Concepts in International Political Economy* (England : E. Elgar Pub. Co.1993), p. 10.

釋國家的意圖與行為，乃至國家間的互動關係，其與古典現實主義相異之處在於結構的概念。

首先，摩根索認為國際政治的本質就是權力爭奪，因此當個別國家試圖透過國際政治來實現其所追求的目標，這些國家就是為權力爭奪。新現實主義指出，由於國際秩序屬於無政府的狀態，並沒有更高的權威能夠給予仲裁，各別國家的存亡端視其所採取有利其生存的作為，因此國家所追求的目標是安全而非權力，權力僅是手段而非目的。[19]

其次，由於國際社會權力爭奪與衝突的本質，古典現實主義認為各別國家都在極力的擴張其所擁有的權力，即使國際合作對於各個國家都是有利可圖的，任何國際合作終究會在衝突與爭奪中毀滅。新現實主義認為組織與制度的角色效果有限，主要是依賴大國的主導，但並不否認國際組織與制度合作出現的可能，其認為具有主宰力的國家會尋求建立與維繫有利於己的組織與制度，其他國家則會選擇加入該組織與制度，在既定的遊戲規範中保障自身的利益。

最後，新現實主義並未有理性抉擇的假設，主要是瓦茲重視系統結構的概念，解釋國家若是理性，應該學習其他國家歷史成功經驗才能適合生存於系統中，但是歷史上有太多證明顯示國家並未追求理性的行為，或是

[19] Gideon Rose, “Neoclassical Realism and Theories of Foreign Policy” , *World Politics* , Vol. 51, No. 1, 1998, p. 151.

無法記取教訓只能走向衰敗，因此瓦茲不認為國家是理性的行為者。瓦茲的「國際政治理論」一書奠定學術上的領導地位，[20]最主要原因是運用社會科學分析把古典現實主義從傳統的權力分析中跳脫出來。但瓦茲未預測到冷戰結束，而所推崇的二元體系一樣宣告結束，對於現實主義造成的衝擊直到 2000 年後才逐漸平息。

國際關係學者對於新現實主義的研究並沒有停止，更多著作相繼問世，其中又以米爾斯海默的「大國政治的悲劇」一書最具代表性。[21]他沿襲古典現實主義對權力政治角度分析和新現實主義的國際體系的論述。關於攻勢現實主義理論的探究，以下分為三點而論之。

首先，攻勢現實主義承襲古典現實主義和新現實主義理論的傳統對部分假設與立論進行修改。據此提出「國際體系為無政府狀態」、「國家想要擁有攻擊性的武力」、「生存是國家首要的目標」、「國家從未能確定其他國家的意圖」，以及「國家是理性的行為者」等五個重要的假設。

其一，國際體系為無政府狀態。攻勢現實主義雖然承襲古典現實主義與新現實主義之國際體系的無政府狀態之假設，然而攻勢現實主義最主要論述是由新現實主義之國際體系結構對國家行為的影響，作為推論國家追

[20] 林碧炤，〈國際關係的典範發展〉，《國際關係學報》，頁 30。
[21] John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: Norton, 2001), pp. 30-32.

求安全需求的依據，而並非以古典現實主義從人性對權力的貪婪的角度作為探究國際關係之根據。[22]

其二，國家想要擁有攻擊性的軍事武力。古典現實主義按照修昔提底斯將權力當作理論的假設之一，並強調國家追求權力特性的分析進而提出政治是為權力而鬥爭者。而新現實主義將權力是為其理論之關鍵性的變數，包含自然資源、工業能力、軍事的能力等。而攻勢現實主義亦重視權力，並將其為理論的核心，但不同於古典和新現實主義的是權力內涵的主要是在於攻擊性的軍事能力。[23]其認為基於國際體系為無政府狀態以及國家對其他國家以在潛在威脅之故，一個國家擁有愈多的軍力，會造成其他國家更大的威脅，因此，最強的軍力就是安全最強的保障，以對抗他國之威脅。[24]

其三，國家從未能確定其他國家的意圖。相較於古典和現實主義而言，攻勢現實主義更關注國家不確定性意圖的問題，故將此列為五大假設之一。其認為無政府狀態的國際體系，國家意圖的不確定姓，當作是制約國家行為之決定性因素，面對持續性的生存威脅的恐懼之下，強權會把握權力極大化的時機，擴張權力，以確保國家安全。[25]

[22] 林宗達，〈國際關係攻勢現實主義理論之評析〉，《朝陽人文社會學刊》，第 9 卷第 2 期，2011 年，頁 64。
[23] John Mearsheimer 著，張登及、唐小松、潘崇易、王義桅譯，《大國政治的悲劇》(臺北，麥田出版社，2014 年 7 月)，頁 77。
[24] John Mearsheimer 著，張登及、唐小松、潘崇易、王義桅譯，頁 104。
[25] John Mearsheimer 著，張登及、唐小松、潘崇易、王義桅譯，頁 77-78。

其四，生存是國家的首要目標。古典現實主義在權力決定利益的情形下，追求權力，就是促進國家利益，從經驗探知，權力的差異是決定國家是否能繼續存在的關鍵，擁有較大權力的國家，生存機會比較小國家大。至於新現實主義國家最終的目標是安全極大化。攻勢現實主義沿襲現實主義的傳統，強權國將會尋求領土的完整和國內秩序的自主性，生存掌控強權的動機，安全成為國家最為重要的目標。[26]

其五，國家是理性的行為者。古典現實主義者摩根索認為權力等同於利益，而國家的外交作為都是以獲取權力與安全為主要目的，因而追求權力的極大化。而新現實主義者瓦茲，均承襲古典現實主義對國家理性的假設，但新現實主義者認為追求權力是手段，安全才是國家的最終的目的，因此，新現實主義者認為是追求安全極大化。攻勢現實主義是結合古典和新現實主義，認為國家理性的思考如何因應外部環境和生存戰略，因權力愈高安全愈高，權力愈大安全最有保障，故追求權力極大化以獲取國家安全極大化。[27]

依據前述五項重要的假設，米爾斯海默推論強權彼此間互相猜忌與懷疑對方的意圖，而心生恐懼，唯有依靠自身的力量維護國家安全，以追求相對權力極大化。然而國際體系是無政府狀態，必須依靠自助，但勢必會加劇他國的不確定性與軍事能力的恐懼，而在追求權力和安全最大化下，

[26] 林宗達，〈國際關係攻勢現實主義理論之評析〉，頁 65。
[27] John Mearsheimer 著，張登及、唐小松、潘崇易、王義桅譯，《大國政治的悲劇》，頁 78。

國家要追求的就是成為區域霸權。然就當前政治發展而論，中國大陸自從2008 年後成為網路使用人數的大國，勢必採取攻勢作為而獲取權力，改變現有網路空間治理的規則，終極目標是成為網路空間的霸權國。

第三節　中國大陸在國際網路空間規則戰略應用

隨著網路資訊技術日新月異，網路空間對全球化影響扮演相當重要的角色，國與國之間在經濟、貿易、交通、文化等範疇憑藉著網路交流互動，形成安全與利益錯綜複雜的國際關係。[28]從攻勢現實主義角度認為確保其生存，安全才是國家的目標，權力只是追逐安全的手段。根據攻勢現實主義的基本假設，最後認定大國間會因追逐權力而成為霸權：[29]一是國際體系處於無政府狀態，而國家無法保證其他國的意圖，因此國家必須採取自助。二是透過攻勢獲取權力。三是大國想要「改變現狀」。四是大國的終極目標是成為區域霸權。

從這基本假設分析中國大陸網路空間戰略。網路空間有虛擬性、即時性、跨國性等特性，成為繼陸、海、空、天之外國家所競逐的第五領域。網路空間涉及經濟、科技、能源、社會等多項領域，中國大陸對於網路安

[28] 梁德昭、朱志平、林凱薰，〈國家主權延伸至網路空間之討論〉，《前瞻科技與管理》，第 2 卷第 2 期，2012 年 11 月，頁 3-4。

[29] 張國城，《從「攻勢現實主義」看台灣的「活路外交」及「外交休兵」》，《台灣國際研究季刊》，第 11 卷第 1 期，2015 年春季號，頁 78-79。

全威脅的恐懼，因而尋求自助，而自助便是追求國家權力和安全的最大化。筆者將從三個部分，結合攻勢現實主義論點進行驗證。

首先，美國為網路空間的既有霸權。全球網際網路起源於美國，自啟用之日起，美國就主導其過程。其一，運用非政府組織「網際網路名稱與數字位址分配機構」對網路資源的分配有支配權。其二，通過美國八大科技企業[30]掌握網路資訊產業軟、硬體的關鍵技術。其三，利用網路空間制定規範和規則，倡導其他國家加入規範，將國際規範或規則內化成國內法等方式，成為網路間制度的霸權國。[31]其四，美國於 2013 年稜鏡事件的爆發，使各國震驚美國透過網路侵犯他國主權。其五，美國積極組建網路部隊。曾任美國網路司令部(Cyber Command)司令亞歷山大(Keith Alexander)於 2013 年表示，美國 40 支網路部隊，其中有 13 支的重點是進攻，其他 27 支的重點是培訓和監控。如果美國在網路空間遭受重大攻擊時，將可向其他國家發起進攻性的網路攻擊。[32]從攻勢現實主義角度而言，上述這些舉措，突顯出美國作為網路空間的既有霸權，仍試圖採取權力極大化的手段，以維持在世界的優勢。

[30] 美國科技業的「八大企業」是指思科、IBM、谷歌、高通(Qualcomm)、英特爾(Intel)、蘋果(Apple)、甲骨文(Oracle)、微軟(Microsoft)。

[31] 王向陽，〈進攻性現實主義視角下中美網絡空間關係〉，《南方論刊》，第 5 期，2019 年，頁 25-26。

[32] Mark Mazzetti & David E. Sanger, “Security Leader Says U.S. Would Retaliate Against Cyberattacks,” *New York Times,* March12, 2013, <http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-posethreat-to-us.html>.（瀏覽日期 2020 年 2 月 15 日）.

然而，中國大陸對美國網路竊密如此恐懼，因美國八大企業以深入中國大陸各個關鍵領域，如中國大陸電信骨幹網路、四大銀行、海關、公安、武警、工商、教育等政府機構，以及鐵路、航空、港口、石油、傳媒等不同領域，亦是全面滲透到中國大陸電信、金融、石油、化工等關係到國計民生的關鍵資訊基礎設施，危害中國大陸國家安全；[33]其次，中國大陸為網路空間潛在大國，面對既有霸權美國本身為獲取權力採取攻勢作為，中國大陸無法掌握美國之意圖，因此必須採取自助的行為。在此背景下，中國大陸欲想改變現狀，不僅在對內推動多項政策和對外參與國際組織並企圖影響國際網路規則治理，對中國大陸網路空間戰略區分為內部及國際層面兩部份觀察。

一為內部層面。自從 2012 年習近平接任國家領導人，面對美國的科技壟斷和嚴重的網路空間安全威脅，於 2014 年成立「中共中央網絡安全和資訊化領導小組」，藉由組織調整並由習近平親自擔任組長，彰顯中國大陸保障網路安全、維護國家利益及推動資訊化發展的決心，[34]以及擴增共軍編制，於 2015 年成立「戰略支援部隊」，除整合過往共軍情報組織外，更將偵查、電子對抗、航太作戰、網路部隊都納入管轄，解決過去中國大陸情報體系

[33] 秦安〈對美國「八大金剛」不能不設防〉，《環球網》，2013 年 6 月 4 日。〈https://opinion.huanqiu.com/article/9CaKrnJALYl〉。(檢索日期 2020 年 2 月 15 日)。

[34] 新華網〈中央網絡安全和資訊化領導小組成立：從網絡大國邁向強國〉，《中國共產黨新聞網》，2014 年 2 月 27 日。〈http://cpc.people.com.cn/BIG5/n/2014/0227/c64094-24486382.html〉。(檢索日期 2020 年 2 月 15 日)。

涉及多部門、情報整合不易和資源分散的問題，對於未來共軍戰力在航太、太空、網路等取得相當優勢。[35]

習近平於2014年召開中共中央網路安全和資訊化領導小組首次會議提到網路安全和資訊化，攸關國家安全與國家發展的重大戰略問題，雖然已成為網路大國，但沒有網路安全就沒有國家安全，沒有資訊化就沒有現代化，要建設網路強國，不僅要有自己的技術，還要匯聚人才資源，以建設政治強、業務精的強大隊伍。[36]

近年陸續推出《「十三五」規劃綱要》、《「十三五」國家信息化規劃》、《國家資訊化發展戰略綱要》、《資訊通信行業發展規劃（2016-2020 年）》、「互聯網+」、「雲計算創新發展」、「寬帶中國」和「5G 移動通訊技術」等政治規劃，積極推展 5Gt 產業發展，預計到 2025 年建設 1140 萬 5G 基地台。[37]中國大陸在資訊技術經歷落後到追趕再到領先，挾帶的龐大的人力和廣大的市場引起跨國企業參與 5G 的建設和佈署全球的 5G 專利，使 5G 成為中國大陸引領雲端計算、大數據、人工智慧等戰略產業。

二為外部層次。中國大陸政府擴大國際合作，推動「數位絲綢之路」和「東協資訊港」等建設方案，協助周邊地區資訊網路的發展，增進電子商務活動及網路創業產業的合作，藉此深化互賴關係，並擴大中國大陸在

[35]林穎佑，〈中共戰略支援部隊任務與規模〉，《展望與探索》，第 15 卷第 10 期，2017 年 10 月，頁 112。
[36]新華網〈中央網絡安全和資訊化領導小組成立：從網絡大國邁向強國〉，《中國共產黨新聞網》，2014 年 2 月 27 日。〈http://cpc.people.com.cn/BIG5/n/2014/0227/c64094-24486382.html〉。(檢索日期 2020 年 2 月 15 日)。
[37]新華網，〈中央網絡安全和資訊化領導小組成立：從網絡大國邁向網絡強國〉，《中國共產黨新聞網》，2014 年 2 月 27 日，< http://cpc.people.com.cn/BIG5/n/2014/0227/c64094-24486382.html>

區域內的影響力，逕而成為區域霸權。透過籌備「世界互聯網大會」廣邀世界各國的網路事務主管、網路資訊產業領袖與網路技術專家等與會交流，並試圖將其主張的「網路主權」概念導入其中，不僅展現中國大陸的網路科技實力與政策理念，同時也向國際社會宣傳中國大陸在國際事務上日益增加的影響力。

中國大陸在提振網路科技實力的同時，對網路安全的問題與日遽增。「中國國家互聯網資訊辦公室」在 2017 年底公佈《國家網絡空間合作戰略》提出推進和平、安全、開放、合作和秩序等五項具體目標。其中，和平與合作是著眼於國際，目的是有效遏止資訊技術的濫用，反對世界各國在網路空間軍備競賽，有效防範網路空間衝突，逕而加強資訊技術交流、打擊網路恐怖組織和犯罪等合作，建立完善多邊和透明機制的全球網際網路治理體系。

積極參與網路治理事務，強調國家主權應及於網路空間，並要求世界各國尊重網路主權，中國大陸的訴求在普遍傾向網路管制的國家響應，包含俄羅斯、阿拉伯聯合大公國及「上海合作組織」成員國，皆與中國大陸合作在「聯合國大會」及「國際電信大會」試圖將「網路主權」的理念導入國際網路規則建制的規範之中，此舉措也隱含改變全球網際網路規則制定，並挑戰美國網路空間的霸權地位。

最後，中美雙方在網路空間認知分歧，在習近平擔任國家領導人之前就已有 2010 年谷歌退出中國大陸、駭客竊密等事件。習近平擔任國家領導人後為解決網路安全的問題，雙方也透過理性的溝通及對話試圖降低雙方的緊張關係。

然而從攻勢現實主義的基本假設，網路空間可比現實國際體系更處於無政府狀態，現今的國際法規範無法處理網路安全議題，使各國的網路空間安全直接受到影響。同時，各國永遠無法把握其他國家的意圖和兼具在網路空間能夠傷害或摧毀對手的攻勢力量，使得大國更加以維護自身利益與生存為首要考量，進而以權力極大化的手段來維持在世界的優勢。

從美國史諾登揭露對世界各國實施稜鏡計畫後，及發佈網路空間戰略和建立網路司令部，突顯出既有強權美國對於其他崛起網路大國可能挑戰自身的地位而產生恐懼，試圖以權力極大化的手段來維持世界的優勢於不墜並強化與盟國的合作，確保國家利益免遭受網路攻擊而受到損害。

反觀中國大陸，自身與美國之間的科技實力有所差距，中國大陸的網軍部隊也成立較美國晚，規模也不如美國，但試圖改變並運用國內立法手段及對外國科技公司實施網路審查，減少網路竊密的情事發生，並加強輿論控制。由於美國與中國大陸雙方互有疑慮和猜忌及對於網路空間治理意識形態的分歧，在國際網路治理上欠缺相關法律規範，終將成為無政府狀態，美、中兩國在網路空間的摩擦只會日益加劇。

國防大學
National Defense University

第三章 中國大陸網路空間戰略的內涵與國內運用

習近平於 2012 年接任成為國家領導人，美國與中國大陸在網路空間領域的競爭成為兩國之間的焦點。美國是網路空間領域霸權國家，然隨著中國大陸經濟實力崛起後，不論在組織層面、立法層面及軍事層面的抗衡，以不時出現，除實現習近平提出的「網路強國」目標外，更有意改變美國在網路空間霸權的地位。因此，本章主要目的係從攻勢現實主義角度，檢視「中國大陸網路空間威脅概況」、「中國大陸網路空間戰略意涵」及「國內執行與特點」，析論中國大陸網路空間戰略之意涵。

第一節 中國大陸網路空間威脅概況

全球網際網路是 20 世紀人類偉大的發明，以網路乘載的新科技正改變著人們。誕生於美國的網際網路問世以來，運用在軍事、教育和科技領域，後來迅速向政治、經濟、社會等各領域蔓延，其戰略地位超越領土、領海、領空和太空之上，給人類帶來歷史變革。隨著資訊成為國家發展的重要戰略資源，國家間所圍繞著資訊的獲取、使用和控制的競爭也愈強烈，網路空間的安全成為維護國家安全和社會最重要的部分。

網路空間是隨著網路而出現的新的空間概念，根據聯合國國際電信聯盟的定義：「網路空間是指由電腦、電腦系統、網路及其軟體、電腦數據、

流量數據及用戶組成的物理或非物理的領域。」[1]而中國大陸所定義的依照2011年出版《中國人民解放軍軍語》指：「融合於物理層、資訊層、認知層和社會層，以網際網路為平臺，通過無線電、有線電信傳信號、資訊、控制實體行為的資訊活動空間。」[2]歸納出網路空間是一種相互依賴的資訊基礎設施網路構成的資訊交換區，由全球網際網路、通信網、電腦系統、伺服器、和數據等系統組成。

隨著資訊技術的進步，網際網路以全面進入到國家政治、金融、能源、資訊、軍事等各個領域。然而，網路有雙面刃的特質，享受著快速和便利的同時，一旦出現網路漏洞，不僅國家安全遭受到威脅，相關的民生、經濟和資訊系統失靈遭致癱瘓，危及國家安全。因此，網路空間擁有極大戰略利益，成為國家競爭的新空間。依據攻勢現實主義的基本假設，網路空間為無政府狀態，對於別國意圖不明時，國家必須採取自助的手段獲取安全，並尋求權力極大化進而改變現狀，終極目標是成為區域的霸權。因此，網路安全威脅儼然成為國家安全的首要解決問題。

首先，定義網路空間安全，依據中國大陸所頒布的《總體國家安全觀》指：「國家範圍內的資訊數據、資訊基礎設施、資訊軟體系統、網路、資訊人才、公共資訊秩序和國家資訊不受來自國內外各種形式威脅的狀態。」[3]網

[1] 翟賢軍、楊燕南、李大光，《網絡空間安全戰略-問題研究》(北京：人民出版社，2018年9月)，頁5。
[2] 全軍軍事術語管理委員會，《中國人民解放軍軍語》(北京，軍事科學院出版社，2011年)，頁288。
[3] 〈習近平在中國共產黨第十九次全國代表大會上的報告〉，《人民網》，2017 年 10 月 28 日。

路空間之所以易受攻擊，因網路系統具有開放、快速、分散、互聯、虛擬和脆弱等特點。網路用戶可自由訪問任何網站，不受時間與空間的限制，使得網路攻擊者有可乘之機，運用各種技術與漏洞，傷害網路空間的秩序與安全。

其次，中國大陸政府從 1991 年波斯灣戰爭，美軍展示掌握資訊主導權是戰場獲勝的唯一法寶。愛沙尼亞於 2007 年遭受到大規模的網路攻擊，國家安全、經濟和社會秩序嚴重癱瘓。伊朗核電廠設施遭受到「震網」蠕蟲病毒攻擊，網路攻擊的目標不單只是軍事系統，包含其他經濟的操作系統和美國前國安局雇員史諾登披露「稜鏡事件」，美國國家安全局長期監看電子郵件、網路訊息、影片等，上述國際事件引起中國大陸對網路空間安全的重視。

最後，網路安全的威脅已危害到中國大陸內部的各個領域。一是危害政治安全。網路作為新型的資訊傳播的新媒介，改變傳統政治生活，拓寬公民訴求和參與政治的管道，然而網路資訊的流通乘載美式的價值觀和意識形態，利用網路干涉內政、煽動民眾思緒、從事顛覆政權活動，這些舉措嚴重危害到中國大陸政府統治的合法性。

二是威脅經濟安全。網路和資訊系統已成為關鍵基礎設施和整個經濟社會的中樞，遭受到嚴重網路攻擊，將導致交通、金融、經濟、能源等基

〈http://cpc.people.com.cn/n1/2017/1028/c64094-29613660-7.html〉。(瀏覽日期：2020 年 3 月 29 日)。

礎設施癱瘓，嚴重危害國家經濟安全和公共利益。依據《2019 年上半年中國互聯網網絡安全態勢》顯示，2019 年上半年，發現電腦惡意程式數量約 3,200 萬個，遭感染的電腦主機數量約 240 萬台，位於境外的 3.9 萬個電腦惡意程式控制大陸地區約 210 萬台主機，主要境外的 IP 位址來源來自美國、日本和菲律賓等地區，利用電腦病毒竊取資料，嚴重威脅經濟安全。[4]

三是網路攻擊威脅軍事安全。資訊技術的發展改變未來戰爭型態和作戰模式，虛擬的網路空間成為新的戰場，制網權如同制空、制海、制天一樣成為兵家必爭新領域。誰掌握資訊網路，誰就控制政治、軍事及經濟。[5]網路間諜，可透過網路武器植入電腦病毒、木馬程式、駭客攻擊、訊息篡改和利用分散式阻斷服務攻擊（Distributed Denial of Service attack, DDoS），癱瘓對方系統或利用病毒試圖破壞關鍵基礎設施都是近期網路作戰的模式。打擊敵對勢力的指揮控制、武器操作系統，可迅速癱瘓敵方作戰體系，實現不戰而屈人之兵。這些有組織、有目的的破壞性網路攻擊對軍事安全威脅程度最高。[6]

[4] 國家計算機網絡應急技術處理協調中心〈2019 年上半年我國互聯網網絡安全態勢〉，《中華人民共和國國家互聯網資訊辦公室網站》，2019 年 8 月。〈http://www.cac.gov.cn/2019-08/13/c_1124871484.htm〉。

[5] 所謂制網權是指一個主權國家對電腦和網際網路系統的控制權與主導權，主要包含國家對國際網際網路根功能變數名稱的控制權、IP 位址的分配權、網路標準的制定權、網路輿論的話語權等。依據翟賢軍、楊燕南、李大光，《網絡空間安全戰略-問題研究》，頁 153。

[6] 網路戰是指敵對雙方使用網路攻防技術手段，針對國家安全特別是戰爭，可利用資訊和網路環境，圍繞制網權而進行的軍事對抗，以電腦和網路為主要攻擊目標。依據翟賢軍、楊燕南、李大光，《網絡空間安全戰略-問題研究》，頁 165。

四是網路恐怖主義破壞社會安全。恐怖份子早期以駭客手法，藉電腦病毒使電腦癱瘓，進行竊密和執行實體破壞等網路攻擊行動，已轉變為透過網際網路散發訊息，進行人員招募、資金募集、理念傳播與威脅利誘等重要手段，並透過精神施壓、意識轉變等方式發揮「激進式」影響，使新型網路恐怖主義成為危害當前大陸地區社會秩序與國家安全主因。[7]

中國大陸對恐怖主義、分裂主義、極端主義等合稱「三股勢力」，於 2014 年境內發生多起暴力或恐怖攻擊事件，諸如 5 月中旬新疆維吾爾自治區最南端的和田地區，發生維吾爾族向警方發動自殺炸彈攻擊；9 月中旬新疆阿克蘇地區發生「拜城煤礦攻擊案」；以及 9 月底時，廣西省柳城縣發生連環包裹炸彈事件。伊斯蘭國組織從 2014 年 9 月「建國」後，領導人巴格達迪（Abu Bakr al-Baghdadi）強調中國大陸壓迫穆斯林信眾，已有約 300 名新疆的維吾爾族人加入伊斯蘭國組織。[8]

通過上述分析，網路空間安全涉及政治、軍事、文化、科技、意識形態等多方面向，改變原本人與人之間的交流形式。網路空間的實用性，使國家在原本的政治體制、經濟運行、社會治理等受到挑戰，上述安全威脅衝擊中國大陸政府的現有體制和國家安全。呼應攻勢現實主義的推論，生

[7] 網路恐怖主義是「非國家組織或個人以破壞一國或多國政治穩定、經濟安全、擾亂社會秩序，製造使人心生恐懼地效果為目標，實行利用網路或對網路進行攻擊的活動。」依據黎雪琳，〈網絡恐怖主義探悉〉，《廣西警官高等專科學校學報》， 2008 年第 1 期，頁 17。

[8] 張文偉，〈上海合作組織資訊安全合作：必要性、現狀及前景〉，《俄羅斯東歐中亞研究》， 2016 年第 3 期，頁 95-97。

存是大國的目標，面對網路空間處於無政府狀態，中國大陸政府採取自助的手段來應對網路安全的威脅，尋求安全極大化。

第二節 中國大陸網路空間戰略意涵

以網際網路為代表的電腦網路時代已經徹底改變人類生活和生產方式，隨著資訊技術的持續變革，網路虛擬空間和現實生活也不斷融合。網路空間的安全性不僅關係到人們的日常生活方式,同時也關係到中國大陸政治、軍事、經濟、社會、文化等各個領域的安全。雖然網路空間安全已得到中國大陸領導階層的重視，但近年來人工智慧、物聯網、大數據和雲端運算等應用和發展，網路空間安全面臨的壓力也愈大，中國大陸在網路空間安全體系戰略的建構刻不容緩。

為此，中共中央網絡安全和資訊化領導小組成立後，習近平提出，領導小組要發揮集中統一的領導作用，協調各個領域的網路安全和資訊化的問題，制定實施國家網路安全和資訊化發展戰略和政策，以下區分為《國家信息化化發展戰略綱要》、《國家網絡空間安全戰略》和《網絡空間國際合作戰略》等三部分。

首先，中共中央辦公廳和國務院於 2016 年 7 月 27 日公佈《國家資訊化發展戰略綱要》(以下簡稱《戰略綱要》)。要求資訊化驅動現代化加快建設網路強國。實現這一目標分為三階段：第一階段到 2020 年，核心關鍵技

術部分領域達到國際先進水準，資訊化產業國際競爭力大幅提升，資訊化成為驅動現代化建設的引導力量。第二階段，到 2025 年，建設國際領先的移動通訊網路，改變核心關鍵技術受制於人的局面，培養具有國際競爭力的網路資訊企業。第三階段，到本世紀中葉，資訊化全面支撐社會主義現代化國家建設，引領全球資訊化發展。[9]由於，過去中國大陸資訊化應用做得比較好，但技術產業自主能力仍不足，關鍵核心技術受制於美國企業，打造自主研發的技術產業生態體系，需要做好戰略規劃，而這就是本戰略綱要推出的重大意義之一。

其次，中國大陸全國人民代表大會於 2015 年通過《中華人民共和國國家安全法》，首次把網路主權這概念提升到法律高度。2016 年 11 月通過《中華人民共和國網絡安全法》，載明「國家主權延伸到網路空間」，「網路主權成為國家主權的重要組成部分」，「網路主權不容侵犯」強調網路主權的重要性。中國大陸互聯網信息辦公室於 2016 年 12 月 27 日發布《國家網絡空間安全戰略》和 2017 年 3 月 1 日互聯網資訊辦公室與外交部共同發布《網絡空間國際合作戰略》。

前者明確指示「捍衛網路主權，維護國家安全，保護關鍵基礎設施，加強網絡文化建設，打擊網絡恐怖和違法犯罪，完善網絡治理體系，夯實

[9] 中共中央辦公廳、國務院辦公廳，〈《國家信息化發展戰略綱要》〉，《中華人民共和國中央人民政府站》，2016 年 7 月 27 日。〈 http://big5.www.gov.cn/gate/big5/www.gov.cn/gongbao/content/2016/content_5100032.htm 〉。(檢索日期 2020 年 4 月 11 日)。

網絡安全基礎，提升網絡空間防護能力，強化網絡空間國際合作」等九項任務。[10]

中國大陸首次以國家戰略文件的形式，從中國大陸國際和內部等層面分析。國際層面提出推進和平、安全、開放、合作和秩序等五項具體目標。其中，和平與合作是著眼於國際，目的是有效遏止資訊技術的濫用，反對各國於網路空間實施軍備競賽，有效防範網路空間衝突，逕而加強資訊技術交流、打擊網路恐怖組織和犯罪等合作，建立完善國際網路治理體系。

中國大陸內部則側重於安全與開放。安全目標具體在掌握核心技術裝備，穩定網路、資訊系統技術和滿足網路安全人才的需求，提升網路安全意識和基本防護能力。開放顯現在政策和市場開放，使產品流通更為順暢，並消弭開發中國家與已開發國家的在網路資訊科技領域的數位鴻溝，即不分國力強弱和貧富懸殊的國家都能分享科技技術，公平參與網路空間全球治理。[11]

後者，《網絡空間國際合作戰略》。確立中國大陸參與網路空間國際合作的戰略目標，其中維護網路主權是首要目標，顯見中國大陸對於網路空間的重視程度。《網絡空間國際合作戰略》提出 9 項中國大陸推動參與網路空間國際合作的行動計畫：「維護網路空間和平與穩定、構建以規則為基礎

[10] 中國國家互聯網資訊辦公室，〈國家網絡空安全戰略〉，《中國國家互聯網信息辦公室網站》，2018 年 12 月 27 日。〈http://www.cac.gov.cn/2016-12/27/c_1120195878.htm〉。(檢索日期 2019 年 11 月 11 日)。

[11] 朱莉欣、韓曉陽，〈基於機遇和挑戰，謀求發展和安全-比較中解讀《國家網絡空安全戰略》〉，《資訊安全與通信保密》，2017 年 2 月，頁 28-31。

的網路空間秩序、拓展網路空間夥伴關係、推進全球互聯網治理體系改革、打擊網路恐怖主義和網路犯罪、保護公民權益、推動數位經濟發展、加強全球資訊基礎設施建設和保護、促進網路文化交流互鑑。」這九項闡述中國大陸在國際網路空間中享有的權利及義務，同時表明中國大陸在國際網路空間治理的原則與立場。

然而，美國與中國大陸以在國家安全戰略下，將網路空間視為新的戰場，彼此競爭，相互指責。對於網路主權的主張也產生歧見。美國指責中國大陸軍方人員從事駭客行動，自美國企業盜取資訊，據 2017 年 7 月 26 日《BBC NEWS》的報導，中情局局長表示美國最大威脅來自中國大陸而非俄國。[12]另一方面中國大陸也不甘示弱地指責美國對包括中國大陸在內等外國開展監控行動，因此，為維護網路安全與實踐網絡主權，應儘快擺脫美國科技干擾。網路空間戰的你爭我奪，彼此較勁，相互指責。一時之間，美、中間的網路空間爭奪戰，難以化解。然而，網路空間的安全與穩定攸關中國大陸主權的伸張，從安全和發展利益的全球關切視角審視，中國大陸因而適時提出《網絡空間國際合作戰略》，以便建構美國與中國大陸或國際組織間的合作平臺，共同面對網路空間治理的難題。

從中國大陸推出《網絡空間國際合作戰略》，筆者認為中國大陸雖願意持續與國際社會攜手合作，然而更是向各國展現中國大陸對網路主權建設

[12] 蒙克，〈中情局局長：美國最大威脅來自中國而非俄國〉，《BBC 中文網》，2017 年 7 月 26 日。〈https://www.bbc.com/zhongwen/trad/world-40735176〉。(檢索日期 2020 年 1 月 11 日)。

與維護是不容他國介入與干擾的。從中國大陸學者赤東陽〈從《網絡空間國際合作戰略》-看我國維護網路空間主權的思路〉一篇中，舉出三點中國大陸在國際上發展網路主權的對策。其一，匯聚開發中國家的力量。研究有利於開發中國家利益的網路空間規則，先為開發中國家接受，再為國際接受。其二，使網路主權的理論和網路空間規則得到國際上的認可，必須在聯合國主導下，提高中國大陸在網路空間規則制定中的話語權。其三，借鑑北大西洋公約組織編纂《塔林手冊》的經驗，鼓勵中國大陸相關專家積極參與網路空間國際交流，從學術觀點到集結成官方檔案再到國際法律的轉變，並達到國際共識，並最終獲得國際承認。[13]

面對網路空間的新戰場，沒有網路安全就沒有國家安全。各國皆開始從國家戰略高度來審視與解決網路安全問題。從「中共中央網絡安全和信息化領導小組」的成立和《網絡空間安全戰略》和《網絡空間國際合作戰略》的發布，顯見中國大陸以看出網路空間爭奪戰是關係到網路安全與主權的新戰場，中國大陸勢必有所準備，並取得全球網路安全治理的發言權，這不僅對中國大陸提升網路空間話語權，[14]同時也適時向國際社會呈現習近平在 2014 年，中國大陸中央國家安全委員會第一次全體會議中提出「共同安全、綜合安全、合作安全、可持續安全」等總體國家安全觀的新思路。

[13] 赤東陽、劉權，〈從《網絡空間國際合作戰略》-看我國維護網路空間主權的思路〉，《網絡空間安全》，2017 年 2 月，頁 15-16。

[14] 中央網絡安全和資訊化領導小組，〈《網絡空間國際合作戰略》(全文)〉，《新華網》，2017 年 3 月 1 日。〈http://www.xinhuanet.com/politics/2017-03/01/c_1120552767.htm〉。(檢索日期 2019 年 11 月 11 日)。

這也呼應攻勢現實主義的基本假設，網路空間為無政府狀態，潛在大國的中國面對霸權美國本身在網路科技創新的能力，可以鉗制住中國大陸的關鍵性基礎設施，使中國大陸在資訊核心能力受制於人。而中國大陸無法把握網路霸權美國的企圖，從公佈《國家資訊化發展戰略綱要》、《國家網絡空間安全戰略》和《網絡空間國際合作戰略》的舉措可看出中國大陸因對美國掌握網路資訊等關鍵基礎領域而採取自助的手段，而達到生存是大國首要目標。

第三節 中國大陸國內執行與特點

英國衛報於 2013 年 6 月報導以美國國家安全局的情報機構展開代號為「稜鏡」的監聽項目，該項目可准許美國情報機關透過網路公司，可直接對所有用戶的網路即時通訊、電子郵件、照片、音訊、影片、個人資訊和既存資料進行監聽，而監聽對象包含盟國的政治領袖，此次事件是史諾登揭露美國對世界各國的監聽行動。

上海復旦大學學者沈逸分析史諾登事件產生四個影響。首先，國家安全面臨新的挑戰和威脅。其次，政府須設計新的戰略，建構新的能力，塑造新的環境，構成包含國家在內的各類行為體面臨的共同任務。最後，國際體系在此過程中，經歷並完成深刻的變遷。[15]沈逸的觀點指出中國大陸面

[15] 沈逸〈轉型與建構：後斯諾登時代國家網絡安全戰略設計與能力建設〉,《中國共產黨新聞網》, 2014 年 7 月 22 日。〈http://theory.people.com.cn/n/2014/0722/c386965-25317991.html〉。(瀏覽日期：2020 年 2 月 12 日)。

對史諾登事件的反應，並指出習近平在「中共中央網絡安全和資訊化領導小組」第一次會議提出的沒有網路安全就沒有國家安全，代表中國大陸針對史諾登事件後所形成的「網絡空間安全戰略」意識和「總體國家安全觀」的國家安全戰略思維。

史諾登事件被中國大陸認為是敲響網路安全的警鐘，中國大陸網路安全專家泰安指出，成立「中共中央網絡安全和資訊化領導小組」，即時啟動戰略架構的頂層設計。本節對中國大陸網路空間戰略的應對模式分為「立法層面」和「組織層面」，提出深入分析及論述。

壹、立法層面

一、總體國家安全觀

中國大陸於 1993 年制定《國家安全法》，主要指國家主權、領土完整和人民民主專政的國家政權不受威脅和侵犯。在當時國際與國內情勢下，此舉主要任務是防範和打擊境內、外敵對勢力顛覆政府、分裂國土；從事間諜活動；竊取、刺探、收買、非法提供國家秘密等危害國家安全的活動。進入二十一世紀以來，國際情勢發生巨變，維護國家安全的任務和要求也相應產生變化。

非傳統領域安全問題日益突顯，中共中央政治局於 2014 年 1 月 24 日確定設置「中央國家安全委員會」，並明確將其定位為中共中央關於國家安

全工作的決策和議事協調機構，向中央政治局、中央政治局常務委員會負責，統籌協調涉及國家安全的重大事項和工作。[16]國家安全委員會的主要職責是制定和實施國家安安全戰略，推動國家法制建設，制定國家安全工作方針，以及解決國家安全工作中的重大問題。[17]

習近平於 2014 年 4 月 15 日在中央國家安全委員會第一次全體會議上首次正式提出《總體國家安全觀》提到中國大陸基於國內外複雜變化，國家安全面臨諸多挑戰和壓力，認為必須增強憂患意識，做到居安思危；尤其治黨治國，要鞏固統治地位，保障國家安全就是頭號大事。[18]因此，強調設立國家安全委員會的目的是推動國家治理體系和治理現代化、實現國家長治久安的迫切要求，是全面建立小康社會、實現中華民族偉大復興的「中國夢」的重要保障，更能適應國家面臨的新威脅和任務，建立集中統一和高效權威的國家安全體制。

習近平列舉十一項安全：政治、國土、軍事、經濟、文化、社會、科技、資訊、生態、資源、核安等，強調要建構各項安全於一體的國家安全體系。他又提出五大要素和五對關係。五大要素就是以人民安全為宗旨，以政治安全為根本，以經濟安全為基礎，以軍事、文化、社會安全為保障，

[16] 〈中共中央政治局研究決定中共中央安全委員會設置〉,《中華人民共和國中央人民政府網》, 2014 年 1 月 24 日。〈http://www.gov.cn/ldhd/2014-01/24/content_2575011.htm〉。(瀏覽日期：2020 年 2 月 12 日)。

[17] 胡瑞舟,〈中共中央國家安全委員會及其運作：從總體國家安全觀及國家安全工作座談會觀察〉,《展望與探索》第 15 卷第 4 期， 2017 年 4 月，頁 40。

[18] 〈習近平主持召開中央國家安全委員會第一次會議強調:堅持總體國家安全觀,走中國特色國家安全道路〉,《人民網》, 2014 年 4 月 16 日。〈http://politics.people.com.cn/n/2014/0416/c1024-24900227.html〉。(瀏覽日期：2020 年 2 月 12 日)。

以促進國際安全為依託。貫徹落實總體國家安全觀則必須重視五對關係，亦即既重視外部安全，又重視內部安全；既必須既重視外部安全，又重視內部安全；既重視國土安全，又重視國民安全；既重視傳統安全，又重視非傳統安全；既重視發展問題，又重視安全問題；既重視自身安全，又重視共同安全。[19]

習近平總體國家安全觀，以此衡量，1993 年版的《國家安全法》主要規定國家安全機關的權責和反間諜的滲透，所涵蓋範圍已不足以對應現今的國內外情勢。為此，中國大陸全國人大常委在 2014 年 11 審議通過《反間諜法》同時廢除舊國家安全法。於 2015 年 7 月 1 日中國大陸全國人大常委通過「中華人民共和國國安法」並且當即實施。

新版《國家安全法》就維護政治、人民、國土、軍事、經濟、金融、文化、科技、宗教、社會、生態等諸多安全，以及防範、處置恐怖主義、極端主義做出規定。第二十五條規定網路安全：「國家建設網絡與資訊安全保障體系，提升網絡與資訊安全保護能力，加強網絡和資訊技術的創新研究和開發應用，實現網絡和資訊核心技術、關鍵基礎設施和重要領域資訊系統數據的安全可控；加強網絡管理，防範、制止和依法懲治網絡攻擊、

[19]〈習近平主持召開中央國家安全委員會第一次會議強調:堅持總體國家安全觀,走中國特色國家安全道路〉,《人民網》,2014 年 4 月 16 日。〈http://politics.people.com.cn/n/2014/0416/c1024-24900227.html〉。(瀏覽日期：2020 年 2 月 12 日)。

[20]〈中華人民共和國國家安全法〉,《全國人民代表大會網》,1993 年 2 月 22 日。〈http://www.npc.gov.cn/wxzl/gongbao/1993-02/22/content_1481246.htm〉。(瀏覽日期：2020 年 2 月 12 日)。

入侵、竊密、散佈違法有害資訊等犯罪行為，維護國家網絡空間主權、安全和發展利益。」[21]《國家安全法》規定在中國共產黨領導建立集中統一、高效權威的國家安全領導體制並有效面對網路安全威脅。[22]

二、《網路安全法》

中國大陸在接入全球網際網路時制定的第一件行政法規《中華人民共和國計算機資訊系統安全保護條例》也正是維護網路安全的法規。之後各部門相繼發布多個有關網路安全的規章和規範性檔。如下表 3-1「1994-2019 年中國大陸歷年資訊安全的規範性文件。」

表 3-1 1994-2019 年中國大陸歷年資訊安全的規範性文件

時間	檔案名	內容
1994	《中華人民共和國計算機資訊系統安全保護條例》	重點維護國家事務、經濟、國防、科技等重要領域電腦資訊系統的安全。
1997	《計算機資訊網路國際網安全保護管理辦法》	任何單位和個人不得利用全球網際網路危害國家安全，洩漏國家秘密，不得侵犯國家、社會、集體的利益和公民的合法權益，不得從事違法犯罪活動。
2002	《稅務系統網路與資訊安全防範處置預案》	根據資訊的性質和重要程度劃分為四級：A 級高敏感訊息，實行絕對強制保護。B 級敏感訊息，實行強制保護。C 級內部管理訊息，實行自主安全保護。D 級公共資訊，實行一般安全保護。
2004	《關於資訊安全等級保護工作的實施意見》	資訊安全等級保護是指對國家秘密資訊、法人和其他組織及公民的專有資訊、公開資訊和儲存、傳輸、處理這些資訊的訊息系統分等級實行安全保護。

[21] 〈授權發布：中華人民共和國國家安全法〉，《新華網》，2015 年 7 月 1 日。〈http://www.xinhuanet.com/politics/2015-07/01/c_1115787801.htm〉。(瀏覽日期：2020 年 2 月 12 日)。

[22] 〈聚焦新國家安全法五大亮點〉，《新華網》，2015 年 7 月 1 日。〈http://www.xinhuanet.com//politics/2015-07/01/c_1115787097_2.htm〉。(瀏覽日期：2020 年 2 月 12 日)。

2004	《中共中央關於加強黨的執政能力建設決定》	針對傳統安全威脅和非傳統安全威脅的因素相互交織的新情況，確保國家的政治安全、經濟安全、文化安全和資訊安全。
2007	《資訊安全等級保護管理辦法》	第七條 資訊系統的安全保護等及分為五級。 第一級 資訊系統受到破壞後，會對公民、法人和其他組織的合法權益造成損害，但不損害國家安全、社會秩序和公共利益。 第二級 資訊系統受到破壞後，會對公民、法人和其他組織的合法權益造成嚴重損害，或者對社會秩序和公共利益造成損害，但不損害國家安全。 第三級 資訊系統受到破壞後，會對社會秩序和公共利益造成嚴重損害，或對國家安全造成損害。 第四級 資訊系統受到破壞後，會對社會秩序和公共利益造成特別嚴重損害，或對國家安全造成嚴重損害。 第五級 資訊系統受到破壞後，會對國家安全造成特別嚴重損害。
2012	《資訊安全技術公共及商用服務資訊系統個人資訊保護指南》	可為資訊系統所處理與特定自然人相關，能夠單獨或通過與其他資訊結合識別該特定自然人的電腦數據。個人資訊可以分為個人敏感資訊和個人一般資訊。
2012	《全國人大常委會關於加強網絡信息保護的決定》	國家保護網路資訊安全，保障公民、法人和其他組織的合法權益，維護國家安全和社會公益。國家保護能夠識別公民個人身分和涉及公民個人隱私的電子訊息。任何組織和個人不得竊取或以其他非法方式獲取公民個人電子訊息，不得出售或非法向他人提供公民電子訊息。
2015	《中華人民共和國國家安全法》	實現網路和資訊核心技術，關鍵基礎設施和重要領域資訊系統及數據的安全可控制；加強網路管理、防範、制止和依法懲治。
2016	《關於加強國家網絡安全標準化工作的若干意見》	構建網路安全標準體系的方面提出方案。
2017	《中華人民共和國網絡安全法》	網路安全是指通過採取必要措施，防範對網路的攻擊、侵入、干擾、破壞和非法使用以及意外事故，使網路處於穩定可運行的狀態，以及保障網路數據的完整性、保密性、可用性的能力。
2017	《個人資訊和重要數據出境安全評估辦	明確規定網路運營者向境外提供在中國境內營運中收集的個人資訊時需進行安全評

	法》	估，極大地擴大了個人資訊主體的權益，加強出境資料非法利用的限制。
2017	《網絡產品和服務安全審查辦法》	規定關係國家安全的網路和資訊系統採購的重要網路產品和服務，應當經過網路安全審查，審查重點是網路產品與服務的安全性和可控性。
2017	《關鍵資訊基礎設施安全保護條例》	對支援和保障措施、關鍵資訊基礎設施範圍、運營者安全保護、產品和服務安全、監測預警、應急處置和檢測評估等作了具體規定。
2017	《互聯網使用者公眾帳號資訊服務管理規定》	要求網路新聞資訊服務提供者，建立應用安全評估管理制度和保障制度，自行展開安全評估，並請中央或者省級網路資訊辦公室組織展開安全評估。
2017	《互聯網論壇社區服務管理規定》	要求網路論壇服務者提供者落實主體責任，建立健全資訊審核、公共資訊即時巡查、應急處置及個人資訊保護等資訊安全管理制度，不得利用網路論壇發佈、傳播法律法規禁止的資訊。
2017	《互聯網跟帖評論服務管理規定》	要求網站實行用戶實名制，加強直播留言管理，建立跟帖評論審核管理、即時巡查、應急處置等資訊安全管理制度，及時發現和處置違法資訊。
2017	《互聯網群組資訊服務管理規定》	具體規劃群組服務提供者的責任，並提出群組建立者、管理者應當履行群組管理責任
2017	《互聯網使用者公眾帳號資訊服務管理規定》	要求互聯網群組資訊服務提供者應當對違反法律法規和國家有關規定的群組建立者、管理者和使用者，依法依約採取降低信用等級、暫停管理許可權、取消建群資格等管理措施，建立黑名單管理制度。
2017	《國家網絡安全事件應預案》	網路安全事件分為四級：特別重大網路安全事件、重大網路安全事件、較大網路安全事件、一般網路安全事件。
2019	《密碼法》	加強核心密碼、普通密碼的科學規則和使用，加強制度建設，完善管理措施，增強密碼通信服務和網路空間密碼保障能力。

筆者自製。參考來源：蕭君擁、孟達華，〈總體國家安全觀視野中的資訊網絡安全法治研究〉，《網絡空間安全》，第 10 卷第 5 期，2019 年 5 月，頁 9。魏永征，〈從《中華人民共和國國家安全法》到《中華人民共和國網絡安全法》-學習習近平總體國家安全觀〉，《社會治理》，2018 年第 1 期，頁 30-33。中華人民共和國國家互聯網資訊辦公室〈http://www.cac.gov.cn/index.htm〉。

《網絡安全法》總共有 7 章，79 個條文，幾乎將網路空間管理所面臨的問題都加以防範，根據新華社報導以下 6 大特點：1.明確網路空間主權的原則；2.明確網路產品和服務提供者的安全義務；3.明確網路運營者的安全義務;4.完善個人資訊保護規則;5.建立了關鍵資訊基礎設施安全保護制度；6.確立關鍵資訊基礎設施重要數據跨境傳輸的規則。[23]

此部法律涉及各個法律部門、深入社會各個領域的龐大法律系統，他不只自身運行，還與習近平提出的《總體國家安全觀》特別是政治、文化、社會、科技、軍事等安全存在著密切關連。網路傳播具有無界、瞬息等特點，在資訊時代，網路安全對國家安全可謂牽一髮動全身，成為國家安全不可缺少的組成分，「沒有網絡安全就沒有國家安全」，便是習近平的重要論述。《網絡安全法》主要內容整理如下。

(一)以網路主權為主旨

維護網路空間的國家主權是習近平的一貫主張。網路空間已成為與陸、海、空、太空等重要第五疆域。網路空間主權成為國家主權的重要組成部分，包含於國家對於領土屬地範圍內網路設施、網路活動和資訊的管轄權，對於本國網路政策、法律的制定權，對於本國公民、法人網上合法權益的保障，對於他國的網路入侵的自衛權益的自衛權。

[23] 專家解讀《網絡安全法》，具有六大突出亮點〉，《中國江蘇網》，2016 年 11 月 8 日。〈http://news.jschina.com.cn/zt2017/docs/201709/t20170911_1029164.shtml〉。(瀏覽日期：2020 年 2 月 18 日)。

《網絡安全法》規定政府採取措施，監測、防禦、處置來自境內、外的網路安全和風險，並依法追究和制裁境外機構、組織、個人的攻擊、侵入、干擾、破壞等網路犯罪活動，且立法這項舉措也是行使國家主權的一個象徵。這突顯中國大陸對網路主權的堅持相對於美國提出網路空間類似於公海「全球公域」的概念，提出挑戰。

(二)資訊安全一般規定

依據中國大陸《網絡安全法》第七十六條定義，網路安全是指通過採取必要措施，防範對網路的攻擊、侵入、干擾、破壞和非法使用以及意外事故，使網路處於穩定可靠運行的狀態，以及保障網路數據的完整性、保密性、可用性。習近平強調：「加快建構關鍵資訊基礎設施安全保障體系」指出這些一旦出問題，會具有強大破壞性和殺傷力。網路和資訊安全保障體系可分為四個方面。[24]

首先，設施安全。《網絡安全法》第 76 條將網路定義為：「由計算機或者其他資訊終端及相關設備組成的按照一定的規則和程式對資訊進行收集、存儲、傳輸、交換、處理的系統。《網絡安全法》第 21-23 條不僅對網路產品、服務規定應符合中國大陸所訂立標準規定，並強制性要求並持續提供安全維護而且特別規定網路關鍵基礎設施和網路安全專用產品應該按照中

[24] 《中華人民共和國網絡安全法》〉，《全國人民代表大會網》，2015 年 6 月。〈 https://web.archive.org/web/20161029174914/http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm〉。(瀏覽日期：2020 年 2 月 18 日)。

國大陸國家標準通過安全認證和安全檢測。第 35 條明定關鍵基礎設施營運者採購可能影響國家安全的網路產品和服務應當通過國家安全審查。

其次，數據安全。《網絡安全法》規定的資訊安全，在學理上可以分為數據安全和內容安全。數據即網路數據，是指通過網路收集、存儲、傳輸、交換、處理的以電子方式記錄的各訊息。數據安全是指保障網路數據的完整性、保密性和可用性，不受破壞、竊取和損害。第 40-45 條規定網路運行安全的規中包含保障數據安全的內容，並對保護網路用戶資訊和個人訊息訂立多項措施。把個人資訊安全列入網路安全範疇，突顯出中國大陸對個人訊息任意洩漏、傳播甚至用來牟利，不僅損害當事人，而且會影響社會穩定，更可能危及國基安全。這反映中國大陸保護個人訊息與西方在意識形態上的不同理念。[25]

最後，內容安全。是指在網路空間公開傳輸的文字、聲音、圖像等各種型態的訊息不得對國家、社會和他人產生損害效果。《網絡安全法》第 16 條規定通過傳播社會主義核心價值觀。第 12-13 條規定網路傳播內容的底線，有利於未成年身心健康的原則。第 46 條規定不得利用網路從事違法犯罪活動或傳播涉及違法犯罪活動的訊息。第 27 條用戶必須實施實名制以保證網路訊息具可追溯性。

[25] 〈中華人民共和國網絡安全法〉，《全國人民代表大會網》，2015 年 6 月。〈https://web.archive.org/web/20161029174914/http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm〉。(瀏覽日期：2020 年 2 月 18 日)。

(三)建立以政府主導，各方參與的網路安全責任制

習近平指出：「維護網絡安全是全社會的共同責任，需要政府、企業、社會組織、網民共同參與，共築網絡安全防線。」和「企業要承擔企業的責任，黨和政府要承擔黨和政府的責任，哪一邊都不能棄自己的責任。網上資訊管理，網站應負主體責任，政府行政管理部門要加強監管。」落實安全責任方面顯現「政府」、「網路營運商」、「公民和法人」維護網路安全職責。

首先，政府維護網路安全職責。《網絡安全法》第 50 條規定國家網信部門、國務院電信部門和公安部門以及有關維護網路安全職責的部門，各級政府應當採取支持與促進網路安全的措施，網信等部門有要求網路營運者對違法有害訊息採取措施、通知有關機構來在境外有害資訊採取阻斷措施等職責。第 51-53 條規定建立網路安全監測預警和訊息通報的職責。第 54-56 條規定在網路安全事件風險增大或發生省級以上，政府有關部門應採取相應對措施的職責。[26]

其次，網路營運商維護網路安全的責任和義務。網路營運者不僅負有遵守安全等級制度，採取技術措施保障安全運行，使用合格的網路設備、產品和定期進行風險檢測等義務；而第 24 條規定網路用戶須落實用戶實名

[26]《中華人民共和國網絡安全法》〉，《全國人民代表大會網》，2015 年 6 月。〈 https://web.archive.org/web/20161029174914/http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm〉。(瀏覽日期：2020 年 2 月 18 日)。

制。第 40 條規定網路營運商承擔對用戶資訊保密的義務。第 47 條特別規定網路營運商還負有管理用戶發布的資訊的責任，發現法律禁止發布的訊息，應當立即停止傳輸、保存紀錄，並向有關部門報告。第 28 條明定網路營運者應當為公安、國安部門提供技術支援和協助。網路營運者拒絕履行管理義務，要承擔行政責任以至刑事責任。

最後，公民、法人使用網路之權利。第 12 條規定任何人使用網路應當遵守法律、秩序和道德，不得發布法律禁止的訊息；第 14 條任何人有權舉報危害網路安全行為；第 27 條任何人不得從事危害網路安全的活動；用戶需實行實名制以保證網絡訊息具備可追溯性。綜上所述，《網絡安全法》以上內容可以認為是《國家安全法》第 25 條的具體化。

三、網路安全相關性規範文件

《網絡安全法》確立法律原則，也授與行政機關執行法律、制定實行細則的權力。《網絡安全法》實行後，相關網路資訊部門密集公佈出一系列規章和規範性文件。以下分段敘述。

首先，針對網路設施安全。2016 年 8 月，中國大陸國家互聯網信息辦公室發布《關於加強國家網絡安全標準化工作的若干意見》，構建網路安全標準體系的方面提出方案。[27]2017 年 5 月，中國大陸國家互聯網信息辦公室

[27] 新華社〈《關於加強國家網絡安全標準化工作的若干意見》〉，《中共網路資訊辦公室網》，2016 年 8 月 24 日。〈http://www.cac.gov.cn/2016-08/24/c_1119448735.htm〉。(瀏覽日期：2020 年 2 月 18 日)。

《網絡產品和服務安全審查辦法》規定關係國家安全的網路和資訊系統採購的重要網路產品和服務，應當經過網路安全審查，審查重點是網路產品與服務的安全性和可控性；[28]2017 年 7 月，中國大陸國家互聯網信息辦公室《關鍵資訊基礎設施安全保護條例》，對支援和保障措施、關鍵資訊基礎設施範圍、運營者安全保護、產品和服務安全、監測預警、應急處置和檢測評估等作了具體規定；[29]2017 年 10 月，中國大陸國家互聯網信息辦公室發佈《互聯網新聞資訊服務新技術新應用安全評估管理規定》，要求網路新聞資訊服務提供者，建立應用安全評估管理制度和保障管理制度，自行展開安全評估，並請中央或省（市）級網路資訊辦公室組織展開安全評估。[30]

其次，網路數據安全。2017 年 4 月中國大陸國家互聯網信息辦公室發佈《個人資訊和重要數據出境安全評估辦法》，就《網路安全法》第 38 條規定網路運營者在境內運營中收集和產生的個人資訊和重要資料應當在境內存儲，因業務需要向境外提供的，應當進行安全評估，制定具體辦法。[31]

最後，網路內容安全。早在《網路安全法》通過之前，2016 年 8 月，中國大陸國家互聯網信息辦公室為貫徹習近平關於「網上資訊管理，網站

[28] 中國網信網〈《網絡產品和服務安全審查辦法》〉，《中共網路資訊辦公室網》，2017 年 5 月 2 日。〈http://www.cac.gov.cn/2017-05/02/c_1120904567.htm〉。(瀏覽日期：2020 年 2 月 18 日)。

[29] 中國網信網〈《關鍵資訊基礎設施安全保護條例》〉，《中共網路資訊辦公室網》，2017 年 7 月 11 日。〈http://www.cac.gov.cn/2017-07/11/c_1121294220.htm〉。(瀏覽日期：2020 年 2 月 18 日)。

[30] 中國網信網〈《互聯網新聞資訊服務新技術新應用安全評估管理規定》〉，《中共網路資訊辦公室網》，2017 年 10 月 30 日。〈http://www.cac.gov.cn/2017-10/30/c_1121878049.htm〉。(瀏覽日期：2020 年 2 月 18 日)。

[31] 中國網信網〈《個人資訊和重要數據出境安全評估辦法》體現以人為本的數據治理理念〉，《中共網路資訊辦公室網》，2019 年 6 月 18 日。〈http://www.cac.gov.cn/2019-06/18/c_1124644976.htm〉。(瀏覽日期：2020 年 2 月 18 日)。

應負主體責任」的指示，對 8 家從事網路新聞資訊服務的商業網站進行專項檢查，發現存在「資訊內容安全性漏洞」等問題，對新聞資訊服務網站提出完善總編輯負責制等 8 項要求。同時，對社交媒體的監管明顯強化。2017 年 8 月，中國大陸國家互聯網信息辦公室發佈《互聯網論壇社區服務管理規定》，要求網路論壇服務者提供者落實主體責任，建立健全資訊審核、公共資訊即時巡查、應急處置及個人資訊保護等資訊安全管理制度，不得利用網路論壇發佈、傳播法律法規禁止的資訊。[32]

同時還有《互聯網跟帖評論服務管理規定》，要求網站實行用戶實名制，加強直播留言管理，建立跟帖評論審核管理、即時巡查、應急處置等資訊安全管理制度，及時發現和處置違法資訊。[33]2017 年 9 月，中國大陸國家互聯網信息辦公室發佈《互聯網使用者公眾帳號資訊服務管理規定》，要求互聯網群組資訊服務提供者應當對違反法律法規和國家有關規定的群組建立者、管理者和使用者，依法依約採取降低信用等級、暫停管理許可權、取消建群資格等管理措施，建立黑名單管理制度。[34]同月公佈的《互聯網群組

[32] 中國網信網〈《互聯網論壇社區服務管理規定》〉，《中共網路資訊辦公室網》，2017 年 8 月 25 日。〈https://www.cac.gov.cn/2017-08/25/c_1121541921.htm〉。(瀏覽日期：2020 年 2 月 18 日)。

[33] 中國網信網〈《互聯網跟帖評論服務管理規定》〉，《中共網路資訊辦公室網》，2017 年 8 月 25 日。〈https://www.cac.gov.cn/2017-08/25/c_1121541842.htm〉。(瀏覽日期：2020 年 2 月 18 日)。

[34] 中國網信網〈《互聯網使用者公眾帳號資訊服務管理規定》〉，《中共網路資訊辦公室網》，2017 年 9 月 7 日。〈http://www.cac.gov.cn/2017-09/07/c_1121624233.htm〉。(瀏覽日期：2020 年 2 月 18 日)。

資訊服務管理規定》,具體規劃群組服務提供者的責任,並提出群組建立者、管理者應當履行群組管理責任。[35]

截至 2019 年中國大陸網路用戶數已經高達世界第一,已成為網路大國,也是面臨網路安全威脅最嚴重國家之一。因此,對與保護網路空間的合法權益,通過《網路安全法》溯源追蹤,突顯習近平《總體國家安全觀》經過制定並實施《國家安全法》和《網路安全法》,建構出網路空間的安全秩序,而《網路安全法》充分體現網路安全立法的核心理念,符合中國大陸當前網路安全工作的實際和需要。

貳、組織層面

一、黨部組織與政府部門變革

中國大陸政府於 2013 年以來加大網路安全和資訊化發展的力度,中共成立領導小組背後成因與歷年來中國大陸國家資訊化領導小組的發布政策,從鄧小平改革開放以來,開始擘劃資訊化管理體制。1982 年 10 月,中國大陸國務院成立「計算機與大規模集成電路領導小組」迄 2008 年成立工業和資訊化部經歷多次組織變革,由於「工業和信息化部」屬於國務院體系及位階的問題,在推動資訊化工作,受到地方本位主義的排斥,造成資訊化停滯不前。曾任中國大陸互聯網資訊辦公室副主任王秀軍表示,中國大陸網路管理層是「九龍治水」存在多頭管理、職能交叉、權責不分、效率不

[35] 中國網信網〈《互聯網群組資訊服務管理規定》〉,《中共網路資訊辦公室網》,2017 年 9 月 7 日。〈https://www.cac.gov.cn/2017-09/07/c_1121623889.htm〉。(瀏覽日期:2020 年 2 月 18 日)。

彰等弊端，已到非解決不可的地步。[36]從下表 3-2「中共中央網路安全和資訊化領導小組歷史沿革」分析如下。

表 3-2 中共中央網路安全和資訊化領導小組歷史沿革

時間	組織名稱	內容
1982 年	計算機與大規模集成電路領導小組	確立中共發展大中型電腦與小型電到腦系列的依據
1986 年	國家經濟資訊管理小組	為統一領導中共國家經濟資訊系統建設，加強經濟資訊管理
1993 年	國家經濟信息化聯席會議	統一領導和組織協調政府經濟領域資訊化建設工作。
1996 年	成立國務院資訊化工作領導小組	統領中國大陸地區資訊化任務，由時任國務副總理鄧家華擔任組長。
1999 年	國家信息化推進辦公室	國務院資訊化工作領導小組不單設辦事機構，具體工作由資訊產業部承擔，並將國家信息化辦公室改名為國家資訊化推進工作辦公室。
2001 年	國家信息化領導小組	負責審議國家信息化發展戰略，宏觀規劃、擬定草案、規章和重大決議，協調資訊化和資訊安全工作。
2003 年	在國家資訊化領導小組下成立國家網絡與資訊安全協調小組	中共中央政治局常委、國務院總理溫家寶任組長。
2008 年	組織變革將國務院資訊化工作辦公室裁撤，將職責合併新組建的工業和信息化部	根據《國務院關於機構設置的通知》，統一納入新成立的「中華人民共和國工業和資訊化部」。
2014 年	中共中央網絡安全和資訊化領導小組	根據 2013 年 11 月中共十八屆三中全會通過的《中共中央關於全面深化改革若干重大問題的決定》成立。
2018 年	改名為中央網絡安全和	根據《深化黨和國家機構改革方案》

[36] 人民網〈汪玉凱：中央網絡安全與資訊化領導小組的由來及其影響〉，《中國共產黨新聞網》，2014 年 3 月 3 日。〈http://theory.people.com.cn/BIG5/n/2014/0303/c40531-24510897.html〉。(瀏覽日期：2020 年 2 月 18 日)。

	資訊化委員會	改名。

筆者自製。參考來源：〈中共中央網路安全和資訊化領導小組歷史沿革〉，《保密科學技術》，2014 年 2 月，頁 5。

中國大陸於 2013 年 8 月 8 日《國務院關於促進資訊消費擴大內需的若干意見》強調，加強資訊基礎設施建設，加快資訊產業升級，大力豐富消費內容，提高網路安全保障能力。2013 年 11 月中共十八屆三中全會通過的《中共中央關於全面深化改革若干重大問題的決定》提出，要堅持積極利用、科學發展、依法管理、確保安全的方針，加大依法管理網路力度，完善網際網路管理領導體制。

「中共中央網絡安全和資訊化領導小組」於 2014 年 2 月 27 日宣告成立，在北京召開第一次會議，會議審議通過《中央網絡安全和資訊化領導小組工作規則》、《中央網絡安全和資訊化領導小組辦公室工作細則》、《中央網絡安全和資訊化領導小組 2014 年重點工作》，與之前國務院層級上的國家資訊化領導小組相比，中共中央層級上設置的中央網絡安全與資訊化領導小組改變過去由國務院總理任國家信息化領導小組組長時難以協調中共中央、中央軍委、全國人大等的弊端，提高整體規劃能力和高層協調能力，並且將網路安全放在更首要位置。[37]

[37] 〈中國互聯網二十年：1994-2014 年〉，《中央網絡安全和資訊化辦公室網》，2014 年 11 月 16 日。〈http://www.cac.gov.cn/2014-11/16/c_1113265290.htm〉。(瀏覽日期：2020 年 2 月 12 日)。

中共中央於 2018 年 3 月印發的《深化黨和國家機構改革方案》稱，「中央網絡安全和資訊化領導小組改為委員會。為加強黨中央對涉及黨和國家事業全域的重大工作的集中統一領導，強化決策和統籌協調職責。

中央網路安全和資訊化委員會負責相關領域重大工作「頂層設計、總體佈局、統籌協調、整體推進、督促落實。」[38]資訊化建設涉及黨、政、軍和社會各領域，在資訊化領導小組底下，迫切需要建立一個國家層面的管理機構，落實資訊化領導小組制定的戰略和政策並統籌協調堆進中國大陸地區資訊化發展工作，這個管理機構須具備權威性和戰略性，2014 年 2 月 27 日成立的「中央網絡安全與資訊化領導小組」沿襲 90 年代設立的國家資訊化領導小組的格局，可以歸納以下幾點特性。

首先，新組建的「中央網絡安全與信息化領導小組」是由中國共產黨黨中央層級上設置的議事協調機構又屬於國務院的機構，為「兩塊招牌一套人馬」。習近平在第一次中央網路安全與資訊化領導小組會議中提到「中央網絡安全和資訊化領導小組要發揮集中統一的領導作用，統籌協調各個領域的網絡安全和資訊化重大問題。制定實施國家網絡安全和資訊化發展戰略、宏觀規劃和重大政策。」出任組長的已不是過去國務院總理，而是由中國共產黨黨書記和國家最高領導人擔任，從根本解決由國務院總理擔

[38] 〈中共中央印發《深化黨和國家機構改革方案》〉，《新華網網》，2018 年 3 月 21 日。〈http://www.xinhuanet.com/2018-03/21/c_1122570517.htm〉。(瀏覽日期：2020 年 2 月 12 日)。

任國家信息化領導小組組長難以協調、黨中央、軍委、人民大會等橫向協調的問題，提高該小組整體規劃能力與協調能力。[39]

其次，網路安全議題備受關注。安全與發展一直處於矛盾與爭論不休的問題。過往領導小組將安全放在資訊裡面，但新組建的領導小組強調「網絡安全」，從名稱上不僅將網路安全與資訊化並列，且將網路安全放在前面，這說明網路安全在現階段的重要性。習近平在第一次會議說明「網路安全和資訊化是一體之兩翼、驅動雙輪，必須統一謀劃、統一部署、統一推進、統一實施。」也強調「沒有網絡安全就沒有國家安全，沒有資訊化就沒有現代化。」首重網路輿論力量，改進網上宣傳，杜絕錯誤、有害訊息甚至危害國家安全之訊息。

最後，重視資訊化戰略和建設。中國大陸資訊化管理體制和管理機構歷年來發生多次變化，為因應資訊技術不斷進步，經濟社會和國際環境劇烈變化，顯現在戰略思想、資訊化管理體制和管理機構的變化。從戰略層面來看應對資訊技術革新到大力推展胡錦濤時期的「國民經濟和社會信息化」[40]到「資訊化覆蓋現代化建設全域的戰略舉措」[41]再到「信息化帶動工

[39] 〈中央網絡安全和資訊化領導小組第一次會議召開〉，《中華人民共和國中央人民政府網站》，2014 年 2 月 27 日。〈http://www.gov.cn/ldhd/2014-02/27/content_2625036.htm〉。(瀏覽日期：2020 年 2 月 12 日)。

[40] 〈發展改革委有關負責人就《國民經濟和社會發展資訊化"十一五"規劃》答記者問〉，《中華人民共和國中央人民政府網站》，2008 年 4 月 17 日。〈http://big5.www.gov.cn/gate/big5/www.gov.cn/zwhd/2008-04/17/content_947090.htm〉。(瀏覽日期：2020 年 2 月 12 日)。

[41] 人民日報〈資訊化覆蓋現代化建設全域的戰略舉措〉，《國脈電子政務網》，2007 年 12 月 26 日。〈http://www.echinagov.com/info/316〉。(瀏覽日期：2020 年 2 月 12 日)。

業化」[42]、「兩化融合」[43]，習近平則提到「沒有資訊化就沒有現代化」。相對地，管理機構也歷經電子振興領導小組、國家經濟資訊化聯席會議到國家資訊化工作領導小組的變化，其辦事機構以及所屬部門及規劃層級均有調整，也說明中國大陸領導人對資訊化的重視程度。

二、共軍組織變革

資訊技術的發展和進步改變未來的戰爭型態及作戰樣式。網路空間作為一個全新的作戰領域，伴隨著網路空間的形成，國家主權向網路延伸，被譽為繼土地、海洋、天空、太空之外第五領域的戰爭空間，爭奪網路空間控制權，如同爭奪陸、海、空、天領域，關乎著國家主權與安全。制網權是指一個主權國家對電腦資訊世界的控制權和主導權。隨著電腦網路網路滲入金融、商業、交通、資訊、軍事等各領域，網路安全也直接關乎國家安全，從 1991 年波灣戰爭、1999 年科索沃戰爭、2001 年阿富汗戰爭、2003 年伊拉克戰爭的相關經驗，網路技術已成為現代化軍隊 C^4ISR 系統的基礎[44]，使共軍認知到未來軍事衝突不僅侷限在陸、海、空等傳統領域，也

[42] 信息化帶動工業化，以工業化促進信息化〉，《中國經濟網》，2009 年 8 月 13 日。〈http://www.ce.cn/cysc/ztpd/09/ind/informatization/200908/13/t20090813_19579290.shtml〉。(瀏覽日期：2020 年 2 月 12 日)。

[43] 兩化融合是指電子資訊技術廣泛應用到工業生產的各個環節，資訊化成為工業企業經營管理的常規手段。資訊化進程和工業化進程不再相互獨立進行，不再是單方的帶動和促進關係，而是兩者在技術、產品、管理等各個層面相互交融，彼此不可分割，並催生工業電子、工業軟體、工業資訊服務業等新產業。參考來源：網路與資料管理部〈兩化融合管理體系評估〉，《中國電子技術標準化研究院網》，2017 年 4 月 7 日。〈http://www.cesi.cn/lhrh/201704/2305.html〉。(瀏覽日期：2020 年 2 月 12 日)。

[44] C^4ISR 是指由英語的指揮、管制、通信、資訊、情報、監視和偵查七個詞（Command、Control、Communications、Computers、Intelligence、Surveillance、Reconnaissance）的首字母縮寫而來，取中文首字譯作指、管、通、資、情、監、偵。

可能發生在網路空間或電磁空間等新型領域，並發展出資訊作戰的相關軍事理論。[45]

習近平於 2015 年 12 月 31 日在北京八一大樓舉行戰略支援部隊成立大會，並將軍旗授予該部隊司令員高津和政治委員劉福連，宣告戰略支援部隊正式成立。[46]然而，共軍原有的資訊作戰力量分散在四大總部，沒有統一的領導機制，難以在聯合作戰中發揮體系作戰的力量。因此習近平推動軍改後，創立戰略支援部隊網路系統部，統一領導共軍的資訊作戰能力，其中整合技術偵查和電子對抗的作戰單位，未來將肩負網路和電磁空間的作戰任務。[47]

(一)網路系統部的組織

網路系統部的單位組成來自軍改前的總參謀部第三部（技術偵查部）、總參四部（電子對抗與雷達部）下的作戰單位，相較於航太系統部，網路系統部的組成來自情報單位，因此公開資訊更加隱晦。目前顯示總參三部下轄 12 個局已全數移入網路系統部內，而總參四部在軍改後成為聯合參謀

[45] 中華人民共和國國務院新聞辦公室，〈2008 年中國的國防〉，《中華人民共和國國防部》，2009 年 1 月 16 日。〈http://www.mod.gov.cn/big5/regulatory/2011-01/06/content_4617809.htm〉。（瀏覽日期 2020 年 2 月 6 日）

[46] 台灣稱解放軍為共軍。為了行文和閱讀的嚴整性，除非文章必要維持之外，均以共軍一詞表示。來源：李宣良等人，〈習近平向中國人民解放軍陸軍火箭軍戰略支援部隊授予軍旗並致訓詞〉，《人民日報》，2016 年 1 月 2 日，版 1。

[47] John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era* (Washington: National Defense University Press, 2018), p. 23.

部的網路電子局，僅將電子作戰部隊移入網路系統部內。[48]關於網路系統部的單位組成，以下條列相關資訊：

1. 來自總參三部

(1) 第一局(61786)部隊,駐地與網路系統部總部共同駐於北京海澱區，主要任務包括網路解密、加密等資訊安全任務。

(2) 第二局(61398)部隊，駐地設於上海浦東新區，主要以美國和加拿大為攻擊目標，重點置於政治、經濟和軍事情報偵蒐。[49]

(3) 第三局(61785)部隊，該局總部設在大興區南部的北京郊區，已知至少有 13 個處；各辦事處設在哈爾濱、大連、北京、杭州等地。其所賦任務以無線電訊號偵蒐為主。[50]

(4) 第四局(61419)部隊，該局總部設在青島，負責對日本和韓國的情蒐工作。

(5) 第五局(61565)部隊，該局總部設在北京市大興區黃村新村，負責俄羅斯情蒐工作。

(6) 第六局(61726)部隊，該局總部原集中在湖北省荊門市一帶，主要負責台灣及東南亞情蒐工作。[51]

---

[48] John Costello and Joe McReynolds, China’s Strategic Support Force: A Force for a New Era, pp. 25-26.斜體

[49] Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure* (Virginia: Project 2049 Institute, 2011), p. 8.

[50] 翁衍慶,《中共情報組織與間諜活動》(臺北：新銳文創，2018 年 9 月)，頁 179。

[51] Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure, p. 8. 第一字空格?(註 49 有空一格，全文一併調整)、書名斜體

(7) 第七局(61580)部隊，該局目前資料極少，僅可從過去資料看出是負責共軍網路攻防演練之部隊(網 路藍軍)，並兼負類似白帽駭客，從事內部滲透測試工作。

(8) 第八局(61046)部隊，位於北京韓家川，負責對歐洲、中東、非洲和南美洲的情蒐工作。

(9) 第九局，位於北京，可能擔負總參三部主要的戰略情報分析以及管理數據庫。

(10) 第十局(61886)部隊，該局位於北京地區，主要負責對中亞和俄羅斯方面偵蒐任務。

(11) 第十一局(61672)部隊，位於北京地區，負責對俄羅斯的情蒐工作，任務有別於第五局，更重於情報分析層面。

(12) 第十二局(61486)部隊，駐地設於上海浦東新區，以美國和加拿大為攻擊目標，置重點於政治、經濟和軍事情報偵蒐。[52]

2. 來自總參四部的部隊

網路作戰單位，位於北京市區海澱區，依據美國華盛頓時報（Washington Times）於 2017 年 1 月 4 日報導，內容引用美國陸軍亞洲研究小組的情報資料，表示位於北京市區海澱區的金唐酒店與全季酒店可能用於掩護總參

[52] 宋兆理、劉濯銨，〈中共戰略支援部隊-網路系統部序列介紹〉，《陸軍通資半年刊》第 131 期，2019 年 4 月，頁 25-28。

四部的網路作戰單位。[53]雖然目前關於其部隊代號、成員組成、任務方向仍不明朗，但確定總參四部底下的網路作戰部隊已移入戰略支援部隊的網路系統部，可做為整合共軍分散的網路作戰力量。

(二)網路系統部的任務

共軍於 1999 年 11 月 10 日首次在《解放軍報》中提出隨著網路空間的發展，網軍將成為陸軍、海軍、空軍之後的新軍種，肩負捍衛網路主權，進行網路作戰之任務。[54]而共軍在發展網路作戰能力時，也仿效美軍模式，將網路作戰區分為「攻擊」、「防禦」及「安全維護」部門。[55]除發展網路作戰，也同時發展電子作戰，由 2004 年軍科院出版的《21 世紀綜合電子戰系統中》詳細描述共軍電子戰的編成模式，也開始討論整合戰區內的電子偵查、雷達對抗、通信對抗、敵我識別、導航對抗以及光電對抗等各電戰系統，成為整合的電子作戰系統。[56]而隨著「共軍軍事概念革新」，網路作戰與電子作戰也受到聯合作戰的影響，發展出網電一體戰概念。

曾擔任共軍總參四部部長戴清明少將於 2009 年時在《求道無形之境》一書中首先定義網電一體戰：「在資訊戰場上，將電子與網路戰兩種手段綜合運用，為破壞敵方戰場資訊化系統，並保證我方戰場資訊系統正常運行，

[53] Bill Gertz, "PLA's Hacking Hotel," *The Washington Times*, January 4, 2017.At〈https://www.washingtontimes.com/news/2017/jan/4/inside-the-ring-plas-hacking-hotel/〉。(瀏覽日期 2020 年 2 月 15 日)

[54] 冷冰淩等人，〈網路戰：納入軍事體系〉，《解放軍報》，1999 年 11 月 10 日，版 7。

[55] 敖志剛編著，《網路空間作戰：機理與籌劃》(北京：電子工業出版社，2018 年 9 月)，頁 62-64。

[56] 朱和平編著，《21 世紀綜合電子戰系統》(北京：軍事科學出版社，2004 年 9 月)，頁 1-3。

而採取一體化攻擊行動。」[57]軍科院 2013 年出版的《資訊作戰教程》已將網電一體戰納入共軍的資訊作戰軍事教材中。[58]而原總參謀部的資訊作戰力量即是由總參三部及總參四部組成，並在軍改後移入網路系統部，其任務內容可做為我們判斷網路系統部任務的參考。另外對照中國大陸國防大學 2017 年出版的《戰略學》，將共軍網路作戰需求區分為四點，可做為我們對照網路系統部作戰能力的指標，分別是：

1. 網路偵察能力。利用網路、電磁特性和資訊儲存特性，對敵電腦資訊系統實施偵查，以獲取情報資訊、偵查手段，區分為網路竊密、電磁竊密和介質竊密等三種方式。
2. 網路攻擊能力。透過資訊干擾、資訊破壞、資訊摧毀等方式，滲透敵方網路系統內部，對敵留在網路、主機等資訊，實施擾亂、破壞以及摧毀等作戰行動。
3. 網路防護能力。主要是抵禦網路偵察核攻擊，透過提高自身網路設備和主機系統的防護能力，阻止敵方使用非法途徑訪問、侵入與破壞網路設施，並防止我方網路癱瘓，以確保資訊系統安全。
4. 網路運行維護。使網路空間、通訊網路、電腦系統和相關處理器穩定運行，並在硬體、軟體、數據機、路由器遭到敵方破壞，能立即

[57] 戴清民，《求道無形之境》（北京：中國人民解放軍出版社，2009 年 1 月），頁 170。
[58] 葉征，《資訊作戰學教程》（北京：軍事科學出版社，2013 年 1 月），頁 27-29。

使用數據備份進行恢復。[59]

除上述網路作戰能力的四點需求，網路系統部的任務也可以對照軍改後納入戰略支援部隊的軍事院校，透過軍事院校的專業領域，判斷網路系統部未來作戰能力與方展方向。過去總參三部底下設有解放軍外國語學院和解放軍資訊工程大學等兩所院校，[60][61]但 2017 年因應國防和軍隊的深化改革，解放軍外國語學院併入解放軍工程大學內，而整個解放軍資訊工程大學也在軍改後，納入戰略支援部隊管理。[62]目前資訊工程大學共有七十八個本科專業而網路系統部主要任務是蒐集各國的重要情報，除需要情蒐專長外，更需要相應的語言專長人員去分析所獲取的情報，解放軍外國語學院整併至資訊工程大學之下，更能培養語言、情蒐、資訊、通訊、密碼、網路、遙感科學、資訊對抗技術等人才，讓未來進入網路系統部人才具有更佳的作戰能力。

(三)網路系統部對網路作戰的影響

[59] 肖天亮主編，《戰略學》（北京：國防大學出版社，2017 年 5 月），頁 403-405。

[60] 解放軍外國語學院，設有 47 個專業科系，包括英語、俄語、日語、德語、法語、西班牙語、阿拉伯語等 33 個語種的外語專業以及資訊研究與安全、國際關係與安全等非外語專業。另外還負責預備出國人員外語培訓、幹部軍事外語培訓、中級指揮幹部培訓、參謀業務培訓和外軍留學生中文培訓等任務。資料來源：〈2015 年解放軍外國語學院招生簡章〉，《中國教育網》。〈https://gkcx.eol.cn/school/2624/provinceline〉。（瀏覽日期 2020 年 2 月 15 日）。

[61] 解放軍資訊工程大學，設有八大專業領域，區分資訊系統工程學院、地理空間資訊學院、密碼工程學院、網路空間安全學院、導航與空天目標工程學院、理學院、指揮軍官基礎教育學院、資訊技術研究所。主要任務是培養資訊領域高端人才，是目前解放軍唯一的國家網路安全人才培養學校。資料來源：〈2015 年解放軍資訊工程大學招生簡章〉，《中國教育網》。〈https://gkcx.eol.cn/school/2624/provinceline〉。（瀏覽日期 2020 年 2 月 15 日）。

[62] 〈資訊工程大學簡介〉，《中國人民解放軍戰略支援部隊資訊工程大學招生資訊網》。〈https://souky.eol.cn/HomePage/index_134.html〉。（瀏覽日期 2020 年 2 月 15 日）。

網路系統部的作戰行動，可以參照 2013 年軍科院出版的《資訊作戰教學教程》，分別論述網路作戰和電子作戰等相關技術，首先談到網路作戰是利用軍用或民用網路來擷取、使用、竄改、破壞敵方的訊息，或是利用假冒訊息、來破壞敵方資訊系統，保護我方資訊系統正常運作的作戰行動，而網路作戰又區分以下幾種手段：[63]

1. 網路對抗偵查。利用網路工具來收集、判斷目標系統網路結構、資訊流的特徵，直接從敵方網路獲取情報技術。
2. 網路攻擊。利用網路通訊協議的安全性漏洞、用戶操作系統的不當配置或程式語言的內在缺陷，使得進入用戶主機系統，並獲得、修改、刪除其系統資訊或是添加有害的訊息。
3. 網路防禦。關於反網路偵察和反網路攻擊的手段，包含訪問控制、身分驗證、防火牆、資料加密、病毒防治、安全檢測與入侵檢測等。

在共軍公佈的戰略支援部隊任務中指出，戰略支援部隊除整合過往共軍情報組織外，更將技術偵查、電子對抗、航太，甚至心理戰、輿論戰都納入管轄。這些單位都不會參與實際的軍事行動，而是提供情報給作戰部隊以供決策。這些單位不適合隸屬於單一軍種，但又無法與各軍種脫離關係。[64]過去中國大陸情報體系涉及總參三部、總參四部和總政戰部等多個部門，造成整合不易，資源分散，現今透過軍改後歷經整合，在管理層面和

[63] 葉征，《資訊作戰學教程》（北京：軍事科學出版社，2013 年 1 月），頁 70-71。
[64] 田斌，《習近平推動軍隊改革組建資訊軍》（香港：前哨出版社，2016 年 2 月），頁 31。

資源集中上，更能發揮統合戰力是聯合作戰的重要力量，對未來共軍的戰力應有相當助益。

參、小結

美國是網路空間領域的霸權，從 1946 年世界第一台計算機 ENIAC 在美國誕生，時隔 23 年後第一個網路由美國軍方建制的 ARPA 網也誕生，網路世界的控制權、主導權，根功能變數名稱的控制權、IP 位址的分配權、國際標準的制定權、網上輿論的話語權都掌握在美國手中。

面對中國大陸的崛起，既有強國的美國有所警惕，從稜鏡計畫的曝光，可看出美國為確保在網路空間的主導地位，採取權力極大化的手段，來遏止中國大陸等潛在大國在網路空間的威脅。然而中國大陸試圖改變由美國主導網路空間的規則制定，從戰略層面於 2014 年成立「中共中央網絡安全和資訊化領導小組」，並由習近平親自擔任組長，公佈《國家資訊化發展戰略綱要》、《國家網絡空間安全戰略》和《網絡空間國際合作戰略》體現中國大陸保障網路安全、維護國家利益及推動資訊化發展的決心。從立法層面制定《國家安全法》和《網絡安全法》不僅突顯出其欲確保對境內網路的絕對控制權力之外，亦具對外積極宣示之意涵。在共軍部分，中國大陸成立戰略支援部隊網路系統部，整合網路、電子、偵查等部隊，展現聯合作戰的能力。中國大陸基於恐懼而採取自助，進而以權力極大化的手段消

除恐懼，並藉由厚實自身的實力，以提升中國大陸在網路空間全球治理領域中之能見度與話語權，並試圖改變由美國和西方等國家主導的全球網路治理規則的制定。

第四章 中國大陸影響國際網路空間治理

攻勢現實主義源自於米爾斯海默於 2001 年出版的《大國政治的悲劇》，其認為國際體的無政府狀態，迫使各國權力最大化，尋求權力的優勢，以使自己更加安全，從而提高生存機率。使得各國無法預測他國的動機和意圖而採取自助，成為系統中最強的國家是保證生存的最佳途徑。[1]

美國是網路空間的霸權，其掌握全球網際網路的網路名稱、IP 位址、根伺服器的分配權，美國八大企業掌握網路資訊產業的軟、硬體關鍵核心技術和網路技術的標準制定上都掌握主導權和制訂規則的權力。

中國大陸是網路空間崛起的大國，2008 年後已成為全世界使用網際網路人數最多的國家，為使自己在網路空間能更加安全，尋求權力最大化。中國大陸外交部長王毅於 2019 年是中國大陸建政 70 周年發表：「中國大陸是聯合國（United Nations，以下簡稱 UN）安理會常任理事國，擔任聯合國國際電信聯盟（International Telecommunication Union，以下簡稱 ITU）等 4 個附屬機構主要負責人。參與東南亞國協（Association of Southeast Asian Nations，以下簡稱 ASEAN）、北大西洋公約組織（North Atlantic Treaty Organization，以下簡稱 NATO）和上海合作組織（Shanghai Cooperation Organization，以下簡稱 SCO）等區域組織，成功主辦上海合作組織、二十

[1] John Mearsheimer 著，張登及、唐小松、潘崇易、王義桅譯，《大國政治的悲劇》，頁 77-79。

國集團（Group of Twenty 以下簡稱 G20）、金磚五國[2]和世界互聯網大會等多場國際峰會，致力於提升網路空間的國際話語權、規則制定權和議程制定權。」[3]本章以攻勢現實主義的角度檢視中國大陸影響「聯合國架構下網路空間平台」、「區域性國際組織」、「網路空間多邊會議」等分節論述。

第一節 中國大陸影響聯合國組織及架構下網路治理平台

中國大陸面對網路空間仍由美國等西方國家控制，而身為網路使用大國和開發中國國家的代表，積極推出網路空間命運共同體的建設。中共中央政治局於 2016 年 10 月 9 日第 36 次集體學習上，習近平提出包含「加快推進網絡信息技術自主創新」,「加快數字經濟對經濟發展的推動」、「加快提高網絡管理水平」,「加快增強網絡空間安全防禦能力」,「加快用網絡信息技術推進社會治理」,「加快提升我國對網絡空間的國際話語權和規則制定權」等「六個加快」。[4]

當前，網路空間仍停留在網路能力決定網路權力的霍布斯「叢林法則」時代，應積極參與國際合作機制，增強在國際規則制定上的主動權與話語

[2] 「金磚五國」(BRICS)，是以美國投資銀行高盛首席經濟師奧尼爾(Jim O'Neil) 於 2001 年首先提出「金磚四國」的概念。四國是巴西（Brazil）、俄國（Russia）、印度（India）和中國（China）。取每個國家英文名稱第一個字母，加起來成為 BRIC。因發音近似英文 Brick（磚），中文名稱被巧妙譯成「金磚」，於 2011 年加入南非變成「金磚五國。參考來源：〈分析：金磚五國到底能有多大作為？〉,《BBC 中文網》, 2013 年 3 月 26 日。〈https://www.bbc.com/zhongwen/trad/world/2013/03/130326_brics_future.shtml〉。(檢索日期 2020 年 4 月 21 日)。

[3] 〈王毅：譜寫中國特色大國外交的時代華章〉,《中華人民共和國中央人民政府》, 2019 年 9 月 23 日。〈http://www.gov.cn/guowuyuan/2019-09/23/content_5432243.htm〉。(檢索日期 2020 年 4 月 21 日)。

[4] 新華社,〈中共中央政治局就實施網絡強國戰略進行第 36 次集體學習〉,《中華人民共和國中央人民政府網》2016 年 10 月 9 日。〈http://www.gov.cn/xinwen/2016-10/09/content_5116444.htm〉。(檢索日期 2020 年 3 月 2 日)。

權。目前，聯合國是最具代表性、影響力的國際組織，擁有 193 個成員國，在聯合國的框架下推動國際多邊、雙邊合作，共同治理網路空間是中國大陸所支持的治理模式。聯合國涉及網路空間治理的相關組織「國際電信聯盟」和以聯合國架構下的網路治理平台「資訊社會世界峰會」（World Summit on the Information Society，以下簡稱 WSIS）、「網際網路治理論壇」（Internet Governance Forum，以下簡稱 IGF）與「資訊安全政府專家組」（United Nations Governmental Group of Expert, 以下簡稱 UNGGE）等，以下分段敘述。

壹、國際電信聯盟

20 世紀末，通訊和資訊技術飛速發展，以全球網際網路和移動通訊改變人們的生活方式，推動社會、經濟、文化和科技等各領域的發展，人們預測 21 世紀將是「資訊世紀」，有效的國際合作顯然是關鍵性，誕生於 1865 年的國際電報聯盟（International Telegraph Union，ITU），1932 年改稱為國際電信聯盟，1947 年聯合國成立時將其設立為下設機構，是最早成立的國際組織。中國大陸於 1949 年成立電信總局，之後於 1971 年因聯合國通過《2758 號決議》，加入 ITU。其宗旨是促進各種電信業務的研發和國際合作；提高電信服務的效率，增加使用率和達到大眾化和普遍化；協調各國電信標準化、無線通訊規範和通訊發展的目的。[5]

[5] 陳陽，〈國際電信聯盟簡介〉，《現代通信》，第 8 期，1998 年，頁 2。

美國在網際網路空間既是創造者，也是規則制定者，從對網路技術標準，像日常所用的傳輸控制協定/網際網路互聯協定(TCP/IP)、用於網頁製作的標記語言(HTML)、無線網路傳輸技術(WIFI)等的制定推廣和 ICANN 機構的建制，美國都是先行者。然而 ITU 是聯合國重要的資訊技術機構，中國大陸、俄羅斯等開發中國家表達應由聯合國主導網路空間治理，這與美國在網路管理的模式採取「多利益相關方」中產生分歧。

顯見於 2012 年在杜拜舉行的電信聯盟大會，主要對 1988 年通過的《國際電信規則》（International Telecommunication Regulations）進行修改，新的條約闡述為開發中的國家提供援助和應由聯合國主導網路空間治理，中國大陸和俄羅斯為代表的 89 個國家同意並簽署。然而美國之所以拒簽的原因是：「在這項提案裡，我國拒絕接受一些國家試圖在國際網路管控內容中插入政府管控選項，尤其是想在 ICANN 分配權力進行掌控。我們堅持這些管控只能由「多利益相關方」（Multistakeholder）參與的組織，[6]通過合法的方式來處理新的國際通訊條例」。[7]此草案因美中在網路空間管理模式的分歧擱置至今。

[6] 多利益相關方的定義是美國商務部資訊助理部長 Lawrence E. Strickling 所提出：「是包含所有利益相關者的完全參與，在意見一致基礎上的決策，以及在開放透明的方式下執行，促進網路的表達自由，保證網路是包含開發中國家在內的創新投、投資平台。」將參與網路治理的多利益相關方定義為四個方面：政府、公民社會、私有企業或機構、技術團體。參考來源：郭良，〈聚焦多利益相關方模式：以聯合國互聯網治理論壇為例〉，《汕頭大學學報》第 33 卷第 9 期，2017 年，頁 25-27。

[7] 〈國際電信大會修訂《國際電信規則》 美國等國抵制〉，《聯合國新聞網》**2012 年 12 月 14** 日。〈https://news.un.org/zh/story/2012/12/185462〉。(檢索日期 2020 年 3 月 2 日)。

ITU 的誕生在於制定通訊技術的統一標準，誰掌握網路技術標準，誰就能在通信領域掌握「控制權」；而誰掌握通信領域的控制權，誰就有能力對本國及他國的政治、經濟及安全增加影響力和話語權。中國大陸和俄羅斯等開發中國家，支持推動新的《國際電信規則》，賦予 ITU 參與國際域名的分配、增加管控垃圾郵件、網路安全和網路技術標準的制定等議題進行改革，要使開發中國家能平等、民主等方式參與。

而中國大陸自從改革開放後，鄧小平認為「中國大陸發展經濟，搞現代化，要從通訊入手，這是經濟發展的起點。」[8]習近平領導時期，中國大陸電信業已獨立自主，成為中國大陸「走出去」的重要戰略目標，在中國大陸政府的鼓勵下，「中國移動」及」中國電信」等電信產業也紛紛走向世界，以中興、華為等晶片製造業也至海外拓點，中國大陸政府制定的資訊政策與 ITU 的政策大體一致，中國大陸不僅參與國際通訊領域的治理，而且要透過國際標準制定得利。

因此，中國大陸所推薦的趙厚麟獲選成為 1998 年 ITU 組織之一標準化局局長，有利推動中國大陸自主研發的技術標準通行於全世界。經過幾年在 ITU 的努力，趙厚麟於 2014 年成功獲選為 ITU 秘書長，改變一直由美國

[8] 信息產業部辦公廳〈我國電信領域改革開放大事記〉，《中國信息產業網》，2001 年 2 月 27 日。〈http://www.cnii.com.cn/20020808/ca79451.htm〉。(檢索日期 2019 年 11 月 11 日)。

與西方等已開發國家擔任秘書長的格局，有利於中國大陸在網路空間議題的創設和技術標準的制定，藉此增加網路空間的影響力與話語權。[9]

中國大陸國務院於 2015 年 5 月 8 日公布《中國製造 2025》的戰略規劃，目標是到 2025 年，將中國大陸從「製造大國」變身為「製造強國」。[10]

中國大陸無意在傳統科技工業領域和美國糾纏，企圖以「彎道超車」直接進入最新的科技領域，並大量投入資源以爭取領先機會。而具有指標的產業是第五代移動通訊系統（5th generation mobile networks ，以下簡稱 5G），資料傳輸能大量且快速的進行演算，可使智慧醫療、智慧城市、智慧車、無人駕駛等系統更趨穩定，在中國大陸政府的支持下於 2019 年由「中國信息通信研究院」、「華為」、「中興」、「中國信息通信科技集團」、「中國移動」等企業向國際電信聯盟「WP-5D」提交 IMT-2020 技術方案，已獲得 ITU 的正式接收確認函。[11]

美國身為網路空間的霸權，掌握著網路空間軟、硬體的關鍵技術和網路技術的標準制定。面對中國大陸政府上有政策指導，下有產業配合，華為在 5G 的專利已達 10%，重視研發和爭取人才，因而在 2018 年底全球通

[9] 〈趙厚麟成國際電信聯盟 150 年來首位中國籍秘書長〉，《人民網》，2014 年 10 月 24 日。〈http://ip.people.com.cn/BIG5/n/2014/1024/c136655-25900794.html〉。(檢索日期 2019 年 4 月 12 日)。

[10] 〈國務院印發《中國製造 2025》〉，《新華網》，2015 年 05 月 19 日。〈http://www.xinhuanet.com//politics/2015-05/19/c_1115331338.htm〉。(檢索日期 2020 年 4 月 12 日)。

[11] 中國信通院〈中國完成面向國際電信聯盟的 5G 候選技術方案提交〉，《新浪科技網》，2019 年 7 月 18 日。〈https://tech.sina.com.cn/5g/i/2019-07-18/doc-ihytcerm4459560.shtml〉。(檢索日期 2020 年 4 月 12 日)。

信設備市場占有率達到 28%，智慧型手機的銷量以超越蘋果（Apple），僅次韓國三星（以下簡稱 Samsung），成為全球第二大手機製造商。[12]

中國大陸政府積極參與 ITU 標準局和秘書長的遴選與華為和中興等資訊通訊產業，積極參與國際通信標準化，有利推動《中國製造 2025》戰略執行，使得網路資訊產業在國際市場能見度大增和 5G 等自主科技研發的標準通行於全世界，並擴大在網路空間創設議題的話語權和資訊技術領域的影響力，從製造大國邁向製造強國。[13]

貳、以聯合國架構下的網路治理平台

網際網路起源於美國，在 90 年代之前一直為軍事和教育領域服務，最初的網際網路的地址資源分配，是由美國政府合約下的網路號碼分配局負責（Internet Assigned Numbers Authority，以下簡稱 IANA），隨著網際網路全球性的發展，美國開始進行改革，著手成立 ICANN 執行 IANA 的職權。因此，ICANN 在 1998 年成立，由美國商務部監管的非營利組織，著手管理網路域名及地址資源的分配權。2009 年 IANA 成為 ICANN 下的一個職能機構。[14]

[12] 〈貿易戰從來不是貿易問題：美國為什麼要防堵華為，占領全球 5G 市場？〉，《經濟日報》，2019 年 6 月 4 日。〈https://money.udn.com/money/story/10511/3852873#prettyPhoto〉。(檢索日期 2020 年 4 月 12 日)。

[13] 左志，〈國際電信聯盟與中國崛起-以中國電信政策研究為視角〉，《新聞大學學報》，第 3 期，2016 年，頁 16-17。

[14] 陳萊姬，〈從 IANA 移交看 ICANN 新全球網路治理模式〉，《網絡空間研究》，第 8 期，2016 年，頁 35。

然而，隨著國際社會對資訊技術和網路依賴持續增加，由美國商務部監管 ICANN 與中國大陸、俄羅斯等國產生嚴重分歧。中國大陸及俄羅斯等開發中國家認為網路空間是建立在國家資訊基礎設施上，屬於國家主權範圍，主張各國政府和聯合國在網路治理應發揮更大的控制權。聯合國大會於 2001 年 12 月 21 日通過舉辦資訊社會世界峰會。其主旨是為全球範圍內資訊社會的協調發展的規制定，利用資訊技術推動聯合國發展目標，及各國經濟社會持續發展，促進全人類的進步。

WSIS 的歷史發展過程大致分為兩大階段，第一階段是峰會階段，第二階段為論壇階段。首先，峰會階段是以 2002 年至 2005 年分別舉行日內瓦峰會和突尼斯峰會。前者，日內瓦峰會由美國、中國大陸等 176 個國家、國際組織、非政府組織等萬餘人與會。中國大陸在在日內瓦峰會上提出:「網路治理應由政府主導、多方參與、民主決策的原則」與美國和歐洲等已開發國家對於網路治理等議題產生嚴重分歧。[15]

其一，消除開發中國家和已開發國家，網路科技的差異造成數位鴻溝的問題。由於網路關鍵基礎設施的差異和貿易的鴻溝，中國大陸等開發中國家和美國等已開發國家存在著基礎設施和技術發展上的差異。已開發國家將網路的關鍵基礎設施認定為智慧財產權保護的對象，而中國大陸等開發中國家認為正是因已開發國家對資訊技術和智慧財產權的壟斷，才導致

[15] 劉靜，《網絡強國助推器-網絡空間國際合作共建》，（北京：知識產權出版社，2018 年 7 月），頁 145-146。

資訊通訊技術應用的差距擴大，因此中國大陸等開發中國家提出建立專門基金，如團結基金（Solidarity Fund）來幫助開發中國家開發資訊技術，但卻遭美國等已開發國家反對。

其二，全球網際網路管理權歸屬問題。中國大陸等開發中國家認為網際網路的管理應納入聯合國領導框架下，各政府機構可參與協作，而美國堅持以商業利潤為原則堅持由多利益相關模式實施網路管理。中國大陸和巴西等代表提出要把網際網路域名和 IP 地址管理組織的業務交由 ITU 管理，而美國和歐洲等已開發國家仍堅持由 ICANN 負責管理。[16]

因此，各方未能就縮小數位鴻溝和網路國際管理這兩個問題取得共識，只通過《日內瓦原則宣言》（Declaration of Principles）和《日內瓦行動計畫》（Plan of Action）。[17]而後續的突尼斯峰會也因美國政府堅持 ICANN 的管理權，與中國大陸等開發中國家就網路治理問題的談判也陷入僵局，最後通過《突尼斯承諾》（Tunis Commitment）和《突尼斯議程》（Tunis Agenda for the Information Society）。

為尋求網路治理的解決方案，WSIS 在 2005 年突尼斯峰會提出成立一個廣泛參與、沒有約束力的論壇，名為網際網路治理論壇。IGF 主旨在探討如何加強聯合國在網路治理的建設，展開多領域和多邊網路治理，推動全

[16] 許瑋陰，陳帥，方興東，〈信息社會世界峰會的演進歷程和發展現狀〉，《汕頭大學學報》，第 33 卷第 7 期，2017 年，頁 30。

[17] "Declaration of Principles,"*World Summit on the Information Society*, December 12, 2003< https://www.itu.int/net/wsis/docs/geneva/official/dop.html >.（瀏覽日期 2020 年 3 月 15 日）

球網路資訊產業的持續發展。聯合國在 2006 年 4 月通過 IGF 的五年授權，2006 年 10 月在希臘雅典舉辦首次 IGF，至今成功舉辦 14 屆。（如下表 4-1）

表 4-1 網際網路治理論壇歷屆會議

網際網路治理論壇歷屆會議			
項次	時間	地點	主題
1	2006 年 10 月	希臘雅典	網際網路治理促進發展
2	2007 年 11 月	巴西里約熱內盧	網際網路治理促進發展
3	2008 年 12 月	印度海得拉巴	人人享有網際網路
4	2009 年 11 月	埃及沙姆沙伊赫	網際網路治理–為所有人創造機會
5	2010 年 9 月	立陶宛維爾紐斯	共同發展未來
6	2011 年 9 月	肯亞內羅畢	網際網路是變革的催化劑：獲取，發展，自由和創新
7	2012 年 11 月	亞塞拜然巴庫	網際網路治理促進可持續的人類，經濟和社會發展
8	2013 年 10 月	印度尼西亞巴厘島	以網路安全促進經濟社會發展
9	2014 年 9 月	土耳其伊斯坦堡	將各大洲聯繫起來，以增強多利益相關方的網路治理

10	2015 年 11 月	巴西 若昂佩索阿	網際網路治理的發展
11	2016 年 12 月	墨西哥哈利斯科州	實現包容性和可持續增長
12	2017 年 12 月	瑞士日內瓦	塑造你的數位化未來
13	2018 年 11 月	法國巴黎	信任的網際網路
14	2019 年 11 月	德國柏林	一個網路一個願景

筆者自製。參考來源：方興東、陳帥、徐濟函，〈中國參與互聯網治理論壇的歷程、問題與對策〉，《理論前沿》，第 7 期，2017 年，頁 25。《網際網路治理論壇網站》，〈https://www.intgovforum.org/multilingual/content/igf-2019〉。(檢索日期 2020 年 3 月 2 日)。

中國大陸積極參與歷屆 IGF，以下詳細整理中國大陸參與 IGF 的階段與歷程。第一階段（2006 年至 2007 年）積極參與 IGF 機制和議程設置。在 2006 年 IGF 第一次籌備會議時，中國大陸與開發中國家組成 77 國集團（Group of 77,以下簡稱 G77）[18]強調需要確保來自開發中國家的政府、公民和企業的有效參與，在正式與非正式的會議，所有審議和決策的過程都要有代表權。尤其在論壇的「多利益相關方諮詢小組」（Multistakeholder Advisory Group，以下簡稱 MAG）席位的分配上，中國大陸和 G77 堅持由政府、公民社會和企業等三個分別代表的委員會進行監督。[19]

[18] 77 國集團於 1964 年正式成立，該組織有 77 個創始成員，是聯合國的開發中國家，旨在促進其成員的集體經濟利益，並創建聯合國的增強聯合談判能力。但到 2019 年 11 月，該組織已擴展到 135 個成員國（包括中國）。參考來源：〈77 國集團〉，《中華人民共和國外交部》，2001 年 2 月 27 日。〈https://www.fmprc.gov.cn/web/wjb_673085/zzjg_673183/gjjjs_674249/gjzzyhygk_674253/qsqg_674549/gk_674551/〉。(檢索日期 2020 年 3 月 1 日)。

[19] 多利益相關方的定義是美國商務部資訊助理部長史瑞奇克里（Lawrence Strickling）所提出：「是包含所有利益相關者的完全參與，在意見一致基礎上的決策，以及在開放透明的方式下執行，促進網路的表達自

第一屆由中國大陸時任資訊產業部外事司長陳因、中國大陸互聯網協會理事長胡啟恆院士和秘書長黃澄清參加。第二屆會議與會人員相較於第一屆參與背景較為多元，除資訊產業部和外交官員外，和來自中國大陸互聯網協會、中國大陸科學技術協會等民間組織和香港的學校、公民社會等機構參與。[20]中國大陸在 IGF 的議程創設與主導上起到關鍵性作用，其中 2007 年會議提出四條具體建議：[21]

一、 在關鍵網路資源的舉體管理中加上能力培訓。

二、 所有利益相關者，尤其是各國政府，應利用網際網路治理論壇的多邊、民主和透明原則來討論如何參與關鍵網路資源管理的公共政策。

三、 應在網際網路治理論壇的框架內討論如何確保開發中國家從 IPv4 到 IPv6 過渡期間所有國家都能平等獲得網路位址的資源。

四、 應討論增加、刪除和調整通用頂級網路域名的問題。[22]

第二階段(2008 年至 2010 年)中國大陸在會議籌備階段重申，在 ICANN 網域名分配權上，政府應處於領導地位並發揮更多權力。然而現階段的論壇，不足以解決美國壟斷網際網路領域的問題和開發中國家缺乏平台對話

由，保證網路是包含開發中國家在內的創新投、投資平台。」將參與網路治理的多利益相關方定義為四個方面：政府、公民社會、私有企業或機構、技術團體。參考來源：郭良，〈聚焦多利益相關方模式：以聯合國互聯網治理論壇為例〉，《汕頭大學學報》第 33 卷第 9 期，2017 年，頁 25-27。

[20] Avri Doria and Wolfgang Kleinwächter edited, The First Two Years, *Internet Governance Forum*,2009, 〈https://www.intgovforum.org/multilingual/filedepot_download/3367/5〉。(檢索日期 2020 年 3 月 1 日)。

[21] 方興東、陳帥、徐濟函，〈中國參與互聯網治理論壇的歷程、問題與對策〉，《理論前沿》，第 7 期，2017 年，頁 27。

[22] 王甜，〈互聯網治理論壇第二次會議在巴西召開〉，《互聯網天地》，2007 年，頁 2。

與所需要的網路資源和話語權。因此，中國大陸建議以論壇成果為基礎，發起聯合國框架下的政府間討論，以解決網路治理的問題。[23]這階段會議中強調網路安全的重要性、為打擊網路恐怖主義和網路犯罪，國家有權力過濾網站的內容，這也是將網路主權的概念融入會議內。

第三階段（2011 年至今），中國大陸致力於擴大開發中國家在 IGF 的參與。一方面中國大陸的席位不再僅限於政府代表，增至 2-3 人。於 2011 年時，中國大陸政府代表重返 MAG 參與籌備工作，同時首次有香港企業和非政府組織代表進入 MAG，並開始組織研討會，中國大陸政府代表提出聯合國是討論網路安全的政府間最佳論壇，應把「安全」、「開放」、「隱私」等議題納入聯合國討論的範圍。[24]2012 年時中國大陸社會科學院郭良成為 MAG 的成員，參與「網際網路治理促進發展」的主要會議，中國大陸互聯網協會主辦「移動改變世界」的研討會，邀請「百度」、「中國電信」等企業參與。[25]

美國 2013 年因史諾登揭露稜鏡事件後，美國監聽和監控活動受到國際社會的巨大壓力，被迫宣布有條件放棄 IANA 的監管。美國、中國大陸、俄羅斯等國互相指責遭受到他國網路駭客、監聽、竊密等問題，網路安全

[23] William J. Drake, edited, "Internet Goverance: Creating Opportunties for all", *The Fourth Internet Governance Forum*, November. 15-18, 2009,〈https://www.intgovforum.org/multilingual/filedepot_download/3367/7〉。(檢索日期 2020 年 3 月 1 日)。

[24] 〈中國互聯網協會出席聯合國互聯網治理論壇舉行〉,《中國信息安全》，2011 年 11 月，頁 15。

[25] 〈第七屆互聯網治理論壇舉行〉,《計算機安全》，2012 年 11 月，頁 78。

已成為危害國家安全的議題，並於 2015 年 7 月組成聯合國資訊安全問題政府專家組，向聯合國提交報告。第一次各國同意約束自身在網路空間的行為，不能利用網路攻擊他國核電廠、銀行、交通等重要關鍵基礎設施，以及不能在資訊產品中植入後門程式。在達成此共識之前，美國有條件做出讓步，宣告把網路域名管理權交給 ICANN，並堅持 ICANN 係由「多利益相關方」原則的管理模式，反對交給由政府主導的聯合國治理模式。[26]

這與中國大陸、俄羅斯等國家所提倡在聯合國框架下解決網路空間問題有所分歧。為此，中國大陸政府因美國等歐洲國家堅持網路空間維持「多利益相關方」原則，改變中國大陸多由政府官員參與網路空間治理的模式。從 2013 年開始擴大與會人員背景的多元性，一開始只有政府代表，陸續加入非政府代表進入 MAG，例如中國大陸技術社群、民間團體、學界、企業機構等都積極參與這一全球網路治理的盛會，提交研討會方案，創設議題，藉此平台發出「中國大陸聲音」，有利於網路社群理解多利益相關方的治理模式，透過民間參與方式傳遞中國大陸聲音，並能影響全球網際網路治理的作用。

然而中國大陸在 IGF 參與中仍存在諸多問題。首先，政府各部門缺乏協調與合作。政府部門缺乏長期計劃和部門職責，從工信部、外交部以及

[26] 陳萊姬，〈從 IANA 移交看 ICANN 新全球網路治理模式〉，《網絡空間研究》，第 8 期，2016 年，頁 35。

網絡信息辦公室等相關部門前後都參與 IGF 活動，中國大陸互聯網協會、中國大陸科協等民間組織也參與其中，缺乏系統性和持續性參與。[27]

其次，議題影響力有限。中國大陸在申辦組織的研討會數量極少，也不是核心議題。除研討會外，在 IGF 其他多種會議形式中，如開放性會議、動態聯盟、最佳實踐論壇，中國大陸參與更是少見。

最後，迄今沒有成為主辦國。中國大陸提倡聯合國主導網路治理，中國大陸代表曾因 IGF 缺乏決策權和執行能力，而建議停止。但如今沒有一個更具全球代表性，更好的全球網路治理意識平台超越過 IGF，相比之下，ICANN 已形成由美國政府、網域商和網路企業巨頭的多方參與機制，已形成既有強大的制度體系，然而中國大陸要深入參與，發揮影響力難度大於 IGF。IGF 係在聯合國框架下，中國大陸在聯合國為常任理事國其可透過聯合國機制下的平台創設議題及議程，提升網路空間的話語權和影響力，突顯出中國大陸未來持續影響 IGF 是顯而預見的。[28]

參、小結

中國大陸政府積極參與聯合國框架下網路治理的模式，從推薦趙厚麟成為國際電信聯盟的秘書長，改變由西方已開發國家擔任秘書長的格局。進而透過 WSIS 和 IGF 在網路空間治理平台發出中國大陸聲音。再者，華

[27] 方興東、陳帥、徐濟函，〈中國參與互聯網治理論壇的歷程、問題與對策〉，《理論前沿》，第 7 期，2017 年，頁 29。
[28] 方興東、陳帥、徐濟函，〈中國參與互聯網治理論壇的歷程、問題與對策〉，頁 30。

為、中興等網路科技公司在 5G 的積極建制，已威脅到美國在網路科技領域的佈局。最後，中國大陸亟欲拉攏開發中國家在聯合國或附屬組織內建立標準、技術、規範和規則，有效遏止美國網路強國利用技術、人才、企業等優勢主導網路空間議題的設置、輿論的控制及規則的制定。上述舉措可視為改變由美國在網路空間主導議題設定和八大企業科技壟斷，這也呼應攻勢現實主義既有強權美國與潛在大國中國大陸，因無法預測他國的動機和意圖而採取自助，讓影響力極大化以及改變現狀，使中國大陸為成為體系中最強的國家，不僅要加強在網路空間議題創設的影響力，也要在聯合國擔任機構領導人，改變由美國在網路空間領域的長期主導地位。

第二節 中國大陸參與區域性組織影響網路空間規則制定

隨著中國大陸網路與資訊化發展，在網路空間的活動日益增多，逐漸在技術、安全、政治和經濟等各個領域與國家及區域性國際組織展開不同程度的合作。本節主要梳理中國大陸與「北大西洋公約組織」、「上海合作組織」和「東南亞國協」三個部分，分析中國大陸與區域性國際組織之間在網路空間合作存在的問題及發展趨勢作出整理。

壹、北大西洋公約組織

北大西洋公約組織是美國、英國及法國於第二次世界大戰後為與蘇聯（Russian Soviet Federative Socialist Republic）為首的東歐集團國成員相抗衡而建立的國際組織。於 1949 年 4 月 4 日美國華盛頓（Washington, D.C.）

簽署《北大西洋公約》（North Atlantic Treaty）後正式成立。陸續加入希臘、土耳其、德國、西班牙等國家直至 2020 年北馬其頓共和國加入後，成為美國主導的跨域歐洲和北美 30 個國家組成的區域性國際組織。[29]

近年來，全球網路安全威脅問題受到各國重視，特別自 2007 年愛沙尼亞首都塔林遭受到網路攻擊和 2010 年伊朗核電廠受到震網病毒事件以來，有關利用網路攻擊的新形態攻擊模式，受到主權國家日益重視，通過國際法規則來建構網路空間秩序，爭奪網路空間的話語權與主導權，除此之外，目前有關網路攻擊的定義與國際法之間的發展仍不明確，各國正努力共同形塑應對網路攻擊的規範。[30]

由於網路空間國際規則制定是一個全新的領域，以中國大陸、俄羅斯等國及美國、北約等兩陣營意見分歧。其一，中國大陸、俄羅斯、塔吉克和烏茲別克於 2012 年向聯合國提交《資訊安全國際行為準則》（the International Code of Conduct for Information Security）的草案，遭到美國為首的西方國家強烈抵制。中國大陸及俄羅斯等國主張：「應尊重各國在網路空間的主權，不利用資訊通信技術包括網路實施敵對行動、侵略行徑和製造對國際和平與安全的威脅，並主張在涉及上述活動時產生的任何爭端，

[29] 湯紹成，〈後冷戰時期北大西洋公約組織角色與功能的轉變〉，《問題與研究》，2000 年 1 月，第 39 卷，頁 68-69。

[30] 陳舒、劉賢剛、葉潤國、胡影，〈塔林手冊 2.0 視角下的網路空間國際規則理論的發展〉，頁 44。

都以和平方式解決，不得使用武力或以武力相威脅。」[31]但美國認為，網路空間具有「全球公域」（the global Commons）的性質，網路空間既屬於國家也包含公司、非政府組織、學術團體及個人，不為任何一個國家所支配而所有，政府過多限制會損害網路自由。[32]

其二，聯合國大會於 2013 年 12 月，通過第 68/243 號決議，決定成立由 20 名專家組成政府專家小組，討論《聯合國憲章》（Charter of the United Nations）及其他國際法規範能否適用於網路空間。美國、歐洲等國贊成將聯合國武裝衝突法（International Humanitarian Law）適用於網路空間，但中國大陸及俄羅斯等國反對，認為會導致網路空間軍事化。[33]

愛沙尼亞於 2007 年遭受到網路攻擊後，國際間應對網路戰與網路威脅的發展，在美國的推動下愈來愈受到重視，其中 2013 年 3 月，由北大西洋公約組織（The North Atlantic Treaty Organization, 簡稱 NATO）所主導與贊助的「卓越合作網路防衛中心」（Cooperative Cyber Defense Centre of Excellence, NATO CCD COE）著手制定網路戰如何適用現行國際法的《塔林網路戰國際法手冊》（Tallinn Manual on the International Law Applicable to Cyber Warfare），簡稱《塔林手冊 1.0》，列出 7 章 95 條規範，內容涉及「國家主權」、「國家責任」、「訴諸戰爭權」、「國際人道法」和「中立法」，以網

[31] 〈中俄等國向聯合國提交《信息安全國際行為準則》〉，《中華人民共和國中央人民政府》，2011 年 09 月 13 日。〈http://www.gov.cn/jrzg/2011-09/13/content_1945825.htm〉。(檢索日期 2020 年 5 月 1 日)。

[32] 魯傳穎，〈試析當前網路空間全球治理困境〉，《現代國際關係》，2013 年，第 11 期，頁 46。

[33] 朗平，〈全球網路空間規則制定的博弈與合作〉，《國際展望》，2014 年，第 6 期，頁 146。

路戰的國際法條款並詳加注釋，主要偏重「網路戰」訴諸武力和自衛權等方面的問題。例如對一國家的關鍵基礎設施採取網路軍事行動，或向敵對指揮控制系統發動網路攻擊等。[34]

然而，中國大陸政府認為美國和 NATO 聯合編撰《塔林手冊 1.0》，無助於網路空間領域的國際合作。其一，美國學者史密斯(Michael Schmit)倡導將《聯合國憲章》第 2 和 4 條的「訴諸武力使用」和第 51 條對攻擊者行使武力自衛權適用於網路戰，得到美國和 NATO 的支持。反觀中國大陸不認同將武力使用等國際法規範適用於網路空間，會造成網路空間軍事化。其二，編撰《塔林手冊 1.0》的 20 名國際專家組成員來自美國、英國、德國等軍事法和戰爭法專家，未納入俄國、中國大陸等意見不同國家的專家學者。其三，《聯合國憲章》的武力使用和自衛等相關國際法問題，是當前最具爭議的問題，由於網路戰是否適用於國際法規範仍處於不明確狀態，亦是中國大陸政府最為關注的問題。中國大陸政府認為美國和 NATO 在編撰《塔林手冊 1.0》僅是為形塑網路行為規範的話語權和主導權並未解決網路戰所衍生出的問題。[35]

有鑒於此，與美國爭奪話語權與主導權，中國大陸政府於 2014 年 2 月 27 日成立「中共中央網絡和信息化領導小組」從網路空間的角度來審視網

[34] Michael Schmitt, *Tallinn Manual on the International Law Applicable to Cyber warfare* （Cambridge ： Cambridge University Press, 2013), pp. 16-17.

[35] 黃志雄，〈國際法視角下的「網路戰」及中國的對策-以訴諸武力權為中心〉，《現代法學》，2015 年，第 37 卷第 5 期，頁 154-155。

路空間國際規則，積極參與聯合國及區域組織探討網路空間安全等議題。2014 年初 NATO 舉辦網路衝突研討會探討日益氾濫的網路安全威脅，急需一部和平時期對網路行為的國際法《塔林手冊 2.0》(Tallinn Manual 2.0 on the International Law Applicable to Cyber Operation)。

國際專家組 19 名成員中，邀請中國大陸、泰國及白俄羅斯等 3 名非 NATO 成員國家代表，分別於 2015 年 6 月 29 日至 7 月 3 日、10 月 5 至 9 日和 2016 年 3 月 19 至 23 日在愛沙尼亞首都塔林召開三次會議並與荷蘭外交部合作。除此之外，還分別於 2015 年 4 月和 2016 年 2 月在荷蘭海牙舉行網路空間國際會議。[36]

其中，邀請中國大陸、美國、英國等 50 名國際法專家擔任評審專家，提供匿名評審意見。中國大陸代表團團長陳旭於表示中國大陸主張網路空間活動應遵守國家主權，不干涉內政，和平解決爭端等原則。[37]這兩次會議中國大陸派遣「外交部」、「國家互聯網資訊辦公室」、「國防部」、「工業和資訊化部」、「公安部」、「中國現代國際關係研究院」等與其他國際法專家針對網路安全等議題交換意見，也突顯出中共中央網路安全和資訊化領導小組跨越黨政軍和跨部會協調的能力和高度關注塔林手冊第二版的製作。

[36] 黃志雄，〈網絡空間規則的新趨向-基於塔林手冊 2.0 的考察〉，《廈門大學學報》，2018 年，第 1 期，頁 3。
[37] 〈中國代表團出席海牙網路空間國際會議〉，《中共中央網絡安全和信息化辦公室》，2015 年 4 月 21 日。〈http://www.cac.gov.cn/2015-04/21/c_1115037999.htm〉(檢索日期 2020 年 5 月 1 日)。

《塔林手冊 2.0》的問世對中國大陸網路安全影響具有兩面。有利中國大陸的是肯定網路主權的存在及不可侵犯性，明確定義網路攻擊和網路間諜的差異，承認網路行動溯源的困難，禁止在網路空間使用武力或以武力威脅。《塔林手冊》是美國與北約爭奪網路空間國際規則制定權的重要舉措，是美國進行網路空間戰略布局的重要法律文件。同時它對中國大陸的網路安全利益及和平穩定構成潛在威脅，主要顯現在肯定先發制人的合理性、承認對關鍵基礎設施的攻擊會造成大規模的破壞，在網路攻擊中嚴格規範軍對與平民的分別，預留進行反制干涉措施的伏筆。透過對《塔林手冊》的分析，可看出美國網路空間戰略布局的思路，這將會影響中國大陸等開發中國家對網路空間規則制定和重塑網路空間全球治理產生深遠影響。

依據攻勢現實主義推論中國大陸作為網際網路使用的大國，必須透過自助手段積極改變由美國掌握的國際網路規則的制定。中國大陸政府於 2016 年 3 月正式通過《中華人民共和國國民經濟和社會發展第十三個五年規劃綱要》明確提出要「積極參與網路、深海、極地、太空等領域國際規則制定。」[38]突顯出積極參與網路空間規範，可看出中國大陸將「網路主權」概念納入規範制定議程並且成為重要的論述主軸，使得中國大陸更能避免議題設定和規範制度遭美國等西方國家把持，同時採取攻勢作為擴大國際

[38] 〈《中華人民共和國國民經濟和社會發展第十三個五年規劃綱要》〉，《新華網》，2016 年 03 月 17 日。〈http://www.xinhuanet.com//politics/2016lh/2016-03/17/c_1118366322.htm〉(檢索日期 2020 年 5 月 1 日)。

參與，走出符合中國大陸期待的制度規範。

貳、上海合作組織

冷戰時期，國際政治受到美國與蘇聯兩大超強競爭影響，使得中國大陸的角色依兩大超強的興衰隨之改變。隨著東歐變色、蘇聯解體後形成十五個新興國家，其中有擁有豐富天然資源的中亞也成為國際各方角力的戰場。中國大陸依據「和平共處五原則」與俄羅斯和中亞等國家，[39]就邊界問題展開談判。「上海合作組織」（以下簡稱上合組織）的前身「上海五國」即是中國大陸與俄羅斯、哈薩克、吉爾吉斯、塔吉克等國於 1996 年簽署「關於在邊境地區加強軍事領域信任協定」以裁減邊界地區軍事力量和保持邊界安寧等問題形成區域論壇。[40]直到 1988 年「上海五國」的地區論壇逐漸朝向地區安全合作，促使中亞國家，除土庫曼外成立「上海合作組織」。在 2017 年增加巴基斯坦和印度兩國，以及阿富汗、白俄羅斯、伊朗、蒙古等 4 個為觀察員國。這次擴員後，成為人口最多、地域最大的區域組織，經過 19 年發展在安全和經濟層面，為中亞地區發展和安全奠定基礎。[41]

[39] 和平共處五原則，包含相互尊重領土完整、互不侵犯、互不干涉、互惠平等與和平共處。參考來源：〈和平共處五項原則〉，《中國共產黨新聞網站》，2014 年 06 月 28 日。〈http://cpc.people.com.cn/BIG5/n/2014/0628/c64387-25212801.html〉(檢索日期 2020 年 5 月 1 日)。

[40] 〈中華人民共和國和哈薩克共和國、吉爾吉斯共和國、俄羅斯聯邦、塔吉克斯坦共和國關於在邊境地區加強軍事領域信任的協定〉，《全國人民代表大會網站》，1996 年 4 月 21 日。〈http://www.npc.gov.cn/wxzl/wxzl/2000-12/06/content_3612.htm〉(檢索日期 2020 年 5 月 1 日)。

[41] 〈上海合作組織〉，《中華人民共和國外交部網站》，2019 年 12 月。〈https://www.fmprc.gov.cn/web/gjhdq_676201/gjhdqzz_681964/lhg_683094/jbqk_683096/t528036.shtml〉(檢索日期 2020 年 5 月 1 日)。

中亞地區在歷史上貿易商旅網來頻繁，是絲綢之路的必經之地，在蘇聯解體後，基於邊境問題與中國大陸進行談判。此外，中亞地區與中國大陸新疆地區維吾爾族與伊斯蘭教也有關聯，產生的宗教極端主義、民族分裂主義和恐怖主義，形成中國大陸所謂的「三股勢力」，[42]並在 2001 年後由上海合作組織六國元首共同簽署「打擊恐怖主義、分裂主義和極端主義上海公約」等協定，[43]對中國大陸而言確保西北邊境安全和國家領土完整是核心利益。

在網路媒體興起使得話語權[44]的較量多新的變數。過去，話語權主要操之於政府手中的報紙和電視引導大眾的閱聽取向和社會意象。然而社群網站的遍佈和智慧通訊設備的普及，使民眾閱聽的習慣改變，訊息從單向接收變成雙向互動，多方共享地使得網路媒體傳播速度和效果遠超過傳統媒體。中亞地區從 2003 年起發生一系列「顏色革命」，特別是現今的滋事份子利用網路社群媒體掌握話語權後，製造、放大和傳播有關政府高層腐敗、內鬨等訊息，從而以引發社會矛盾與衝突。使得上合組織成員國對非傳統安全威脅形成共識，並展開對話及合作。以下分為三部分探討上合組織成員國面臨網路安全威脅。

[42] 王桂芳，《中亞戰略格局與中國安全》（北京：軍事科學出版社，2004 年 12 月），頁 270-271。
[43] 余建華，〈中亞的民族問題及其影響論析〉，《俄羅斯研究》，第 1 期，2002 年，頁 73-74。
[44] 關於「話語權」的概念，源自法國社會學家福科（Michel Foucault）提出「話語即權力」，運用語言的技巧來影響他人的思考、行為，藉著傳遞價值觀念、意識形態形成一種權力。參考來源米歇爾福科，嚴鋒譯，《權力的眼睛-福科訪談錄》（上海：上海人民出版社，1997 年），頁 228。

首先，美國等西方國家借助網路等媒體推動「顏色革命」。吉爾吉斯於2005 年舉行議會選舉，其國內反對派利用報紙不斷攻擊時任總統阿卡耶夫（Askar Akayev）及其家屬的奢華生活，激起民眾對總統的不滿。最終，吉國爆發大規模騷亂並使政權更迭，時任總統阿卡耶夫則逃往國外。[45]烏克蘭於 2014 年 2 月發生政權更迭，美國等西方國家資助反對派，利用 Facebook 或是 Twitter 等網路社群媒體組織遊行示威活動，進行宣傳鼓動，最終引發時任總統亞努科維奇（Viktor Yanukovych）政府垮台。

中國大陸近年也出現反政府組織利用網際網路輸入民主自由的意識形態，作為煽動中國大陸的「顏色革命」。例如香港於 2014 年發生的佔中事件，目的是為爭取在 2017 年香港特首選舉落實真普選，抗爭行動持續到當年 12 月 15 日落幕，估計香港市民 700 萬人中有 120 萬人參與。2019 年 6 月反送中事件，都是藉由網路社群媒體掌握話語權，運用網路傳播政府違法濫權的事情，使得政府公信力喪失，進而達到政治訴求的目的。

其次，「三股勢力」利用網路媒體進行傳播和招募人才。近年來，通過網路、社群平台等在中亞各國青年中快速蔓延，不僅利用社群媒體進行人才招募、教唆民眾製造爆裂物，甚至威脅發動恐怖襲擊，成為破壞中國大陸及中亞地區安全穩定的重要因素。例如哈薩克，宗教極端主義份子利用伊斯蘭國「哈里發戰士」所發布的網路影片，在哈薩克西部地區製造恐怖

[45] 孫壯志主編，《獨聯體國家「顏色革命」之研究》，（北京：中國社會科學出版社，2011 年），頁 396。

襲擊。[46]俄羅斯與車臣第一次戰爭時，俄羅斯新聞媒體大肆渲染俄軍在車臣的非法行為及詆毀俄羅斯政府的消息，使俄羅斯軍事優勢大打折扣。

中國大陸自從成為網路使用大國後，恐怖份子也利用網際網路、手機和移動通訊散布意識形態和民族仇恨。2014 年大陸境內發生多起暴力或恐怖攻擊事件，諸如 5 月中旬新疆維吾爾自治區最南端的和田地區，發生維吾爾族向警方發動自殺炸彈攻擊；9 月中旬新疆阿克蘇地區發生「拜城煤礦攻擊案」；以及 9 月底時，廣西省柳城縣發生連環包裹炸彈事件。[47]

最後，網路犯罪頻繁。上海合作組織成員國中，中俄兩國使用網路用戶眾多，據中國大陸互聯網信息中心《中國互聯網路發展狀況統計報告》統計，截至 2018 年 12 月底，中國大陸網路使用數量世界第一，其中手機等移動通訊規模達 8.29 億。[48]根據俄羅社交媒體管理平台 Hootsuite 和 We Are Socia 編撰《2019 年全球數字年鑑》（2019 Global Digital Yearbook），目前在歐洲國家網際網路普及率已達到 76%，網路使用數 1.09 億和手機普及率已達 65%。[49]

[46] 新華社，〈哈薩克官員稱"哈里發戰士"威脅哈國安全〉，《環球網》，2012 年 12 月 5 日。〈https://world.huanqiu.com/article/9CaKrnJy24z〉。(檢索日期 2020 年 3 月 10 日)。

[47] 張文偉，〈上海合作組織信息安全合作：必要性、現狀及前景〉，《俄羅斯東歐中亞研究》，2016 年，第 3 期，頁 96。

[48] 中國互聯網路資訊中心，〈2019 年中國互聯網路發展狀況統計報告〉，《中國網信網》，2019 年 8 月。〈http://www.cac.gov.cn/2019-02/28/c_1124175677.htm〉。(檢索日期 2020 年 3 月 10 日)。

[49] Alyssa Yorgan, "10 key statistics on internet usage in Russia (2019)",*Russian search marketing,* February 20, 2019, https://russiansearchmarketing.com/internet-usage-russia-2019-10-key-statistics/.

網路的開放性、匿名性和跨國性的特點使得網路空間成為犯罪滋長的沃土，俄羅斯與中國大陸是網路使用大國，是惡意網路活動和網路竊密最多的國家之一。在中國大陸網路使用遭遇安全事件類別於 2018 年 12 月的統計網上詐騙 28.1%，個人資訊洩漏 27.3%、帳號或密碼被竊 17.7%，資訊設備種病毒或木馬等惡意程式等 14.5%，突顯出網路犯罪問題已威脅經濟安全。(圖 4-1 所示)

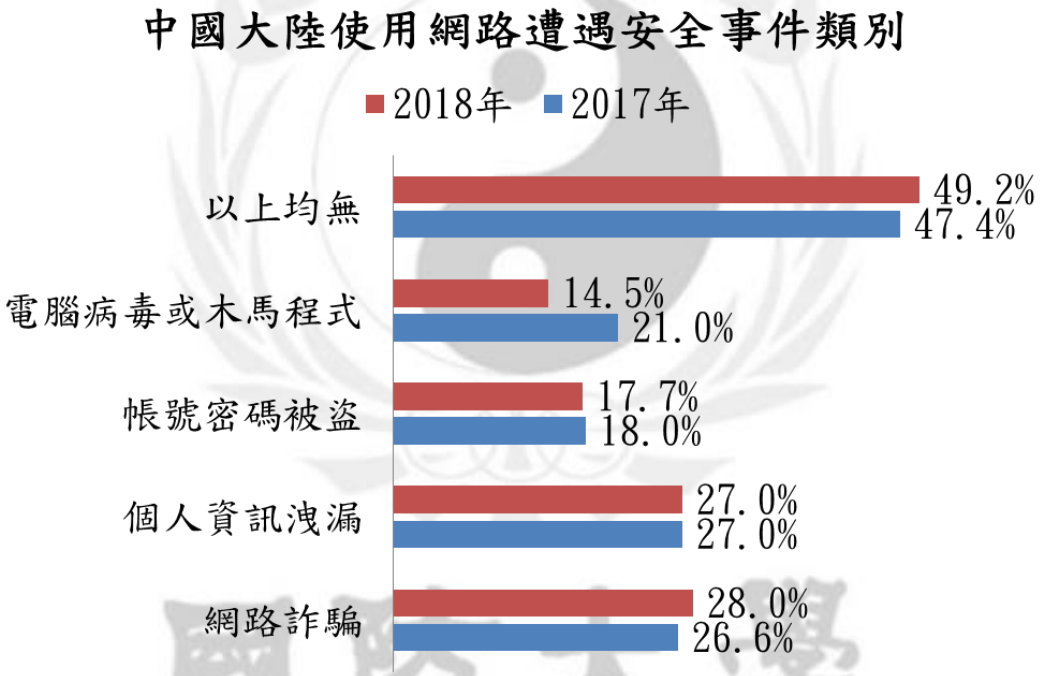

圖 4-1 中國大陸使用網路遭遇安全事件類別

筆者自製。來源：中國互聯網路資訊中心，〈2019 年中國互聯網路發展狀況統計報告〉，《中國網信網》。

上海合作組織成員國所遭受到「顏色革命」、「三股勢力」和「網路犯罪」等網路安全威脅，使得成員國在網路治理形成一致的看法和意見。首先，上合組織各國元首一致認為，各成員國在資訊安全領域面臨威脅，並

於 2006 年上海峰會於發表《上海合作組織成員國元首關於國際信息安全的聲明》認為資訊安全領域面臨政治、軍事、犯罪和恐怖主義等威脅，將威脅提升到與大規模殺傷性武器相等的程度，必須透過雙邊、地區和國際層面合作，加強保障各國資訊安全的強度。[50]

塔吉克首都杜尚別於 2014 年 9 月召開元首峰會，各成員國在尊重國家主權和不干涉內政原則上，共同合作防止使用資訊技術危害其他成員國政治、經濟和社會安全，以阻止不法份子利用全球網際網路，宣傳恐怖、極端、分裂、法西斯、激進主義等，一致採取共同行動應對網路威脅。[51]

中國大陸提議並組建資訊安全專家小組，增設秘書處和地區反恐機構執行委員會等兩個常設機構，於 2009 年 6 月 15 日在俄羅斯葉卡捷琳堡峰會上簽署《上海合作組織成員國保障國際信息安全政府間合作協定》，確保各成員國在框架內透過雙邊、組織內部和國際等三個層面展開合作，提高打擊網路恐怖主義、網路犯罪、保障境內資訊安全的能力，防止不法份子利用網路傳播「三股勢力」的思想及利用網路干涉他國內政。[52]

中國大陸首先與俄羅斯展開網路空間議題的雙邊合作，於 2015 年 5 月 8 日簽訂《中華人民共和國政府和俄羅斯聯邦政府關於在保障國際資訊安全

[50]〈上海合作組織成員國元首關於國際信息安全的聲明〉，《中華人民共和國外交部》，2006 年 6 月 15 日。〈https://www.fmprc.gov.cn/web/ziliao_674904/1179_674909/t346576.shtml〉(檢索日期 2020 年 3 月 10 日)。

[51]〈上海合作組織成員國元首杜尚別宣言〉，《新華網》，2014 年 9 月 13 日。〈http://www.xinhuanet.com/world/2014-09/13/c_126981562.htm〉。(檢索日期 2020 年 3 月 10 日)。

[52]〈《上海合作組織成員國保障國際信息安全政府間合作協定》〉，《澳門特別行政區政府印務局網》，2013 年 7 月 24 日。〈https://bo.io.gov.mo/bo/ii/2013/30/aviso28_cn.asp#cht〉。(檢索日期 2020 年 3 月 10 日)。

領域合作協定》協定將利用網路技術侵犯他國主權、破壞資訊基礎設施、干涉他國內政等列為主要威脅；規劃雙方展開合作的主要方向，[53]包括建立共同應對國際資訊安全威脅、打擊恐怖主義和犯罪活動的情報交流和溝通管道並共同組建專家小組實施網路攻擊的聯合演習，以應對外來的網路安全威脅。[54]

組織內部的多邊合作的例子是 2011 年 9 月 12 日向聯合國提交《資訊安全國際行為準則》（International Code of Conduct for Information Security）並呼籲各國在聯合國框架內討論網路空間安全問題，以盡早規範各國在資訊和網路空間行為達成共識，然而美國任為該草案限制網路自由，而遭到擱置。[55]2015 年上合組織成員國更新草案內容，推動以聯合國框架下各國平等參與網路治理、彌合數位鴻溝並建立網路領域信任機制，雖然不被美國等西方國家接受，但也使開發中國家接受並達成共識。[56]

最後，共同舉辦網路反恐演習。在俄羅斯城市舉行的地區反恐機構的會議上同意成立由各成員國主管網路安全專家組成聯合專家工作小組，旨

[53]〈《中華人民共和國政府和俄羅斯聯邦政府關於在保障國際資訊安全領域合作協定》〉，《中華人民共和國外交部網站》，2015 年 5 月 12 日。〈https://www.fmprc.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/jksxwlb_674635/t1263088.shtml〉。(檢索日期 2020 年 3 月 10 日)。

[54]〈俄媒：中俄兩國將就對抗資訊戰進行演習 並交換經驗〉，《新華網》，2015 年 12 月 23 日。〈http://www.xinhuanet.com/world/2015-12/23/c_128558988.htm〉。(檢索日期 2020 年 4 月 10 日)。

[55]〈美國務部：中國所提信息安全準則限制網絡自由〉，《美國駐華大使館》，2015 年 3 月 4 日。〈https://china.usembassy-china.org.cn/zh/internetfreedom2015-zh/〉。(檢索日期 2020 年 3 月 10 日)。

[56]〈《信息安全國際行為準則》〉，《中華人民共和國外交部》，2015 年 3 月 5 日。〈https://www.fmprc.gov.cn/web/ziliao_674904/tytj_674911/zcwj_674915/t858317.shtml〉。(檢索日期 2020 年 3 月 10 日)。

在打擊「三股勢力」展開跨國合作。中國大陸政府主導首次聯合網路反恐演習，代號為「廈門-2015」。聯合網路反恐演習於 2015 年 10 月 14 日舉行，透過演習各成員國互相交流，反恐行動中的作業流程、法律程序和組織能力，進步一步完善成員國相關部門的合作機制，共同建立網路空間反恐技術平台。[57]

中國大陸作為上海合作組織創始國，其組織的命名也以中國大陸地名，可以看出中國大陸在成立過程中試圖扮演主導的角色。中國大陸所面臨的不僅只是利用網路傳播意識形態等有害訊息、「三股勢力」的威脅和網路犯罪等行為，需要與週邊國家對話合作，所以發表「上海精神」以對話求合作，以合作促安全，以發展謀安全為主旨，即互信、互利、平等、協商、尊重多樣文明、謀求共同發展。資訊安全作為非傳統安全中重要且新穎的領域，事關中國大陸與中亞地區社會安全及區域穩定，在各成員國的共識下，首先，加強地區反恐機構的作用，將反恐演習成為組織內常態化的聯合軍事演習。其二，將網路主權的概念推行到組織成員國內並制定成國內法。最後，依據攻勢現實主義之假設，中國大陸透過上合組織的影響力，主導議題將網路安全威脅融入相關安全議程中，突顯中國大陸在區域組織間的主導性進而達到權力最大化，才符合其利益。[58]

[57] 〈上海合作組織首次網絡反恐演習在廈門成功舉行〉，《中華人民共和國國防部》，2015 年 10 月 14 日。〈http://www.mod.gov.cn/big5/topnews/2015-10/14/content_4624849.htm〉。(檢索日期 2020 年 3 月 10 日)。

[58] 張文偉，〈上海合作組織信息安全合作：必要性、現狀及前景〉，《俄羅斯東歐中亞研究》，2016 年，第 3

參、東南亞國協

東南亞國家協會（Association of Southeast Asian Nations, ASEAN，以下簡稱東協），是集合東南亞區域國家的一個政府性國際組織。東協於 1967 年成立，主要任務為防止區域內共產主義勢力擴張，合作側重在軍事安全與政治中立。冷戰結束後印尼、馬來西亞、菲律賓、泰國、新加坡等東南亞各國在政經情勢趨穩，陸續加入汶萊、柬埔寨並接納越南、緬甸和寮國。目前共有 10 個正式的成員國，另外還有一個候選國東帝汶和一個觀察國巴布亞紐幾內亞。[59]

其地處於亞洲東南部的中南半島與中國大陸相連，身處戰略要地，成為大國爭相合作的重點對象。根據統計，東協國家總人口超過六億，但從網際網路應用，使用網路人數近 2 億，網路普及率不足 30%，各成員國網路水平差距頗大，發展不均衡。因此，東協逐漸成為世界大國網路外交施加影響力的戰場，美國、俄羅斯、日本、韓國等紛紛尋求與東協建立網路合作機制，通過與東協合作提高網路領域話語權。

中國大陸自 1991 年與東協建立對話關係開始，到 2003 年建立戰略夥伴關係，把東南亞地區化為重點發展區域，積極展開多邊和雙邊交流。中國－東協資訊港（China-ASEAN Information Harbor）是中國大陸近年配合

期，頁 103-105。

[59] 東南亞國協在中國大陸稱為東盟。為了行文和閱讀的方便，均以東協一詞表示。〈「東南亞國家協會」發展簡介〉，《台灣東南亞國家協會研究中心》，2014 年 3 月 31 日，〈http://www.aseancenter.org.tw/ASEANintro.aspx〉。(檢索日期 2020 年 3 月 10 日)。

「一帶一路」（One Belt One Road）戰略中的「21 世紀海上絲綢之路」（21st-Century Maritime Silk Road）建設提出的重大項目。透過與東協國家在網路空間領域的合作，藉此提高中國大陸在全球網路空間治理中的話語權，以下區分三部分講述中國大陸與東協網路空間合作的主要特點。

首先，透過中國大陸與東協領袖高峰會議及部長級會議建立網路空間安全合作。從 2005 年中國大陸與東協制定《中國-東協面相共同發展的信息通信領域夥伴關係北京宣言》意旨為加快建設大湄公河次區域資訊高速公路，於 2008 年初步完成網路基礎設施建設，並於 2010 年展開業務營運。[60]2009 年通過《中國-東協電信監管理事會關於網絡安全問題的合作框架》為加強網路安全領域的交流與合作，連續九次召開中國大陸與東協電信監管理事會圓桌會，建立部長會議和網路安全研討會等合作對話機制。2013 年公布《中國-東協非傳統安全領域合作諒解備忘錄》確立雙方在網路反恐、禁毒、打擊國際經濟犯罪、跨境網路犯罪等重要領域合作，透過雙方資訊交流、人員培訓、執法協作等合作方式。[61]

2015 年提出建立《中國-東協計算機應急響應合作機制》，為網路安全領域提供資訊共享和事件處理機制，提高跨境網路安全事件處理速度。[62]這

[60]〈中國-東盟面相共同發展的信息通信領域夥伴關係北京宣言〉，《吉林省服務貿易指南網》，2007 年 1 月 14 日。〈http://www.jlfwmy.com/NewsShow.asp?pageclass=1010402&id=1627〉。(檢索日期 2020 年 4 月 10 日)。

[61]〈外交部發布中國-東盟合作：1991-2011(全文)〉，《中華人民共和國中央人民政府網》，2011 年 11 月 5 日。〈http://big5.www.gov.cn/gate/big5/www.gov.cn/gzdt/2011-11/15/content_1993964.htm〉。(檢索日期 2020 年 4 月 10 日)。

[62]〈李克強在第 20 次中國-東盟領導人會議上的講話(全文)〉，《中國外交部網》，2017 年 11 月 13 日。

一系列舉措突顯出中國大陸與東協在網路安全多邊合作上，主要圍繞在部長級會議與東協成員國就網路空間安全問題展開交流與闡述各自立場，[63]另一方面透過舉辦區域網路安全論壇研討會的形式，增強對網路空間規則的認識，謀求在制訂網路空間規則領域的共識。[64]

其次，初步建構網路空間國際合作平台。首屆「中國-東協網路空間論壇」於 2014 年在廣西南寧舉行，主題圍繞在網際網路發展與治理經驗。時任「中央網絡安全和信息化領導小組辦公室」主任魯煒在演講中提到：「加快推動網絡互聯、信息互通，引領市場贏得商機，用信息深化合作和驅動發展，使中國-東盟信息港成為建設 21 世紀海上絲綢之路的信息樞紐和信息共同體的重要平台。」[65]

習近平於 2015 年在博鰲論壇時提出「中國-東協命運共同體」推動區域網絡資訊基礎設施建設；尊重各國網路主權，推動建立多邊的國際網路治理體系；維護網路安全，防範網路攻擊和公民合法權益；共同打擊網路恐怖主義活動及網路犯罪活動；利用網際網路加強經貿、人文、科技等各領域合作。[66]

〈 https://www.fmprc.gov.cn/web/gjhdq_676201/gjhdqzz_681964/dmldrhy_683911/zyjhywj_683921/t1510228.shtml〉。(檢索日期 2020 年 4 月 10 日)。

[63] 陳時勇、于洪羽，〈雲南、廣西參與國際區域合作，實施一帶一路戰略的平台和機制比較研究〉，《東南亞縱橫》，2015 年 7 月，頁 51-52。

[64] 鄭怡君、薛志華，〈中國-東盟網路安全合作及其布局〉，《東南亞南亞研究》，2017 年，第 2 期，頁 17-18。

[65] 新華社，〈魯煒:打造中國—東盟信息港 建設 21 世紀「海上絲綢之路」的信息樞紐〉，《文匯網》，2014 年 9 月 18 日。〈http://news.wenweipo.com/2014/09/18/IN1409180073.htm〉。(檢索日期 2020 年 4 月 10 日)。

[66] 新華社，〈中國東盟攜手邁向命運共同體〉，《新華網》，2015 年 10 月 12 日。〈http://www.xinhuanet.com/world/2015-10/12/c_128306979.htm〉。(檢索日期 2020 年 4 月 10 日)。

「中國-東協信息港股份有限公司」於 2016 年 6 月，由中國大陸國務院批准，在廣西南寧正式掛牌上市，強調「多方入股、市場化導向」等以結合市場、資本與創新技術為目標，對外和馬來西亞、印尼、泰國和越南等網路企業建立合作關係，對內則與各地方政府簽署合作協定，反映出中國大陸有意採取政策與產業雙軌並進的方式，培育新興及中小企業發展，形成資訊產業聚落。[67]

整體而言，「中國-東協信息港」作為「21 世紀海上絲綢之路」的重要一環，正為一帶一路導入更多網路資訊元素，期望透過網路資訊的建設和產業發展，強化中國大陸和東協在電子商務領域就網路安全合作與成員國展開溝通交流，藉以深化區域內國家在經貿與網路經濟安全領域的合作與互信，輔助一帶一路的推展。

最後，網路安全的法律制度是維護網路空間安全、防範網路攻擊與犯罪的重要保障。網路空間仍是無政府狀態，尚未制定規則來防範，東協成員國在資訊通訊技術的普及帶來網路安全的嚴重挑戰，尤其新加坡和馬來西亞的網際網路普及率已達已開發國家水準，越南、菲律賓和泰國都高於亞洲平均水準。網路普及造成馬來西亞從 2007 年到 2016 年，網路犯罪案件從 1139 起增加到 4738 起，損失約 1893 萬人民幣。新加坡有關電子商務

[67] 人民網，〈中國-東盟信息港股份有限公司成立，構築信息絲綢之路〉，《人民網》，2016 年 6 月 19 日。〈http://gx.people.com.cn/n2/2016/0619/c179430-28531189.html〉。(檢索日期 2020 年 4 月 10 日)。

詐騙案從 2013 年到 2014 年增加 504 起等網路犯罪案件層出不窮。[68]至此，大量的網路犯罪案件伺服器均設在境外，單憑一國的力量難以打擊犯罪，國家勢必要相互合作。

為打擊網路犯罪「中國-東協電信部長會議」透過發表「中國-東協成員國總檢察長會議聯合聲明」強調加強合作，共同打擊國家間和區域間網路犯罪、網路安全相關威脅及其他跨國有組織犯罪。[69]簽署《關於非傳統安全領域合作諒解備忘錄》雙方在打擊販毒、非法移民、海盜、恐怖主義、網路犯罪等跨國犯罪進行密切合作。簽署聯合聲明及備忘錄等形式宣示打擊跨國網路犯罪的決心，並運用刑事司法協助制度，引渡、取證、逮不犯罪嫌疑人等領域展開合作，避免犯罪份子消遊法外，對於維護網路空間秩序有重要作用。[70]

中國大陸與東協發展關係存在著諸多的因素，這會影響網路空間合作的深入發展進而影響網路安全領域的互信，以下區分三點來講述中國大陸與東協的問題及挑戰。

首先，領土爭議問題影響網路安全互信。近年來，中國大陸經濟飛速發展使得越南和菲律賓與中國大陸有南海爭端的問題，對於中國大陸推行的「一帶一路」深感壓力，擔心中國大陸崛起後，在南海問題更趨強硬。

[68] 袁正清、蕭瑩瑩，〈網路安全治理的東盟方式〉，《當代亞太》，2016 年 2 期，頁 83-84。
[69]〈第十一屆中國—東盟成員國總檢察長會議聯合聲明〉，《中國最高人民法院網》，2018 年 9 月 27 日。〈http://www.ca-pgc.org/xdxy/201809/t20180927_2370625.shtml〉。(檢索日期 2020 年 4 月 10 日)。
[70] 鄭怡君、薛志華，〈中國-東盟網路安全合作及其布局〉，《東南亞南亞研究》，2017 年，第 2 期，頁 18。

隨著，時任美國總統歐巴馬提出「重返亞太」之際，希望借助美國的力量並積極拉攏日本、印度等國介入南海問題，遏止和牽制中國大陸的發展。因此，南海爭端是造成中國大陸與東協關係破裂的因素之一，對於展開網路安全領域的合作造成程度影響。[71]

其次，東協成員國內網路資訊化程度參差不齊。從網路應用上，東協地區 6 億人口中，使用網路用戶數不足 2 億，網路普及率低於 30%。從網路用戶數，東協成員國之間用戶數量分布不均。汶萊、馬來西亞、新加坡網路用戶數較多。反之，緬甸、柬埔寨等國網路用戶數偏低。網路用戶數量和資訊設備差異會擴大數位落差，影響網路安全的深入合作。[72]正如，習近平所言：「金融、能源、電力、資訊、交通等領域關鍵的基礎設施是經濟運行的神經中樞，是網路安全的重中之重。」[73]在一帶一路的推進下，中國大陸與東協拓展經貿、基礎設施、能源領域的合作，勢必推展關鍵資訊基礎設施建設，藉以提升東協地區網路安全領域的合作。

最後，中國大陸與東協對於網路空間意識形態的界定存在差異。由於東協國家在歷史、文化和社會發展狀況不同，對於網路空間界定、網路資訊保護、網路犯罪等問題存在分歧。在穆斯林佔人口多數的印尼，政府將網路上的色情內容和反伊斯蘭言論視為威脅，並要求網路提供商暫停網站

[71] 劉靜主編，《網路強國推進器-網絡空間國際合作共建》，（北京：知識產權出版社，2018 年 7 月），頁 124。
[72] 孫偉、朱啟超，〈東盟網路安全合作現狀與展望〉，《東南亞研究》，2016 年，第 1 期，頁 18。
[73] 〈習近平：金融、能源是關鍵的基礎設施是網路安全的重中之重〉，《中國能源網》，2016 年 9 月 23 日。〈http://www.cnenergynews.cn/tt/201609/t20160923_385773.html〉。(檢索日期 2020 年 4 月 10 日)。

的影片共享功能，以阻止一部反伊斯蘭電影的傳播。而做為君主立憲的泰國，將網路上汙辱或威脅國王及王室行為視為安全威脅，因此多次關閉 Youtube 等社群媒體。但在受到美國自由主義影響較深的菲律賓，政府將視為言論自由，並未構成安全威脅。[74]在網路社群媒體批評政府等意識型態問題卻是中國大陸認定網路犯罪。其各國文化、宗教和意識形態的迥異，會影響中國大陸與東協在網路安全的合作。

中國大陸與東協僅通過會議等形式重申對於網路恐怖主義及網路犯罪的打擊與合作外，尚未制定合作機制。由於國家之間不僅是資訊設備的差距和意識形態的分歧，或是對於網路主權的問題，使得網路合作機制尚未通過對話協商，形成代表立場的法律文件，這使得中國大陸與東協缺乏必要的法律指引，消除網路空間問題的分歧。

綜合上列所述，「中國-東協信息港」已有雛型，中國大陸政府在國際合作上力推動「網際網路+東協」，推動東協的網路發展速度。目前廣西壯族自治區的南寧市成為中國大陸國家級跨境貿易電子商務的試點城市，引入「京東」、「騰訊」、「阿里巴巴」等電商企業，與越南、馬來西亞等國家建立合作關係。[75]此外，作為「中國-東協信息港」運用的北斗系統，也積極

[74] 袁正清、蕭瑩瑩，〈網路安全治理的東盟方式〉，《當代亞太》，2016 年 2 期，頁 83-84。

[75] 〈阿里巴巴馬來西亞辦公室開幕〉，《人民網》，2018 年 6 月 19 日。〈http://world.people.com.cn/n1/2018/0619/c1002-30064814.html〉。(檢索日期 2020 年 4 月 10 日)。

參與並深化與東南亞各國在衛星導航應用的交流與合作，提升北斗系統在東南亞地區的服務能力。[76]

網際網路成為繼陸運、海運、航運後連接中國與東南亞各國的絲綢之路，中國大陸就土地面積、人口和經濟總量來看，在東亞地區無疑是大國，同時也會持續採取攻勢獲取權力，這權力包含經濟和外交，同時中國大陸也關切東南亞各國一方面運用經貿領域，獲得中國大陸發展帶來的商機，另一方面又引入美國、印度和日本制衡中國大陸的崛起。中國大陸積極運用「一帶一路」、「中國-東協信息港」將電子商務等企業引入東南亞各國獲得財富，維持經濟高速成長，使得中國大陸逐漸成為區域霸權，試圖改變美國在亞太地區的領導地位。

肆、小結

近年因網路攻擊事件頻傳和美國的稜鏡計畫，使習近平更加強調參與網路空間區域組織的規則制定是對中國大陸發展至關重要。中國大陸國務院於 2016 年 3 月通過《中華人民共和國國民經濟和社會發展第十三個五年規畫綱要》，明確指出要積極參與網路、深海、極地、太空等領域國際規則制定。[77]中國大陸外交部及國家互聯網信息辦公室於 2017 年 3 月 1 日發佈

[76] 彭茜，〈中國北斗衛星導航定位系統將“照亮”東盟 10 國〉，《中國軍網》，2017 年 3 月 30 日。〈http://www.81.cn/jwgz/2017-03/30/content_7545156.htm〉。(檢索日期 2020 年 4 月 10 日)。

[77] 中華人民共和國國務院，〈中華人民共和國國民經濟和社會發展第十三個五年規畫綱要〉，《新華社》。2016 年 3 月 17 日。〈http://www.xinhuanet.com//politics/2016lh/2016-03/17/c_1118366322.htm〉，（檢索日期：2020 年 3 月 12 日。）

《網路空間國際合作戰略》，提出要推動網路空間國際法治，主張在聯合國框架下制定各國家普遍能接受的網路空間國際規則和國家行為規範，推動建構以規範為基礎的網路空間秩序。[78]

習近平認為網路空間現已成為陸地、海洋、空中和太空之外的第五空間，是國家主權延伸的新疆域，網路空間的國際規則制定關係到中國大陸的核心利益。首先是網路安全是全球性的議題，任何國家不能獨善其身，因網路安全是跨國性、威脅滲透廣泛等特點，但目前東協及上合組織成員國普遍存在網路安全防護能力薄弱，難以有效應對國家及組織的高強度網路攻擊，是必要加強國際合作以面對網路安全的威脅。[79]

其次是，中國大陸在網路空間裡，運用外交參與雙邊與多邊外交活動與國際規則制定。習近平於 2013 年 3 月 24 日在莫斯科國際關係學院發表《順應時代前進潮流，促進世界和平發展的》的演講中提出「和平、發展、合作、共贏成為新時代潮流。」[80]中國大陸要通過與上合組織和東協在網路空間領域創設議題到主導議程，實踐中國大陸「網路空間國際合作戰略」。其目的是，一是標榜美國是唯一網路超強國家是霸權主義，呼籲東協和上合組織等開發中國家尊重網路主權、支持聯合國在網路空間國際規則的建構下發揮主導地位，和推動開發中國家參與網路空間國際規則制定。二是

[78] 中國外交部及國家互聯網信息辦公室，〈網路空間國際合作戰略〉，《新華社》，2017 年 3 月 1 日。〈http://www.xinhuanet.com//politics/2017-03/01/c_1120552767.htm〉，（檢索日期：2020 年 4 月 8 日。）

[79] 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 18。

[80] 〈國家主席習近平在莫斯科國際關係學院的演講〉，《中華人民共和國人民府網》，2013 年 3 月 24 日。〈http://www.gov.cn/ldhd/2013-03/24/content_2360829.htm〉，（檢索日期：2020 年 3 月 15 日。）

利用其在聯合國常任理事國的地位，與上海合作組織成員國共同提交《資訊安全國際行為準則》，對美國領導的國際政治進行牽制與弱化，使中國大陸能從地區性大國走向全球性大國，進入國際政治的舞臺中心，達到兩個一百年的民族復興目標。[81]

最後，增加網路空間治理的話語權和提升國際地位。話語（discourse）源於 1970 年法國後現代主義思想家福科（Michel Foucault）於（College de France）演講《話語的秩序》提出話語即權力。外交上有兩重意義，即是外交話語權利與外交話語權力。外交話語權利（discourse right）是國際社會主權國家都享有的權利。而外交話語權力（discourse power）是指一個國家對他國的影響和威脅。話語權展現的是國與國之間的地位，實力的角逐。[82]

長期以來，美國為首的西方國家是國際外交話語的生產者及傳播者，美國憑藉著在國際組織和機制的主導權，去設置議題和主導議程，利用傳統媒體與網路社群媒體壟斷國際話語走勢，強推美國思想和價值觀等，增強在他國的政治影響力。[83]然而，中國大陸等開發中國家實力提升，其話語權也逐步增加。中國共產黨於十八屆三中全會通過《中共中央關於全面深化改革若干重大問題的決定》強調加強國際傳播能力和話語權的建立和積

[81] 楊志恆，〈中共外交的策略與原則〉，《中國大陸研究》，1999 年 10 月，第 42 卷，第 10 期，頁 42。
[82] Michel Foucault，《話語的秩序》，許寶強、袁偉選編《語言與翻譯的政治》，（北京：中央編譯出版社，2001 年），第 7 頁。
[83] 楊潔勉，〈中國特色大國外交和話語權的使命與挑戰〉，《國際問題研究》，2016 年，第 5 期，頁 26。

極參與全球治理，融入全球治理體系。[84]顯現在從參與由美國主導的北大西洋公約組織塔林手冊制定、主導上合組織網路空間安全合作和掌握東協資訊港的建設等議題上，從話語權利，轉變為話語權力，正是彰顯攻勢現實主義推論下中國大陸在國際場合地位的提升有助於權力最大化。

第三節 中國大陸增加國際網路空間及多邊會議之角色

中國大陸政府近年來致力於參與聯合國與區域性國際組織漸具有主導性，透過舉辦國際會議、提出國際倡議和主動設置國際議程等方式，試圖將「網絡主權」等理念傳達至其中，而在中國大陸政府主導的「世界互聯網大會」和透過主辦國際活動「G20 元首峰會」、「金磚元首峰會」等，這些作為不僅展現中國大陸在參與國際網路治理的影響力與日俱增，也間接重塑國際網路運行規則，試圖改變美國與歐洲等國家的主導地位。本節以攻勢現實主義探討中國大陸參與其他國際活動等實際案例。

在虛擬、自由的網路空間中，政府合法監控網路用戶的數據資料權力，勢必會影響到現行網路空間秩序，但隨著雲端技術、物聯網和手機移動通訊的發展，數據資料已成為戰略資源。因此，建構數據管理，強化國家在網路空間的監管責任，以成為中國大陸維護網路安全的重要手段。

根據 2010 年中國大陸《中國互聯網狀況白皮書》首度指出，維護網路安全，是保障國家安全與維護社會公共利益的必然要求；在中國大陸境內

[84] 新華社，〈中共中央關於全面深化改革若干重大問題的決定〉，《中華人民共和國中央人民政府網》，2013 年 11 月 12 日。〈http://www.gov.cn/jrzg/2013-11/15/content_2528179.htm〉，（檢索日期：2020 年 3 月 15 日。）

的網際網路屬於國家主權管轄範圍內，應受到尊重和維護。[85]隨後於 2015 年 7 月 1 日第十二屆全國人大常委會第十五次會議通過的《中華人民共和國國家安全法》，首次明確「網路空間主權」概念，規定:「加強網路管理，防範、制止和依法懲治網路攻擊、網路入侵、網路竊密等違法犯罪行為，維護國家網路空間主權、安全和發展利益。」[86]由中國大陸宣示網路主權的行為，突顯出數據資訊傳播的自由，對中國大陸內部的政治穩定已造成極大的威脅。

網路主權的定義，依據聯合國於 2013 年 6 月 24 日《從國際安全的角度來看資訊和電信領域發展政府專家組》（United Nations General Assembly）決議內容第 20 條指出：國家對在其領土內對資訊、通訊技術基礎設施具有管轄。[87]另外，2015 年聯合國大會的政府專家組指出：「在使用資訊通信技術時，各國必須遵守其他原則中的國際法、國家主權，以和平手段解決紛爭，並且不干預其他國家的內部事務。」[88]因此，在資訊網路技術等關鍵基礎設施被視為國家主權範疇後，網路主權概念在未來處理網路安全爭議性的問題時扮演極為重要的角色。

[85] 〈中國互聯網狀況白皮書〉，《國務院新聞辦公室網》，2010 年 6 月。〈http://www.scio.gov.cn/tt/Document/1011194/1011194.htm〉，（檢索日期：2020 年 3 月 15 日。）

[86] 〈《中華人民共和國國家安全法》〉，《人大新聞網》，2015 年 7 月 10 日，〈http://npc.people.com.cn/BIG5/n/2015/0710/c14576-27285049.html〉。(檢索日期 2019 年 11 月 1 日)。

[87] 聯合國大會，〈從國際安全的角度來看資訊和電信領域發展的政府專家組的報告 A/65/201〉，《聯合國第 65 屆會議》，2010 年 7 月 30 日，頁 4-8。

[88] 聯合國大會，〈從國際安全的角度來看資訊和電信領域發展的政府專家組的報告 A/70/174〉，《聯合國第 70 屆會議》，2015 年 7 月 22 日，頁 6-11。

中國大陸學者方濱興認為網路主權有四個方面：一維護本國網路獨立運營，無需受制其他國家的獨立權；二網路之上各主體互聯互通、互相尊重的平等權；三保護本國網路免於攻擊和打壓的防衛權；四主權者對網路的維護管理權。[89]由中國大陸形塑出網路主權概念得知，凡是連接進入中國大陸境內的網路空間中均為管轄對象，也意涵著隨著中國大陸國力擴張，所包含的跨境網路電商、移動通訊等企業遍布全球和國防武力佈署全世界，其網路空間的疆域也隨之擴大。[90]

中國大陸宣告網路主權的目的，在於網路安全已威脅到中國大陸維護國家主權、安全及利益。為實現「網路強國」和「中國夢」，須建構安全的網路空間秩序。

首先，增加國際政治影響力。主權意味著以國家行為者，在其境內具有最高的統治權。根據 2016 年底公布，《國家網路空間安全戰略》指出，網路空間已成為國家主權的新疆域，確保在自由、開放的網路空間中維護國家主權、安全與發展利益，實現網路強國的戰略目標。同時，參與國際網路空間規則制定，形塑負責任的大國形象。從宣揚網路主權的概念，由政府去主導網路規則的制定並透過多邊的外交手段積極參與聯合國其附屬機構、區域組織和國際元首峰會。

[89]〈人民日報權威論壇：網絡主權，一個不容迴避的議題〉，《人民網》，2014 年 06 月 23 日。〈http://opinion.people.com.cn/n/2014/0623/c1003-25183666.html〉，（檢索日期：2020 年 3 月 12 日。）

[90] 王清安、黃基禎，〈中共對網路空間主權之概念與作為〉，《中國大陸研究》，第 62 卷第 1 期，2018 年，頁 71。

中國大陸透過主辦二十國集團峰會（Group of Twenty, G20，以下簡稱G20）[91]和金磚五國峰會[92]宣揚網路主權的概念。前者 G20 峰會自 2008 年成立以來，一共舉行 10 次峰會，自 2010 年韓國首爾舉辦後，2016 年再次由亞洲國家中國大陸杭州市舉辦,是中國大陸建政以來層級最高的一場峰會，身為世界第二大經濟體和經濟增長快速的開發中國家代表，中國大陸不僅與肩負替開發中國家發言及試圖改變由美國主導的國際網路規則制定的任務。

其峰會主要討論世界經濟、貿易和投資、數位經濟等議題。在峰會期間各國元首共同簽署《二十國集團數位經濟發展與合作倡議》，這是全球首個由多國元首共同簽署的數位經濟政策文件，強調 G20 各成員國應積極倡導尊重各國網路主權，維護網路空間安全可信並弭平開發中國家與已開發國家在網路科技領域的數位鴻溝。以聯合國關於網路主權的公約制定為基礎，推進國際公約的制定，保障各國自主選擇適合國情的網路發展道路、網路治理模式、自主制定網際網路公共政策和平等參與國際網路空間治理

[91] G20 是一個國際經濟合作論壇，於 1999 年 12 月 16 日在德國柏林成立，屬於布雷頓森林體系框架內對話的一種機制，由七國集團（加拿大、美國、英國、法國、德國、義大利、日本），金磚五國（巴西、俄羅斯、印度、中國、南非），七個重要經濟體（墨西哥、阿根廷、土耳其、沙烏地阿拉伯、韓國、印度尼西亞、澳大利亞），以及歐聯組成。參考來源：嚴震生，〈杭州 G20 峰會與「中國方案」〉，《展望與探索》，第 14 卷第 10 期，2016 年 10 月，頁 1-2。

[92] 金磚五國（BRICS）是指五個主要的新興市場國家，分別為巴西、俄羅斯、印度、中國、南非，2001 年，其來源是由美國高盛公司首席經濟師吉姆·奧尼爾（Jim O'Neill）首次提出來自這四個國家的英文國名開頭字母所組成的詞 BRIC，後來加入南非，合稱金磚五國。〈金磚國家〉，《中華人民共和國外交部》，2019 年 12 月。〈https://www.fmprc.gov.cn/web/wjb_673085/zzjg_673183/gjjjs_674249/gjzzyhygk_674253/jzgj_674283/gk_674285/〉。(檢索日期 2020 年 5 月 1 日)。

的權利。[93]而身為主辦國的中國大陸，從峰會的安排、議題的設定，「中國方案」的宣布及雙邊會議的安排等，顯現出中國大陸已擺脫過去韜光養晦時期，正式進入習近平有所作為的時代，並積極將網路主權等議題納入合作倡議中，彰顯出中國大陸在國際組織中日益重視的角色及國際規則制定的主導性。

後者，金磚五國領導人於 2017 年 9 月 4 日在廈門會晤並公布《廈門宣言》。[94]金磚五國從 2013 年南非《德班宣言》（Durban Declaration）、2014 年巴西《福塔萊薩宣言》（Fortaleza Declaration），到 2015 年俄羅斯《烏法宣言》（Ufa Declaration）、2016 年印度《果阿宣言》（Goa Declaration），再到 2017 年中國《廈門宣言》（Xiamen Declaration），五國領導人表示，支持聯合國在制定網絡空間行為規範方面發揮中心作用，強調《聯合國憲章》確立的國際法原則，認為要在聯合國主導下制定國際法律規範，打擊資訊通信技術領域的犯罪行為。因此，其政治目的是形塑網路主權，並透過建構網路空間的新秩序，形塑中國大陸的國際形像，將利於提升國際政治的影響力。

其次，提升數位經濟競爭力。隨著數位經濟的整合，網路主權的建構，有利於網路科技自主化的發展，提升市場占有率。根據 2015 年 10 月 29 日

[93]〈《二十國集團數位經濟發展與合作倡議》〉，《G20 官方網站》，2016 年 09 月 20 日。〈http://www.g20chn.org/hywj/dncgwj/201609/t20160920_3474.html〉。(檢索日期 2020 年 5 月 1 日)。

[94]〈金磚國家領導人廈門宣言〉，《新華網》，2017 年 09 月 04 日。〈http://www.xinhuanet.com/world/2017-09/04/c_1121603652_2.htm〉。(檢索日期 2020 年 5 月 1 日)。

《中國共產黨第十八屆中央委員會第五次全體會議公報》指出，為實現網路強國戰略目標，須推動「互聯網+」行動計畫。2016 年《中華人民共和國國民經濟和社會發展第十三個五年規劃綱要》第六篇拓展網路經濟空間更指出:「加快建立網路空間應用的基礎共性標準,和關鍵技術標準研製推廣，將增強國際標準制定中的話語權。」[95]2016 年 7 月 27 日公佈《國家資訊化發展戰略綱要》到 2025 年，建設國際領先的移動通訊網路，改變核心關鍵技術受制於人的局面，培養具有國際競爭力的網路資訊企業。[96]

中國大陸大力扶植的企業華為是全球第一大通訊設備公司，2017 年總營收高達 6,036 億人民幣，年增長率 15.7%、淨利達 457 億人民幣，年增長率 28.1%。旗下的業務分為三大類：第一大營收來源為電信商業務，包含銷售電信設備，像是傳統基地台、路由器以及 5G 相關設備銷售，主要競爭者為 Ericsson 及 Nokia。第二大智慧型手機品牌，僅次於全球 Samsung 市占比 14.6%，包含自家的麒麟（Kirin）行動處理器的研發及銷售、筆記型電腦、數據機、穿戴式裝置等，主要競爭者是 Samsung 及 Apple。第二大企業通訊設備商,全球市占比25.6%,僅次於Cisco。業務涵蓋電腦、乙太交換器（Switch）及通訊設備對企業銷售，競爭對手是 Cisco 及 Hewlett Packard Enterprise

[95]〈《中華人民共和國國民經濟和社會發展第十三個五年規劃綱要》〉,《新華網》, 2016 年 03 月 17 日。〈http://www.xinhuanet.com//politics/2016lh/2016-03/17/c_1118366322.htm〉(檢索日期 2020 年 5 月 1 日)。

[96] 中共中央辦公廳、國務院辦公廳,〈《國家信息化發展戰略綱要》〉,《中華人民共和國中央人民政府站》,2016 年 7 月 27 日。〈http://big5.www.gov.cn/gate/big5/www.gov.cn/gongbao/content/2016/content_5100032.htm〉。(檢索日期 2020 年 4 月 11 日)。

（HPE）已經帶給這些公司極大的市場威脅。[97]因此，建構網路主權，其經濟目的，將有助扶植其國內網路科技產業的競爭力，改變核心關鍵技術受制於人的局面，達到網路強國的目標。

最後，主導網路空間國際會議。中國大陸於 2014 年舉辦第一屆世界互聯網大會（World Internet Conference , WIC），至今已舉辦六屆。中國大陸重視及發展網路治理，將政治、經濟、文化、社會、軍事等資訊化和網路安全等問題，做出決策。到中國共產黨第十九次全國代表大會提出「加快佈署網路基礎設施，大力培育網路創新能力，務實推動網際網路產業發展，不斷開發互聯網應用潛力，打造網路強國」。[98]

中國大陸舉辦世界互聯網大會，能夠增加「中國大陸方案」的傳播力可從中國大陸內部和國際兩個層次進行分析。首先，內部層面。中國大陸舉辦世界互聯網大會，表示自從 1994 年接入全球網際網路開始至今習近平主政時期對網路的重視已從過去的被動轉向主動，從建立「中共中央網絡安全和信息化領導小組」，到立法層面通過《國家安全法》和《網路安全法》，和頒布《網路空間安全戰略》和《網路空間國際合作戰略》，彰顯出中國大

[97] 寫點科普 Lynn，〈沒美國施壓，這些國家都差點用華為 5G 設備，看懂華為 5G 霸權崛起的 3 大關鍵〉，《商業週刊》，2018 年 12 月 18 日。〈https://www.businessweekly.com.tw/business/blog/24584〉，（檢索日期：2020 年 4 月 12 日。）

[98] 新華社，〈習近平：決勝全面建成小康社會 奪取新時代中國特色社會主義偉大勝利——在中國共產黨第十九次全國代表大會上的報告〉，《中華人民共和國中央人民政府網》，2017 年 10 月 27 日。〈http://www.gov.cn/zhuanti/2017-10/27/content_5234876.htm〉，（檢索日期：2020 年 3 月 12 日。）

陸在網路治理中的決心，反映中國大陸對自身在國際社會中定位有所調整，要從網路大國邁向網路強國。

世界互聯網大會召開，能夠讓世界各國客觀瞭解中國大陸網路發展狀況，並藉由這一平台有效增進不同國家與地區的共識，並在制定全球網路空間國際機制的過程中增強自身的話語權，並嘗試扮演領導者的角色，主導參與國際機制的創設。[99]

後者，國際層面而言。網路空間為無政府狀態，網路空間是人類生產、生活的新空間，更是國家間競爭的全新戰場，各國之間國情不同、發展階段有別、面臨的挑戰相異，因此，全球網路空間治理存在一定分歧，而中國大陸藉由世界互聯網大會以多邊主義的合作姿態，應對美國為首的單邊主義，探討網路空間議題及資訊科技領域，進和緩解全球網路空間無政府狀態。

從 2015 年第二屆世界互聯網大會，習近平在開幕儀式上表示網路世界和現實世界一樣，追求自由的同時，也要維持秩序。他呼籲，各國都應該尊重彼此的「網路主權」，強調《聯合國憲章》確立的主權平等原則，其原則和精神也應適用於網路空間，尊重各國自主選擇網路發展道路、網路管理模式等權利。同時，網路空間是繼領土、領海、領空與太空後的「第五

[99] 余麗、趙秀贊，〈中國貢獻：國際機制理論視域下的：世界互聯網大會〉，《河南社會科學》，2019 年 5 月，第 27 卷第 5 期，頁 2。

疆域」。習近平強調，網路空間不應成為各國角力戰場，並提出「尊重網絡主權、維護和平安全、促進開放合作、建構良好秩序」四原則，主導網路話語權意味濃厚。[100]

至 2018 年第五屆世界互聯網大會，中國大陸網路空間研究院與美國智庫布魯金斯學會（Brookings Institution）探討「網路空間中美關係」共同就網際網路治理與網路空間國際秩序的技術層面和政策層面展開對話。[101]

世界互聯網大會從 2014 年舉辦至今，所面臨的現實挑戰以下分為三方面：其一，在全球網路使用人數上中國大陸等開發中國家網路用戶數已高於已開發國家，但在全球網路治理卻無話語權。截至 2019 年 12 月歐洲網路用戶數占全球網路用戶數比率為 10.7%，北美地區網路使用數為 4.7%兩區域相加為 15.4%(參照表 4-2)，相較於亞洲網路使用比率 50.3%高出 39.1%，尤其中國大陸 2019 年 8 月公布《第 44 次中國互聯網絡發展狀況統計報告》顯示中國大陸網路用戶數規模已達 8.54 億人，網路普及率達 61.2%，[102]以高出北美地區及歐洲兩倍多，但美國及歐洲仍在網路空間治理中掌握話語權。

[100]〈習近平出席第二屆世界互聯網大會開幕式並發表主旨演講〉，《中華人民共和國國家互聯網信息辦公室網》，2015 年 12 月 16 日。〈http://www.cac.gov.cn/2015-12/16/c_1117480642.htm〉，（檢索日期：2020 年 3 月 12 日。）

[101] 世界互聯網大會，〈互聯網國際高端智庫論壇探討「網路空間的中美關係」〉，《世界互聯網大會網》，2018 年 11 月 09 日。〈http://2018.wicwuzhen.cn/web18/release/release/201811/t20181109_8705733.shtml〉，（檢索日期：2020 年 3 月 12 日。）

[102] 中國互聯網絡信息中心，〈第 44 次中國互聯網絡發展狀況統計報告〉，《中華人民共和國國家互聯網信息辦公室網》，2019 年 8 月。〈http://www.cac.gov.cn/pdf/20190829/44.pdf〉，（檢索日期：2020 年 3 月 12 日。）

表 4-2 全球網際網路用戶數和人口統計表（2019 年 12 月）

世界地區	人口數(2019)	佔世界人口比例(%)	網路用戶人數	普及率	網路用戶占世界總數比例(%)
非洲	1,340,598,447	17.2%	526,374,930	39.3%	11.5%
亞洲	4,294,516,659	55.1%	2,300,469,859	53.6%	50.3%
歐洲	834,995,197	10.7%	727,814,272	87.2%	15.9%
中南美洲	658,345,826	8.5%	453,702,292	68.9%	10.0%
中東地區	260,991,690	3.9%	180,498,292	69.2%	3.9%
北美地區	368,869,647	4.7%	348,908,868	94.6%	7.6%
大洋洲	42,690,838	0.5%	28,775,373	67.4%	0.6%
總計	7,796,615,710	100%	4,574,150,134	58.7%	100%

筆者自製。參考來源：Internet Usage and World Population Statistics estimates are for, *Internet World Stats*, Dec 31, 2019,< https://www.internetworldstats.com/stats.htm>

其二，中國大陸政府在世界互聯網大會主張由各國政府代表參與制定的網路治理模式與美國採取由多元利益關係人團體組成決策機制的「多利益相關方模式」有所分歧。全球網路的服務提供者如伺服器、光纖、網路資訊服務等都是屬於私人企業，因此 MSG 模式經由個人、企業、非政府組織和政府，係由下對上形成決策模式，產生共識後形成網路政策，在網路治理的相關組織如國際組織 ICANN、聯合國 IGF 等都採行的網路治理機制。[103]

[103] 黃勝雄，〈從 ICANN 多元利益關係人(Multistakeholders) 之架構談未來網路治理〉，《臺網中心電子報》，2014 年 5 月。〈http://www.myhome.net.tw/2014_05/p02.htm〉，（檢索日期：2020 年 3 月 12 日。）

相較於中國大陸對於推動以政府為主體的多邊網路治理模式，係因中國大陸網路電信公司均由政府主導的國營企業或是取得發行執照的私人企業，是上對下的決策模式。早在 2005 年突尼斯舉行的資訊社會世界峰會，中國大陸代表黃菊就已提出網路治理遵循政府主導、多方參與原則。[104]經過歷屆互聯網大會的提倡，仍無法取代「多利益相關方模式」，理由在於中國大陸的網路生態是自我封閉也缺乏與全球網路「共通互連」，美國等西方的私人機構與政府，亦不支持中國大陸政府的多邊網路治理的作法。因此，中國大陸政府透過世界互聯網大會向開發中國家，宣揚國家主權適用於網路空間和由政府主導參與網路治理的多邊模式，以便與美國等西方國家爭奪網路空間治理的主導權與話語權。

其三，箝制言論自由疑慮。甫於 2014 年浙江省烏鎮市開幕的世界互聯網大會，首屆是由國務院總理李克強出後，第二屆世界互聯網大會由中國大陸國家主席習近平與各國領袖，如俄羅斯、塔吉克等上海合作組織，或開發中國家網路部門負責人，及各國相關網路企業和專家學者等。唯獨美國網路巨擘 Google、Facebook 等企業未出席大會。因中國大陸政府利用發行合法執照限制網路公司，只能按照政府法令，提供審查過濾的資訊，以控制民眾網路言論，但美國 Google、Facebook 等外國企業多半秉持捍衛自

[104]〈黃菊在信息社會世界峰會突尼斯階段會議上講話〉，《中央政府門戶網站》，2005 年 11 月 17 日。〈http://www.gov.cn/ldhd/2005-11/17/content_101716_2.htm〉，（檢索日期：2020 年 4 月 12 日。）

由開放的網路環境，不願配合中國大陸政府的網路審查進而退出中國大陸市場。

近年中國大陸政府對網路傳播的管制愈加嚴控，中國大陸國家互聯網辦公室公布《互聯網信息搜索服務管理規定》，要求網路資訊搜索服務提供者建立資訊審核、公共資訊實時巡查等資訊安全管理制度。[105]例如中國大陸企業百度、阿里巴巴和騰訊等網路平台企業，必須符合中國大陸政府的「自我審查」的表現。[106]誠如《紐約時報》〈烏鎮互聯網大會與科技的陰暗面〉介紹，騰訊高層表示會定期向政府報告在平台上發現的非法活動，政府可隨時向騰訊等企業索取用戶個人資料。中科虹霸公司的高層表示與新疆有關部門合作，建立所有新疆居民的視網膜數據庫。[107]

隨著中國大陸網路的普及與深入社會，藉由電子商務等網路新創產業的應用推動經濟發展，中國大陸政府勢必保障網路資訊流通，並協助網路企業向海外發展。然而，依據攻勢現實主義之假設，中國大陸政府推出《國家安全法》和《網絡安全法》等多項限制網路活動的重大法案和行政規範文件，反映中國大陸政府對網路應用，使得國內社會急速發展下危及到政治穩定的疑慮，採用攻勢作為獲取權力，因此藉由主導國際會議的形式，

[105]〈互聯網信息搜索服務管理規定〉，《中國網信網》，2016 年 6 月 25 日。〈http://www.cac.gov.cn/2016-06/25/c_1119109085.htm〉，（檢索日期：2020 年 4 月 12 日。）

[106] 張裕亮，〈第二屆世界互聯網大會評析〉，《展望與探索》，2016 年 1 月，第 14 卷第 1 期，頁 19-20。

[107] Raymond Zhong，〈烏鎮互聯網大會與科技的陰暗面〉，《紐約時報中文網》，2018 年 11 月 9 日。〈https://cn.nytimes.com/china/20181109/china-world-internet-conference/zh-hant/〉，（檢索日期：2020 年 4 月 12 日。）

舉辦世界互聯網大會試圖拉攏上海合作組織會員國或是一帶一路沿線開發中國家，在國際會議中提倡以政府為主體的多邊網路治理模式和宣揚網路主權的概念，並藉由「一帶一路」的戰略規劃，試圖打造「全球數位極權同盟」，引發美國為首的國家所芥蒂的。[108]

[108] 吳介聲，〈中共封網、萬人翻牆：世界互聯網大會，淪極權科技採買會？〉，《聯合新聞網》，2019 年 10 月 24 日。〈https://opinion.udn.com/opinion/story/120611/4123796〉，（檢索日期：2020 年 3 月 12 日。）

第五章 結論

本文旨在探究中國大陸網路空間戰略，以「攻勢現實主義」為研究途徑，探討網路空間處於一個無政府狀態體系結構下，中國大陸為追求權力及安全極大化目標，所發展出具有中國大陸特色的網路空間戰略，並搭配文獻分析之研究方法輔以相關數據進行研究。以實際參與聯合國組織及其網路治理平台或區域性組織的案例，來檢視中國大陸網路戰略之作為與成效。

本章結論針對本文第二至四章之研究，第二章先對攻勢現實主義的內涵做出系統性說明，後以攻勢現實主義理論者米爾斯海默的基本假設，來解析中國大陸網路空間國際戰略的作為。第三章以攻勢現實主義推論中國大陸網路戰略內涵及國內運用。第四章中國大陸網路空間戰略影響國際網路規則制定，探討中國大陸透過參與聯合國及其網路治理平台和影響區域性組織網路規則制定及主辦網路空間多邊會議，提出國際合作倡議和創建國際議程等作為，檢視中國大陸網路空間戰略之國際參與的成效分析。在此章的第一節為本文綜合前述章節所得的研究成果，在第二節提出對我國學者未來有意在繼續此議題之相關研究參考。

第一節　研究發現

本研究目的為探討中國大陸網路空間戰略的發展現況和檢視中國大陸影響國際網路規則制定的動機與成效。藉由瞭解中國大陸網路空間戰略內涵，以因應網路安全威脅，從設立中共中央網絡安全信息化小組及國務院體系國家互聯網信息辦公室以提升領導層級，經由國內立法法手段，加強網路空間的監控，以突顯中國大陸政府對其國內網路空間治理管控已有增加趨勢。組織變革中，共軍新成立戰略支援部隊，整合電子、通訊、偵查聯合作戰等方式，借以完善網路部隊攻擊和防禦的能力，以彰顯網路空間與軍隊發展之連動性已密不可分。中國大陸參與國際事務逐漸具有主導性，以參與聯合國、區域性組織和透過舉辦國際會議、提出國際倡議和主動設置國際議程等方式，提升在網路空間的制定權及話語權。以下針對兩項研究目的提出系統性論述

壹、中國大陸網路空間戰略發展內涵

一、解決網路安全威脅

全球網際網路是 20 世紀人類偉大的發明，以網路乘載的新科技正改變著人們，隨著資訊技術的進步，網際網路以全面進入到國家政治、金融、能源、資訊、軍事等各個領域，一旦出現網路漏洞，不僅國家安全遭受到威脅，相關的民生、經濟和資訊系統失靈遭致癱瘓，危及國家安全。中國大陸所面臨的網路安全威脅，區分為國際層面及國內層面。前者，從 1991

年波斯灣戰爭，美軍展示資訊主動權，迅速贏得戰爭。2007 年愛沙尼亞於遭受到大規模的網路攻擊，使國家安全、經濟社會嚴重坍會。美國史諾登披露「稜鏡事件」,美國國家安全局長期監看電子郵件、網路訊息和影片等。上述事件引起中國大陸對網路空間安全的重視，並提出網路空間戰略以因應國際情勢威脅。

後者，國內層面威脅。其一，國內因網路作為新型的傳播媒體，改變傳統的政治生態，拓寬公民訴求和參與政治的管道，網路的流通乘載著美式民主、意識形態和不實訊息危害中國大陸政府執政的合法性，危害政治安全。其二,網路和資訊系統已成為支撐整體經濟和關鍵基礎設施的核心，若遭受網路攻擊，其影響層面拓及交通、金融、能源、社會等基礎設施，嚴重危脅經濟安全。其三，網路資訊技術的發展改變現有的戰爭型態和作戰方式，虛擬的網路空間成為新的戰場，制網權，如同制空、制海、制天一樣，誰能掌控資訊網路，誰就能控制政治、軍事和經濟。敵人的網路部隊可通過網路武器植入電腦病毒，癱瘓對方指揮系統，實現不戰而屈人之兵，威脅到軍事安全。其四，早期恐怖份子以駭客手法，藉電腦病毒進行竊密或是執行實體破壞，然而現今的恐怖份子利用網路進行人員招募、資金募集和理念傳播，危害社會安全。上述呼應攻勢現實主義的假設，生存

是大國的目標，面對網路空間處於無政府狀態，中國大陸政府採取自助的手段來應對網路安全的威脅。

二、中國大陸網路空間戰略特點

現今的網路時代已徹底改變人類生活和生產方式，隨著資訊技術的變革也關係到中國大陸政治、經濟、社會和文化等各個領域的安全。中國大陸在網路空間戰略的建制已刻不容緩。因此，成立「中共中央網絡安全和信息化領導小組」和國務院體系「國家互聯網信息安全辦公室」。習近平擔任小組長於第一次會議時提出，「沒有網路安全就沒有國家安全，領導小組要發揮集中統一的領導作用，協調各個領域的網路安全和資訊化的問題，制定實施國家網路安全和資訊化發展戰略和政策」，隨後公布《國家信息化發展戰略綱要》、《國家網絡空間安全戰略》和《網絡空間國際合作戰略》等三項戰略性文件，彰顯中國大陸領導人對網路空間戰略的重視。

首先頒布《國家信息化發展戰略綱要》，區分為三個階段。第一階段到2020 年，核心關鍵技術部分領域達到國際水準。第二階段到 2025 年建設國際領先的移動通訊網路，改變核心關鍵技術受制於人的局面。第三階段到本世紀中葉，建設成為資訊化社會主義現代化國家。此戰略也呼應攻勢現實主義的假設，中國大陸採取自助的手段，尋求改變現狀，打破由美國科技資訊產業壟斷核心的關鍵技術，打造由自己本國企業自主研發的資訊技術產業體系，逕而成為網路強國。

其次，公布《國家網絡空間安全戰略》。從中國大陸內部和國際層面提升網路空間的防護能力。內部層面著重在掌握核心技術、穩定網路和資訊系統、培養網路安全人才，藉以提升網路安全防護能力。國際層面是呼籲各國有效防範網路空間衝突、遏止資訊技術濫用、打擊網路恐怖組織和網路犯罪合作等。提倡網路資訊技術能開放和交流，並消弭開發中國家和已開發國家在網路科技領域的數位鴻溝，使得開發中的國家都能平等參與網路空間全球治理。

最後，發布《國家網絡空間合作戰略》。維護網路主權為首要目標，提出中國大陸對於網路空間國際合作的行動計劃。其一，匯聚開發中國家的力量，規劃研究有利於開發中國家的網路空間規則，先為開發中國家接受，再為國際接受，進而改變由美國等西方國家主導的網路空間治理的局面。其二，使網路主權理論得到國際的認可，必須在聯合國框架下，提高中國大陸在網路空間規則中的話語權。其三，鼓勵中國大陸學者參與網路空間的規則制定，例如北大西洋公約組織編撰的《塔林手冊》的經驗。將學術觀點集結而成官方文件，再轉變成國際法律，進而獲得國際承認。

上述中國大陸所公布的三項戰略也呼應攻勢現實主義的基本假設，網路空間為無政府狀態，中國大陸為潛在霸權國面對美國本身在網路科技創新和箝制住中國大陸的關鍵性基礎設施的能力，使中國大陸在資訊科技領

域的核心能力受制於人。而中國大陸無法把握美國的企圖，從公布《國家信息化發展戰略綱要》、《國家網絡空間安全戰略》和《網絡空間國際合作戰略》的舉措可看出中國大陸對美國掌握網路資訊等核心技術，試圖改變由美國掌握在科技領域的現狀，運用攻勢的手段，逕而達到網路強國和中華民族偉大復興的戰略目標。

三、中國大陸內部執行與特點

中國大陸所面臨的網路安全威脅應對模式，區分為立法層面及組織層面。首先，立法層面頒布《總體國家安全觀》，成立國家安全委員會，職責是制定和實施國家安全戰略，推動國家法制建設，制定國家安全工作方針，以及解決國家安全工作中的重大問題。

通過《國家安全法》第二十五條規定網路安全係以國家建設網路與資訊安全保障體系，提升網路與資訊安全保護能力，加強網路和資訊技術的創新研究和開發應用，實現網路和資訊核心技術、關鍵基礎設施和重要領域資訊系統數據的安全可控；加強網路管理，防範、制止和依法懲治網路攻擊、入侵、竊密、散佈違法有害資訊等犯罪行為，維護國家網路空間主權、安全和發展利益，藉以突顯中國共產黨領導建立集中統一、高效權威的國家安全領導體制。

頒布《網絡安全法》和相關網路安全規範性文件等，藉以保障中國大陸內部的設施安全、數據安全及內容安全，建構出以政府為主導，企業、

社會組織和網路使用者共同參與的網路安全責任制度，以提升網路空間的安全與秩序，突顯出中國大陸政府以立法手段管控網路空間日趨嚴謹。

其次，組織層面，區分為黨、政和軍隊三個部分。其一，黨部組織和與政府部門變革。中國大陸於 2014 年 2 月成立「中共中央網絡安全和資訊化領導小組」由中國共產黨中央層級上設置議事協調機構又屬於國務院的機構，為「一套人馬兩塊招牌」，出任組長的是由中國共產黨黨書記和國家最高領導人擔任，改變由過去國務院總理擔任國家資訊化組組長，難以協調中共中央、中央軍委、全國人民大會等的弊端，提高整體規劃、集中統一和統籌協調的能力。其管理機構和規劃層級也歷經多次變革，突顯出中國大陸領導人對資訊化已日漸重視。

其二，共軍組織變革。於 2015 年 12 月 31 日，將原太空部隊、網路部隊及電子對抗部隊，整併為「戰略支援部隊」成為第五個軍種，並直屬於中共中央軍委，為共軍遂行聯合作戰提供資訊鏈結保障。上述舉措突顯出中國大陸領導階層對網路空間爭奪是關係到網路安全與主權的連動性是密不可分，這也符合攻勢現實主義安全及權力極大化之推論。

最後，美國是網路空間的既有霸權，然而中國大陸試圖改變由美國主導網路空間的規則制定，從戰略層面於 2014 年成立「中共中央網絡安全和資訊化領導小組」，並由習近平親自擔任組長，公佈《國家資訊化發展戰略

綱要》、《國家網絡空間安全戰略》和《網絡空間國際合作戰略》體現中國大陸保障網路安全、維護國家利益及推動資訊化發展的決心。從立法層面制定《國家安全法》和《網絡安全法》不僅突顯出其欲確保對境內網路的絕對控制權力之外，亦具對外積極宣示網路主權之意涵。在共軍部分，中國大陸成立戰略支援部隊網路系統部，整合網路、電子、偵查等部隊，展現聯合作戰的能力。

因此，中國大陸進行組織調整、立法規範制定，獲得網路空間的治理權力，不僅可以消除內部的網路訊息流動可能帶來政權不穩的威脅，同時也擴大應對國內與國外網路空間防禦能力，與攻勢現實主義所強調無政府狀態下，國家必須尋求自助，進而以權力極大化的手段的論點相符合。

貳、中國大陸參與國際網路規則制定之影響

習近平於 2012 年接任國家領導人開始，雖然中國大陸網路用戶數排名世界第一位，但科技研發落後、管理體制缺乏統整，以及全球網路空間治理影響力都處於劣勢。因而提出全面強化網路產業，深化資訊創新技術及提升網路空間國際影響力，由「網路大國」轉變成為「網路強國」的願景。中國大陸在網路空間領域作為日益積極參與聯合國、區域性國際組織和其他國際活動，提出國際合作倡議、創建國際規則和主導國際議程，藉以提升網路空間的話語權和規則制定權。

一、中國大陸主張聯合國框架下推動網路空間治理

中國大陸主張聯合國框架下推動網路空間治理。擁有 193 個會員國的聯合國是當今最具合法性、影響力的國際組織。國際電信聯盟倡導下 2003 年和 2005 年舉辦資訊社會世界峰會分別在日內瓦和突尼斯召開，以政府主導的網路空間治理的聯合國平台，以解決開發中國家和已開發國家在資訊科技領域的數位鴻溝等議題。於 2006 年成立網路空間治理論壇，討論網路空間的治理問題。中國大陸積極與上合組織和東協等區域性國際組織包合作以及俄羅斯、巴西和印度等新興國家和多數開發中國家合作，運用多邊等外交手段持續推動聯合國主導下網路空間全球治理。

中國大陸政府近期在聯合國的攻勢作為有以下三點。一是積極派遣人員擔任聯合國及附屬機構主要負責人。統計目前在任的共有 6 位中國大陸籍的官員，掌握聯合國旗下的重要國際機構：包含國際民航組織（ICAO）秘書長柳芳；聯合國工業發展組織（UNIDO）秘書長李勇；國際電信聯盟（ITU）秘書長趙厚麟；世界銀行常務副行長、首席行政官楊少林；聯合國主管經濟和社會事務的副秘書長劉振民。聯合國全部 15 個附屬機構當中，就有高達 6 個國際組織由中國大陸籍人士掌握，這將使中國大陸成為聯合國體系裡最具影響力的國家。而美國駐聯合國大使克拉芙特（Kelly Craft）

日前特別點出：「目前沒有任何一個國家領導的聯合國組織超過一個以上，除了中國大陸。」

二是中國大陸政府積極遊說聯合國附屬組織前往北京或上海，成立海外辦公室。例如聯合國附屬組織世界知識產權組織目前的海外辦公室共有 6 個，當中就包含北京辦公室。

三是近年在由中國大陸籍擔任聯合國機構主要負責人，明顯偏袒特定國家的言論，時常被歐美為主的國際媒體抨擊。例如，國際電信聯盟秘書長趙厚麟，亦多次因以聯合國官員身份做出「過於偏袒中興、華為和中國電信等中國大陸科技公司」的公開發言引發爭議。

中國大陸的影響力在聯合國及附屬機構中日益擴大，加上聯合國的組織主要負責人遴選方式，改為一個國家一張票的方式進行。而中國大陸近年大量投資中亞、東南亞和非洲等開發中國家自然挾其優勢票數，當選國際組織主要負責人。例如由中國大陸籍趙厚麟擔任秘書長的國際電信聯盟，在制定網路資訊技術開發的標準和規則方面在中亞、東南亞和非洲等發展中國家具有很大的影響力。中國大陸大量推薦人員進入聯合國及附屬機構的問題，不僅顯現在延伸出中國大陸的影響力，或是執行中國大陸的外交政策，最大的問題在於利用這些機構為中國大陸治理模式背書，甚至輸出給開發中國家。上述攻勢作為勢必將成為聯合國的新常態，改變由美國等西方在聯合國的主導性，最終成為能與美國抗衡的強權國家。

二、中國大陸對區域性組織影響力與日俱增

中國大陸政府運用雙邊及多邊外交與區域組織形成良好互動。中國大陸於 2013 年參與北大西洋公約組織《塔林手冊網路戰國際法手冊》編撰，是國際法對網路戰爭最全面的文獻，也代表美國為首的西方國家對於網路戰爭的思考。《塔林手冊網路戰國際法手冊》對中國大陸網路安全的影響具有兩面性：有利一面是肯定網路主權不可侵犯性、禁止在網路空間使用武力或以武力相威脅及網路行為溯源困難。但不利於中國大陸的是肯定先發制人自衛攻擊的合理性及網路攻擊中嚴格規範軍隊和個人之區別，對中國大陸和開方發中國家參與網路空間行為規則的制定造成影響。而中國大陸需要借鑒《塔林手冊網路戰國際法手冊》的經驗，鼓勵中國大陸學者參與網路空間國際交流，從學術觀點匯集合成官方文件，再轉變成國際法律，最終獲得國際承認，提高中國大陸在網路空間的話語權。

中國大陸參與上海合作組織，成員國所遭受到「顏色革命」、「三股勢力」和「網路犯罪」等網路安全威脅，各成員國於上海峰會發表 2006 年《上海合作組織成員國元首關於國際信息安全的聲明》各國領導人認為資訊安全領域面臨政治、軍事、犯罪和恐怖主義等威脅，因此中國大陸於 2014 年積極主導建立資訊安全專家小組，增設秘書處和地區反恐機構執委會等兩個常設機構。並於 2015 年由中國大陸主導舉辦首次的網路反恐演習，代號

為「廈門-2015」，以彰顯中國大陸對網路反恐演習的重視，並主導成員國建立網路反恐技術平台，藉以交流反恐行動中的作業流程、法律程序和組織能力，進步一步完善成員國相關部門的合作機制。

中國大陸參與東協網路空間國際合作，東協國家總人口超過 6 億，但從網際網路應用，使用網路人數僅 2 億，網路普及率不足 30%。各成員國網路水準大相逕庭，發展失衡。中國大陸自 1991 年與東協建立對話關係開始積極展開多邊和雙邊交流，並提出「中國－東協信息港」配合「一帶一路」透過網路空間領域的合作，藉此提高中國大陸在全球網路空間治理中的話語權。

從中國大陸與東協網路安全合作包含中國大陸政府層級和地方政府層級合作。前者，經由元首高峰會議及部長級會議等以會議的形式展開交流，2005 年《中國-東協面相共同發展的信息通信領域夥伴關係北京宣言》、2009 年《中國-東協電信監管理事會關於網絡安全問題的合作框架》、2013 年《中國-東協非傳統安全領域合作諒解備忘錄》和 2015 年《中國-東協計算機應急響應合作機制》其目的在於加強雙方在資訊高速公路建設、網路領域標準制定和網路安全技術領域等合作，彰顯中國大陸領導人與東協各國元首在深化網路合作上的決心。

地方政府層級合作，以雲南省和廣西壯族自治區與東協的合作機制，於 2004 年廣西南寧舉辦「中國-東協博覽會」;2013 年雲南省昆明市舉辦「南

亞博覽會」藉以提升中國大陸在東南亞與南亞地區的主導能力與影響力。大湄公河次區域經濟合作已逐漸形成每三年召開領導人會議，每年舉行部長級會議、工作組和專題論壇的三層次合作架構雲南省和廣西壯族自治區是中國大陸參與大湄公河次區域經濟合作的主要省區,與參與各國在交通、電力、資訊、環境、經濟、貿易等多領域展開交流，彰顯出中國大陸民間企業的勢力已深入中亞及東南亞的各個角落。中國大陸在人口、面積和經濟總量都是亞洲第一，已在許多方面符合攻勢現實主義所假定的霸權候選國。目前，中國大陸透過民間企業與中亞及東南亞網路空間合作交流，藉此提升中國大陸在該地區的影響力和主導性。符合攻勢現實主義所的假定，挑戰或改變現有制度與規範。

三、中國大陸強化網路空間多邊會議之影響力

中國大陸開始透過主辦國際會議、提出國際合作倡議、創建國際規則和主導國際議程。由中國大陸倡導並主辦的 2014 年世界互聯網大會，舉辦地點在浙江省烏鎮更成為該大會永久會址，有利於中國大陸在網際網路全球治理，推動網路空間共享共治上掌握主動權和話語權。中國大陸政府開始運用主辦國際會議和利用聯合國平台發出中國大陸聲音，提出一系列中國大陸主張和方案。近年來，中國大陸相繼主辦金磚國家峰會、上海合作組織峰會和主辦 G20 集團峰會。這些會議上，中國大陸領導人多次提出《網

路空間命運共同體》和《「一帶一路」數字經濟國際合作倡議》等議題，成功在國際社會造成迴響。中國大陸還相繼提出共建「絲綢之路經濟帶」和「21 世紀海上絲綢之路」倡議，主導成立亞洲投資銀行、絲路金基金、開發銀行，使中國大陸多邊外交的提升與轉型，建構制度和規則，使得自身企業和社群媒體等得以「走出去」，以協助中亞和東南亞地區資訊化的發展，增進網路空間的合作，並擴大中國大陸在區域內的影響力。

整體而言，呼應攻勢現實主義的假設，中國大陸政府的目標，不只是與美國間爭奪「國際的話語權與領導權」而已；更重要的是，透過更大的國際組織影響力，試圖「改變或重新定義全球治理的原則」，利用在聯合國的高階領導職位和區域性國際組織的影響力來宣傳「中國共產黨」的準則與價值觀，甚至逐步改變美國在第二次世界大戰後與歐洲國家共同建立的國際規則，實現中華民族偉大復興，並達到區域霸權的目標。

第二節 後續研究建議

研究主要針對中國大陸網路空間戰略為研究主旨，試圖探究中國大陸網路空間戰略的執行能力。然而，上述研究議題仍在持續發展階段，未來在該領域仍有許多值得持續觀察及研究的空間。

首先，建設網路強國。2016 年公布《國家資訊化發展戰略綱要》，提出網路強國建設三步走，第一步到 2020 年，核心關鍵技術部分領域達到國際水準，到 2025 年，改變核心關鍵技術受制於人的局面，到本世紀中葉資訊

化全面支持社會主義現代化國家建設，然而華為、中興等兩大企業隨著中美貿易戰越演越烈，美國多次要求全球電信企業禁用華為的 5G 商用設備，因歐洲等國家及地區採用中國大陸主導的 5G 標準，就等於把國家的數位神經中樞控制權送給中國大陸。2019 年底爆發新型冠狀肺炎(COVID-19)蔓延全球，英國、法國和德國等主要歐洲國家因疫情的影響還處於政策反覆的階段，此舉措影響中國大陸網路空間戰略的布局受阻，值得後續繼續深入研究。

最後，中國－東協資訊港是中國近年配合「一帶一路」的戰略中的「21 世紀海上絲綢之路」建設提出的重大項目。中國大陸政府期望經由資訊港工程，在網路科技及資訊產業領域，有效增進和東協各成員國間的技術合作和經濟交流，藉以提升區域影響力，並支撐「21 世紀海上絲綢之路」的鋪展。然而 2019 年底中國大陸爆發新型冠狀病毒(COVID-19)之後，大規模停工與暫停人員流動政策，不僅打擊中國大陸經濟，也嚴重影響中國大陸力推的一帶一路政策，因原料、人工多來自中國大陸，現在不少建設都出現停滯，這也意味著商業運用的時間延後，同時也讓不少東協國內生產總值較小的國家，債務還款的壓力因此大增。因此，中國大陸－東協資訊港的建設與數位絲綢之路的前景，目前尚未明確，值得後續研究與觀察。

參考文獻

壹、中文部分

一、專書

中共年報編輯委員會編，2017 年。《2017 中共年報》。臺北：中共研究雜誌社。

中國現代國際關係研究院主編，2006 年。《國際戰略與安全形勢評估》。北京：時事出版社。

中國現代國際關係研究院經濟安全研究中心主編，2005 年。《全球能源大棋局》。北京：時事出版社。

方興東、胡懷亮，2014 年。《網絡強國：中美網絡空間大博弈》。北京：電子工業出版社。

日本防衛研究所，2019 年。《中國安全戰略報告 2019－圍繞亞洲秩序的戰略及其影響》。東京：防衛研究所。

王良能，2000 年。《中共崛起的國際戰略環境》。臺北：唐山出版社。

王逸舟，1999 年。《國際政治學-歷史與理論》，臺北：五南出版社。

王逸舟，2006 年。《西方國際政治學：歷史與理論》，上海：上海人民出版社。

包宗和主編，2011 年。《國際關係理論》。臺北：五南圖書出版股份有限公司。

田斌，2016 年。《習近平推動軍隊改革組建資訊軍》，香港：前哨出版社。

全軍軍事術語管理委員會，2011 年。《中國人民解放軍軍語》(北京：軍事科學院出版社。

朱和平編著，2004 年。《21 世紀綜合電子戰系統》，北京：軍事科學出版社。

朱浤源，1999 年。《撰寫博碩士論文實戰手冊》。臺北市：正中書局.、流傳文化.、墨文堂文化。

吳東林，2002 年。《巨變中的強權政治-體系變遷與美中台》，臺北：時英出版社。

呂亞力，1987 年。《政治學方法論》。臺北：三民書局出版社。

呂秋文，2007 年。《如何撰寫學術論文: 以政治學方法論為考察中心》。臺北：臺灣商務印書館。

汪玉凱、高新民，2012 年。《互聯網發展戰略》。北京：學習出版社。

沈雪石，2018 年，《國家網絡空間安全理論》。湖南：湖南教育出版社。

肖天亮，2005 年。《戰略學》。北京市：國防大學出版社。

周文欽，2000 年。《研究方法概論》臺灣：國立空中大學。

周世雄，2000 年。《國際關係－權力與制度》。臺北：五南圖書出版有限公司。

周湘華、董致麟主編，2009 年。《國際關係：理論與實務》，新北市：新文京出版社。

林宗達，2011 年，《國際關係理論概論》。臺北：晶典文化事業出版社。

林碧炤，1990 年。《國際政治與外交政策》，臺北：五南圖書出版有限公司。

倪世雄，2003 年。《當代國際關係理論》。臺北：五南圖書出版有限公司。

孫壯志主編，2011 年。《獨聯體國家「顏色革命」之研究》，北京：中國社會科學出版社。

翁明賢，2013 年。《戰略安全理論建構與政策研析》，臺北：淡江大學出版社。

翁衍慶，2018 年。《中共情報組織與間諜活動》，臺北：新銳文創。

張登及，2003 年。《建構中國-不確定世界的大國定位與大國外交》，臺北：揚智出版社。

敖志剛編著，2018 年。《網路空間作戰：機理與籌劃》，北京：電子工業出版社。

陳偉華，2003 年。《軍事研究方法論》。臺北：國防大學。

葉征，2013 年。《資訊作戰學教程》，北京：軍事科學出版社。

翟賢軍、楊燕南、李大光，2018 年，《網絡空間安全戰略-問題研究》。北京：人民出版社。

劉靜，2018 年，《網絡強國助推器-網絡空間國際合作共建》。北京：知識產權出版社。

戴清民，2009 年《求道無形之境》，北京：中國人民解放軍出版社。

魏亮、魏薇，2016 年。《網路空間安全》。北京：電子工業出版社。

羅伯特吉爾平著、楊宇光、楊炯譯，2001 年。《全球資本主義的挑戰-21 世紀的世界經濟》，上海：上海人民出版社。

二、外文專書譯著

Foucault. Michel 著，許寶強、袁偉譯，2001 年。《語言與翻譯的政治》，北京：中央編譯出版社。

Mearsheimer, John 著，張登及、唐小松、潘崇易、王義桅譯，2014 年 7 月。《大國政治的悲劇》，臺北：麥田出版社。

李柏彥譯，2011 年，《中共的國際行為：積極參與、善用機會、手段多樣》。臺北：國防部史政編譯室。譯自 Evan S. Medeiros, China’s International Behavior: Activism, Opportunism, and Diversification, USA: RAND Corporation Publishing Company Press.

胡祖慶譯，1989 年，《國際政治體系理論解析》。臺北：國立編譯館。譯自 Kenneth N. Waltz, Theory of International Politics, USA: McGraw-Hill Higher Education.

高一中譯，2012 年，《資訊作戰》。臺北：國防部史政編譯室。譯自 Leigh, Armlistead, Information Operations Matters, USA: University of Nebraska Press.

國防部史政編譯局譯，2001 年。《美國陸軍戰爭學院戰略指南》，臺北：國防部史政編譯室。Cerami, Joseph, U.S. Army War College Guide to Strategy, USA: Army War College.

國防部譯，2014 年。《網路戰爭；下一個國安威脅及因應之道》。臺北：國防部史政編譯室。譯自 Clarke, Richard, Cyber War: The Next Threat to National Security and What To Do About It, USA: Haper Collins Publishers.

國防部譯，2017 年。《網路安全：捍衛網路戰時代中的關鍵基礎設施》。臺北：國防部譯印。譯自 Johnson, Thomas, Cybersecurity: Protecting Critical Infrastructures from Cyber and Cyber Warfare ,U.S.: Taylor & Francis Group, LLC.

三、期刊

2011 年。〈中國互聯網協會出席聯合國互聯網治理論壇舉行〉，《中國信息安全》，頁 1-15

2012 年。〈第七屆互聯網治理論壇舉行〉，《計算機安全》，頁 69-78。

2014 年。〈中共中央網路安全和資訊化領導小組歷史沿革〉，《保密科學技術》，頁 1-13。

丁藝，2014 年。〈網絡安全視角下的網絡空間安全戰略構建〉，《電子政務》，第 7 期，頁 4-10。

方興東、胡懷亮、蕭亮，2016 年。〈中美網絡治理主張的分歧及期對策研究〉。《新疆師範大學學報報》第 36 卷，第 5 期，頁 64-72。

方興東、陳帥、徐濟函，2017 年。〈中國參與互聯網治理論壇的歷程、問題與對策〉，《理論前沿》，第 7 期，頁 12-25。

方濱興、杜阿寧、張熙、王忠儒，2016 年。〈國家網絡空間安全國際戰略研究〉，《中國工程科學》第 18 卷，第 6 期，頁 13-16。

木子衄，2014 年。〈網絡空間漸成全球政治博弈新角鬥場〉，《熱點聚焦專題》，頁 32-41。

王孔祥，2015 年。〈評《國際法適用於網絡戰的塔林手冊》〉，《現代國際關係》，第 5 期，頁 56-60。

王永華，2017 年。〈論網絡空間的體系結構及對抗層次〉，《中國軍事科學》，第 1 期，頁 126-132。

王向陽，2019 年。〈進攻性現實主義視角下中美網路空間關係〉，《南方論刊》，第 5 期，頁 23-29。

王明國，2015 年。〈網絡空間治理的制度困境與新興國家的突破路徑〉，《國際展望》第 6 期，頁 98-137。

王明國，2016 年。〈網絡空間秩序轉型的國際制度基礎〉，《全球傳媒學刊》第 3 卷第 4 期，頁 24-35。

王明進，2016 年。〈全球網絡空間治理的未來：主權、競爭與共識〉，《學術前沿》，頁 15-26。

王清安，2019 年。〈中共解放軍戰略支援部隊之發展對我陸軍威脅評估-以網路作戰部隊為例〉，《陸軍通資半年刊》，第 131 期，頁 4-22。

王清安、黃基禎，2018 年。〈中共對網路空間主權之概念與作為〉，《中國大陸研究》，第 62 卷第 1 期，頁 60-71。

王甜，2007 年。〈互聯網治理論壇第二次會議在巴西召開〉，《互聯網天地》，頁 2-10。

王翔，2016 年。〈中美網絡安全領域博弈機裡分析及未來展望〉，《中國與國際關係學刊》，第 2 期，頁 34-51。

王雲龍，2019 年。〈全面推動網絡強國建設的科學指南-學習習近平〉於網絡強國戰略的重要思想，《中國軍事科學》，第 2 期，頁 90-98。

左志，2016 年。〈國際電信聯盟與中國崛起-以中國電信政策研究為視角〉，《新聞大學學報》，第 3 期，頁 10-17。

左志，2016 年。〈國際電信聯盟與中國崛起-以中國電信政策研究為視角〉，《新聞大學學報》，第 3 期，頁 10-20。

安生，2015 年。〈對話中外專家：聚焦中美網絡博弈〉，《熱點聚焦》，頁 52-58。

曲星、蘇曉暉、李靜，2012 年。〈國際輿論中的中國國家形象〉，《當代世界》，第 4 期，頁 28-33。

朱志平、梁德昭，2016 年。〈習近平時期美中網路安全競逐〉，《遠景基金會季刊》，第 27 卷第 2 期，頁 4-14。

朱莉欣，2014 年。〈《塔林網絡戰國際法手冊》的網絡主權評介〉，《河北法學》，第 32 卷第 10 期，頁 39-42。

朱莉欣，2015 年。〈聚焦《塔林手冊》透視網絡戰規則〉，《中國資訊安全》，頁 39-42。

朱莉欣、韓曉陽，2017 年。〈基於機遇和挑戰，謀求發展和安全-比較中解讀《國家網絡空安全戰略》〉，《資訊安全與通信保密》，頁 20-31。

朱聽昌，2001 年。〈論中國睦鄰政策的理論與實踐〉，《國際政治研究》，第 2 期，頁 43-52。

何奇松，2015 年。〈建構中國網絡威懾戰略〉，《中國資訊安全》，頁 30-42。

余建華，2002 年。〈中亞的民族問題及其影響論析〉,《俄羅斯研究》，第 1 期，，頁 65-74。

余麗、趙秀贊，2019 年。〈中國貢獻：國際機制理論視域下的：世界互聯網大會〉,《河南社會科學》，第 27 卷第 5 期，頁 2-12。

冷冰淩等人，1999 年。〈網路戰：納入軍事體系〉,《解放軍報》，版 7。

呂晶華，2015 年。〈網絡空間治理：若干關鍵爭議的是與非〉,《學術前沿》，第 6 期，頁 94-99。

呂晶華、方寧，2015 年。〈完善網絡空間安全管理國際立法〉,《國防》，頁 26-31。

宋兆理、劉濯銨，2019 年。〈中共戰略支援部隊-網路系統部序列介紹〉,《陸軍通資半年刊》第 131 期，頁 23-40。

宋曉龍，2015 年。〈網絡監控與國家網絡空間治理〉,《中國資訊安全》，頁 47-50。

李宣良等人，2016 年。〈習近平向中國人民解放軍陸軍火箭軍戰略支援部隊授予軍旗並致訓詞〉,《人民日報》，版 1。

李恆陽，2014 年。〈斯諾登事件與美國網絡安全政策的調整〉,《外交評論》，第 6 期，頁 107-124。

李繼東、陳舟，2017 年。〈試論戰略網絡戰〉,《中國軍事科學》，第 6 期，頁 47-55。

李艷，2015 年。〈當前國際互聯網治理改革新動向探悉〉,《現代國際關係》，第 4 期，頁 44-50。

沈逸，2013 年。〈以實力保安全還是以治理謀安全?-兩種網絡安全戰中國戰略選擇〉,《外交評論》，第 3 期，頁 140-148。

沈逸，2013 年 10 月。〈全球網絡空間治理需要國際視野〉,《中國資訊安全》，頁 30-36。

沈逸,2014 年。〈全球網絡空間治理與金磚國家合作〉,《國際觀察》,第 4 期，頁 145-157。

沈逸，2014 年。〈後斯諾登時代的全球網路空間治理〉,《世界經濟與政治》，第 5 期，頁 144-155。

沈逸，2015 年。〈全球網路空間治理原則之爭與中國的戰略選擇〉,《外交評論》，第 2 期，頁 65-69。

沈逸，2016 年。〈ICANN 治理架構變革進程中的方向之爭：國際化還是私有化？〉,《汕頭大學學報》，第 6 期，頁 61-69。

赤東陽、劉權，2017 年。〈從《網絡空間國際合作戰略》-看我國維護網路空間主權的思路〉,《網絡空間安全》，頁 10-26。

阮宗澤，2019 年。〈一帶一路：塑造共用 21 世紀〉,《國際問題研究》，第 2 期，頁 6-21。

季華，2016 年。〈《塔林手冊》中有關網絡戰爭的武力使用問題-從國際法角度展開〉,《江漢學術》，第 35 卷第 3 期，頁 28-34。

林宗達，2019 年。〈國際關係攻勢現實主義理論之評析〉,《朝陽人文社會學刊,》，第 9 卷第 2 期，頁 59-105。

林碧炤，2010 年。〈國際關係的典範發展〉,《國際關係學報》，第 29 期，頁 10-29。

林穎佑，2017 年。〈中共戰略支援部隊任務與規模〉,《展望與探索》，第 15 卷第 10 期，頁 109-125。

況臘生，2015 年。〈世界主要國家網絡安全體系建設〉,《中國軍事科學》，第 6 期，頁 116-123。

施本植、湯海濱，2019 年。〈中國-東盟自由貿易區升級版建設路徑及雲南應發揮的作用〉,《學術探索》，頁 101-110。

胡培禹，2016 年。〈塔林網絡戰國際法手冊探析〉,《企業導報》，第 8 期，頁 170-176。

胡瑞舟，2017 年。〈中共中央國家安全委員會及其運作：從總體國家安全觀及國家安全工作座談會觀察〉,《展望與探索》第 15 卷第 4 期,頁 32-40。

苗圩,2013 年。〈實施中國製造 2025 建設製造強國網絡強國〉,《資訊評論》,頁 10-17。

唐嵐，2016 年。〈網絡安全法立足國內安全，放眼全球治理〉,《中國資訊安全》， 頁 98-157。

唐項登、班文濤，2018 年。〈習近平網絡安全理論〉,《中國軍事科學》，第 5 期，頁 70-76。

夏葦航、劉清才，2017 年。〈淺析中美在東盟區域合作中的博弈〉,《人民論壇・學術前沿》，第 24 期，頁 72-81。

孫偉、朱啟超，2016 年。〈東盟網路安全合作現狀與展望〉,《東南亞研究》，第 1 期，頁 4-18。

朗平，2013 年。〈網絡空間安全：一項新的全球議程〉,《國際安全研究》，第 1 期，頁 128-160。

朗平，2014 年。〈全球網絡空間規則制定的合作與博奕〉,《國際展望》，第 6 期，頁 138-152。

朗平，2014 年。〈全球網路空間規則制定的博弈與合作〉,《國際展望》，第 6 期，頁 135-146。

泰安，2015 年。〈相互尊重、合作共贏，建立新型中美大國網絡關係〉,《熱點聚焦》，頁 50-57。

泰安，2015 年。〈國家網絡空間治理有序開展-網絡強國建設之行動〉,《中國資訊安全》，頁 20-28。

泰安,2015 年。〈構建新型中美大國網絡關係〉,《中國資訊安全》,頁 30-39。

秦亞青，2018 年。〈《十九大報告》與中國外交的新時代〉,《亞太安全與海洋研究》，第 3 期，頁 1-14。

袁正清、蕭瑩瑩，2016 年。〈網路安全治理的東盟方式〉,《當代亞太》， 2 期，頁 80-94。

袁軻、張海娟、劉哲，2013 年。〈資訊網絡戰新趨勢研究〉,《數字技術與應用》，頁 40-48。

袁藝，2015 年。〈建設網絡強國必須謀劃打贏網絡戰爭〉,《中國資訊安全》，頁 29-41。

郝葉力，2015 年。〈大國網絡戰略博弈與中國網絡強國戰略〉,《國際關係研究》，第 3 期，20-36。

郝葉力，2015 年。〈把過國際網絡新秩序的著力點和切入點〉,《網事焦點》，頁 62-64。

馬民虎、張敏，2015 年。〈資訊安全與網絡社會法律治理：空間、戰略、權利、能力〉,《西安交通大學學報》，第 35 卷第 2 期，頁 92-97。

崔立如，2016 年。〈管理戰略競爭：中美新關係格局的挑戰〉,《美國研究》，第 2 期，頁 9-17。

崔學民，2016 年。〈美國移交 IANA 管理權事件啟示〉,《情報雜誌》，第 35 卷第 3 期，頁 24-27。

張文偉，2016 年。〈上海合作組織資訊安全合作：必要性、現狀及前景〉,《俄羅斯東歐中亞研究》，第 3 期，頁 90-97。

張倍維，2016 年。〈淺談我國我絡主權的國際法保護-從《塔林手冊》切入分析利弊〉,《法制與社會》，第 9 期，頁 9-10。

張訓譯，2019 年。〈習近平的「中國夢之一帶一路」：從攻勢現實主義的觀點分析〉,《樹德科技大學學報》第 21 卷第 2 期，頁 169-182。

張國城，2015 年。《從「攻勢現實主義」看台灣的「活路外交」及「外交休兵」》,《台灣國際研究季刊》，第 11 卷第 1 期，頁 78-85。

張貴洪，2016 年。〈中國聯合國外交的轉型〉,《中國發展觀察》，第 11 期，頁 17-20。

張裕亮，2016 年。〈第二屆世界互聯網大會評析〉，《展望與探索》，第 14 卷，第 1 期，頁 1-18。

從培影、黃日涵，2015 年。〈網絡空間衝突的治理困境與路徑選擇〉，《國際展望》第 6 期，頁 98-116。

梁德昭、朱志平、林凱薰，2012 年。〈國家主權延伸至網路空間之討論〉，《前瞻科技與管理》，第 2 卷第 2 期，頁 1-14。

盛辰超，2016 年〈聯合國在全球網絡安全治理中的規範功能研究〉，《國防》，第 18 卷第 3 期，頁 7-12。

許瑋陰，陳帥，方興東，2017 年。〈資訊社會世界峰會的演進歷程和發展現狀〉，《汕頭大學學報》，第 33 卷第 7 期，頁 20-34。

郭良，2017 年。〈聚焦多利益相關方模式：以聯合國互聯網治理論壇為例〉，《汕頭大學學報》第 33 卷第 9 期，頁 22-27。

陳時勇、于洪羽，2015 年。〈雲南、廣西參與國際區域合作，實施一帶一路戰略的平台和機制比較研究〉，《東南亞縱橫》，頁 41-52。

陳舒、劉賢剛、葉潤國、胡影，2015 年。〈塔林手冊 2.0 視角下的網路空間國際規則理論的發展〉，頁 40-52。

陳萊姬，2016 年。〈從 IANA 移交看 ICANN 新全球網路治理模式〉，《網絡空間研究》，第 8 期，頁 20-35。

陳陽，1998 年。〈國際電信聯盟簡介〉，《現代通信》，第 8 期，頁 1-12。

陳煥森，2016 年。〈習近平軍隊指揮結構改革工作之研究：以鞏固軍權重振「黨指揮槍」紀律為分析觀點〉，《展望與探索》，第 14 卷第 10 期，頁 41-66。

湯紹成，2000 年。〈後冷戰時期北大西洋公約組織角色與功能的轉變〉，《問題與研究》，，第 39 卷，頁 61-69。

黃仁偉，2015 年。〈中美秩序之爭與網絡治理〉，《熱點聚焦》，頁 50-58。

黃玉沛，2019 年。〈中非共建數字絲綢之路：機遇、挑戰與路徑選擇〉,《國際問題研究》，第 4 期，頁 50-63。

黃志雄，2015 年。〈國際法視角下的「網路戰」及中國的對策-以訴諸武力權為中心〉,《現代法學》，第 37 卷第 5 期，頁 154-155。

黃志雄，2018 年。〈網絡空間規則的新趨向-基於塔林手冊 2.0 的考察〉,《廈門大學學報》，第 1 期，頁 3。

楊志恆，1999 年。〈中共外交的策略與原則〉,《中國大陸研究》，第 42 卷，第 10 期，頁 42。

楊潔勉，2016 年。〈中國特色大國外交和話語權的使命與挑戰〉,《國際問題研究》，第 5 期，頁 26。

楊潔篪，2019 年。〈倡導國際合作，維護多邊主義，推動構建人類命運共同體〉,《國際問題研究》，第 2 期，頁 1-5。

楊嶸均,2014 年。〈論網絡空間治理國際合作面臨的難題及其應對策略〉,《南京工業大學學報》，第 13 卷第 4 期，頁 78-90。

葉征,2015 年。〈我國網絡空間的主要威脅和基本對策〉,《中國資訊安全》，頁 32-35。

董愛先，2014 年。〈國際網絡空間治理的主要舉措、特點及發展趨勢〉,《資訊安全與通信保密》，頁 36-41。

鄒軍，2015 年。〈全球互聯網治理的模式重構、中國機遇和參與路徑〉,《南京師大學報》，第 2 期，頁 57-63。

趙志國，2017 年。〈深化網絡與資訊安全監管助力網絡強國建設〉,《資訊評論》，頁 18。

趙武、周璞芬、王鳳才，2019 年。〈網絡主權的法理認識與思考〉,《中國軍事科學》，第 2 期，頁 44-51。

趙保獻，2015 年。〈網絡空間規則制定，戰略博弈加劇〉,《中國資訊安全》，頁 30-41。

趙隆，2013 年。〈全球治理中的議題設定：要素互動與模式適應〉,《國際關係研究》，第 4 期，頁 53-60。

劉宏，2013 年。〈跨國網絡與全球治理：東亞政治經濟發展的趨勢與挑戰〉，《當代亞太》第 6 期，頁 4-29。

劉貞曄、楊天宇，2016 年。〈中國與互聯網全球治理體系的變革〉,《二十四個重大問題研究》，頁 6-14。

劉楊鉞，2012 年。〈全球網絡治理機制演變、衝突與前景〉,《國際論壇》，第 14 卷第 1 期，頁 14-19。

劉楊鉞、張旭，2018 年。〈網絡空間國際安全秩序構建：現實困境與中國方案〉,《中國軍事科學》，第 4 期，頁 121-136。

劉鳴，2016 年。〈中美競合關係發展：基於國際規範、國際戰略對衝與協調的視角〉,《國際觀察》第 5 期，頁 94-105。

劉衛華、孫鵬，2015 年。〈建構網絡空間後備力量的必要性與對策〉,《後備力量》，頁 31-32。

劉震，2017 年。〈評《塔林手冊 2.0》對人權的保護與限制〉,《法制與社會》，頁 8-19。

樓項飛，2019 年。〈中拉共建數字絲綢之路：挑戰與路徑選擇〉,《國際問題研究》，第 2 期，頁 49-59。

潘兆民，2017 年。〈中國大陸發布《網絡空間國際合作戰略》政策意涵之評析〉,《展望與探索》，第 15 卷第 5 期，頁 28-34。

蔡軍、何駿、於小紅，2018 年。〈美軍網絡空間作戰理論〉,《中國軍事科學》，第 1 期，頁 149-156。

蔡翠紅，2015 年。〈網絡空間治理的大國責任當議〉,《當代世界與社會主義》，第 1 期，頁 171-177。

蔣麗、張小蘭、徐飛彪，2013 年。〈國際網絡安全合作的困境與出路〉,《現代國際關係》，第 9 期，頁 52-58。

談劍峰，2015 年。〈高度重視國家網絡安全審查制度的戰略效應〉,《中國資訊安全》，頁 34-37。

鄭怡君、薛志華，2017 年。〈中國-東盟網路安全合作及其布局〉,《東南亞南亞研究》，第 2 期，頁 10-18。

餘麗，2013 年。〈互聯網對國際政治影響機理探究〉,《國際安全研究》第 1 期，頁 105-127。

魯傳穎，2013 年。〈試析當前網路空間全球治理困境〉,《現代國際關係》，第 11 期，頁 46。

魯傳穎，2013 年。〈試析當前網絡空間全球治理困境〉,《現代國際關係》，第 11 期，頁 48-54。

魯傳穎，2017 年。〈網絡空間治理的力量博弈、理念演變與中國戰略〉,《國際展望》，頁 117-134。

黎雪琳，2008 年。〈網絡恐怖主義探悉〉,《廣西警官高等專科學校學報》，第 1 期，頁 17。

蕭君擁、孟達華，2019 年。〈總體國家安全觀視野中的資訊網絡安全法治研究〉,《網絡空間安全》，第 10 卷第 5 期，頁 1-9。

賴明明、袁翼倫，2016 年。〈中美網絡空間競合出現新動向-評蘭德公司《謀求與中國達成網絡空間共識》報告〉,《網絡空間研究》第 8 期,頁 67-71。

賴明明、黃衛平，2016 年。〈互聯網時代中美雙贏未來展望〉,《汕頭大學學刊》第 6 期，頁 116-125。

閻學通，2016 年。〈政治領導與大國崛起安全〉,《國際安全研究》，第 4 期，頁 3-19。

應琛，2015 年。〈從文化視角看美國在網絡空間治理中的立場與行動〉,《當代世界》第 6 期，頁 50-52。

檀有志，2016 年。〈大數據時代中美網絡空間合作研究〉，《國際觀察》，第 3 期，頁 28-41。

鞠德風、董慧明，2010 年。〈中共崛起的理論與實際：國際關係理論的檢視與分析〉，《復興崗學報》，第 100 期，頁 135-157。

韓璐，2019 年。〈上海合作組織與一帶一路的協同發展〉，《國際問題研究》，第 2 期，頁 22-35。

魏永征，2018 年。〈從《中華人民共和國國家安全法》到《中華人民共和國網絡安全法》-學習習近平總體國家安全觀〉，《社會治理》，第 1 期，頁 20-33。

嚴震生，2016 年。〈杭州 G20 峰會與「中國方案」〉，《展望與探索》，第 14 卷第 10 期，頁 1-10。

四、官方文件

國務院新聞辦公室，2010 年。〈中國互聯網狀況〉，《政府之聲》。

聯合國大會，2010 年 7 月 30 日。\〈從國際安全的角度來看資訊和電信領域發展的政府專家組的報告 A/65/201〉，《聯合國第 65 屆會議》。

聯合國大會，2015 年 7 月 22 日。〈從國際安全的角度來看資訊和電信領域發展的政府專家組的報告 A/70/174〉，《聯合國第 70 屆會議》。

五、網路資料

〈2015 年解放軍外國語學院招生簡章〉，《中國教育網》。〈https://gkcx.eol.cn/school/2624/provinceline〉。（瀏覽日期 2020 年 2 月 15 日）。

〈2015 年解放軍資訊工程大學招生簡章〉，《中國教育網》。〈https://gkcx.eol.cn/school/2624/provinceline〉。（瀏覽日期 2020 年 2 月 15 日）。

〈中央網絡安全和資訊化領導小組第一次會議召開〉2014 年 2 月 27 日。中華人民共和國中央人民政府網站》，〈http://www.gov.cn/ldhd/2014-02/27/content_2625036.htm〉。(瀏覽日期：2020 年 2 月 12 日)。

〈資訊工程大學簡介〉,《中國人民解放軍戰略支援部隊資訊工程大學招生資訊網》。〈https://souky.eol.cn/HomePage/index_134.html〉。(瀏覽日期 2020 年 2 月 15 日)。

1993 年 2 月 22 日。〈中華人民共和國國家安全法〉,《全國人民代表大會網》，〈http://www.npc.gov.cn/wxzl/gongbao/1993-02/22/content_1481246.htm〉。(瀏覽日期：2020 年 2 月 12 日)。

1996 年 4 月 21 日。〈中華人民共和國和哈薩克共和國、吉爾吉斯共和國、俄羅斯聯邦、塔吉克斯坦共和國關於在邊境地區加強軍事領域信任的協定〉,《全國人民代表大會網站》，〈http://www.npc.gov.cn/wxzl/wxzl/2000-12/06/content_3612.htm〉(檢索日期 2020 年 5 月 1 日)。

2001 年 2 月 27 日。〈77 國集團〉,《中華人民共和國外交部》，〈https://www.fmprc.gov.cn/web/wjb_673085/zzjg_673183/gjjjs_674249/gjzzyhygk_674253/qsqg_674549/gk_674551/〉。(檢索日期 2020 年 3 月 1 日)。

2005 年 11 月 17 日。〈黃菊在信息社會世界峰會突尼斯階段會議上講話〉,《中央政府門戶網站》，〈http://www.gov.cn/ldhd/2005-11/17/content_101716_2.htm〉,(檢索日期：2020 年 4 月 12 日。)

2006 年 6 月 15 日。〈上海合作組織成員國元首關於國際信息安全的聲明〉，《中華人民共和國外交部》，〈https://www.fmprc.gov.cn/web/ziliao_674904/1179_674909/t346576.shtml〉。(檢索日期 2020 年 3 月 10 日)。

2007 年 1 月 14 日。〈中國-東盟面相共同發展的信息通信領域夥伴關係北京宣言〉,《吉林省服務貿易指南網》,〈http://www.jlfwmy.com/NewsShow.asp?pageclass=1010402&id=1627〉。(檢索日期 2020 年 4 月 10 日)。

2008 年 4 月 17 日。〈發展改革委有關負責人就《國民經濟和社會發展資訊化“十一五”規劃》答記者問〉,《中華人民共和國中央人民政府網站》,〈http://big5.www.gov.cn/gate/big5/www.gov.cn/zwhd/2008-04/17/content_947090.htm〉。(瀏覽日期：2020 年 2 月 12 日)。

2009 年 8 月 13 日。〈信息化帶動工業化，以工業化促進信息化〉《中國經濟網》,〈http://www.ce.cn/cysc/ztpd/09/ind/informatization/200908/13/t20090813_19579290.shtml〉。(瀏覽日期：2020 年 2 月 12 日)。

2010 年 1 月 21 日。〈美國國務卿希拉蕊柯林頓關於網際網路自由的演說 華盛頓新聞博物館〉,《美國在台協會》,〈http://ait.org.tw/zh/news/officialtext〉,檢索日期:2019 年 10 月 15 日。

2011 年 09 月 13 日。〈中俄等國向聯合國提交《信息安全國際行為準則》〉,《中華人民共和國中央人民政府》,〈http://www.gov.cn/jrzg/2011-09/13/content_1945825.htm〉。(檢索日期 2020 年 5 月 1 日)。

2011 年 09 月 13 日。〈中俄等國向聯合國提交《信息安全國際行為準則》〉,《中華人民共和國中央人民政府》,〈http://www.gov.cn/jrzg/2011-09/13/content_1945825.htm〉。(檢索日期 2020 年 5 月 1 日)。

2011 年 11 月 5 日。〈外交部發布中國-東盟合作：1991-2011(全文)〉,《中華人民共和國中央人民政府網》,〈http://big5.www.gov.cn/gate/big5/www.gov.cn/gzdt/2011-11/15/content_1993964.htm〉。(檢索日期 2020 年 4 月 10 日)。

2012 年 12 月 14 日。〈國際電信大會修訂《國際電信規則》 美國等國抵制〉《聯合國新聞網》,〈https://news.un.org/zh/story/2012/12/185462〉。(檢索日期 2020 年 3 月 2 日)。

2013 年 3 月 24 日。〈國家主席習近平在莫斯科國際關係學院的演講〉,《中華人民共和國人民府網》,〈http://www.gov.cn/ldhd/2013-03/24/content_2360829.htm〉,(檢索日期:2020 年 3 月 15 日。)

2013 年 3 月 26 日。〈分析:金磚五國到底能有多大作為?〉《BBC 中文網》。〈https://www.bbc.com/zhongwen/trad/world/2013/03/130326_brics_future.shtml〉。(檢索日期 2020 年 4 月 21 日)。

2013 年 7 月 24 日。〈《上海合作組織成員國保障國際信息安全政府間合作協定》〉,《澳門特別行政區政府印務局網》,〈https://bo.io.gov.mo/bo/ii/2013/30/aviso28_cn.asp#cht〉。(檢索日期 2020 年 3 月 10 日)。

2014 年 06 月 23 日。〈人民日報權威論壇:網絡主權,一個不容迴避的議題〉,《人民網》,〈http://opinion.people.com.cn/n/2014/0623/c1003-25183666.html〉,(檢索日期:2020 年 3 月 12 日。)

2014 年 06 月 28 日。〈和平共處五項原則〉,《中國共產黨新聞網站》,〈http://cpc.people.com.cn/BIG5/n/2014/0628/c64387-25212801.html〉(檢索日期 2020 年 5 月 1 日)。

2014 年 10 月 24 日。〈趙厚麟成國際電信聯盟 150 年來首位中國籍秘書長〉,《人民網》,〈http://ip.people.com.cn/BIG5/n/2014/1024/c136655-25900794.html〉。(檢索日期 2019 年 11 月 12 日)。

2014 年 11 月 16 日。〈中國互聯網二十年:1994-2014 年〉,《中央網絡安全和資訊化辦公室網》,

〈http://www.cac.gov.cn/2014-11/16/c_1113265290.htm〉。(瀏覽日期：2020 年 2 月 12 日)。

2014 年 1 月 24 日。〈中共中央政治局研究決定中共中央安全委員會設置〉，《中華人民共和國中央人民政府網》，〈http://www.gov.cn/ldhd/2014-01/24/content_2575011.htm〉。(瀏覽日期：2020 年 2 月 12 日)。

2014 年 3 月 31 日。〈「東南亞國家協會」發展簡介〉，《台灣東南亞國家協會研究中心》，〈http://www.aseancenter.org.tw/ASEANintro.aspx〉。(檢索日期 2020 年 3 月 10 日)。

2014 年 4 月 16 日。〈習近平主持召開中央國家安全委員會第一次會議強調：堅持總體國家安全觀，走中國特色國家安全道路〉，《人民網》，〈http://politics.people.com.cn/n/2014/0416/c1024-24900227.html〉。(瀏覽日期：2020 年 2 月 12 日)。

2014 年 9 月 13 日。〈上海合作組織成員國元首杜尚別宣言〉，《新華網》，〈http://www.xinhuanet.com/world/2014-09/13/c_126981562.htm〉。(檢索日期 2020 年 3 月 10 日)。

2015 年 05 月 19 日。〈國務院印發《中國製造 2025》〉《新華網》。〈http://www.xinhuanet.com//politics/2015-05/19/c_1115331338.htm〉。(檢索日期 2020 年 4 月 12 日)。

2015 年 10 月 14 日。〈上海合作組織首次網絡反恐演習在廈門成功舉行〉，《中華人民共和國國防部》，〈http://www.mod.gov.cn/big5/topnews/2015-10/14/content_4624849.htm〉。(檢索日期 2020 年 3 月 10 日)。

2015 年 12 月 16 日。〈習近平出席第二屆世界互聯網大會開幕式並發表主旨演講〉，《中華人民共和國國家互聯網信息辦公室網》，〈http://www.cac.gov.cn/2015-12/16/c_1117480642.htm〉，（檢索日期：2020 年 3 月 12 日。）

2015 年 12 月 18 日。〈烏鎮倡議〉,《新華網》,〈http://www.xinhuanet.com/politics/2015-12/18/c_1117512543.htm〉。(檢索日期 2019 年 11 月 15 日)。

2015 年 12 月 23 日。〈俄媒：中俄兩國將就對抗資訊戰進行演習 並交換經驗〉,《新華網》,〈http://www.xinhuanet.com/world/2015-12/23/c_128558988.htm〉。(檢索日期 2020 年 4 月 10 日)。

2015 年 3 月 4 日。〈美國務部：中國所提信息安全準則限制網絡自由〉,《美國駐華大使館》,〈https://china.usembassy-china.org.cn/zh/internetfreedom2015-zh/〉。(檢索日期 2020 年 3 月 10 日)。

2015 年 3 月 5 日。〈《信息安全國際行為準則》〉,《中華人民共和國外交部》,〈https://www.fmprc.gov.cn/web/ziliao_674904/tytj_674911/zcwj_674915/t858317.shtml〉。(檢索日期 2020 年 3 月 10 日)。

2015 年 4 月 21 日。〈中國代表團出席海牙網路空間國際會議〉,《中共中央網絡安全和信息化辦公室》,〈http://www.cac.gov.cn/2015-04/21/c_1115037999.htm〉(檢索日期 2020 年 5 月 1 日)。

2015 年 5 月 12 日。〈《中華人民共和國政府和俄羅斯聯邦政府關於在保障國際資訊安全領域合作協定》〉,《中華人民共和國外交部網站》,〈https://www.fmprc.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/jksxwlb_674635/t1263088.shtml〉。

2015 年 7 月 10 日。〈中華人民共和國國家安全法〉,《人大新聞網》,〈http://npc.people.com.cn/BIG5/n/2015/0710/c14576-27285049.html〉。(檢索日期 2019 年 11 月 1 日)。

2015 年 7 月 1 日。〈聚焦新國家安全法五大亮點〉,《新華網》,〈http://www.xinhuanet.com//politics/2015-07/01/c_1115787097_2.htm〉。(瀏覽日期：2020 年 2 月 12 日)。

2015 年 7 月 20 日。〈關於《中共中央關於全面深化改革若干重大問題的決定》的說明〉,《中國共產黨新聞網》,
〈http://cpc.people.com.cn/xuexi/n/2015/0720/c397563-27331312.html〉

2016 年 03 月 17 日。〈《中華人民共和國國民經濟和社會發展第十三個五年規劃綱要》〉,《新華網》,
〈http://www.xinhuanet.com//politics/2016lh/2016-03/17/c_1118366322.htm〉(檢索日期 2020 年 5 月 1 日)。

2016 年 03 月 17 日。〈《中華人民共和國國民經濟和社會發展第十三個五年規劃綱要》〉,《新華網》,
〈http://www.xinhuanet.com//politics/2016lh/2016-03/17/c_1118366322.htm〉(檢索日期 2020 年 5 月 1 日)。

2016 年 11 月 7 日。〈中華人民共和國網絡安全法〉,《新華網》,
〈http://www.xinhuanet.com/politics/2016-11/07/c_1119867015.htm〉。(檢索日期 2019 年 11 月 1 日)。

2016 年 11 月 8 日。〈專家解讀《網絡安全法》,具有六大突出亮點〉,《中國江蘇網》,
〈http://news.jschina.com.cn/zt2017/docs/201709/t20170911_1029164.shtml〉。(瀏覽日期：2020 年 2 月 18 日)。

2016 年 6 月 25 日。〈互聯網信息搜索服務管理規定〉,《中國網信網》,
〈http://www.cac.gov.cn/2016-06/25/c_1119109085.htm〉,(檢索日期：2020 年 4 月 12 日。)

2016 年 9 月 23 日。〈習近平：金融、能源是關鍵的基礎設施是網路安全的重中之重〉,《中國能源網》,
〈http://www.cnenergynews.cn/tt/201609/t20160923_385773.html〉。(檢索日期 2020 年 4 月 10 日)。

2017 年 05 月 14 日。〈習近平在“一帶一路”國際合作高峰論壇開幕式上的演講〉,《“一帶一路”國際合作高峰論壇官方網站》,

〈http://www.beltandroadforum.org/BIG5/n100/2017/0514/c24-407.html〉。(檢索日期 2019 年 11 月 15 日)。

2017 年 09 月 04 日。〈金磚國家領導人廈門宣言〉,《新華網》,〈http://www.xinhuanet.com/world/2017-09/04/c_1121603652_2.htm〉。(檢索日期 2020 年 5 月 1 日)。

2017 年 11 月 13 日。〈李克強在第 20 次中國-東盟領導人會議上的講話(全文)〉,《中國外交部網》,〈https://www.fmprc.gov.cn/web/gjhdq_676201/gjhdqzz_681964/dmldrhy_683911/zyjhywj_683921/t1510228.shtml〉。(檢索日期 2020 年 4 月 10 日)。

2018 年 3 月 21 日。〈中共中央印發《深化黨和國家機構改革方案》〉,《新華網網》,〈http://www.xinhuanet.com/2018-03/21/c_1122570517.htm〉。(瀏覽日期：2020 年 2 月 12 日)。

2018 年 6 月 19 日。〈阿里巴巴馬來西亞辦公室開幕〉,《人民網》,〈http://world.people.com.cn/n1/2018/0619/c1002-30064814.html〉。(檢索日期 2020 年 4 月 10 日)。

2018 年 9 月 27 日。〈第十一屆中國—東盟成員國總檢察長會議聯合聲明〉,《中國最高人民法院網》,〈http://www.ca-pgc.org/xdxy/201809/t20180927_2370625.shtml〉。(檢索日期 2020 年 4 月 10 日)。

2019 年 12 月。〈上海合作組織〉,《中華人民共和國外交部網站》,〈https://www.fmprc.gov.cn/web/gjhdq_676201/gjhdqzz_681964/lhg_683094/jbqk_683096/t528036.shtml〉(檢索日期 2020 年 5 月 1 日)

2019 年 6 月 4 日。〈貿易戰從來不是貿易問題：美國為什麼要防堵華為，占領全球 5G 市場？〉,《經濟日報》,〈https://money.udn.com/money/story/10511/3852873#prettyPhoto〉。(檢索日期 2020 年 4 月 12 日)。

Raymond Zhong，2018 年 11 月 9 日。〈烏鎮互聯網大會與科技的陰暗面〉，《紐約時報中文網》，〈https://cn.nytimes.com/china/20181109/china-world-internet-conference/zh-hant/〉，（檢索日期：2020 年 4 月 12 日。）

人民日報 2007 年 12 月 26 日。〈資訊化覆蓋現代化建設全域的戰略舉措〉，《國脈電子政務網》，〈http://www.echinagov.com/info/316〉。(瀏覽日期：2020 年 2 月 12 日)。

人民日報 2019 年 9 月 23 日。〈王毅：譜寫中國特色大國外交的時代華章〉，《中華人民共和國中央人民政府》。〈http://www.gov.cn/guowuyuan/2019-09/23/content_5432243.htm〉。(檢索日期 2020 年 4 月 21 日)。

人民日報撰稿，2017 年 10 月 28 日。〈習近平在中國共產黨第十九次全國代表大會上的報告〉，《人民網》，〈http://cpc.people.com.cn/n1/2017/1028/c64094-29613660-7.html〉。(瀏覽日期：2020 年 3 月 29 日)。

人民網，2014 年 3 月 3 日。〈汪玉凱：中央網絡安全與資訊化領導小組的由來及其影響〉，《中國共產黨新聞網》，〈 http://theory.people.com.cn/BIG5/n/2014/0303/c40531-24510897.html 〉。(瀏覽日期：2020 年 2 月 18 日)。

人民網，2016 年 6 月 19 日。〈中國-東盟信息港股份有限公司成立，構築信息絲綢之路〉，《人民網》，〈http://gx.people.com.cn/n2/2016/0619/c179430-28531189.html〉。(檢索日期 2020 年 4 月 10 日)。

中央網絡安全和資訊化領導小組，2014 年 2 月 27 日。〈中央網絡安全和資訊化領導小組成立：從網絡大國邁向強國〉，《中國共產黨新聞網》，〈http://cpc.people.com.cn/BIG5/n/2014/0227/c64094-24486382.html〉。(檢索日期 2019 年 11 月 11 日)。

中央網絡安全和資訊化領導小組，2017 年 3 月 1 日。〈《網絡空間國際合作戰略》(全文)〉，《新華網》，〈http://www.xinhuanet.com/politics/2017-03/01/c_1120552767.htm〉。(檢索日期 2019 年 11 月 11 日)。

中共中央辦公廳、國務院辦公廳，2016 年 7 月 27 日。〈《國家信息化發展戰略綱要》〉，《中華人民共和國中央人民政府站》，〈http://big5.www.gov.cn/gate/big5/www.gov.cn/gongbao/content/2016/content_5100032.htm〉。(檢索日期 2020 年 4 月 11 日)。

中國互聯網絡信息中心，2019 年 8 月。〈第 44 次中國互聯網絡發展狀況統計報告〉，《中華人民共和國國家互聯網信息辦公室網》，〈http://www.cac.gov.cn/pdf/20190829/44.pdf〉，（檢索日期：2020 年 3 月 12 日。）

中國互聯網路資訊中心，2019 年 8 月。〈2019 年中國互聯網路發展狀況統計報告〉，《中國網信網》，〈http://www.cac.gov.cn/2019-02/28/c_1124175677.htm〉。(檢索日期 2019 年 10 月 1 日)。

中國信通院，2019 年 7 月 18 日。〈中國完成面向國際電信聯盟的 5G 候選技術方案提交〉，《新浪科技網》。〈https://tech.sina.com.cn/5g/i/2019-07-18/doc-ihytcerm4459560.shtml〉。(檢索日期 2020 年 4 月 12 日)。

中國國家互聯網信息辦公室，2018 年 12 月 27 日。〈習近平：沒有網絡安全就沒有國家安全〉，《中國國家互聯網信息辦公室網站》，〈http://www.cac.gov.cn/2018-12/27/c_1123907720.htm〉。(檢索日期 2019 年 11 月 1 日)。

中國國家互聯網資訊辦公室，2018 年 12 月 27 日。〈國家網絡空安全戰略〉，《中國國家互聯網信息辦公室網站》，〈http://www.cac.gov.cn/2016-12/27/c_1120195878.htm〉。(檢索日期 2019 年 11 月 11 日)。

中國國家互聯網資訊辦公室，2018 年 12 月 27 日。〈國家網絡空安全戰略〉，《中國國家互聯網信息辦公室網站》，〈http://www.cac.gov.cn/2016-12/27/c_1120195878.htm〉。(檢索日期 2019 年 11 月 11 日)。

中國網信網，2017 年 10 月 30 日。〈《互聯網新聞資訊服務新技術新應用安全評估管理規定》〉，《中共網路資訊辦公室網》〈http://www.cac.gov.cn/2017-10/30/c_1121878049.htm〉。(瀏覽日期：2020 年 2 月 18 日)。

中國網信網，2017 年 5 月 2 日。〈《網絡產品和服務安全審查辦法》〉，《中共網路資訊辦公室網》〈http://www.cac.gov.cn/2017-05/02/c_1120904567.htm〉。(瀏覽日期：2020 年 2 月 18 日)。

中國網信網，2017 年 7 月 11 日。〈《關鍵資訊基礎設施安全保護條例》〉，《中共網路資訊辦公室網》〈http://www.cac.gov.cn/2017-07/11/c_1121294220.htm〉。(瀏覽日期：2020 年 2 月 18 日)。

中國網信網，2017 年 8 月 25 日。〈《互聯網跟帖評論服務管理規定》〉，《中共網路資訊辦公室網》〈https://www.cac.gov.cn/2017-08/25/c_1121541842.htm〉。(瀏覽日期：2020 年 2 月 18 日)。

中國網信網，2017 年 8 月 25 日。〈《互聯網論壇社區服務管理規定》〉，《中共網路資訊辦公室網》〈https://www.cac.gov.cn/2017-08/25/c_1121541921.htm〉。(瀏覽日期：2020 年 2 月 18 日)。

中國網信網，2017 年 9 月 7 日。〈《互聯網使用者公眾帳號資訊服務管理規定》〉，《中共網路資訊辦公室網》〈http://www.cac.gov.cn/2017-09/07/c_1121624233.htm〉。(瀏覽日期：2020 年 2 月 18 日)。

中國網信網，2017 年 9 月 7 日。〈《互聯網群組資訊服務管理規定》〉，《中共網路資訊辦公室網》〈https://www.cac.gov.cn/2017-09/07/c_1121623889.htm〉。(瀏覽日期：2020 年 2 月 18 日)。

中國網信網，2019 年 6 月 18 日。〈《個人資訊和重要數據出境安全評估辦法》體現以人為本的數據治理理念〉，《中共網路資訊辦公室網》〈http://www.cac.gov.cn/2019-06/18/c_1124644976.htm〉。(瀏覽日期：2020 年 2 月 18 日)。

中華人民共和國國務院，2016 年 3 月 17 日。〈中華人民共和國國民經濟和社會發展第十三個五年規畫綱要〉，《新華社》。〈http://www.xinhuanet.com//politics/2016lh/2016-03/17/c_1118366322.htm〉，（檢索日期：2020 年 3 月 12 日。）

中華人民共和國國務院新聞辦公室，2009 年 1 月 16 日。〈2008 年中國的國防〉，《中華人民共和國國防部》。〈http://www.mod.gov.cn/big5/regulatory/2011-01/06/content_4617809.htm〉。（瀏覽日期 2020 年 2 月 6 日）。

世界互聯網大會，2018 年 11 月 09 日。〈互聯網國際高端智庫論壇探討「網路空間的中美關係」〉，《世界互聯網大會網》，〈http://2018.wicwuzhen.cn/web18/release/release/201811/t20181109_8705733.shtml〉，（檢索日期：2020 年 3 月 12 日。）

余俊傑、白瀛，2019 年 3 月 20 日。〈在通向網絡強國的征程上穩步前進-寫在中央網絡安全和資訊畫委員會成立一周年之際〉，《新華網》，〈http://www.xinhuanet.com/2019-03/20/c_1124261185.htm〉。(檢索日期 2019 年 11 月 1 日)。

吳介聲，2019 年 10 月 24 日。〈中共封網、萬人翻牆：世界互聯網大會，淪極權科技採買會？〉，《聯合新聞網》，〈https://opinion.udn.com/opinion/story/120611/4123796〉，（檢索日期：2020 年 3 月 12 日。）

沈逸，2014 年 7 月 22 日。〈轉型與建構：後斯諾登時代國家網絡安全戰略設計與能力建設〉，《中國共產黨新聞網》，〈http://theory.people.com.cn/n/2014/0722/c386965-25317991.html〉。(瀏覽日期：2020 年 2 月 12 日)。

信息產業部辦公廳，2001 年 2 月 27 日。〈我國電信領域改革開放大事記〉，《中國信息產業網》。〈http://www.cnii.com.cn/20020808/ca79451.htm〉。(檢索日期 2019 年 11 月 11 日)。

秦安，2013 年 6 月 4 日。〈對美國「八大金剛」不能不設防〉，《環球網》，〈https://opinion.huanqiu.com/article/9CaKrnJALYl〉。(檢索日期 2020 年 2 月 15 日)。

國家計算機網絡應急技術處理協調中心，2019 年 8 月。〈2019 年上半年我國互聯網網絡安全態勢〉，《中華人民共和國國家互聯網資訊辦公室網站》，〈http://www.cac.gov.cn/2019-08/13/c_1124871484.htm〉。

彭茜，2017 年 3 月 30 日。〈中國北斗衛星導航定位系統將“照亮”東盟 10 國〉，《中國軍網》，〈http://www.81.cn/jwgz/2017-03/30/content_7545156.htm〉。(檢索日期 2020 年 4 月 10 日)。

黃勝雄，2014 年 5 月。〈從 ICANN 多元利益關係人(Multistakeholders) 之架構談未來網路治理〉，《臺網中心電子報》，〈http://www.myhome.net.tw/2014_05/p02.htm〉，（檢索日期：2020 年 3 月 12 日。）

新華社，2012 年 12 月 5 日。〈哈薩克官員稱”哈里發戰士”威脅哈國安全〉，《環球網》，〈https://world.huanqiu.com/article/9CaKrnJy24z〉。(檢索日期 2020 年 3 月 10 日)。

新華社，2013 年 11 月 12 日。〈中共中央關於全面深化改革若干重大問題的決定〉，《中華人民共和國人民府網》，

〈http://www.gov.cn/jrzg/2013-11/15/content_2528179.htm〉,(檢索日期：2019 年 10 月 14 日。)

新華社,2013 年 11 月 12 日。〈中共中央關於全面深化改革若干重大問題的決定〉,《中華人民共和國中央人民政府網》,〈http://www.gov.cn/jrzg/2013-11/15/content_2528179.htm〉,(檢索日期：2020 年 3 月 15 日。)

新華社,2014 年 9 月 18 日。〈魯煒:打造中國—東盟信息港 建設 21 世紀「海上絲綢之路」的信息樞紐〉,《文匯網》,〈http://news.wenweipo.com/2014/09/18/IN1409180073.htm〉。(檢索日期 2020 年 4 月 10 日)。

新華社,2015 年 10 月 12 日。〈中國東盟攜手邁向命運共同體〉,《新華網》,〈http://www.xinhuanet.com/world/2015-10/12/c_128306979.htm〉。(檢索日期 2020 年 4 月 10 日)。

新華社，2016 年 10 月 9 日。〈中共中央政治局就實施網絡強國戰略進行第 36 次集體學習〉,《中華人民共和國中央人民政府網》。〈http://www.gov.cn/xinwen/2016-10/09/content_5116444.htm〉。(檢索日期 2020 年 3 月 2 日)。

新華社,2016 年 8 月 24 日。〈《關於加強國家網絡安全標準化工作的若干意見》〉,《中共網路資訊辦公室網》〈http://www.cac.gov.cn/2016-08/24/c_1119448735.htm〉。(瀏覽日期：2020 年 2 月 18 日)。

新華社，2017 年 10 月 27 日。〈習近平：決勝全面建成小康社會 奪取新時代中國特色社會主義偉大勝利——在中國共產黨第十九次全國代表大會上的報告〉,《中華人民共和國中央人民政府網》,〈http://www.gov.cn/zhuanti/2017-10/27/content_5234876.htm〉,(檢索日期：2020 年 3 月 12 日。)

新華網，2014 年 2 月 27 日。〈中央網絡安全和資訊化領導小組成立：從網絡大國邁向強國〉,《中國共產黨新聞網》,

〈http://cpc.people.com.cn/BIG5/n/2014/0227/c64094-24486382.html〉。(檢索日期 2020 年 2 月 15 日)。

資訊產業部辦公廳，2001 年 2 月 27 日。〈我國電信領域改革開放大事記〉，《中國資訊產業網》，〈http://www.cnii.com.cn/20020808/ca79451.htm〉。(檢索日期 2019 年 11 月 11 日)。

網與資料管理部〈兩化融合管理體系評估〉，2017 年 4 月 7 日。《中國電子技術標準化研究院網》，〈http://www.cesi.cn/lhrh/201704/2305.html〉。(瀏覽日期：2020 年 2 月 12 日)。

蒙克，2017 年 7 月 26 日。〈中情局局長：美國最大威脅來自中國而非俄國〉，《BBC 中文網》，〈https://www.bbc.com/zhongwen/trad/world-40735176〉。(檢索日期 2020 年 1 月 11 日)。

貳、英文部分

一、專書

Baldwin, David, 2002. *Key concepts in international political economy*, England: E. Elgar Pub. Co.

Booth, Ken, 1977. *Navies and Foreign Policy*. New York: Crane, Russak & Company, Inc..

Costello, John and Joe McReynolds, 2018. *China's Strategic Support Force: A Force for a New Era* ,Washington: National Defense University Press.

Donnelly, Jack, 2000. *Realism and International Relations*, New York: Cambridge University Press.

Mearsheimer, John, 2001. *The Tragedy of Great Power Politics*, New York: Norton.

Saunders, Phillip C, 2019. *Chairman Xi Remakes the PLA.* Washington D.C.: National Defense University Press.

Schmitt, Michael, 2013. Tallinn Manual on the International Law Applicable to Cyber warfare ,Cambridge ：Cambridge University Press.

Stokes, Mark, Jenny Lin and, L.C. Russell Hsiao, 2011. The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure, Virginia: Project 2049 Institute.

Waltz, Kenneth N., 1979. *Theory of International Politics*. Reading: Addison-Wesley.

二、期刊

Gilpin, Robert, 1984. “The Richness of the Tradition of Political Realism”, *International Organization*, Vol. 38, No.2.

Rose, Gideon, 1998. ”Neoclassical Realism and Theories of ForeignPolicy”, *World Politics*, Vol . 51, No. 1.

三、網路電子資料

2003, “The National Strategy to Secure Cyberspace,” *The White House*, <https://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf >.(Accessed 2020/1/26).

2003. “Declaration of Principles,”*World Summit on the Information Society*, <https://www.itu.int/net/wsis/docs/geneva/official/dop.html >.(Accessed 2020/2/26)

2011, ”International Strategy for Cyberspace,” *The White House*, <https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf >.(Accessed 2020/1/26)

2011,” The U.S. Department of Defense Strategy for Operating in Cyberspace,” *The U.S. Department of Defense*, <https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf >.(Accessed 2020/1/26).

2019. “Internet Usage and World Population Statistics estimates are for”, *Internet World Stats*,< https://www.internetworldstats.com/stats.htm>.(Accessed 2020/5/1).

Alyssa Yorgan, 2019. “10 key statistics on internet usage in Russia”,*Russian Search Marketing*,, <https://russiansearchmarketing.com/internet-usage-russia-2019-10-key-statistics/>.(Accessed 2020/4/1)

Bill Gertz, 2017. “PLA's hacking hotel,” *The Washington Times*, <https://www.washingtontimes.com/news/2017/jan/4/inside-the-ring-plas-hacking-hotel/>.(Accessed 2020/2/26)

David C. Gompert & Martin Libicki, 2014. “Cyber Warfare and Sino-American Crisis Instability,” *Survival*, Vol. 56, No. 4, pp. 7-22, *IISS*, <http://www.iiss.org/en/publications/survival/sections/2014-4667/survival--global-politics-and-strategy-august-september-2014-838b/56-4-02-gompert-and-libicki-04fc>. (Accessed 2020/3/26)

David E. Sanger, David Barboza, & Nicole Perlroth, 2013. “Chinese Army Unit Is Seen as Tied to Hacking Against U.S.,” *New York Times*, < https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html>.(Accessed 2020/4/26)

Declaration of Principles, 2003. ”*World Summit on the Information Society*, <

https://www.itu.int/net/wsis/docs/geneva/official/dop.html > (Accessed 2020/3/24)

Edited by William J. Drake, 2009. Internet Goverance: Creating Opportunties for all , *The Fourth Internet Governance Forum* ,. <https://www.intgovforum.org/multilingual/filedepot_download/3367/7>. (Accessed 2020/3/1)

Mark Mazzetti & David E. Sanger, 2013. “Security Leader Says U.S. Would Retaliate Against Cyberattacks,” *New York Times*, <http://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-posethreat-to-us.html>.(Accessed 2020/4/26)

四、官方文件

Office of the Security of Defense, 2018. “Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2018.” Washington D.C.: United States Department of Defense.