

# 第三章 科技安全

王綉雯、杜貞儀\*

## 壹、前言

2019年5月15日，美國總統川普簽署行政命令，禁止美國企業使用具國安疑慮企業所生產的電信設備，商務部隨即將「華為」及旗下68家子公司列為出口管制黑名單，正式揭開美中科技戰之序幕。

隨著「華為」5G布局的推展，新興關鍵技術已成為未來地緣政治甚至全球霸權的決定性因素。大部分的關鍵技術屬於軍民兩用技術，研發創新和民生應用上的突飛猛進，不僅將左右一國之生存發展，其技術擴散亦可能造成安全威脅。因此，先進各國莫不特別注重關鍵技術之保護，並嚴格防範其流出。

然而，關鍵技術之安全必須置於國內與國際兩個層面來觀察，才較能掌握全貌。甚或在各國之綜合比較中，得出相近的共同意涵。本章即針對科技安全主題，就關鍵技術之發展、擴散與管制，嘗試從各主要國家之國內與國際兩個層面一一深入探討。

## 貳、關鍵技術之發展

關鍵技術 (critical technologies) 一般指為維持一國之軍事優勢密切相關的科技。冷戰時期，美國國防部根據 1979 年《出口管理法》(Export Administration Act 1979)，於 1980 年成立軍事關鍵技術計畫 (Military Critical Technologies Program) 以建立軍事關鍵技術清單 (Military Critical Technologies List, MCTL) 及發展中科技清單 (Developing Science and Technologies List, DSTL)，各分為二十項，是現今技術管制體制的基礎。

近年隨著科技演進及國際戰略環境改變，各界對於新興科技 (emerging technologies) 未來將能在軍事及戰略上「改變遊戲規則」(game-changer)，也已逐漸有所共識。至於對既有的戰略優勢威脅之因應作為，具體展現即是 2016 年美國的「第三波抵銷戰略」(Third Offset Strategy)，透過科技、作戰概念以及組織變革，維持其武力投射的能力。<sup>1</sup>2018 年及其後之《國防授權法》(National Defense Authorization Act for Fiscal Year 2018, NDAA 2018, NDAA 2019 & NDAA 2020)，即延續此一脈絡，將科技快速發展視為未來安全環境的最大挑戰。

---

\* 王綉雯，國防資源與產業研究所博士後研究，負責本章第壹與肆節；杜貞儀，網路作戰與資訊安全研究所博士後研究，負責本章第貳、參、伍節

<sup>1</sup> Cheryl Pellerin, "Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence," U.S. Department of Defense, October 31, 2016, <https://www.defense.gov/Newsroom/News/Article/Article/991434/deputy-secretary-third-offset-strate/>.

然而，日新月異的科技，究竟哪些是對既有戰略優勢造成威脅的關鍵，又應如何找出其優先順序，並投注資源納入技術管制體制，仍是目前尚未有定論的課題。冷戰時期基於核武共同嚇阻（mutual deterrence）建立的戰略穩定（strategic stability），其實際意涵包括危機穩定（crisis stability）及軍備競賽穩定（arm race stability）兩者。前者指缺乏動機在第一擊使用核武，後者則是缺乏建立核武之動機。<sup>2</sup>

而新興科技的破壞性，則可對其是否將會激烈衝擊既有之戰略與安全環境，在程度上做出區別。目前對新興科技研發投注大量資源的國家，主要仍為美、中、俄三國。「美國科學家聯盟」（Federation of American Scientists）於 2018 年發表報告，就新興、關鍵技術進行系統性的探討，並依照技術特性、發展趨勢以及未來對於核戰略穩定（strategic nuclear stability）及國家安全造成的威脅，列出數個破壞性技術的篩選條件：

- 此技術將在近 20 年內發展成熟
- 將對於下列一或多項造成極大挑戰：
  1. 攻勢戰略武力的存活率
  2. 守勢武力的能力
  3. 戰略武力指管通情監偵的穩定運作
  4. 加速危機動盪
- 成本較低廉（not cost-prohibitive）
- 可用於或增強現有的威脅
- 將增強一國私自製造核武的能力

符合以上條件的新興科技，約包含下列數項：

- 雷射同位素分離（laser isotope separation）
- 中子與反中子偵測技術（neutrino and anti-neutrino detection technology）
- 高能雷射（high-energy lasers）
- 極音速打擊科技（hypersonic strike technology）
- 人工智慧（artificial intelligence）與大數據分析（big data analysis）
- 低成本高空持續感測技術（low-cost overhead persistent sensing technology）
- 高階網路作戰能力（advanced cyber capability）

除「美國科學家聯盟」的分析，美國 2019 年及 2020 年《國防授權法》（NDAA 2019 & NDAA 2020）也同樣反映出對新興科技相關發展的重視。其中除高能雷

---

<sup>2</sup> Christopher A. Bidwell, JD & Bruce W. MacDonald, “Special Report: Emerging Disruptive Technologies and Their Potential Threat to Strategic Stability and National Security,” *Federation of American Scientists*, September 2018, <https://fas.org/wp-content/uploads/media/FAS-Emerging-Technologies-Report.pdf>.

射、極音速打擊科技、人工智慧及高階網路作戰能力外，另有量子運算 (quantum computing)，共同作為新興科技的重要項目，並持續以政策支持研發及國防應用。

中共 2019 年 7 月公布之《新時代的中國國防》白皮書，指出「在新一輪科技革命和產業變革推動下，人工智能、量子信息、大數據、雲計算、物聯網 (Internet of Things, IoT) 等前沿科技加速應用於軍事領域，國際軍事競爭格局正在發生歷史性變化」，顯示中共同樣將人工智慧、量子運算、高階網路作戰能力之軍事應用，視為未來發展重點，並表示「武器裝備遠程精確化、智能化、隱身化、無人化趨勢更加明顯，戰爭形態加速向信息化戰爭演變，智能化戰爭初現端倪」。<sup>3</sup>對照十一閱兵首次亮相的新型武器，亦預示未來共軍作戰概念與意圖，應包括高能雷射及極音速打擊技術。

俄羅斯雖無定期公布國防白皮書或類似官方文件，指出未來戰略發展方向之習慣。然而，當美國於 8 月 2 日正式退出《中程飛彈條約》(Intermediate-Range Nuclear Forces Treaty, INF) 後，即有評論指出，俄羅斯應會把握此時機，加速其極音速飛彈研發與部署。<sup>4</sup>另外，俄羅斯亦傳出近期已在莫斯科物理技術學院 (Moscow Institute of Physics and Technology) 成立人工智慧研究中心，藉由公私合營 (public-private partnership) 進行人工智慧基礎研究以及應用探討。<sup>5</sup>

綜合各國技術研發方向，高能雷射、極音速打擊技術、人工智慧及量子運算等四項技術，是目前研發的重點項目，以下將簡介其近期重要發展。

## 一、高能雷射

高能雷射目前仍屬概念性武器，但由於近年固態雷射 (solid-state laser)、光纖雷射 (fiber laser) 發展迅速，已經逐漸具軍事應用價值。透過光譜光束合併 (spectral beam combining) 技術，可將多個相位略有差異的低出力光纖雷射，合併為單一高出力雷射光束。如美國洛克希德馬汀公司 (Lockheed Martin) 曾於 2016 年進行實驗，成功將 96 個 300 瓦光纖雷射合併為總出力達 3 萬瓦的雷射光束，並可擴大其應用範圍。<sup>6</sup>據估計，高能雷射若作為武器，其出力需達到 50 萬至 1 百萬瓦，才能達到影響戰略層級，但現行開發之戰術層級武器，出力約在 1 萬至 15 萬瓦左右，研發方向逐漸針對較小型目標如無人機、小型船舶等。<sup>7</sup>

中國大陸對雷射科技的前端研究由來已久，應用部分，已有由學術單位與其延伸企業共同研發推出高能雷射武器系統，如中國工程物理研究院之子公司「久

<sup>3</sup> 〈《新時代的中國大陸國防》白皮書全文〉，中華人民共和國國防部，2019 年 7 月 24 日，[http://www.mod.gov.cn/big5/regulatory/2019-07/24/content\\_4846424.htm](http://www.mod.gov.cn/big5/regulatory/2019-07/24/content_4846424.htm)。

<sup>4</sup> Chris Miller, "The INF Treaty Is Dead, and Russia Is the Biggest Loser," *Foreign Policy*, August 2, 2019, <https://foreignpolicy.com/2019/08/02/the-inf-treaty-is-dead-and-russia-is-the-biggest-loser/>.

<sup>5</sup> Samuel Bendett, "Russia's National AI Center Is Taking Shape," *Defense One*, September 27, 2019, <https://www.defenseone.com/technology/2019/09/russias-national-ai-center-taking-shape/160219/>.

<sup>6</sup> Jeff Hecht, "Fiber Lasers Mean Ray Gun Are Coming," *IEEE Spectrum*, March 27, 2018, <https://spectrum.ieee.org/aerospace/military/fiber-lasers-mean-ray-guns-are-coming>.

<sup>7</sup> Megan Eckstein, "Navy to Field High-Energy Laser Weapon, Laser Dazzler on Ships This Year As Development Continues," *USNI News*, May 30, 2019, <https://news.usni.org/2019/05/30/navy-to-field-high-energy-laser-weapon-laser-dazzler-on-ships-this-year-as-development-continues>.

遠高新技術裝備」，以及中國工程科學院光電所合作研發之萬瓦級近程防空系統「低空衛士」。<sup>8</sup> 而基礎研究部分，專注於基礎技術研發、名列「國防七校」的哈爾濱工業大學，擁有運用 46 束雷射激發燃料丸以產生能源的雷射型慣性侷限融合（inertial confinement fusion with lasers）裝置「神光-III 靶場」，並藉由此項新能源研究，同步開發精密光電及控制系統並申請相關專利，其研發團隊也於 2016 年選入中共國家國防科技工業局之年度國防科技工業十大創新團隊。<sup>9</sup>

另外一項基礎研究項目是固態雷射不可或缺的晶體，近年則有中國科學院福建物質結構研究所毛江高教授團隊，新合成銻酸鉍銻（cesium bismuth germanate，化學式  $\text{Cs}_2\text{Bi}_2\text{O}(\text{Ge}_2\text{O}_7)$ ，簡稱 CBGO）晶體，並於 2019 年 8 月發表於國際學術期刊。與目前廣泛使用的磷酸二氫鉀（potassium dihydrogen phosphate，化學式  $\text{KH}_2\text{PO}_4$ ，簡稱 KDP）晶體相比，銻酸鉍銻晶體具有更高的轉換效率，能將紅外線雷射轉為更高能的綠色雷射。雖然使用銻酸鉍銻晶體，並未改變影響現今固態雷射應用範圍的耗電與散熱瓶頸，但此新合成晶體未來可能具有潛在軍事應用價值。<sup>10</sup>

## 二、極音速打擊科技

極音速（hypersonic）一般定義是能達五馬赫（超過音速五倍）以上，目前關注多集中在空射飛彈以及彈道飛彈的重返載具。尤其若洲際彈道飛彈重返載具在大氣層頂部以極音速移動，現行技術如衛星及雷達，幾乎無法追蹤，也難以進行攔截。<sup>11</sup> 極音速的技術挑戰，在於材料科學、導引、控制及推進系統四個項目。達極音速時，載具或武器外部溫度將可達華氏 2,000 度（約攝氏 1,093 度），故須使用耐高溫材料以保護內部電子系統。另外，極音速載具或武器若以超音速燃燒衝壓引擎（supersonic combustion ramjet，簡稱 scramjet）為推進系統，則需在達到次音速進氣後才能工作，這使得一般極音速武器或載具，初始發射階段仍需仰賴火箭推進，具從靜止推進至極音速能力之引擎，目前則還在開發階段。<sup>12</sup>

<sup>8</sup> 〈破壁壘、重孵化、強人才—來自第六屆科博會的軍民融合啟示〉，2018 年 9 月 8 日，《新華網》，[http://www.xinhuanet.com/local/2018-09/08/c\\_1123399905.htm](http://www.xinhuanet.com/local/2018-09/08/c_1123399905.htm)。

<sup>9</sup> 「國防七校」指現由中共工業和信息化部直屬、與軍事工業有極深淵源的七所高等院校，包括北京航空航天大學、北京理工大學、哈爾濱工業大學、哈爾濱工程大學、南京航空航天大學、南京理工大學以及西北工業大學，均為中共國家重點院校。「神光-III 靶場」相關報導見〈“神光-III 靶場光電及控制系統研制”團隊入選國防科技工業十大創新人物（團隊）〉，《哈工大報》，2016 年 12 月 30 日，<http://sme.hit.edu.cn/2016/1230/c6475a169599/page.htm>。

<sup>10</sup> 〈中國合成新晶體 或促進定向能武器〉，《BBC 中文網》，2019 年 9 月 5 日，<https://www.bbc.com/zhongwen/trad/chinese-news-49597090>。（此新聞內文銻酸鉍銻翻譯有誤，另參戴元起，〈銻酸鉍(BGO)晶體研究開發的啟示〉，《中國科學院院刊》，1988 年 1 月號，[http://www.bulletin.cas.cn/zgkxyyk/ch/reader/view\\_abstract.aspx?file\\_no=19880109&flag=1](http://www.bulletin.cas.cn/zgkxyyk/ch/reader/view_abstract.aspx?file_no=19880109&flag=1)。）

<sup>11</sup> Michael T. Klare, “An ‘Arm Race in Speed’: Hypersonic Weapons and the Changing Calculus of Battle,” *Arms Control Today*, June 2019, <https://www.armscontrol.org/act/2019-06/features/arms-race-speed-hypersonic-weapons-changing-calculus-battle>.

<sup>12</sup> “Science & Tech Spotlight: Hypersonic Weapons” *GAO Science, Technology Assessment, and Analytics*, September 2019, <https://www.gao.gov/assets/710/701369.pdf>.

值得注意的是，極音速武器透過高速移動以及其本身所具質量，即使未裝備彈頭，其產生之動能即足以造成極大的物理損害。因此，極音速武器將徹底改變作戰節奏與型態，壓縮決策時間，以致容易因恐懼或缺乏考慮倉促決斷，而造成衝突升高。美國應認為極音速武器已經實質進入與中國大陸、俄羅斯之間的軍備競賽，討論國際軍備管制的時機可能已經成熟。因此，除了加強研發以及應用外，在 2019 及 2020 年之《國防授權法》，均將《新削減戰略武器條約》(Strategic Arms Reduction Treaty, New START) 納入極音速武器列為重要工作項目，未來或將考慮提案使相關科技加入飛彈技術管制體制 (Missile Technology Control Regime, MTCR) 清單。

### 三、人工智慧

人工智慧 (Artificial Intelligence, AI) 作為廣泛運用的通用科技，具有高度戰略價值，也是美、中、俄三國目前競逐的主要領域。不過，雖然 AI 有非常廣泛的商業應用，且商用領域在特定項目發展 (如自動駕駛) 一般認為已明顯超前軍用領域，但相較於演算法所受到的關注，AI 由發展進入應用所依賴的運算資源與硬體架構，則較容易被忽略。尤其在結合物聯網情境下，為因應邊緣運算 (edge computing) 需求，硬體設備更應具有足以執行 AI 應用之運算能力。資料中心為進行雲端運算，也需針對 AI 進行系統架構優化。

因此，2019 年，各大廠紛紛推出針對物聯網及資料中心市場的 AI 晶片。由 AI 應用端區分，輸入資料進行模型最佳化的階段稱為「訓練」，將模型及參數應用於實際場景階段則為「推論」，亦各有因應不同階段需求所開發的晶片產品。以圖形處理器發跡的「輝達」(NVIDIA)，2019 年 3 月推出採用其 CUDA-X 架構的單版電腦 Jetson Nano，預定售價僅 99 美元，主要針對邊緣系統開發市場，大幅降低 AI 運算之硬體成本。<sup>13</sup>「英特爾」(Intel) 則於 2019 年 8 月發表新款 AI 晶片系列—Nervana 神經網路處理器 (Neural Network Processor)。Nervana 屬於系統單晶片 (System on a Chip, SoC)，將數個系統整合至單一晶片的積體電路，以更小體積執行相同功能，並有訓練與推論晶片兩種構型。<sup>14</sup>生產主力為手機晶片的「高通」(Qualcomm)，以 Cloud AI 100 跨足雲端運算領域，並宣布將與積極推展雲端運算服務的「微軟」(Microsoft) 進行合作測試，預計於 2020 年正式推出。<sup>15</sup>

---

<sup>13</sup> “NVIDIA Announces Jetson Nano: \$99 Tiny, Yet Mighty NVIDIA CUDA-X AI Computer That Runs All AI Models,” *NVIDIA*, March 18, 2019, <https://nvidianews.nvidia.com/news/nvidia-announces-jetson-nano-99-tiny-yet-mighty-nvidia-cuda-x-ai-computer-that-runs-all-ai-models>.

<sup>14</sup> Anthony Spadafora, “Intel reveals first AI chips,” *techradar.pro*, August 21, 2019, <https://www.techradar.com/news/intel-reveals-first-ai-chips>.

<sup>15</sup> Ryan Smith, “The AI Race Expands: Qualcomm Reveals “Cloud AI 100” Family of Datacenter AI Interference Accelerators for 2020,” *ANANTECH*, April 9, 2019, <https://www.anandtech.com/show/14187/qualcomm-reveals-cloud-ai-100-family-of-datacenter-ai-inference-accelerators-for-2020>.

中國大陸公司部分，「華為」2018年首次發布的升騰910晶片，在2019年8月宣布即將上市，挑戰目前主導市場的美國「英特爾」及「輝達」。<sup>16</sup>「阿里巴巴」於9月該公司年度雲計算大會上，推出首次自行開發的晶片—含光800，不僅展現進入硬體市場的企圖，也試圖降低在美中貿易戰下，對於屬美國智慧財產權晶片的依賴。<sup>17</sup>

至於AI應用，真實環境的不確定性，仍然是機器人及自動駕駛車輛等技術進入實用階段的一大門檻，但透過遊戲已取得顯著進展。Google AI開發團隊DeepMind，在2019年1月發表針對即時戰略遊戲《星海爭霸II》(StarCraft II)開發的AlphaStar，並且在與遊戲公司合作下，讓AI以玩家身分與真人在官方歐洲地區的伺服器對戰。最終版的AlphaStar，在歐洲伺服器上的9萬名玩家中排名前0.15%。而在與該伺服器同等級的高階玩家的90場對戰中，已經能於61場勝出。<sup>18</sup>

《星海爭霸II》遊戲步調非常緊湊，玩家實質上面對的是一連串不間斷的複雜賽局問題。為克服《星海爭霸II》的複雜性，DeepMind採用多代理人增強式學習法(multi-agent reinforcement learning)進行訓練。正如人類玩家會透過與朋友共同針對特定策略彼此對戰，藉此找出自身弱點進行強化，DeepMind讓代理人彼此以特定策略對戰，即能讓AlphaStar設法從中學習到所有可能的策略模式，以及應對方式。<sup>19</sup>

雖然專家與評論多認為，短期內AlphaStar應無法完全超越所有人類對手，但DeepMind在此已經達成原先設定的目標，將使AI更能面對真實世界充滿不確定的開放性環境。而自AlphaStar取得的突破，亦可應用於決策支援系統以及軍事模式模擬系統中。

#### 四、量子運算

由於物理學限制現有半導體的運算模式，電腦進行運算的最小單元，僅會有0與1兩種狀態。然而，奠基於量子力學的量子運算，其量子位元(qbite)能容納無限多種的量子疊加態(quantum superposition)，故能夠同時執行巨量運算，以達到傳統電腦無法達到的速度，甚至在更短時間內，破解目前常用的RSA-2048等公鑰加密演算法(public-key encryption，又稱非對稱式加密)。因此，美、中均將量子運算視為能夠取得絕對技術優勢的關鍵，影響經濟發展與國家安全。<sup>20</sup>

---

<sup>16</sup> Arjun Kharpal, "Huawei launches A.I. chip as it looks to defy US pressure, pitting it against giants like Qualcomm and Nvidia," *CNBC*, August 23, 2019, <https://www.cnbc.com/2019/08/23/huawei-launches-ai-chip-ascend-910-pitting-it-against-nvidia-qualcomm.html>.

<sup>17</sup> Coco Liu and Cheng Ting-Fang, "Alibaba unveils AI chip to boost cloud plans and cut reliance on US," *Nikkei Asian Review*, September 25, 2019, <https://asia.nikkei.com/Business/China-tech/Alibaba-unveils-AI-chip-to-boost-cloud-plans-and-cut-reliance-on-US>.

<sup>18</sup> Dan Garisto, "Google AI beats top human players at strategy game StarCraft II," *Nature News*, October 30, 2019, <https://www.nature.com/articles/d41586-019-03298-6>.

<sup>19</sup> The AlphaStar Team, "AlphaStar: Grandmaster level in StarCraft II using multi-agent reinforcement learning," *DeepMind Blog*, October 30, 2019, <https://www.deepmind.com/blog/article/AlphaStar-Grandmaster-level-in-StarCraft-II-using-multi-agent-reinforcement-learning>.

<sup>20</sup> Jeremy Hsu, "The Race to Develop the World's Best Quantum Tech," *IEEE Spectrum*, January 9,

不過，美國國家科學院於 2018 年底所發布的研究報告《量子計算：進展與前景》(Quantum Computing: Progress and Prospects)，由 13 位美國量子計算領域專家共同主筆，對於量子計算前景進行評估，並對其發展前景持審慎態度。報告中指出，目前量子運算應用仍有許多技術困難尚待克服，包括量子位元容易受到電路噪音干擾、量子糾錯 (quantum error correction) 技術不成熟、<sup>21</sup>量子位元錯誤率高、量子計算所需之軟體及數據載入方法欠缺等，這些都將推遲量子計算及量子電腦的進一步發展。因此，該報告認為，近期內量子計算及量子電腦依舊處於技術探索階段，距推出具備普適應用價值的普及化量子電腦產品，恐仍有相當差距。並且就目前研發現況以及進程而言，在下一個十年內，研究團隊建造出能夠破解 RSA-2048 一類加密演算法的量子電腦可能性並不高。<sup>22</sup>

另一方面，Google 於 2019 年 10 月聲稱其在量子演算有重大突破，已經達到量子霸權 (quantum supremacy) 的門檻。理論上，在足夠時間下，傳統電腦能夠解決所有計算問題，而量子霸權則是指同一個定義良好的問題時，量子電腦運算錯誤率顯著降低，達到傳統電腦所無法達成的速度，因而在短時間解決傳統電腦無法計算的問題。Google 最新發表的研究成果指出，他們已成功製造出具有 53 量子位元數的量子處理器，其運算維度大約可達二的三十五次方 (約相當於 4.29GB)，能夠在 200 秒解決傳統超級電腦需要 10000 年才能計算出的問題。<sup>23</sup>

但同樣於量子運算投入大量研發資源的 IBM 則認為，處理器不等於完整的電腦架構，Google 在此誇大其研究成果，不過仍肯定 Google 在成功提升量子位元數上的技術突破。<sup>24</sup>而就公開訊息觀察，中國大陸量子電腦發展在此與美國仍有落差，但科學家表示若資源情況許可，應有希望於數年內趕上。<sup>25</sup>

## 參、兩用技術與技術擴散的威脅

兩用技術 (dual-use technology) 為同時具有軍民應用的科技，其出口、轉移一向為科技安全關注的重點。「索尼」(SONY) 的遊戲機 PlayStation 2，即為商用

---

2019, <https://spectrum.ieee.org/tech-talk/computing/hardware/race-for-the-quantum-prize-rises-to-national-priority>.

<sup>21</sup> 量子系統和環境容易因為量子糾纏 (quantum entanglement, 即量子相互作用後，僅能描述到整體系統之性質) 互相耦合，但在開放系統下，量子間的相干性會隨著時間消失，這表示量子所攜帶的訊息將會持續流失，此現象稱為量子退相干 (quantum decoherence)，亦是量子噪音的主要來源之一。量子糾錯即是透過檢驗錯誤來源，讓量子所傳遞的訊息得以克服噪音穩定傳輸的技術。詳細說明可參考 Devitt, Simon J, William J Munro, and Kae Nemoto. "Quantum Error Correction for Beginners." *Reports on Progress in Physics* 76.7 (2013): 076001.

<sup>22</sup> David Schneider, "The U.S. National Academy Reports on the Prospects for Quantum Computing," *IEEE Spectrum*, December 5, 2018, <https://spectrum.ieee.org/tech-talk/computing/hardware/the-us-national-academies-reports-on-the-prospects-for-quantum-computing>.

<sup>23</sup> Frank Arute et al., Quantum supremacy using a programmable super conducting processor. *Nature* 574, 505-510 (2019) doi:10.1038/s41586-019-1666-5.

<sup>24</sup> John Oates, "Google: We've achieved quantum supremacy! IBM: Nope. And stop using that word please," *The Register*, October 22, 2019, [https://www.theregister.co.uk/2019/10/22/ibm\\_poopos\\_google\\_quantum\\_claims/](https://www.theregister.co.uk/2019/10/22/ibm_poopos_google_quantum_claims/).

<sup>25</sup> 〈「量子霸權」來了，中國如何發力〉，《北京新浪網》，2019 年 10 月 25 日，<https://news.sina.com.tw/article/20191025/33076934.html>。

產品可能轉為軍事用途，並因此列為管制項目的一例。PlayStation 2 於 2000 年推出時，由於美製的中央處理器具備高階圖形處理能力，可用於飛彈導航系統，日本經濟產業省（以下稱為「經產省」）曾一度將 PlayStation 2 列入出口管制，限制出口至特定國家。當時日本的擔憂並非空穴來風，1996 年於韓國江原道的江陵市發生「江陵潛艇滲透事件」，在北韓特種部隊使用的鯊魚級潛艇（Sang-O submarine）上，即發現有大量來自日本的商規現貨（commercial-off-the shelf）通訊和導航設備。<sup>26</sup>較近期的案例，如美國發展高能雷射武器，也是基於既有工業雷射裝置進行改裝。<sup>27</sup>

在科技迅速發展後的技術擴散除了民用技術轉為軍事用途，更包括以政府經費資助，原為軍事目的開發，卻在民用領域持續發展的例子。雖然一般認為自動駕駛車輛是源自矽谷，但實際上最早是美國國防先進研究計畫署（Defense Advanced Research Projects Agency, DARPA）於 1960 年代開始的研究計畫。DARPA 為縮短軍民科技發展的落差，並希望能藉此促使機器人領域快速發展，以達到在 2015 年時，三分之一的地面部隊自動化的目標，DARPA 在 2004 年主辦自駕車挑戰賽 Grand Challenge，邀請美國國內團隊參與。由於國會授權 DARPA 直接與獲勝團隊合作，並有高額獎金，促使更多創新團隊加入挑戰，最終成為成長迅速、全球市場估值超過 500 億美金的自動駕駛產業。<sup>28</sup>

然而，技術擴散除使軍民應用間分野逐漸模糊，新形態管制項目出現，也成為科技管制體制的挑戰。無論是微處理器還是雷射，均為實體的管制標的，尚能依照其運算能力或是功率，制定分級管制規範並予以落實。但近年來，如此技術管制體制，對於新興科技發展卻顯得力有未逮。出口管制的核心，需要辨別三大要素：最終使用目的（end use）、使用者（end user）、地點（end location），並各自進行審查，對於非實體標的，如仍在快速發展階段的 AI 及網路安全相關軟體等科技，其應用範圍廣泛，不易進行定義，也增加討論新興科技在技術管制上的難度。

以 AI 為例，AI 結合無人機，已經發展出精準的商用無人物流服務，足以將物品送至特定地址，若更多行為者取得這樣的程式，即能以低廉的價格增強其作戰能力，如遠程精準打擊。因此這一類的無人機，在安全上可能有未知的風險。程式可以透過各種形式存在，包括未編譯的程式原始碼，或是編譯過的程式，並以橫跨實體儲存裝置及虛擬之網路空間進行傳遞，無論形式還是媒介均難以限制。若是將其部屬為雲端主機服務，究竟應如何界定其最終使用者或是地點，也是仍未有定論的問題。

---

<sup>26</sup> Peter Martin, "Could the Playstation 2 be used as nuclear weaponry," *ABC Local Radio PM Monday*, April 18, 2000, <https://www.abc.net.au/pm/stories/s119754.htm>.

<sup>27</sup> Kimberly Underwood, "Army Makes a Point of Putting Lasers on Vehicles," *SIGNAL*, December 1, 2019, <https://www.afcea.org/content/army-makes-point-putting-lasers-vehicles>.

<sup>28</sup> Alex Davies, "Inside the Races that Jump-Started the Self-Driving Car," *Wired*, November 11, 2017, <https://www.wired.com/story/darpa-grand-urban-challenge-self-driving-car/> 及 John Markoff "Military Lags in Push for Robotic Ground Vehicles," *New York Times*, September 22, 2013, <https://www.nytimes.com/2013/09/24/science/military-lags-in-push-for-robotic-ground-vehicles.html>.

對於技術擴散所產生的安全威脅，一般的因應作為可分為幾個層面：1.軍備控制條約；2.建立行為規範；3.刑事起訴；4.法律戰（包括專利保護相關訴訟）；5.出口管制。

過去軍備控制條約是限制相關科技散布的主要方式，但由於是國與國之間的協定，當對象是國家、且針對特定項目（如核武），較能有效率的發揮其作用，但以今日國際政治情勢而言，美、中、俄等國在概念上有明顯分歧，在軍備控制框架下討論新興科技可能已是緩不濟急。

行為規範雖然不具條約的國際法效力，但若能夠形成政治或道德上的約束，也可能成為有效的管制方向。例如《塔林手冊》（*Tallinn Manual*）針對國家於網路空間的作戰行為建立底線，並且在十年內由專家群針對近期發展進行更新，顯示就網路作戰而言，行為規範可能仍是一個有效途徑。

刑事起訴則多半是指竊取商業機密等行為，尤其在竊取本身即有刑責的情況下，實際上不僅能涵蓋未有規範的科技，對於參與個人或是公司，在有前科紀錄的狀況下，亦可能造成不易取得資金、或是在業界內留下不良名聲等隱性影響，也能對意圖竊取商業機密者產生一定程度的嚇阻力。至於法律戰及專利訴訟等，則是一般大型企業為保護其商業利益的必要手段，但在此同時亦可能間接嚇阻科技流出。

簡而言之，針對新興科技的技術管制，重新檢討各種手段，以克服科技快速發展與規範間的時間落差，以及了解科技可能應用的範圍，實有其必要性。其中最廣泛使用的出口管制，在美中之貿易戰的脈絡下，各國在近期已進行相當程度的修訂，必須就此獨立深入探討。

## 肆、科技管制體制之進展

2019 年由於中美貿易戰激化、日韓關係交惡、美國與伊朗之齟齬等國際政治層面的緊張態勢升高，美日歐等先進國家或地區大幅強化出口貿易及外國直接投資之管制體制。其主要目的是避免高科技產品或技術流入競爭對手或敵對國家，以確保該國或該地區之國家安全、產業發展和科技優勢。由於軍民兩用技術在軍事領域之應用逐漸增加，而實際的最後使用者（end user），如：極權國家或恐怖組織等可能透過種種方法，取得先進國家之重要技術或一般貨品而轉為軍事用途，強化高科技管制體制遂成為歐美日先進國家之共同課題。

以美國而言，面對中國大陸在科技發展上的追趕與挑戰，2019 年 5 月，商業部工業暨安全局（Bureau of Industry and Security, BIS）將擁有最多 5G 專利的中國大陸「華為」集團及其旗下 68 家企業，列入出口管制實體清單（entity list）；6 月 24 日又將中科曙光等 5 家研發產製超級電腦的中國大陸企業列入；8 月底，又列入了具有人工智慧人臉辨識技術等監視科技的商湯科技和曠視科技等中國大陸企業。

日本則是在日韓關係因徵用工判決等事件不斷惡化之背景下，<sup>29</sup>2019年7月4日起管制三項半導體生產之關鍵原料（含氟聚醯亞胺、光阻劑及蝕刻氣體）等出口至韓國，對韓國半導體產業造巨大衝擊，並間接影響韓國對中國大陸之半導體關鍵材料和零組件之供應；8月2日又宣布將韓國排除在原先進出口不必取得經濟產業大臣許可的「白色名單」外，使韓國成為第一個從日本「白色名單」除名的國家。

歐盟在2019年3月發布《歐盟議會與理事會第2019/452號規章》(Regulation 2019/452 of the European Parliament and of the council of 19 March 2019: establishing a framework for the screening of foreign direct investments into the Union)，建立外國對歐盟直接投資審查之總體架構。<sup>30</sup>其主要背景也是基於中國大陸企業近年來在歐洲各地以研發補助、投資或併購等方式，取得先進國家的企業經營權和新興技術等行為。在此之前，國際間的出口管理機制主要針對傳統武器和大規模毀滅性武器之擴散。既有的4個主要管制機制，分別是：管制傳統武器的《瓦聖納協定》(Wassenaar Arrangement)、管制核子兵器的核能供給國集團(Nuclear Suppliers Group, NSG)、管制生化兵器的澳大利亞集團(Australia Group)，以及管制飛彈技術的飛彈技術管制體制。各管制體制依據國際條約或協定組成並運作，參與國家也都遵守相關的國際規約，是傳統型的武器出口管制機制。

然而，2019年歐美日等先進各國對出口管制卻與以往有顯著的不同。第一，管制焦點集中在防止大規模毀滅性武器擴散的全面管制(catch-all control)上，特別是對軍民兩用技術或貨品之管制(dual-use regulation)。全面管制是美、英、德等國為了加強防止大規模毀滅性武器之擴散，在原本列為國際管制對象的貨品和技術之外，規定業者只要知悉其出口貨品或提供之技術被用於大規模毀滅性武器之開發等用途，就必須依法申請進出口許可。第二，管制對象從以往的成熟技術之應用，轉為新興技術、基礎技術(foundational technology)，或關鍵技術。因此，包括：人工智慧、生物科技(bio-technology)等都成為被管制的對象。

政府加強科技管制，特別是對新興技術之管制，無疑將增加國內產業界之因應負擔，並影響大學等學研機構研發創新之進展。因此，無論美國、日本還是歐盟，加強科技管制都引發該國或該地區學研界和產業界的高度關心和討論。至目前為止，各國科技管制體制仍在建立或發展中，全球也尚未建立起一致的國際管制架構。

以下分別就美國、日本和歐盟之科技管制體制進行說明。

---

<sup>29</sup> 南韓最高法院於2018年10月判決，日本企業須為二次大戰期間徵用南韓工人給予賠償。對此，日本政府聲稱，日韓兩國1965年恢復邦交時簽署的《日韓請求權協定》，已解決南韓勞工請求權問題，南韓民眾不能再向日方索賠。

<sup>30</sup> “Document 32019R0452: Regulation 2019/452 of the European Parliament and of the council of 19 March 2019: establishing a framework for the screening of foreign direct investments into the Union,” <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0452>.

## 一、美國

美國之國家安全貿易管理體制，主要分為三個系統進行。一般貨品出口管制，依據《出口管制改革法》(Export Control Reform Act, ECRA)及其下的《出口管理規則》(Export Administration Regulations, EAR)，由商務部負責；武器品項出口管制，依據《武器出口管制法》(Arms Export Control Act)下的《武器貿易管制條例》(International Traffic in Arms Regulations, ITAR)，由國務院負責；至於對伊朗、俄羅斯、委內瑞拉等特定國家或區域之經濟制裁，則由美國財政部外國資產管理局 (Office of Foreign Assets Control, OFAC) 負責。

川普總統上任後，除了在 2017 年 8 月宣布國家緊急狀態宣言之外，更引用 1977 年成立的《國際緊急經濟權力法》(International Emergency Economic Powers Act, IEEPA)，以行政命令加強對科技出口之管制。2018 年 8 月，美國將《外國投資風險審查現代化法案》(Foreign Investment Risk Review Modernization Act, FIRRMA) 和《出口管制改革法》併入《2019 年度國防授權法》(NDAA 2019)<sup>31</sup>並進行制度改革，希望從科技出口管制、外國對美直接投資管制、學研機構之保護與管制等方面，防範具有國防及國家安全顧慮之新興技術流出。

### (一) 科技出口管制

#### 1. 新興技術首度列為出口管理之內容

《出口管制改革法》是美國戰後首度對「新興且基礎技術」(emerging and foundational technologies) 進行出口管制，並將進出口許可證核准與否之關鍵設為「是否對美國國防產業基礎帶來顯著的負面影響」。

美國出口管制清單主要分為三類，分別是：拒絕人員清單 (Denied Persons List, DPL)、未經驗證清單 (Unverified List, UVL) 和實體清單 (Entity List, EL)，並以實體清單之管制最為嚴格。實體清單源自老布希總統 1990 年提出的「增強擴散控制倡議」(Enhanced Proliferation Control Initiative, EPCI)，並於 1997 年首次公布。所謂「實體」包括：企業、研究機構、政府、民間組織、個人、法人等。列入之主要理由是「威脅美國國家安全和外交利益」。<sup>32</sup>

依據《出口管制改革法》下的《出口管理規則》，美國商業部工業暨安全局 (BIS) 製作出商業控制清單 (Commerce Control List, CCL)，並編列「出口管制分類編碼」(Export Control Classification Number, ECCN)。列入清單之新興技術，無論是從美國出口至管制國家、從美國以外的國家轉手出口至管制國家，或在管制國家國內供應或販售《出口管理規則》所管制之品項，都必須事先申請並獲得美國商業部工業暨安全局許可。但實際上通常不被美國商業部工業暨安全局核准。因此，美國 2019 年將「華為」等多家中國大陸企業列入清單，等於全面禁止美

<sup>31</sup> FY2019 National Defense Authorization Act (H.R.5515), pp.18-19, <https://fas.org/sgp/crs/natsec/R45816.pdf>.

<sup>32</sup>“Overview of U.S. Export Control System,” State.Gov., <https://2009-2017.state.gov/strategictrade/overview/index.htm>; 劉昱辰，〈美國對中國大陸的進出口管制措施〉，《經濟前瞻》第 185 期，2019 年 9 月，第 27-32 頁。

國高科技產業與「華為」等中國大陸企業之貿易往來，近乎全面斷供。

## 2. 滾動調整對列管技術之界定

《出口管制改革法》也要求美國政府商業部、國防部、能源部、國務院及其他相關政府機關，對於具美國國家安全重要性的新興且基礎技術，必須定期且持續地調整其界定，而且每隔 180 天要向「美國外來投資審查委員會」(Committee on Foreign Investment in the United States, CFIUS) 和國會提出書面報告。

據此，美國商業部工業暨安全局在 2018 年 11 月 19 日公告所謂「新興技術」之定義和認定標準等，並展開為期 30 天的公開評論。BIS 所界定的「新興技術」有 14 個領域，包括：生物科技、人工智慧及自動學習、定位定時導航、微處理器、先進演算、數據分析、量子通訊與感測、物流技術、積層製造(3D 列印等)、機器人、腦機介面、極音速、先進材料、先進監視技術等。<sup>33</sup>這些軍民兩用技術若應用在軍事用途上，可大幅提升軍事作戰能力，對美國國家安全極具重要性。

### (二) 外國對美直接投資之管制

#### 1. 擴大審查外國投資人之其他投資行為

另一方面，針對外國對美直接投資，《外國投資風險審查現代化法案》將「美國外來投資審查委員會」之審查對象，從原本的併購／買收行為，擴大到「外國人士」的「其他投資行為」。這些投資行為包括：(1) 對非公開資訊之接近；(2) 擔任企業主管或準主管職位；(3) 利用／收集／保有／揭露美國人民之機敏個資；(4) 利用／開發／獲得／揭露關鍵技術；(5) 管理／運用／製造／供給關鍵基礎設施等。其中，所謂「關鍵技術之利用、開發、獲得與揭露」，具體而言是指關鍵技術之生產、設計、測試、製造、改變或開發。<sup>34</sup>

#### 2. 列管之關鍵技術擴大至新興且基礎之技術

所謂的「關鍵技術」，除了美國《武器貿易管制條例》和《出口管理規則》管制清單上所列的技術之外，還包括前述《出口管制改革法》規定的「新興且基礎之技術」。如前所述，美國商業部工業暨安全局公布了 14 項「新興且基礎之技術」之領域，但是具體的管制內容尚未明確公布。

#### 3. 擴大外國人士之界定範圍

至於「外國人士」之定義，《2019 年國防授權法》委由「美國外來投資審查委員會」界定。依據《外國投資風險審查現代化法案》，所謂「外國人士」不只限於外國法人和外國自然人，還包括受外國自然人或外國政府控制的美國法人，即使該當外國人或外國政府之持股比率未滿 50%，也包括在「外國人士」之範圍內。

### (三) 學研機構之保護與管制

此外，為了防止國家安全相關技術從大學和研究機構流出，並避免研究者受

<sup>33</sup> “Review of Controls for Certain Emerging Technologies,” *Federal Register*, Vol.83, No.223, November 19,2018, <https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies>.

<sup>34</sup> 顏慧欣，〈美國外人投資審查機制之改革方向與影響〉，中華經濟研究院 WTO 及 RTA 中心，2019 年 1 月 17 日，<https://web.wtcenter.org.tw/Page.aspx?pid=318503&nid=251>。

到不當影響或安全威脅，《2019 年度國防授權法》提出對研究者提供國家安全保護的倡議。

該法第 1286 條規定，國防部長在與其他相關政府機關協議後，應與從事國防相關研發活動之大學、研究機構、其他教育或研究組織合作，提出確保以下 3 項目標之政策倡議：1. 支援對智慧財產權、列管資訊、核心人才、與國家安全有關之關鍵技術的保護；2. 管制外國對於國防部研究下之美國技術、科技、創新型企業的不當利用和影響（包括外國的人才計畫）；3. 支援相關科學與研發領域之美國人才的發展。更具體的措施則包括：1. 建立對美國基礎研究、科技應用、創新型企業安全構成威脅的資訊交換論壇或基礎；2. 支援學研機構防範人才被不當影響之安全措施和教育訓練；3. 評估國防相關計畫之研究者是否參加外國之人才交流計畫或專家聘任計畫；4. 強化與學研機關在保護關鍵技術和防範外國諜報活動之合作等。在此倡議下建立共識並設立規則，大學等學研機構或其研究者若違反規定，國防部應限制或停止對其之經費支持。

## 二、日本

日本的科技管制體制也是分為「技術出口管制」、「外國直接投資管制」和「學研機構管制」三方面進行。

### （一）技術出口管制

日本出口管制即國家安全貿易管制，主要依據《外幣匯兌及外國貿易法》（以下簡稱「外匯法」），加上政府相關部門之行政法令，來管理貨物出口及對外之技術提供。管理貨物出口之行政法令，主要是《出口貿易管理令》，而管理技術出口之行政法令，則是《外幣匯兌令》（以下稱「外匯令」）。此外，還有各省依據《出口貿易管理令》和《外幣匯兌令》制訂的部會法令（稱為「省令」），以及針對國防裝備出口至海外的《防衛裝備移轉三原則》。<sup>35</sup>

#### 1. 清單管制和全面管制

管制方法主要分為「清單管制」和「全面管制」。清單管制之對象是政令及省令規定之品項，如：武器、具敏感性的多用途貨品（核能、生化武器、飛彈之相關品項，新興技術材料、工具機等），適用範圍遍及全球所有地區，一經列入清單即完全禁止出口。全面管制之管制對象則為清單管制品項以外的所有品項，並分為大規模毀滅性武器和傳統武器兩大類，若要出口至列管國家或地區，必須有經濟產業大臣之許可。其中，大規模毀滅性武器出口全面管制的例外地區，是包括韓國在內的 27 個「白色名單」國家。這些國家因為參與出口管制之國際體制，遵照國際規約實施嚴格的出口管制，獲得日本政府信賴，不列在全面管制範圍之內。

#### 2. 技術出口之認定

技術出口（對外提供技術）和貨品出口最大的不同之點，在於技術出口不受

<sup>35</sup> 經濟產業省貿易管理部，〈安全保障貿易管理について〉，日本經濟產業省網站，2019 年 8 月，[https://www.meti.go.jp/policy/anpo/seminer/shiryo/setsumei\\_anpokanri.pdf](https://www.meti.go.jp/policy/anpo/seminer/shiryo/setsumei_anpokanri.pdf)。

所在地點限制，而技術提供的形式主要有「技術資料」和「技術支援」兩種。例如：日本接受外國人士（非居住者）以「研修員」身份赴日進修，並在日本國內給予技術指導，而後外國人研修員以電子郵件或返國行李將技術資料傳回或帶回母國，即算是技術出口。此外，日本也可向外國提供在當地進行的技術指導或技術支援，如：技能培訓、提供操作知識、諮詢顧問等，這些也都算是技術出口。因此，針對特定技術，若是以日本居住者向非居住者提供技術為目的、以在外國當地提供為目的，或是將特定技術帶出日本、以電子郵件向外國傳送特定技術之電子數據，這些都需要日本政府之許可。上述之「日本居住者」並不限於日本國籍，也包括駐日外籍人士和外國企業之日本分公司，而「非居住者」除了日籍駐外人士之外，還包括日本企業之外國分公司等，規定可說非常詳細。

### 3. 列管技術之界定

至於被管制之技術，主要是指管制清單所列貨物之相關技術，但是非管制貨品之製造技術也有可能成為管制對象。日本在政令《外匯令》「附表」中載明被管制之技術，而相關省令中則載明管制技術之規格。被管制技術之範圍涵蓋該項貨品的全部產製階段，分為：製造前的「設計」階段、「製造」的全部過程，後段的「使用」階段。「設計」階段之技術，包括：設計研究、設計分析、設計概念、產品原型的製作與測試、試品生產計劃、設計資料、將設計資料轉為產品之過程、外觀設計、綜合設計、規劃圖等。「製造」階段之技術則包括：建設、生產工程、產品化、整合、組裝／組合、檢查、測試、品質保證等。至於「使用」階段之技術，則包括：操作、安裝、維護（安檢）、修理、翻修、分解修理等。特別是可達到或超越管制之性能水準、特性或機能之技術，被視為重點列管之「必要技術」，更是不能輕易外流。

#### （二）外國對日直接投資之管制

##### 1. 增加外來直接投資事先申報之業種

為了防止國家安全方面重要技術之流出，以及損害日本防衛生產與技術之基礎，日本財務省與總務省於2019年5月27日公告《外匯法》所定外國對日直接投資需事先申報之對象業種追加名單，並於2019年8月1日起實施。<sup>36</sup>新增的事先申報業種共有20個，主要分為三類：

(1) 資訊處理相關機器或零組件製造業：積體電路製造業、半導體記憶體製造業、光碟/磁碟/磁帶製造業、電子回路板製造業、有線通訊機器器材製造業、行動電話/PHS 電話機製造業、無線通訊機器器材製造業、電子計算機製造業、個人電腦製造業、外部記憶裝置製造業。

(2) 資訊處理相關軟體製造業：受託開發軟體業、軟體整合業、包裹軟體業。

(3) 資通訊服務相關產業：地區型電信業、長距離電信業、有線廣播業、其他固定

<sup>36</sup> 〈对内直接投資等に係る事前届出対象業種の追加等を行います〉，日本財務省網站，2019年5月27日，  
[https://www.mof.go.jp/international\\_policy/gaitame\\_kawase/gaitame/recent\\_revised/20190527.htm](https://www.mof.go.jp/international_policy/gaitame_kawase/gaitame/recent_revised/20190527.htm)。

電信業、移動電信業、資訊處理服務業、支援網路利用之產業等。<sup>37</sup>

這些產業幾乎都是 IT 領域的主要投資對象，日本政府擴大外國投資人取得國內企業股份時必須事先申報之範圍，目的是將資通訊產業設為關鍵產業並予以保護。但是，軟體開發業和資訊處理服務業是科技創新之主要領域，其間企業幾乎都是新創公司，大多需要外國創投基金之投入。<sup>38</sup>因此，日本政府擴大外國直接投資事先申報之管制範圍，引發外資圈和創投圈高度關注。

## 2. 擴大外來直接投資事先申報之範圍

日本《外匯法》修正案已於 2019 年 10 月 18 日在內閣會議中通過，正送往國會審議中，預計 2020 年開始實施。<sup>39</sup>該修正案之主要內容，是對於有國家安全顧慮之產業，強化對其外來直接投資之監視，而對於以資產運用而非參與經營為目的、沒有國安顧慮之產業，則導入其外來直接投資免除事先申報之制度。

依據《外匯法》，原本外國企業或外國投資人取得日本國內上市企業股票達 10% 時才需事先申報，修正案將標準設為 1%，並特別針對可能威脅日本國家安全之外資投資行為，例如：來自外國國有企業之投資，以及對日本核能、武器製造、電力、通訊等有國家安全顧慮產業之外來投資。

此一修正內容使外國直接投資之事先申報標準更加嚴格化，並大幅擴大日本政府對外國直接投資之監視範圍。修法之主要目的是防止日本企業的重要技術流往國外，同時配合出口管制體制之改革方向進行調整。日本出口管制體制向來依循國際管制架構來設定管制對象，但鑑於歐美分別在 2019 年強化高科技出口管制，日本也將其生物科技、人工智慧等先端技術列為保護重點，未來將依據日本國情設計其出口管制體制。<sup>40</sup>

### (三) 學研機構之管制

日本身為世界技術先進國家，對於學研機構重要技術流出管制原已相當完善，主要是針對大量破壞兵器相關技術提供之管理。由於學者在學術雜誌之論文投稿或學術會議之發表等技術公開之行為，不需要經濟產業大臣之許可，但是，大學或研究機關接受海外人員赴日研修、參與國際共同研究，或是研究人員赴海外出差、將量測機器或試驗材料等貨物或技術資料等，依據《外匯法》則需事先獲得經濟產業大臣之許可。為免學界人士不慎觸法，日本自 2006 年開始強化對大學

<sup>37</sup> 〈追加等する業種〉，日本財務省網站，

[https://www.mof.go.jp/international\\_policy/gaitame\\_kawase/gaitame/recent\\_revised/kokuji.pdf](https://www.mof.go.jp/international_policy/gaitame_kawase/gaitame/recent_revised/kokuji.pdf)。

<sup>38</sup> 這些外國創投基金主要來自美國，但也包含來自中國大陸或其他國家。例如：2016 年成立的「軟銀願景基金」(Softbank Vision Fund)，規模達 1,000 億美元，資金來源主要是沙烏地阿拉伯的公共投資基金和阿布達比的投資公司，出資比例超過 60%。

<sup>39</sup> 占部繪美，〈外資規制の改正案を閣議決定—安保分野の監視強化と審査簡素化〉，

《Bloomberg》，2019 年 10 月 18 日，<https://www.bloomberg.co.jp/news/articles/2019-10-17/PZI3Z1DWX2PX01>。

<sup>40</sup> 〈安全保障技術で外資規制強化へ：株取得届け出 1% から〉，《共同通信》，2019 年 10 月 8 日，<https://this.kiji.is/554225355401643105>；Min Jeong Lee, "A \$3.4 Billion Hedge Fund Is Let Down by Japan on Foreign Buying Rules," *Bloomberg*, October 15, 2019, <https://www.bloomberg.com/news/articles/2019-10-14/a-3-4-billion-hedge-fund-let-down-by-japan-on-foreign-buying>。

和公共研究機關之出口管理體制。近年來，基於國際間對敏感技術管制之重視和《外匯法》之修正，經產省在 2017 年頒布新改訂之《安全保障貿易相關敏感技術管理指導方針（大學、研究機關用）》，<sup>41</sup>並委託文部科學省發佈給各大學和公共研究機關。同時，經產省也自 2017 年度在全國各大學舉辦安全保障貿易說明會，並派遣顧問至各大學協助。

依據該指導方針，經產省明訂出與《外匯法》管制深度相關的主要技術領域，分別是：核能、精密機械、自動控制／機器人、化學、生物醫學、高性能材料、航太與高性能發動機、航行方法、海洋、資通訊／電子／光學、列管貨品之設計／製造／使用等程式開發、模擬程式技術等。但是，主要考量仍是基於防止大量破壞兵器之擴散，並非近期的防範尖端科技之流出。<sup>42</sup>

### 三、歐盟

#### （一）外國直接投資之管制

歐盟對於外國直接投資之管理，基本上並不設定特殊管制，但是具戰略價值的重要產業和技術之外國直接投資則必須接受審查。如前已述，歐盟於 2019 年 3 月提出《歐盟議會與理事會第 2019/452 號規章》，首度建立審查外來直接投資之總體架構。其立法背景主要因為中國大陸自 2008 年起不斷以國家資金進行對外直接投資，透過研發補助、投資或併購等方式，取得歐洲先進國家的新興技術、擁有軍民兩用技術之企業和戰略性的基礎設施。

中國大陸併購歐盟地區企業最具指標性的案例，是中國大陸「美的」集團於 2016 年以 12 億歐元收購德國工業機器人製造大廠「庫卡」(KUKA AG)，取得 94.55% 之股權和經營權。為此，德國政府於 2017 年向歐盟提出申訴，並修改《德國對外經濟條例》(Außenwirtschaftsverordnung, AWV)，規定外國企業收購德國企業股份若超過 25%，即需獲得當地政府之批准，其後又將標準降為持股 10%。基本上，外資進入德國市場之條件和德國國內企業一致，但是對於銀行、保險、藥品、發電和運輸等產業之外國直接投資，則需要德國政府特別審核。

英國於 2017-2018 年之間陸續強化對外資在國家安全和基礎設施之投資審查，並於 2018 年 7 月發布《國家安全與投資》(National Security and Investment) 白皮書，擴大英國政府對外資安全審查之範圍。在科技管制方面，英國政府主要管制外資對軍民兩用產品、電腦硬體和量子技術之投資。法國則於 2014 年 4 月修改其外來投資規定，對於具敏感性或受保護之數據儲存、網路安全、人工智慧、半導體、軍民兩用技術等領域設下限制。

歐盟 2019 年 3 月建立的外來直接投資審查制度，主要審查對象除了外國企

<sup>41</sup> 日文為：《安全保障貿易管理に係る機微技術管理ガイダンス(大学・研究機関用)》，第一版於 2008 年頒佈、第二版於 2010 年頒佈，2017 年為第三版。

<sup>42</sup> 經濟產業省貿易管理部，《安全保障貿易管理に係る機微技術管理ガイダンス(大学・研究機関用)》第三版，第 30 頁，2017 年 10 月，日本經產省網站，[https://www.meti.go.jp/policy/ampo/law\\_document/tutatut07sonota/t07sonota\\_jishukanri03.pdf](https://www.meti.go.jp/policy/ampo/law_document/tutatut07sonota/t07sonota_jishukanri03.pdf)。

業和投資人之外，也包括來自特定國家國營企業之不透明投資，以及關係外國直接投資的 EU 大型計畫等。具體的審查領域，除了歐洲議會原先通過的「關鍵基礎設施」：水資源、醫療/健康、國防、媒體、生物科技、食品安全之外，再加上能源、運輸、通訊、資料數據、航太、金融、新興技術等。其中的「新興技術」主要指：半導體、人工智慧、機器人。

依據該規章，歐盟也將在歐盟執委會和會員國之間設立外來投資相關資訊交換和警示的合作機制，並與國際分享投資審查制度之最佳實踐和投資趨勢等資訊。但是，基於歐盟體制之特殊性，各會員國未來是否導入此管制制度，或是維持該國現有之投資審查制度，則由各會員國基於國家安全之考量自行判斷。各國國內特定外來投資案之批准與否，最終仍由各會員國自行決定。

此外，外國對歐盟地區直接投資若是橫跨二個以上之會員國，並產生國家安全或公共秩序之顧慮時，或是可預測將影響歐盟之整體利益時，如：參與歐盟大型研發補助計畫「地平線 2020」(Horizon 2020)，或是參與歐洲衛星定位系統「伽利略」(Galileo) 等，歐盟執委會都可提出意見書來進行干預。

## (二) 出口管制

歐盟對於可應用於軍民兩用和大規模毀滅性武器之物品、一般商品、軟體和技術之出口管制，主要依據國際管制架構和《歐盟理事會第 428/2009 號規章》(Council Regulation (EC) No 428/2009 of 5 May 2009)，並於 2013 年開始實施。為了因應全球情勢變化和各方面之挑戰，2014 年起歐盟內部有出口管制應與時並進加以調整之聲音，要求制訂具體政策和重新檢討歐盟出口管制機制。

歐盟法規雖然已對軍民兩用貨物之出口管制提出總體架構，具體的法律規定和政策執行仍委由各會員國決定。因此，歐盟內部對於軍民兩用貨品之出口管制，實際上呈現多頭馬車、各自為政的狀態，沒有統一的標準認定，也沒有特定的歐盟機構來負責。歐盟議會現正在進行對歐盟軍民兩用出口管制系統之檢討和法令修正之研究。<sup>43</sup>至於科技出口管制，歐盟內部對於「技術出口」如何界定？與「技術協助」有何不同？哪些技術應納入出口管制？尚未得出共識，技術出口管制主要依賴各大公司內部法令遵從機制。目前歐盟內部正在討論其高科技出口管制，並聚焦於歐洲領先全球之新興技術，如：人工智慧、機器人、半導體、網路安全、奈米科技和生物科技等。<sup>44</sup>

美國、日本、歐盟三方於 2019 年 5 月同意就防範技術強制轉讓、國家安全投資審查、出口管制等方面進行合作，並強化相關新規則之制訂和執法。目前美、日、歐三方科技管制體制進展之比較，可整理如表 3-1 (見頁 49)。

<sup>43</sup> European Parliament Research Service, "Review of dual-use export controls," *European Parliament*, [http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS\\_BRI\(2016\)589832](http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)589832).

<sup>44</sup> Philip Haellmigk, "The concept of European export controls on technology transfers: Risks and strategies for international companies," *World Customs Journal*, Volume 13, Number 1, pp.21-30.

## 伍、小結

綜合以上各節之探討，本章可歸納出結論如下。首先，對於關鍵技術之定義，先進各國逐漸形成共識，並以高能雷射、極音速打擊、人工智慧、量子運算為主要的共同項目。第二，軍民兩用技術之擴散，雖可能產生安全威脅，但同時亦能促進科技創新和提高經濟價值，而新興技術對既有技術管制體制形成的挑戰，將是未來關注重點。第三，為防範高技術流出，美國、日本、歐盟今（2019）年都加強對關鍵技術之管制，從出口管制、外來投資管制，到對學研機關之規範，管制方法和措施均逐漸細膩化。

科技安全雖日益受各國政府重視，並仰賴國際合作，但仍屬於國家安全和經濟發展議題之前段，而後段之市場應用和產業發展，由於其龐大規模和潛在效益，將使產業安全成為繼科技安全之後必須重視之課題。

表 3-1、美國、日本、歐盟目前科技管制體制進展之比較

	美國	日本	歐盟
主要法規依據	《2019 年度國防授權法》《出口管理改革法》《外國投資風險審查現代化法案》	《外幣匯兌及外國貿易法》《出口貿易管理令》《外幣匯兌令》	《歐盟議會與理事會第 2019/452 號規章》
主要主事機關	商業部工業暨安全局	經濟產業省	歐盟執委會
列管技術之內容(暫)	生物科技、人工智慧及自動學習、定位定時導航、微處理器、先進演算、數據分析、量子通訊與感測、物流技術、積層製造(3D 列印等)、機器人、腦機介面、極超音速、先進材料、先進監視技術	以管制清單所列貨物之相關技術為主，涵蓋其設計、製造、使用階段之全部技術	正在討論中，可能是歐洲領先全球之新興技術：人工智慧、機器人、半導體、網路安全、奈米科技和生物科技
管制方法	技術出口管制	1. 清單管制和全面管制 2. 技術出口之認定 3. 列管技術之界定	軍民兩用貨品之出口管制，各自為政；技術出口管制尚在研議中
	外來直接投資管制	1. 擴大審查外國投資人之其他投資行為 2. 擴大列管技術至新興且基礎之技術 3. 擴大外國人士之界定範圍	2019 年建立審查外來直接投資之總體架構，但核准與否仍由各會員國自行決定
	學研機構之保護管制	支援對智慧財產權、列管資訊、核心人才、國安相關技術的保護	N/A

資料來源：王綉雯整理自公開資料。

(責任校對：許智翔、姚宇庠)