

中美數位霸權競爭之理論、意涵與啟示*

姚宏旻

國防大學戰略研究所助理教授

摘 要

本文運用國際關係理論中安全研究的分析視角，探討中美兩國於網路空間爭奪數位霸權之案例。當前文獻中，無論是權力最大化或是安全最大化論者，這些傳統現實主義的安全邏輯，皆仰賴競爭中國家行為體對於威脅源物質力量之評估，俾做出回應。美國近年雖不斷聲稱中共於網路空間執行間諜活動，並透過華為及中興通訊擴展其網路權力，而我國亦成立資通電軍以遏制中共之網路威脅，然現存學界對網路權力之學理分析仍甚缺乏。這除肇因以往學界對網路「無國界」的認知，難以與立基於「有國界」形式的傳統國關理論匹配；同時網路武器及資訊能力的物質基礎，亦無法像軍事戰機及潛艇般具體量化；再者網路上可匿名的特性也對網路安全領域研究學者產生認識論上的限制，並阻礙國安及司法單位有效辨別攻擊源頭。因此，本研究立基於資訊科學所認知之網路空間概念，來評估網路權力變動，並進而反思其對我國網路安全戰略之意涵與啟示。

關鍵字：中美關係、網路安全、數位霸權、國際關係理論、葛蘭西霸權

* 作者誠摯感謝兩位匿名審查者及編輯委員會在全文精進及題目修改上的寶貴建議，並感謝國防部在本項研究的支持，惟所有文責當由作者承當。

A Case Study in the Sino-US Competition for Digital Hegemony: Theories, Meanings and Implications

Hon-Min Yau

Assistant Professor at the Graduate Institute of Strategic Studies
(GISS), War College, National Defence University

Abstract

This article investigates the competition of digital hegemony between the US and China via the approach of Security Studies in the discipline of International Relations (IR). Traditional Security Studies, either power maximizer or security maximizer, devise a security policy in response to the assessment of an adversary's material power. Although the US and Taiwan argued that China has presented a threat via the use of cyber espionage and the leverage of its ICT enterprises, such as Huawei and ZTE, there are still challenges, which limit the capacity of scholars to explain how China's cyberpower can be measured. First, the so-called "borderless" nature of cyberspace is incompatible with traditional IR theories based on national borders. Furthermore, a country's capacity for cyberpower cannot be quantified as the same way as number of fighters or submarines. Besides, the anonymity on the Internet also presented an epistemological challenge that inhibits the timely attribution of attackers by the national security authority. Hence, this study argues

that the perception of cyberpower is possible only if our conceptual understanding of cyberspace is based on the knowledge from computer science. This article further explains what cyber dynamics between the US and China are and how their implications and meanings can affect Taiwan's policy-making.

Keywords: Sino-US Relations, Cybersecurity, Digital Hegemony, International Relations Theories, Gramscian Hegemony

壹、前言

二十一世紀的網路空間，已成為國家間權力擅場的領域，並開啟了全球網路衝突的興起時代，這可從以下案例觀察。首先位於波羅地海的愛沙尼亞 (Estonia)，於 2007 年因計劃搬遷前蘇聯時代遺留軍事紀念雕像，而遭到據信為俄羅斯 (Russia) 資助的網路攻擊。¹ 其後 2008 年時，當俄羅斯以軍事行動介入喬治亞共和國北方 (Georgia)，南奧賽提亞 (South Ossetia) 及阿布哈茲 (Abkhazia) 對喬治亞之獨立戰爭，使得喬治亞境內網站遭到巨量之分散式阻塞攻擊 (DDoS)，癱瘓眾多公私部門網路服務。² 2010 年國際社會更進一步發現據稱為以色列及美國合作發展的震網 (Stuxnet) 蠕蟲，該惡意程式不但成功滲透伊朗納坦茲 (Natanz) 核武設施內部網路，並破壞濃縮鈾提煉設備，拖延伊朗核武發展時程。³ 而 2017 年紐約時報更大幅報導，美國政府透過網路攻擊對北韓執行被稱為「主動抑制發射」(Left-of-launch) 的機密反導彈措施。⁴ 這些例子顯示，傳統的威脅 (主權國家) 透過非傳統手段 (網路攻擊) 引發安全問題 (網路安全)，網路空間已實然成為國家與國家間爭奪權力、影響國家安全的另一場域，而無論是國際關係或兩岸安全學者也嘗試運用理論瞭解國家行為體於網路空間

¹ Otto Kreisher, "Risk to One Is Risk to All," *Sea Power* 50, No. 12 (2007): 62.

² Steven Bucci, P, "A Most Dangerous Link," *US Naval Institute Proceedings* Vol. 135, No. 10 (2009).

³ K. Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (New York, US: Crow Publishing Group, 2014).

⁴ William J. Broad and David E Sanger, "U.S. Strategy to Hobble North Korea Was Hidden in Plain Sight," *New York Times*, 14 March 2017.

之互動；⁵ 因此，國家間對於數位霸權 (Digital Hegemony) 的爭奪，如何瞭解、分析甚至量測網路權力 (Cyberpower)，也成為學者所關注之議題。

然而國際關係學者透過安全理論分析視角觀察國家於網路空間之互動卻遭遇許多挑戰。首先，網路空間傳統上被視為沒有國家疆界 (Borderless)，也因此學者喬克里 (Nazli Choucri) 認為：「傳統國際關係理論立基於 ... 實體空間 ...，但是網路空間是另一種空間」。⁶ 艾克森 (Johan Eriksson) 及賈柯梅洛 (Giampiero Giacomello) 甚至認為：「國際關係理論與政府網路政策的實踐之間距離非常遙遠，也因此理論與實踐間毫無聯繫」。⁷ 也因此安全研究學者蓋瑞 (Colin Gray) 總結這現象，並認為現行著重網路空間之技術類文獻非常豐富，但運用理論來檢視該領域現象之研究則非常缺乏。⁸ 其次，網路攻擊的可匿名性 (Anonymity) 又為國際

⁵ 運用國際關係理論檢驗網路互動的研究可參閱 Hon-min Yau, "Explaining Taiwan's Cybersecurity Policy Prior to 2016: Effects of Norms and Identities," *Issues & Studies*, Vol. 54, No. 2 (2018); "A Critical Strategy for Taiwan's Cybersecurity: A Perspective from Critical Security Studies," *Journal of Cyber Policy* (2019).

⁶ 原文為："Traditional international relations theory is anchored ... in the physical venues ... , Cyberspace is yet another arena." 請見 Nazli Choucri, *Cyberpolitics in International Relations* (Cambridge MA: MIT Press, 2012).

⁷ 原文為："[IR] theory and practice [for digital policy] on this matter are so distinct that they hardly ever inform each other." 請見 Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: (Ir) Relevant Theory?," *International political science review*, Vol. 27, No. 3 (2006), p. 236.

⁸ 原文為："... the technical and even tactical literature on cyber is as abundant as the strategic theoretical treatment is both thin and poor." Colin S Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling* (Pennsylvania,

關係學者產生另一認識論上的限制 (Epistemological Constraint)，文獻上稱為「網路攻擊歸責問題」(Attribution Issue)。當發生電腦緊急事件時，社會大眾很難瞭解事件本質是否是肇因於意外、人為錯誤或惡意攻擊。甚至當確認為惡意攻擊時，政府機關也難以辯證攻擊來源是否出自犯罪團體、敵國或恐怖組織。由於沒有明確證據指明具體攻擊者的身分，也因此發起網路攻擊的國家常藉由推諉不知情 (Plausible Deniability) 來撇清責任。最後，傳統現實主義安全觀往往仰賴就對手國家之權力的計量來決定後續行動方案，⁹ 諸如人口數、領土面積、軍事資源等，然一國所擁有的網路武器及能力，其物質基礎並無法像軍事戰機及潛艇般能具體量化或概估，特別是程式碼的數量可以無限複製、惡意軟體攻擊距離沒有航程限制，也因此當我們缺乏對網路權力之瞭解，無法估算或掌握國家間於網路空間之權力消長，則吾人將能依據何基礎作為安全政策發展之立論根據呢？

有鑑於此，本研究將以國際關係理論，宏觀檢視中美兩國間之數位霸權爭奪，並進而探究對我國網路安全之啟示。事實上中美兩國在網路空間的齟齬已久，始自 2003 年時美國便發現來自中國大陸的網路間諜活動 - 極光行動 (Operation Aurora)，¹⁰ 其他為人熟知的例子還有 2010 年 Google 被迫退出中國市場、¹¹ 2014

U.S.: Strategic Studies Institute, US Army War College, 2013), p.iii.

⁹ Hans J. Morgenthau and Kenneth W. Thompson, *Politics among Nations : The Struggle for Power and Peace*, 7th ed. (Maidenhead: McGraw-Hill Education, 2005).

¹⁰ Marie Baezner, "Cybersecurity in Sino-American Relations," *CSS Analyses in Security Policy*, April 2018.

¹¹ 立法院，《立法院公報第 104 卷第 23 期》，台北：立法院，2015 年，

年美國司法部起訴據信是中國大陸 61398 部隊的 5 名駭客，¹² 以及 2015 年爆發美國人事管理局 (Office of Personnel Management, OPM) 遭中國大陸駭客入侵而大規模洩密，¹³ 而 2019 年 5 月 15 日美國政府商務部進一步宣布將中國大陸資訊大廠華為技術有限公司 (Huawei) 及其 68 家附屬公司納入貿易黑名單後，中國大陸也立刻於 2019 年 5 月 31 日宣布將建立「不可靠實體清單」反制，¹⁴ 中美兩國於數位空間的爭奪，似乎已進入到堅壁清野的科技冷戰 (Tech Cold War)。¹⁵ 而我國除於 2014 年時由馬英九總統時期副行政院長張善政指出，我國所遭受網路攻擊來源多來自對岸，¹⁶ 而自 2016 年起蔡英文總統更提出「資安即國安」指導。也因此我國於 2015 年由國安局成立網域第七處，¹⁷ 2016 年改組原資安

頁 383。Google, [https://www.google.cn/press/new-approach-to-china/update.html\(2020/05/21 查詢\)](https://www.google.cn/press/new-approach-to-china/update.html(2020/05/21 查詢))。

¹² Department of Justice, “U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a Labor Organization for Commercial Advantage,” *Department of Justice*, [https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.\(2020/05/21 查詢\)](https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.(2020/05/21 查詢))

¹³ 陳曉莉，〈美國人事管理局遭網路攻擊，400 萬公務員資料外洩，疑是中國所為〉，《iThome》，[https://www.ithome.com.tw/news/96493.\(2020/05/21 查詢\)](https://www.ithome.com.tw/news/96493.(2020/05/21 查詢))

¹⁴ 倪浩，〈商務部：中國將建立「不可靠實體清單」制度，具體措施近期出臺〉，《環球網》，<https://world.huanqiu.com/article/9CaKrKkMCF>。

¹⁵ Meng Jing, “Will Trump’s Assault on Huawei Create a Digital Iron Curtain?,” *South China Morning Post*, 26 May 2019.

¹⁶ Michael Gold and J.R Wu, “Taiwan Seeks Stronger Cyber Security Ties with U.S. To Counter China Threat,” *Reuters*, 30 May 2015.

¹⁷ 立法院，《立法院公報第 104 卷第 23 期》，台北：立法院，2015 年，頁 383。

辦公室而成立行政院資安處，¹⁸ 並於 2017 年成立資通電軍，¹⁹ 處處彰顯我國對於中國大陸網路權力上昇之戒心。然誠如前述所言，即便網路空間面臨許多不可輕易跨越的挑戰，諸如：跨國界 (Transnational) 活動、可逆名性及難以量化等問題，各國能基於何網路權力觀察基礎來決定其政策？而國際關係學者如何能就網路權力執行學理分析並為我國政策行動作出建議呢？有鑑於海峽兩岸之安全互動難以脫離美、中間互動，²⁰ 也因此本文將引入國際關係權力論述檢驗各方網路權力變動關係。

本文論述架構如下：首先就當前安全研究領域中，有關網路安全及網路權力之主要文獻執行回顧綜述，以界定理論缺口。其次釐清學界對網路空間認知之落差，以界定後續探討網路權力計量之網路空間概念架構。再者，依據網路空間概念架構綜合比較中美網路權力差異。最後，本文將就中美網路競爭之戰略意涵及對我當前政策作為進行反思，俾對後續政策提供可能建議。

貳、權力、安全與國際關係

假如網路權力決定數位霸權並影響國家安全，那現行文獻中對於網路安全研究所採取的途徑為何？首先，社會科學對於

¹⁸ China Post, “Cabinet Forms Department for Cyber Security,” *China Post*, 2 August 2016.

¹⁹ MOFA, “Ministry of National Defense Launches New Cybersecurity Command,” *Taiwan Today*, <https://taiwantoday.tw/news.php?unit=2,6,10,15,18&post=117794>. (2020/05/21 查詢)

²⁰ C. Clark, *The Changing Dynamics of the Relations among China, Taiwan, and the United States* (Newcastle upon Tyne, UK: Cambridge Scholars Publisher, 2011), 10-29.

權力的研究汗牛充棟，從古典論述到當代文獻包羅萬象令人目不暇給，也因此本段將集中在討論當代有關「網路權力」(Cyberpower)一詞之理論文獻。目前主要有學者，有喬丹 (Tim Jordan) 定義網路權力為規範網路空間文化及政治活動的權力，並進一步將其細分為三個層次：個人所能擁有的權力、宰制的權力及構成社會秩序的權力；²¹ 他的研究著重於瞭解網路空間在影響社會秩序層次的研究及對人類社會互動模式的影響。而庫爾 (Daniel T. Kuehl) 則定義網路權力為「能運用網路的能力以在各種作業環境及權力的工具中，創造利基及影響事件走向」。²² 另一學者史達爾 (Stuart H. Starr) 則進一步認為可以透過瞭解政治、外交、資訊及軍事等四面向掌握。²³ 庫爾及史達爾兩者似乎從純軍事安全面向思考「網路權力」的運用。而奈伊 (Joseph S. Nye) 則深化他軟、硬實力理論分野進一步探討網路權力如何可以被運用於國際間各層次互動，這延續奈伊認為權力包含物質及意識力兩層面的思維。²⁴ 貝茲 (David J. Betz) 及史蒂文 (Tim Stevens) 則依照巴奈特 (Michael Barnett) 及杜瓦爾 (Raymond Duvall) 就權力的研究，探討網路權力如何可以成為強性的 (Compulsory)、制度化的 (Institutional)、結構性 (Structural) 的及生產性 (Productive) 的權

²¹ T. Jordan, *Cyberpower: An Introduction to the Politics of Cyberspace* (Oxford, UK: Taylor & Francis, 2002), p. 4.

²² Daniel T. Kuehl, "From Cyberspace to Cyberpower: Define the Problem," in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, *Cyberpower and National Security* (Washington, DC, US: Potomac Books, Inc., 2009), pp. 41-42.

²³ Stuart H. Starr, "Toward a Preliminary Theory of Cyberpower," in *ibid.*, 46.

²⁴ Joseph S. Nye, "Cyber Power," (MA, US: Belfer Center for Science and International Affairs, 2010).

力，以影響國際政治各項議題走向。²⁵ 很明顯的，「網路權力」與權力一詞般，是一個本質上具有爭辯的概念，也常被國際研究學者稱為具有家族相似性 (A Family of Contested Resemblance)，²⁶ 由於所選定的權力意義 (Meaning) 往往與其希望分析的事件背景 (Context) 相關聯，也因此需進一步檢視現行安全研究中，對網路安全有關之權力論述。

在國際關係領域之安全研究文獻中，大部分有關網路權力的論述是採取戰略研究 (Strategic Studies) 途徑，並聚焦在軍事層面的互動，並側重在網路戰或是軍事事務革新的論述，例如紐麥爾 (Jacqueline Newmyer) 及高得曼 (Emily O. Goldman) 探討資訊科技對軍事事務革新的助益，強調網路能成為軍事行動的戰力倍增器，並提供軍事作戰以小搏大的利基。²⁷ 而達特內爾 (Michael Dartnell) 則著重在網路權力如何改變個人認同、重塑政治疆界，並認為網路空間中非國家行為體日益重要並將試圖傳播不同政治意識。²⁸ 而隨著 2010 年起震網病毒的發現，林賽 (Jon Lindsay) 及立夫 (Adam Liff) 則著重在探討震網病毒的威力對於未來戰

²⁵ D.J. Betz and T. Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power*, ed. International Institute for Strategic Studies (Oxford, UK: Routledge, 2011), pp. 35-54.

²⁶ Henri Goverde and Howard H Lentner, *Power in Contemporary Politics: Theories, Practices, Globalizations* (Sage, 2000), p. 17.

²⁷ Jacqueline Newmyer, "The Revolution in Military Affairs with Chinese Characteristics," *The Journal of Strategic Studies* 33, No. 4 (2010); Emily O Goldman, "Introduction: Information Resources and Military Performance," *Journal of Strategic Studies*, Vol. 27, No. 2 (2004).

²⁸ Michael Dartnell, "Weapons of Mass Instruction: Web Activism and the Transformation of Global Security," *Millennium*, Vol. 32, No. 3 (2003).

爭與軍事行動的潛在意涵。²⁹ 而當上述分析多來自政策圈或軍事智庫社群，國際關係理論學者也逐漸提供理論上的見解，德里安（James Der Derian）採用後結構途徑並認為「數位時代」在許多方面轉變了國家安全的定義與意涵，而他著重在瞭解話語建構 (Discursive Construction) 的「過程」及分析如何產製「資訊戰」的論述。³⁰ 卡維迪 (M.D. Cavelty) 則延伸德里安的視角，但進一步採取國際關係批判安全研究中的哥本哈根學派 (Copenhagen School) 途徑，以安全化的理論結合大眾傳播之議題設定與框架理論，據以論證美國政府之所以能在未有明確網路攻擊關鍵基礎設施事證前，仍能投注巨大資源防範威脅的可能，乃是由於論述的力量 (Power of Discourse)。³¹ 這樣著重於論述效用的還有韓森 (Lene Hansen) 與尼森鮑姆 (Helen Nissenbaum) 等學者，但這些學者跳脫過去著重語言建構 (construction) 的效果，轉而瞭解語言構成 (Constitution) 的效用，並認為「社會實體」(Social Reality) 無法獨立存在於人類語言之外，也強調社會實體如何受語言的效用而組成 (a Constitutive Effect of Discourse)。³² 也因此當我們未曾體驗到因遭網路攻擊而產生之大災難事件前，政治人物不斷用

²⁹ Jon R Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, Vol. 22, No. 3 (2013); Adam P Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies*, Vol. 35, No. 3 (2012).

³⁰ James Der Derian, "The Question of Information Technology in International Relations," *Millennium*, Vol. 32, No. 3 (2003).

³¹ M.D. Cavelty, *Cyber-Security and Threat Politics: Us Efforts to Secure the Information Age* (Oxford, UK: Taylor & Francis, 2007).

³² Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* Vol. 53, No. 4 (2009).

Cyber 911³³、數位珍珠港或是數位核冬天 (Digital Nuclear Winter)³⁴ 描述網路攻擊時，這些語言的效用「組成」(Constitute) 網路威脅的社會實體。³⁵ 顯然的，在與前述有關「網路權力」之回顧結合後發現，目前國際關係雖然對於運用理論來檢視網路安全逐步發展中，惟運用網路權力的理論來檢視並連結國際安全之研究仍多集中在政治影響力的意識層次之研究，尚未有就物質網路權力之計量，以協助界定數位霸權之形式。

最後，有關中美或台海的網路安全研究，似乎反映艾克森及賈柯梅洛認為國際關係理論與政府網路政策的實踐之間毫無聯繫的觀察；一方面來自戰略社群的分析多發表於智庫或評論性雜誌，並憑藉經驗的觀察描述而甚少與理論建立聯繫，³⁶ 而學術性強烈的期刊出版品，也未見有與網路權力或數位霸權相關的理論分析。例如，波爾特（Pau J. Bolt）、布倫納（Carl N. Brenner）及謝恩（Benjamin Shearn）曾經探討資訊戰在台海衝突的角色，

³³ P.W. Singer and A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know?* (Oxford, UK: Oxford University Press, 2014), p. 68.

³⁴ Larry Greenemeier, "Estonian Attacks Raise Concern over Cyber 'Nuclear Winter'," *Information Week*, May 24 (2007).

³⁵ Evgeny Morozov, "Cyber-Scare: The Exaggerated Fears over Digital Warfare," *Boston Review* 34, no. 4 (2009).

³⁶ Hon-min Yau (姚 宏 旻), "Evolution of cyber policy," Strategic Vision for Taiwan Security, Vol.4, Issue.24 (2015), Hon-min Yau, "Handle with Care: The Pandora's Box of Cyber Attacks," Thinking Taiwan, <http://thinking-taiwan.com/thinking-taiwan.com/handle-with-care-pandoras-box-cyber-attacks/index.html>; Russell Hsiao, "Critical Node: Taiwan's Cyber Defense and Chinese Cyber-Espionage," *China Brief* 13, no. 24 (2013); Michal Thim, "Taiwan's Invisible Frontier: Cyberspace," Thinking Taiwan Foundation, <http://thinking-taiwan.com/taiwans-invisible-frontier-cyberspace/>. (2020/05/21 查詢)

但他們的分析著重在中共資訊戰思維及準則的演變，而非網路戰力量的比較。³⁷ 羅恩斯利（Gary Rawnsley）則著重在網路空間如何能傳播恐懼，但他的分析著重在瞭解資訊所能造成的心理影響及欺敵效果等軟性權力，而非網路權力的物質面向。³⁸ 而隨著國際間報導中共網路活動頻繁，有關中國大陸網軍部隊的研究也不斷增加，較重要的有黃基禎及林穎佑等學者曾探討中共的網路戰略思維，及其軍事改革後的戰略支援部隊 (Strategic Support Force) 發展，惟前述研究除皆未著墨網路權力亦或未與其他國際關係或安全理論之連結。³⁹ 而自 2018 年起，雖然有學者嘗試運用國際關係理論探究台海網路問題，其中姚宏旻於 *Issues & Studies* 運用建構主義途徑解釋形成台灣網路政策的原因，及 *International Journal of Cyber Policy* 運用批判安全研究途徑，探究網路戰的負面影響及台灣其它策略可能，惟前述分析偏屬國家安全政策分析領域，並未對中美數位競爭執行研究。⁴⁰

³⁷ Paul J. Bolt and Carl N. Brenner, “Information Warfare across the Taiwan Strait,” *Journal of Contemporary China* Vol. 13, No. 38 (2004); M.M. Chu and S.L. Kastner, *Globalization and Security Relations across the Taiwan Strait: In the Shadow of China* (Taylor & Francis, 2014), pp. 158-182.

³⁸ Gary D Rawnsley, “Old Wine in New Bottles: China–Taiwan Computer-Based ‘Information Warfare’ and Propaganda,” *International Affairs*, Vol. 81, No. 5 (2005).

³⁹ Ji-Jen Hwang, “China’s Military Reform: The Strategic Support Force, Non-Traditional Warfare, and the Impact on Cross-Strait Security,” *Issues & Studies*, Vol. 53, No. 3 (2017); “Chinas Cyber Strategy: A Taiwanese Perspective,” *Korean journal of defense analysis*, Vol. 29, No. 1 (2017); 林穎佑，〈中國近期網路作為探討：從控制到攻擊〉，《臺灣國際研究季刊》，第 12 卷第 3 期 (2016).

⁴⁰ Yau, “Explaining Taiwan’s Cybersecurity Policy Prior to 2016: Effects of Norms and Identities.” ; “A Critical Strategy for Taiwan’s Cybersecurity:

總之，目前學界對於如何利用網路權力來解釋美中霸權競爭的研究尚未完備，大部分網路權力論者著重在非物質基礎的政治影響力分析；而部分嘗試探討物質基礎的網路權力分析，又僅多集中在經驗性分析而未能與安全理論相結合；少部分嘗試運用理論的研究則採用無須計量網路權力物質基礎的途徑。這樣的狀況顯示出學界對於如何連結傳統認知的「無國界」網路空間到國際關係安全研究中「有國界」物質權力基礎論述仍非常缺乏，也因此下一段將探究傳統現實主義安全研究途徑，可採用何種合適概念架構來支持後續客觀地網路權力計量。

參、網路空間與權力：從網路無國界到網路有國界

何謂「網路空間」(Cyberspace)呢？普遍而言，網路空間一詞可追溯到美國作家吉布森(William Gibson)於1984年所撰寫的《神經漫遊者》(Neuromancer)一書，⁴¹然時至今日，隨著資訊科技不斷發展，網路空間已不再是科幻小說中的一個詞彙，而是一個全新世界的代名詞。吉布森或許創造了一個新名詞，但是就這種全新科技空間的使用，實際卻可追溯到19世紀電報的運用，後人稱為「維多利亞網際網路」(Victoria Internet)。⁴²後來隨著美蘇冷戰的對峙，美國國防高等研究署(Defense Advanced Research Projects Agency, DARPA)於1960年代發展高等研究計畫署網路(The Advanced Research Projects Agency Network, ARPANET)，成

A Perspective from Critical Security Studies.”

⁴¹ Singer and Friedman, 12.

⁴² T. Standage, *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's on-Line Pioneers* (Bloomsbury USA, 2014).

為後來網際網路運用 TCP/IP 協定構建全球開放性網路的濫觴。惟隨著 1990 年代社會學家卡斯特斯（Manuel Castells）著作《網絡社會的崛起》（*The Rise of the Network Society*），⁴³ 網路空間常被認為是網際網路（Internet）或是全球資訊網（WWW）的代名詞，並且具無國家邊界的特殊空間。但這樣網路空間的認知基礎，對研究網路安全學者而言卻是一種意識型態的阻礙。誠如許多安全研究文獻所探討的震網病毒，該病毒滲透的伊朗核設施網路，非但未連接全球資訊網，也未與網際網路構聯，也因此過去立足「網路無國界」認知的網路安全研究，對於處理當前與時俱進的網路問題顯有不足處。也因此部分安全研究文獻常常過度渲染，若全球資訊網遭駭客攻擊，將造成電力、水源供應、國際金融傳輸及安全號誌的癱瘓。⁴⁴

事實上，網路空間是有邊界的。首先，常見的全球資訊網實際是由英國科學家伯納斯 - 李（Tim Berners-Lee）於 1989 年所發展的一種在網際網路上的服務，換言之網際網路上尚有許多不同服務，如傳輸電子郵件的 Simple Mail Transfer Protocol (SMTP) 及檔案交換的 File Transfer Protocol (FTP)。其次，網路空間包含網際網路之外其他網路，如公用電話交換網路 (Public Switch Telephone Network, PSTN)、負責自動控制的監督控制及資料獲取系統 (Supervisory control and data acquisition, SCADA)⁴⁵ 以及軍事用途的戰術數位資訊鏈路 (Tactical Digital Information Link,

⁴³ Manuel Castells, *The Rise of the Network Society* (Blackwell Publisher, 1996).

⁴⁴ Jan-Frederik Kremer and Benedikt Müller, *Cyberspace and International Relations* (London, UK: Springer, 2014), p. 68.

⁴⁵ Singer and Friedman, p. 115.

TADIL)。⁴⁶ 這些網路可能使用非 TCP/IP 的特殊協定，除可能與國際網路互聯亦或可獨立存在未與外界構聯。這樣的技術認知，反映在資訊學門對於計算機網路不同於人文學者的兩個認知：第一，各個網路之涵蓋是有限的，如：電腦科學常使用的區域網路、都會網路以及廣域網路等詞彙；其次，網路空間是多層次的服務，並由不同通訊協定之裝置所構聯；⁴⁷ 也因此資訊技術學門常以開放式系統互聯模型 (Open System Interconnection Model, OSI) 來描繪網路空間，透過將網路空間區分為 7 層次的概念化設計，⁴⁸ 例如：5G 無線網路所能提供的服務量雖然大於 4G 無線網路，但兩者主要差異在於 OSI 模組的底層協定不同，所以 5G 網路能增加資料傳輸頻寬並改善延遲率 (Latency)，故透過 OSI 模組的對應，位於這兩個不同網路系統的裝置還是能透過協定轉換執行訊息交換。⁴⁹

換言之，現行部分安全研究將所有技術細節籠統的以網路空間代稱，也因此形塑出網路「無國界」的印象；正如同霍克海默 (Max Horkheimer) 及阿多莫 (Theodor W. Adorno) 於《啟蒙

⁴⁶ Northrop Grumman, *Understanding Voice and Data Link Networking* (CA, US: Northrop Grumman, 2014).

⁴⁷ 趙坤茂 et al., 《計算機概論：當代資訊通鑑》(第 14 版)(全華圖書, 2019).

⁴⁸ 這七個層次分別是實體層 (Physical Layer)、資料連結層 (Data Link Layer)、網路層 (Network Layer)、傳輸層 (Transport Layer)、會議層 (Session Layer)、表達層 (Presentation Layer) 與應用層 (Application Layer)。功能性描述可以簡述為，實體層負責實體裝置規格、資料連結層負責裝置間訊框傳輸、網路層負責資料路徑選擇、傳輸層負責資料傳輸分割、會議層負責軟體間資料構連、表達層解讀資料成合適軟體格式、應用層將資料以正確格式呈現。

⁴⁹ Shara Tibken, "No, 5g Isn't Going to Make Your 4g Lte Phone Obsolete," cnet, <https://www.cnet.com/news/no-5g-isnt-going-to-make-your-4g-lte-phone-obsolete/>.(2020/05/21 查詢)

辯證法》所提出的警告般：所有的具體化都是要讓人們遺忘細節 (All Reification is a Forgetting)，也因此學者如能跳脫過去「使用者角度」的認知，改採「工程師角度」的技術細節觀點，則網路空間將變成類似水管管線般，可以區分「國界」縱橫交錯的銜接方式，也因此對網路權力的理解，便可以依附在傳統的權力框架下進行詮釋。所以當重要網路銜接點遭到網路攻擊時，網路不再是一個無國界的疆界，而是能成為前國防部副部長林中斌先生所稱「點穴戰」效用的有國界空間。⁵⁰

肆、美國於網路空間的數位霸權：設備與規則

如前所述，假如網路空間可以透過 OSI 模型來呈現，那我們如何透過這樣的框架來瞭解各國網路權力分布呢？由於網路空間是由支援不同 OSI 階層功能的軟體（包含作業系統及應用軟體等）及硬體（手機、電腦、伺服器、基地台及纜線等）所組成，也因此誰能主導對 OSI 各階層網路通訊協定及資源分配機制的訂定，誰就掌握對網路空間的權力。誠如學者萊西格（Lawrence Lessig）所指出的：在網路空間上，科技力主宰權力的運用，誰能掌握對各個軟硬體元件的設計、分發及管理，誰就擁有權力。⁵¹

而美國早在當前智慧手機及多媒體影音主導的資訊社會前，便佔據網路空間的戰略要地。回顧過去，無論是全球資訊網、個人電腦及電子商務發展，美國都手執牛耳。特別是當年柯林頓政

⁵⁰ 林中斌，《核霸：透視跨世紀中共戰略武力》（臺灣學生書局，1999），頁 5-9。

⁵¹ L. Lessig, *Code: And Other Laws of Cyberspace, Version 2.0* (New York, US: Basic Books, 2008), p. 15.

府將原為美國國防部所擁有的全球網際網路設施商業化，並據此帶領美國脫離 1990 年代初期的經貿遲滯，造就其任內輝煌經濟成果。⁵² 然而美國在網路空間的優勢，卻是立基在其對通訊協定規格制定及網路資源分配的宰制，例如美國對於網際網路通訊協定 TCP/IP v4 的發展主導，塑造其在網際網路上的主導地位。⁵³ 如同網際網路學者阿貝特（Janet Abbate）所論：通訊協定規格的定義是一種政治能力，因為這樣的能力代表著對科技的掌控能力。回顧早期資訊科技發展歷史，網路空間初期是由多種通訊協定所構成，雖然美國國防部大力支持網際網路的發展，但現在網際網路所通用的 TCP/IP v4 是遲至 1978 年才由美國加州大學洛杉磯分校的一群學者所開發完成。⁵⁴ 然當時的技術規格制訂，是有其它的競爭者的。當時聯合國轄下的國際電訊聯盟 (International Telecommunication Union)，挾著悠久的電報系統發展經驗及多數歐洲國家的支持，在 1976 年倡議另一通訊協定 X.25 挑戰美國主導規格。也由於這樣的競爭，在 1980 年代初期，網路空間事實上是由使用不同通訊協定的區域網路所組成，然美國後續透過 OSI 層次的另一元件作業系統的運用，亦即經由免費提供 TCP/IP v4 在所有 UNIX 系列的作業系統，美國終於在通訊協定主導權上獲得勝利。⁵⁵

⁵² Madeline Carr, *Us Power and the Internet in International Relations: The Irony of the Information Age* (Hampshire, UK: Palgrave Macmillan, 2016).

⁵³ 鍾兆真、蕭全政，〈美國的網際霸權：網路層、傳輸層與應用層的政治經濟分析〉，《台灣社會研究季刊》，第 68 期 (2007)。

⁵⁴ Milton L. Mueller, *Ruling the Root: Internet Governance and the Taming of Cyberspace* (MIT Press, 2009), pp. 74-75.

⁵⁵ J. Abbate, *Inventing the Internet* (MA, US: MIT Press, 2000), p. 133.

假如權力就像偉伯（Max Weber）所述「權力是個人在其社會關係中令他人服從其意志的力量」，⁵⁶ 換言之，在仰賴科技建構的網路空間，誰能決定 OSI 各階層軟硬體規格，誰便有能力主宰網路世界。由於權力是改變他人行為而獲致所望結果的能力，⁵⁷ 而在網路空間中，誰能掌控程式碼誰就擁有權力 (the Control of the Code is Power)。⁵⁸ 因此，美國透過 TCP/IP v4 通訊協定的掌握維繫其數位霸權的地位，這樣的霸權結構類似葛蘭西霸權理論中的文化霸權形式，透過其優勢資源與較佳的統治地位掌控網路空間。換言之，美國自 20 世紀以來在網際網路的霸權，來自於對映到各 OSI 個階層的設備供應商及掌控通訊協定及資源分配規範制的各種組織。現時 CISCO 是全球領先的網路設備製造商；IBM 是著名伺服器及企業服務供應商上；Google 是搜索引擎服務大廠，也是各種線上服務的主要提供者；Qualcomm 是通訊晶片的主要設計及供應商、Intel 是領先的計算機中央處理器 (Central Processing Unit, CPU) 設計及製造商；而 Apple 是商用消費型電子設備、手機、平板及軟體供應商；Oracle 是商用資料庫大廠；而 Microsoft 是作業系統主導者。而這樣的優勢還透過包含其位於全球網際網路治理體系所建構的各個不同的國際組織，包含網際網路名稱與數字位址分配機構 (Internet Corporation for Assigned Names and Numbers, ICANN) 負責 IP 配置管理、通訊參數設定、網域名稱轉譯服務伺服器管理及網域名稱管理；網際網路號碼分

⁵⁶ Talcott Parsons, *The Theory of Social and Economic Organization* (New York: Free Press; London: Collier Macmillan, 1964), p. 152.

⁵⁷ Joseph Nye, *The Future of Power* (New York: PublicAffairs, 2011).

⁵⁸ Lessig, 79.

配局 (Internet Assigned Number Authority, IANA) 負責網址分配及網域名稱分配；網際網路工程任務組 (Internet Engineering Task Force, IETF) 負責通訊協定規格討論與制定及網際網路協會 (Internet Society, ISOC) 為名目上的網路公民社會，參與網路世界議題討論。也因此國際知名的資安專家施耐爾 (Bruce Schneier) 便曾明確指出，幾乎世界上所有最受歡迎的軟硬體或是網路公司都是位於美國並受其法律所影響，毫無疑問的美國是一個數位霸權。⁵⁹

伍、中國大陸數位霸權網路權力的崛起：設備與規則

一、設備方面

中國大陸自改革開放後政經實力即不斷成長，而這樣的發展，在 1990 年代初期也逐漸延伸到網路世界，改變後續 21 世紀的網路空間版圖。在當時，來自韓國、日本、美國及台灣科技公司受到中國大陸廉價土力成本及充沛人力所吸引，競相於該地投資，使其影響力進一步延伸到構建網路空間的底層，即軟體與硬體的製造。這樣的現象，可以從佛里曼 (Thomas Friedman) 的《世界是平的：一部二十一世紀簡史》(The World Is Flat: A Brief History of the Twenty-first Century) 一窺究竟，書中描述戴爾電腦 (Dell) 雖然是一個美國公司，但是銷售部門卻位在印度，電腦由馬來西亞的廠商所組裝且台灣公司設計，而所使用的主要電腦零附件，事實上卻全是由中國大陸所生產製造，也因此中國大陸穩然成為世界工廠。⁶⁰

⁵⁹ B. Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (New York, US: W. W. Norton, 2015), 64.

⁶⁰ Thomas Friedman, 《世界是平的：一部二十一世紀簡史》(台北：雅言文化出版股份有限公司，2005)。

然中國大陸除在科技製造實力成長外，也不忘扶植本土技術巨擘。在「資訊性民族主義」的驅動下，中國大陸不斷發展本土性軟體系統，以降低對西方廠商依賴。⁶¹ 從 2000 年起，中國大陸啟動多項自主科研計畫，其中最有名的便是「揚帆遠航」計畫，希望透過「揚帆」子計畫執行發展以 Linux 為基礎的作業系統，以擺脫對 Microsoft 的依賴；並透過「遠航」子計畫，延伸發展自主作業系統上可以使用的軟體。⁶² 中國大陸的技術深耕已取得具體成果，至 2016 年時便已擁有 Deepin、Red Flag、Kylin、Neokylin、StarOS 及 Raspberrypi Idev OS 等多種作業系統。除此之外，就網路通訊設備而言，自 2018 年起，華為雖因財務長孟晚舟遭美國引渡及因美國政府認定網通設備有國安疑慮而遭到美國禁制令而聲名大噪，然早在 2003 年時，華為便與美國網通大廠 Cisco 陷入多項網路技術專利司法訴訟，然由於畏懼影響於中國市場的銷售，Cisco 後來放棄對該訴訟的相關權利。⁶³ 隨著中國大陸國內市場於資訊科技產業的重要日益增加，美歐國家的資訊廠日益屈服於中國大陸國家意向，例如：2017 年時美商 Microsoft 為贏得中國大陸官方信賴，宣布與中國大陸推出 Windows 10 中國政府官方版，除允許中國大陸檢視作業系統原始碼、移除不受信賴程式模組，並同意加裝中國政府授權之安全軟體及演算法。⁶⁴

⁶¹ 蔡裕明，〈資訊性民族主義 -Linux 對中國大陸的意義〉，《中國大陸研究》，第 44 卷第 14 期（2001）。

⁶² 張憶嬋，《開放原始碼軟體商業模式及相關法律問題之探討》（國立政治大學，2006），頁 47。

⁶³ Richard A Clarke and Robert K Knake，《網路戰爭：下一個國安威脅及因應之道》（國防部史政編譯室編譯處，2014）。

⁶⁴ Microsoft，“Announcing Windows 10 China Government Edition

換言之，中國大陸現在除擁有強大的製造能力、逐漸強大的軟硬體供應商，加之日益重要的國內軟硬體市場，它不再僅是世界工廠，儼然成為世界市場的重要一環。

透過人才、技術、製造能力及市場的結合，中國大陸已不再侷限於以往倚重製造設備的全球定位，並逐漸擴展版圖至技術與制度的掌控；然而這種中美間的數位爭霸的本質，已不再是過往對軟、硬體的製造掌控，而是昇華為對不同 ICT 次領域「規則」的主宰，這可從以下幾個例子觀察出這樣的趨勢。

首先，承前文所述，由於過去全球網際網路是立基於美國主導的 TCP/IP v4 協定，它所能提供全球網路位址的數量理論上能達 2^{32} 個，然而隨著全球網站數量增加、智慧型手機及平板的普及，以及中國大陸超過 8 億網民的加入，並以每年 6% 的比率增加，國際社會必須開發一新的通訊協定以解決網路位址不足問題 - 又稱為 IP v4 位址耗竭 (IPv4 Address Exhaustion)。⁶⁵ 中國大陸藉由過去觀察美國於網路空間獲取領導權的經驗，積極介入新協定開發。中國大陸教育和科研計算機網 (CERNET) 除自 1999 年時便加入新一代通訊協定 TCP/IP v6 國際發展計畫 6bone 行列，2003 年時更由中國官方發起「中國下一代互聯網」計畫，至 2004 年時成立中國大陸教育和科研計算機網第二號網路 (CERNET2) 落實 TCP/IP v6 布建，而至 2017 年時已成為連接超過 200 所科研

and the New Surface Pro,” Microsoft, <https://blogs.windows.com/windowsexperience/2017/05/23/announcing-windows-10-china-government-edition-new-surface-pro/>.(2020/05/21 查詢)。

⁶⁵ 中國互聯網路信息中心，《中國互聯網路發展狀況統計報告》（北京：中國互聯網路信息中心，2016）。

中心及 20 個城市的大型純 TCP/IP v6 網路。⁶⁶

其次，過去網際網路網域名稱 (Domain Name) 都是以拉丁字母為主所構成的體系，為改變西方所主導的網名秩序，中國大陸開始倡導建立以中文字母為主的網域名稱。中國大陸於 2000 年由信息產業部 (MIIT) 授予中國互聯網絡信息中心 (CNNIC) 研析建立中文域名的可能，並於隨後建立中文域名具體應用規劃；至 2000 年底時，中國大陸境內已可透過中文域名指引至指定網站。⁶⁷ 伴隨著這樣的局勢發展，負責通訊協定規格討論與制定的國際網際網路工程任務組於 2009 年以技術規格 RFC4713 定義非拉丁字母中文域名規範，這樣的趨勢象徵過去由西方主導的網名秩序受到挑戰。⁶⁸ 至 2010 年時，負責網域名稱轉譯服務的網際網路名稱與數字位址分配機構正式發布以中文文字顯示國家和地區頂級域名 (ccTLD) 的支援，並於 2013 年進一步通過以中文文字顯示通用頂級域名 (gTLD) 的功能。⁶⁹ 時至今日，我們已可用「亞馬遜.公司」拜訪 Amazon 中國，「微博.公司」拜訪微博，「BBC.在线」拜訪 BBC 中文網；由於超過四分之一以上的網民位在中國大陸，中國大陸未來不僅可透過中文域名的註冊掌控網站的拜訪轉址，

⁶⁶ Xing Li, "China's First Ipv6-Only Backbone Network to Connect a Further 1,200 Campuses," APNIC, <https://blog.apnic.net/2017/01/31/chinas-first-ipv6-backbone-network-connect-1200-campuses/>. (2020/05/21 查詢)。

⁶⁷ 國家互聯網信息辦公室，〈2000 年～ 2001 年互聯網大事記〉，《國家互聯網信息辦公室》，http://www.cac.gov.cn/2009-04/13/c_126500434.htm (2020/05/21 查詢)。

⁶⁸ 國家互聯網信息辦公室，〈2000 年～ 2001 年互聯網大事記〉，《國家互聯網信息辦公室》，http://www.cac.gov.cn/2009-04/13/c_126500434.htm (2020/05/21 查詢)。

⁶⁹ ICANN, "Delegated Strings," Internet Corporation For Assigned Names and Numbers, <http://newgtlds.icann.org/en/program-status/delegated-strings>.

同時由於域名往往與企業商標相關，因此透過中文域名的註冊及買賣，中國大陸將能獲得另一層次的經濟收益。⁷⁰

最後，中國大陸的網路權力發展也擴展到 4G 及 5G 網通領域技術規格的發展。在 2011 年以前，僅有少部分 4G 專利是屬於中國大陸公司，然屆 2013 年時，中國大陸在全球 4G 專利數量急速增加，並僅次於美國。⁷¹ 由於 5G 技術往往是 4G 技術的延伸，中美之間的技術專利競賽也延伸到 5G 通訊時代，而根據日經新聞於 2019 年 5 月 3 日的統計，中國大陸佔據當前全世界三分之一強的 5G 專利技術，其中，將近一半的專利是由華為所掌控。⁷² 也因此，美國政府首先於 2019 年《國防授權法案》(National Defense Authorization Act) 中明文禁止政府各部門向中國大陸通訊大廠發包任何專案，⁷³ 該法案顯示美國不希望向中國採購電信設備之具體意向。後川普更於 2019 年 5 月以國安顧慮考量禁止美國華為產品，美國國務院更通過將華為等 68 間中國科技公司列入出口管制的實體名單 (Entity List) 管制，中國大陸便因此宣稱將建立其相對應制度反制。⁷⁴ 其後，於 2019 年 11 月，美國聯

⁷⁰ R. Deibert et al., *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (MIT Press, 2011).

⁷¹ 國家實驗研究院, "From Manufacturing to Intellectual Property! The 4g Lte Standard-Essential Patent Databa," National Applied Research Laboratories, <https://www.narlabs.org.tw/en/xmdoc/conf?xsmsid=01160457997407279810&sid=01171806216745679608>.

⁷² Akito Tanaka, "China in Pole Position for 5g Era with a Third of Key Patents," *Nikkei Asian Review*, 3 May 2019.(2020/05/21 查詢)。

⁷³ US Congress, "National Defense Authorization Act for Fiscal Year 2019," (US Congress, 2019).

⁷⁴ 倪浩，〈商務部：中國將建立「不可靠實體清單」制度，具體措施近期出臺〉，《環球網》，<https://world.huanqiu.com/article/9CaKmKkMCF>.

邦通訊委員會 (Federal Communications Commission) 更通過決議將華為列入任何使用聯邦經費所執行之公私採購契約的禁制名單內，⁷⁵ 而美國國會後於 2020 年 3 月亦立法通過《安全可信通信網絡法》(Secure and Trusted Communications Networks Act)，⁷⁶ 藉由對於華為禁令的明確法制化，明確斷絕華為透過法律途徑的任何反制動作。2020 年 5 月美國政府更發布新規，禁止國外供應商使用「美國來源」製造設備及技術提供華為半導體通訊晶片供應，以上各項作為除代表美國不再向中國大陸購買通訊設備，亦不再向其輸出科技。⁷⁷

綜上所論，從美國各項作為觀察發現，在網路空間中，美國似乎認為誰能掌控程式碼誰就擁有權力，也因此誰能透過通訊標準的制定，誰便能在網路空間中制訂「規則」，擁有爭奪數位霸權的墊腳石。

陸、意涵與啟示

透過國際關係權力視角下的理論分析，本文除闡釋如何將現實主義的安全觀，結合源自於國家領土疆界的權力論，透過 OSI 模式對網路空間的概念化，使得本文跨越過去就網路空間不具體

⁷⁵ Carrie Mihalcik, "Fcc Bars Huawei, Zte from Billions in Federal Subsidies," Cnet, <https://www.cnet.com/news/fcc-bars-huawei-zte-from-billions-in-federal-subsidies/>.(2020/05/21 查詢)。

⁷⁶ Shelby Brown, "Trump Signs Law Barring Rural Carriers from Using Huawei Gear," Cnet, <https://www.cnet.com/news/trump-signs-law-barring-rural-carriers-from-using-huawei-gear/>.(2020/05/21 查詢)。

⁷⁷ Davis Bob and Katy Stech Ferek, "U.S. Moves to Cut Off Chip Supplies to Huawei," *Wall Street Journal*, 15 May 2020.

而抽象，對網路權力難以捉摸的印象，轉而提供一個專注在網路權力物質基礎的影響性，並為中美如何爭奪數位霸權的問題，提供一宏觀並具體之解釋分析。以下分就理論、戰略意涵及對我啟示等三方面，分述其影響性。

首先，就網路權力理論的啟發而言，本文一開始所企希發掘的網路權力物質基礎，乃是透過 OSI 網路空間概念模式，藉由依附傳統的權力論框架詮釋網路權力，以瞭解中美雙方所掌控的科技潛能，然而這樣的潛能，最終卻導引出如同葛蘭西的文化霸權般的宰制，代表著可能性的「能量」而非必然性的「能力」。可能性能量根源於雙方所擁有不均衡的物質力量基礎 (Imparity of Power)，雖然這樣的物質基礎不等同必然性的能力，惟若有一方不具任何物質潛能，則代表無「必然性」的可能，也因此就國際行為體 (actor) 潛能的掌握能增加我們對於可能未來的判斷。然而，這樣的計算基礎並不意謂未來學者僅能採行傳統國家力量 (National Power) 的網路權力計量模式。傳統的國家力量計算公式，往往忽略考究多大程度上權力是否可轉換的問題 (fungibility)，⁷⁸ 這正是 Nye 所稱的：即使多花一塊錢在硬實力上的投資，也不代表等同多一塊錢的安全；⁷⁹ 也因此，由於網路硬實力的計量困難，本文對物質力量的網路權力最終僅能達成初步結論，亦即中國大陸網路權力的資源相較過去大幅增加；換言之本文僅能強調中國大陸是崛起的數位強權 (Rising Cyberpower)，

⁷⁸ 張登及，〈習時代中共的「銳權力」戰略？概念構成與理論反思〉，《展望與探索》，第 16 卷第 4 期（2017）。

⁷⁹ Richard L Armitage and Joseph S Nye Jr, "Implementing Smart Power: Setting an Agenda for National Security Reform," *Statement before the Senate Foreign Relations Committee* 24 (2008).

而非新的數位霸權 (Cyber Superpower)。同時，傳統國家權力的增加來自於政、經、軍實力的成長及國際社會對這樣發展現象的認可；⁸⁰ 所以當中國大陸的可能性能量受到美國「認可」後並執行制裁，即便網路能量無法像軍事戰機及潛艇般具體量化，亦或網路攻擊仍具有可匿名的特性，都無礙美國政府認知到中國大陸爭奪數位霸權的判斷。然而這樣的初步觀察，卻同時引導出權力的理性化或建構化間意識的拉扯，也因此未來學者可以進一步針對「必然性」的理性計量與「可能性」的權力建構進行思辨，俾持續深化此兩種途徑的異同，豐富網路權力的研究核心。

其次，就戰略意涵的啟發而言，中國大陸已非過去般僅聚焦於境內防禦，並轉而顯露其爭奪數位霸權的意圖。首先中國大陸除自 2014 年起由習近平成立「中央網絡安全和信息化領導小組」，次年更於中國大陸浙江烏鎮所召開的第二屆「世界互聯網大會」中，習近平更提出從「網路大國」邁向「網路強國」的願景。⁸¹ 而其後於 2016 年的《國家網絡空間安全戰略》，更提出達成建設「與國際地位相稱」的網路力量。⁸² 2017 年於第一屆「一帶一路國際合作高峰論壇」時更由習近平提出建立「數字絲綢之路」(Digital Silk Road) 目標。⁸³ 時至今日，中國大陸於數位

⁸⁰ Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (University of Georgia Press, 2011), 283.

⁸¹ 新華網，〈習近平：把我國從網路大國建設成為網路強國〉，《新華網》，2014 年 2 月 27 日。

⁸² 國家互聯網信息辦公室，〈國家網絡空間安全戰略全文〉，《國家互聯網信息辦公室》，http://www.cac.gov.cn/2016-12/27/c_1120195926.htm。

⁸³ Hong Shen, "Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative," *International Journal of Communication* 12 (2018).

霸權的爭奪已取的具體進展，並擁有眾多取代西方主導秩序的替代機制。例如：當西方國家使用 Google 搜索網路資料時，中國大陸卻使用百度；當別人使用 Youtube 分享影片時，中國大陸使用優酷；中國大陸的騰訊及新浪取代 Twitter；人人及開心網取代 Facebook；中國大陸人民使用支付寶而不是 Paypal，用淘寶而不是 ebay 作網購；中國大陸支持國內外市場使用聯想電腦，數據網路可以使用華為或中興設備。換言之，中國大陸許多作為已超越傳統聚焦於境內防禦需求，當其全力發展支援不同 OSI 階層服務的軟硬體供應商時，不但可以立足國內市場，亦可積極透過一帶一路及政府支持的國際發展援助計畫立足海外市場並拓展國際影響力。傳統現實主義安全觀認為，當一個國家因為內生原因 (Endogenous Reason) 改變時 (如：安全、經濟或意識形態)，其後的權力轉移的產生將造成世界秩序的不穩固。⁸⁴ 換言之，當身為我國最大威脅的中國大陸網路權力不斷增長，加之其爭奪數位霸權意圖明顯，這樣的發展不僅之於美國，對於我國未來網路安全也造成衝擊。

最後，就對我國之啟示而言，呼應蔡總統「資安即國安」指導，⁸⁵ 我國雖於 2016 年於行政院成立資通安全處強化網路防禦能力，後於 2017 年由國防部成立資通電軍增進攻勢能力，並於

⁸⁴ 吳玉山，《抗衡或扞從：兩岸關係新詮 -- 從前蘇聯看臺灣與中國大陸間的關係》(台北：正中書局，1997)。

⁸⁵ 總統府，〈國家資通安全戰略報告 - 資安即國安〉，《總統府》，<https://www.president.gov.tw/Page/317/969/%E5%9C%8B%E5%AE%B6%E8%B3%87%E9%80%9A%E5%AE%89%E5%85%A8%E6%88%B0%E7%95%A5%E5%A0%B1%E5%91%8A-%E8%B3%87%E5%AE%89%E5%8D%B3%E5%9C%8B%E5%AE%89>。(2020/05/21 查詢)。

2018 年通過「資通安全管理法」來強化法治作為，期望藉由公私部門的合作來捍衛數位國土。⁸⁶ 然誠如 2019 年國防報告書所述，目前國軍的戰略目標是「防衛固守、重層嚇阻」，⁸⁷ 並希望透過「建立可恃的網路攻防戰力」，⁸⁸ 來成為重層嚇阻戰略下的「第一層嚇阻兵力」。⁸⁹ 然嚇阻戰略主要內涵是心理性的，須透過傳達 (Communicate) 可信 (Credible) 能力 (Capability) 來改變敵人的威脅評估，使其心理上認知對我之軍事行為未來可能受到我軍之反制而付出極高成本，由於預期獲利可能降低而因而勸阻敵輕啟戰端之意願，故成功的嚇阻戰略需包含傳達、可恃及能力等三要素。⁹⁰ 然反觀我國目前之網路安全嚇阻作為，雖透過公開政策文件宣示及媒體傳播來向中國大陸「傳達」我軍之企圖，並透過組織、人才及法律面向整合，來呈現「能力」之要素，惟現行仍缺少「可信」的呈現，依據權力理論的論述，勢將阻礙整體「嚇阻」戰略心理層面的效應。就如同美國之所以「認可」中國大陸上升中的網路權力般，我國網路嚇阻戰略的成功與否，在於中國大陸能否「認可」我國的網路戰力，也因此未來政府應考量適度呈現「可信的網路攻防戰力」，這除可透過網路攻防搶旗賽 (Catch the Flag) 的執行來公開呈現網路能量，後續若能透過適度的攻防演練，以實際

⁸⁶ 行政院國家資通安全會報，〈資通安全管理法 (總統令公告 107 年 6 月 6 日)〉，《行政院國家資通安全會報》，<https://nicst ey.gov.tw/Page/D94EC6EDE9B10E15/e0650fa1-3527-42e8-8078-3146c35b8409>。(2020/05/21 查詢)。

⁸⁷ 國防部，《中華民國 108 年國防報告書》，台北：國防部，2019 年，頁 6

⁸⁸ 《中華民國 108 年國防報告書》，頁 6。

⁸⁹ 立法院，《立法院公報第 106 卷第 74 期》，台北：立法院，2017 年，頁 211

⁹⁰ P.M. Morgan, *Deterrence Now* (Cambridge, UK: Cambridge University Press, 2003), 59.

資訊戰力呈現資訊系統破壞，方能有效改變共軍對我資訊能量之心理認知，震懾敵不法意圖，並真正成為第一層的嚇阻兵力。

柒、結論

本研究兼具學理與政策面之意涵。在學理上屬國際關係安全領域研究，藉由導入網路安全研究文獻及國際關係權力概念的論述，使網路安全研究具備理論基礎，同時豐富傳統國際關係領域權力論述的案例分析，而引用西方理論檢視網路空間的兩岸互動，也提供一新跨科際交流的場域。而在政策上，本文論述成果也有助提供一新視角瞭解與評估美中網路權力互動，特別是迄今未有「數位珍珠港」⁹¹發生，也因此過去採哥本哈根學派途徑的學者多認為網路攻擊是部份政府官員、媒體及學者的「語言行動」(Speech Act)，⁹²並透過話語建構 (Discursive Construction) 出「恐懼」的概念影響安全。是故，透過本文利用中美數位霸權競奪案例，對網路權力的理論分析提出一物質基礎的可能選擇途徑，並主張我國須採取必要措施，回應世界局勢網路權力變化，除對我國發展網路安全戰力的其必要性做出說明，使各項施政有所依據，並為如何維繫我國網路安全，提供更適切之建議。

(收稿：2020 年 3 月 18 日；第一次修正：2020 年 5 月 21 日；
接受：2020 年 7 月 14 日)

⁹¹ Singer and Friedman, 68.

⁹² 如學者 Myriam Dunn Cavelty 依據英國分析語言學家 John Austin 的語言行動理論，論證美國網路威脅的根源來自語言。請見 M. D. Cavelty, "Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the Us Cyber-Threat Debate," *Journal of Information Technology & Politics* 4, no. 1 (2008): 19-36.

參考資料

一、中文部分

(一) 期刊論文

張登及，〈習時代中共的「銳權力」戰略？概念構成與理論反思〉，

《展望與探索》第 16 卷，第 4 期 (2017 年) 頁 119-33。

林穎佑，〈中國近期網路作為探討：從控制到攻擊〉，《臺灣國際研究季刊》第 12 卷，第 3 期 (2016 年) 頁 51-68。

蔡裕明，〈資訊性民族主義 -Linux 對中國大陸的意義〉，《中國大陸研究》第 44 卷，第 12 期 (2001 年): 頁 21-36。

鍾兆真、蕭全政，〈美國的網際霸權：網路層，傳輸層與應用層的政治經濟分析〉，《台灣社會研究季刊》，第 18 期 (2007 年) 頁 297-344。

(二) 專書論文

吳玉山，1997，《抗衡或扈從：兩岸關係新詮 -- 從前蘇聯看臺灣與中國大陸間的關係》，台北：正中書局。

林中斌，1999 年，《核霸：透視跨世紀中共戰略武力》，臺灣學生書局。

趙坤茂、張雅惠、黃俊穎、黃寶萱，2019 年，《計算機概論：當代資訊通鑑 (第 14 版)》，全華圖書。

Clarke, Richard A, and Robert K Knake. 2014 年，《網路戰爭：下一個國安威脅及因應之道》，國防部史政編譯室編譯處。

Friedman, Thomas. 2005 年，《世界是平的：一部二十一世紀簡史》，台北：雅言文化出版股份有限公司。

（三）學位論文

張憶嬋，2006 年，《開放原始碼軟體商業模式及相關法律問題之探討》。國立政治大學智慧財產研究所。

（四）官方文件

中國互聯網路信息中心，2016 年，《中國互聯網路發展狀況統計報告》。北京：中國互聯網路信息中心。

國防部，2019 年，《中華民國 108 年國防報告書》，台北：國防部。

立法院，2015 年，《立法院公報第 104 卷第 23 期》，台北：立法院。

立法院，2017 年，《立法院公報第 106 卷第 74 期》，台北：立法院。

（五）網際網路

倪浩，〈商務部：中國將建立“不可靠實體清單”制度，具體措施近期出臺〉，《環球網》，<https://world.huanqiu.com/article/9CaKrnKkMCF>. (2020/05/21 查詢)

國家互聯網信息辦公室，〈2000 年～2001 年互聯網大事記〉，《國家互聯網信息辦公室》，http://www.cac.gov.cn/2009-04/13/c_126500434.htm. (2020/05/21 查詢)

——〈2006 年中國互聯網發展大事記〉，《國家互聯網信息辦公室》，http://www.cac.gov.cn/2014-02/24/c_126182771.htm. (2020/05/21 查詢)

——〈國家網路空間安全戰略全文〉，《國家互聯網信息辦

公室》，http://www.cac.gov.cn/2016-12/27/c_1120195926.htm.
(2020/05/21 查詢)

國家實驗研究院．“From Manufacturing to Intellectual Property! The 4g Lte Standard-Essential Patent Databa.” National Applied Research Laboratories, <https://www.narlabs.org.tw/en/xmdoc/cont?xsmsid=0I160457997407279810&sid=0I171806216745679608>. (2020/05/21 查詢)

新華網，〈習近平：把我國從網路大國建設成為網路強國〉，《新華網》，2014 年 2 月 27 日。

總統府，〈國家資通安全戰略報告 - 資安即國安〉，《總統府》，<https://www.president.gov.tw/Page/317/969/%E5%9C%8B%E5%AE%B6%E8%B3%87%E9%80%9A%E5%AE%89%E5%85%A8%E6%88%B0%E7%95%A5%E5%A0%B1%E5%91%8A-%E8%B3%87%E5%AE%89%E5%8D%B3%E5%9C%8B%E5%AE%89->. (2020/05/21 查詢)

行政院國家資通安全會報，〈資通安全管理法 (總統令公告 107 年 6 月 6 日)〉，《行政院國家資通安全會報》，<https://nicst ey.gov.tw/Page/D94EC6EDE9B10E15/e0650fa1-3527-42e8-8078-3146c35b8409>. (2020/05/21 查詢)

陳曉莉，〈美國人事管理局遭網路攻擊，400 萬公務員資料外洩，疑是中國所為〉，《iThome》，<https://www.ithome.com.tw/news/96493>. (2020/05/21 查詢)

二、英文部分

(一) 期刊論文

- Bolt, Paul J., and Carl N. Brenner. "Information Warfare across the Taiwan Strait." *Journal of Contemporary China* Vol. 13, No. 38 (2004/02/01 2004): 129-50.
- Bucci, Steven, P. "A Most Dangerous Link." *US Naval Institute Proceedings* , Vol. 135, No. 10 (2009): 38-42.
- Cavelty, M. D. "Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the Us Cyber-Threat Debate." *Journal of Information Technology & Politics* , Vol. 4, No. 1 (2008): 19-36.
- Dartnell, Michael. "Weapons of Mass Instruction: Web Activism and the Transformation of Global Security." *Millennium* , Vol. 32, No. 3 (2003): 477-99.
- Der Derian, James. "The Question of Information Technology in International Relations." *Millennium* , Vol. 32, No. 3 (2003): 441-56.
- Eriksson, Johan, and Giampiero Giacomello. "The Information Revolution, Security, and International Relations: (Ir) Relevant Theory?". *International political science review* , Vol. 27, No. 3 (2006): 221-44.
- Goldman, Emily O. "Introduction: Information Resources and Military Performance." *Journal of Strategic Studies* , Vol. 27, No. 3 (2004): 195-219.
- Greenemeier, Larry. "Estonian Attacks Raise Concern over Cyber 'Nuclear Winter'." *Information Week*, May 24 (2007).

- Hansen, Lene, and Helen Nissenbaum. "Digital Disaster, Cyber Security, and the Copenhagen School." *International studies quarterly* , Vol. 53, No. 4 (2009): 1155-75.
- Hsiao, Russell. "Critical Node: Taiwan's Cyber Defense and Chinese Cyber-Espionage." *China Brief* , Vol. 13, No. 24 (5 December 2013).
- Hwang, Ji-Jen [黃基禎]. "China's Military Reform: The Strategic Support Force, Non-Traditional Warfare, and the Impact on Cross-Strait Security." *Issues & Studies* , Vol. 53, No. 3 (2017): 1750008.
- . "Chinas Cyber Strategy: A Taiwanese Perspective." *Korean journal of defense analysis* , Vol. 29, No. 1 (2017): 95-111.
- Kreisher, Otto. "Risk to One Is Risk to All." *Sea Power* , Vol. 50, No. 12 (December 2007): 3.
- Liff, Adam P. "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* , Vol. 35, No. 3 (2012): 401-28.
- Newmyer, Jacqueline. "The Revolution in Military Affairs with Chinese Characteristics." *The Journal of Strategic Studies* , Vol. 33, No. 4 (2010): 483-504.
- Rawnsley, Gary D. "Old Wine in New Bottles: China-Taiwan Computer-Based 'Information Warfare' and Propaganda." *International Affairs* , Vol. 81, No. 5 (2005): 1061-78.
- Shen, Hong. "Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative." *International Journal of Communication* , Vol. 12 (2018): 19.
- Yau, Hon-min [姚宏旻]. "A Critical Strategy for Taiwan's Cyber-

security: A Perspective from Critical Security Studies.” *Journal of Cyber Policy* (2019): 1-21.

———. “Explaining Taiwan’s Cybersecurity Policy Prior to 2016: Effects of Norms and Identities.” *Issues & Studies* , Vol. 54, No. 2 (2018): 1-30.

(二) 專書論文

Abbate, J. 2000. *Inventing the Internet*. MA, US: MIT Press.

Baezner, Marie. April 2018. “Cybersecurity in Sino-American Relations.” *CSS Analyses in Security Policy*.

Betz, D.J., and T. Stevens. 2011. *Cyberspace and the State: Toward a Strategy for Cyber-Power*. Edited by International Institute for Strategic Studies Oxford, UK: Routledge.

Carr, Madeline. 2016. *Us Power and the Internet in International Relations: The Irony of the Information Age*. Hampshire, UK: Palgrave Macmillan.

Castells, Manuel. 1996. *The Rise of the Network Society*. Blackwell Publisher.

Cavelty, M.D. 2007. *Cyber-Security and Threat Politics: Us Efforts to Secure the Information Age*. Oxford, UK: Taylor & Francis.

Choucri, Nazli. 2012. *Cyberpolitics in International Relations*. MIT Press.

Chu, M.M., and S.L. Kastner. 2014. *Globalization and Security Relations across the Taiwan Strait: In the Shadow of China*. Taylor & Francis.

Clark, C. 2011. *The Changing Dynamics of the Relations among*

China, Taiwan, and the United States. Newcastle upon Tyne, UK: Cambridge Scholars Publisher.

Deibert, R., J. Palfrey, R. Rohozinski, and J. Zittrain. 2011. *Access Contested: Security, Identity, and Resistance in Asian Cyberspace.* MIT Press.

Demchak, Chris C. 2011. *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security.* University of Georgia Press.

Goverde, Henri, and Howard H Lentner. 2000. *Power in Contemporary Politics: Theories, Practices, Globalizations.* Sage.

Gray, Colin S. *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling.* Pennsylvania, U.S.: Strategic Studies Institute, US Army War College, 2013.

Jordan, T. 2002. *Cyberpower: An Introduction to the Politics of Cyberspace.* Oxford, UK: Taylor & Francis.

Kramer, Franklin D, Stuart H Starr, and Larry K Wentz. 2009. *Cyberpower and National Security.* Washington, DC, US: Potomac Books, Inc.

(三) 網際網路

Armitage, Richard L, and Joseph S Nye Jr. “Implementing Smart Power: Setting an Agenda for National Security Reform.” *Statement before the Senate Foreign Relations Committee* 24 (2008). <https://www.csis.org/analysis/implementing-smart-power-setting-agenda-national-security-reform>

Department of Justice. “U.S. Charges Five Chinese Military Hackers for Cyber Espionage against U.S. Corporations and a La-

bor Organization for Commercial Advantage.” Department of Justice, <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>.

Google. “關於谷歌中國的最新聲明.” Google, <https://www.google.cn/press/new-approach-to-china/update.html>.

ICANN. “Delegated Strings.” Internet Corporation For Assigned Names and Numbers, <http://newgtlds.icann.org/en/program-status/delegated-strings>.

Yau, Hon-min. “Handle with Care: The Pandora’s Box of Cyber Attacks.” Thinking Taiwan, <http://thinking-taiwan.com/thinking-taiwan.com/handle-with-care-pandoras-box-cyber-attacks/index.html>.

(四) 報紙

Broad, William J., and David E Sanger. “U.S. Strategy to Hobble North Korea Was Hidden in Plain Sight.” *New York Times*, 14 March 2017.

China Post. “Cabinet Forms Department for Cyber Security.” *China Post*, 2 August 2016.

Gold, Michael, and J.R Wu. “Taiwan Seeks Stronger Cyber Security Ties with U.S. To Counter China Threat.” *Reuters*, 30 May 2015.

Jing, Meng. “Will Trump’s Assault on Huawei Create a Digital Iron Curtain?” *South China Morning Post*, 26 May 2019.

Kremer, Jan-Frederik, and Benedikt Müller. *Cyberspace and International Relations*. London, UK: Springer, 2014.

- Lessig, L. *Code: And Other Laws of Cyberspace, Version 2.0*. New York, US: Basic Books, 2008.
- Li, Xing. "China's First Ipv6-Only Backbone Network to Connect a Further 1,200 Campuses." APNIC, <https://blog.apnic.net/2017/01/31/chinas-first-ipv6-backbone-network-connect-1200-campuses/>.
- Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22, no. 3 (2013): 365-404.
- Microsoft. "Announcing Windows 10 China Government Edition and the New Surface Pro." Microsoft, <https://blogs.windows.com/windowsexperience/2017/05/23/announcing-windows-10-china-government-edition-new-surface-pro/>.
- MOFA. "Ministry of National Defense Launches New Cybersecurity Command." Taiwan Today, <https://taiwantoday.tw/news.php?unit=2,6,10,15,18&post=117794>.
- Morgan, P.M. *Deterrence Now*. Cambridge, UK: Cambridge University Press, 2003.
- Morgenthau, Hans J., and Kenneth W. Thompson. *Politics among Nations : The Struggle for Power and Peace*. 7th ed. Maidenhead: McGraw-Hill Education, 2005.
- Morozov, Evgeny. "Cyber-Scare: The Exaggerated Fears over Digital Warfare." *Boston Review* 34, no. 4 (2009): 17-20.
- Mueller, Milton L. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. MIT Press, 2009.
- Northrop Grumman. *Understanding Voice and Data Link Networking*. CA, US: Northrop Grumman, 2014.
- Nye Jr, Joseph S. "Cyber Power." MA, US: Belfer Center for Sci-

- ence and International Affairs, 2010.
- . *The Future of Power*. PublicAffairs, 2011.
- Parsons, Talcott. *The Theory of Social and Economic Organization*. New York: Free Press; London: Collier Macmillan, 1964.
- Schneier, B. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York, US: W. W. Norton, 2015.
- Singer, P.W., and A. Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know?* Oxford, UK: Oxford University Press, 2014.
- Standage, T. *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's on-Line Pioneers*. Bloomsbury USA, 2014.
- Tanaka, Akito. "China in Pole Position for 5g Era with a Third of Key Patents." *Nikkei Asian Review*, 3 May 2019.
- Thim, Michal. "Taiwan's Invisible Frontier: Cyberspace." Thinking Taiwan Foundation, <http://thinking-taiwan.com/taiwans-invisible-frontier-cyberspace/>.
- Tibken, Shara. "No, 5g Isn't Going to Make Your 4g Lte Phone Obsolete." cnet, <https://www.cnet.com/news/no-5g-isnt-going-to-make-your-4g-lte-phone-obsolete/>.
- Zetter, K. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York, US: Crow Publishing Group, 2014.