「避險」視角下中國對美國的網路強國戰略研究*

張 凱 銘

(國立臺中科技大學通識教育中心助理教授)

摘 要

過去多年間，中國在網路科技領域取得了突出的建設成果，成為當代國際網路事務要角。北京當局近期更提出「網路強國」戰略，試圖全面強化國家網路實力。中國在網路領域的進取，不僅對美國的固有優勢構成挑戰，也助長了美國政府對其戰略意圖的疑慮，從而增添雙邊關係的不穩定性。為瞭解中國網路建設藍圖與對美政策立場，本文審視了「網路強國」戰略的主要內容，及美國因素在其間的影響；同時透過國際關係研究中的「避險戰略」探討中國對美網路互動態樣，說明中國政府如何在網路事務中，同步推動對美國的有限抗衡及務實合作，以兼顧國家安全與利益發展需求。

關鍵詞：網路強國、美中關係、避險戰略、網路安全、網路衝突

* * *

壹、前 言

自改革開放時期以來，中國在政治、經濟與軍事影響力持續增長的同時，也憑藉占全球總數五分之一強的龐大網路用戶市場，成爲備受國際社會關注的網路大國。①基於對網路技術龐大潛力的認識，中國政府近年提出建設「網路強國」的構想，冀望進一步提升本國網路科技實力。總體以觀，中國當前推動的「網路強國」戰略牽涉範疇甚廣，舉凡數位經濟、技術研發、網路防務、線上輿情管理以至人才培育等政策面向

* 本文爲科技部補助專題研究計畫「美『中』網路空間競合之研究：從『避險戰略』分析」之部分研究成果，計畫編號：MOST 105-2410-H-025-001-，特此致謝。

註① "Press Release: China, India Now World's Largest Internet Markets," *International Telecommunication Union*, http://www.itu.int/en/mediacentre/Pages/2016-PR35.aspx. Accessed on April 20, 2017；Wayne M. Morrison, *China-U.S. Trade Issues* (Washington, D.C.: Congressional Research Service, 2017), p. 6.

DOI：10.30390/ISC.201809_57(3).0003

皆涵蓋其中，顯現旺盛的企圖心。②但中國在追求「網路強國」地位的過程中，如何於完善內部建設及治理的同時，有效處理與美國之間的網路互動，將是成敗關鍵所在。

回顧近代歷史，美國與中國的交往一向複雜且充滿權力算計，進入後冷戰時代後，隨著中國國力大幅提升，美中在形成深厚經貿連結的同時，彼此間的猜疑角力也持續深化，③這一現象在網路空間中有過之而無不及。部分學者注意到，網路事務已成爲當代美中關係最爲敏感的面向之一，兩國在其中的對立較其他領域更顯尖銳。④例如美國對中國的網路管制政策深爲反感，對解放軍網軍建設及大量源自中方的網路攻擊活動也頗有疑慮；而在中國看來，掌握技術優勢與關鍵資訊基礎設施的美國，不但積極建設網路戰力，更在「震網病毒」(Stuxnet) 等事件中使用網路武器攻擊他國。⑤然而，一如美中關係利害並存的雙面性，兩國在網路領域中雖不乏矛盾，但彼此在發展網路經濟、防範駭客及網路恐怖主義威脅等方面仍存在廣泛合作利益。這種利害交錯的關係形態，意味著中國政府在處理和美國間的網路互動時，須設法於安全與利益兩者間取得平衡，以免對「網路強國」的建設進程造成阻礙，甚或損及總體美中關係。⑥

本文以中國對美網路競合爲題，旨在探究中國政府在推動「網路強國」戰略的背景下，如何處理與美國於網路領域中的對立，同時保持雙邊合作交流不受影響。本文在研究過程中運用文獻分析法，廣泛蒐集檢析了與主題相關的政策文件、學術論著、領導人發言及媒體報導等文獻資料，藉以梳理中國政府近期的相關政策舉措。此外，爲求更深入且有系統地瞭解其行爲取向與意圖，文中援用國際關係學界中的「避險戰略」(Hedging Strategy) 作爲分析途徑，該戰略主張現代國家在交往過程中，爲求同步迴避安全損害與利益損失的雙重風險，往往綜合運用各種對抗性和合作性策略。「避險戰略」兼顧競合的研究視角與類型多元的操作框架，有助於引導研究者跨越零散瑣碎的時事資訊等表象，洞察國家行爲的基本態樣與深層意涵。

在以下篇幅中，本文首先將介紹「避險戰略」的內容與各種操作選項，其次分別說明中國目前的「網路強國」戰略規畫及美國因素對其造成之影響，隨後則依循「避險戰略」的操作框架逐一檢視中國近年在網路領域中對美國採取的各種策略作爲並探析其效用。

註② 「習近平：把我國從網絡大國建設成爲網絡強國」，**新華網**，http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm，檢索日期 2017 年 4 月 22 日。

註③ Kenneth G. Lieberthal and Wang Jisi, *Addressing U.S.-China Strategic Distrust* (Washington, D.C.: The Brookings Institution, 2012), pp. 34~38.

註④ Kenneth G. Lieberthal and Peter W. Singer, *Cybersecurity and U.S.-China Relations* (Washington, D.C.: The Brookings Institution, 2012), p. 6.

註⑤ David E. Sanger, "Obama Order Sped up Wave of Cyberattacks against Iran," *The New York Times*, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0. Accessed on April 20, 2017.

註⑥ Mark A. Stokes and L. C. Russell Hsiao, *Countering Chinese Cyber Operations: Opportunities and Challenges for U.S. Interests* (Arlington: Project 2049 Institute, 2012), pp. 2~12；周琪、汪曉風，「網絡安全與中美新型大國關係」，**當代世界**，第 11 期 (2013 年 11 月)，頁 30~34。

貳、國際關係研究中的「避險戰略」

面對後冷戰時代利害關係日形複雜的國際格局，部分國際關係學者注意到傳統巨型理論的研究視角已不足以完整觀照現代國家間的複雜互動，因而嘗試跨越過往的研究藩籬，在不同理論模型中擷取有益學術資源並予融合，進以提出更具彈性且能貼切對應現實情勢的理論學說。自平衡理論（Balancing Theory）發展而來的「避險戰略」正是此波研究風潮中的分支之一。本文以中國對美網路競合爲研究主題，爲求較具系統性地瞭解中國政府近年如何在網路科技領域中和執掌技術優勢的美國互動並探究其戰略思維，文中將運用該戰略的研究框架進行觀察，於下對「避險戰略」的發展背景與主要論述內容進行回顧與介紹。

一、「避險戰略」的發展脈絡

自國際關係學界研究傳統以觀，源於現實主義的平衡理論向來是各方學者分析國際安全事務的重要途徑。諸如「權力平衡」（Balance of Power）、「威脅平衡」（Balance of Threat）與「利益平衡」（Balance of Interests）等觀點，分由不同角度探討國家在面臨他國挑戰時，爲何與如何透過軍備競賽及締結同盟等手段加以抗衡，或採取扈從（Bandwagoning）策略順服對方。⑦ 1990 年代後，冷戰終結與全球化現象擴散，導致國際社會的競合特徵日益突出，部分學者隨之注意到傳統平衡理論的論述漸難對應現實變遷，⑧因而嘗試改造理論架構，尋找足以切合國際現勢的分析方向，各式新興研究如「柔性平衡理論」（Soft Balancing Theory）、「制度平衡理論」（Institutional Balancing Theory）與「避險戰略」等由此陸續浮現。⑨

「避險」（Hedging）一詞本爲財金專業詞彙，意指投資者在情勢混沌不明的情況下，以「兩面下注」形式配置資源以規避風險。⑩這一詞彙在 1990 年代後期被導入國際關係學界，用於詮釋當代國家在面臨與他國間既存在安全紛爭又建有利益連結時，如何同步運用「競爭」與「合作」兩類性質相反的作法加以因應。

美國智庫「蘭德公司」（RAND Corporation）在 1999 年發表的研究報告「美國與

註⑦ Randall Schweller, “Managing the Rise of Great Powers: History and Theory,” in Alastair Iain Johnston and Robert S. Ross eds., *Engaging China: The Management of an Emerging Power*（London: Routledge, 1999）, pp. 9~12.

註⑧ John G. Ikenberry ed., *America Unrivaled: The Future of the Balance of Power*（Ithaca: Cornell University Press, 2002）, pp. 2~6.

註⑨ 相關研究如：T. V. Paul, “The Enduring Axioms of Balance of Power Theory,” in T. V. Paul, James J. Wirtz, and Michel Fortmann eds., *Balance of Power: Theory and Practice in the 21st Century*（Stanford: Stanford University Press, 2004）, pp. 1~28；Robert A. Pape, “Soft Balancing Against the United States,” *International Security*, Vol. 30, No. 1（Summer 2005）, pp. 7~45；Kai He, “Institutional Balancing and International Relations Theory: Economic Interdependence and Balance of Power Strategies in Southeast Asia,” *European Journal of International Relations*, Vo. 14, No. 3（September 2008）, pp. 489~518.

註⑩ 潘曉霞、黃建濱，「Hedging 的交際功能」，**美中外語**，第 2 卷第 7 期（2004 年 7 月），頁 11~18。

崛起中的中國：戰略與軍事意涵」(*The United States and a Rising China: Strategic and Military Implications*) 中，建議美國政府在應對中國崛起時，可捨棄冷戰時代的「圍堵」(Containment) 思維，改採兼具抗衡與合作的「避險」作爲政策方針，是最早將「避險」一詞引入國際關係研究的論著。⑪此後，「避險」這一概念漸受國際關係學界關注，許多著述先後面世。例如美國俄亥俄大學 (Ohio University) 教授維茨曼 (Patricia A. Weitsman) 主張當代中小型國家在面臨潛在安全威脅時，基於實力差距或利益考量，將運用「避險同盟」(Hedging Alliance) 等混合式戰略，既在暗中強化與他國的安全合作，亦維持與對手交往以兼顧本國安全及利益。⑫澳洲國立大學 (Australian National University) 教授吳翠玲 (Evelyn Goh) 也認爲「避險」是中小型國家面對大國挑戰時用以自保的戰略選擇，並提出多種策略選項，爲「避險戰略」建立初步操作框架。⑬

美國國家安全會議 (National Security Council) 前亞洲事務資深主任麥艾文 (Evan S. Medeiros) 在 2006 年發表的論文「戰略避險與亞太區域穩定的未來」(Strategic Hedging and the Future of Asia-Pacific Stability) 中，指出「避險」不僅適用於中小型國家，也可用以解析美國和中國等強權國家的政策動向。⑭馬來西亞國民大學 (Universiti Kebangsaan Malaysia) 教授郭清水 (Kuik Cheng-Chwee) 則是近年對「避險戰略」研究最爲深入的學者，其論著大幅充實了該戰略的內容。⑮

回顧上述歷程，國際關係研究中的「避險」本爲單純的形容語彙，但在過往十數年中漸受相關學者重視，進而被賦予更爲豐富的學術意涵，形成獨立論述及操作架構，成爲學界中的一項新興理論研究主題。

二、「避險戰略」的內涵與操作形態

綜覽各方學者對「避險戰略」的闡述，可歸納爲以下三點：

第一，「避險戰略」的基本概念：國際關係學界中的「避險戰略」，承繼現實主義等主流理論基底，大抵接納了「國家中心論」(State-centric Approach)、「理性行爲體

註⑪ Zalmay M. Khalilzad et al., *The United States and a Rising China: Strategic and Military Implications* (Santa Monica: RAND Corporation, 1999), pp. 63~72.

註⑫ Patricia A. Weitsman, *Dangerous Alliances: Proponents of Peace, Weapons of War* (Stanford, CA: Stanford University Press, 2004), pp. 29~30.

註⑬ Evelyn Goh, *Meeting the China Challenge: The U.S. in Southeast Asian Regional Security Strategies* (Washington, D.C.: East-West Center, 2005), pp. 2~4.

註⑭ 美國小布希 (George W. Bush) 政府於 2006 年公布的「國家安全戰略報告」與「四年期國防總檢報告」中，也都以「避險」一詞描述其國際戰略思維，請見：Evan S. Medeiros, "Strategic Hedging and the Future of Asia-Pacific Stability," *The Washington Quarterly*, Vol. 29, No. 1 (Winter 2005~2006), pp. 145~146；The White House, *National Security Strategy 2006* (Washington, D.C., The White House, 2006), pp. 41~42；U.S. Department of Defense, *Quadrennial Defense Review Report 2006* (Washington, D.C.: U.S. Department of Defense, 2006), pp. 28~30.

註⑮ Cheng-Chwee Kuik, "The Essence of Hedging: Malaysia and Singapore's Response to a Rising China," *Contemporary Southeast Asia*, Vol. 30, No. 2 (August 2008), pp. 159~185.

假定」(Rational Actor Assumption)與「物質主義」(Materialism)本體論等觀點，主張作爲理性行爲體的國家，面對無政府狀態(Anarchy)下的安全稀缺，及國際互賴格局中的利益交連，與他國互動時將以同時迴避「安全損害風險」與「利益損失風險」爲目標。⑯

第二，「避險戰略」的適用情境：「避險戰略」是全球化時代國際競合格局下的理論演進成果，適用於他國對本國造成安全壓力或有限威脅，而彼此間同時存在一定程度利益連結的情況。由於威脅非屬強烈，且欲保全共同利益，國家並無立即締結對抗性同盟，或開展軍備競賽以正面抗衡的迫切必要，而可在這種利害交錯的情境中探求兩全之道。⑰

第三，「避險戰略」的運作特徵：「避險」一詞本有「兩面下注」的意涵，因此在國際關係研究中，「避險戰略」指國家同時應用「對抗性」和「合作性」作爲，以求既消除他國帶來的安全威脅，又與其保持合作交流以獲利。與傳統「平衡理論」不同，「避險戰略」的對抗性作爲係爲控管安全威脅，而非爲壓制對手或改變國際權力分配格局。⑱此外，基於維護利益的考量，其採取的抗衡措施一般具有溫和節制等特徵以免過度激化對立。⑲

受到研究起步時程較晚的影響，各方學者對於「避險戰略」具體操作形態的觀點目前尚存歧異。例如維茨曼的研究側重探討國家如何透過策略性結盟達成「避險」目標。⑳美國加州大學柏克萊分校(University of California, Berkeley)教授彭佩爾(T. J. Pempel)等人將「制度平衡」(Institutional Balancing)視作一種「避險」策略。㉑吳翠玲經由分析東南亞國家外交案例，提出三種「避險」策略選項：具對抗性質的「間接或柔性平衡」(Indirect or Soft Balancing)、具合作性質的「複合式交往」(Complex Engagement)，及藉由多邊機制等途徑實施的「牽連」(Enmeshing)。㉒郭清水則分別提出「間接平衡」(Indirect Balancing)與「優勢拒阻」(Dominance Denial)兩類「風險應變型」(Risk-Contingency)策略，以及「經濟務實主義」(Economic Pragmatism)、「約束性交往」(Binding Engagement)和「有限扈從」(Limited Bandwagoning)等三

註⑯ 蔡明彥、張凱銘，「『避險』戰略下大國互動模式之研究：以美中亞太戰略競合爲例」，**遠景基金會季刊**，第 16 卷第 3 期(2015 年 7 月)，頁 6~7。

註⑰ Cheng-Chwee Kuik, Nor Azizan Idris and Abd Rahim Md Nor, "The China Factor in the U.S. 'Reengagement' with Southeast Asia: Drivers and Limits of Converged Hedging," *Asian Politics & Policy*, Vol. 4, No. 3 (July 2012), pp. 316~317.

註⑱ 蔡明彥、張凱銘，「『避險』戰略下大國互動模式之研究：以美中亞太戰略競合爲例」，頁 7。

註⑲ Cheng-Chwee Kuik and Kong Chian Lee, "Rising Dragon, Crouching Tigers?" *Biblioasia*, Vol. 3, No. 4 (January 2008), pp. 5~6.

註⑳ Patricia A. Weitsman, *Dangerous Alliances: Proponents of Peace, Weapons of War*, pp. 29~30.

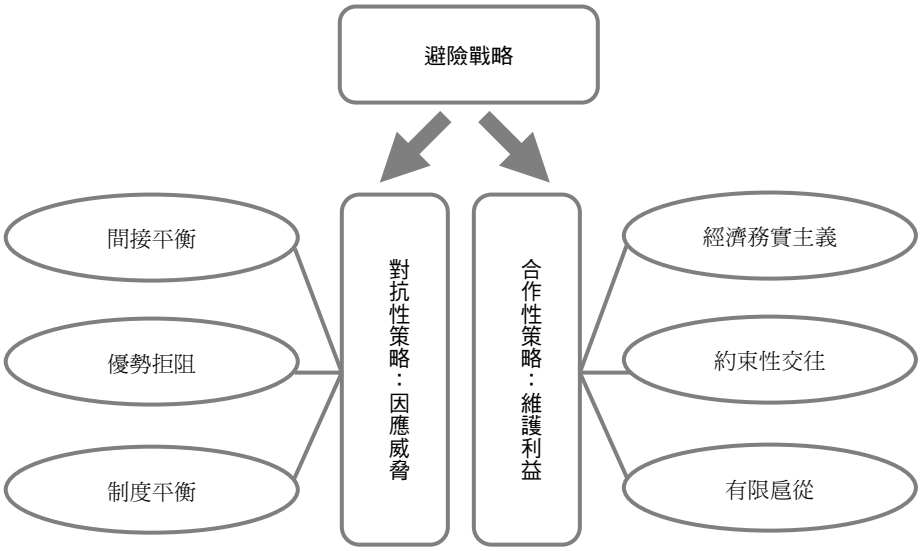
註㉑ T. J. Pempel, "Soft Balancing, Hedging, and Institutional Darwinism: The Economic-Security Nexus and East Asian Regionalism," *Journal of East Asian Studies*, No. 10 (2010), pp. 212~219；Seungjoo Lee, *The Evolutionary Dynamics of Institutional Balancing in East Asia* (Seoul: The East Asia Institute, 2012), pp. 14~15.

註㉒ Evelyn Goh, *Meeting the China Challenge: The U.S. in Southeast Asian Regional Security Strategies*, pp. 3~4

類「報償最大化型」(Return-Maximizing) 策略。[23]

雖然名稱各有不同，但上述各種策略選項的實際內涵多所重疊，故本文在綜整既有研究論點的基礎上，將「避險戰略」的操作框架整合如下 (請見圖 1)：

圖 1　「避險戰略」操作策略示意圖



資料來源：作者自製。

(一) 對抗性策略

1.間接平衡：「避險戰略」的「間接平衡」選項，源自傳統平衡理論的「內部平衡」(Internal Balancing) 概念。「內部平衡」意指國家藉由提升安全實力，產生防範對手威脅並傳達警示訊息等效用。[24]但「間接平衡」策略僅要求有限及非針對性的實力強化，並不主張以全面超越對手爲目標或開展軍備競賽等作法，以免過度激化彼此間的對立。

2.優勢拒阻：「避險戰略」的「優勢拒阻」選項，源自傳統平衡理論的「外部平衡」(External Balancing) 概念。「外部平衡」意指國家面臨安全威脅時，經由締結國際同盟等作法制約對手。[25]但「優勢拒阻」策略認爲在威脅程度有限且欲維持合作空間的情況下，國家無須組建正式同盟以壓制對手並改變國際權力結構，而可以非正式跨國協調爲主。

註 [23]　Cheng-Chwee Kuik, "The Essence of Hedging: Malaysia and Singapore's Response to a Rising China," pp. 166~171.

註 [24]　Kenneth N. Waltz, *Realism and International Politics* (New York: Taylor & Francis, 2008), p. 186；Denny Roy, "Southeast Asia and China: Balancing or Bandwagoning?" *Contemporary Southeast Asia*, Vol. 27, No. 2 (August 2005), pp. 306~310.

註 [25]　Kenneth N. Waltz, *Theory of International Politics* (New York: McGraw-Hill, 1979), pp. 125~128.

3.制度平衡：「避險戰略」的「制度平衡」選項，與國際關係研究中的「制度平衡理論」相仿，㉖視國際機制爲可資運用的抗衡工具，建議國家透過建立國際多邊機制或主導既有機制等途徑，整合成員國力量並操作機制規範，削弱對手的行動自由及合法性以發揮抗衡效用。

（二）合作性策略

1.經濟務實主義：「避險戰略」的「經濟務實主義」選項，認爲國家在因應他國威脅時，倘若彼此間在經貿等領域中存在利益連結，而對方造成的安全危害非屬重大迫切，則應在予以制約的同時，維持甚或增進合作關係以免本國利益蒙受損失。

2.約束性交往：「避險戰略」的「約束性交往」選項，建議國家可與競爭對手建立制度性交流機制以維持有序互動。與一般外交相比，制度性交流機制更爲穩定可測，若非遭遇重大事件衝擊而中斷，多可長期維繫，參與國家可透過定期會談增進互信與合作空間，進而建立互動規範，甚或影響對手的認知。

3.有限扈從：「避險戰略」的「有限扈從」選項，認爲中小型國家在面臨強權大國造成的安全壓力時，由於實力差距過大導致對抗性策略無法發揮效用，可在部分議題上選擇性順服，以迴避衝突或藉此在其他方面換取利益，但並不因此捨棄本國外交政策自主性，或斷絕與其他國家的交往。㉗

上述六項策略分別展現抗衡和合作兩類相反的性質，同時具備溫和有限等特徵，說明了「避險戰略」在實務情境中的操作態樣。國家可根據自身與對手的條件及彼此關係形勢，選擇合宜的對抗性與合作性策略並行運用，以達到風險迴避的目標。

值得注意的是，國際關係學界近年在探討「避險戰略」與「柔性平衡」等新興理論的過程中，對於意圖判斷問題時有爭論。部分學者質疑，觀察者如何確認國家行爲的背後確實具備「避險」或「平衡」等意圖，而非僅是例行性或缺乏直接聯繫的外交活動？㉘然如前文所述，「避險戰略」等新興研究，在學術脈絡上承繼「國家中心論」和「理性行爲體假定」等主流理論基礎。於其論述中，作爲理性行爲體的國家，必然在無政府狀態下遵行「自助」（self-help）原則以確保自身的生存發展。由此，在利害交錯的情境中，國家自然會採取兼具抗衡及合作性質的行爲，以迴避可能危害安全和利益的風險。㉙布蘭迪斯大學（Brandeis University）教授阿特（Robert J. Art）等學者

註㉖ 「制度平衡理論」是國際關係新興平衡理論研究中，對於國際機制可發揮的平衡效用論述最爲深入的分支，有關其內容可參考：Kai He, *Institutional Balancing in the Asia Pacific, Economic Interdependence and China's Rise*（New York: Routledge, 2009）, pp. 8~14.

註㉗ Cheng-Chwee Kuik and Kong Chian Lee, "Rising Dragon, Crouching Tigers?" pp. 6~11.

註㉘ Stephen G. Brooks and William C. Wohlforth, "Hard Times for Soft Balancing," *International Security*, Vol. 30, No. 1（Summer 2005）, pp. 72~108；Keir A. Lieber and Gerard Alexander, "Waiting for Balancing: Why the World is not Pushing Back," *International Security*, Vol. 30, No. 1（Summer 2005）, pp. 109~139.

註㉙ Jurgen Ruland, "Interregionalism and International Relations: Reanimating an Obsolescent Research Agenda?" in Francis Baert, Tiziana Scaramagli and Fredrik Soderbaum eds., *Intersecting Interregionalism: Regions, Global Governance and the EU*（Dordrecht: Springer, 2014）, pp. 22~25.

因而主張，研究者在探討國家行爲動機時，應將行爲效用作爲意圖判斷的基準。㉚易言之，國家應對他國的政策作爲，若形式上符合「避險戰略」的論述內容，且有降低安全威脅及利益損害風險的效果，即爲對「避險戰略」的運用。

整體而言，「避險戰略」在現實主義理論的基礎上拓展了研究視野，在安全保障議題外，也將合作利益納入考量以完整觀照當代國際政治運作。本文認爲該戰略兼顧競合的觀察視角，應可對中國近年在網路領域與美國的互動舉措提供可資依循的觀察框架，揭示中國政府制定推行的政策作爲中蘊含的風險迴避思路。在以下篇幅中，本文將回顧中國近年積極推行的「網路強國」戰略，及其與美國在網路領域利害交連的關係形態，並透過「避險戰略」的操作框架分析北京當局近年採取的相關舉措與意涵。

參、「避險戰略」視角下的中國對美網路競合

一、中國的「網路強國」戰略規畫

現任中國國家領導人習近平在任福建省長期間，便展露對網路科技的高度重視，在國際歐亞科學院（International Eurasian Academy of Sciences, IEAS）等智庫協助下，推出「數字福建」建設計畫，嘗試在省務行政中擴大應用網路科技並建立數位管理體系。㉛接任中國共產黨總書記後的首個京外參訪行程，習近平也選擇遠赴廣東視察「騰訊」等網路企業的營運狀況。㉜此後，中國政府陸續發表多項有關網路科技的法規政策，並提出「網絡強國」戰略，宣示將全面提升國家網路實力。綜觀北京當局近年施政作爲與論述，可將該戰略的重點內容彙整爲以下數點（請見圖 2）：

（一）調整網路管理體制：中國過往的網路治理權責分散，諸多黨政軍機構皆參與其間，導致政策執行長期欠缺效能。㉝爲改善此現象，中國於 2014 年 2 月成立「中共中央網絡安全和信息化領導小組」，由習近平親任組長，並設置「中央網絡安全和信息化領導小組辦公室」和「中國國家互聯網信息辦公室」等執行單位，㉞顯示中國政府期望經由建立具充足權威的核心建制，有效確立治理方針並統籌資源以推進「網路強

註㉚　Robert J. Art, "Striking the Balance," *International Security*, Vol. 30, No. 3 (Winter 2005-06), pp. 178~180；Kai He and Huiyun Feng, "If Not Soft Balancing, Then What?" *Security Studies*, Vol. 17, No. 2 (April 2008), pp. 365~370.

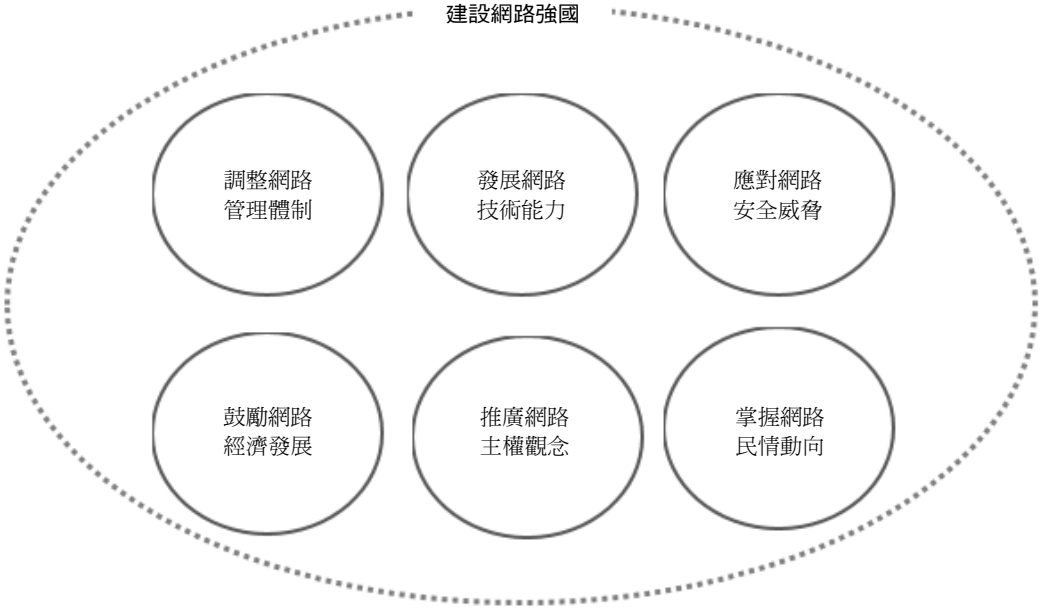
註㉛　「從『數位福建』到『數位中國』習近平擘畫科技發展新高度」，人民網，http://politics.people.com.cn/n1/2016/0427/c1001-28308778.html，檢索日期 2017 年 4 月 22 日。

註㉜　「習近平『南巡』：訪前海察騰訊探母親」，文匯網，http://news.wenweipo.com/2012/12/08/IN1212080018.htm，檢索日期 2017 年 4 月 22 日。

註㉝　FireEye Corporation, *Red Line Drawn: China Recalculates Its Use of Cyber Espionage* (Milpitas: FireEye Corporation, 2016), p. 5；Mikk Raud, *China and Cyber: Attitudes, Strategies, Organisation* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2016), pp. 15~18.

註㉞　「習近平親自出馬，主掌中國網絡安全」，BBC 中文網，http://www.bbc.com/zhongwen/trad/china/2014/02/140227_china_xi_web_security，檢索日期 2017 年 4 月 22 日。

圖 2　中國「網路強國」戰略重點示意圖



資料來源：作者自製。

國」建設。㉟

（二）發展網路技術能力：雖然擁有龐大用戶市場，但中國目前對先進網路技術的掌握仍嫌不足，習近平強調這一情形若未獲改善，將使中國的網路系統與產業受制於人，對國家安全造成不利影響。㊱故中國政府近年的網路施政格外著重技術開發，除責成官方科研單位加強鑽研外，也鼓勵民間企業組建產業聯盟，藉由資源共享加速技術創新。㊲同時籌組「網絡空間安全學院」等人才培育單位，㊳並設計更具彈性的人員進用及外籍專家延攬制度以提升研發能量。㊴

（三）應對網路安全威脅：「中國國家互聯網信息辦公室」在 2016 年 12 月發表的「國家網絡空間安全戰略」中，由政治、經濟、文化、社會與國際等五大面向論述網路科技可能造成的威脅。爲因應上述威脅，中國政府責成相關部門加強維護國家關鍵信息基礎設施，設置「網絡安全監測預警機制」、「網絡安全重大事件應急處置機制」、

註㉟　汪玉凱，「中央網絡安全和信息化領導小組的由來及其影響」，**中國信息安全**，第 3 期（2014 年 3 月），頁 24~28。

註㊱　「習近平在網信工作座談會上的講話全文發表」，**新華網**，http://news.xinhuanet.com/politics/2016-04/25/c_1118731175.htm，檢索日期 2017 年 4 月 22 日。

註㊲　「習近平：讓互聯網更好造福國家和人民」，**新華網**，http://news.xinhuanet.com/politics/2016-04/19/c_1118672059.htm，檢索日期 2017 年 4 月 22 日。

註㊳　「東莞理工學院成立全國首個網絡空間安全學院」，**中國新聞網**，http://www.chinanews.com/gn/2017/03-11/8171430.shtml，檢索日期 2017 年 4 月 22 日。

註㊴　「烏鎮指數：全球人工智能發展報告（精華篇）」，**思客－新華網高端智庫平台**，http://sike.news.cn/hot/pdf/10.pdf，檢索日期 2018 年 6 月 22 日。

「網絡安全信息有序共用機制」，並透過國際合作加強查緝網路犯罪活動，以防範各種數位安全危害。㊵

（四）鼓勵網路經濟發展：隨著經濟進入「新常態」階段，中國政府認爲具跨領域功能的網路科技可爲下一階段的經濟增長提供強大動力，故陸續提出「寬帶中國」、「互聯網+」、「雲計算創新發展」等計畫，希望將網路技術導入各種產業，形成「以資訊流帶動技術流、資金流、人才流、物資流」的格局；同時設下爲貧困農村擴大鋪設光纖網路，加速偏遠地區無線區域網路（Wireless LAN, WLAN）構建等目標，㊶以改善網路城鄉失衡問題，並在建設過程中創造經濟效益。㊷

（五）推廣網路主權觀念：中國近年的國家網路戰略論述格外強調網路主權的重要性。㊸「中國國家互聯網信息辦公室」指出，網路主權意謂國家主權及於網路空間，政府有權決定本國網路發展模式和政策法令，並得採取必要措施防衛網路系統及管理公民網路活動，各國應相互尊重彼此的主權地位，不干涉他國網路事務。㊹中國黨政領導人及相關部門官員皆曾於公開場合對外提倡網路主權觀念並呼籲各國採納。㊺近期通過的新版「國家安全法」與「網絡安全法」亦將網路主權明文納入其中。㊻

（六）掌握網路民情動向：中國政府在「網路強國」建設規畫中，反覆強調控管網路輿情的重要性，㊼既強硬箝制具危險性的言論，也並用疏導安撫等溫和作法。例如

註㊵ 「國家網絡空間安全戰略全文」，**中央網絡安全和信息化領導小組辦公室**，http://www.cac.gov.cn/2016-12/27/c_1120195926.htm，檢索日期 2017 年 4 月 16 日；「關於促進移動互聯網健康有序發展的意見」，**中國國務院**，http://news.xinhuanet.com/politics/2017-01/15/c_1120315481.htm，檢索日期 2017 年 8 月 15 日；「國家網絡安全事件應急預案」，**中國國家互聯網信息辦公室**，http://news.xinhuanet.com/zgjx/2017-06/28/c_136400422.htm，檢索日期 2017 年 8 月 15 日。

註㊶ 「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」，**中國人大網**，http://www.npc.gov.cn/npc/dbdhhy/12_4/2016-03/18/content_1985670.htm，檢索日期 2017 年 4 月 22 日。

註㊷ 中國互聯網絡信息中心，**第 39 次中國互聯網絡發展狀況統計報告**（北京：中國互聯網絡信息中心，2017 年），頁 37；「農村電子商務發展的戰略與政策」，**新華網**，http://news.xinhuanet.com/tech/2017-03/09/c_1120593562.htm，檢索日期 2017 年 4 月 22 日。

註㊸ 同註㊱。

註㊹ 「國家網絡空間安全戰略全文」，前引文。

註㊺ 「習近平巴西談互聯網治理」，**新華網**，http://news.xinhuanet.com/world/2014-07/17/c_1111673270.htm，檢索日期 2017 年 4 月 22 日；「習近平向首屆世界互聯網大會致賀詞」，**新華網**，http://news.xinhuanet.com/politics/2014-11/19/c_1113319278.htm，檢索日期 2017 年 4 月 22 日；「李克強同世界互聯網大會中外代表座談時強調，促進互聯網共用共治，推動大眾創業萬眾創新」，**新華網**，http://news.xinhuanet.com/politics/2014-11/20/c_1113340416.htm，檢索日期 2017 年 4 月 22 日。

註㊻ 「中華人民共和國國家安全法」，**中國全國人民代表大會**，http://www.npc.gov.cn/npc/xinwen/2015-07/07/content_1941161.htm，檢索日期 2017 年 4 月 20 日；「中華人民共和國網絡安全法」，**中國全國人民代表大會**，http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm，檢索日期 2017 年 4 月 20 日。

註㊼ 「網絡強國，習近平呼籲對網絡輿論的引導」，**多維新聞**，http://china.dwnews.com/news/2016-10-09/59774082.html，檢索日期 2017 年 4 月 20 日；新華網網絡輿情監測分析中心，**2016 年度社會熱點事件網絡輿情報告**（北京：新華網網絡輿情監測分析中心，2017 年），頁 16。

習近平在網路事務會議中要求各級機關應在網上瞭解民意、回應質疑。[48] 2013 年發表的「中共中央關於全面深化改革若干重大問題的決定」，亦要求黨政部門推動政務資訊化，籌設網路信訪制度以利民眾反映心聲。[49]但中國政府也強調網路並非「法外之地」，相關部門仍應積極查緝網路中的危險思想和禁忌言論，並建立網路突發事件應變機制。[50]

二、美國因素對中國網路戰略發展的影響

在中國致力建設「網路強國」的同時，網路事務也逐漸成爲美中關係的敏感領域。對中國而言，美國因素的影響爲其推動國家網路戰略發展時無法忽視的關鍵，於下分三點說明：

（一）美國的網路技術優勢

回顧歷史，美國軍方與科研機構是近代網路技術高速發展的主要推手。時至今日，美國在網路領域仍保持技術領先，許多廣爲各國採用的資訊產品如搜尋引擎、社交媒體與電腦晶片等皆來自美國企業。[51]此外，美國「國家電信暨資訊管理局」（National Telecommunications and Information Administration, NTIA）長期透過監管「網際網路號碼分配機構」（Internet Assigned Numbers Authority, IANA）而掌握關鍵的「網域名稱系統」（Domain Name System, DNS）管理權限，全球 13 組根域名伺服器中的 10 組亦位於其境內，從而對網際網路頂級域名分配享有極大影響力。[52]美國也憑藉前述優勢形塑國際網路管理規則，要求各國接受網路自由（Freedom Online）與網路人權（Human Rights Online）理念，尊重網際網路的開放、自由與無國界特質。但隨著決意建設「網路強國」的中國大力強調提升技術自主能力及維護網路主權的重要性，勢將和美國的既有優勢產生矛盾。如同總體層次的雙邊關係，美中在網路空間中同樣呈現新興強權與既存強權間的對立態勢。[53]

註 [48] 「中共中央政治局進行第 36 次集體學習，習近平主持」，**央廣網**，http://china.cnr.cn/news/20161010/t20161010_523185107.shtml，檢索日期 2017 年 4 月 22 日。

註 [49] 「授權發佈：中共中央關於全面深化改革若干重大問題的決定」，**新華網**，http://news.xinhuanet.com/politics/2013-11/15/c_118164235.htm，檢索日期 2017 年 4 月 22 日。

註 [50] 「互聯網新聞信息服務單位約談工作規定」，**人民網**，http://politics.people.com.cn/n/2015/0429/c1001-26920835.html，檢索日期 2017 年 8 月 15 日；「習近平在網信工作座談會上的講話全文發表」，前引文；「網絡產品和服務安全審查辦法（試行）」，**中國國家互聯網信息辦公室**，http://www.cac.gov.cn/2017-05/02/c_1120904567.htm，檢索日期 2017 年 8 月 15 日。

註 [51] Raphael Cohen-Almagor, "Internet History," *International Journal of Technoethics*, Vol. 2, No. 2 (April-June 2011), pp. 45~64.

註 [52] 王德培，**再平衡：中國的優勢與美國的強勢**（上海：文匯出版社，2013 年），頁 122~123。

註 [53] The White House, *International Strategy for Cyberspace* (Washington, D.C.: The White House, 2011), p. 5；Scott Busby, "10 Things You Need to Know about U.S. Support for Free Internet," *IIP Digital*, http://iipdigital.usembassy.gov/st/english/article/2014/05/20140530300596.html#ixzz4XMASG4Pj. Accessed on April 20, 2017.

（二）美國對中國的負面認知

在技術層面之外，長期關注網路安全的美國也視中國爲主要威脅來源：[54]

首先，美國政府近年在許多場合，反覆向中國強調網路安全與自由保障的重要性及其關切。例如美國前總統歐巴馬（Barack Obama）在習近平就任時發送的賀電中，便提及美方對日益增多的網路攻擊深感憂慮。美國政府在過去幾屆的美中元首峰會，也將改善網路安全與維護網路智慧財產權列爲會談焦點，要求中國在相關議題上合作應對。[55]美國國務卿和國防部長等外交及防務部門首長，也多次在公開場合批判源自中國的大量網路竊密及攻擊事件，並呼籲北京當局加強管制非法網路活動同時提升對網路人權的保障，[56]而美國司法部更於 2014 年 5 月時以網路商業間諜罪名起訴五名解放軍軍官。[57]經由此類作法，美國不僅向中國與國際社會明確傳達自身對網路安全與自由的重視，也將破壞網路秩序的責任歸於中國，將其塑造爲國際網路環境的主要威脅來源。

註 [54] Lisa O. Monaco, “Counterterrorism, Cybersecurity, and Homeland Security,” *Council on Foreign Relations*, http://www.cfr.org/cybersecurity/counterterrorism-cybersecurity-homeland-security/p38642. Accessed on April 22, 2017.

註 [55] 回顧近年各次美中元首會談，可發現網路安全始終是雙方磋商重點，美國總統與其團隊反覆向中方強調維護網路安全與處理中國方面活躍的網路間諜活動等問題的重要性。請參考：Nicole Perlroth, “Cyberattacks a Topic in Obama Call With New Chinese President,” *The New York Times*, https://bits.blogs.nytimes.com/2013/03/14/cyberattacks-prominent-in-obama-call-with-new-chinese-president/?_r=0. Accessed on April 22, 2017； “Press Briefing by National Security Advisor Tom Donilon,” *The White House*, https://obamawhitehouse.archives.gov/the-press-office/2013/06/08/press-briefing-national-security-advisor-tom-donilon. Accessed on April 22, 2017；Anugrah Kumar, “Obama, Xi Jinping Meet in California to Discuss North Korea, Cybersecurity,” *The Christian Post*, http://www.christianpost.com/news/obama-xi-jinping-meet-in-california-to-discuss-north-korea-cybersecurity-97603/. Accessed on April 22, 2017；Dan Roberts, “US and China Back off Internet Arms Race but Obama Leaves Sanctions on the Table,” *The Guardian*, https://www.theguardian.com/us-news/2015/sep/25/us-china-cyber-security-obama-xi-jinping-inconclusive-summit. Accessed on April 10, 2018；陳一新，「美『中』雙方在歐習會的得失及與對兩岸的影響」，**展望與探索**，第 13 卷第 10 期（2015 年 10 月），頁 6~8。

註 [56] 例如曾任美國國務卿的希拉蕊（Hillary Clinton）與凱瑞（John F. Kerry），都曾點名批判中國的網路竊密活動及其對網路人權的侵害。而曾任美國國防部長一職的海格（Chuck Hagel）與卡特（Ashton B. Carter）等官員，也在公開演說和「香格里拉對話」（The Shangri-La Dialogue, SLD）等場合中，向外界闡述源自中國的網路間諜活動如何危害美國的國家安全。請見：Hillary Clinton, “Remarks on Internet Freedom,” *American Institute in Taiwan*, https://www.ait.org.tw/en/officialtext-ot1004.html. Accessed on April 22, 2017；“Hagel in Singapore on U.S. Security Policy in Asia-Pacific Region,” *U.S. Department of Defense*, http://iipdigital.usembassy.gov/st/english/texttrans/2013/06/20130601148324.html#ixzz4XMHSZORO. Accessed on April 22, 2017；Tal Kopan, “Kerry: ‘Very Likely’ China, Russia Read my Emails,” *CNN*, https://edition.cnn.com/2015/08/11/politics/kerry-emails-chinese-russian-hackers/index.html. Accessed on April 10, 2018；USA Features Media, “SECDEF Carter Shifts Focus to Chinese Cyber-espionage as Shangri-La Summit Approaches,” *Glitch News*, http://glitch.news/2016-06-08-secdef-carter-shifts-focus-to-chinese-cyber-espionage-as-shangri-la-summit-approaches.html. Accessed on April 10, 2018.

註 [57] “US-China Cyber Security Working Group Meets,” *BBC News*, http://www.bbc.com/news/world-asia-china-23177538. Accessed on April 22, 2017.

其次，美國資安企業持續追查中國與對美網路攻擊的關連，相關調查結論並獲官方肯認。例如美國網路安全公司「麥迪安特」(Mandiant Corporation) 在 2013 年 2 月揭露解放軍 61398 部隊長期入侵美國網路系統時，[58]美國眾議院情報委員會 (House Intelligence Committee) 主席與國家安全會議發言人等皆對調查報告表達認同，[59]當另一資安企業「群擊」公司 (CrowdStrike Corporation) 揭露解放軍網軍 61486 部隊資訊時，同樣獲得官員與媒體的呼應。[60]

此外，美國近年許多政策文件皆直指中國爲其網路安全威脅，例如 2014 年版「四年期國防總檢報告」(Quadrennial Defense Review Report)、2015 年版「國家安全戰略報告」(National Security Strategy)、2016 年版「中國軍力與安全發展報告」(Military and Security Developments Involving the People's Republic of China)，及美中經濟暨安全檢討委員會 (U.S.-China Economic and Security Review Commission, USCC) 的多份例行報告，皆提及中國試圖透過網路科技開發與網路間諜活動削弱美國的經濟與軍事優勢。[61]而美國國務院與國會亦在人權事務等報告文件中嚴厲批判中國政府操弄網路輿情與箝制線上言論的作法嚴重侵害人權。上述情況顯示美國已將中國視作網路領域的重要競爭對手，認爲中國不但挑戰其優勢地位，亦對網路安全與自由造成危害，進而展現相互抗衡的意向。

(三) 美國的網路軍事作為

自 2004 年版「國家軍事戰略報告」(National Military Strategy) 首次將網路與陸地、海洋、天空及太空並列爲獨立國防領域以來，[62]美國政府便積極強化網路防務，除陸續發表多份政策文件外 (請見表 1)，亦在組織編制上做出相應調整。在 2009 年 6

註 58 Mandiant Corporation, *APT1: Exposing One of China's Cyber Espionage Units* (Washington, D.C.: Mandiant Corporation, 2013), pp. 2~4.

註 59 David E. Sanger, David Barboza and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *The New York Times*, http://cn.nytimes.com/china/20130219/c19hack/en-us/. Accessed on April 22, 2017；Mark A. Stokes, *The PLA General Staff Department Third Department Second Bureau: An Organizational Overview of Unit 61398* (Arlington: Project 2049 Institute, 2015), pp. 3~14.

註 60 "Hat-tribution to PLA Unit 61486," *CrowdStrike*, https://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486/. Accessed on April 22, 2017；Nicole Perlroth, "2nd China Army Unit Implicated in Online Spying," *The New York Times*, https://www.nytimes.com/2014/06/10/technology/private-report-further-details-chinese-cyberattacks.html?_r=0. Accessed on April 22, 2017.

註 61 U.S. Department of Defense, *Quadrennial Defense Review Report 2014* (Washington, D.C.: U.S. Department of Defense, 2014), p. 6；The White House, *National Security Strategy 2015* (Washington, D.C.: The White House, 2015), p. 24；U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2016* (Washington, D.C.: U.S. Department of Defense, 2016), p. 64；U.S.-China Economic and Security Review Commission, *2015 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington, D.C.: U.S.-China Economic and Security Review Commission, 2015), pp. 192~219；U.S.-China Economic and Security Review Commission, *2016 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington, D.C.: U.S.-China Economic and Security Review Commission, 2016), pp. 289~303.

註 62 U.S. Department of Defense, *National Military Strategy 2004* (Washington, D.C.: U.S. Department of Defense, 2004), p. 1.

月宣布組建網路司令部（U.S. Cyber Command, USCYBERCOM）後，[63]各軍種亦陸續設置網戰指揮單位，[64]並持續擴編網路司令部員額，[65]撥列高額資金採購網路戰爭所需的軟硬體設施以強化總體網路戰力。[66]而從經驗來看，美國確曾運用網路防務力量打擊與監控他國。除透過「震網病毒」遲滯伊朗核能發展計畫外，[67]歐巴馬政府在處理利比亞內戰時，也曾考慮以網路入侵利比亞國防資訊系統以癱瘓其空防體系。[68]美國國家安全局（U.S. National Security Agency）前雇員史諾登（Edward Snowden）揭露的「稜鏡計畫」（PRISM），更說明美國政府如何透過網路技術大規模監控他國政府、企業與平民。[69]

註[63] 2009 年 6 月，時任美國國防部長蓋茲（Robert Gates）正式宣佈建立網路司令部，由曾任國家安全局（U.S. National Security Agency）局長的海軍中將亞歷山大（Keith Alexander）出任首任司令，該司令部於 2010 年 10 月全面運作，請參考：David M. Hollis, "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command," *Joint Force Quarterly*, No. 58（June 2010）, pp. 48~53.

註[64] "Navy Stands up Fleet Cyber Command, Reestablishes U.S. 10th Fleet," *U.S. Fleet Cyber Command*, http://www.stratcom.mil/Media/News/News-Article-View/Article/983834/navy-stands-up-fleet-cyber-command-reestablishes-us-10th-fleet/. Accessed on April 22, 2017；J. R. Wilson, "MARFORCYBER: Marines Fight in a New Domain," *Defense Media Network*, http://www.defensemedianetwork.com/stories/marforcyber-marines-fight-in-a-new-domain/. Accessed on April 22, 2017； "History of HQ Twenty-Fourth Air Force and 624th Operations Center," *24 AF Office of History*, http://www.24af.af.mil/Portals/11/documents/About_Us/AFD-140429-035.pdf?ver=2016-04-26-113101-810. Accessed on April 22, 2017；Jeffrey L. Caton, *Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications*（Carlisle: U.S. Army War College, 2015）, pp. 23~24.

註[65] U.S. Department of Defense, *The Department of Defense Cyber Strategy*（Washington, D.C.: U.S. Department of Defense, 2015）, p. 6.

註[66] "DOD Releases Fiscal Year 2014 Budget Proposal," *U.S. Department of Defense*, http://dodcio.defense.gov/Portals/0/Documents/Library/2014%20Press%20Release.pdf. Accessed on April 22, 2017；"DoD Releases Fiscal Year 2016 Budget Proposal," *U.S. Department of Defense*, https://www.defense.gov/News/News-Releases/News-Release-View/Article/605365. Accessed on April 22, 2017；李恆陽，「美國網絡軍事戰略探析」，**國際政治研究**，第 1 期（2015 年 2 月），頁 121~122。

註[67] Ellen Nakashima and Joby Warrick, "Stuxnet was Work of U.S. and Israeli Experts, Officials Say," *The Washington Post*, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.847875342088. Accessed on April 20, 2017.

註[68] Eric Schmitt and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," *The New York Times*, http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html. Accessed on April 22, 2017.

註[69] David Wright and Reinhard Kreissl, "European Responses to the Snowden Revelations: A Discussion Paper," *Increasing Resilience in Surveillance Societies*, http://irissproject.eu/wp-content/uploads/2013/12/IRISS_European-responses-to-the-Snowden-revelations_18-Dec-2013_Final.pdf. Accessed on June 22, 2018; Aiesha Y. Khudayer et al., "Impact of NSA-PRISM to National Information Security Strategy & Policy," *International Journal of Information and Communication Technology Research*, Vol. 4, No. 1（January 2014）, pp. 25~31.

表 1　近年美國網路防務重點政策文件概覽

日期	文件名稱	發佈單位	內容重點
2006/12	網路空間作戰國家軍事戰略（The National Military Strategy for Cyberspace Operations）	參謀長聯席會議	介紹網路環境背景與威脅形態，探討如何保障美國的軍事優勢，提出加強技術研發與人才培育、擴大國際合作、強化網路攻防及情蒐能力，和整合指揮協調系統等措施。
2009/5	全面性國家網路安全倡議（The Comprehensive National Cybersecurity Initiative）	白宮	透過建立應變機制、改善人員教育與修補安全缺口，強化聯邦政府網路系統安全，同時責成相關部門提升網路嚇阻及情報能力，以應對可能威脅。
2009/5	網路空間政策評估（Cyberspace Policy Review）	白宮	以宏觀角度檢討國家網路政策規劃，提出整合領導體系、建設數位國家、建立網路應變機制等目標，並強調發展網路軍事及情蒐能力的重要性。
2011/5	網路空間國際戰略（International Strategy for Cyberspace）	白宮	宣示與友邦在維護網路自由、打擊網路犯罪、保障關鍵設施安全等方面加強合作，並推動跨國網路防務協調，幫助友邦提升網路戰力。
2011/7	國防部網路空間作戰戰略（Department of Defense Strategy for Operating in Cyberspace）	國防部	由軍事角度分析美國在網路領域的優勢與威脅，提出維護既有優勢、實行主動防禦、保護關鍵設施、推動國際合作與促進技術創新等方針。
2013/2	聯合出版3-12：網路空間作戰（Joint Publication 3-12 (R): Cyberspace Operations）	參謀長聯席會議	此文件至2014年10月方對外公開，全面介紹了網路空間特徵、網路作戰形態、網路聯合作戰的指揮、分工、協調與評估等要點。
2014/2	作戰手冊3-38：網路電磁活動（Field Manual 3-38: Cyber Electromagnetic Activities）	陸軍部	爲美國陸軍首度公開的網路作戰教則，內容包含網路作戰基本概念和技術知識，以及網路攻防行動方針。
2015/4	國防部網路戰略（The Department of Defense Cyber Strategy）	國防部	提出建立可隨時行動的網路戰力、加強資安防護、擴大國際合作等目標，並將中國界定爲「關鍵網路威脅」（Key Cyber Threats）。

資料來源：作者自行整理。相關文獻請見：U.S. Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*（Washington, D.C.: U.S. Joint Chiefs of Staff, 2006）; The White House, *Cyberspace Policy Review*（Washington, D.C.: The White House, 2009）; The White House, *International Strategy for Cyberspace*; U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*（Washington, D.C.: U.S. Department of Defense, 2011）; U.S. Joint Chiefs of Staff, *Joint Publication 3-12（R）: Cyberspace Operations*（Washington, D.C.: U.S. Joint Chiefs of Staff, 2013）; U.S. Department of the Army, *Field Manual 3-38: Cyber Electromagnetic Activities*（Washington, D.C.: U.S. Department of the Army, 2014）; U.S. Department of Defense, *The Department of Defense Cyber Strategy*.

綜上所述，美國不僅在技術層面和追求「網路強國」地位的中國間存在客觀競爭性，也對中國表現出明顯的威脅認知與對立傾向，同時具有運用網路科技攻擊監控他國的記錄。在各項條件匯聚下，美國因素從而成爲中國建設「網路強國」時無可迴避的重要挑戰。[70]

然而網路事務畢竟僅是美中互動的眾多領域之一，對於總體美中關係的主導力有

註[70] Amy Chang, *Warring State: China's Cybersecurity Strategy*（Washington, D.C.: Center for a New American Security, 2015）, pp. 22~29.

其界限，且美國與中國在網路領域中亦存在諸多合作利益。以網路經濟爲例，「高盛集團」(Goldman Sachs Group) 對美國企業 2015 年營收申報的分析顯示，諸如「博通」(Broadcom Corporation)、「美光科技」(Micron Technology)、「輝達」(Nvidia Corporation) 等科技廠商，對中國市場的營收依賴度皆有五至八成的比例。而「英特爾」(Intel Corporation) 和「德州儀器」(Texas Instruments) 等廠商對中國的營收依賴度也達三至四成之譜。相關數據說明，美中之間若爆發劇烈衝突，將嚴重影響美國網路產業營運。[71]在中國方面，其國內用戶對美國資訊產品的依賴度仍然偏高，以電腦作業系統爲例，中國政府近年雖積極開發本土作業平臺，但多數公家機關、國營企業與民間用戶依舊使用「微軟公司」(Microsoft) 的「視窗」(Windows) 系列作業系統。[72]而中國在擴大國內網路基礎建設的過程中，亦大量採用來自美國企業的硬碟、記憶體和電腦晶片等產品。[73]此外，同爲當代網路大國的美國與中國，面對日益猖獗的網路犯罪及網路恐怖主義威脅，雙方在相關議題上也存在利益交會。[74]

因此，即便美國與中國在網路領域的對立日漸凸顯，但兩國關係的競合本質並未改變。這意味著中國政府在推動「網路強國」戰略時，面對美國因素的影響，仍須採取抗衡與合作並行的因應方式，以求在消解安全壓力的同時，維護彼此間的合作利益。

三、中國對美網路「避險」作為

承上所述，中國在網路崛起過程中對於美國因素的處理，既有予以適度制約以應對潛在威脅的必要，亦需維繫彼此間的合作交流，藉此緩和對立俾確保共同利益不受影響。爲認識中國近年在網路領域對美國採取的各種政策作爲及其意涵，下文將透過「避險戰略」的框架進行觀察。

(一) 威脅應對層面

在威脅應對方面，「避險戰略」承襲平衡理論思路，關注國家如何透過競爭作爲因應安全威脅。然如前述，冷戰式的同盟對抗和軍備競賽在當代國際政治中已極爲少見，且國家間縱有難以調和的安全紛爭，彼此亦常在其他領域保持合作。發軔於全球化時代的「避險戰略」因而將威脅的有限性和共同利益納入考量，提出「間接平衡」、「優勢拒阻」和「制度平衡」等策略選項，指導國家以迂迴有限的方式應對挑戰，避

註 [71]　"These are the 20 China-exposed Stocks to avoid," *MarketWatch*, http://www.marketwatch.com/story/these-are-the-20-china-exposed-stocks-to-avoid-2015-08-10. Accessed on April 20, 2017.

註 [72]　Jin Kai, "Why China Banned Windows 8," *The Diplomat*, http://thediplomat.com/2014/05/why-china-banned-windows-8/. Accessed on April 22, 2017；「中國 Windows 10 用戶數超過 Mac 只用了 2 天」，**網易數碼**，http://digi.163.com/15/0812/06/B0Q3EKAG00162OUT.html，檢索日期 2017 年 4 月 21 日。

註 [73]　「2016 年中國半導體記憶體行業市場現狀及發展趨勢預測」，**中國產業發展研究網**，http://www.chinaidr.com/tradenews/2016-09/103234.html，檢索日期 2017 年 4 月 21 日。

註 [74]　Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime* (Washington, D.C.: Center for Strategic and International Studies, 2014), pp. 3~9.

免引發與對手間的正面衝突。

1.間接平衡：強化安全實力

「間接平衡」策略建議國家可在有限度與非針對性的前提下，提升安全實力以應對威脅。面對美中兩國近年於網路領域矛盾日深，及美軍網路戰力持續發展等趨勢，中國政府不僅公開反駁美國的指責與批評，[75]近年更積極建設網路安全實力，在避免觸發大國網路軍備競賽的同時，逐步強化本國的網路作戰體系、網路情蒐能量及輿情管控能力。

(1) 調整網路作戰體系

中國的網路防務權責長期由多重部門分司職掌。例如：負責組建軍事網路系統與網路反制力量的解放軍總參四部 (中國人民解放軍總參謀部電子對抗與雷達部)，負責國防資安維護與戰情蒐集的解放軍總參三部 (中國人民解放軍總參謀部技術偵察部)，負責研究網路軍事科技、網路戰術及人才培育工作的國防大學等軍事校院，以及責成各戰區設置的「信息對抗中心」等。[76]這種多元體系固然展現對網路安全的高度重視，卻也不免造成統合運作上的困難。

有鑒於此，中國在近年的軍事改組中設立「戰略支援部隊」，專責網路攻防、衛星操控等攸關國家安全的「新型作戰力量」。過去長期擔負網路軍事活動重任的總參三部、總參四部等單位也被併入其中，轉型爲「戰略支援軍網絡空間作戰部隊」。[77]此一措施顯示「戰略支援部隊」已成爲解放軍網路戰力核心，其網路軍事體系由此轉趨集權，使中央可更直接地掌握並落實高層意志，[78]也將更有力量在網路入侵與作戰情境中抗衡美國。[79]

(2) 發展網路間諜部隊

在公開防務建制外，中國也暗中建設秘密網路間諜部隊持續蒐集各國情資。除前文提及的 61398 部隊和 61486 部隊外，相關資訊顯示解放軍總參三部近年另設一支總

註[75] 「中共官媒批美『中國網絡威脅論』：不要搞唯我獨尊」，**多維新聞**，http://news.dwnews.com/global/big5/news/2013-03-16/59156042.html，檢索日期 2017 年 8 月 17 日；「2017 年 3 月 9 日外交部發言人耿爽主持例行記者會」，**中國外交部**，http://www.mfa.gov.cn/web/fyrbt_673021/t1444510.shtml，檢索日期 2017 年 8 月 17 日。

註[76] James Mulvenon, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in Roy Kamphausen, David Lai and Andrew Scobellm eds., *Beyond the Strait: PLA Missions Other Than Taiwan* (Carlisle: The Strategic Studies Institute of the U.S. Army War College, 2009), pp. 272~276；Deepak Sharma, "Integrated Network Electronic Warfare: China's New Concept of Information Warfare," *Journal of Defence Studies*, Vol. 4, No. 2 (April 2010), pp. 38~40.

註[77] John Costello, "The Strategic Support Force: China's Information Warfare Service," *China Brief*, Vol. 16, No. 3 (February 2016), pp. 15~19；Mikk Raud, *China and Cyber: Attitudes, Strategies, Organisation*, pp. 21~22.

註[78] Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure* (Arlington: Project 2049 Institute, 2015), pp. 4~11.

註[79] 「中國戰略支援部隊接收『黑客部隊』提高網路戰能力」，**美國之音**，https://www.voachinese.com/a/china-cyber-security-20160129/3169386.html，檢索日期 2017 年 12 月 12 日。

部位於青島市的 61419 部隊，以日本與韓國的政府機關及企業爲目標，曾大規模入侵日本防衛省與其承包商的網路系統。[80]此類事例說明中國的網路間諜活動在編制上日趨周延，呈現針對不同國家或領域專業分工的現象。此外，基於隱匿性等考量，中國政府的網路間諜工作有時亦以論件計酬方式聘用民間駭客，在官方指導下實行網路攻擊或竊密。[81]部分研究也發現中國政府似在幕後長期支持 Axiom 與 Mirage 等廣泛滲透美國政府和民間企業網路系統的駭客集團。[82]

(3) 加強網路輿論管控

中國近年積極提升掌控網路輿論的能力。在正規編制方面，其中央與地方政府紛紛組建網路輿論部隊，招聘技術專家和專業寫手，在網路平臺中針對重要政策或特定公眾事件發表有利黨政體系的言論，[83]部分大專院校似亦參與其間。[84]在非正規力量方面，許多中國網路用戶具強烈民族主義傾向，常在網路中抨擊異議人士，或發表大量呼應官方立場的言論。此類用戶因遭外界質疑暗中收受政府酬勞，而被冠以「五毛黨」這一具諷刺意味的稱號。[85]「五毛黨」雖不若正規網路輿論部隊專業，但因數量龐大而能在短時間內創造大量資訊流，迅速影響輿論走向並淹沒不同意見，成爲政府的有力後盾。[86]

值得注意的是，網路輿情控制能力的增長，不僅有助於中國政府加強管控國內社會以防範外部勢力滲透，從 2016 年美國總統大選經驗來看，網路空間的即時、跨國界與匿名特質，使擅長操縱輿論走勢的國家有機會藉由塑造民意風向等方式，干擾他國政治運作或選舉活動，因而具有一定程度的攻勢意義。[87]

註 80 Jonathan Racicot, “The Past, Present and Future of Chinese Cyber Operations,” *Canadian Military Journal*, Vol. 14, No. 3 (Summer 2014), p. 29；「中國網路監控大軍被懷疑有 800 萬」，**法國國際廣播電臺**，https://tinyurl.com/y74heydb，檢索日期 2017 年 4 月 21 日。

註 81 劉得民，「中國大陸網軍外圍組織現況研究」，**中共研究**，第 48 卷第 7 期 (2014 年 7 月)，頁 134~139。

註 82 James Scott and Drew Spaniel, *ICIT Briefing: China's Espionage Dynasty* (Washington, D.C.: Institute for Critical Infrastructure Technology, 2016), pp. 8~20.

註 83 哈佛大學教授金 (Gary King) 等人在追蹤近五億筆疑似與官方有關的網路言論後，發現其中超過 99% 的發言來自兩百多個政府局處公務員，請見：Gary King, Jennifer Pan and Margaret E. Roberts, “How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument,” *American Political Science Review*, http://gking.harvard.edu/files/gking/files/50c.pdf. Accessed on April 22, 2017.

註 84 「中國解放軍令大學配合徵五毛黨公文曝光」，**新頭殼**，http://newtalk.tw/news/view/2016-04-11/71990，檢索日期 2017 年 4 月 24 日。

註 85 宋筱元，「習近平時期中共的網絡輿論管理」，**展望與探索**，第 14 卷第 3 期 (2016 年 3 月)，頁 63~64；「焦點對話：自乾五是如何煉成的」，**美國之音**，http://www.voachinese.com/a/VOAWeishi-ProandCon-20160617-The-rise-of-Chinas-volunteer-50-centers-Is-Chinas-education-to-blame/3380445.html，檢索日期 2017 年 4 月 21 日。

註 86 Gary King, Jennifer Pan and Margaret E. Roberts, “How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument.”

註 87 Max Fisher, “Russia and the U.S. Election: What We Know and Don’t Know,” *The New York Times*, https://www.nytimes.com/2016/12/12/world/europe/russia-trump-election-cia-fbi.html?_r=0. Accessed on April 20, 2017；Catherine A. Theohary and Cory Welt, “Russia and the U.S. Presidential Election,” *Congressional Research Service*, https://fas.org/sgp/crs/natsec/IN10635.pdf. Accessed on April 20, 2017.

2.優勢拒阻：拓展國際合作

「優勢拒阻」策略建議國家以非結盟形式加強與他國間的外交合作以抵銷來自對手的安全壓力。爲提升對國際網路議題的影響力，並因應大國網路競逐加劇等趨勢，中國近年在國際間大力推廣網路主權觀念，爭取俄羅斯等國家支持，在網路領域漸進構築跨國合作陣線，共同抵制美國的網路價值觀。

（1）操作網路主權論述

在中國看來，主權是一種具變動性的概念，隨著人類文明與科技進步，其涵蓋範圍由陸地延伸至海洋、天空，進而衍化出領土、領海和領空等對應劃界。循此，當網路空間成爲人類生活不可或缺的領域時，自亦爲主權概念所適用，[88]故中國國務院於2010 年的「中國互聯網狀況」白皮書中宣示：「中華人民共和國境內的互聯網屬於中國主權管轄，中國的互聯網主權應受到尊重和維護。[89]」

中國的觀點與美國長期主張的網路自由理念明顯抵觸，部分美國學者批評網路主權觀念若獲得國際社會認同，將導致網路空間的無國界狀態裂解，造成「網路巴爾幹化」（Cyberbalkanization）現象。[90]事實上，從國際政治角度思考，中國對網路主權的宣揚，確有在網路議題上劃分陣線的戰略意義：透過加劇網路自由與網路主權的觀點之爭，凡意圖加強管制本國網路體系的國家，其與美國之間的矛盾，及與中國的合作基礎都將得到凸顯。

（2）推動國際網路合作

在前述背景下，中國與部分理念相近國家近年的網路合作漸趨深化。例如中國政府及企業提供亟於加強管控國內網路的伊朗政府各類技術，協助其鎖定異議人士並加強監控國民網路活動。[91]中國與北韓的關係近年雖略顯疏離，但在平壤當局對「索尼影視娛樂公司」（Sony Pictures Entertainment）等外國企業發動的網路攻擊中，似仍提供其網路部隊必要的協助與掩護。[92]俄羅斯更是中國在網路領域的最重要合作伙伴，其不僅接納網路主權概念，更在各種國際場合公開表達與中國的一致立場，[93]中俄元首並於

註 [88] Li Zhang, “A Chinese Perspective on Cyber War,” *International Review of the Red Cross*, Vol. 94, No. 886（Summer 2012）, p. 806；「卿昱：解讀中華人民共和國網絡安全法」，**東方安全**，http://www.cnetsec.com/article/20374.html，檢索日期 2017 年 4 月 21 日。

註 [89] 中國國務院，**中國互聯網狀況**（北京：中國國務院新聞辦公室，2010 年），頁 11。

註 [90] 吳家恆等譯，Eric Schmidt and Jared Cohen 著，**數位新時代**（臺北：遠流，2013 年），頁 103~117。

註 [91] Cinnamon Nippard, “International Blogging Conference Puts Internet Press Freedom on the Agenda,” *Deutsche Welle*, http://www.dw.com/en/international-blogging-conference-puts-internet-press-freedom-on-the-agenda/a-5474714. Accessed on April 20, 2017；Aida Akl, “Iran Plans Its Own Sanitized Internet with Chinese Help,” *Voice of America*, https://www.voanews.com/a/iran-plans-its-own-sanitized-internet-with-chinese-help/1713638.html. Accessed on August 17, 2017.

註 [92] Jordan Wilson, *China’s Position on the Sony Attack: Implications for the U.S. Response*（Washington, D.C.: U.S.-China Economic and Security Review Commission, 2015）, pp. 1~3.

註 [93] Jack Margolin, “Russia, China, and the Push for ‘Digital Sovereignty’,” *IPI International Peace Institute*, https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization. Accessed on April 22, 2017；Farid Gueham, *Digital Sovereignty*（Paris: The Fondation pour l’Innovation Politique, 2017）, pp. 15~16.

2016 年 6 月發表聯合聲明，強調兩國「一貫恪守尊重信息網絡空間國家主權的原則，支持各國維護自身安全和發展的合理訴求…」，且反對「侵犯他國網絡主權的行爲」。[94]

由當前情勢觀察，雖不存在正式締約的國際網路同盟，但透過操作網路主權議題，中國逐步在國際間劃分陣營，以中俄合作爲核心，和其他具網路管控傾向的國家保持交流，漸進塑造一個隱然與美歐國家分庭抗禮的跨國合作集團。

3.制度平衡：爭取機制主導權

「制度平衡」策略建議國家經由組建多邊機制或操縱既有機制規範，削弱對手的行動自由與合法性。中國近年推動國際網路合作時，也憑藉各國支持，在國際機制中謀求網際網路治理準則的制定權並挑戰美國的主導地位。於下分以中國與俄羅斯等國家聯手在聯合國提交「信息安全國際行爲準則」(Code of Conduct for Information Security)，及推動「國際電信規則」(International Telecommunication Regulations, ITRs)修訂的嘗試爲例，說明中國政府的相關舉措。

(1)提交「信息安全國際行爲準則」

2011 年 9 月，中國、俄羅斯與部分「上海合作組織」(Shanghai Cooperation Organization, SCO)成員向第 66 屆聯合國大會(UN General Assembly)共同提交「信息安全國際行爲準則」，這份文件要求各國在網路空間中應：[95]

- 尊重他國的主權，領土完整和政治獨立。
- 瞭解與網路相關的公共政策問題決策權屬於各國主權。
- 不以網路技術干涉他國內政，或破壞他國政治、經濟和社會穩定。
- 認識各國皆有責任和權利依法保護本國網路及關鍵資訊基礎設施免受威脅、干擾和攻擊。
- 不利用網路技術優勢，削弱他國對資訊產品和服務的自主控制權。

從內容來看，網路主權顯然是這份準則的主旨，中俄等國家不僅藉聯合提案行動展示彼此的一致立場，更意圖透過聯合國賦予網路主權觀念國際法層面的正當性。

(2)推動「國際電信規則」修訂案

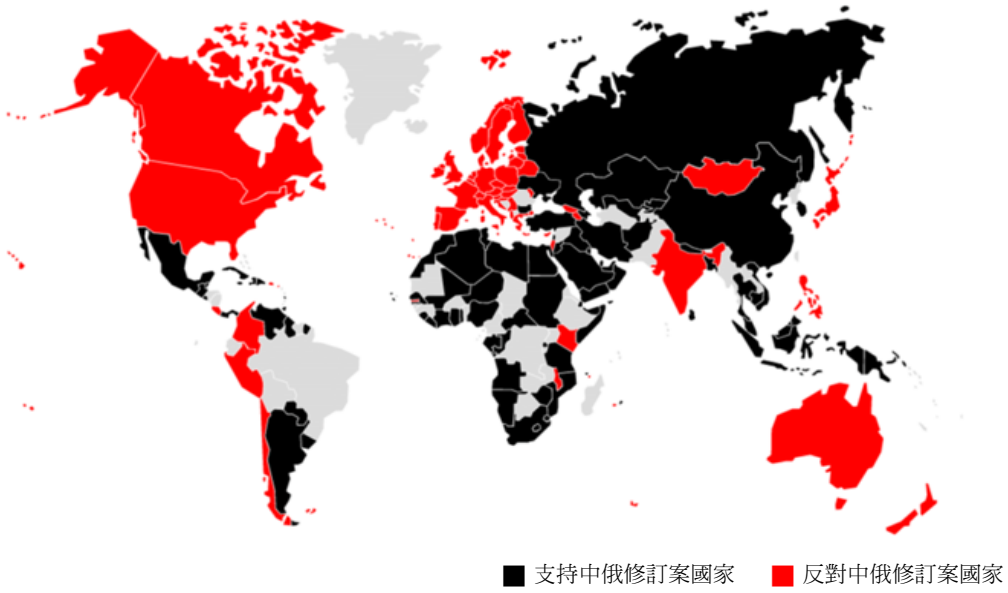
2012 年 12 月，「國際電信聯盟」(International Telecommunication Union, ITU)於杜拜舉行的「國際電信大會」(World Conference on International Telecommunications, WCIT)中，193 國政府代表共同針對修訂「國際電信規則」等事務進行磋商。中國與俄羅斯邀集阿拉伯聯合大公國、阿爾及利亞等國家共同提案，要求將該規則的管轄範圍由傳統電信領域擴大至網際網路，並承認各國政府擁有管控網路活動及審查線上言

註[94] 「中華人民共和國主席和俄羅斯聯邦總統關於協作推進資訊網絡空間發展的聯合聲明」，**新華網**，http://news.xinhuanet.com/politics/2016-06/26/c_1119111901.htm，檢索日期 2017 年 4 月 22 日。

註[95] 「信息安全國際行爲準則(2011)」，**中國外交部**，http://wcm.fmprc.gov.cn/pub/chn/gxh/zlb/zcwj/t858317.htm，檢索日期 2017 年 4 月 22 日；「信息安全國際行爲準則(2015)」，**中國外交部**，http://www.mfa.gov.cn/chn//pds/ziliao/tytj/zcwj/P020150316571763224632.pdf，檢索日期 2017 年 4 月 22 日。

論的權力。這份議案試圖全面賦予網路主權和審查制度合法性，正面挑戰美國的網路自由理念。[96]該修訂案在會議中雖獲 89 個國家支持，但也遭到美國強力反對。美國代表團團長克拉莫（Terry Karamer）指稱該案內容違反民主自由與網路開放等基本價值。在美方推動下，包含加拿大和英國在內的 55 國選擇拒絕簽署議案（請見圖 3）。[97]

圖 3　世界各國對中俄 2012 年「國際電信規則」修訂案立場示意圖



資料來源：Melody Patry, *Brazil: A New Global Internet Referee?* (London: Index on Censorship, 2014), p. 20.

雖因無法取得與會國家一致共識導致修訂案未能通過，但無論是提交「信息安全國際行爲準則」或修改「國際電信規則」的嘗試，都顯示中國的網路主權主張已獲得許多國家認同，[98]並在國際機制內持續挑戰美國的影響力。

（二）合作交流層面

「避險戰略」認爲國家在處理威脅之餘，亦應與存在利益連結的對手保持合作，以確保共同利益不因抗衡舉措受損，因而提出多種合作性策略供決策者參考。相關選項中，「經濟務實主義」和「約束性交往」分別聚焦於經濟合作與制度化交流，「有限

註 96　Jacey Fortin, "Russia, Saudi Arabia, China and others fail to Impose Internet Regulations at WCIT," *International Business Times*, http://www.ibtimes.com/russia-saudi-arabia-china-others-fail-impose-internet-regulations-wcit-931654. Accessed on April 22, 2017.

註 97　Kevin Reed, "Global Split over Telecom Treaty," *World Socialist Web Site*, https://www.wsws.org/en/articles/2012/12/28/wcit-d28.html. Accessed on April 22, 2017.

註 98　Catherine Howell and Darrell M. West, "The Internet as a Human Right," *The Brookings Institution*, https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/. Accessed on April 20, 2017.

扈從」則關注中小型國家如何在面臨強國壓力時適度退讓以換取實益。[99]本文以中國對美網路競合爲題，鑑於美國與中國在國際政治及網路領域皆爲實力突出的大型強國，以下將排除「有限扈從」，集中探討中國對「經濟務實主義」和「約束性交往」兩類策略的應用。

1.經濟務實主義：營造友善氛圍並推進經濟交流

「經濟務實主義」策略建議國家如與對手間存在經貿互賴，則應在設法制衡之餘，同步促進合作交流以維護國家利益。中國近年在網路事務中雖和美國多有矛盾，但仍持續透過外交途徑向美方傳達善意並積極推進雙邊網路經濟合作。於下分由「傳遞友善訊息」及「維繫經濟交流」兩方面觀察中國的政策動向。

(1) 傳遞友善訊息

中國政府近年在各式外交活動中，持續向美國強調其無意於網路領域和美方對抗，期望兩國經由友好交流化解歧見，進而擴大各層面的網路合作。以領導人發言爲例，習近平於 2015 年 9 月訪美時，特地安排參訪「微軟公司」總部，會見多位美國網路企業代表，邀請相關企業加強對中投資，並表示願與美國在相互尊重的基礎上推展雙邊網路合作；[100]北京當局隨後發佈的領導人訪美成果清單也指出美中在防範網路犯罪、打擊網路恐怖主義、收束網路間諜活動與研擬網際網路治理規範等議題上達成加強合作的共識。[101]

2015 年 11 月，習近平在「亞洲太平洋經濟合作會議領導人非正式會議」(APEC Economic Leaders' Meeting) 中，公開宣示中國願與亞太各國加強網路經濟合作，並共同營造和平穩定的國際環境。[102]而李克強在 2016 年 1 月會見美國哥倫比亞大學 (Columbia University) 校長布林格爾 (Lee C. Bollinger) 時，亦與其深入討論美中網路交流前景，提出中國期望與美國學研機構加強合作，培養更多有助國家網路建設的高階科技人才。[103]

(2) 維繫經濟交往

在傳達善意的同時，中國政府也積極邀請美國企業參與「互聯網+」等政策規畫，[104]並強調網路產業合作已成美中經濟交流中最具前瞻性的「藍海」。[105]據「中國互聯網絡

註[99] Cai Dexian, "Hedging for Maximum Flexibility: Singapore's Pragmatic Approach to Security Relations with the US and China," *Pointer*, Vol. 39, No. 2 (July 2013), pp. 6~7.

註[100] 「習近平參觀美國微軟公司總部」，**新華網**，http://news.xinhuanet.com/world/2015-09/24/c_1116667179.htm，檢索日期 2017 年 4 月 28 日。

註[101] 「習近平訪美中方成果清單發佈」，**人民網**，http://politics.people.com.cn/n/2015/0926/c1001-27637282.html，檢索日期 2017 年 4 月 28 日。

註[102] 「習近平在亞太經合組織第 23 次領導人非正式會議上的講話」，**新華網**，http://news.xinhuanet.com/world/2015-11/19/c_1117201278.htm，檢索日期 2017 年 4 月 22 日。

註[103] 「李克強會見美國哥倫比亞大學校長、法學教授博林格」，**中國國家外國專家局**，http://www.safea.gov.cn/content.shtml?id=12748685，檢索日期 2017 年 4 月 22 日。

註[104] 「中國經濟發展新趨勢與中美經貿合作新機遇」，**中國外交部**，http://www.fmprc.gov.cn/web/dszlsjt_673036/zls_673040/t1408800.shtml，檢索日期 2017 年 8 月 17 日。

註[105] Wang Qun, "Shared Interests and Responsibility: The US and China Must Join to Promote a Rules-based Cyberspace," *The Huffington Post*, http://www.huffingtonpost.com/wang-qun/shared-interests-and-resp_b_9873642.html. Accessed on August 17, 2017.

信息中心」統計，至 2016 年 12 月止，中國在海外上市的網路企業數量已達 91 間，總市值高達 5.4 兆人民幣，其中在美國上市的企業數量最多，占總市值的 55.7%。⑯另一方面，雖有「谷歌事件」與部分網路社交媒體遭排拒的負面經驗在前，⑰但充滿潛力的中國市場仍吸引眾多美國網路企業爭相投入。⑱近年來，諸如「印象筆記」（Evernote）、「亞馬遜」（Amazon）、「領英」（LinkedIn）等，皆在中國取得相當的營運成果。而「谷歌」（Google）和「臉書」（Facebook）等遭北京當局限阻的企業，也積極尋求進入或重返中國市場的機會。⑲

從網路經濟角度觀察，美中之間的互補特質十分明顯。作爲網路科技發祥地的美國迄今仍在網路領域掌握技術優勢，優秀的高等教育和產學連結、靈活的資金流動，及對網路自由的保障等環境條件，使美國得以持續開發各種新型技術與產品。⑩中國的網路技術創新雖有不足，但其擁有全球最大用戶市場，配合各類網路建設政策的執行，展現深厚發展潛力。美中網路經濟合作倘能更趨緊密，不但使美國網路企業可藉由在中國的營運獲利支持各種新興科技研發，也使中國可取得先進技術並透過雙邊交流培育科技人才，滿足政府擴大網路民生應用與數位經濟規模的期望。就此而言，促進美中網路經濟交流，不僅可緩和雙方在安全層面的對立，更可爲「網路強國」建設工作提供支持。⑪

2.約束性交往：運作與維持交流機制

「約束性交往」策略建議國家與對手共建制度性交流機制，透過穩定溝通緩和矛盾並拓展合作。檢視美國與中國的交往進程，可發現「雙邊對話機制擴散」（proliferation of bilateral dialogue mechanisms）是近年美中關係運作的一大特徵。⑫兩國領導人及高階官員，透過涵蓋政治、經濟、防務、文化、科技與民生等方面超過 90 個對話機制定期交流。⑬這種現象同樣存在於網路領域，美中在近年的網路互動中，

註⑯ 中國互聯網絡信息中心，**第 39 次中國互聯網絡發展狀況統計報告**，頁 29。

註⑰ Justine Lau, “A History of Google in China,” *The Financial Times*, http://www.ft.com/cms/s/0/faf86fbc-0009-11df-8626-00144feabdc0.html?ft_site=falcon#axzz4dGMpKxlN. Accessed on April 22, 2017；Jefferson Graham, “Google CEO: Open to Returning to China,” *USA Today*, https://www.usatoday.com/story/tech/2016/06/01/google-ceo-open-returning-china/85247082/. Accessed on April 20, 2017.

註⑱ Xu-Dong Zhu and Rachel Hong, “How some of America’s Biggest Tech Companies are Expanding into China,” *Business Insider*, http://www.businessinsider.com/us-tech-companies-expanding-into-china-2014-6. Accessed on April 20, 2017.

註⑲ Josh Horwitz, “A New Wave of US Internet Companies is Succeeding in China,” *Quartz*, https://qz.com/435764/a-new-wave-of-us-internet-companies-is-succeeding-in-china-by-giving-the-government-what-it-wants/. Accessed on April 20, 2017.

註⑩ 林幼嵐譯，Frédéric Martel 著，**全球網路戰爭**（新北市：稻田，2016 年），頁 18~29。

註⑪ Susan A. Aaronson and Kimberly A. Elliott, “A China-U.S. Approach to Digital Trade,” *China-United States Exchange Foundation*, http://www.chinausfocus.com/finance-economy/a-china-us-approach-to-digital-trade. Accessed on April 22, 2017.

註⑫ Susan V. Lawrence, *U.S.-China Relations: An Overview of Policy Issues* (Washington, D.C.: Congressional Research Service, 2013), pp. 10~11.

註⑬ 關慶豐，「中美如何通過 90 多個平臺對話？」，**北京青年報**，http://bjyouth.ynet.com/3.1/1306/10/8068300.html，檢索日期 2017 年 4 月 21 日。

已形成「政府間對話」與「官產學複合對話」兩類制度性交流框架。

(1) 政府間對話機制的運作

在政府間對話部分，曾備受各界關注的「美中網路安全工作組」(U.S.-China Cyber Security Working Group) 雖因美國政府起訴解放軍軍官事件而告中斷，[114]但北京與華府仍透過「美中打擊網路犯罪及相關事項高階聯合對話」(U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues) 穩定交流，雙方官員以年度會議形式共商網路安全議題與合作事項。[115]美中在「戰略與經濟對話」(U.S.-China Strategic and Economic Dialogue) 中也持續分享彼此對網路事務的觀點，並針對防範網路侵權、打擊網路犯罪、維護網路金融安全，擴大主管部門間交流等議題達成合作共識。[116]此外，爲協調在網際網路治理方面的歧異，美中於 2016 年 5 月正式啓動「網路空間國際規則高階專家組會議」(Senior Experts Group on International Norms in Cyberspace) 以探求建立共識的可能性。[117]

(2) 官產學複合對話機制的運作

在官產學複合對話部分，「美中互聯網論壇」，(U.S.-China Internet Industry Forum)[118]和「中美高級網路技術研討會」(Chinese American Networking Symposium) 等機制，[119]使美國與中國的網路主管官員、企業代表及專家學者得以年度會議形式交換彼此的網路治理觀點，並探討技術開發和產業合作等議題。「世界互聯網大會」這一由「中國國家互聯網信息辦公室」主導的會議雖具官方色彩，卻已成爲美中網路產業交流的最重要場合之一，[120]自 2014 年 11 月起至今的歷屆會議中，美中重點網路企業領導人皆踴躍

註[114] Michael S. Schmidt and David E. Sanger, "5 in China Army Face U.S. Charges of Cyberattacks," *The New York Times*, https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html?_r=0. Accessed on April 22, 2017；「陸決定中止中美網路工作組活動」，**中時電子報**，http://www.chinatimes.com/realtimenews/20140519005093-260409，檢索日期 2017 年 4 月 21 日。

註[115] "First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes," *U.S. Department of Justice*, https://www.justice.gov/opa/pr/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary-outcomes-0. Accessed on April 22, 2017；"Second U.S.-China Cybercrime and Related Issues High Level Joint Dialogue," *U.S. Department of Justice*, https://www.justice.gov/opa/pr/second-us-china-cybercrime-and-related-issues-high-level-joint-dialogue. Accessed on April 22, 2017；"Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues," *U.S. Department of Justice*, https://www.justice.gov/opa/pr/second-us-china-cybercrime-and-related-issues-high-level-joint-dialogue. Accessed on April 22, 2017.

註[116] 「楊潔篪在第六輪中美戰略與經濟對話聯合記者會上的講話」，**大公網**，http://finance.takungpao.com.hk/q/2014/0711/2591950.html，檢索日期 2017 年 4 月 21 日。

註[117] "U.S., China Cyber Group Holds First Talks Since September Pact," *Reuters*, http://uk.reuters.com/article/us-usa-china-cyber-idUKKCN0Y22OB. Accessed on April 27, 2017.

註[118] 「背景資料：中美互聯網論壇」，**中國網**，http://t.m.china.com.cn/convert/c_uDe56F.html，檢索日期 2017 年 4 月 21 日；「中美互聯網巨頭熱議習近平講話」，**人民網**，http://politics.people.com.cn/n/2015/0924/c1001-27631110.html，檢索日期 2017 年 4 月 22 日。

註[119] "Internet 2 China Program," *Internet 2*, http://www.internet2.edu/communities-groups/international-community/internet2-china-program/. Accessed on April 21, 2017.

註[120] 「習近平：在第三屆世界互聯網大會開幕式上的視頻講話」，**新華網**，http://news.xinhuanet.com/2016-11/16/c_1119925133.htm，檢索日期 2017 年 4 月 21 日；「2016 年世界互聯網發展烏鎮報告」，**世界互聯網大會官網**，http://www.wicwuzhen.cn/system/2016/11/18/021373284.shtml，檢索日期 2017 年 4 月 20 日。

出席，「領英」、「紅杉資本」(Sequoia Capital)、「騰訊」等企業領袖，更在 2015 年的會議中共同成立「中美數字經濟合作協會」(China-US Council of Digital Economic Cooperation) 以促進兩國網路經濟合作。⑪

綜上所述，可發現中國政府在開展對美網路競逐的同時，也透過各種交流機制緩和彼此的矛盾並促進雙邊合作。此類機制的價值可概括爲以下三者：

首先，相關機制是穩定的政府間對話管道，美中官員可透過例行會談交換各自的看法與政策意圖，避免不必要的猜疑誤解。雖然「網路安全工作組」的中斷，爲外界視作美中網路交流的挫敗，但即使在該事件衝擊中，兩國官員仍透過「戰略與經濟對話」等場合私下傳達善意，並探求重啓工作組運作的可能，⑫顯現制度性交流機制對於維繫雙邊溝通的重要性。

其次，相關機制可促進實質合作。以網路犯罪爲例，在「打擊網路犯罪及相關事項高階聯合對話」的推動下，中國公安部與美國國土安全部間建立了熱線、合作準則與網路執法暨情資互助制度，⑬並於 2016 年 2 月聯手查緝網路兒童色情案件，⑭同時宣示鎖定「網路色情」、「網路詐騙」、「網路恐怖主義」和「網路軍火銷售」四大重點項目加強協作。⑮而「世界互聯網大會」也成爲美中網路企業分享新型科技與加強技術暨商業合作的平臺。⑯

最後，從觀念建構的角度而言，中國政府積極利用相關機制，向美國乃至國際社會強調其無意在網路領域和他國對抗，以緩解外界疑忌。例如中國國家領導人與網路主管官員，近年在「美中互聯網論壇」中，持續對美方傳達願意進一步深化雙邊合作的立場；⑰「世界互聯網大會」亦是中國政府高層向各界陳述其推進國際網路合作、

註⑪ 「領英騰訊紅杉寬頻聯合發起中美數字經濟合作協會」，**騰訊科技**，http://info.3g.qq.com/g/index5/ttnews/yidian.jsp?aid=yidian&id=tech_20151217044055&g_f=23748，檢索日期 2017 年 4 月 15 日。

註⑫ 「中美恢復網絡安全對話」，**明報新聞**，https://tinyurl.com/y99szukh，檢索日期 2017 年 4 月 20 日。

註⑬ 「中美打擊網絡犯罪及相關事項高級別聯合對話聯絡熱線開通」，**中共中央網絡安全和信息化領導小組辦公室**，http://www.cac.gov.cn/2016-08/28/c_1119466923.htm，檢索日期 2017 年 4 月 20 日。

註⑭ 「中美半年內兩度商討打擊網絡犯罪，抓獲 17 名涉兒童色情嫌犯」，**澎湃新聞**，http://www.thepaper.cn/newsDetail_forward_1482997，檢索日期 2017 年 4 月 22 日。

註⑮ 「第二次中美打擊網絡犯罪對話成果清單出爐」，**國際在線**，http://news.cri.cn/20160616/fbed4663-df67-1e13-4863-82851416907c.html，檢索日期 2017 年 4 月 22 日。

註⑯ 「世界互聯網大會觀察：人工智慧、技術創新成絕對主角」，**騰訊科技**，http://tech.qq.com/a/20161118/004229.htm，檢索日期 2017 年 4 月 20 日。

註⑰ 「錢小芊在第六屆中美互聯網論壇發表主旨演講」，**新華網**，http://big5.news.cn/gate/big5/news.xinhuanet.com/info/2013-04/10/c_132296277.htm，檢索日期 2017 年 4 月 24 日；「尚冰出席第六屆中美互聯網論壇開幕式」，**中國工業和信息化部**，http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057709/n3057722/c3651813/content.html，檢索日期 2017 年 4 月 21 日；「第七屆中美互聯網論壇在華盛頓舉行，魯煒提出中美網絡關係五點主張」，**新華網**，http://news.xinhuanet.com/world/2014-12/03/c_1113493517.htm，檢索日期 2017 年 4 月 21 日；「習近平：中國宣導建設和平、安全、開放、合作的網絡空間」，**新華網**，http://news.xinhuanet.com/world/2015-09/24/c_1116663156.htm，檢索日期 2017 年 4 月 20 日。

確保網路和平及鼓勵網路經濟互利等正向理念的重要管道。⑱

肆、結　論

中國當前對於「網路強國」地位的追求，不僅牽動國際網路事務運作前景，更可能對美國固有的網路優勢造成挑戰，進而激化美中關係的競爭性。中國政府如何在這一過程中處理對美互動以趨利避害，應爲值得深入探究的重要議題。本文逐一檢視了中國「網路強國」戰略的主要內容，及美國因素對中國國家網路建設的影響，並在此基礎上援用國際關係研究中的「避險戰略」觀察中國近年對美網路競合舉措。

透過「避險戰略」的視角，可察見中國在處理對美網路關係時兼顧安全與利益的企圖。在威脅應對層面，中國在避免觸發正面衝突之餘，漸進加強網路防務建設，並於國際間推廣網路主權觀念以塑造跨國合作陣線，進而在多邊機制中挑戰美國的主導地位。在合作交流層面，中國政府利用各種外交場合向美國傳達善意，並積極推動雙邊網路經濟合作。美中兩國也逐步建構起各類制度性交流機制以持續交換政策思維及技術知識。

長遠來看，中國能否在對美網路互動中達成「避險」目標，以下三者將爲關鍵所在：

第一是技術競爭的調和：中國過往在建設網路系統和發展資訊產業時曾承接大量美國技術與產品，爲美國企業創造豐厚收益。然而隨著建設「網路強國」的戰略目標確立，其政府部門與企業積極提升技術自主性，美中在技術層面的競爭料將漸增。如何避免可能由此衍生的對立氛圍，當爲兩國需審愼應對的課題。

第二是防務透明度的提升：美國與中國近年雖已逐步加強網路安全方面的合作，但主要聚焦於打擊網路犯罪等低階政治層級，對網路軍事建設等高階議題的交流仍相對有限，雙方未來或有提升網路防務透明度以增進互信的必要。

第三是交流機制的延續：如上文所言，相關機制使兩國得以保持穩定溝通，藉以提升相互理解並發掘合作機遇。然由中國片面中斷「美中網路安全工作組」運作等事例來看，美中未來仍須在確保關鍵機制延續等問題上強化共識。

美中關係在網路領域的動向近年深受國際關係學界關注，部分論著指出美國與中國在網路議題上頻繁摩擦、欠缺互信，且皆積極發展網路戰力，對於雙邊關係因之受損，甚或爆發網路戰爭的風險表達了深切憂慮。⑲相關研究凸顯了美中網路互動的競爭

註⑱　「習近平向首屆世界互聯網大會致賀詞」，前引文；「魯煒出席首屆世界互聯網大會並致辭」，**中國新聞網**，http://www.chinanews.com/gn/2014/11-19/6793335.shtml，檢索日期 2017 年 4 月 20 日；「習近平在第二屆世界互聯網大會開幕式上的講話」，**新華網**，http://news.xinhuanet.com/politics/2015-12/16/c_1117481089.htm，檢索日期 2017 年 4 月 20 日；「習近平：在第三屆世界互聯網大會開幕式上的視頻講話」，前引文。

註⑲　Kenneth G. Lieberthal and Peter W. Singer, *Cybersecurity and U.S.-China Relations*, p. 6；James B. Steinberg, *Strategic Reassurance and Resolve: U.S.–China Relations in the Twenty-First Century*（New Jersey: Princeton University Press, 2014）, pp. 177~180；Scott W. Harold, Martin C. Libicki and Astrid S Cevallos, *Getting to Yes with China in Cyberspace*（Santa Monica: RAND Corporation, 2016）, pp. 5~12.

性，並對可能的負面發展趨勢預作警示。然而在本文的探討中，可發現美中在網路領域的互動與總體關係性質相仿，仍然維持競爭與合作並存的特徵。各種對抗性策略的運用，固然反映出難解的猜疑與防備，但整體而言仍屬溫和而有節制。至若各種友善表態、合作交流與制度性對話，不但反映美中當局試圖緩和對立的意向，也是利益驅動下的理性選擇。在可預見的未來中，網路領域的美中關係，或仍將延續這種競合交錯的局面，在保持有限度競逐的同時，持續開展務實互惠的合作交流。

* * *

(收件：106 年 5 月 24 日，接受：107 年 3 月 29 日)

China's Cyber Power Strategy vis-à-vis the U.S. using a 'Hedging' Perspective

Kai-Ming Chang

Assistant Professor
Center for General Education
National Taichung University of Science and Technology

Abstract

China has made huge advances in the field of cyber technology in the past few years and it is now an important player in international cyber affairs. Beijing recently introduced its 'Cyber Power Strategy' in a bid to comprehensively strengthen the nation's cyber capabilities. China's cyber ambitions not only constitute a real challenge to the U.S. but have also prompted concerns in Washington about China's strategic purpose and have more uncertainty to their already unstable bilateral relations. To understand China's cyber development plans and how that will affect U.S. policy, this article will analyze China's Cyber Power Strategy and the U.S. factor. 'Hedging Strategy' from international relations is used to explore the dynamics of Sino-U.S. interactions in cyberspace and to explain how Beijing has used a limited counter-balance strategy against while collaborating with the U.S. to protect national security and advance its interests.

Keywords: Cyber Power Strategy, Sino-U.S. Relations, Hedging Strategy, Cyber Security, Cyber Conflict

參考文獻

「2016 年中國半導體記憶體行業市場現狀及發展趨勢預測」，**中國產業發展研究網**，http://www.chinaidr.com/tradenews/2016-09/103234.html，檢索日期 2017 年 4 月 21 日。

「2016 年世界互聯網發展烏鎮報告」，**世界互聯網大會官網**，http://www.wicwuzhen.cn/system/2016/11/18/021373284.shtml，檢索日期 2017 年 4 月 20 日。

「2017 年 3 月 9 日外交部發言人耿爽主持例行記者會」，**中國外交部**，http://www.mfa.gov.cn/web/fyrbt_673021/t1444510.shtml，檢索日期 2017 年 8 月 17 日。

「中共中央政治局進行第 36 次集體學習，習近平主持」，**央廣網**，http://china.cnr.cn/news/20161010/t20161010_523185107.shtml，檢索日期 2017 年 4 月 22 日。

「中共官媒批美『中國網絡威脅論』：不要搞唯我獨尊」，**多維新聞**，http://news.dwnews.com/global/big5/news/2013-03-16/59156042.html，檢索日期 2017 年 8 月 17 日。

「中美互聯網巨頭熱議習近平講話」，**人民網**，http://politics.people.com.cn/n/2015/0924/c1001-27631110.html，檢索日期 2017 年 4 月 22 日。

「中美半年內兩度商討打擊網絡犯罪，抓獲 17 名涉兒童色情嫌犯」，**澎湃新聞**，http://www.thepaper.cn/newsDetail_forward_1482997，檢索日期 2017 年 4 月 22 日。

「中美打擊網絡犯罪及相關事項高級別聯合對話聯絡熱線開通」，**中共中央網絡安全和信息化領導小組辦公室**，http://www.cac.gov.cn/2016-08/28/c_1119466923.htm，檢索日期 2017 年 4 月 20 日。

「中美恢復網絡安全對話」，**明報新聞**，https://tinyurl.com/y99szukh，檢索日期 2017 年 4 月 20 日。

「中國 Windows 10 用戶數超過 Mac 只用了 2 天」，**網易數碼**，http://digi.163.com/15/0812/06/B0Q3EKAG00162OUT.html，檢索日期 2017 年 4 月 21 日。

「中國經濟發展新趨勢與中美經貿合作新機遇」，**中國外交部**，http://www.fmprc.gov.cn/web/dszlsjt_673036/zls_673040/t1408800.shtml，檢索日期 2017 年 8 月 17 日。

「中國解放軍令大學配合徵五毛黨公文曝光」，**新頭殼**，http://newtalk.tw/news/view/2016-04-11/71990，檢索日期 2017 年 4 月 24 日。

「中國網路監控大軍被懷疑有 800 萬」，**法國國際廣播電臺**，https://tinyurl.com/y74heydb，檢索日期 2017 年 4 月 21 日。

「中國戰略支援部隊接收『黑客部隊』提高網路戰能力」，**美國之音**，https://www.voachinese.com/a/china-cyber-security-20160129/3169386.html，檢索日期 2017 年 12 月 12 日。

「中華人民共和國主席和俄羅斯聯邦總統關於協作推進資訊網絡空間發展的聯合聲明」，**新華網**，http://news.xinhuanet.com/politics/2016-06/26/c_1119111901.htm，檢

索日期 2017 年 4 月 22 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」，**中國人大網**，http://www.npc.gov.cn/npc/dbdhhy/12_4/2016-03/18/content_1985670.htm，檢索日期 2017 年 4 月 22 日。

「中華人民共和國國家安全法」，**中國全國人民代表大會**，http://www.npc.gov.cn/npc/xinwen/2015-07/07/content_1941161.htm，檢索日期 2017 年 4 月 20 日。

「中華人民共和國網絡安全法」，**中國全國人民代表大會**，http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm，檢索日期 2017 年 4 月 20 日。

「互聯網新聞信息服務單位約談工作規定」，**人民網**，http://politics.people.com.cn/n/2015/0429/c1001-26920835.html，檢索日期 2017 年 8 月 15 日。

「世界互聯網大會觀察：人工智慧、技術創新成絕對主角」，**騰訊科技**，http://tech.qq.com/a/20161118/004229.htm，檢索日期 2017 年 4 月 20 日。

「李克強同世界互聯網大會中外代表座談時強調，促進互聯網共用共治，推動大眾創業萬眾創新」，**新華網**，http://news.xinhuanet.com/politics/2014-11/20/c_1113340416.htm，檢索日期 2017 年 4 月 22 日。

「李克強會見美國哥倫比亞大學校長、法學教授博林格」，**中國國家外國專家局**，http://www.safea.gov.cn/content.shtml?id=12748685，檢索日期 2017 年 4 月 22 日。

「尚冰出席第六屆中美互聯網論壇開幕式」，**中國工業和信息化部**，http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057709/n3057722/c3651813/content.html，檢索日期 2017 年 4 月 21 日。

「東莞理工學院成立全國首個網絡空間安全學院」，**中國新聞網**，http://www.chinanews.com/gn/2017/03-11/8171430.shtml，檢索日期 2017 年 4 月 22 日。

「信息安全國際行爲準則（2011）」，**中國外交部**，http://wcm.fmprc.gov.cn/pub/chn/gxh/zlb/zcwj/t858317.htm，檢索日期 2017 年 4 月 22 日。

「信息安全國際行爲準則（2015）」，**中國外交部**，http://www.mfa.gov.cn/chn//pds/ziliao/tytj/zcwj/P020150316571763224632.pdf，檢索日期 2017 年 4 月 22 日。

「背景資料：中美互聯網論壇」，**中國網**，http://t.m.china.com.cn/convert/c_uDe56F.html，檢索日期 2017 年 4 月 21 日。

「卿昱：解讀中華人民共和國網絡安全法」，**東方安全**，http://www.cnetsec.com/article/20374.html，檢索日期 2017 年 4 月 21 日。

「烏鎮指數：全球人工智能發展報告（精華篇）」，**思客－新華網高端智庫平台**，http://sike.news.cn/hot/pdf/10.pdf，檢索日期 2018 年 6 月 22 日。

「國家網絡安全事件應急預案」，**中國國家互聯網信息辦公室**，http://news.xinhuanet.com/zgjx/2017-06/28/c_136400422.htm，檢索日期 2017 年 8 月 15 日。

「國家網絡空間安全戰略全文」，**中央網絡安全和信息化領導小組辦公室**，http://www.cac.gov.cn/2016-12/27/c_1120195926.htm，檢索日期 2017 年 4 月 16 日。

「從『數位福建』到『數位中國』習近平擘畫科技發展新高度」，**人民網**，http://

politics.people.com.cn/n1/2016/0427/c1001-28308778.html，檢索日期 2017 年 4 月 22 日。

「授權發佈：中共中央關於全面深化改革若干重大問題的決定」，**新華網**，http://news.xinhuanet.com/politics/2013-11/15/c_118164235.htm，檢索日期 2017 年 4 月 22 日。

「第七屆中美互聯網論壇在華盛頓舉行，魯煒提出中美網絡關係五點主張」，**新華網**，http://news.xinhuanet.com/world/2014-12/03/c_1113493517.htm，檢索日期 2017 年 4 月 21 日。

「第二次中美打擊網絡犯罪對話成果清單出爐」，**國際在線**，http://news.cri.cn/20160616/fbed4663-df67-1e13-4863-82851416907c.html，檢索日期 2017 年 4 月 22 日。

「習近平：中國宣導建設和平、安全、開放、合作的網絡空間」，**新華網**，http://news.xinhuanet.com/world/2015-09/24/c_1116663156.htm，檢索日期 2017 年 4 月 20 日。

「習近平：在第三屆世界互聯網大會開幕式上的視頻講話」，**新華網**，http://news.xinhuanet.com/2016-11/16/c_1119925133.htm，檢索日期 2017 年 4 月 20 日。

「習近平：把我國從網絡大國建設成爲網絡強國」，**新華網**，http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm，檢索日期 2017 年 4 月 22 日。

「習近平：讓互聯網更好造福國家和人民」，**新華網**，http://news.xinhuanet.com/politics/2016-04/19/c_1118672059.htm，檢索日期 2017 年 4 月 22 日。

「習近平『南巡』：訪前海察騰訊探母親」，**文匯網**，http://news.wenweipo.com/2012/12/08/IN1212080018.htm，檢索日期 2017 年 4 月 22 日。

「習近平巴西談互聯網治理」，**新華網**，http://news.xinhuanet.com/world/2014-07/17/c_1111673270.htm，檢索日期 2017 年 4 月 22 日。

「習近平向首屆世界互聯網大會致賀詞」，**新華網**，http://news.xinhuanet.com/politics/2014-11/19/c_1113319278.htm，檢索日期 2017 年 4 月 20 日。

「習近平在亞太經合組織第 23 次領導人非正式會議上的講話」，**新華網**，http://news.xinhuanet.com/world/2015-11/19/c_1117201278.htm，檢索日期 2017 年 4 月 22 日。

「習近平在第二屆世界互聯網大會開幕式上的講話」，**新華網**，http://news.xinhuanet.com/politics/2015-12/16/c_1117481089.htm，檢索日期 2017 年 4 月 20 日。

「習近平在網信工作座談會上的講話全文發表」，**新華網**，http://news.xinhuanet.com/politics/2016-04/25/c_1118731175.htm，檢索日期 2017 年 4 月 22 日。

「習近平參觀美國微軟公司總部」，**新華網**，http://news.xinhuanet.com/world/2015-09/24/c_1116667179.htm，檢索日期 2017 年 4 月 28 日。

「習近平訪美中方成果清單發佈」，**人民網**，http://politics.people.com.cn/n/2015/0926/c1001-27637282.html，檢索日期 2017 年 4 月 28 日。

「習近平親自出馬，主掌中國網絡安全」，**BBC 中文網**，http://www.bbc.com/zhongwen/trad/china/2014/02/140227_china_xi_web_security，檢索日期 2017 年 4 月 22 日。

「陸決定中止中美網路工作組活動」，**中時電子報**，http://www.chinatimes.com/realtimenews/20140519005093-260409，檢索日期 2017 年 4 月 21 日。

「焦點對話：自乾五是如何煉成的」，**美國之音**，http://www.voachinese.com/a/VOAWeishi-ProandCon-20160617-The-rise-of-Chinas-volunteer-50-centers-Is-Chinas-education-to-blame/3380445.html，檢索日期 2017 年 4 月 21 日。

「楊潔篪在第六輪中美戰略與經濟對話聯合記者會上的講話」，**大公網**，http://finance.takungpao.com.hk/q/2014/0711/2591950.html，檢索日期 2017 年 4 月 21 日。

「農村電子商務發展的戰略與政策」，**新華網**，http://news.xinhuanet.com/tech/2017-03/09/c_1120593562.htm，檢索日期 2017 年 4 月 22 日。

「網絡強國，習近平呼籲對網絡輿論的引導」，**多維新聞**，http://china.dwnews.com/news/2016-10-09/59774082.html，檢索日期 2017 年 4 月 20 日

「網絡產品和服務安全審查辦法（試行）」，**中國國家互聯網信息辦公室**，http://www.cac.gov.cn/2017-05/02/c_1120904567.htm，檢索日期 2017 年 8 月 15 日。

「領英騰訊紅杉寬頻聯合發起中美數字經濟合作協會」，**騰訊科技**，http://info.3g.qq.com/g/index5/ttnews/yidian.jsp?aid=yidian&id=tech_20151217044055&g_f=23748，檢索日期 2017 年 4 月 15 日。

「魯煒出席首屆世界互聯網大會並致辭」，**中國新聞網**，http://www.chinanews.com/gn/2014/11-19/6793335.shtml，檢索日期 2017 年 4 月 20 日。

「錢小芊在第六屆中美互聯網論壇發表主旨演講」，**新華網**，http://big5.news.cn/gate/big5/news.xinhuanet.com/info/2013-04/10/c_132296277.htm，檢索日期 2017 年 4 月 24 日。

「關於促進移動互聯網健康有序發展的意見」，**中國國務院**，http://news.xinhuanet.com/politics/2017-01/15/c_1120315481.htm，檢索日期 2017 年 8 月 15 日。

中國互聯網絡信息中心，**第 39 次中國互聯網絡發展狀況統計報告**（北京：中國互聯網絡信息中心，2017 年）。

中國國務院，**中國互聯網狀況**（北京：中國國務院新聞辦公室，2010 年）。

王德培，**再平衡：中國的優勢與美國的強勢**（上海：文匯出版社，2013 年）。

吳家恆等譯，Eric Schmidt and Jared Cohen 著，**數位新時代**（臺北：遠流，2013 年）。

宋筱元，「習近平時期中共的網絡輿論管理」，**展望與探索**，第 14 卷第 3 期（2016 年 3 月），頁 63~64。

李恆陽，「美國網絡軍事戰略探析」，**國際政治研究**，第 1 期（2015 年 2 月），頁 113~134。

汪玉凱，「中央網絡安全和信息化領導小組的由來及其影響」，**中國信息安全**，第 3 期（2014 年 3 月），頁 24~28。

周琪、汪曉風，「網絡安全與中美新型大國關係」，**當代世界**，第 11 期（2013 年 11 月），頁 30~34。

林幼嵐譯，Frédéric Martel 著，**全球網路戰爭**（新北市：稻田，2016 年）。

陳一新，「美『中』雙方在歐習會的得失及與對兩岸的影響」，**展望與探索**，第 13 卷第 10 期 (2015 年 10 月)，頁 1~11。

新華網網絡輿情監測分析中心，**2016 年度社會熱點事件網絡輿情報告** (北京：新華網網絡輿情監測分析中心，2017 年)。

劉得民，「中國大陸網軍外圍組織現況研究」，**中共研究**，第 48 卷第 7 期 (2014 年 7 月)，頁 131~139。

潘曉霞、黃建濱，「Hedging 的交際功能」，**美中外語**，第 2 卷第 7 期 (2004 年 7 月)，頁 11~18。

蔡明彥、張凱銘，「『避險』戰略下大國互動模式之研究：以美中亞太戰略競合爲例」，**遠景基金會季刊**，第 16 卷第 3 期 (2015 年 7 月)，頁 1~68。

關慶豐，「中美如何通過 90 多個平臺對話？」，**北京青年報**，http://bjyouth.ynet.com/3.1/1306/10/8068300.html，檢索日期 2017 年 4 月 21 日。

"DOD Releases Fiscal Year 2014 Budget Proposal," *U.S. Department of Defense*, http://dodcio.defense.gov/Portals/0/Documents/Library/2014%20Press%20Release.pdf. Accessed on April 22, 2017.

"DoD Releases Fiscal Year 2016 Budget Proposal," *U.S. Department of Defense*, https://www.defense.gov/News/News-Releases/News-Release-View/Article/605365. Accessed on April 22, 2017.

"First U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues Summary of Outcomes," *U.S. Department of Justice*, https://www.justice.gov/opa/pr/first-us-china-high-level-joint-dialogue-cybercrime-and-related-issues-summary-outcomes-0. Accessed on April 22, 2017.

"Hagel in Singapore on U.S. Security Policy in Asia-Pacific Region," *U.S. Department of Defense*, http://iipdigital.usembassy.gov/st/english/texttrans/2013/06/20130601148324.html#ixzz4XMHSZORO. Accessed on April 22, 2017.

"Hat-tribution to PLA Unit 61486," *CrowdStrike*, https://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486/. Accessed on April 22, 2017.

"History of HQ Twenty-Fourth Air Force and 624th Operations Center," *24 AF Office of History*, http://www.24af.af.mil/Portals/11/documents/About_Us/AFD-140429-035.pdf?ver=2016-04-26-113101-810. Accessed on April 22, 2017.

"Internet 2 China Program," *Internet 2*, http://www.internet2.edu/communities-groups/international-community/internet2-china-program/. Accessed on April 21, 2017.

"Navy Stands up Fleet Cyber Command, Reestablishes U.S. 10th Fleet," *U.S. Fleet Cyber Command*, http://www.stratcom.mil/Media/News/News-Article-View/Article/983834/navy-stands-up-fleet-cyber-command-reestablishes-us-10th-fleet/. Accessed on April 22, 2017.

"Press Briefing by National Security Advisor Tom Donilon," *The White House*, https://obamawhitehouse.archives.gov/the-press-office/2013/06/08/press-briefing-national-security-advisor-tom-donilon. Accessed on April 22, 2017.

"Press Release: China, India Now World's Largest Internet Markets," *International Telecommunication Union*, http://www.itu.int/en/mediacentre/Pages/2016-PR35.aspx. Accessed on April 20, 2017.

"Second U.S.-China Cybercrime and Related Issues High Level Joint Dialogue," *U.S. Department of Justice*, https://www.justice.gov/opa/pr/second-us-china-cybercrime-and-related-issues-high-level-joint-dialogue. Accessed on April 22, 2017.

"These are the 20 China-exposed Stocks to avoid," *MarketWatch*, http://www.marketwatch.com/story/these-are-the-20-china-exposed-stocks-to-avoid-2015-08-10. Accessed on April 20, 2017.

"Third U.S.-China High-Level Joint Dialogue on Cybercrime and Related Issues," *U.S. Department of Justice*, https://www.justice.gov/opa/pr/second-us-china-cybercrime-and-related-issues-high-level-joint-dialogue. Accessed on April 22, 2017.

"U.S., China Cyber Group Holds First Talks Since September Pact," *Reuters*, http://uk.reuters.com/article/us-usa-china-cyber-idUKKCN0Y22OB. Accessed on April 27, 2017.

"US-China Cyber Security Working Group Meets," *BBC News*, http://www.bbc.com/news/world-asia-china-23177538. Accessed on April 22, 2017.

Aaronson, Susan A. and Kimberly A. Elliott, "A China-U.S. Approach to Digital Trade," *China-United States Exchange Foundation*, http://www.chinausfocus.com/finance-economy/a-china-us-approach-to-digital-trade. Accessed on April 22, 2017.

Akl, Aida, "Iran Plans Its Own Sanitized Internet with Chinese Help," *Voice of America*, https://www.voanews.com/a/iran-plans-its-own-sanitized-internet-with-chinese-help/1713638.html. Accessed on August 17, 2017.

Art, Robert J., "Striking the Balance," *International Security*, Vol. 30, No. 3 (Winter 2005-06), pp. 178~180.

Brooks, Stephen G. and William C. Wohlforth, "Hard Times for Soft Balancing," *International Security*, Vol. 30, No. 1 (Summer 2005), pp. 72~108.

Busby, Scott, "10 Things You Need to Know about U.S. Support for Free Internet," *IIP Digital*, http://iipdigital.usembassy.gov/st/english/article/2014/05/20140530300596.html#ixzz4XMASG4Pj. Accessed on April 20, 2017.

Caton, Jeffrey L., *Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications* (Carlisle: U.S. Army War College, 2015).

Center for Strategic and International Studies, *Net Losses: Estimating the Global Cost of Cybercrime* (Washington, D.C.: Center for Strategic and International Studies, 2014).

Chang, Amy, *Warring State: China's Cybersecurity Strategy* (Washington, D.C.: Center for

a New American Security, 2015).

Clinton, Hillary, "Remarks on Internet Freedom," *American Institute in Taiwan*, https://www.ait.org.tw/en/officialtext-ot1004.html. Accessed on April 22, 2017.

Cohen-Almagor, Raphael, "Internet History," *International Journal of Technoethics*, Vol. 2, No. 2 (April-June 2011), pp. 45~64.

Costello, John, "The Strategic Support Force: China's Information Warfare Service," *China Brief*, Vol. 16, No. 3 (February 2016), pp. 15~20.

Dexian, Cai, "Hedging for Maximum Flexibility: Singapore's Pragmatic Approach to Security Relations with the US and China," *Pointer*, Vol. 39, No. 2 (July 2013), pp. 1~12.

FireEye Corporation, *Red Line Drawn: China Recalculates Its Use of Cyber Espionage* (Milpitas: FireEye Corporation, 2016).

Fisher, Max, "Russia and the U.S. Election: What We Know and Don't Know," *The New York Times*, https://www.nytimes.com/2016/12/12/world/europe/russia-trump-election-cia-fbi.html?_r=0. Accessed on April 20, 2017.

Fortin, Jacey, "Russia, Saudi Arabia, China and others fail to Impose Internet Regulations at WCIT," *International Business Times*, http://www.ibtimes.com/russia-saudi-arabia-china-others-fail-impose-internet-regulations-wcit-931654. Accessed on April 22, 2017.

Goh, Evelyn, *Meeting the China Challenge: The U.S. in Southeast Asian Regional Security Strategies* (Washington, D.C.: East-West Center, 2005).

Graham, Jefferson, "Google CEO: Open to Returning to China," *USA Today*, https://www.usatoday.com/story/tech/2016/06/01/google-ceo-open-returning-china/85247082/. Accessed on April 20, 2017.

Gueham, Farid, *Digital Sovereignty* (Paris: The Fondation pour l'Innovation Politique, 2017), pp. 15~16.

Harold, Scott W., Martin C. Libicki and Astrid S Cevallos, *Getting to Yes with China in Cyberspace* (Santa Monica: RAND Corporation, 2016).

He, Kai and Huiyun Feng, "If Not Soft Balancing, Then What?" *Security Studies*, Vol. 17, No. 2 (April 2008), pp. 363~395.

He, Kai, "Institutional Balancing and International Relations Theory: Economic Interdependence and Balance of Power Strategies in Southeast Asia," *European Journal of International Relations*, Vo. 14, No. 3 (September 2008), pp. 489~518.

He, Kai, *Institutional Balancing in the Asia Pacific, Economic Interdependence and China's Rise* (New York: Routledge, 2009).

Hollis, David M., "USCYBERCOM: The Need for a Combatant Command versus a Subunified Command," *Joint Force Quarterly*, No. 58 (June 2010), pp. 48~53.

Horwitz, Josh, "A New Wave of US Internet Companies is Succeeding in China," *Quartz*,

https://qz.com/435764/a-new-wave-of-us-internet-companies-is-succeeding-in-china-by-giving-the-government-what-it-wants/. Accessed on April 20, 2017.

Howell, Catherine and Darrell M. West, "The Internet as a Human Right," *The Brookings Institution*, https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/. Accessed on April 20, 2017.

Ikenberry, John G. ed., *America Unrivaled: The Future of the Balance of Power* (Ithaca: Cornell University Press, 2002).

Kai, Jin, "Why China Banned Windows 8," *The Diplomat*, http://thediplomat.com/2014/05/why-china-banned-windows-8/. Accessed on April 22, 2017.

Khalilzad, Zalmay M. et al., *The United States and a Rising China: Strategic and Military Implications* (Santa Monica: RAND Corporation, 1999).

Khudayer, Aiesha Y. et al., "Impact of NSA-PRISM to National Information Security Strategy & Policy," *International Journal of Information and Communication Technology Research*, Vol. 4, No. 1 (January 2014), pp. 25~31.

King, Gary, Jennifer Pan and Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument," *American Political Science Review*, http://gking.harvard.edu/files/gking/files/50c.pdf. Accessed on April 22, 2017.

Kopan, Tal, "Kerry: 'Very Likely' China, Russia Read my Emails," *CNN*, https://edition.cnn.com/2015/08/11/politics/kerry-emails-chinese-russian-hackers/index.html. Accessed on April 10, 2018.

Kuik, Cheng-Chwee and Kong Chian Lee, "Rising Dragon, Crouching Tigers?" *Biblioasia*, Vol. 3, No. 4 (January 2008), pp. 4~13.

Kuik, Cheng-Chwee, "The Essence of Hedging: Malaysia and Singapore's Response to a Rising China," *Contemporary Southeast Asia*, Vol. 30, No. 2 (August 2008), pp. 159~185.

Kuik, Cheng-Chwee, Nor Azizan Idris and Abd Rahim Md Nor, "The China Factor in the U.S. 'Reengagement' with Southeast Asia: Drivers and Limits of Converged Hedging," *Asian Politics & Policy*, Vol. 4, No. 3 (July 2012), pp. 315~344.

Kumar, Anugrah, "Obama, Xi Jinping Meet in California to Discuss North Korea, Cybersecurity," *The Christian Post*, http://www.christianpost.com/news/obama-xi-jinping-meet-in-california-to-discuss-north-korea-cybersecurity-97603/. Accessed on April 22, 2017.

Lau, Justine, "A History of Google in China," *The Financial Times*, http://www.ft.com/cms/s/0/faf86fbc-0009-11df-8626-00144feabdc0.html?ft_site=falcon#axzz4dGMpKxlN. Accessed on April 22, 2017.

Lawrence, Susan V., *U.S.-China Relations: An Overview of Policy Issues* (Washington, D.C.: Congressional Research Service, 2013).

Lee, Seungjoo, *The Evolutionary Dynamics of Institutional Balancing in East Asia* (Seoul: The East Asia Institute, 2012).

Lieber, Keir A. and Gerard Alexander, "Waiting for Balancing: Why the World is not Pushing Back," *International Security*, Vol. 30, No. 1 (Summer 2005), pp. 109~139.

Lieberthal, Kenneth G. and Peter W. Singer, *Cybersecurity and U.S.-China Relations* (Washington, D.C.: The Brookings Institution, 2012).

Lieberthal, Kenneth G. and Wang Jisi, *Addressing U.S.-China Strategic Distrust* (Washington, D.C.: The Brookings Institution, 2012).

Mandiant Corporation, *APT1: Exposing One of China's Cyber Espionage Units* (Washington, D.C.: Mandiant Corporation, 2013).

Margolin, Jack, "Russia, China, and the Push for 'Digital Sovereignty'," *IPI International Peace Institute*, https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization/. Accessed on April 22, 2017.

Medeiros, Evan S., "Strategic Hedging and the Future of Asia-Pacific Stability," *The Washington Quarterly*, Vol. 29, No. 1 (Winter 2005-2006), pp. 145~167.

Monaco, Lisa O., "Counterterrorism, Cybersecurity, and Homeland Security," *Council on Foreign Relations*, http://www.cfr.org/cybersecurity/counterterrorism-cybersecurity-homeland-security/p38642. Accessed on April 22, 2017.

Morrison, Wayne M., *China-U.S. Trade Issues* (Washington, D.C.: Congressional Research Service, 2017).

Mulvenon, James, "PLA Computer Network Operations: Scenarios, Doctrine, Organizations, and Capability," in Roy Kamphausen, David Lai and Andrew Scobellm eds., *Beyond the Strait: PLA Missions Other Than Taiwan* (Carlisle: The Strategic Studies Institute of the U.S. Army War College, 2009), pp. 253~285.

Nakashima, Ellen and Joby Warrick, "Stuxnet was Work of U.S. and Israeli Experts, Officials Say," *The Washington Post*, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-ay/2012/06/01/gJQAlnEy6U_story.html?utm_term=.847875342088. Accessed on April 20, 2017.

Nippard, Cinnamon, "International Blogging Conference Puts Internet Press Freedom on the Agenda," *Deutsche Welle*, http://www.dw.com/en/international-blogging-conference-puts-internet-press-freedom-on-the-agenda/a-5474714. Accessed on April 20, 2017.

Pape, Robert A., "Soft Balancing Against the United States," *International Security*, Vol. 30, No. 1 (Summer 2005), pp. 7~45.

Patry, Melody, *Brazil: A New Global Internet Referee?* (London: Index on Censorship, 2014).

Paul, T. V., "The Enduring Axioms of Balance of Power Theory," in T. V. Paul, James J. Wirtz, and Michel Fortmann eds., *Balance of Power: Theory and Practice in the 21st*

Century（Stanford: Stanford University Press, 2004）, pp. 1~28.

Pempel, T. J., "Soft Balancing, Hedging, and Institutional Darwinism: The Economic-Security Nexus and East Asian Regionalism," *Journal of East Asian Studies*, No. 10（2010）, pp. 209~238.

Perlroth, Nicole, "2nd China Army Unit Implicated in Online Spying," *The New York Times*, https://www.nytimes.com/2014/06/10/technology/private-report-further-details-chinese-cyberattacks.html?_r=0. Accessed on April 22, 2017.

Perlroth, Nicole, "Cyberattacks a Topic in Obama Call With New Chinese President," *The New York Times*, https://bits.blogs.nytimes.com/2013/03/14/cyberattacks-prominent-in-obama-call-with-new-chinese-president/?_r=0. Accessed on April 22, 2017.

Qun, Wang "Shared Interests and Responsibility: The US and China Must Join to Promote a Rules-based Cyberspace," *The Huffington Post*, http://www.huffingtonpost.com/wang-qun/shared-interests-and-resp_b_9873642.html. Accessed on August 17, 2017.

Racicot, Jonathan, "The Past, Present and Future of Chinese Cyber Operations," *Canadian Military Journal*, Vol. 14, No. 3（Summer 2014）, pp. 26~37.

Raud, Mikk, *China and Cyber: Attitudes, Strategies, Organisation*（Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2016）.

Reed, Kevin, "Global Split over Telecom Treaty," *World Socialist Web Site*, https://www.wsws.org/en/articles/2012/12/28/wcit-d28.html. Accessed on April 22, 2017.

Roberts, Dan, "US and China Back off Internet Arms Race but Obama Leaves Sanctions on the Table," *The Guardian*, https://www.theguardian.com/us-news/2015/sep/25/us-china-cyber-security-obama-xi-jinping-inconclusive-summit. Accessed on April 10, 2018.

Roy, Denny, "Southeast Asia and China: Balancing or Bandwagoning?" *Contemporary Southeast Asia*, Vol. 27, No. 2（August 2005）, pp. 305~322.

Ruland, Jurgen, "Interregionalism and International Relations: Reanimating an Obsolescent Research Agenda?" in Francis Baert, Tiziana Scaramagli and Fredrik Soderbaum eds., *Intersecting Interregionalism: Regions, Global Governance and the EU*（Dordrecht: Springer, 2014）, pp. 15~36.

Sanger, David E., "Obama Order Sped up Wave of Cyberattacks against Iran," *The New York Times*, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0. Accessed on April 20, 2017.

Sanger, David E., David Barboza and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *The New York Times*, http://cn.nytimes.com/china/20130219/c19hack/en-us/. Accessed on April 22, 2017.

Schmidt, Michael S. and David E. Sanger, "5 in China Army Face U.S. Charges of Cyberattacks," *The New York Times*, https://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html?_r=0. Accessed on April 22, 2017.

Schmitt, Eric and Thom Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," *The New York Times*, http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html. Accessed on April 22, 2017.

Schweller, Randall, "Managing the Rise of Great Powers: History and Theory," in Alastair Iain Johnston and Robert S. Ross eds., *Engaging China: The Management of an Emerging Power* (London: Routledge, 1999), pp. 1~31.

Scott, James and Drew Spaniel, *ICIT Briefing: China's Espionage Dynasty* (Washington, D.C.: Institute for Critical Infrastructure Technology, 2016).

Sharma, Deepak, "Integrated Network Electronic Warfare: China's New Concept of Information Warfare," *Journal of Defence Studies*, Vol. 4, No. 2 (April 2010), pp. 36~49.

Steinberg, James B., *Strategic Reassurance and Resolve: U.S.–China Relations in the Twenty-First Century* (New Jersey: Princeton University Press, 2014).

Stokes, Mark A. and L. C. Russell Hsiao, *Countering Chinese Cyber Operations: Opportunities and Challenges for U.S. Interests* (Arlington: Project 2049 Institute, 2012).

Stokes, Mark A., Jenny Lin and L.C. Russell Hsiao, *The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure* (Arlington: Project 2049 Institute, 2015).

Stokes, Mark A., *The PLA General Staff Department Third Department Second Bureau: An Organizational Overview of Unit 61398* (Arlington: Project 2049 Institute, 2015).

The White House, *Cyberspace Policy Review* (Washington, D.C.: The White House, 2009).

The White House, *International Strategy for Cyberspace* (Washington, D.C.: The White House, 2011).

The White House, *National Security Strategy 2006* (Washington, D.C.: The White House, 2006).

The White House, *National Security Strategy 2015* (Washington, D.C.: The White House, 2015).

Theohary, Catherine A. and Cory Welt, "Russia and the U.S. Presidential Election," *Congressional Research Service*, https://fas.org/sgp/crs/natsec/IN10635.pdf. Accessed on April 20, 2017.

U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, D.C.: U.S. Department of Defense, 2011).

U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2016* (Washington, D.C.: U.S. Department of Defense, 2016).

U.S. Department of Defense, *National Military Strategy 2004* (Washington, D.C.: U.S. Department of Defense, 2004).

U.S. Department of Defense, *Quadrennial Defense Review Report 2006*（Washington, D.C.: U.S. Department of Defense, 2006）.

U.S. Department of Defense, *Quadrennial Defense Review Report 2014*（Washington, D.C.: U.S. Department of Defense, 2014）.

U.S. Department of Defense, *The Department of Defense Cyber Strategy*（Washington, D.C.: U.S. Department of Defense, 2015）.

U.S. Department of the Army, *Field Manual 3-38: Cyber Electromagnetic Activities*（Washington, D.C.: U.S. Department of the Army, 2014）.

U.S. Joint Chiefs of Staff, *Joint Publication 3-12*（*R*）*: Cyberspace Operations*（Washington, D.C.: U.S. Joint Chiefs of Staff, 2013）.

U.S. Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*（Washington, D.C.: U.S. Joint Chiefs of Staff, 2006）.

U.S.-China Economic and Security Review Commission, *2015 Report to Congress of the U.S.-China Economic and Security Review Commission*（Washington, D.C.: U.S.-China Economic and Security Review Commission, 2015）.

U.S.-China Economic and Security Review Commission, *2016 Report to Congress of the U.S.-China Economic and Security Review Commission*（Washington, D.C.: U.S.-China Economic and Security Review Commission, 2016）.

USA Features Media, "SECDEF Carter Shifts Focus to Chinese Cyber-espionage as Shangri-La Summit Approaches," *Glitch News*, http://glitch.news/2016-06-08-secdef-carter-shifts-focus-to-chinese-cyber-espionage-as-shangri-la-summit-approaches.html. Accessed on April 10, 2018.

Waltz, Kenneth N., *Realism and International Politics*（New York: Taylor & Francis, 2008）.

Waltz, Kenneth N., *Theory of International Politics*（New York: McGraw-Hill, 1979）.

Weitsman, Patricia A., *Dangerous Alliances: Proponents of Peace, Weapons of War*（Stanford, CA: Stanford University Press, 2004）.

Wilson, J. R., "MARFORCYBER: Marines Fight in a New Domain," *Defense Media Network*, http://www.defensemedianetwork.com/stories/marforcyber-marines-fight-in-a-new-domain/. Accessed on April 22, 2017.

Wilson, Jordan, *China's Position on the Sony Attack: Implications for the U.S. Response*（Washington, D.C.: U.S.-China Economic and Security Review Commission, 2015）.

Wright, David and Reinhard Kreissl, "European Responses to the Snowden Revelations: A Discussion Paper," *Increasing Resilience in Surveillance Societies*, http://irissproject.eu/wp-content/uploads/2013/12/IRISS_European-responses-to-the-Snowden-revelations_18-Dec-2013_Final.pdf. Accessed on June 22, 2018.

Zhang, Li, "A Chinese Perspective on Cyber War," *International Review of the Red Cross*, Vol. 94, No. 886（Summer 2012）, pp. 801~807.

Zhu, Xu-Dong and Rachel Hong, “How some of America’s Biggest Tech Companies are Expanding into China,” *Business Insider*, http://www.businessinsider.com/us-tech-companies-expanding-into-china-2014-6. Accessed on April 20, 2017.