全球政治評論　*Review of Global Politics*

第六十六期（2019）No.66 頁 27-56

學術論文

對抗或是對話？ AI 未來發展的挑戰與契機

Confrontation or Dialogue? The Challenges and Opportunities for AI's Future Development

杜長青 *Chang-Ching Du*
國防大學戰略與國際事務研究所助理教授
Assistant Professor of Graduate Institute of Strategic Studies
National Defense University

摘要 / Abstract

本文以美國官方已進入政府制度議程的人工智慧（Artificial Intelligence, AI）相關文件作為「國內層次」之分析文本，進行安全化的論述分析；分析單元部分，分別以「國家利益」、「國家安全」、「威脅來源」等字句類別，重新解析官方文本中的關鍵詞與重要概念，協助理解安全化語言的表述方式，以及倡議的對象與政策所望目標為何；至於在安全化論述的效果與影響上，則選取「國際層次」中與美國友好的國家，例如德法日等國對於美國官方文件中建構的 AI 安全化論述之反應，以了解區域其他國家是否在互動中肯認這樣的威脅觀點，進入區域安全複合體的合作架構並承擔相對的風險。

研究發現上述文本或政治菁英中所討論的安全化（Securitization）架

構，其「語言－行動」之論述建構順序為：美國政府資助包含「AI 等 STEM（Science, Technology, Engineering, and Mathematics, STEM）新興技術發展」、強調「技術突破以取得美國軍事、經濟和資訊優勢」、維持「美國本土防衛與國家安全」、以「確保美國國家利益」；而在 AI 議題倡導的角色上，前文分析可以發現已由早期的私人或民間企業自主性發展，透過美國國會「未來人工智慧法案」、總統行政辦公室「川普政府第一年科技政策重點」等官方文件，國家角色快速崛起，除了明確定位為國家戰略，並以政策工具來落實；此外，為了使其他國家認同這樣的安全化論述，並與美國形成安全聯盟，則進一步以中國經濟發展威脅作為載點，於文本中建構「中國傾其全力，積極獲取關鍵科技、智慧財產與發展新興高科技產業，以促進未來國家經濟發展及國防產業升級」、「世界各國（含美國）都是其目標，將威脅各國國家安全與利益」、「各國應與美國偕同一致加強合作，並積極防範中國的威脅」的論述。

This article uses the US official documents of artificial intelligence(AI) as the “domestic level” content to analyze the constructive process of “Securitization” discourse; The analysis units are divided into “national interest,” “national security,” and “the source of threats”, to re-analyze the key words and important concepts in the official text, can help us to understand the way in which the sentence is expressed, and the object it desire to obtain in the very beginning; as for the outside effect of the “Securitization” discourse, the article select the American’ allies as the “international level” units, such as Germany, France and Japan, to observer their policy stance and national attitude toward China’s AI threats which was built by the US. It can help us to understand whether other countries in the region are willing to recognize such threats and step into the “regional security complex” and sharing relative risks with the US.

This study found that the “Securitization” discourse has been constructed

in the following order: US government to fund “the STEM (Science, Technology, Engineering, and Mathematics, STEM) ” technology”; to maintain its “military, economic and information advantages” from technological breakthroughs; to ensure US national security and national interests. In the role of advocator for AI issues, the early position of private enterprises has been taken rapidly by the rise of the country, and the level has been clearly defined as “National Strategy”. Furthermore, in order to gain the like-minded recognition form other allies, the US further to post these threatening perspectives: “The aim of China’s full efforts to actively acquire key technologies, intellectual property and develop emerging high-tech industry, is to promote its national economy and to upgrade national defense industry”; besides, China’s rising will erode other countries interests and threat their national security; hence, all partners should strengthen the cooperation with the US, and actively prevent the threat from China.

關鍵字：安全化、人工智慧、AI 民族主義

Keywords: Securitization, Artificial Intelligence, AI Nationalism

壹、前言

「人工智慧 （Artificial Intelligence, AI）」自 1956 年於美國達特茅斯（Dartmouth）一場研討會被提出後，[1]會議中「計算機、自然語言處理、神經網絡、計算理論、抽象化與隨機創造」等議題後來都成為人工智慧研究發展的重要領域。早期 AI 發展以數理邏輯技術為基礎，約莫十年前，國際關係與外交學界關注的「AI 科技發展焦點」，著重於網際網路對於國際事務的影響，隨著智慧型手機與新興社群媒體 Facebook 或 twitter 出現打破了傳統疆界，數位資訊即時的連結加速各種社會議題傳遞，也間接催生了阿拉伯之春（Arab Spring）與維基解密（Wikileaks）的社會和政治運動；而震網病毒（Stuxnet）更成為網路軍備競賽的原型武器，這些當時的劃時代先進技術對於當代政治產生極大影響。

時序拉回到 2019 年， AI 歷經了 60 多年的發展，包含超級計算機、無人機、虛擬助手、3D 列印、可穿戴傳感器（Wearable Sensors）等等 AI 產品的應用在我們生活日常中已經十分普及，隨著領域中深度學習（Deep Learning）、巨量數據運作以及自然語言處理（Natural Language Processing, NLP）等技術的突破，人工智慧分辨率隨資料質與量逐步提升，逐步由模擬人類思維與行為表現的「弱人工智慧」（Weak AI）、打造人工神經網絡（Artificial Neuron Network），邁向「強人工智慧」（Strong AI）的目標；[2]而 DNA 測序（DNA sequencing）、奈米科技（nanotechnologies）、量

---

[1] 人工智慧一詞在美國新罕布夏州 1956 年一場為期兩個月的研究工作坊「達特茅斯暑期人工智慧研究計畫（The Dartmouth Summer Research Project on Artificial Intelligence）」上，由負責組織會議的電腦高階語言 LISP 學者約翰・麥卡錫（John McCarthy）正式定名。這場工作坊所討論的問題：「計算機、自然語言處理、神經網絡、計算理論、抽象化與隨機創造」後來都成為人工智慧研究發展的重要領域，而達特茅斯會議也因此成為人工智慧領域的經典起源。請參閱數位時代，〈完全解讀：人工智慧新商業〉一文。*https://www.bnext.com.tw/article/41534/3-key-techniques-of-ai*。

[2] 隨著 AI 的逐步發展，不同領域的專家也開始思考 AI 的角色與定位，而加州大學哲學系教授約翰・賽爾（John R. Searle）提出了「弱人工智慧」（Weak or cautious AI）與「強人

子電腦（Quantum Computer）這些與 AI 相關之新興技術性突破及其於跨領域的廣泛融合運用，是促使當前世界正在進行的第四次工業革命（4th Industrial Revolution）本質徹底改變的重要關鍵。[3]

西方的文藝復興和工業革命提高科技發展的驅動力，對人類文明發展產生了重大的意義與衝擊，而人工智慧中機器學習的發展方向，是在設計、分析一些讓電腦可以自動深度學習的演算法，從大量的資料中找出規律與建立規則來，並利用這些規則對還沒有進行分析的未知資料進行預測。與其他領域新興技術或顛覆性發展一樣，AI 資訊技術革命將會直接（如整體國力或政經潛力提升）或間接（如新型態武器發展或通信技術突破）影響或重塑國際間國家權力的空間分布，也對國際關係與外交政策產生了另一種層次的論證挑戰，而本文重點在於探討 AI 領域的技術創新對於國際關係與外交政策研究領域的趨勢與影響，[4]並將人工智慧（Artificial Intelligence, AI）定義為廣義且包含大數據、物聯網（Internet of Things, IoT），以及為了創造人工智慧、研究智慧領域之科學技術（Science, Technology, Engineering, and Mathematics, STEM）。

此外，由於目前全球人工智慧主戰場主要分布於中、美、日、歐洲以及其它少部分國家地區，其中美國人工智慧長期穩居全球範圍內 AI 產業發展的核心地位。根據研究報告，美國 AI 研究機構數量和學者數量在全

工智慧」（Strong AI）的兩種不同類別，所謂「弱人工智慧」，意指電腦運算是用來驗證程式與嚴謹假設的技術工具；而「強人工智慧」，則指電腦已經具備理解其他認知狀態，程序運算本身就是解釋。John R. Searle, “Minds, brains, and programs,” *Behavioral and Brain Sciences*, Vol. 3, No. 3(1980), pp. 417-457.

[3] Klaus Schwab, *The Fourth Industrial Revolution* (New York, USA: Crown Publishing Group, 2017), pp. 6-8.

[4] 關於科技創新對於國際關係領域影響的相關研究有很多，切入的觀點各殊。例如部分論文探討 AI 對於國家政治菁英於決策和國際事務中可能發揮的作用與影響（例如透過分析性、預測性和可操作性人工智能工具，協助決策者於危機時做出高品質的決策等），亦有探討文獻報告集中於探討人工智慧將可能造成的失業、倫理與國家安全等課題。Scott, Ben and Heumann, Stefan and Lorenz, Philippe, “Artificial Intelligence and Foreign Policy,” *Stiftung Neue Verantwortung Policy Brief*, January, 2018, *https://ssrn.com/abstract=3103961*.

球占比接近一半，推估美國目前在此領域的領先地位將持續至 2023 年，而亞洲地區中國未來發展也將佔據更多市場。[5]為了確保全球領先地位，美國科技政策辦公室（Science and Technology Policy）於 2019 年 2 月公布了「美國人工智慧倡議」（American AI Initiative），通過重新分配資金，創造新資源，以確保美國 AI 產業發展優勢。[6]因此本文以美國 AI 政策發展為例，另採用安全研究領域中哥本哈根學派「安全化（Securitization）」觀點，以美國官方對於 AI 相關產業發展的論述，來分析原屬於經濟層面 AI 關鍵技術發展與創新，對於國際關係領域產生的衝擊與影響。

貳、分析架構

安全研究自 1950 年代中期以來，一直是國際關係學科中重要的研究領域，冷戰結束後，以 Barry Buzan、Ole Waever、Jaap de Wilde 等學者所屬的哥本哈根學派（Copenhagen School），與哥本哈根衝突與安全研究中心（Conflict and Peace Research Institute, COPRI）的研究者，提出了「安全化（Securitization）」與「去安全化（Desecuritization）」概念，保存了「安全-生存」的邏輯，並以軍事、環境、經濟、社會與政治五大類的分析路徑，拓展與深化了安全研究的領域，[7]讓安全研究的焦點由傳統的國家中心主義，擴展至個人與全球領域。

在重新定義與拓展安全概念後，哥本哈根學派發展出對安全系統進行

---

[5] WiseGuy Reports, "*Global Artificial Intelligence Market 2018 by Manufacturers, Countries, Type and Application, Forecast to 2023*," (November 5, 2018), *https://www.wiseguyreports.com/reports/3510457-global-artificial-intelligence-in-the-education-sector-market.*

[6] MIT technology Review, "*Trump has a plan to keep America first in artificial intelligence*," (February 10, 2019), *https://www.technologyreview.com/s/612926/trump-will-sign-an-executive-order-to-put-america-first-in-artificial-intelligence/.*

[7] 柯林斯等著，《當代安全研究》（中國北京：世界知識出版社，2016 年），頁 197-198。

分析的框架，主張安全是一種建構出來的社會建構過程，而「安全化（Securitization）」被視為一種強烈的「政治化（Politicization）」描述。簡單來說，議題安全化過程運用「言論-行動（Speech Act）」來說服具體的受眾接受威脅的存在，安全化的建構是「相互主體間及與社會有關地（intersubjective and socially）」，亦即一個行為主體適應其他行為主體對某種威脅的認知，而形塑國際體系內的安全互動。[8]此過程共區分兩個階段，第一，議題先由具有挑選與框架議題權力的「安全行為體（Securitizing Actors）」來界定，雖然安全化理論認為任何人都可以成為安全化的行為體，但實踐中最常見的多為政府、政治菁英、官僚機構、軍隊或說客（Lobbyists）和壓力團體等，可以將安全領域中軍事、環境、經濟、社會與政治的「參照對象（Referent Objects）」之威脅不斷提升與擴張，描繪為對參照對象的嚴重安全挑戰；[9]其次，建構及框架出對參照對象的威脅後，政府、政治菁英這些安全行為體必須說服其他領域的相關受眾（如公共意見、政治家或其他菁英）也感受及認同這樣的急迫性安全威脅。而在回應威脅存在的性質時，政府、政治菁英等行為體常會採取超越一般政治常規的緊急手段來因應，[10]濫用極端政治化形式來實現政治目標，例如宣布戒嚴或不經過國會等監督機關的表決而逕行發布緊急命令等。因此，安全化行動的成功或失敗，取決於文本的說服力。以下為哥本哈根學派「安全化行動」階段圖：

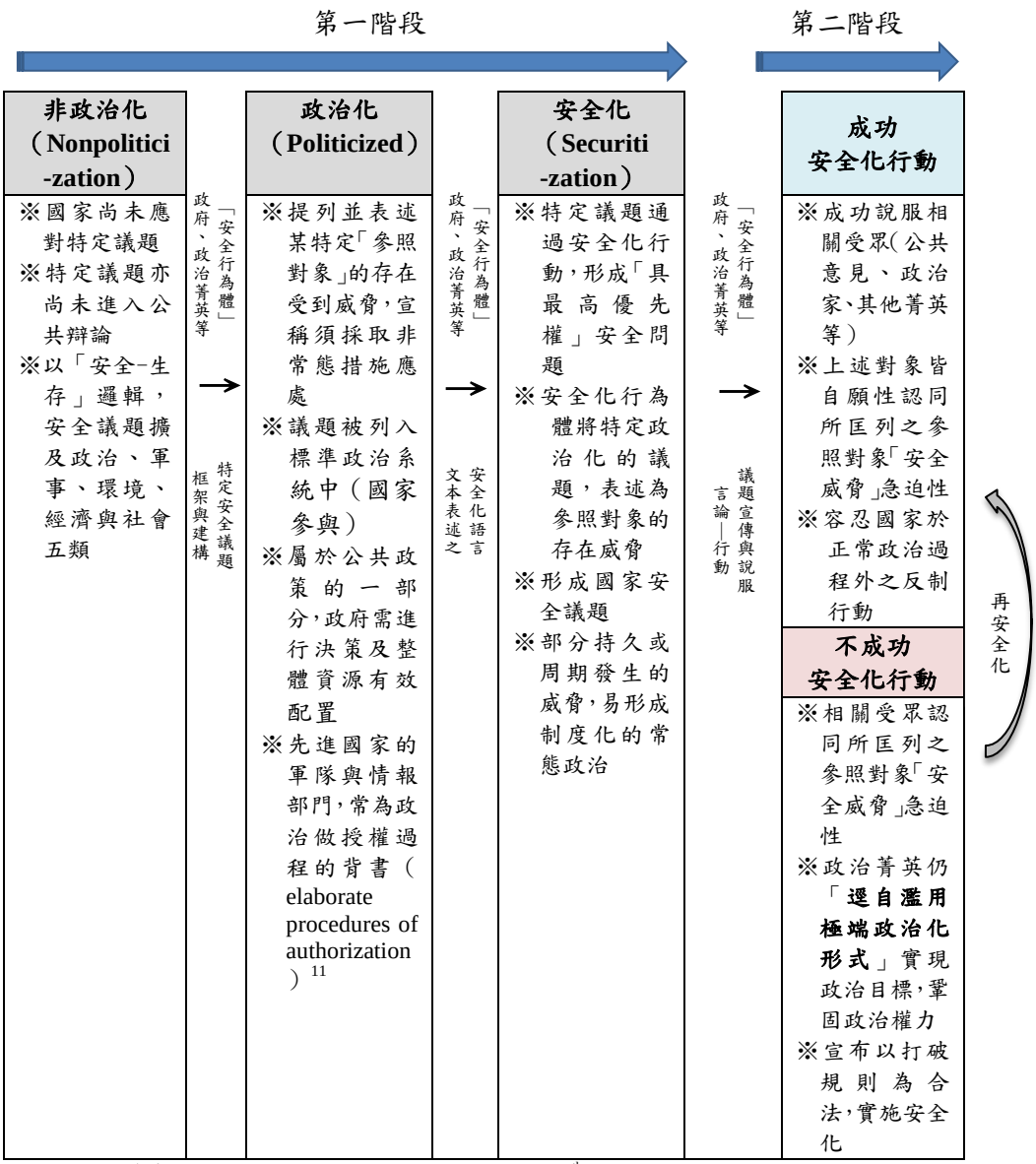
---

8 Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (USA: Lynne Rienner Publishers, 1998), pp. 23-31.

9 Ibid, p. 214.

10 柯林斯等著，《當代安全研究》（中國北京：世界知識出版社，2016 年），頁 199-201。

圖 1：哥本哈根學派「安全化行動」階段



資料來源：參考 Alan Collins, *Contemporary Security Studies*(4th edition)(USA: Oxford University Press, 2016), p.170 圖；以及 Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis*(USA: Lynne Rienner Publishers, 1998), pp. 27-28 等內容綜整繪製而成。

[11] Barry Buzan, Ole Wæver, and Jaap de Wilde, *Security: A New Framework for Analysis* (USA: Lynne Rienner Publishers, 1998), pp. 27-28.

其次，哥本哈根學派跨越國家層次，另提出開放性安全複合體（Opening Security Complex Theory）概念，指涉區域內一定範圍的國家或非國家（如民族、跨國企業）等單元或次團體，因某種相互依存的關係，形成特殊領域間類型相似的「同質性複合體（Homogeneous Complex）」，或跨越多個領域產生互動的「異質性複合體（Heterogeneous Complex）」，此種安全複合體形成的動力與結構，是由複合體內單元安全認識的互動而產生，當然，議題本身的屬性是客觀的，但單元內部或外部政治安全格局安全化論述會拓展實際的範圍，也必須特別注意。[12]

在重新審視安全化的概念後，為了理解經濟層面的議題中，AI 產業未來發展與國際關係領域的互動及可能影響，本文綜合上述論點，在安全的指涉對象上，初步先以「國家」為單元，以美國官方相關文件作為「國內層次」之分析文本，這些文本包括美國前總統歐巴馬時期的總統執行辦公室（Executive Office of the President）2016 年所公布的報告-「未來人工智慧整備（Preparing for the future of artificial intelligence）」，[13]以及現任川普總統任內所公布的 2017 年《美國國家安全戰略（National Security Strategy）》、美國國會 2017 年－「未來人工智慧法案（FUTURE of Artificial Intelligence Act of 2017）」、[14]美國貿易與製造業政策辦公室 2018 年報告－「中國的經濟侵略如何威脅美國和世界的技術和知識產權（How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World）」、[15]美國白宮科技政策辦公室 2019 年報告

---

[12] Ibid, pp. 16-18.

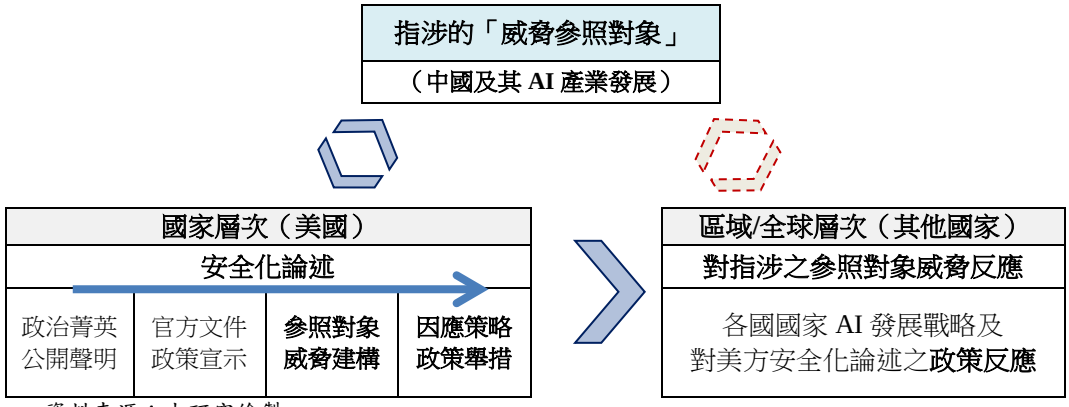
[13] United States. 2016. Executive Office of the President. "Preparing for the future of artificial intelligence." *https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.*

[14] US Congress.Gov 115th Congress(2017-2018), "H.R.4625 - FUTURE of Artificial Intelligence Act of 2017" *https://www.congress.gov/bill/115th-congress/house-bill/4625/text*.

[15] Office of Trade and Manufacturing Policy, "How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World," June 2018,

-「2019 年川普政府第二年科技政策重點(Science & Technology Highlights in the Second Year of the Trump Administration)」,[16]以及 2019 年 2 月，川普總統簽署公布的「美國 AI 倡議（American AI Initiative）」行政命令等六份已進入政府制度議程的官方文件進行安全化的論述分析；分析單元部分，分別以「國家利益」、「國家安全」、「威脅來源」等字句類別，重新解析官方文本中的關鍵詞與重要概念，協助理解安全化語言的表述方式，以及倡議的對象與政策所望目標為何；至於在安全化論述的效果與影響上，則選取「國際層次」中與美國友好的國家，例如德法日等國對於美國官方文件中建構的 AI 安全化論述之反應，以了解區域其他國家是否在互動中肯認這樣的威脅觀點，進入區域安全複合體的合作架構並承擔相對的風險。本文分析架構如下圖所示：

圖 2：本文分析架構



資料來源：本研究繪製。

US White House, *https://www.whitehouse.gov/briefings-statements/office-trade-manufacturing-policy-report-chinas-economic-aggression-threatens-technologies-intellectual-property-united-states-world/.*

[16] 此報告由白宮科技政策辦公室（OSTP）和國家科學技術委員會（NSTC）產出，上述單位負責美國各機構間協調，以及制定重要科學的戰略文件和政策備忘錄。Office of Science and Technology Policy, " Science & Technology Highlights in the Second Year of the Trump Administration,"(February 21, 2019), *https://www.whitehouse.gov/wp-content/uploads/2019/02/Administration-2018-ST-Highlights.pdf.* US White House.

參、AI 科技發展與國家戰略的安全鏈結

目前全世界積極發展 AI 戰略的國家，共計有美國、加拿大、中國、丹麥、臺灣等 18 個，但其中美國和中國在全球 AI 發展上，仍居於世界領先。以 2017 年調查報告為例，全球 2,542 家 AI 企業中，美國佔 42.4%（1,078 家），中國佔 23.3%（592 家），英國佔 5.4%居於第三，其餘則為以色列與加拿大各佔 2.9%及 2.8%。若依據新創公司數量、募資金額及專利數來衡量各國在 AI 產業的實力之指標，中、美兩國這些指標都名列前茅，也是目前全世界 AI 產業觀察重點之一。[17]而中國在近年以國家戰略指導，以追求「速度和規模」積極布局 AI 產業發展，加上中國龐大人口基數以及對於 STEM 教育的重視，使其在未來 AI 發展上具有明顯的優勢。[18]

近期中國國家主席習近平宣示 2030 年前讓中國成為全球領先 AI 創新中心，AI 亦為《2025 中國製造》的核心產業之一，中國透過各種手段獲取關鍵技術（如要求外資企業需轉移技術等智慧財產權），期能成為先進製造業及人工智慧產業的領導者。根據預測，中國 AI 新興技術發展將在 5 年內超越美國。美國早期對於 AI 的技術發展採取自由放任的態度，以最低的干預程度由私人企業與市場機制決定 AI 發展方向和管理規範，這樣的現象讓 AI 大規模推展應用於汽車製造與醫療保健等相關行業。

承前所述，AI 新興技術相關的發展可能改變國際間權力結構，各國對於威脅的感知迫使強權或關鍵技術國家採取行動，進而加速國際間軍備競賽，經濟上則可能有會有更多國家採取貿易保護主義，設立各種壁壘以阻

---

[17] 但若以研發成本投入及全球 AI 技術的專利數來衡量，亞洲地區日本及韓國則另有其優勢。參見李淑蓮，〈人工智慧中美角力賽 其他國家靠邊站?〉，《北美智權報》，2018 年 10 月 31 日，*http://www.naipo.com/Portals/1/web_tw/Knowledge_Center/Industry_Economy/IPNC_181031_0702.htm*。

[18] EE Times, 〈從「AI 和川普」看中國崛起〉，2018 年 11 月 13 日。*https://www.eettaiwan.com/news/article/20181113NT01-China-Fixates-on-AI-and-Trump*。

止其他國家或跨國公司的併購。中國 AI 新興技術急起直追的趨勢使得美國由私部門來發展及維持其技術領先地位的典型立場發生了變化。而美國是目前全球 AI 人工智慧技術發展與應用的主要國家，自歐巴馬政府時期即重視 AI 在國家安全、經濟和全球政治方面扮演重要角色。依據 2016 年總統執行辦公室（Executive Office of the President）所公布的報告「未來人工智慧整備（Preparing for the future of artificial intelligence）」，內容著重於 AI 對於國家安全和全球的影響，並強調如無人機等 AI 發展有助於強化國家安全，亦即以「AI 研究與開發的全球領先地位」與國家利益結合，而軍事和經濟領先有助維持美國在國際的霸權地位。除此之外，國際合作在相關領域的必要性亦被提及。[19]相較之下，川普政府時期的 AI 政策除了延續相同的優先順序（皆認同 AI 政策具有不同程度的軍事與經濟重要性），但川普政府更重視中國潛在 AI 領域競爭與國家利益的連結，面對中國崛起可能的競爭威脅，選擇將國家利益置於國際利益之上，並以自利的方式行事，以確保本身國際與經濟霸權。

2017 年 12 月，美國國會提出未來人工智慧法案（FUTURE of Artificial Intelligence Act of 2017），[20]要求白宮與國會扛起領導責任，全面增加對 AI 的研究投資；而美國總統行政辦公室（Executive Office of the President）於 2018 年 3 月的「川普政府第一年科技政策重點（Science & technology highlights in the first year of the Trump Administration）」中，宣示將致力於推動創新技術發展和研究與開發，消除自動化系統商業化的監管障礙，發展經濟確保國家安全，並捍衛美國技術，[21]後續投入 20 億美元開發軍事

---

[19] United States. 2016. Executive Office of the President. “Preparing for the future of artificial intelligence.” *https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.*

[20] US Congress.Gov 115th Congress (2017-2018), ”H.R.4625 - FUTURE of Artificial Intelligence Act of 2017” *https://www.congress.gov/bill/115th-congress/house-bill/4625/text*.

[21] United States. 2018. Executive Office of the President. “Science & technology highlights in the first year of the Trump Administration.” p3.

AI 科技，以維持及強化美國在人工智能方面的全球競爭力；此外，美國自 2018 年開始對中國廣徵鋼鋁關稅、提出限制出口中國的敏感科技清單，並以 1970 年代通過的《國際緊急狀態經濟權力法》（IEEPA）限制中資收購或投資《中國製造 2025》列出的戰略產業，包括 AI（人工智慧）、機器人、航太、新能源汽車、5G 技術在內；2019 年 2 月，川普總統簽署公布「美國 AI 倡議（American AI Initiative）」行政命令，要求行政當局「投入聯邦政府的所有資源」來協助推動 AI 創新，這項聲明中並未提及中國，但呼籲對研究人員提供更多資源、制定監管法規、在教育領域推動 AI、提高美國的競爭力來「釋放 AI」，捍衛美國在 AI 與關鍵技術上的優勢－因為這對人民與經濟安全利益至關重要，以對抗戰略競爭對手和外國對手，普遍被認為此舉是為了因應中國近年在 AI 技術發展與專利取得大幅成長的威脅。[22]

而在該份行政命令的本文中，更具體將經濟層面的 AI 發展與國家安全扣連，在層次上，透過論述將國內層次－「美國國民與軍隊人員安全」、國家層次－「美國國家與領土安全」、區域與全球層次「美國盟邦與全球安全秩序」三者結合，而「中國近年在 AI 的資金挹注與發展對美國科技優勢造成的威脅」的命題，推論至對上述三個不同層次參照對象的一致性威脅。其文本邏輯結構分析如下：

---

https://www.whitehouse.gov/wp-content/uploads/2018/03/Administration-2017-STHighlights.pdf.

[22] 美國政府基於中國將在 2030 年前投資 1500 億美元，未來可能成為全球 AI 關鍵領域的領導國家。因此川普政府要求政府部門應由政府帶頭加速投資，以避免中國超越。不過，這項命令並未提到具體的資金、或 AI 部署的詳細戰略。請參閱中央廣播電台，〈劍指中國 川普下令傾政府之力推動 AI〉，2019 年 2 月 12 日，*https://www.rti.org.tw/news/view/id/2011053*。

表 1：2019 年美國白宮「AI 倡議（American AI Initiative）」安全化論述分析 [23]

美國國家安全＝國防軍力＋科技優勢	**AI→科技→國防→人民安全→盟邦安全**	**中國與俄羅斯 AI 科技→對美國國防造成威脅→改變全球安全秩序**	**美國被迫因應→成為負責任的 AI 大國→以確保安全與永久和平**
美國國家安全有賴強大軍力保護；而軍力強大與科技先進息息相關	AI 是科技領先的一部分，可協助取得作戰過程各種優勢，也可保護美軍、美國人民及盟邦	中國與俄羅斯在 AI 領域上的軍事鉅額投資已對美國科技與作戰的優勢造成嚴重威脅	美國必須因應與反擊，投入更多資源研發確保優勢，而美國 AI 發展將負責任的朝向符合法律與到道德規範
The U.S. Department of Defense (DoD) protects our nation by deterring war and winning the nation's wars when deterrence fails……to ensure an enduring competitive military advantage against those who threaten our security and safety.	*Artificial intelligence (AI) is one such technological advance. AI refers to the ability of machines to perform tasks that normally require human intelligence…* *We have an opportunity to improve support for and protection of U.S. service members, safeguard our citizens, defend our allies and partners….*	*China and Russia, are making significant investments in AI for military purposes… These investments threaten to erode our technological and operational advantages and destabilize the free and open international order….*	*We will also seek to develop and use AI technologies in ways that advance security, peace, and stability in the long run….* *We will lead in the responsible use and development of AI by articulating our vision and guiding principles for using AI in a lawful and ethical manner.*

資料來源：本研究整理。

由上可知，在安全化過程中，安全化行為體將 AI 技術發展與本身國家生存與安全連結後，透過正式官方文件及主流媒體設定輿論議題，擴大特定國家竊取技術及智慧財產權的潛在威脅，逐步使其他周邊國家接受此

[23] United States. 2019. Executive Office of the President. "SUMMARY OF THE 2018 DEPARTMENT OF DEFENSE ARTIFICIAL INTELLIGENCE STRATEGY, Harnessing AI to Advance Our Security and Prosperity." p.5 *https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF*.

論述，並進一步採去類同的政策措施進行抵制，改變了 AI 的議題領域及主要行為體（原本為私人跨國企業為主，為達成國家戰略的目標，現已進入政策領域）。[24]部分學者認為隨著中美貿易戰的白熱化，雙方競築的關稅障礙會使地緣政治博弈重點轉移至「AI 民族主義（AI Nationalism）」，未來將不利推展使 AI 成為如同 GPS、HTTP 等全球性的公共產品，讓全世界所有國家平等的共享利益；此外，這樣的競爭亦對於未來國際秩序和國際規範的建立有負面影響，[25]值得注意的是，類似上述文件中，將「某一國家 AI 科技領域發展」=「對美國國民與軍隊、國家安全」兩者命題結合的安全化論述，企圖重塑美國人民共同的身份認同與對外威脅認知，激發對國家共同安全體效忠的集體情感，此類「AI 民族主義」的操作方式在一定程度上已擴溢至美中兩國意識形態的對抗。根據美國智庫「皮尤研究中心（Pew Research Center）」於 2018 年 8 月執行的民調顯示，隨著美中貿易緊張局勢的加劇，美國民眾對於中國在經濟威脅、網絡攻擊、環境破壞和人權等等的擔憂已逐步增加，總體而言，對中國有好感的美國民眾自 2017 年的 44%下降為 38%。[26]

---

[24] 2018 年以前，媒體、社會和政府部門人士討論 AI 人工智能發展的未來挑戰和威脅時，他們專注於：認知的 AI 代理人（cognitive AI agents）－可能取代許多職業；自主 AI 設備的法律和道德問題（例如，無人駕駛汽車）；網絡安全問題等等，2018 年後，前述 AI 發展的挑戰並沒有完全消失，隨著政治家和軍方逐漸意識 AI 可能造成的全球變革趨勢，逐步轉亦討論重點於 AI 民族主義（AI nationalism）與 AI 國有化（AI nationalizations）。Sergey Karelov, “AI Nationalism and AI Nationalization Are ahead.” October 2018. *http://russiancouncil.ru/en/analytics-and-comments/analytics/ai-nationalism-and-ai-nationalization-are-ahead/*.

[25] 「AI 民族主義（AI Nationalism）」係由 AI 研究人員 Ian Hogarth 於 2018 年提出，雖然並沒有嚴謹的論述架構，但其提出的 AI 民族主義觀點，一定程度分析目前中美兩國將 AI 發展政策定位為國家戰略的現況，並說明相關重要國家之間的 AI 軍備競賽將會加速，奉行保護主義的國家所採取的行動，將傾全國之力扶植國內企業，阻止外國公司的收購，這場 AI 軍備競賽可能會加快人工智能的發展步伐，縮短做到通用人工智能的時間，但也可能引發國際秩序的不穩定（例如促成新的戰爭模式或造成另種經濟霸權）。Ian Hogarth, “AI Nationalism.” June 13, 2018, *https://www.ianhogarth.com/blog/2018/6/13/ai-nationalism*.

[26] Richard Wike and Kat Devlin, “As Trade Tensions Rise, Fewer Americans See China

回顧冷戰期間，由於美國忌憚於前蘇聯的科技與軍備發展，引發美國對科學和技術的投資浪潮，美蘇兩國在資訊不對等的情況下，於政治、經濟、軍事各層面展開了長達 45 年的對抗。當前由於中美貿易爭端所引發異常複雜的全球局勢，經由前文分析可以發現川普政府透過安全化的論述來連結國家安全，並對中國發起貿易戰；相對來說，中國也持續透過民族主義的渲染，挾國力與軍力成長積極拓張版圖與影響力，步步挑戰美國霸權地位；兩者之間以國家利益為出發點，逐步增強己身的實力以確保自身安全及利益的獨立行為，卻使得雙方更不安全，形成另一種安全困境。由於安全是一種建構的概念，安全與威脅是相對而存在，這亦可充分解釋為何美國面對制度有別於中國的加拿大、墨西哥貿易衝突時，《美墨加協議》（United States-Mexico-Canada Agreement, USMC）比想像中更快達成合作共識，而川普政府對於中國卻採取日趨強勢的制裁與防堵措施。

中美雙方貿易爭端除了帶出 AI 新興科技發展的安全化議題，重塑國家間經濟、安全利益與人力資源的競爭，此項新技術的運用，也引起政府部門系統性的變革呼應，以因應 AI 帶來更快速的資訊流通（例如官僚機構的固定編制改以更彈性的編組與專家團隊，並採取不同的方法以因應重大突發問題產生）。政府部門的相關作法，學者 Ben Scott 認為應包括公共外交(Public diplomacy)：以溝通提升民眾對 AI 與國際關係的影響及認識；多邊參與（Multilateral engagement）：加強與盟友對於 AI 研究的對話及觀點交流，主題應圍繞國際社會在網絡安全方面的因應作為；透過國際和條約組織採取適切行動（Actions through international and treaty organizations）：以正式和非正式的多邊組織進行協議，製定準則甚至具有約束力的國際法，對於部分 AI 新興技術發展有關的重大威脅疑慮，亦需要謹慎評估以

Favorably," *Pew Research Center*, August 28, 2018, *http://www.pewglobal.org/2018/08/28/as-trade-tensions-rise-fewer-americans-see-china-favorably/*.

及協調一致的行動呼應。[27]

肆、國家、區域到全球：逐步建構的中國 AI 技術威脅

自 18 世紀以來的三次工業革命，分別是由於蒸汽機、移動裝配線與大規模生產、電子計算機技術與碳纖維等新材料創新所驅使；[28]而被稱為落實第四次工業革命的「工業 4.0」概念，係由德國政府於 2011 年德國漢諾威工業展（Hannover Messe）上提出，並於 2012 年納入「2020 高科技國家戰戰略」（High-Tech Strategy 2020 Action Plan），其內容結合了機械製造、電子電機、資通訊等 3 大產業，將運算系統與數位網路導入，計劃將網際網絡、大數據、雲計算、物聯網等新技術與工業生產相結合，最終實現工廠智能化生產，讓工廠直接與消費需求鏈結，描繪了全世界製造業的未來願景；[29]世界經濟論壇（World Economic Forum）在 2016 年世界工作

---

[27] Scott, B. and Heumann, S. and Lorenz, P. "Artificial Intelligence and Foreign Policy". Think tank of Stiftung Neue Verantwortung. *https://www.stiftungnv.de/sites/default/files/ai_foreign_policy.pdf*.

[28] 從英國開始的第一次工業革命由於熱力學的發展以及冶金、金屬處理技術的成熟，開創了以機器代替人力勞動的時代，而蒸汽機的運用不僅僅是工廠紡織機、工業設施的動力來源，也是驅動火車的引擎，而為了驅動蒸汽機，對煤炭的需求也促進煤礦業的興起；第二次工業革命發生在 20 世紀初，亨利福特掌握了移動裝配線，並迎來了大規模生產的時代；而第三次革命由於許多卓越的技術融合所催生，包含更聰穎的軟體、嶄新的材料科學、更靈巧的機器人，以及新的製程與一系列基於網絡的服務。The Economist, "The third industrial revolution," April 2012, *https://www.economist.com/leaders/2012/04/21/the-third-industrial-revolution*.

[29] 德國工業 4.0 計劃方案核撥了 2 億歐元的資金，企圖成為醫療、食品、安全、運輸、通訊以及能源領域的科技龍頭。其中未來的智慧工廠（Smart Factory）將部署資訊物理系統（cyber physical system, CPS），該系統使製造與服務的程序更具彈性、自適應性（self-adaptability）與容錯能力（fault tolerance），藉由網際網路協調裝置與電腦，即時更新品質、資源、日期與成本等資訊。而 2018 年展出主題為「產業整合－互聯與合作」，聚焦於人、機器和資訊技術如何進一步融合協作，亦即「工業 4.0」所描繪未來工廠之發展方向。經濟部技術處，〈產業技術評析：從德國漢諾威工業展看智慧製造發展〉，*https://www.moea.gov.tw/MNS/doit/industrytech/IndustryTech.aspx?menu_id=13545&it_id=177*。

報告中，亦認為 AI、遺傳學、納米技術，3D 列印和生物技術，將是推動世界第四次工業革命的重要關鍵因素。[30]

由於人工智慧是未來物聯網及工業 4.0 發展的核心，尤其在零售、交通運輸、自動化、製造業、醫療照護及農業等層面垂直領域具有巨大的潛力，其關鍵在於各種軟硬體的整合，[31]因此技術的合作開發與跨國合作將有利全球未來 AI 發展。近年美國的高階製造業回流政策與 2019 年 2 月川普總統簽署公布的「美國 AI 倡議（American AI Initiative）」行政命令、中國大陸所提出的「『十三五』國家科技創新規劃」以及「次世代人工智能發展計畫」、日本 2017 年 3 月公布之「人工智能的研發目標和工業化路線圖（人工知能の研究開発目標と産業化のロードマップ）」三階段工程以及「AI 科技戰略（Artificial Intelligence Technology Strategy）」、南韓政府 2018 年 5 月公布的「AI 研發戰略（Artificial Intelligence R&D Strategy）」、新加坡政府 2017 年「AI 新加坡計畫（AI Singapore）」，以及我國行政院 2018 年 1 月所提出的「AI 行動計劃（Taiwan AI Action Plan）」等等，相關國家已先後將 AI 提升為國家戰略，大力促進技術和產業發展，聚焦於 AI 與各種產業的應用與落實，惟不同的國家對於 AI 的發展有不同的著重面向。加拿大「先進技術研究院（CIFAR）」於 2018 年「國家與區域 AI 戰略報告（Report on National and Regional AI Strategies）」中，分別以科學研究、AI 人才發展、AI 技能和未來工作發展、AI 技術的工業化、道德化 AI 標準、數據和數位基礎建設、政府人工智能、包容和社會福祉等八個公共政策領域，針對全世界已頒布「國家層級 AI 戰略」的 18 個國家進行比較分析，[32]

---

[30] World Economic Forum. “The Future of Jobs Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution” *2016 Global Challenge Insight Report (*2016). Preface. *https://www.hoover.org/research/emerging-technologies-and-their-impact-international-relations-and-global-security*.

[31] 國家實驗研究院科技政策與研究中心，〈未來 AI 發展八大新趨勢〉，2018 年 10 月 31 日，*http://iknow.stpi.narl.org.tw/Post/Read.aspx?PostID=13837*。

[32] Tim Dutton, *BUILDING AN AI WORLD: Report on National and Regional AI Strategies(*Canada: CIFAR institute, 2018). pp. 9-11.

整體來說，其中有 9 個國家是全面資助戰略發展，並且有具體的政策規劃與執行方針，另外 9 個國家僅提出 AI 未來發展的指導文件，並未編列詳細預算;此外,雖然各國對於國家層級 AI 戰略資源配置的優先順序不同,但工業化（Industrialization）與科學研究為過半數的國家列為優先考慮的重點。

表 2：全球國家 AI 發展戰略重點配置情形

重點 / 國別	科學研究	AI 人才發展	未來工作發展	工業化戰略	道德化 AI 標準	數位基礎建設	政府人工智能	社會福祉
臺灣	3	2		**1**		4		
新加坡	**1**	3		2	4			
日本	2	3		**1**		4		
南韓	**1**	2		3				
中國	2	3	7	**1**	4	5	6	8
澳洲	2	3		**1**	4			
印度	**1**	6	3	4	7	5		2
英國	3	2	6	**1**	5	4	7	
德國	**1**	4	3	2	5	6	7	
法國	2	**1**		3	5	4	7	6
丹麥	3	6	2	**1**	5	4		
義大利		4			3	2	**1**	
瑞典	**1**	3	6	5	2	4		
芬蘭	2	3	6	**1**	7	5	4	
歐盟	**1**	6	5	4	2	3	7	8
加拿大	**1**	2		3	4			
墨西哥	**1**	4	2	6	5	3	7	
阿聯酋		3		2	4		**1**	
備考	方格內數字 1-8，表示單一國家政策重點與資源配置程度，空格代表該國文件無提及。							

資料來源：參考 Tim Dutton, *BUILDING AN AI WORLD: Report on National and Regional AI Strategies* (Canada: CIFAR institute, 2018), p. 10.內容修改。

另外一方面，由過去的工業革命的歷史經驗可以發現，每一次的重大

https://www.cifar.ca/docs/default-source/ai-society/buildinganaiworld_eng.pdf?sfvrsn=fb18d129_4.

技術突破都為人類社會及地球環境帶來改變與衝擊，直接或間接影響一國國內政治經濟運作、政府法律體制、國際典則，甚至進而改變國際政經權力版圖的分布。事實上，就目前的 AI 技術發展，國際間除了網絡安全（Network security）與無人機運用等少數技術已經對各國有明確安全威脅並已產生審查預防機制，惟包含 AI 以及其他領域的技術發展，目前整體仍集中在技術變革與實用推廣上的預期，尚無法達成經濟規模，亦無任何一國在此領域具有全球政治或安全上主導優勢。

以現實主義觀點來看，經濟實力是一個國家發展軍事和政治力量主要基礎，而這些新興技術發展需要完整的工業基礎和國家鉅額投資，雖然國際間潛在競爭對手數量不多，但任何國家新型技術的獲取與突破都可能扭轉現有的權力態勢，因此主權國家人會對潛在威脅家以提防戒備，採取相對應措施以確保國家利益與國際霸權領導地位，這樣的邏輯在川普政府的許多官方文件論述中可以明確掌握其脈絡。近年中國綜合國力提升，其「十三五」規劃綱要（2016－2020 年）中明確以「一帶一路」建設等計劃來執行全方位對外開放戰略，在 AI 新興技術的發展上，更預劃於 2030 年前投入 1500 億美元，美國為了確保國家利益，對於中國發展指涉國家安全、國防安全和情報、AI 和網際網路這些可能取得關鍵優勢和權力投射創新研究領域，日增的威脅讓美國不得不對中國採取更積極的宣示與政策作為。

哥本哈根學派認為在經濟領域的安全威脅認定較為困難，因此必須在「安全指涉對象」和「存在性威脅」上有更為完整的論述。美國 2017 年 12 月國家安全戰略（National Security Strategy）中，明確界定「促進研究、技術和創新中領先以促進美國繁榮（Promote American Prosperity）」為其四大戰略支柱之一，在報告中申明戰略規劃將基於「有原則的現實主義」（Principled realism），透過身力量強劃的方式來確保安全（Preserve Peace through Strength），將經濟安全提升到國家安全的層面；報告中亦認定中國及俄羅斯為「修正主義強權（Revisionist powers）」正在挑戰美國的利益、經

濟與價值觀，因此必須綜合多種戰略手段與之對抗；[33]2018 年 5 月美國國會通過「外國投資風險評估現代化法案」（FIRRMA），目的在加強對外國投資、併購敏感科技企業的管控；2018 年 11 月對外公布《審查部份新興技術控制》（Review of Controls for Certain Emerging Technologies）框架，考慮對包含人工智慧（AI）和機器學習技術、生物技術等 14 類敏感、可能被應用於常規武器、情報收集、大規模殺傷性武器或恐怖主義的新興技術領域進行技術出口進行管制，即是將中國的 AI 發展視為威脅，藉以打擊「中國製造 2025」計劃。[34]

當然，一個國家的「利益」可以透過如美國國家安全戰略（National Security Strategy）或中國「強國戰略藍圖」中之「中國特色大國外交」戰略或「中國方案」文本，明確掌握其內涵與未來發展重點。問題是，原屬於「低階政治」經濟層面之 AI 新興科技發展，如何轉換進入「高階政治」成為國家安全之戰略議題？國家安全的本質與威脅的來源如何界定？對於這些問題，安全研究領域中哥本哈根學派學者認為「安全是一種社會建構過程」，安全行為體如政府、政治家或統治菁英對於主觀性的威脅用一系列的政治語言框架出安全化政策議題，再尋求說服其他國家接受這樣的威脅是存在的，這就是安全化。[35]關於美國如何將中國 AI 新興技術威脅，由國家擴及到區域與全球三個不同層次參照對象，此部分在前文已有分析說明。在區域與國際安全理念的推廣與合作部分，2017 年版的美國國家安全戰略中，述及「美國將動員其他友好國家，聯合以經濟壓力來因應其他潛

---

[33] US WHITE HOUSE, “US National Security Strategy.” *https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf, December 2017. pp.25-32*.

[34] 中國於 2015 年提出的「中國製造 2025」主軸政策，目標是在 2025 年邁入製造強國行列，2035 年成為世界中等製造強國，2049 年則進入世界製造強國前列。自由時報，〈斷中國製造 2025 生路？美擬管制 AI、機器人等新興技術出口〉，2018 年 11 月 19 日，*http://ec.ltn.com.tw/article/breakingnews/2617671*。

[35] 柯林斯等著，《當代安全研究》（中國北京：世界知識出版社，2016 年），頁 201-204。

在安全威脅」的因應手段。[36]

實際上，美國除了重新框架與定義 AI 威脅的指涉對象及內容，並持續透過向歐洲警告中國商品在資安上的疑慮及後續可能不與不同系統合作等方式，對盟友遊說與施壓，希冀各國對中國採取一致性的政策應對措施，惟各國 AI 產業發展條件與需求各殊，在國家層級的 AI 發展戰略上已明確揭示有不同的重點配置，因而美國單方面的安全-威脅的建構，因成員間異質性過高，此領域「安全複合體」尚無法有效形成。

以中美對華為（Huawei）電信設備安全性爭議為例，美國不斷施壓其他國家對中國電信設備製造商採取抵制禁用的措施，雖然一開始澳洲、紐西蘭、日本已於 2018 年年底跟進，歐洲地區英國電信（British Telecom, BT）、德國電信（Deutsche Telekom）亦決定將華為設備由目前 3G/4G 網路核心部分移除，同樣政策也適用於 5G 網路，而德國的決定亦影響以德國為客戶的供應鏈國家，後續波蘭、匈牙利、捷克等歐洲國家可能考慮排除中國華為設備；[37]而這樣的情勢在近期有了微妙轉變，2019 年世界行動通訊大會（MWC）上，部分國家採取了與美國不同的立場，陸續改變立場，對外發表聲明將採用中國華為產品，讓主導反中國技術產品的美國受到挫折。[38]

---

[36] 原文措辭為「Deploy economic pressure on security threats」，請參閱 US WHITE HOUSE, "US National Security Strategy." *https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf*, December 2017. p.34.

[37] 數位時代，〈華為封鎖令席捲歐洲〉，2018 年 12 月 14 日，*https://www.bnext.com.tw/article/51757/huawei-restricted-by-germany*。

[38] 阿拉伯聯合大公國國有電信公司阿聯電信公布最新計劃，已和華為達成協議，2019 年內擬搭建 600 座華為 5G 基地台。工商時報，〈華為中東突圍 部署阿聯 5G 網路〉，2019 年 2 月 28 日，*https://www.chinatimes.com/newspapers/20190228000292-260203*。

表 3：世界各國對中國華為（Huawei）電信參與 5G 態度

各國立場[39]			
封殺限制		觀望開放	
美國	敦促盟友禁止華為參與 5G	德國	查無間諜實據，未準備禁用
臺灣	有資安顧慮，維持一貫進用	紐西蘭	5G 建設從未排除華為參與
日本	政府及三大電信均封殺華為	英國	風險可控，毋須完全排除
南韓	未明令限制，僅第四大電信支持	法國	針對華為的 5G 管控法案尚未通過
澳洲	考量國安，禁華為提供 5G	印度	暫時觀望，尚未採取最後立場
波蘭	考慮禁止滑為市場運作	挪威	考慮排除華為，尚未最後決定
捷克	有安全威脅，禁參與政府標案	阿拉伯聯合大公國	和華為達成協議，將大舉開放與合作

資料來源：參考 2019 年 2 月期間蘋果日報財經版及相關新聞內容修改。

由於美中關係對區域及全球安全情勢具有廣泛的影響力，當前 AI 新興技術威脅已由單一國家建構，逐步的擴散到區域與全球體系中，但美國單方面對中國非慣常的制裁措施（非透過世界貿易組織解決貿易衝突爭端），似乎尚未能獲得其他國家一致的認同，顯示目前建構中的 AI 新興技術威脅，區域或全球安全複合體的概念尚未成形，但此現象除了已經造成全球貿易衝突與對立加劇，相對的，在國際關係與外交政策領域亦帶來新的問題和挑戰。

伍、結論

由於美國掌握有國際話語權及安全論述創造的能力，當前 AI 科技發展由美國的政治菁英與政府官方文本中，已明確建立一套安全化架構，在安全領域上已由單純經濟面向鏈結至美國國家安全中的政治與軍事，其影響已逐步向外擴溢至全球。就目前的 AI 技術發展，國際間除了網絡安全

[39] 蘋果財經，〈盟友轉向，美國圍堵破功—英德 5G 不排除華為〉，《蘋果日報》，2019 年 2 月 21 日，版 B1。

與無人機運用等少數技術已經對各國有明確安全威脅並已產生審查預防機制，其他的部分各國仍對美國建構的中國 AI 安全威脅仍有不同看法與認知，不可否認的是，目前美中雙方都具有一定的 AI 新興技術發展優勢，未來兩國對於 AI 發展所採取的對抗或對話手段，都將直接或間接影響國際政經權力版圖的分布以及 AI 國際規範與典則制定，當然，在全球化跨國產業供應鏈中的其他國家，亦難免受到波及。鑑此，以下針對 AI 對國際關係研究可能的議題發展，以及美中雙方未來競合所產生的挑戰與契機提出逐次分析。

一、未來國際關係領域之可能議題發展

學者 Danilin 由非國家行為者（如次國家行為體或 NGO）、國家與區域行為者，以及全球行為者（強權國家與新興挑戰）等層次，分析 AI 新興技術可能發生的權力強化（Enhancement of current power）、不對稱優勢（Asymmetric advantage）與規則改變，甚至是破壞（Disruption）等不同程度的影響。而對於國際關係與外交政策整體改變與未來趨勢，包括下列幾類：[40]

（一）新興科技將形成國際關係議題設定者（problem-setters）

新興技術發展階段（尤其突破性技術革命）將會帶來一系列問題和挑戰。

（二）技術和創新優勢（Technology and innovation superiority）

此取徑假設國防與商業新興技術領域發展的相互呼應，在商業領域部分，高科技解決方案、一致性標準，數位平台，跨國公司和軟實力的崛起，將

[40] Ivan V. Danilin, “Emerging Technologies And Their Impact On International Relations And Global Security,” Hoover Institution, Stanford University, Issue 118. October 2018. *https://www.hoover.org/research/emerging-technologies-and-their-impact-international-relations-and-global-security*.

是取得全球市場領先地位的重要關鍵，目前美國是這個取徑中重要行為者，而中國也採取相同策略急起直追當中。

（三）選擇性對稱或非對稱回應（Selective symmetric/asymmetric response）

就資源或競爭基礎有限的中小型國家，選擇發展某些重要領域新興技術並取得部分優勢，是改變區域或世界秩序平衡的一種技術威懾（tech-deterrence）策略，重新平衡或修訂區域或世界秩序，其中受到經濟和制度限制的印度目前所採取的新興技術發展戰略也是一種非對稱回應的平衡策略。

（四）軍備競賽和新型擴散（Arms race and neo-proliferation）

在 AI 新興科技發展下，區域間各國新形式的武器或軍民兩用技術競賽似乎是不可避免，亦造成緊張情勢。而新的解決方案不受國際規範的約束，如同美國一樣，單方面的經濟制裁或禁止新興技術轉移與擴散措施，可能會引起重大的國際貿易動盪與其他負面影響。

（五）權力分散與弱化（Dissemination/loss of power）

新興技術可能會導致權力進一步下放到其他非國家行為者（如 NGO、跨國公司、全球網絡社群）或政治實體。實際上，後威斯特伐利亞（post-Westphalia）的體系已經逐步實現，某些大型跨國公司已經與中等規模經濟體相當，並積極透過遊說與經濟影響力來影響國家政策；另外一方面，恐怖主義也透過電子媒體與網路，將安全問題散佈到其他國家或次國家實體，形成國際關係領域關切的另一個重要問題。

（六）國際規則和條例（International rules and regulations）

隨著全球對於新興技術帶來的風險與擔憂日益加劇，目前一些規範倡

議多針對優勢國家或潛在對手的技術發展進行限制，為了確保此領域的利益能夠為全共享，並促進公平競爭，對於數位隱私與智慧財產權的保護亦應該受到重視，由於國際間新的制度和規範對 AI 發展的正常化和安全化至關重要，如同其他領域的議題一樣，需要國際間更多的對話，可預見的是，最終國際關係制度和規範以及外交溝通和協調機制將不可避免也逐步改變。

（七）新興技術時代的權力和新殖民主義

當前全球新興技術發展仍集中於極少數先進國家。無論是人工智能，生物技術，機器人技術還是 3D 列印的發展，除了中國以外，多數的發展中國家大多扮演技術接受者的角色。不可避免的是，新興技術領域的「馬太效應（Matthew effect）」以及大多數國家對少數領先經濟體的技術出口和服務的依賴程度將會日益增加。[41]在 AI 新技術革命領域，即使相關影響散佈於不同的國家與非國家行為體之間，但未來國際關係領域將面臨更為複雜和微妙的統治與屈服的權力關係。

二、政治對抗或是對話-AI 未來的挑戰與契機

由歷史經驗中可以發現，兩個世紀前工業革命從起源的西歐緩慢的擴展到世界每個角落，前兩次工業革命中出現的新興工業如電力工業、化學工業、石油工業和汽車工業等，讓機器取代人力，企業規模的擴大讓生產率進一步提高，促進生產和資本的集中；相對來說，自 1970－1990 年代中葉的廿年間，第三次工業革命因電腦與網際網路的廣泛應用，促進了生產、管理和國防與資訊情報科技現代化，然而，新資訊技術的應用雖然迅速傳布並連結整個世界，但技術革命本身只發生在以美國為主的少數幾個國家當中，不可否認，世界上有許多國家和區段，仍與新資訊技術體系斷

[41] 「馬太效應（Matthew effect）」或「貧困陷阱（poverty trap）」為教育學或經濟學中，在資源不對等的情況下一種可能的長期惡性循環假定。

聯（Switched off），[42]以美國為主的幾個少數國家在 1970 年代所建立的新技術型典範（New technological paradigm）建構出一種特殊區段，並物質化一種生產、傳播、管理與生活的新方式，改變了全球經濟和世界地緣政治的權力互動關係。[43]

世界經濟論壇所提出的「第四次工業革命工業」描述的是一個抽象概念，而德國提出的「工業 4.0 戰略」則是一個實踐中的進行式，AI 新興科技的突破性發展，代表著一種潛在變革正在進行，這樣的變革雖然為人類文明進步帶來更多希望的種籽，但對於社會、文化、歷史變遷與國家權力更迭有著結構性的影響，吾人必須審慎理解及掌握其中意涵。由前文的探討可以發現，科技的發展經由國家干預而加速技術的發展，於短期內（相對於私人企業或 NGO 的研究與發展，而中國國營企業則是另一種不同的類型）改變經濟的命運、軍事的力量與人類的福祉，相當程度塑造了社會的命運，簡言之，決定社會或歷史變遷的是國家的價值判斷，技術本身則是體現社會以及權力轉化的工具，這樣的經驗也可以套用在 AI 新興科技的發展上。惟在議題層次上，由於美國於歐巴馬及川普總統任期內，皆提及 AI 技術發展將可支撐軍事與經濟的領先地位，這是確保全球霸權的重要目標與手段之一，只是川普政府論述框架則以美國的民族主義（a nationalistic, American approach）為基底，更強調「國家利益」大於國際對話與合作夥伴關係。

進一步將前文內容中所討論的安全化（Securitization）架構化約，可以發現其「語言－行動」之論述建構順序為：美國政府資助包含 AI 等 STEM（Science, Technology, Engineering, and Mathematics, STEM）新興技術發展→技術突破以取得美國軍事、經濟和資訊優勢→維持本土防衛與國家安全→確保美國國家利益；而在 AI 議題倡導的角色上，前文分析可以發現已

---

[42] 曼威·柯司特（Manuel Castells）著，《網絡社會之崛起》（臺北：唐山出版社，1998 年），頁 35-37。

[43] 前揭書，頁 5。

由早期的私人或民間企業自主性發展，透過美國國會「未來人工智慧法案」、總統行政辦公室「川普政府第一年科技政策重點」等官方文件，國家角色快速崛起，除了明確定位為國家戰略，並以政策工具來落實；此外，為了使其他國家認同這樣的安全化論述，並與美國形成安全聯盟，則進一步以中國經濟發展威脅作為載點，建構「中國傾其全力，積極獲取關鍵科技、智慧財產與發展新興高科技產業，以促進未來國家經濟發展及國防產業升級」→世界各國（含美國）都是其目標→威脅各國國家安全與利益→各國應與美國偕同一致加強合作，並積極防範中國的威脅。[44]

顯然的，全球 AI 新興技術的議題，已經從原本國家層次正向蓬勃發展、關注經濟與商業利益的第四次工業革命（或工業 4.0 代稱），關注焦點移轉至區域或國際（全球）層次的政治與安全議題，美國由於對中國貿易逆差、智慧財產權保護、減少本國產業外移、促進國內投資意願等因素，一在對外強調想藉此解決中國不尊重智慧財產權、商業間諜眾多和利用龐大內需市場換技術的嚴重問題，因而採取非慣常措施進行抵制或設立關稅壁壘（對於國際貿易爭端通常透過世界貿易組織解決程序裁決，而非逕由單一國家認定並實施報復），此種偏向 AI 民族主義的方式與中國進行經濟衝突與對抗，已造成全球經貿交流減緩、各國經濟成長遲滯，亦可能間接影響部分國家國內政治局勢，對於國際關係與外交政策帶來新的問題和挑戰。

由於當前各國對於美國所建構的「中國 AI 威脅」之安全議題的認知

---

[44] 原文為 *China pursues two categories of economic aggression that are the focus of this report. These include: #1 Acquire Key Technologies and Intellectual Property From Other Countries, Including the United States. #2 Capture the Emerging High-Technology Industries That Will Drive Future Economic Growth and Many Advancements in the Defense Industry.* 參見 White House Office of Trade and Manufacturing Policy, "How China' s Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World" June 2018. p.2. *https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf.*

與立場不同，可以預期的是，美中之間的貿易爭端在短期內無法透過談判解決的情況下，復以美國單方面逐步升高衝突態勢，而各國為了保護國內相關產業，亦將採取政治/經濟層面以相對應，除了不利 AI 專業技術與知識擴散，也將造成製造與應用產業的重組與「短鏈革命」，對目前各國將 AI 及機械學習（Machine Learning）列為國家發展戰略勢必造成衝擊。本文透過單一國家 AI 安全化建構的議程探討，提供另一層安全分析的觀點，避免無限制擴張安全概念，而透過「去安全化（Desecuritization）」的逆向操作過程，可以將傳統「威脅→防衛」的思維框架中解放，並提供另外一個思考選項。易言之，未來各國在對於「中國 AI 威脅」命題的認知，以及在相關領域採取對抗或合作的策略，亦將連動成為此領域未來發展的挑戰或契機。

責任編輯：陳臻