2019 評估報告
國防科技趨勢

主編 蘇紫雲 吳俊德

財團法人國防安全研究院

本頁空白

2019 國防科技趨勢評估報告

主編　蘇紫雲 吳俊德

財團法人國防安全研究院

2019 年 12 月

本頁空白

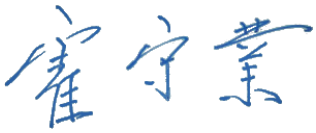
序

2019 年是財團法人國防安全研究院成立後，第一個完整的年度。本院研究同仁在國安會、國防部、外交部、陸委會等相關部會的協助下，致力於研究國防及安全各項重大議題。2019 年，本院在國內承接委託研究案、辦理研討會、年度國防安全論壇，並赴印度、美國、英國、法國、新加坡、德國等國，出席國際研討會、對話座談及各式專業活動，與當地重要智庫學者及專家，進行深度互動交流。

目前政府推動的國機國造、國艦國造可說是重大的國家政策，一方面可滿足國防的需求，同時預算的投入可發揮經濟加乘效果，帶動產業升級與創造就業。台灣的電子產業、精密機械等也是關鍵供應鏈，特別是軍規固態電子、軍規半導體等在全球的軍事裝備中，都處於不可或缺的地位。此外，美國對於敏感科技與產業的安全管理趨勢，以及我國國防產業如產品與供應鏈安全的強化，將可掌握未來市場需求，確保國防安全並同時創造經濟競爭力。

我們希望研究同仁都能按照自己的專長，針對相關課題深入觀察，並透過各種研討、座談、拜會及內部討論，與國內外各界學者專家相互學習討論推敲。本院的三本年度報告—「印太區域安全情勢評估」、「中共政軍發展評估」、「國防科技趨勢評估」是本院同仁這一年來的部分努力成果。這三本報告既反映個別同仁的觀點，也是集體討論切磋後的產物。我們希望透過這三本報告，對上述重要議題提出本院的觀點與見解，疏漏與不成熟之處在所難免，期待各界先進不吝指教。

董事長



中華民國 108 年 12 月 6 日

本頁空白

2019 國防科技趨勢評估報告作者群

主編

蘇紫雲（國防資源與產業研究所 副研究員）
吳俊德（網路作戰與資訊安全研究所 助理研究員）

作者（依姓名筆畫順序）

王綉雯（國防資源與產業研究所 博士後研究）
杜貞儀（網路作戰與資訊安全研究所 博士後研究）
吳俊德（網路作戰與資訊安全研究所 助理研究員）
洪瑞閔（國防資源與產業研究所 博士後研究）
曾怡碩（網路作戰與資訊安全研究所 助理研究員）
許智翔（先進科技與作戰概念研究所 博士後研究）
舒孝煌（先進科技與作戰概念研究所 助理研究員）
蔡榮峰（國防資源與產業研究所 政策分析員）
蘇紫雲（國防資源與產業研究所 副研究員）

編輯與校對（依姓名筆畫排序）

吳宗翰 （網路作戰與資訊安全研究所 博士後研究）
蘇翊豪 （網路作戰與資訊安全研究所 博士後研究）

本頁空白

摘要

蘇紫雲、吳俊德

國防科技趨勢評估報告為國防安全研究院的年度型報告，2019 年度的主題為國防產業之安全機制，一方面是與 2018 年度以軍事科技發展的主題作區隔，其次是針對美中貿易科技戰將使國防產業與高科技供應鏈之安全成為競爭力核心，更可配合我國《國防產業發展條例》的實施，以前瞻科技市場的政策評估，期望能提出具體且實用的政策參考。

2019 國防科技趨勢評估報告內文架構分為三篇七章，分別是美中貿易科技戰的深度分析、科技安全管理接軌國際市場、以及未來戰場科技需求與台灣國防自主等面向進行探討。

第一篇主題是對美中貿易科技戰的評估，共有兩章。第一章是從戰略經濟的角度來解析美中兩國傳統霸權與崛起強權的競爭，敘述貿易戰形成的原因、科技戰因軍備競賽而激化、以及美國試圖壓制中國的各種手段。第二章是科技冷戰，首先指出科技冷戰的本質，其次以中國大陸通訊設備大廠華為為例，說明在資通訊產業這個科技戰的主要戰場上，美國與華為如何較勁，而其結果將會造成科技兩極體系，也就是民主科技聯盟對抗非民主陣營。

第二篇主題是科技與產業的安全控管，由於近年中國大陸以各種方式獲取或竊盜美國關鍵技術，安全議題成為國防科技趨勢的焦點。本篇分為兩章，第三章討論科技安全，首先說明近年來關鍵技術的重點發展項目，由於這些技術多為軍民兩用，因此技術與產品擴散，必須藉管制機制才能避免對國家安全與產業競爭力的威脅。第四章聚焦國防產業安全，以美國為例，介紹運用關鍵技術的商品從製造到銷售的過程中，為防範技術外流的各個面向與規範，分別為審查外資併購的投資審議機制、公司內部的安全治理、生產流程中的供應鏈安全、以及銷售給最終使用者之前的安全認證。其中許多規範都在 2018 年至 2019 年進行改革，部分施行細則尚在研擬階段。

第三篇主題是未來戰場趨勢與台灣國防產業，分為三章。第五章著重創新作戰，陳述當前國際環境下的大國衝突樣態，且未來戰場是多領域協同進行，軍事與非軍事衝突的界線愈來愈模糊，呈現混合戰形式。以不對稱作戰概念且思維上不斷創新，才能抵銷強權在傳統武力上的龐大優勢。第六章則是介紹新興關鍵技術在武器系統上的應用，包括雷射與導能武器、極音速與長程打擊武器、AI 與無人載具、以及未來發展趨勢。第七章則是對台灣國防自主的評估，首先點出國防自主對台灣的安全與產業意義重大，而參酌其他國家經驗，台灣要發展國防自主，要從利基生產切入並擴大在地廠商參與。然而，台灣也面臨許多的挑戰，技術取得、安全控管、尋求出口以及穩定財源支持將會是必須克服的挑戰。

本頁空白

目錄

序.....i
2019 國防科技趨勢評估報告作者群.....iii
摘要.....v
表目錄.....ix
圖目錄.....x
專有名詞中英文對照.....xi
緒論.....1
第一篇 貿易科技戰的評估.....3
第一章 美中戰略與經濟的矛盾 蘇紫雲.....5
壹、前言.....5
貳、貿易戰的形成.....6
參、美中軍備競賽激化產業科技戰.....10
肆、複合模式抑制中國.....13
伍、小結.....17
第二章 科技冷戰 曾怡碩.....19
壹、前言.....19
貳、科技冷戰的本質.....19
參、華為模式：圍堵與反圍堵.....20
肆、民主科技聯盟 vs.中俄非民主陣營.....25
伍、小結.....27
第二篇 接軌國際安全市場：科技與產業的安全控管.....29
第三章 科技安全 王綉雯、杜貞儀.....31
壹、前言.....31
貳、關鍵技術之發展.....31
參、兩用技術與技術擴散的威脅.....37
肆、科技管制體制之進展.....39
伍、小結.....48
第四章 國防產業安全 吳俊德、蔡榮峰.....51
壹、前言.....51
貳、投資審議與安全評價機制.....51
參、公司安全治理與廠商分級.....54
肆、生產流程與供應鏈安全.....60
伍、終端市場及安全認證.....63
陸、小結.....69
第三篇 未來戰場趨勢與台灣國防產業.....71
第五章 創新作戰 舒孝煌、許智翔.....73

壹、前言.....73
貳、新型態大國衝突環境與未來戰爭趨勢.....73
參、多領域化的未來戰場.....76
肆、混合戰與非軍事衝突.....78
伍、創新思維與不對稱作戰.....81
陸、小結.....85
第六章 科技趨勢　舒孝煌、許智翔.....87
壹、前言.....87
貳、雷射與導能武器.....87
參、極音速武器與長程打擊武器.....93
肆、人工智慧與無人載具的運用.....99
伍、戰場無人系統.....105
陸、未來武器與高科技載台發展趨勢.....111
柒、小結.....116
第七章 台灣國防自主前瞻　洪瑞閔.....117
壹、前言.....117
貳、我國國防自主發展趨勢.....117
參、國防自主的意義.....119
肆、重要國家的發展經驗.....123
伍、台灣國防自主的挑戰與機會.....125
陸、小結.....128
結論.....129

第一章責任校對：吳俊德、傅傳君
第二章責任校對：洪瑞閔、林政良
第三章責任校對：許智翔、姚宇庠
第四章責任校對：吳宗翰、盧屏淵
第五章責任校對：杜貞儀、王綉雯、陳俊良
第六章責任校對：杜貞儀、王綉雯、郭恒孝
第七章責任校對：吳宗翰、郭恒孝

表目錄

表 1-1、美國對中貿易戰主要行動 6
表 1-2、美中科技戰後續評估 10
表 3-1、美國、日本、歐盟目前科技管制體制進展之比較 49
表 4-1、公司安全治理機制 56
表 4-2、美國 DPAS 計畫標號分類表 57
表 4-3、美國出口管制分類編碼表 65
表 7-1、「勇鷹號」高級教練機組件自製能力情況 118
表 7-2、「潛艦國造」計畫組件自製能力情況 119
表 7-3、「勇鷹號」高級教練機的可能外溢效應領域 122
表 7-4、「國艦國造」項目的可能外溢效應領域 123
表 7-5、2018 年全球前十大國防企業 127

圖目錄

圖 1-1、中對美貿易順差與 GDP 發展之關聯 14
圖 5-1、美國陸軍的長程火力 85
圖 6-1、機動短程防空系統 89
圖 6-2、高能雷射武器系統 90
圖 6-3、AGM-183 極超音速武器 96
圖 6-4、萊茵金屬「鼬鼠」無人輕裝甲車 109
圖 6-5、英國貝宜航太的「暴風」戰機概念 113
圖 7-1、2014-2018 年全球武器出口市場分布情形 127

專有名詞中英文對照

一、報告/計畫/公約

《1974 年貿易法》	*Trade Act of 1974*
《1976 年武器出口管理法》	*Arms Export Control Act of 1976,* AECA
《2019 財政年度國防授權法》（美國）	*National Defense Authorization Act for Fiscal Year 2019,* NDAA 2019
《2020 年國防授權法》	*National Defense Authorization Act for Fiscal Year 2020*
《小型企業法》（美國）	*Small Business Act*
《中美共同防禦條約》	*Sino-American Mutual Defense Treaty*
《中程核兵力條約》或稱《中程飛彈條約》	*Intermediate-Range Nuclear Forces Treaty,* INF
《以制裁反制美國對手法案》	*Countering America's Adversaries Through Sanctions Act,* CAATSA
《出口管制改革法》（美國）	*Export Control Reform Act of 2018,* ECRA
《出口管理規則》（美國）	*The Export Administration Regulations,* EAR
《台灣關係法》	*Taiwan Relations Act*
《外來投資風險審查現代化法》（美國）	*Foreign Investment Risk Review Modernization Act,* FIRRMA
《外來投資與國家安全法》（美國）	*Foreign Investment and National Security Act*
《外國援助法》（美國）	*Foreign Assistance Act,* FAA
《亞洲再保證倡議法》（2018）	*Asia Reassurance Initiative Act of 2018*
《武器出口管制法》（美國）	*Arms Export Control Act,* AECA
《武器貿易管制條例》（美國）	*International Traffic in Arms Regulations,* ITAR
《國防生產法》（美國）	*Defense Production Act,* DPA
《國家工業安全計畫守則》（美國）	*National Industrial Security Program Operating Manual,* NISPOM
《國家緊急法》	*National Emergencies Act*
《國際武器貿易條例》	*International Traffic in Arms Regulations,* ITAR
《國際緊急狀態經濟權力法》	*International Emergency Economic Powers Act,* IEEPA

《國際緊急經濟權力法》(美國)	*International Emergency Economic Powers Act,* IEEPA
《智慧財產權：航渡商務之海》(美國)	*Intellectual Property: Navigating through Commercial Waters*
《評估與強化美國製造與國防產業基礎與供應鏈韌性》(美國)	*Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*
《經濟間諜法》(美國)	*Economic Espionage Act 1996*
《德國對外經濟條例》	*Außenwirtschaftsverordnung,* AWV
《歐盟保護技能知識與商業資訊（營業秘密）防止非法取得、使用與公開之規程 2016/943》	*Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the Protection of Undisclosed Know-how and Business Information (trade secrets) against their Unlawful Acquisition, Use and Disclosure*
《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*
《確保資通科技與服務供應鏈安全行政命令》	*Executive Order on Securing the Information and Communications Technology and Services Supply Chain*
《學術研究與交流安全輸出之敏感科技管制規範》	*Guidance for the Control of Sensitive Technologies for Security Export for Academic and Research Institutions*
《營業秘密防護法》(美國)	*The Defend Trade Secrets Act of 2016,* DTSA
《聯邦法規》(美國)	*Code of Federal Regulations,* CFR
《聯邦採購條例》(美國)	*Federal Acquisition Regulation,* FAR
《瓦聖納協定》	*Wassenaar Arrangement*
《飛彈技術管制協議》	*Missile Technology Control Regime*
《核子供應國集團》	*Nuclear Suppliers Group*
《禁止化學武器公約》	*Chemical Weapons Convention*

二、專有名詞與技術

F-35 聯合攻擊戰鬥機	F-35 Joint Strike Fighter

人工智慧	Artificial Intelligence, AI
大數據分析	big data analysis
中型無人水面載具	Medium Displacement Unmanned Surface Vehicle, MDUSV
中程傳統打擊武器系統	Intermediate Range Conventional Prompt Strike Weapon System, IRCPS
反潛持續追蹤無人載具	Anti-submarine warfare Continuous Trail Unmanned Vessel, ACTUV
出口管制分類編碼(美國)	Export Control Classification Number, ECCN
出口管理規則（美國）	Export Administration Regulations, EAR
可置換載人戰鬥車輛計畫	Optionally Manned Fighting Vehicle, OMFV
外來直接投資	Foreign Direct Investment, FDI
先行者優勢	first-mover advantages
合格經銷商名單（美國）	Qualified Suppliers List for Distributors, QSLDs
合格製造商名單（美國）	Qualified Suppliers List for Manufacturers, QSLMs
在拒止環境中協同操作	Collaborative Operations in Denied Environment, CODE
多代理人增強式學習法	Multi-Agent Reinforcement Learning
多領域任務兵	Multi-Domain Task Forces
多領域作戰	Multi-Domain Operation
多領域指揮管制	Multi-Domain Command and Control, MDC2
多領域戰鬥	Multi-Domain Battle
有人—無人組合	manned-unmanned teaming
灰色地帶	gray zone
低成本無人機集群技術	Low Cost UAV Swarm Technology, LOCUST
利基生產	niche production
即時虛擬及建構技術	Live Virtual Constructive, LVC
技術標準規定認證（美國）	Technical Standard Orders, TSOs
系統單晶片	System on Chip, SoC
固態雷射	Solid State Lasers, SSL

物聯網	Internet of Things, IoT
空優 2030 飛行計畫	Air Superiority 2030 Flight Plan
信賴自主系統計畫	Trusted Autonomous Systems
幽靈艦隊計畫	Ghost Fleet
穿透性制空	Penetrating Counter-Air, PCA
美中戰略經濟對話	U.S.-China Strategic and Economic Dialogue
美國下一代戰鬥車輛計畫	Next Generation Combat Vehicle, NGCV
美國陸軍機器人與自主系統戰略	The U.S. Army Robotics and Autonomous Systems Strategy
砲射導引武器	Gun-Launched Guided Projectile, GLGP
神經網路處理器	neural network processor
高能雷射	high-energy lasers
高能雷射武器系統	High-Energy Laser Weapon System, HELWS
國防產業基礎	defense industrial base
混合戰	hybrid warfare
第一級武器生產國家	first-tier producer-states
第二級武器生產國家	second-tier producer-states
終端用戶證明書	End User Certificate, EUC
陸基極超音速飛彈計畫	Land-Based Hypersonic Missile
最低限度存取權限	least-privilege access
無侵入交付	Deliver Uncompromised, DU
超音速燃燒衝壓發動機	Supersonic combustion ramjet, scramjet
量子運算	quantum computing
量子霸權	quantum supremacy
量子疊加態	quantum superposition
新削減戰略武器條約	Strategic Arms Reduction Treaty, New START
極音速	hypersonic
極音速巡弋飛彈	Hypersonic Cruise Missile, HCM
極音速滑翔載具	Hypersonic Glide Vehicle, HGV
零信任架構	Zero Trust Architecture, ZTA
電磁軌道砲	Electromagnetic Railgun，EMRG
實體清單（美國）	entity list
網路安全完善模式認證	Cybersecurity Maturity Model Certification, CMMC

豪豬戰略	porcupine strategy
影響力作戰	Influence Operation
德法主要地面作戰系統	Main Ground Combat System, MGCS
數位絲路	digital silk
模組化無人地面系統計畫	Modular Unmanned Ground Systems
歐盟實體清單	EU Consolidated List
戰場覺知	situation awareness
機動高能雷射	Mobile Expeditionary High Energy Laser, MEHEL
機動短程空防系統	Maneuver Short-Range Air Defense, MSHORAD
澳洲集團	Australia Group
應用情境可程式化邏輯陣列	Field Programmable Gate Array, FPGA
磷酸二氫鉀	Potassium Dihydrogen Phosphate, KDP
邊緣防禦	perimeter defense
邊緣運算	edge computing

三、部門/單位

伊諾運輸中心	Eno Center for Transportation
快速能力及關鍵計畫辦公室	Rapid Capabilities & Critical Technologies Office, RCCTO
汽車工程師學會（美國）	Society of Automobile Engineers, SAE
法國原子能和替代能源委員會	Le Commissariat à l'énergie atomique et aux éner
波蘭國際國防工業展	Międzynarodowy Salon Przemysłu Obronnego
俄羅斯軍事工業委員會	Russian Military Industrial Committee
美國內政部	Department of the Interior
美國司法部	Department of Justice
美國外來投資審查委員會	Committee on Foreign Investment in the United States, CFIUS
美國印太司令部	United States Indo-Pacific Command, USINDOPACOM
美國科學與技術政策辦公室	Office of Science & Technology Policy
美國海軍戰院	Naval War College
美國能源部	Department of Energy
美國財政部	Department of the Treasury
美國財政部外國資產管理局	Office of Foreign Assets Control, OFAC

美國商務部	Department of Commerce
美國商務部工業暨安全局	Bureau of Industry and Security, BIS
美國國土安全部	Department of Homeland Security
美國國土安全會議	Homeland Security Council
美國國防部	Department of Defense
美國國防部小型企業計畫辦公室	Office of Small Business Programs
美國國防部反情報與安全局	Defense Counterintelligence and Security Agency, DCSA
美國國防部國防技術安全局	Defense Technology Security Administration, DTSA
美國國防部國防後勤局	Defense Logistics Agency, DLA
美國國防部國防資訊系統局	Defense Information Systems Agency, DISA
美國國防部資訊安全監督辦公室	The Information Security Oversight Office, ISOO
美國國防創新理事會	Defense Innovation Board
美國國家安全會議	National Security Council
美國國家情報總監	Director of National Intelligence
美國國家經濟會議	National Economic Council
美國國家標準暨技術研究院	National Institute of Standards and Technology, NIST
美國國務院	Department of State
美國國務院國防貿易管制處	Directorate of Defense Trade Controls, DDTC
美國陸軍協會	Association of the United States Army
美國陸軍航空卓越中心	US Army Aviation Center of Excellence
美國陸軍機動卓越中心	Army's Maneuver Center of Excellence
美國貿易代表	US Trade Representative, USTR
美國貿易代表辦公室	Office of the U.S. Trade Representative
美國經濟顧問會議	Council of Economic Advisors
美國管理與預算政策辦公室	Office of Management & Budget
美國聯邦航空總署	Federal Aviation Administration, FAA
英國國防科技實驗室	Defence Science and Technology Laboratory, DSTL
英國國際防務與安全裝備展	Defence & Security Equipment International, DSEI

倫敦國際戰略研究所	Institute of International Strategic Studies, IISS
國防先進研究計畫署（美國）	Defense Advanced Research Projects Agency, DARPA
國防研究暨發展組織	Defence Research and Development Organisation, DRDO
國防部研究與工程政策副次長	Deputy Assistant Secretary for Cyber and International Communications and Information Policy
國際海事委員會	Comite Maritime International, CMI
國際海事組織	International Maritime Organization, IMO
國際航太大會	International Aerospace Conference, IAC
國際電信聯盟	International Telecommunication Union, ITU
國際標準化組織	International Organization for Standardization, ISO
傳統基金會	Heritage Foundation
詹氏集團	Jane's Group
電子暨資訊技術實驗室	Laboratoire d'electronique et de technologie de l'information, Leti gies alternatives, CEA
網路與國際通訊副助卿	Deputy Assistant Secretary for Cyber and International Communications and Information Policy
歐洲外交關係理事會	European Council on Foreign Relations
戰略暨預算評估中心	Center for Strategic and Budgetary Assessments, CSBA

本頁空白

緒論

蘇紫雲、吳俊德

前瞻2020年將是全球戰略重新布局的關鍵時間點，2018年3月拉開序幕的美中貿易戰，已經顯示長期化的趨勢。進一步觀察貿易戰的核心是科技戰，其中涉及的科技管理、生產供應鏈的安全等機制將決定科技產業的未來競爭力，特別是國防產業與敏感科技，這是2019年國防科技趨勢報告選擇以產業安全作為主要議題的原因。由於美國是全球最大的消費市場，美中貿易戰將翻轉全球的經濟結構，以及生產與市場的供需關係，進一步連動全球的國際政治、軍事、以及安全情勢。

事實上，要掌握美中貿易科技戰的未來發展，需先了解其背景，本質上並非僅僅因為美中兩國貿易的失衡，真正原因是美國川普政府對於「和平演變」中國政策的質疑。在1989年「天安門」事件後，美國為主的西方民主國家對北京採取經濟制裁，但緊接著柏林圍牆倒塌、蘇聯瓦解、以及東歐非共化等的「蘇東波」現象，使得冷戰瞬間瓦解，全世界處於和平的樂觀氛圍之中，因此寄望中國發展經濟，進而改革政治的「和平演變」便成為民主陣營的政策主軸。

若以北京加入世界貿易組織（WTO）的2000年為基期，則至2017年川普政府上台的17年間，中國大陸之國民生產毛額（Gross National Product, GNP）由2001年的2.4兆美元成長至2017年的10.2兆美元。在同一期間，軍事支出則由200億美元成長至1,500億美元。易言之，中國大陸在21世紀開始的17年之間的總體經濟成長4.25倍，但軍事費用則增加達7.5倍之譜，並用於發展大量的新式裝備，包括飛彈、匿蹤戰機、航艦等新世代戰力用於火力投射、兵力投射，威脅周邊國家甚至區域安全。

另一方面，中國大陸這些新式裝備與武器，其運用的科技有許多來自美國與西方國家，藉由商業手段、情報手段、以及網路駭客等方式取得相關技術或設計。而在對內部分，則運用網路、大數據、影像辨識等科技監控人民，建立新型態的「數位威權」體制，並向外輸出。也就是說，自由經濟並沒有促進中國大陸的政治民主化，反而如同美國副總統彭斯演講時所云，利用美國科技威脅民主國家並箝制中國公民。

也因此，科技管理就成為未來的關鍵議題，在2018年3月啟動貿易戰後的半年，美國國防部再於2018年10月5日公布名為《評估與強化美國製造與國防產業基礎與供應鏈韌性》的報告，直接點名中國相關企業、產品、乃至原物料對國防產業鏈的威脅。警告中國對美軍所需關鍵零組件、原物料的供應構成巨大的和日漸增長的風險。報告列舉近300個可能影響美軍裝備的關鍵原材料和零組件供應之漏洞。

同時，中國大陸的經濟發展促進軍事擴張、並以侵略型經濟戰略、軟實力戰略以及軍事研發開支戰略，甚至文化性的滲透與威脅，在美國取得「科工數理」（STEM）學位者有25%為中國留學生，使得美國大學成為中國大陸經濟與軍事

崛起的最大推手。此皆清楚指出中共對外採取之行為取向具高度的侵略性，卻化整為零並包裝為文化、商務模式，對民主國家滲透。此與冷戰時期前蘇聯的作法完全不同。

如同前文所述，由於美國是全球最大消費市場，台灣由於擁有具代表性產業的先進半導體生產能力、以及完整的電子、資訊、精密機械等完整的供應鏈，因此藉有機會在未來的國防產業、安全裝備供應鏈取代中國大陸空出的供應缺口，此亦為美國國務副助卿米德偉（Derek James Mitchell）認為台灣是美國重要的電子供應鏈夥伴的原因，台美要以「4I」維持合作關係，包括互動（interaction）、創新（innovation）、智慧財產權保護（intellectual property right protection）、投資（investment）。

相對地，台灣在工業安全、科技安全的管理仍有極大改善空間。包括廠區人員、物件安控、原物料品管，以及敏感科技、智慧財產的輸出管理等機制，亟需法令以及新管理觀念的導入。此不僅攸關國家安全事宜，對業者本身的商譽與競爭力也是關鍵。台灣具有良好國防工業基礎，可與美國國防產業具有互補與合作之機會，開創具前瞻性的重要商機。

第一篇　貿易科技戰的評估

本頁空白

第一章 美中戰略與經濟的矛盾

蘇紫雲*

壹、前言

戰略經濟（strategic economics）一般係指經濟議題同時涉及貿易、安全、環境、科技等的跨領域面向，由歷年美國與中國的「美中戰略與經濟對話」（U.S.-China Strategic and Economic Dialogue）的精神及實際內容而言，戰略經濟實際涵蓋兩國關係、雙邊貿易、區域安全等廣泛性議題，並存在若干歧見。尤其值得注意的是，美國副總統彭斯（Michael Pence）在 2018 年 10 月的演講中，將中國共產黨政權統治下的中國大陸區分為中國、中國共產黨、中國人民、中國文化，[1]清晰的描述所指涉的對象以及欲傳達的訊息，代表川普政府對中政策趨向更為精確而細緻，本文也將藉用其方式以盡可能符合雙方的政策意旨。

在美國川普（Donald Trump）政府 2017 年就任後，美中兩國的戰略與經濟衝突，擴大為實際的貿易戰以及科技戰。在 21 世紀科技的應用已成為未來經濟運作的基礎，被稱為「科技經濟」（tech economy），亦即是科技產業對經濟的影響已超越單純製造業的範疇，其衍生的應用與服務往往可開創更多的經濟活動，例如主要國家都有利用行動網路連結實體服務所衍生的物流、載客、食品外送等新創服務業，因此科技經濟成為未來經濟發展的主軸。以發展中的 5G 通訊為例，涉及包括物聯網（Internet of Things, IoT）、自駕車、高解析度影像等的新創服務，也是未來經濟的主要驅動力，而這些應用服務都倚賴 5G 的高速無線網路技術。其他包括電動車的儲能技術、高度運算能力的量子電腦、人工智慧（Artificial Intelligence, AI）等都是未來經濟發展的必要條件，共同構成科技經濟的核心。同時，軍事領域的應用也是科技發展的重點，特別是結合人工智慧、高速運算、影像處理等戰場管理、指揮管制通訊等目標獲得與接戰的指揮鏈（command chain），都是精密軍規電子的高密度應用領域，也是美國擔憂北京對美國進行科技滲透的主因之一。

實例如美國內政部（Department of the Interior）宣布停用中國生產的 800 餘架無人機，因懷疑其有電子間諜的風險，[2]可能將國土、資源測繪等資料外傳給未獲授權的特定網點。因此，相關科技的發展也就決定國家競爭力的關鍵。經濟利益、科技競爭、軍備競賽等形成的複合安全衝突，便成為美中貿易戰的主要背景。

---

* 蘇紫雲，國防資源與產業研究所副研究員，負責研究架構與本章。

1 Mike Pence, “Vice President Mike Pence’s Remarks on the Administration’s Policy Towards China,” Hudson Institute, October 4, 2018, https://www.hudson.org/events/1610-vice-president-mike-pence-s-remarks-on-the-administration-s-policy-towards-china102018.

2 Timothy Puko and Katy Stech Ferek, “Interior Department Grounds Aerial Drone Fleet, Citing Risk From Chinese Manufacturers,” *Wall Street Journal*, October 30, 2019, https://www.wsj.com/articles/interior-dept-grounds-aerial-drone-fleet-citing-risk-from-chinese-manufacturers-11572473703.

貳、貿易戰的形成

目前仍在進行的美中貿易戰的正式啟動，係美國川普總統於 2018 年 3 月 22 日簽署備忘錄，[3]要求美國貿易代表（US Trade Representative, USTR）對中國進口產品的關稅及智慧財產權（intellectual property right）的狀況進行聽證與調查。[4] 其後於 2018 年 7 月 6 日啟動第一波正式加稅行動，對價值 500 億美元的商品加徵關稅。第二波加稅行動則於 2018 年 9 月 24 日發起，再對 2,000 億美元的商品課徵 10%關稅。[5]第三波加稅於 2019 年 5 月 10 日開始，對 2,000 億美元的進口商品加徵 25%關稅。美政府考量除平衡貿易逆差外，更重要的是影響中國財政，以抑制軍力成長，與對「一帶一路」的海外投資，擴增北京影響力。因此儘管川普與習近平可能在 2019 年 12 月於倫敦舉行「川習會」達成初步協議，但是否能立刻解除懲罰關稅，情況仍不樂觀，部分美國學者甚至以美國實際上缺乏所謂的「華盛頓共識」（Washington Consensus）來形容，[6]但在華府的實際政治運作上卻又有所差異。

表 1-1、美國對中貿易戰主要行動

日期	美國政府行動
2018 年 3 月 22 日	啟動 301 條款，對中國進口產品進行調查。
2018 年 7 月 6 日	第一批加稅清單，總值 500 億美元產品。
2018 年 9 月 24 日	第二批加稅清單，總值 2,000 億美元產品。
2019 年 5 月 10 日	第三批加稅清單，總值 2,000 億美元產品。

資料來源：蘇紫雲整理自公開資料。

比較特別的是，在目前美國內部政治處於朝野對抗的氛圍下，共和、民主兩黨在內政議題歧異甚多、甚至對歐盟、中東等區域問題也有歧見的情況下，對於反制中國的政策則具有較高的共識。實例而言，除了軍用科技、華為等明確指標外，包括部分的民用產品也遭鎖定。美國國會對中國科技產業採取進一步禁制令，禁止聯邦政府採購中國生產的大眾運輸工具，包括電動公車、軌道列車等，以確保國家安全。眾議員盧達（Harley Rouda；民主黨，加州）便指出「此不僅是保

[3] Federal Register, "Actions by the United States Related to the Section 301 Investigation of China's Laws, Policies, Practices, or Actions Related to Technology Transfer, Intellectual Property, and Innovation," *Presidential Document*, Vol. 83, No. 59, March 27, 2018.

[4] Diamond Jeremy, "Trump hits China with tariffs, heightening concerns of global trade war," *CNN* March 22, 2018, https://edition.cnn.com/2018/03/22/politics/donald-trump-china-tariffs-trade-war/.

[5]〈美中第二波貿易戰開打〉，《經濟日報》，2018 年 9 月 24 日，https://money.udn.com/money/story/10511/3383905。

[6] Josephine Ma, "No Washington consensus on tough China policies says US academic Ezra Vogel," *South China Morning Post*, 12 November, 2019, https://www.scmp.com/news/china/diplomacy/article/3037187/no-washington-consensus-tough-china-policies-says-us-academic.

護美國巴士與軌道產業，更是避免美國的大眾運輸系統遭到監視與破壞。」[7]此外美國歐巴馬（Barack Obama）政府時期的國防部長卡特（Ash Carter）在面對 Google 公司計畫與中國進行人工智慧的開發，也公開呼籲 Google 公司應立即停止與中國進行人工智慧、網路搜尋技術等科技的合作，以避免遭中共轉為軍事用途。此可看出美國對中國科技圍堵的政策發展方向將更為嚴密。

同樣屬於民主黨的前國防部長卡特、眾議員盧達之所以力挺共和黨對中的科技圍堵，其主要原因可分為三個部分，包括：

（一）國家安全：「關鍵資訊基礎設施」（critical information infrastructure）的無線通訊基地台、網路設備等相關科技，都可能構成複合式的資訊威脅，藉由系統內建元件或軟體蒐集各類資料，或以旁收（side receive）等方式將資訊流外送，使對手得以獲取戰略情資。另一威脅則是科技外流，包括技術合作等方式，都可能使美方的先進科技外流，造成商業與安全的損失與威脅。

（二）軍事競爭：包括通訊、人工智慧、量子電腦、通訊都涉及軍事用途，可提高個別武器的作戰能力，亦可大幅增加通訊、戰場覺知（situation awareness）等整體系統戰的能力。

（三）商業利益：以美國參眾兩院版本的《2020 年國防授權法》（*National Defense Authorization Act for Fiscal Year 2020*）為例，其修正意見（amendment）決議禁止進口中國生產的電動巴士與軌道車輛，除資訊安全考量外，主要為保護美國本土業者。而其政策主張來自智庫「伊諾運輸中心」（Eno Center for Transportation）的建議，「暫時禁止聯邦預算採購中國軌道車輛」可視為美國會相關遊說的活動之一，代表美國軌道車輛生產業者的利益。[8]在這些因素共同影響下，針對中國產業與科技的反制，在美國具有較大的跨黨共識。此一趨勢亦可作為觀察指標，包含後文會提及的台積電等被視為商用的半導體業等。

一、關鍵產業涉及戰略安全

美方的主要考量點為戰略安全，除較常為外界討論的華為 5G 與資訊網路系統外，前述的軌道車輛、電動巴士等的大眾運輸屬於「關鍵基礎設施」（critical infrastructure）也是重點之一，且無論是載具本身、行進過程、以及營運管理都利用資通訊技術整合，以提高總體的營運效能。而中國生產的電動公車、軌道捷運系統等載具，都配置車內外影像設備，以及車輛動態定位系統，透過機電整合可以在行控中心等遠端監控，「如此外國政府將有機會知道美國在運輸戰車、直升機等軍事裝備、燃料、或是糧食的狀況。」[9]

---

[7] Trefor Moss, Lindsay Wise, “Congress Moves Toward Ban on Buying Chinese Buses, Railcars Over Spy Fears,” *Wall Street Journal*, July 23, 2019, https://www.wsj.com/articles/congress-moves-toward-ban-on-buying-chinese-buses-railcars-over-spy-fears-11563874203.

[8] Melina Druga, “Think tank proposes temporary ban on Federal funds for Chinese railcars,” *Transportation Today*, October 1, 2018, https://transportationtodaynews.com/news/10828-think-tank-proposes-a-temporary-ban-on-federal-funds-for-chinese-railcars/.

[9] Melina Druga, “Think tank proposes temporary ban on Federal funds for Chinese railcars.”

同時，美國務院亞太副助卿費德瑋（Jonathan Fritz）也於 2019 年 7 月 24 日在華府智庫傳統基金會（Heritage Foundation）研討會中指出，美國政府針對華為的立場並未變動，川普也沒有解禁。而國務院「網路與國際通訊副助卿」（Deputy Assistant Secretary for Cyber and International Communications and Information Policy）史特耶（Robert L. Strayer）在該研討會指出，針對 5G 網路建設，美國將敦促其他國家透過風險評估來制定安全策略，「我們認為，在沒有合法程序和司法獨立的前提下，任何一個國家如果能夠對當地供應商施加影響力，廠商就可能會被要求執行利於該國家利益的命令」。費德瑋進一步表示，中共 2017 年實施《國家情報法》規定，可以要求有關組織協助國家情報工作，這意味北京當局可以迫使華為執行他們的命令，這也是美國無法信任華為的原因。

二、反制中共科技滲透

矽谷創投企業家提爾（Peter Thiel）公開呼籲美國政府應該調查 Google，因為該公司與中國具深度合作關係，包括被形容為與「AI 的曼哈頓計畫」（AI Manhattan Project）的 Google 人工智慧「深智」（DeepMind）的研發計畫疑似受到中國情報單位滲透，Google 為何放棄與美國防部合作，轉而與中共軍方合作。[10]提爾更直言 Google 行為簡直像是叛國，並表示 Google 旗下的「深智」公司研發的 AI 軟體應被視為軍事武器。主要的原因在於中國的軍民融合策略，且所謂的軍民兩用科技（dual-use），往往成為中國引入新式軍用科技的主要管道。這也是美國前國防部長卡特認為：「若與中國合作，根本無從確認其是否為軍方的專案，且 Google 拒絕與五角大廈合作，卻與中共軍方合作可說是犯了大錯」。[11] Google 與美國防部的合作於 2019 年到期但未再續約，但 Google 卻與中方擴大在上海設置的人工智慧研究中心，此一現象進一步引發美國政界遭中共滲透的疑慮與警覺。

三、北京加速「中國製造 2025」恐形成「科技兩極」體系

相對而言，北京為降低對歐美的科技依賴，將加速之前轉趨低調的「中國製造 2025」策略。短期而言，遭美方科技圍堵的華為已擴大來台尋找替代的零組件供應鏈，[12]然而筆者認為其後續則應考慮將機版重新設計才能完整避開使用美製晶片組。中長期則加速中國本土半導體製造業的能量，以求由設計、生產、組裝都能在本土完成。進一步觀察，未來的科技產品可能將出現兩種規格，這在以往也有類似案例，例如一次大戰前俄國為防止德國入侵，其鐵道採特殊規格，冷戰

[10] Rachel Sandler, "Peter Thiel Says CIA Should Investigate Google For Being Treasonous," *Forbes*, July 16, 2019, https://www.forbes.com/sites/rachelsandler/2019/07/15/peter-thiel-says-cia-should-investigate-google-for-being-treasonous/#66263ea521d0.

[11] Jessica Bursztynsky, "Ex- Defense chief: Google has a duty to the US, not China, to take our values to the battlefield," *CNBC*, Jul 18, 2019, https://www.cnbc.com/2019/07/18/ex-defense-secretary-ash-carter-google-has-a-duty-to-the-us-not-china.html.

[12] 蔡靜紋，〈貿易戰替代概念吸睛〉，《經濟日報》，2019 年 7 月 6 日，https://money.udn.com/money/story/5607/3912473。

期間俄國在軍事裝備以及電子用品也採用俄系規格，包括火砲口徑、電子零組件等以與西方國家區隔，只通用於東歐集團自成體系。主要差異在於，由於美中為全球前二大經濟體，其科技與產品規格的制定，將較冷戰時期的東西方規格的影響來得巨大。或許我們可以說，未來將形成「科技兩極」的國際科技經濟體系。

四、中國反擊籌碼薄弱

依照美國普查統計局（Census Bureau）結算，2018 年對中國的貿易逆差達到 4,195 億美元，[13]對照中國商務部 2017 年公布的資料，在 2017 年美國對中的逆差為 3,750 億美元，等同北京年均外貿順差的 86 %以及 GDP 的 3%都仰賴美國單一市場，形同北京戰略弱點。北京雖已宣布針對美國 600 億美元貨品採取相應的加徵 25%關稅，但相較中美間的鉅額逆差，效果有限。

中共後續可能採行的措施，包括（1）重啟 2010 年的「稀土戰爭」、（2）拋售美國政府債券、（3）操作人民幣貶值等戰略手段。其中，稀土被寄予厚望。

美國國防部於 2018 年 10 月 5 日公布《評估與強化美國製造與國防產業基礎與供應鏈韌性》（*Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*，下簡稱《強化美國防產業》），特別提到中國對一系列被廣泛使用的金屬和特殊金屬、合金以及其它材料，包括稀土礦物和永久磁鐵的控制。中共控制了全球大部分稀土礦物的供應，而稀土礦物被廣泛使用於軍事裝備與安全設備。2013 年至 2016 年，美從中國進口的稀土材料佔據了美國總需求的 78%。同時，也是彈藥與火箭活性推進劑的獨家或主要供應者。不過，由於澳洲已決定將在美國本土設置稀土精煉廠，因此後續影響有限。

拋售美債將使北京損失鉅額外匯，恐不利財政日益窘迫的北京；且拋售美債可能導致美元貶值反增加美國出口競爭力，最後只好操作人民幣貶值以資對抗。不妙的是此為雙面刃，因為將導致原油等輸入成本增加，更重要的是美國商務部（Department of Commerce）正在研擬新對策，對操縱貨幣使其對美元匯率貶值的國家徵收「反補貼稅」（countervailing duty），北京若令人民幣貶值恐使美國對中國商品加徵更高關稅。因此，北京目前可用的反擊籌碼可說極為有限。關於美中科技戰的後續評估，可見表 1-2（下頁）。

[13] "2018: U.S. trade in goods with China," Census Bureau, https://www.census.gov/foreign-trade/balance/c5700.html.

表 1-2、美中科技戰後續評估

國別	主要籌碼	可能效應
美國	藉 IMEI 碼禁止華為手機登入基站*	進一步孤立華為
	加徵反補貼稅	擴大打擊中國製造商
	封鎖中國領頭羊公司，各個擊破	海康威視、大疆無人機等，遭停止供貨
中國	發動稀土戰爭	對美造成短期衝擊
	拋售美債	北京外匯存底量縮
	人民幣貶值	美國加徵「反補貼稅」
台灣	掌握部分關鍵供應鏈，高科技產業回流	如台灣代表性的監視器大廠可遞補監視器市場

資料來源：蘇紫雲整理自公開資料。

說明：*IMEI 為「國際行動設備識別碼」（international mobile equipment identity number）之縮寫。

參、美中軍備競賽激化產業科技戰

中共持續地對美國進行科技滲透，令美國更加提高警覺與加強防範，避免科技外流。例如，美國海軍的中裔美籍軍官楊帆（Fan Yan）與其同為中國裔的妻子於 2019 年 11 月 1 日遭美國聯邦檢察官逮捕，罪名是出售軍品給中國。[14]中國國家航天局副局長吳燕華，其原計劃於 2019 年 10 月間率團赴美參加在華盛頓舉行的「國際航太大會」（International Aerospace Conference, IAC），卻遭美國務院拒絕發給簽證使其無法訪美。北京方面對此指責美方將「簽證武器化」（weaponize visa），但實際上吳燕華也是負責監督中國軍火工業的主要官員，具敏感身分，[15]此可視為美國強化科技管制的趨勢。

此外，美國副總統彭斯於 2019 年 10 月 24 日於威爾森中心（Wilson Center）發表演說時，便公開指責「中共透過軍民融合（military-civilian fusion）的政策，以法律及行政壓力（presidential fiat）迫使中國境內之企業，無論是私人、國有、或外國公司，都必須將科技提供給中國軍方」，[16]「而中共軍方近年則以更多的挑

[14] Jeff Mordock, "U.S. Navy officer, wife charged with attempting to smuggle military equipment to China," *Washington Times*, November 1, 2019, https://www.washingtontimes.com/news/2019/nov/1/us-navy-officer-wife-charged-with-attempting-to-sm/.

[15] "US rejects China claim of weaponizing visas," *Washington Post*, October. 25, 2019. https://www.washingtonpost.com/politics/congress/us-rejects-china-claim-of-weaponizing-visas/2019/10/25/e74f0fa6-f703-11e9-b2d2-1f37c9d82dbb_story.html.

[16] "Remarks by Vice President Pence at the Frederic V. Malek Memorial Lecture," The White House, October 24, 2019. https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-frederic-v-malek-memorial-lecture/.

鬱姿態對應區域議題與周邊國家」。[17]實際上，美中目前仍僵持的貿易戰、以及科技戰，其背後的主要關鍵就是軍事裝備的發展，而科技以及資金的投入將對兩國的軍備競賽造成衝擊，並進而影響未來國際政治的權力結構。

美方拒絕中國航天人員參加航太科技年會，主因為航太火箭與飛彈科技高度相關，且美國退出《中程核兵力條約》或稱《中程飛彈條約》（*Intermediate-Range Nuclear Forces Treaty*, INF）的主因就在重建中程飛彈武力，因此整體戰略背景可視為美中軍備競賽及所衍生的貿易戰、科技戰。

一、中共軍備著重不對稱利基

中共解放軍的新式裝備在近年不斷擴增，包括空中兵力的殲 20、殲 16 戰機、運 20 戰略運輸機，001A 型航艦、075 型兩棲攻擊艦、055 型神盾級驅逐艦、096 型潛艦等都屬於新世代的投射型兵力，不僅質量大為提高，數量也快速增加。相對的，共軍也自知這些新兵力仍無法挑戰美軍，因此另行發展不對稱戰力。主要為飛彈為主的火力投射系統，主要為戰略飛彈，以核打擊為主射程可直達美國本土具多彈頭投射能力的陸基「東風 41」洲際飛彈、以及射程 12,000 公里的「巨浪 2」潛射彈道飛彈，在戰區飛彈層級，則以「東風 17」彈道—高音速滑翔載具（Hypersonic Glide Vehicle, HGV）、以及「東風 100」彈道—巡弋飛彈兩型中程飛彈最具特色。「東風 17」首段為運載火箭，次段為高音速滑翔載具，以火箭爬升後採高—高度彈道遂行攻擊，「東風 100」首段亦為運載火箭（東風 11）爬升，次段則為巡弋飛彈，屬於高-低彈道攻擊模式，此二型飛彈為軍事科技首次出現並加入服役的「高低彈道混種飛彈」，顛覆以往彈道飛彈、巡弋飛彈的分類與特性，具科技創新與戰法創新的實質意義，且將對既有飛彈防禦系統造成立即威脅。

二、美國軍備採高低配途徑

在美國方面，在川普於 2017 年上任後力求重振美軍的絕對優勢，大力擴增軍費就如同副總統彭斯在前述威爾森中心的演講中提及川普政府近 3 年來已投注 2.5 兆美元的國防預算，額度可說是歷年最大。但由於現代武器載台的造價高昂，美國防部在投資新式裝備的同時，也力求尋找提高成本效益的戰力組合，如同 1980 年代的「高低配」（high-low mix）建軍途徑一般。其具體做法包括，改變軍種任務特性，陸軍砲兵部隊將配置反艦飛彈以減輕海軍艦艇的負擔、地面部隊強化機動防空系統以減少對空軍的倚賴、海軍則將兩棲突擊艦航艦化以增加任務彈性並減少正規航艦的負擔與成本，同時發展新式小型水雷、空軍延長 F-16、F-15 機隊服役時間，陸軍則擴大採用商規車輛等做法，凡此都是兼顧戰力與成本的兵力整建方案。

[17] "Remarks by Vice President Pence at the Frederic V. Malek Memorial Lecture," The White House.

三、美方持續緊縮對中特定產業科技管制

自 2017 年川普總統就任後認真看待中共軍力的崛起以及全球部署的企圖，並著手貿易戰以抑制北京對軍費的投資，著手科技戰以圍堵共軍軍事科技的獲得與轉用，隨著美中競爭的長期化，美方類似拒絕中國航天局副局長入境，緊縮對中國簽證的事件也將越為頻繁，也就是由以往的技術、產品管制，擴大為產業、人員的安全管制。這也可以由彭斯副總統在前述演講中，點名美國部分企業順從北京、自我審查的態度看出產業與科技管制的未來走向。此外，「歐洲外交關係理事會」（European Council on Foreign Relations）也以智庫角度發布政策報告，認為中國在中東藉由「一帶一路」的經濟誘因，以及與以色列的科技公司合作，並輸出監控科技給予沙烏地、杜拜等產油國家，將影響歐盟在中東的利益與安全，歐盟也將密切關注類似華為 5G 系統的安全性、以及中共將科技轉用於武器發展與輸出之影響。[18]美方的科技緊縮政策，預估也將擴大對盟國配合的合作力度。

四、科技應用恐意識形態化

意識形態是冷戰時期的兩極對抗之主要區隔，未來在數位科技的技術開發、應用模式、乃至市場區隔，恐也將出現新的兩極體系。美國前總統柯林頓（Bill Clinton）在千禧年演說時認為中共想對網路進行審查，無異是企圖把果凍釘在牆上般，註定徒勞無功。但至 2019 年，中共的網路審查系統在國際市場大有斬獲，包括沙烏地阿拉伯、埃及、土耳其、泰國、寮國、塞爾維亞、阿拉伯聯合大公國都已與中國簽訂「數位絲路」（digital silk），巴基斯坦、盧安達、乃至葡萄牙也預備加入。[19]此一現象清楚表明北京的數位監控已獲得部分國家認同，此種意識形態的選擇，對於未來數位科技的軟硬體規格訂定、安全規範、以及市場分布恐將造成實質的區隔。

五、科技安全聯盟逐步浮現

與此同時，歐盟也開始警覺中國的科技威脅，並建議「歐美貿易合作」（EU-U.S. co-operation on trade）應著眼於戰略高度以反制北京的不當競爭模式，特別是在未來科技標準（technical standard）的制定，這包含中共以政府力量支持的大型公司對「國際電信聯盟」（International Telecommunication Union, ITU）的 5G 通訊以及量子通訊（quantum telecommunications）、「國際標準化組織」（International Organization for Standardization, ISO），其中以華為公司對 5G 的影響更是代表案例。[20]進一步觀察，由於北京提出「中國製造 2025」的發展策略，以往席捲全球

[18] Camille Lons, Jonathan Fulton, Degang Sun, Naser Al-Tamimi, "China's Great Game in the Middle East, EU Council on Foreign Relations," October 2019, https://www.ecfr.eu/publications/summary/china_great_game_middle_east#.

[19] Alan Weedon, Samuel Yang, "China trumpets tech power at 6th World Internet Conference, signalling a digital arms race," *ABC News*, October 23, 2019, https://www.abc.net.au/news/2019-10-23/sixth-world-internet-conference-china-wuzhen/11623426.

[20] Jim Brunsden, "EU urges alliance with US to counter Chinese tech dominance," *Financial Times*,

貿易的「中國價格」將可能轉為「中國規格」，這將對全球的貿易產生結構性轉變，特別是中國為威權政體，其所制定的規格若隱藏安全漏洞，將對民主國家造成嚴重威脅。在美國對中發起科技圍堵的同時，歐盟的此一政策倡議極具戰略意義，對於民主國家的科技安全將形成重要基礎。

肆、複合模式抑制中國

除調高關稅的貿易戰外，美國總統川普於 2019 年 5 月 15 日簽署行政命令，美國企業不得向華為提供研發的技術與產品，此總統行政命令之全稱為《確保資通科技與服務供應鏈安全行政命令》（*Executive Order on Securing the Information and Communications Technology and Services Supply Chain*，下簡稱《資通安全命令》）。[21]其法律依據包括《國際緊急狀態經濟權力法》（*International Emergency Economic Powers Act*, IEEPA）、《國家緊急法》（*National Emergencies Act*），《1974 年貿易法》（*Trade Act of 1974*） 之 301 條款，賦予總統管制商業、財政、金融等權限，以在美國遭遇國家緊急狀態時採取行動限制美國企業可能危害國家安全的經濟活動。此一行政命令將由商務部與其他政府機構合作，在 150 天內擬訂細部計畫並予執行。

綜合觀察，川普政府 2017 年就任後，為壓制中共侵略性擴張，先後調整戰略重心為印太戰略，啟動懲罰性關稅、限制科技輸出，整合軍事、貿易、科技「三戰」遏制中國，軍事戰略為限制其擴張，貿易戰壓制軍費投資、科技戰則弱化其軍備升級，並同時達到制約中國綜合國力的戰略效果。

總體來看，在貿易戰開打前，白宮對中國威脅便已有全盤的戰略思考，且超越傳統的地緣、軍事安全層級，而是更深層的科技與經濟安全，並可能對北京進行全面的戰略壓制。

一、貿易戰壓制軍費

2019 年 3 月 12 日，習近平在與解放軍、武警代表團會議時發表談話，要求軍方「過緊日子」的思想準備。[22]此一情況頗不尋常，類似說法最早係由鄧小平在上世紀 80 年代所提出，以應對當時以「經濟建設為中心」縮減軍費的背景。美政府啟動貿易戰的考量，外界的一般想像在於平衡貿易逆差，然而更重要的是力圖影響中國財政，以抑制軍力成長，與對「一帶一路」的海外投資，抑制北京影響力。

July 25, 2019, https://www.ft.com/content/aabd515e-aed5-11e9-8030-530adfa879c2.

[21] Donald J. Trump, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," The White House, May 15, 2019, https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

[22] 李建文，〈用艱苦奮鬥優良作風推動既定目標任務落實〉，《中國國防報》，2019 年 3 月 15 日，http://www.81.cn/gfbmap/content/2019-03/15/content_229352.htm。

北京軍力的快速發展，仰賴經濟的快速成長，並將大量資源挹注軍事投資。以北京加入 WTO 的 2000 年為基期至 2017 年的 17 年間，總體經濟由 2001 年的 2.4 兆美元成長至 10.2 兆美元。軍事支出則由 200 億美元成長至 1,500 億美元。[23]中國經濟成長 325%，軍事支出增長 650%。依照詹氏集團（Jane's Group）、倫敦國際戰略研究所（Institute of International Strategic Studies, IISS）等智庫的統計，中國海軍主戰艦艇增長約 2.5 倍（130 艘），遠洋投射大為提升。同時，擁有近 290 枚衛星使其成為全球第二大具備太空能力的國家。加上網路作戰能力，以及結合工業產品的資訊滲透能力，使其總體的軍事能力具備全球強權的水準。

以貿易戰開始的 2018 年為例，中國外匯順差 5,750 億美元中的 3,750 億美元來自美國，等同外貿順差的 65%，因此在貿易戰的影響下，倚賴美國市場為主的製造業勢必外移，經濟發展放緩（請見圖 1-1），造成總體財政遭受衝擊，則軍費的增長自然也難逃影響。此即可間接抑制解放軍的裝備發展以及兵力整建，有效壓制北京的戰略企圖。

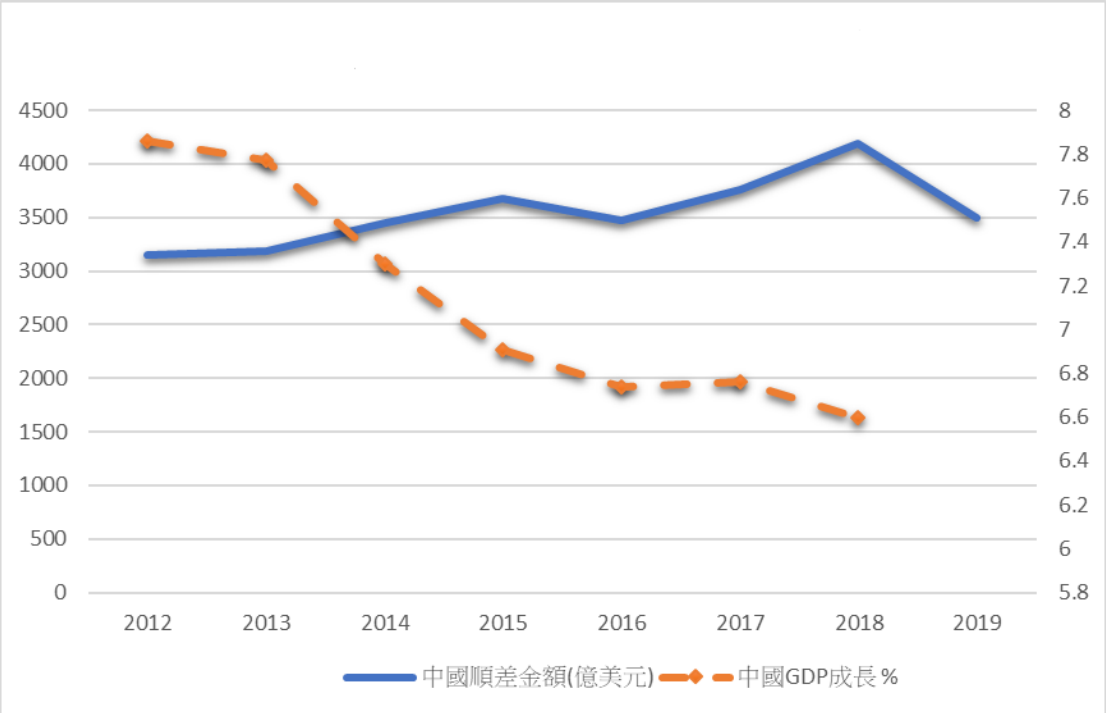


圖 1-1、中對美貿易順差與 GDP 發展之關聯

資料來源：蘇紫雲整理自 World Bank、US Census Bureau。

說明：資料設定時間為 2012 年習近平就任至 2019 年第 3 季。

[23] Department of Defense, "Annual Report to Congress on Military and Security Developments Involving the People's Republic of China 2017," May 2017, p 66.

二、科技戰抑制軍備升級

科技戰方面，主因在於「中國製造 2025」的核心理念，是中國產業升級與轉型的同時，又能促進軍事科技的獲得。在產業轉型方面，脫離廉價代工的產業結構，其目的是讓「中國價格」轉為「中國規格」，掌握產品規格的制定權，就等同擁有價格的制定權，可以產生更多的利益。但問題在於中國的資訊產品常附帶惡意程式，將使用者的數位內容傳遞至特定目的單位，損害消費者個人隱私、及其所屬的組織進而影響國家安全。例如中國知名的「抖音」（TikTok）的服務與對美國企業的併購，便遭美國懷疑有國家安全的顧慮，國會甚至要求「美國外來投資審查委員會」（Committee on Foreign Investment in the United States, CFIUS）進行調查。[24]因此，若包括前述 5G 通訊的規格由中國制定，則潛在的資安風險將更為嚴重。此即為美國國防授權法明文指出中國的中興、華為通訊業者，乃至影像資訊業者具有資安風險的主因，並進一步對民主體制國家造成政治、經濟、軍事的安全威脅。

同時，美國國防部於前文所述的《強化美國防產業》報告提出明確警訊，中國對美軍各式裝備所需關鍵零組件、原物料的供應構成巨大且日漸升高的風險。該報告明確列舉近 300 項可能影響美軍裝備的關鍵原物料、零組件供應造成的安全威脅與漏洞。《2019 年國防授權法》（*NDAA 2019*）也明文指出中國的華為、中興、海康威視、大疆等高科技公司之產品存在資安風險，要求美國政府部門停止採購與後續使用。後續效應也將使中國科技公司取得相關技術更為困難，阻斷其產業升級的同時，也可減少中國軍工企業取得西方科技的管道，阻斷或抑制其武器裝備的研發與升級速度。

三、軍事戰略限縮共軍擴張

而在軍事戰略，面對中國在南海的擴張以及「一帶一路」的地緣戰略，美國將印度洋、太平洋兵力重新整編並新設「印太司令部」（United States Indo-Pacific Command, USINDOPACOM）、通過《亞洲再保證倡議法》（*Asia Reassurance Initiative Act of 2018*）、並大幅修補、增強與台灣的安全合作。同時，2019 年 5 月 22 日通過的美國參院版本之《2020 年國防授權法》將國防預算增加至 7,500 億美元，[25]而訂出的「優先競爭戰略」（Prioritizing Strategic Competition）全都指向印太區域，包括（1）支持陸軍在印太區域的「多領域任務兵力」（Multi-Domain Task Forces）的作戰概念與能力，以重拾美軍在印太區域的軍事優勢。（2）增加印太區域態勢評估以加速美軍轉型為小型、分散、彈性、動態的部署。（3）要求美國防部提出在印太區域的需求報告，包含美軍 2022-2026 年所需的充分資源、

[24] Greg Roumeliotis, Yingzhi Yang, Echo Wang and Alexandra Alper, "US opens national security investigation into TikTok," *Reuters*, November 02, 2019, https://taskandpurpose.com/china-tiktok-investigation.

[25] Senate Armed Services Committee, *FY 2020 National Defense Authorization Act*, Washington, D.C., May 2019. p. 4.

態勢、以及防禦計畫。(4) 修訂《中國軍力與安全報告》(*Military and Security Developments Involving the People's Republic of China*) 需包含中國海外投資與相應的軍事、安全目標之評估。

四、華為恐成科技孤島

目前的 5G 爭議只是科技衝突的序曲，在未來遭受科技限令的情況下，可能另行自定規格而成為特規的「孤島效應」，如同冷戰時期的蘇聯、東歐集團一般。冷戰時期的科技管制著重軍用技術或產品，但因科技進步，若干商規、工規產品也具有軍事潛力。以 Google 停止對華為服務的案例來觀察，該公司於簽訂商業授權時，合約內容皆載明相關限制條款；以 Google Earth 此一產品的授權說明為例，其下載時的服務條款第 5 條便載明「美國政府的限制權利」、第 6 條則載明「出口限制法規」，[26]在必要時可以單方終止服務。其所依據的主要法規，主要為美國商務部的「工業暨安全局」(Bureau of Industry and Security) 所制定的《出口管理規則》(*Export Administration Regulations*, EAR)，以及基於國家安全考量，將華為及所屬 68 家事業體列入貿易黑名單之稱的「實體清單」(entity list)，[27]美國企業與個人都有遵守此行政措施的法律義務。

實際上，軟體部分不只 Google，微軟、Oracle 的所有產品，以及與 Android 作業系統高度關連的 Java，乃至企業服務等軟體也將陸續禁止出口給華為及相關企業。硬體則包含晶片大廠 ARM、高通 (Qualcomm)、英特爾 (Intel)、賽靈思 (Xilinx)、美光 (Micron)、SD 卡協會、wifi 協會等也在第一時間依照美國政府的指示停止對華為供貨、除名，後續才逐案檢討恢復對華為的服務。這將使華為手機失去主要的網路服務功能。若情勢惡化，美國尚可進一步藉由手機內建的 IMEI 碼，停止華為手機在美國與相關國外通訊業者登入，則華為手機將連最基本的語音通話功能都將受限。

五、台積電具高度戰略價值

華為面對主要硬體供應商停止出貨，台灣相關硬體供應商也可能受衝擊，其中最受矚目的為台積電，台積電雖立即表示將持續供貨給華為的海思公司，台積電公開對外表示是基於「盡職調查」(Due-Diligence)，也就是確認出貨符合貿易規範。同時，台積電於中國南京的「晶圓 16 廠」於 2019 年開始提供先進的 16 奈米製程，為中國 IC 設計公司提供晶圓成品的製作服務。但必須注意的是，(1) 美國商務部給予華為緩衝期僅有 90 天、(2) 台積電 16 奈米製程晶片於 2018 年 11 月獲得美國防部認證供應美國 16 奈米級的軍用晶片，台積電南京廠是否替中國軍備公司代工晶圓恐將受關注、(3) 台積電股東結構，依照台積電 2018 年報，

[26] Google，Google 軟體條款與細則，https://earth.google.com/intl/zh-TW/licensepro.html。

[27] Bureau of Industry and Security, "Entity List Additions of Huawei and 68 non-US Affiliates in Effect," *Federal Register*, May 21, 2019, Vol. 84, No.98, p. 22, 961.

其負責人為美國籍，且外資比例達 78%，美籍法人後續恐將影響經營方向。因此，身為國際重要供應鏈的台積電，後續能否繼續對華為供貨，恐有變數。

必須注意的是，台積電公司也逐漸成為科技管制的關注焦點，由於台積電作為西方軍用晶片的主要供應商，甚至 F-35 戰機所使用於人工智慧的「應用情境可程式化邏輯陣列」（Field Programmable Gate Array, FPGA）便是由台積電生產並在台灣封裝，然而又在中國南京廠投資 100 億美元並開始量產 16 奈米的晶圓，這都使得矽谷人士與美國國防部部分官員覺得不安，並認為依賴台積電太深，將影響國防產業的供應鏈安全。代表性人物包括英特爾前執行長布萊恩（Diane Bryant）便憂心「萬一中國對台灣動手，台積電會如何？」美國防部主管研究與工程政策副次長（Deputy Under Secretary of Defense for Research and Engineering）波特（Lisa Porter）也公開主張「美國需重建晶片製造業」。[28]美方相關人士對台灣產業逐漸出現信任危機的認知，應為台灣敏感科技管理的重要訊號。

伍、小結

安全價值將成為產業競爭關鍵。前文所述的各實際議題與案例，重點在於管理機制，由於涉及經濟競爭與國家安全，防堵中共科技滲透將成為西方國家的主要考量。相形之下，台灣具良好科技製造基礎可填補中國遭反制後在市場的空缺，但台灣若要獲得成功，則關鍵在於儘速彌補「敏感科技保護機制」的缺口。然而，產業界對科技保護的認知不足，目前僅有《營業秘密保護法》作為基本的把關，亟需予以強化。

因此應將敏感科技保護為企業競爭力關鍵。依照美中軍備競爭、以及科技戰趨勢觀察，敏感科技或戰略科技產業的安全管理體系將成為關鍵競爭力，建議政府相關部門應優先考量：

（一）完善科技管理體系的法制，並與利害關係人強化溝通；

（二）參考美國、日本等民主國家做法，給予業者、從業人員、乃至學者完整的政策說明與指引；

（三）除國家安全的傳統說法外，導入「公共利益」（public interest）的概念，令其理解安全管理可深化客戶的信任替企業開拓更廣泛的市場，以強化科技管制的正當性與說服力。

相較之下，美國、日本等西方民主國家為確保科技經濟的競爭力，擁有完整的敏感科技保護機制，甚至在著重自由度最高的大學、學術研究機關亦提供完整規範，如美國、英國、澳洲等各大學設有科技管理辦公室或提供「出口管制」（Export Control）法規的說明，核心研究人員出國甚至需向學校單位提出「國際旅行通報」（international travel registry），而日本經產省制定《學術研究與交流安

[28] Don Clark, “Pentagon, With an Eye on China, Pushes for Help from American Tech,” *New York Times*, October 25, 2019, https://www.nytimes.com/2019/10/25/technology/pentagon-taiwan-tsmc-chipmaker.html.

全輸出之敏感科技管制規範》（*Guidance for the Control of Sensitive Technologies for Security Export for Academic and Research Institutions*）等。

易言之，與敏感科技的利害關係者溝通除以國家安全角度切入外，敘明科技研發本身除智慧財產權外，並具有「公共性」須受管理，如同手機無線頻譜的分配、生物科技的倫理、基因科技的安全等較易為一般業者理解，同時輔以貿易戰的市場誘因，較易說服業者接受科技管制的必要性與市場價值，兼顧台灣國家安全與經濟的進一步發展。

（責任校對：吳俊德、傅傳君）

第二章　科技冷戰

曾怡碩*

壹、前言

美國在 2019 年對於華為的圍堵，以及華為的反圍堵，體現出科技冷戰的氛圍。只是，過去冷戰時期美蘇全面圍堵對峙局勢，這次是呈現在與高科技產業發展相關的各個面向。美國除對外勸說友盟共同構築陣線以圍堵中國大陸科技產業擴張，也鑒於在此圍堵藩籬初步成形階段，友盟因缺乏明確依循規範而遲疑不定，故加緊腳步從自身做出示範—美國接續對於科技進出口加強管制，除加強對於中國大陸投資高科技產業的審查限制，並強烈關切中共運用在美中國留學生與科技移民於科技實驗室竊取營業秘密，還限制國防產業及政府採購不能採用中國大陸製產品或關鍵零組件。美國甚至要求關鍵廠商將生產鏈移至美國境內設廠，藉由美國製造的鮮明旗幟，號召友盟加入美國陣營，從法律、規章、審查、監管各個層面，加速築造科技藩籬，以共同對抗中國大陸製造的科技產業。

貳、科技冷戰的本質

冷戰的傳統概念，是源自二次世界大戰結束後，以美國為首的民主自由陣營圍堵以蘇聯為首的共產主義擴張。這樣的兩極世界格局因各自擁有的核武與傳統軍力而達成均勢之對峙。壁壘分明的界線，從軍事聯盟、意識形態、國際組織與外交場域的鬥爭，一路延伸到先進高科技，尤其是軍民兩用科技的發展、移轉與進出口，一般都會對貨品、服務與人力資源施行出口管制措施，對於違規者，往往施加經濟制裁予以懲罰。若是單方或雙方應用議題連結，則甚至波及到安全合作的範疇。

美中貿易戰自2018年3月以來，美方即以中方侵犯智慧財產權以及中方補貼其科技業者造成不公平貿易為由，遂行關稅、出口管制及禁止輸入等貿易制裁。其後美國以國家安全威脅隱憂為由，於全球大肆圍堵華為第5代行動通訊網路（5G）系統。由於傳統盟友仍未能全面禁用華為系統，美國甚至威脅將切斷情報交換機制。在2019年5月，美國川普政府以國家安全為由，祭出出口管制「實體清單」（entity list）；華為在全球分支企業均列入制裁清單。緊接著的是一連串美國科技軟硬體系統及服務大廠陸續宣布終止支援華為產品與服務。

中共商務部隨後在2019年5月31日公布出口管制「不可靠實體清單」機制，以反制美國商務部之「實體清單」，美中科技戰於此正式展開。由於科技戰開打時機，正值中方宣布在6月1日起對600億美元商品加徵關稅，而美國揚言將對約

* 曾怡碩，網路作戰與資訊安全研究所助理研究員，負責本章。

3,000億美元的中國大陸商品開徵25%的關稅，也拉開後續美中兩國斷斷續續的貿易談判的序曲。這不免讓人聯想，各自除反擊對方貿易關稅報復，也是在增加自身之貿易談判籌碼。

然而，美中科技戰本身並非兩國貿易戰籌碼或由貿易戰衍生。科技業者咸認，無論美中貿易戰是否平息，美國與中共之間高科技產業已然由美國提供技術、中國大陸提供代工組裝與廣大市場的互利模式，逐漸進入衝突零和競爭態勢的科技戰模式。因此，美國基於國家安全與科技競爭力之國家利益，美國對於中國大陸科技產業的圍堵，不會因為貿易戰歇息而就此罷手，反而加緊腳步構築科技藩籬，形成科技冷戰態勢。[1]科技冷戰所呈現的圍堵與反圍堵態勢，決不僅止於華為，而將體現在科技產業對於關鍵原物料與零組件、軟體應用程式、人力資源、銷售市場所劃出的分明界線與對於違規越線國家的懲罰。

回顧冷戰的歷史，美蘇陣營在冷戰階段，因惟恐爆發不可挽回的相互毀滅，開始建立熱線等信心建立措施。美中若未來形成分庭抗禮局面，全球各國也將紛紛選邊站，無國界網路安全成為相互攻防無煙硝戰爭的戰場。未來發展壁壘分明的趨勢，也提供了未來建立網路安全區域信心建立措施的基礎。

參、華為模式：圍堵與反圍堵

過去冷戰為美蘇兩核武強國帶領各自陣營對峙，美國圍堵共黨赤化，而共黨陣營防制西方和平演變。如今所謂「美中科技冷戰」雖為各自媒體與網路渲染，但是截至目前為止，主要體現的還是美國與中國大陸華為在技術與服務市場的雙重圍堵與反圍堵。此外，美國防制措施還包括針對中共藉「千人計畫」等措施，鎖定美國高科技產業營業秘密與高等教育機構科研實驗室，以人員情報及網路攻擊遂行滲透竊密，而中方對這些措施也有反彈。華為的圍堵與反圍堵模式，已開始複製擴散，美國對於「抖音」的疑慮即為一鮮明例證。

華為即使面對美國圍堵衝擊—依影響程度排列依序為「安謀（ARM） 停止交易」、「Google 限制 Android 服務」、「射頻晶片（RF）零件」和「英特爾（Intel）製伺服器用晶片」，其他還包括社群媒體與App停止提供服務，仍在營運獲利上有所成長。然而，由於軟體相容性受限，華為後續推出的手機新機型，包括率先全球推出的5G手機，在中國大陸以外的市場銷售受挫，只能仰賴中國大陸國內市場以民族主義情緒支撐其營收。華為的反制措施，除大肆宣傳營收不受美國封鎖的影響，也在美國興訟，控訴美國政府的不當干預。

[1] Michael Schuman, “China’s Likely to Lose a Tech Cold War,” *Bloomberg*, June 11, 2019, https://www.bloomberg.com/opinion/articles/2019-06-11/why-china-is-likely-to-lose-technology-cold-war-with-u-s.

一、美國對華為的圍堵

首先，在技術層面，科技冷戰迄今最具體的呈現，是在於美國切斷中國大陸資通訊產業技術與服務系統之供應鏈，迫使中國大陸必須尋求自力發展之軟體作業系統暨相容之App、硬體之記憶體晶片以及資料傳輸之5G通訊天線、基地台、資料節點、處理器，甚至包括光纖海纜與接收站。

中國大陸在技術方面，迄今仍欠缺形成足以與美冷戰對峙的「核武級」技術。中國大陸不僅在硬體的半導體晶片與快閃記憶體方面，宣稱2019年年底即將量產的「長鑫」動態隨機存取記憶體（DRAM），據信與美國仍有5至6年的差距，[2]而快閃記憶體則因良率趨近於零而陷入停滯困境。在軟體作業系統方面，華為即將推出的「鴻蒙」作業系統未能持續與美國微軟、蘋果之作業系統或臉書等社群媒體服務相容，不僅市場預期不樂觀，中國大陸也承認該系統未臻成熟。因此，中國大陸一方面釋放「長鑫」與「鴻蒙」等軟硬體自主的訊號，並以民族主義驅動消費者購買華為新推出之5G手機，衝高市場銷售量，以彰顯華為雖受困仍大有可為之氣勢；另一方面則謹慎營造其科技自主論述，不諱言其硬體技術差距與作業系統使用友善性，均仍有相當大的精進空間。

其次，在市場層面，美國則積極遊說並施壓各國排除華為5G，但力有未逮，連「五眼聯盟」（Five Eyes）的組成國都未必買單。前英國首相梅伊（Theresa May）允許華為向英國5G工程提供通訊天線等非敏感核心設備。英國聲稱將限於非敏感核心網路，例如天線與基地台，才能採用華為5G系統。此外，身為北約盟國的德國，其首相梅克爾（Angela Dorothea Merkel）也不主張排除華為5G系統，因此德國也可能比照英國區隔核心網路與非核心網路的作法。

敏感核心網路包括設備認證、語音和數據傳輸、計費等運算功能，而非核心網路則為天線與基地台等傳輸電波以接取（access）核心網路的設施。若依照華為的5G部署規劃，其提供的完整解決方案（total solution）包含基地台、核心網、承載網與終端等產品和技術服務。換言之，英國與德國可能允許採用華為5G的範疇，其實包括：基地台、承載網與終端等產品和技術服務。另一方面，美國的國安官員則強烈質疑，隨著5G時代帶來的寬頻與快速運算，核心網路與非核心網路在4G時代存在的界線將逐漸消失。因此，想要降低風險，就得要全面禁止採用華為5G網路。

敏感核心網路設施不僅是關鍵資訊基礎設施的要素，其運算能量也是未來5G鏈結物聯網的「工業4.0」關鍵核心。因此，敏感核心網路的資訊安全將對供應鏈安全影響甚鉅。在供應鏈與關鍵資訊基礎設施中，隨著資訊科技（information technology, IT）與作業科技（operation technology, OT）界線漸趨模糊，不僅氣密隔離內網的工控系統資訊安全防護屢遭攻破，也等於讓敏感核心網路與非敏感核

[2] Diego Oré, "Huawei says it is readying possible Hongmeng software roll-out," *Reuters*, June 14, 2019, https://www.reuters.com/article/us-huawei-tech-hongmeng-launch/huawei-says-in-process-of-preparing-hongmeng-software-roll-out-idUSKCN1TE3E0.

心網路之間的安全隔離逐漸失效，這將增加關鍵資訊基礎設施保障與供應鏈的資安風險。

「五眼聯盟」及北約盟國若依循英國與德國可能的作法，在非敏感核心網路採用華為設施，即使成功隔離敏感核心網路與非敏感核心網路，若在非核心的使用端與通訊傳輸網路間，有別於過去運用wifi或藍芽，而全面改採用5G，進行邊緣運算（edge computing），並設置後門回傳運算結果，一樣可獲取大量情資，遂行即時大規模的網路竊密與監控。據此，當外界仍質疑華為會否成為中共政府遂行網路竊取機密及大規模監控的幫兇，英國與德國一旦在非敏感核心網路採用華為5G，將因核心與非核心之間，在安全風險管控與技術層次上都愈來愈難以區隔，讓「五眼聯盟」與北約盟國在國家間的情報交換，增添洩密風險，並使反制網路竊密與監控的反情報作業更形複雜。

二、中共與華為的反圍堵

前述的發展可能導致中共借助俄羅斯獨立自主根伺服器之網路系統Runet，並在中國大陸的國內市場與「一帶一路」沿線國家之外，把反圍堵陣線擴大到俄羅斯廣大市場，以形成中俄陣營與美歐陣營之間壁壘分明的對峙。華為已針對俄羅斯提出以 Aurora 為架構的作業系統，而希望順利進入俄羅斯市場。此外，在二分的格局下，不排除華為可能買回已售出之華為海纜，為將來中俄陣營進行海纜布局，形成從資料傳輸到消費者使用端設施均為完整自主系統局面。

(一)華為的「無間諜協議」提議

對於許多國家而言，華為 5G 不僅物美價廉，其售後服務具有更大的吸引力。由於 5G 技術尚未成熟，在數據傳輸品質與穩定性上，必須由 5G 設備供應廠商持續測試與改進。然而，這也意謂設備供應商提供服務與設定參數後，可能就掌握使用客戶的數據。若是對供應廠商不是完全信任，自然有安全疑慮。美國對華為就以華為總裁任正非具解放軍背景、華為資通訊產品暗設後門裝置，以及中共之《國家情報法》要求中國大陸公民與業者配合中共政府蒐集情報之三大安全憂慮為由，以「五眼聯盟」為起點，發動全球抵制華為 5G。中共反制之道，即由華為聲稱願意與德國、英國以及其他國家政府，簽訂「無間諜協議」（No Spy Agreement）。考量網路安全技術層面，若要有效防禦網路攻擊，「無間諜協議」其實技術層面意義不大，主要是在國安層面的宣示安撫意味濃厚。

美國為圍堵華為5G設備所提出的主要安全疑慮，就是華為會在軟硬體裝置上裝置後門，將資料非法傳輸回中國大陸。華為過去採用的反制論調，是以技術安全驗證為主，論證自身的軟硬體設備經得起使用國公私部門的驗證。雖然華為軟硬體如同其他廠商產品一樣存在資安漏洞，但以其在英國、德國設置實驗室之測試結果為例，強調並未發現華為有裝置後門之行徑。美國為了反制華為技術無安全疑慮之論述，特別強調5G技術尚未成熟，必須由5G設備供應廠商持續測試與改進，故設備供應商除可藉此掌握使用客戶的資料，並能於必要時，藉更新軟體或維修硬體以裝置後門。

華為借鑒德國於2013年對美國提議簽署網路「無間諜協議」（美國後來予以婉拒）、俄羅斯與中共於2015年5月簽署的《網路互不侵犯條款》（*Cyber Non-aggression Pact*），以及2015年9月美國與中共簽署的《美中網路協議》（*U.S.-China Cyber Agreement*），積極對德、英兩國倡議簽署「無間諜協議」，強調華為除了不會裝置後門，也將不接受中共政府提供用戶資料之要求。現在華為將目標轉向亞洲，開始對印度提議簽署類似性質的「無後門協議」，但由於過去華為在印度的資安紀錄欠佳，而且印度對中共的安全威脅有所忌憚，故印度各界迄今對此提議興趣不高。[3]

(二)中共官方配合華為反圍堵舉措

美國對華為的安全疑慮，還包括華為總裁任正非具解放軍背景，以及在中共的《國家情報法》下，華為必須配合中共政府要求，將資料提供情報部門。如此一來，華為從後門竊取的資料即可為中共「國家安全部」等情報部門所用，對使用華為5G的國家而言，形成重大的國家安全威脅。英國智庫「亨利·傑克遜學會」（The Henry Jackson Society）於2019年5月中旬發表的研究報告，即為最有力的例證。該學會研究人員在研究大量華為員工簡歷後，發現華為與中共情報部門和軍方的聯繫，以及許多華為員工與中共安全部門及軍隊曾經合作的經歷。[4]然而，科技產業員工與國安部門合作計畫，其實並不少見，故該智庫報告尚不足以坐實美國的指控。

前述所呈現最大的癥結，還是在於中共的《國家情報法》所造成的安全威脅。但僅有華為高層單方面承諾不接受中共官方要求提供資料，還不足讓其「無間諜協議」具有說服力。中共駐英大使利用回應「亨利·傑克遜學會」研究報告的機會，趁勢表態不會要求華為替中共情報部門提供用戶資料，並表示英國若採用華為設備，華為不會被當作蒐集英國情報的工具。中共官方此舉無異於替華為的「無間諜協議」背書，在美國對華為全力圍堵之際，中共官方除在「孟晚舟事件」後抵制加拿大，此刻在美國川普政府對華為箝制尚未實質鬆綁之前，更積極出擊，配合華為倡議，以突破美國的圍堵。

（三）中國大陸將更難以推動海外科研合作

伴隨中國大陸境內與世界多國的5G布局與智慧城市建設，中共勢必加強鼓吹與推銷中國大陸的華為5G布建及其他諸如「抖音」之短影片軟體。中共為消除各國安全疑慮，甚至可能由官方出面積極為「無後門協議」背書。但隨著「學習強國」App暗設後門以及「中譯語通」協助中共國安機構在新疆從事大規模監控等種種疑雲的擴散，預料將讓中國大陸5G「無後門協議」前景愈加不樂觀。此外，中共國企或者私營之科技營運商為確保創新技術可持續產出，過去積極投資或捐助海外科研高等教育或研究機構，隨著技術用戶個資經後門而外洩到中國的疑雲

[3] Rahul Satija, "India still wary of Huawei's 5G despite 'no back door' pledge," *Nikkei Asian Review*, July 8, 2019, https://asia.nikkei.com/Spotlight/Huawei-crackdown/India-still-wary-of-Huawei-s-5G-despite-no-back-door-pledge2.

[4] Bob Seely, Peter Varnish, and John Hemmings, *"Defending our Data: Huawei, 5G and the Five Eye," The Henry Jackson Society Report, May 2019,* https://henryjacksonsociety.org/wp-content/uploads/2019/05/HJS-Huawei-Report-A1.pdf.

升起，加上先前即甚囂塵上的竊密風波衝擊，以及美國從2018年延續到2019年反制中共「千人計畫」風潮，未來中國大陸科技廠商之海外產學或產研合作將因諸多資安疑慮而愈發困難。

（四）華為與海纜業務布局

根據《法新社》2019 年 6 月 3 日報導，華為的合資企業、全球第四大海底電纜業者華為海洋（Huawei Marine Networks）將出脫他們的大部分股份。根據上海證券交易所的資料，江蘇光纖通訊網路商亨通光電股份有限公司，將買下華為海洋 51%的股份。華為海洋已成為海底電纜工程界第 4 大業者。除了參與約 90 項海底電纜鋪設或升級工程，更負責不少重大的海底電纜工程，包括 2018 年 9 月連接巴西與喀麥隆之間的 6035 公里海底電纜完工，橫跨墨西哥加州灣的海底電纜則即將完工，而連接歐亞非三大洲的 1.2 萬公里海底電纜也在 2019 年開工。2015 至 2020 年，華為海洋預計鋪設完成 28 條海底電纜，占這段期間全球完工數量近 1/4。華為可藉華為海洋在海底電纜的全球擴張，介接其全球擴張的 5G 建設，構成不受制於美歐國家的全球網路基礎設施。[5]

美國全力抵制華為 5G，強調 5G 安全風險不分核心與邊緣，而海纜傳輸一直是監控資料流的目標，尤其華為持股 51%的華為海洋已成為全球第 4 大海底電纜工程商，美國也絕對不會予以輕忽。由於華為海洋可以接觸海底電纜，可能暗中裝設監控設備或是引導資料傳輸轉向的裝置，一旦爆發衝突時，便能隨時切斷整個國家的網路連線。另一方面，美國電信業者與網路內容提供業者也不樂見華為在海底電纜的擴張，畢竟華為可能藉此確立其通訊傳輸標準的全球領導地位，進而威脅美國的國家競爭力與國家安全。美國的國安單位因此發動類似抵制華為 5G 的圍堵攻勢，先於 2017 年藉由「五眼聯盟」成員澳洲，試圖擋下華為海洋承建連接雪梨與索羅門群島的海底電纜合約，聲稱這將讓中國大陸有能力透過雪梨電纜登陸點連到澳洲網路系統，形成資安風險。澳洲隨後宣布出資鋪設這條電纜，並將工程轉包給一家澳洲廠商。類似抵制華為 5G 作為之成敗互見，在 2018 年 9 月，美國、澳洲與日本即未能成功擋下華為海洋與巴布亞紐幾內亞簽訂海底電纜工程合約。

華為在 2019 年 6 月初決定出售華為海洋股份給中國大陸本土企業，極可能是以限縮業務、累積財力，作為因應川普下重手之避險手法。未來若受歐美進一步圍堵抵制其 5G 系統，則將可能重新購回，讓自身可以由海纜到接收站、以及 5G 系統之資料傳輸，一直到 5G 手機、含晶片在內的手機元件與其作業系統，都一一發展出自主系統，以擺脫歐美箝制，並以中國大陸以及「一帶一路」國家為市場，期能在系統運作及資料應用上有所突破，形成足以與歐美分庭抗禮的局勢。

（五）中共營造科技自主論調

至目前為止，所謂「美中科技冷戰」所體現的，主要還是美國對中國大陸華為在技術與市場的雙重圍堵，包括社群媒體與App停止提供服務，造成2019年5至

[5] Adam Satariano, "How the Internet Travels Across Oceans," *New York Times*, March 10, 2019, https://www.nytimes.com/interactive/2019/03/10/technology/internet-cables-oceans.html.

6月華為智慧型手機銷售下跌4成，華為因此暫緩推出新型筆電及折疊式手機。[6]為穩固市場，華為甚至開始在菲律賓推出新銷售方案，將來華為智慧手機若不適用Facebook、Instagram、WhatsApp、YouTube和Gmail，可享全額退費。[7]然而，中國大陸在技術方面，迄今仍欠缺形成足以與美歐匹敵的技術。因此，中國大陸一方面釋放軟硬體自主發展的訊號，並以國內市場支撐銷售量，另一方面，則謹慎地營造其科技自主論述，避免科技民族主義在網路上暴衝，造成國際負面觀感而導致進一步反彈與圍堵，如此反而不利於中共刻意營造之受害者與被迫害形象。

肆、民主科技聯盟 vs.中俄非民主陣營

「美中科技冷戰」的成型並非一蹴可及，中方考量到中國大陸、俄羅斯及「一帶一路」沿線國家的市場接受度，不太可能一開始就完全切斷與歐美國家之作業系統、通訊協定及社群媒體軟體規格之相容性。歐美科技大廠考慮到前述陣營之龐大市場與訂單，也會在利益驅動下遊說緩步進行全面禁止支援中方技術規格與系統服務。如此將讓中國大陸自主開發的軟硬體一開始將強調相容性，以換取市場空間與研發時間。但隨著「美中科技冷戰」的成形，國安因素將不斷介入，強化雙邊陣營間技術與服務的區隔，這將讓技術規格與市場也漸趨涇渭分明，進一步將明確劃出技術限制移轉界線，導致市場區隔藩籬與技術限制鐵幕將趨向一致。

如同過去美蘇冷戰一般，科技冷戰藩籬界線的劃訂，主要還是以民主與專制為區隔基準。中共代表的專制威權，隨著網路與人工智慧科技成熟而更加無所遮掩。在意識形態影響與思想控制上，中國大陸網路各式媒體興起，自媒體與簡訊、短影片尤其蓬勃發展。中國大陸字節跳動推出的「抖音」應用程式，不僅在中國大陸境內廣受歡迎，更是風靡全球。北京除嚴加監控網路新媒體上的言論與行徑以進行輿情監測，更對於中共官方認定的有害資訊內容，予以嚴密審查管制。根據中共國務院工業和信息化部所轄「中國信息通信研究院」2018 年 9 月發布的《人工智能安全白皮書》指出，中共官方所認定的資訊安全，不單是資訊傳播安全，還涵蓋了資訊內容安全。[8]據此，網路媒體內容審查的監管，便落在「中央網路安全和資訊化委員會辦公室/國家互聯網資訊辦公室」，即「網信辦」身上，準備以「網路生態治理」為名，要求網路資訊內容服務平台業者，擔負起內容審查的責任。

---

[6] Dan Strumpf, "Huawei Postpones Launch of Mate X Foldable Phone," *Wall Street Journal*, June 14, 2019, https://www.wsj.com/articles/huawei-postpones-launch-of-mate-x-foldable-phone-11560502468.

[7] Zak Doffman, "Huawei Special Warranty Offers '100% Refund If Google And Facebook Stop Running'," *Forbes*, June 18, 2019, https://www.forbes.com/sites/zakdoffman/2019/06/18/first-huawei-offers-of-100-refunds-if-google-and-facebook-apps-stop-running-appear/#50a3e00160c6.

[8] 中國信息通信研究院，《人工智能安全白皮書》，2018 年 9 月，頁 4，http://www.caict.ac.cn/kxyj/qwfb/bps/201809/P020180918473525332978.pdf。

對於內容審查標準，中共官方對於網路內容管制仍以負面表列居多。習近平於 2019 年 1 月 25 日在中共中央政治局第十二次集體學習時，強調官方傳媒及黨媒必須要加速融合各式網路新媒體，「探索將人工智慧運用在資訊蒐集、製作與傳播，以主流價值導向駕馭演算法」。這意味著官方傳媒需要轉型成為網路資訊內容服務平台業者的主體，方能承擔資訊內容安全審查之責任。依照《網路生態治理規定》所擬，網路資訊內容受鼓勵的有七項，遭禁止製作的違法資訊及不良資訊則各十項，顯見中共官方對於網路內容管制仍以負面表列居多。這樣的做法，除讓網路資訊內容服務平台業者在執行審查實務上有較為具體之標準可以依循，也有助於平台業者依照一定標準設計演算法以限縮內容審查範圍。

此外，北京在消極管制網路論言論行為內容與傳播手段之餘，轉為積極主導輿論走向。習近平所強調的官媒黨媒藉助人工智慧演算法，以強化官方價值輿論的主導性，各黨國喉舌紛紛呼應，除依指示積極結合諸如「抖音」、「快手」等工具，希望打入年輕族群，更強調在傳播手段上，藉助演算法之推薦技術，加速官方輿論之散播，並期能依照大數據分析後，針對個別特性之閱聽族群，以精準輿論導引與資訊傳播，形成網路聲浪，塑造官方輿論為主流輿論之聲勢。

人工智慧應用雖強調機器自主學習，但北京對於人為介入並未鬆手。在資訊內容方面，北京仍著重於資訊內容安全的管制面，對於前述負面表列之禁止與不良資訊，除列為有害資訊，並強調結合社會信用體系，對製作及散播有害資訊者施予聯合懲罰機制。習近平所謂的「以主流價值導向駕馭算法」，就是排除自主性人工智慧，並高度倚重人為監管的演算法，不斷調整負面表列清單，並視機器學習後的成果調節演算法。按照《網路生態治理規定》所擬，用來管制網路媒體內容與傳播手段的人工智慧科技本身，也必須要建立符合官方價值觀的推薦模式與人工干預機制，如此不僅為人為干預演算法奠定合法基礎，也毫不避諱只要依照官方價值，即為依循主流價值的演算法內建偏見。

中共運用官方強調管制與威權的價值偏見，將人工智慧應用於諸如網路內容審查、辨識虛假訊息與輿情監測之資訊內容安全，這方面舉措已展現相當成果。前述中共國務院工信部「中國信息通信研究院」的《人工智能數據安全白皮書》指出，百度所推出的「人工智慧+廣告打假」，僅2018年上半年，所處理的有害資訊就達145.4億條之多。2019年「阿里巴巴」推出「人工智慧謠言粉碎機」，對新聞內容的可信度識別，在特定場景中的準確率已達到81%。此外，「中國資訊通信研究院」基於所積累的標準樣本資料庫，開展對淫穢色情、涉恐涉暴等違法資訊識別的模式訓練，初步實現基於人工智慧技術的不良資訊檢測能力，識別準確率達到97%以上。[9]可以預見，北京勢將以網路生態治理之名義，運用網路內容審查所累積之機器學習與演算法，設計出足以製造虛假輿論訊息、具影響力的人工智慧演算法，以及足以迅速散播的網路媒體推薦模式，為境內維穩所施行之輿論戰、心理戰等資訊作戰預作演練。

[9] 中國信息通信研究院，《人工智能數據安全白皮書》，2019 年 8 月，頁 21-22，http://www.caict.ac.cn/kxyj/qwfb/bps/201908/P020190809481299621393.pdf。

中國大陸的人工智慧應用於產製傳播內容，並將逐漸輸出境外，以竟「影響力作戰」之功。中國大陸各網路資訊內容服務平台業者運用主要來自境內之大數據資料，進行前述網路思想暨輿論維穩。在北京對於管制有害訊息嫻熟後，運用演算法實現推薦機制，以及運用機器學習推展官方論述成為主流輿論的作法，將逐漸成為輔助北京遂行「大外宣」以對外輸出中共價值觀的利器。在中共對外宣傳內容屢遭譏為刻板不入心的時候，以人工智慧輔助之宣傳內容輸出，一開始或許因資料不足，未能掌握國外各地民眾對中國的認知與心態，而導致內容不能達到足夠影響力，但隨著對境外資料積累，以及演算法能逐漸因地與因人制宜，長久下來將可望呈現機器學習的成效，讓「大外宣」的內容與管道，更加貼近境外閱聽眾，達到其「影響力作戰」之目的。

最後，中國大陸發展的App影響力開始受全球矚目，主要是因為「抖音」的興起。「抖音」已然成為全球最受歡迎的短影片App，但曾因其未善盡平台管理責任，未將不當內容移除，而遭印度政府暫時禁用。此外，美國對於「抖音」會否將用戶資料回傳中國，存有高度國安疑慮。儘管「抖音」雇用公關與法律顧問，宣稱在美先行加強內容管理之平台責任，且用戶資料會儲存在非中國大陸的第三地，但基於美國資訊平台服務廠商備受威脅，國會仍執意以國安考量，對「抖音」展開調查，美國國防部也開始關注美軍使用「抖音」會否造成國安機密外洩的風險。美國產官界對付「抖音」的方式與步驟，類似複製當初對付華為的招數與步驟，而「抖音」也積極消除疑慮，這除了體現華為圍堵與反圍堵模式的逐步擴散，也彰顯背後民主與專制價值的互斥，並將進一步鞏固科技冷戰兩極陣營的對峙態勢，雙方相互施展影響力的交手也將愈形激烈。

伍、小結

「美中科技冷戰」在資通訊設施軟硬體安全上的考量，驅動生產供應鏈的移轉，尤其是移出中國大陸，以及未來一旦中俄非民主陣營成型，生產供應鏈將進一步移出「一帶一路」沿線國家。台灣除藉此機會迎接台商回流，更藉此爭取高科技大廠來台加碼投資設廠，在台灣打造高科技生產供應鏈。

隨著台灣在高科技產業生產供應鏈重要性隨之提升，全球高科技產業也將因此更在意台灣的安全處境。這將促使美歐陣營對於中共的威脅更加積極注意並提出警告，以維持台灣這重要夥伴的安全穩定。因此，美方也將台灣納入反制陣線，對抗中方陣營藉科技輔助之影響力滲透。與此相關的美台之間互動交流，從軍事、經貿、文化、傳播、教育、科技轉移，均將隨之加強，為台灣之安全，帶來更大的保障。

「美中科技冷戰」讓台灣在高科技產業生產供應鏈重要性隨之提升，相關挑戰也伴隨而來。首先，中共官方與科技業者為尋求突破技術圍堵，極可能進一步加強滲透竊取我方高科技營業秘密。產官學研需加強與國安部門反情報單位之聯

繫合作，共同協防我科技產業。對於包括科技專案計畫之科研項目，均予以加強內控，並在通報可疑事件後，配合執法單位調查，以反制中方竊取營業秘密。

其次，「美中科技冷戰」本身的安全考量，也可能促使美歐科技大廠基於台海安全風險而將資金廠房轉移回美歐。美國對於科技冷戰有其務實的實踐途徑，尤其是在聯合友盟以限制華為5G部署力有未逮之後，開始從自身的生產鏈安全要求做起，而其對於台積電的做法，就是最佳例證。一方面，在台灣的台積電仍可維持對中國大陸的市場，並繼續控制美國製造之關鍵技術與零組件成份。另一方面，台積電被要求回美國設廠，讓美國得以落實技術管制，優先轉移最新技術下單給台積電美國廠，並遵循其國防產業與政府採購不使用中國大陸製關鍵零組件的規範。台灣對此必須予以正視，雖然科技廠基於風險分散原則，不將關鍵廠房全都集中在一地，實乃務實之舉。但是，對於「美中科技冷戰」衍生之台海安全風險，台灣本身可提出交易成本與風險投資組合的實證分析與安全論述，除藉此作為積極因應，並進一步鞏固台灣在民主科技陣營中的價值鏈區位。

（責任校對：洪瑞閔、林政良）

第二篇 接軌國際安全市場：

科技與產業的安全控管

本頁空白

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。[1]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

[1] 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。[2]

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

[2] 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」。[3]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。[4]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。[5]

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。[6]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。[7]

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

---

[3] 〈《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。

[4] Chris Miller, "The INF Treat 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/.

[5] 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/.

[6] 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.

[7] 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」。[8] 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。[9]

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，新合成鍺酸鉍銫（cesium bismuth germanate，化學式 $Cs_2Bi_2O(Ge_2O_7)$，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 KH_2PO_4，簡稱 KDP）晶體相比，鍺酸鉍銫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。雖然使用鍺酸鉍銫晶體，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。[10]

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。[11]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。[12]

---

[8] 〈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。

[9] 「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。

[10] 〈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。（此新聞內文鍺酸鉍銫翻譯有誤，另參戴元超，〈鍺酸鉍(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。）

[11] 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.

[12] "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。[13]「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。[14]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。[15]

---

[13] "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.

[14] Anthony Spadafora, "Intel reveals first AI chips," *techradar.pro*, August 21, 2019, https://www.techradar.com/news/intel-reveals-first-ai-chips.

[15] 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」。[16]「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。[17]

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。[18]

《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。[19]

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。[20]

---

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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、[21]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。[22]

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。[23]

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。[24]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。[25]

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.

[21] 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.

[22] 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.

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

[24] 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_poopoos_google_quantum_claims/.

[25] 〈「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。[26]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。[27]

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。[28]

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。

---

[26] 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.

[27] 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.

[28] 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，[29]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。[30]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。

---

[29] 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。

[30] "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）[31]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」。[32]

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

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

[32]"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。[33]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。[34]

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

[33] "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.

[34] 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.wtocenter.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》。[35]

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

[35] 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。

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。[36]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 電話機制造業、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

[36] 〈対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 。

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。[37]

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。[38]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。[39]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。[40]

（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

[37]〈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。

[38] 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%。

[39] 占部絵美，〈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。

[40]〈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）》，[41]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。[42]

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

[41] 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。

[42] 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/anpo/law_document/tutatu/t07sonota/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。[43]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。[44]

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）。

[43] 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.

[44] 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.新興技術首度為管制對象 2.滾動調整對列管技術之界定	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	1.增加外來直接投資事先申報之業種 2.擴大外來直接投資事先申報之範圍	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	頒布專用指導方針，並召開說明會和派遣顧問。	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)

本頁空白

第四章　國防產業安全

吳俊德、蔡榮峰*

壹、前言

在今日專業且分工的生產體系下，一項產品的製造要經歷複雜的流程，各部分的零組件分由位在不同國家的不同廠商製造，最後加以組裝才得以完成。跨國產業鏈已經成為今日工業製造的常態，其中如果有一個環節出了差錯，產品的品質就會受到影響。因此，產業安全成為一項重要的課題，這個問題在國防軍事裝備以及武器系統的生產製造上尤其重要。這些產品應用尖端科技與關鍵技術、其性能攸關一國國力、又有許多民間廠商協力，如何在軍事用品的製造過程中確保品質，又不會讓關鍵技術或機敏資料外洩，成為國防產業的重中之重。本章將由各個面向來探討國防產業安全，由於美國在此議題上的規範較為完備，本章將以介紹美國的機制為主。第貳部分是投資審議與安全評價機制，第參部分是公司安全治理與廠商分級，第肆部分是生產流程與供應鏈安全，第伍部分是終端市場及安全認證，第陸部分為小結。

貳、投資審議與安全評價機制

在經濟活動中，不論是生產商品或提供服務，都必須要使用人力、原料、工具、空間等各項因素，因此在經濟學中，勞動、土地、資本、以及企業才能被稱為是生產要素（factors of production）。當一個國家擁有愈充足的生產要素，其經濟活動就可能愈蓬勃；反之，當一個國家的生產要素不足，經濟活動就會受到限制，因此，生產要素是否能充分供給，成為一國經濟發展的關鍵因素。在這四項生產要素中，除了土地之外，其他三項都可以從國外引入。若是一個國家有著開放的經濟環境，讓生產要素能夠較輕易地跨境流通，將對其經濟發展提供正面及積極的貢獻，並能提升在國際上的競爭力。

雖然勞動、資本、以及企業才能都能從國外引入，在這三者當中，最普遍也最受重視的莫過於外國資本進入本國。這是因為勞動力的進入涉及到人的移動，所造成的問題較多也較複雜；資本流動可能造成的問題比較容易管制，且今日的科技可以很迅速地將非常大量的金額轉移到另一個國家。職是之故，世界上大部分國家對於外國資本進入本國，也就是所謂的「外來直接投資」（Foreign Direct Investment, FDI）大多抱持歡迎態度，以利產業與經濟發展。

然而，FDI 也可能對一國造成負面影響。倘若 FDI 是以「兼併與收購（下稱併購）」（Merge & Acquisition, M&A）的方式，亦即外國公司對本國企業透過購

* 吳俊德，網路作戰與資訊安全研究所助理研究員，負責本章第壹、貳、肆、陸節；蔡榮峰，國防資源與產業研究所政策分析員，負責本章第參、伍節。

買或轉讓股權取得經營權，可能會產生許多問題。首先，企業被外資併購後可能將本國勞工裁員或調職，傷害本國人民權益。其次，外資企業可能從事會造成污染的產業，破壞本國環境。第三，外資企業可能將公司資產移至海外，形同淘空本國資產。第四，原物料或是土地開發產業若是被外資掌握，對本國市場穩定反而不利。第五，外資企業若是進入可做軍事用途的敏感科技或是關鍵技術產業，等於協助其提升技術能力，本國技術領先優勢將不保。最後，某些產業攸關人民日常生活及政府運作，例如能源產業與關鍵基礎設施（critical infrastructure），若是由外國企業掌控，恐將危及國家生存。[1]

由於這些負面影響，各國政府在歡迎 FDI 的同時，也都設立投資審議機制對 FDI 加以審核，尤其是對由外國政府所擁有或是控制的企業所進行的投資，更是格外謹慎。在世界各國當中，美國的投資審議機制可說是最為完備而嚴謹，本節將簡介美國的投資審議機制及其最新發展，以為借鏡。

一、美國外來投資審查委員會

美國政府對於 FDI 的審查，「美國外來投資審查委員會」（Committee on Foreign Investment in the United States, CFIUS）扮演舉足輕重的角色。CFIUS 是在 1975 年由福特（Gerald Ford）總統以行政命令所成立，為一個跨部會的委員會，由內閣中不同部會的首長所組成，主要職掌為審視可能會對美國國家利益有重大影響的外來投資。自成立至今，CFIUS 的成員組成歷經數次立法及修法變革，目前是由財政部長擔任主席，成員包括 9 個常設成員、5 個參與及觀察成員、以及 2 個不具投票權但依法必須參與的成員。

CFIUS 的 9 個常設成員為財政部（Department of the Treasury）、司法部（Department of Justice）、國土安全部（Department of Homeland Security）、商務部（Department of Commerce）、國防部（Department of Defense）、國務院（Department of State）、能源部（Department of Energy）、美國貿易代表辦公室（Office of the U.S. Trade Representative）、科學與技術政策辦公室（Office of Science & Technology Policy）；5 個參與及觀察成員為管理與預算政策辦公室（Office of Management & Budget）、經濟顧問會議（Council of Economic Advisors）、國家安全會議（National Security Council）、國家經濟會議（National Economic Council）、國土安全會議（Homeland Security Council）；2 個不具投票權的成員為國家情報總監（Director of National Intelligence）以及勞工部長。[2]

CFIUS 可以針對任何外國投資人對美國進行跨州投資併購行為時，審查其是否威脅國家安全。CFIUS 以多數決作出對外來投資審查之決議，包括在任何情況

[1] 王震宇，〈外人投資併購與國家安全審查機制之比較研究—以中國大陸國營企業海外併購個案為例〉，《台北大學法學論叢》，第 98 期（2016 年 6 月），頁 248-249。

[2] 關於 CFIUS 的成員組成，請見 https://www.treasury.gov/resource-center/international/foreign-investment/Pages/cfius-members.aspx。

下要求該交易停止，但是該決議並不具有法律強制力，僅為提供總統建議之用，美國總統才是外來投資最後的裁決者。[3]

美國政府對國家安全一詞未曾提出明確定義，這使得 CFIUS 在審查 FDI 時有著相當彈性的空間去詮釋國家安全。然而，在一些重大歷史事件及歷次關於 CFIUS 的立法及修法過程中，某些國家安全的內涵有被提及，此也造成 CFIUS 管轄範圍的演變。2001 年 9 月 11 日發生 911 恐怖攻擊事件，讓美國的國家安全面臨恐怖主義的陰影，時任總統的小布希（George W. Bush）除設立國土安全部，也在 2003 年將該部首長納入 CFIUS 的常設成員。這使得 CFIUS 原來傾向以經濟觀點考量外來投資，開始轉變為以國家安全來考量；對 FDI 的審查焦點，也從較狹隘的國防產業，逐漸轉移到關鍵基礎設施。[4]

2007 年美國通過《外來投資與國家安全法》（*Foreign Investment and National Security Act*）並在 2008 年 1 月開始實施，該法除了規範 CFIUS 的法定權限及成員組成外，最重要的是將國土安全與關鍵基礎設施作為識別國家安全的成分，且明訂總統在評估外來投資對國家安全的影響時，必須將這兩項因素列入考量。此外，該法也要求 CFIUS，凡外國投資者是由外國政府持有或控制的，無論其交易本質為何，一律進行調查。在《外來投資與國家安全法》實施以後，CFIUS 的運作更為嚴密完整，其管轄範圍也正式擴大到關鍵基礎設施。[5]

二、美國改革投資審議機制以因應中共威脅

近五年來，美國具有高度機敏性的關鍵技術外流嚴重，在全球的科技領先優勢急遽縮小，究其原因，矛頭直指在 2015 年提出「中國製造 2025」，意圖成為世界製造強國的中國。根據 2018 年 1 月美國國防部的研究，中國取得美國技術的管道，雖然有部分是駭客經由網路侵入美國企業竊取資料而得，但大多數仍是透過投資進入美國市場後，藉由取得公司股東身份得以接觸到機密資訊，或是收買公司內部人士取得技術文件。[6]

基於此，美國政府從行政部門到立法部門對 FDI，尤其是來自於中國的投資提升警覺，參眾兩院在 2018 年對此議題分別提出法案，對 CFIUS 的審查機制進行改革，最後協調出《外來投資風險審查現代化法》（*Foreign Investment Risk Review Modernization Act*, FIRRMA），該法合併於《2019 財政年度國防授權法》（*National Defense Authorization Act for Fiscal Year 2019*, NDAA 2019）之下提出，並於 2018 年 8 月 13 日經川普（Donald Trump）總統簽署通過。FIRRMA 的大部

[3] 王震宇，〈外人投資併購與國家安全審查機制之比較研究—以中國大陸國營企業海外併購個案為例〉，頁 290。

[4] Edward M. Graham and David Marchick, *US National Security and Foreign Direct Investment* (Washington D.C., Peterson Institute Press, 2006).

[5] 邱奕宏，〈美國外來投資審查及「外來投資與國家安全法」之發展〉，《貿易政策論叢》，第 21 期（2014 年 7 月），頁 22-25。

[6] Michael Brown and Pavneet Singh, *China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation* (Washington D.C.: Defense Innovation Unit Experimental, 2018), https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf.

分條款要等到施行細則公布後才生效，在此之前，美國政府在 FIRRMA 授權下，對關鍵技術領域的 FDI 實施「新前導方案」（New Pilot Program）。該方案於 11 月 10 日正式開始實施，預計試行到 2020 年 3 月 5 日。[7]

「新前導方案」公布 27 項產業為關鍵技術領域，較受矚目者包括先進製造（含飛機及發動機）、機器人、半導體及晶片、人工智慧、生物醫藥技術、無線通信設備、以及奈米技術等。只要是與此 27 項產業當中任何一個環節相關，不論是設計、開發、生產乃至於組裝之 FDI 交易，都必須在交易完成日前 45 天向 CFIUS 履行通報。值得一提的是，FIRRMA 並非針對特定國家，普遍適用於所有外資，但 FIRRMA 仍有具體的防堵中資規定，要求美國商務部必須針對中國 FDI，每兩年向國會及 CFIUS 提出報告，以確切掌握中資對美國整體投資情況。[8]可以說，FIRRMA 對美國投資審議機制的改革，是為了因應中共威脅而來。

過去 FDI 投資審議僅在交易方自願通報 CFIUS 後才啟動審查，且僅限於外國投資人對美國企業取得控制權的投資。FIRRMA 的亮點在於不僅擴充 CFIUS 可審查的交易型態，且有若干類型的交易強制在事前必須向 CFIUS 通報，即便是該項投資並不足以取得美國企業的控制權，即「非控制性投資」（non-controlling investment）。這些必須事前通報的交易包括：第一、涉及國家安全的敏感性不動產交易；第二、使外國投資人得以取得基礎關鍵設施、非公開的關鍵技術、或個人敏感資訊的「非控制性投資」，如取得董事會席次、觀察員、或其他得以介入公司決策的權利；第三、變更既有投資下外國投資人的權利，而該變更可使外國投資人獲得上述關鍵技術資訊或個人敏感資訊。[9]

美國財政部於 2019 年 9 月 17 日公布 FIRRMA 施行細則的草案，並以 1 個月的時間徵求大眾意見。此草案對投資國設有例外條款，來自例外國家之 FDI 只要不違反美國法律，可以不受 CFIUS 擴大之管轄限制。例外國家之認定是由 CFIUS 主席及成員以三分之二多數決投票決定，美國財政部至本年報出版前尚未確認任何國家為例外國。[10]

參、公司安全治理與廠商分級

隨著國防領域所涉及的各類尖端科技發展資本門檻越來越高與私部門於軍民通用科技之創新速度逐漸超越公部門的情況下，各國政府需要民間創新技術，企業則需政策鼓勵才有能力持續研發。受到國際經濟自由化潮流影響，包括台灣在內，先進國家的製造工業於過去 30 年間快速全球化，致使跨國產業鏈成為工

[7] 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.wtocenter.org.tw/mobile/page.aspx?pid=318503&nid=126。

[8] 顏慧欣，〈美國外人投資審查機制之改革方向與影響〉。

[9] 孫欣、洪唯真，〈美中角力關係下，跨境商務和投資如何管理法律風險〉，安侯法律事務所，2019 年 9 月 9 日，https://home.kpmg/tw/zh/home/insights/2019/09/tw-american-china-trade-war-investment-cross-border-law-risk-management.html。

[10] 李宜靜，〈美國盟友之企業團體要求暫緩投資審查〉，《WTO 及 RTA 電子報》，第 667 期，2019 年 10 月 24 日，https://web.wtocenter.org.tw/Page.aspx?pid=331027&nid=120。

業製造之常態。然而，全球分工對於保護智慧財產權帶來新的挑戰。該如何透過政府機制保持商業彈性而又同時有效管控國安風險，已是國家發展國防工業重要課題。

一、公司安全治理

根據 2001 年美國國防部報告《智慧財產權：航渡商務之海》（*Intellectual Property: Navigating through Commercial Waters*）的概念，國防科技涉及專利、著作權、商標、營業秘密（trade secrets）、技術資料（technical data）與電腦軟體。其中，只有營業秘密這一項無專用期限，只要不公開就可以永久專用；除了保護範圍較廣，它也有專利替代效果，為國防與科技產業之基礎，因而備受重視。[11]

營業秘密必須符合「秘密性」、「具經濟價值」、「採取合理保密措施」三大元素，可概分為「商業性營業秘密」及「技術性營業秘密」兩大類。商業性營業秘密指涉與經營相關之資訊，如客戶名單、定價策略、交易底價、人事管理等。技術性營業秘密則指特定領域的創新技術，如技術、製程等。而營業秘密與企業內部安全管理機制息息相關。

公司安全治理機制可用「管理標的」來區分為「物件管理」、「人員管理」、「組織管理」三大區塊。首先，「物件管理」的核心要旨在於如何依照資訊生命週期來保護記載營業秘密的實體與數位載體，諸如網路資訊安全、機密卷宗歸檔等。其次，「人員管理」強調錄取前的安全查核，以及錄用後員工對於保密責任的認知與遵守。最後，「組織管理」則是指以設計安全機制來宏觀管控前述的物件與人員互動所產生的安全風險，可說是安全管理的成敗關鍵。其兩大核心分別為「機敏資訊管理」與「存取權限管理」。資訊可依其特性、可被利用的方式以及經濟價值等來制定機密等級，且包括標示方式皆屬機敏資訊之管理範疇。而判定需保密之資料，就按照「需知原則」（Need-to-Know Principle），讓只有業務上需要知道的人員才能取得。因此，公司內的成員須依其職務給予差異化的資訊存取權限，藉此避免單一人員掌握完整業務資訊。

[11] 技術資料包括任何涉及研製、後勤過程或訓練等技術相關的圖像與文字記錄，例如圖紙或操作手冊等，但是不包括數位程式碼，因此電腦軟體單獨成類，見 U.S. Government, *Intellectual Property: Navigating through Commercial Waters Appendix B* (Washington D.C.: Department of Defense, 2001), https://www.acq.osd.mil/dpap/specificpolicy/intelprop.pdf。

表 4-1、公司安全治理機制

物件管理	門禁管制、卷宗/數位檔案管理、網路資訊安全、內外網實體隔離
人員管理	背景安全查核、身分識別系統、資安訓練、保密協定、外部合作規範
組織管理	機敏資訊分類/儲存/傳輸制度、實體/數位存取權限設定

資料來源：蔡榮峰整理自公開資料。

除了公司企業內部規範之外，政府為鼓勵創新與扶植包括國防在內的國內產業，也會透過立法保護境內廠商，以遏止非法竊用智慧財產之惡性競爭，尤其涉外商業間諜案之襲擾。

美國為彌補各州政府僅以民事責任追訴之不足，遂於 1996 年通過聯邦層級的《經濟間諜法》（*Economic Espionage Act 1996*）正式追訴侵害營業秘密者之刑事責任，將企圖使外國代理人獲益之行為、無須經過物理移轉之侵害行為，如非法洩漏前雇主營業秘密之離職員工等犯罪納入法。[12]2016 年 5 月 11 日則通過《營業秘密防護法》（*The Defend Trade Secrets Act of 2016,* DTSA），把原本屬於州法層級的民事法律適用範圍提升至聯邦層級一體適用，並加入吹哨者保護條款。[13]類似條款也同樣出現在 2016 年 6 月 8 日歐盟通過的《歐盟營業秘密規程 2016/943》，該規程整合了歐盟成員國營業秘密保護法，就民法範圍內給予法律保護，2018 年 6 月 9 日正式生效。[14]我國《營業秘密法》也參考美國《經濟間諜法》，於 2013 年增訂刑事規範第 13 條之 1 項至第 4 項。

二、廠商分級

發展國防產業涉及一個國家的工業基礎與科技發展。單一國防工業產品之產業鏈往往涉及不計其數的上下游承包商。因此，管理相關市場機制的規範，除了經濟考量之外，還必須兼顧國家安全與國防需求，涵蓋的專業領域十分廣泛。為了在管控風險的同時避免阻礙技術創新，國防產業先進國家就會按照國家現有需求的急迫性、須因應的情勢，以及廠商的技術能力與專業領域等面向來制定分級管理制度，藉此避免其國防供應鏈產生薄弱環節，例如台灣軍購的主要來源國—美國就是最標準的例子。

根據美國《聯邦法規》（*Code of Federal Regulations,* CFR）第 7 章第 700 節，以及《國防生產法》（*Defense Production Act,* DPA）所建立的「國防等級與配置系統」（Defense Priorities & Allocations System, DPAS），擇定國防出口由美國商務

[12] Thierry Olivier Desmet, "The Economic Espionage Act of 1996: Are We Finally Taking Corporate Spies Seriously?" *Houston Journal of International Law*, Vol. 22, No. 1 (1999), pp.105-106.

[13] "Senate Bill 1890-Defend Trade Secrets Act of 2016," 114th Congress of United States, May 11, 2016, Section 7, https://www.congress.gov/bill/114th-congress/senate-bill/1890.

[14] 該規程正式全稱為《歐盟保護技能知識與商業資訊（營業秘密）防止非法取得、使用與公開之規程 2016/943》（*Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*）, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0943.

部為業管單位，國防採購項目則由美國國防部提供準則來制定廠商分級制度。採購計畫與廠商人員分成三級制，分別為：國防急迫需求等級的「DX」、國防關鍵等級「DO」以及無等級，個別計畫的分級還會加上分類標號（見表 4-2），例如 DX-A1 為最高等級的航空器製造類別、DO-A3 則為中階等級的船舶製造類別。人員方面，例如持有 DO-A3 的製造商採購人員要採購半導體設備來製造產品時，就必須依照 DO-A3 規定來向下游廠商採購。[15]

事實上，美國的國防採購還將就業機會、新創潛力與社會正義納入考量。根據美國《小型企業法》（*Small Business Act*）第 15 條 g 項，包括美國國防部在內的聯邦政府各部門於招標時，小型企業的「得標主約」（prime contract）以及「轉包」（subcontract）金額加總，不得低於採購總額的 23%。美國國防部的「小型企業計畫辦公室」（Office of Small Business Programs）為業管單位，負責政策協調與相關作業。[16]

表 4-2、美國 DPAS 計畫標號分類表

標號	計畫類型	業管單位
國防採購計畫		
A1	航空器 Aircraft	美國國防部
A2	飛彈 Missiles	美國國防部
A3	船舶 Ships	美國國防部
A4	戰車—汽車 Tank-Automotive	美國國防部
A5	武器 Weapons	美國國防部
A6	彈藥 Ammunition	美國國防部
A7	電子通訊設備 Electronic and communications equipment	美國國防部
B1	軍用建築之供應 Military building supplies	美國國防部
B8	廠商國防生產設備	美國國防部

[15] "Defense Priorities & Allocations System (DPAS)," Defense Contract Management Agency, https://www.dcma.mil/DPAS/.

[16] 保留額內部可細分為 3%為「因公致殘退伍軍人持有之小型企業」（Service Disabled Veteran Owned Small Businesses, SDVOSB）、3%保留給位於「歷史上發展落後地區」（historically underutilized business zones，簡稱 HUBZones）之小型企業、5%「社經弱勢族群持有之小型企業」（Small Business Concerns Owned and Controlled by Socially and Economically Disadvantaged Individuals）、5%為「女性持有之小型企業」（The Woman-Owned Small Business, WOSB），見"Small Business Act," U.S. Small Business Administration, https://www.sba.gov/document/policy-guidance--small-business-act。

	Production equipment (for defense contractor's account)	
B9	政府國防生產設備 Production equipment (Government owned)	美國國防部
C1	戰備糧食 Food resources (combat rations)	美國國防部
C2	國防部建築 Department of Defense construction	美國國防部
C3	國防部設施保養、維修、運作之供應 Maintenance, repair, and operating supplies (MRO) for Department of Defense facilities	美國國防部
C9	雜項 Miscellaneous	美國國防部
針對加拿大的之軍事協助		
D1	加拿大軍事計畫 Canadian military programs	美國商務部
D2	加拿大生產與建造 Canadian production and construction	美國商務部
D3	加拿大原子能計畫 Canadian atomic energy program	美國商務部
針對其他外國之軍事協助		
G1	外國政府所採購經美國國內商業管道出口之特定彈藥項目 Certain munitions items purchased by foreign governments through domestic commercial channels for export	美國商務部
G2	來自加拿大以外的外國政府之特定直接國防需求 Certain direct defense needs of foreign governments other than Canada	美國商務部
G3	除加拿大以外的其他外國製造與建造 Foreign nations (other than Canada) production and construction	美國商務部
針對外國關鍵基礎設施之協助		
G4	外國關鍵基礎設施計畫 Foreign critical infrastructure programs	美國商務部
合作生產		
J1	F-16 合作生產計劃 F-16 Co-Production Program	美國商務部 美國國防部
原子能計畫		
E1	建築 Construction	美國能源部

E2	運轉-包括保養、維修、運作之供應 Operations-including maintenance, repair, and operating supplies (MRO)	美國能源部
E3	私人擁有設施 Privately owned facilities	美國能源部
國內能源計畫		
F1	探勘、製造、提煉與運輸 Exploration, production, refining, and transportation	美國能源部
F2	儲存 Conservation	美國能源部
F3	建築、維修與保養 Construction, repair, and maintenance	美國能源部
其他國防、能源及相關計畫		
H1	其他綜合 Certain combined orders (see section 700.17(c))	美國商務部
H5	國內私人製造 Private domestic production	美國商務部
H6	國內私人建築 Private domestic construction	美國商務部
H7	保養、維修、運作之供應 Maintenance, repair, and operating supplies (MRO)	美國商務部
H8	指定計畫 Designated Programs	美國商務部
K1	聯邦供應項目 Federal supply items	美國總務署
國土安全計畫		
N1	聯邦緊急事態準備、減緩、因應及重建 Federal emergency preparedness, mitigation, response, and recovery	美國國土安全部
N2	州、地方、部落政府緊急事態準備、減緩、因應及重建 State, local, tribal government emergency preparedness, mitigation, response, and recovery	美國國土安全部
N3	情報及預警系統 Intelligence and warning systems	美國國土安全部
N4	邊境與運輸安全 Border and transportation security	美國國土安全部
N5	國內反恐，包括強制執法 Domestic counter-terrorism, including law enforcement	美國國土安全部
N6	化學、生物、放射線及核能應變措施 Chemical, biological, radiological, and nuclear countermeasures	美國國土安全部

N7	關鍵基礎設施保護與重建 Critical infrastructure protection and restoration	美國國土安全部
N8	雜項 Miscellaneous	美國國土安全部

資料來源：蔡榮峰翻譯自“Code of Federal Regulations Part 700-Defense Priorities and Allocations System,” Electronic Code of Federal Regulations, https://reurl.cc/6gq3vZ。

肆、生產流程與供應鏈安全

在今日的工業生產體系下，軍事裝備或武器系統並不是由獲得合約的主承包商（prime contractor）獨力製造，而是由下游眾多協力廠商層層轉包，每一家廠商負責一部份零組件，最後再組裝成最終產品。美國武器製造大廠洛克希德馬丁（Lockheed Martin）宣稱與大約 1 萬 6,000 家供應商合作，而美國國防部總共大約有 30 萬家供應商。[17]這麼多的協力廠商加上層層轉包，很容易造成供應鏈的安全漏洞。從 2017 年起，美國有為數不少的國防承包商（contractor）與轉包商（subcontractor）被中國駭客入侵並竊走重要資料，例如中國駭客於 2018 年 1 月及 2 月入侵一家為海軍水下戰中心（Naval Undersea Warfare Center）進行研發的承包商，竊取了 614GB 的資料，包括由潛艦發射的超音速反艦飛彈、感測器及訊號資料、潛艦無線電室密碼系統、以及海軍潛艦發展單位的電子戰資料庫。[18]

這個事件對美國來說非常嚴重，在軍事力量上，中國與美國最大的差距在於水下作戰能力，如果這些先進科技為中國所用，將會削弱美軍在水下作戰的優勢，一旦未來與中國發生戰爭，整個局勢將可能改觀。因此，加強供應鏈安全（supply chain security）成為美國國防部自 2018 年以來的重點工作。[19]本節將介紹美國目前正在建立的兩項供應鏈安全規範，一是「無侵入交付」（Deliver Uncompromised, DU）；另一是「網路安全完善模式認證」（Cybersecurity Maturity Model Certification, CMMC），最後再介紹美國當前對於供應鏈及網路安全的新思維—「零信任架構」（Zero Trust Architecture, ZTA）。

[17] Nicole Ogrysko, “DoD unveils new cybersecurity certification model for contractors,” *Federal News Network*, September 5, 2019, https://federalnewsnetwork.com/defense-main/2019/09/dod-unveils-new-cybersecurity-certification-model-for-contractors.

[18] Ellen Nakashima and Paul Sonne, “China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare,” *Washington Post*, June 8, 2018, https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html.

[19] Gordon Lubold and Dustin Volz, “Chinese Hackers Breach U.S. Navy Contractors,” *Wall Street Journal*, December 14, 2018, https://www.wsj.com/articles/u-s-navy-is-struggling-to-fend-off-chinese-hackers-officials-say-11544783401.

一、無侵入交付

供應鏈通常會在兩個方面出現安全漏洞。首先，轉包商的規模有大有小。在供應鏈下游的轉包商通常都是小型企業，比較不注意網路安全，也比較沒有財力建立完善的資訊安全系統。因此，這些小型廠商很容易被駭客鎖定並入侵，成為軍事科技被竊取的管道。其次，在層層轉包的機制下，上游廠商往往不知道最後是轉包給哪一家下游廠商。若是最下游廠商發生資安事件，最上游的主承包商無法掌握。這兩項因素會造成關鍵技術在供應鏈的某個環節外洩，或是軍事裝備在生產、組裝流程中被植入後門，而主承包商在完成最終產品交貨時一無所知。

為了增進供應鏈安全，美國國防部現正大力推動「無侵入交付」。DU 的概念最早出現於美國米崔公司（MITRE Corporation）接受國防部委託在 2018 年 8 月提出的報告，該報告強調，民間廠商要承接國防部合約，除了成本、製造時程、產品性能外，安全是第四項考量因素，未能達到安全標準的廠商無法獲得合約。[20]DU 的精神在於供應鏈安全由上游廠商負責，上游廠商要知道每一項零組件是由哪一家下游廠商生產，第一層和第二層的承包商要監督其下的所有轉包商，並且負責管理整個供應鏈，確保每一層廠商往上一層交付的商品沒有受到侵入。[21]

在 DU 的概念下，每一家承包商必須做到兩件事。第一、其自身要符合美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）所頒布的工業標準規範，例如 NIST SP 800-171。第二、確認其下游所有轉包商也符合工業標準規範，若是一家承包商的下游轉包商不符合安全標準，該承包商就無法承接國防部合約。[22]DU 的具體辦法和時程至本年報出版前尚在制訂中，但美國國防部官員已經數次在公開場合倡導，未來必定會具體落實，我國廠商若是有意成為美國國防產業轉包商，必須特別注意 NIST 的工業標準規範。

二、網路安全完善模式認證

美國國防部於 2019 年 8 月公布「網路安全完善模式認證」（CMMC）草案、9 月 4 日公布修正版草案、11 月 8 日再公布第 0.6 版草案。CMMC 是對於國防承包商與轉包商在網路安全上新的標準及規範，以確保供應鏈安全。根據 CMMC 草案，美國國防部將廠商分為 5 級，第 1 級最低，第 5 級最高，要獲得國防部的合約成為承包商，該廠商的網路安全防護至少要達到第 3 級；要成為轉包商，網

[20] Christopher A. Nissen, John E. Gronager, Robert S. Metzger, and Harvey Rishikof, "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War," MITRE Corporation, August 2018, https://www.mitre.org/publications/technical-papers/deliver-uncompromised-a-strategy-for-supply-chain-security.

[21] Justin Doubleday, "New DOD contracts language will hold companies 'accountable' for cyber, supply chain security," *Inside Defense*, May 15, 2019, https://insidedefense.com/daily-news/new-dod-contracts-language-will-hold-companies-accountable-cyber-supply-chain-security.

[22] "Deliver Uncompromised: The Department of Defense's Latest Security Initiative," Aronson LLC, August 27, 2018, https://aronsonllc.com/deliver-uncompromised-the-department-of-defenses-latest-security.

路安全防護也至少要達到第 1 級。而要被評定為第 3 級，一家廠商必須符合 NIST SP 800-171 所規定的 110 項安全管制措施。[23]

具體而言，要成為 CMMC 第 3 級以上的廠商，必須達成的幾項重要安全措施包括：第一、建立與維持由專職人員運作的安全行動中心；第二、建立與維持 24 小時待命的網路安全應變小組；第三、使用自動化機制偵測電腦系統中是否有未獲授權軟體、硬體、或是檔案；第四、當資訊從一個系統轉移到另一個系統時，必須以安全的方式進行控制資訊流，例如資料加密。此外，美國國防部也要求所有承包商與轉包商建立資安事件通報機制，有任何網路入侵事件，都必須在發現後的 72 小時之內通報。[24]

CMMC 的第 0.6 版草案主要是對第 1 級到第 3 級的廠商提出規範，美國國防部要求第 3 級廠商要做到：員工只能接觸到或使用完成其工作所必須的資料與服務。另外，第 3 級廠商也要能夠控制與管理與外部網路相連的公司內部網路，並且控制與限制能夠連接公司網路並獲取資訊的個人通訊裝置，如筆記型電腦、平板電腦、以及手機。[25]

CMMC 按照規劃已經有比較明確的時程，美國國防部預計在 2019 年 11 月底提出第 0.7 版草案，將對第 4 級與第 5 級廠商制訂較明確的規定，然後在 12 月完成最後修訂；美國國防部同時計劃於 12 月建立評鑑機構，並於 2020 年 1 月開始試行 CMMC。[26]因此，想要進入美國國防產業供應鏈的廠商，必須深入瞭解美國的工業標準規範，並加強在網路安全防護機制的投資，才有可能通過認證。

三、零信任架構

在網路安全與供應鏈安全的思維上，美國現今正在進入「典範轉移」（paradigm shift）的時期。最早的安全思維是個別防禦（individual defense），也就是在個別終端設備安裝防毒軟體，掃描並移除電腦病毒。後來個別終端設備彼此相連，系統漸趨複雜，安全思維轉變為「邊緣防禦」（perimeter defense），也就是在系統的對外連接的出入端點設立防火牆，將電腦病毒與入侵者擋在系統外面，系統內部就是安全的。然而，今日的系統太過複雜，可以和外部相連的端點太多，如果還是以設立防火牆的方式來防禦，防火牆的數量將一直增加，造成成本過高且效率不彰。兼以5G通訊技術以及物聯網（Internet of Things, IoT）的發

[23] Nicole Ogrysko, "DoD unveils new cybersecurity certification model for contractors," *Federal News Network*, September 5, 2019, https://federalnewsnetwork.com/defense-main/2019/09/dod-unveils-new-cybersecurity-certification-model-for-contractors.

[24] Kristen Soles and Bhavesh Vadhani, "New DOD requirements – supply chain, risk management, and Cybersecurity Maturity Model Certification," CohnReznick LLP, August 15, 2019, https://www.cohnreznick.com/insights/achieve-compliance-with-new-dod-supply-chain-cybersecurity-rules-and-maturity-model.

[25] Rick Weber, "Pentagon issues draft cyber certification plan, delays input on controls for 'advanced' threats," *Inside Defense*, November 8, 2019, https://insidedefense.com/daily-news/pentagon-issues-draft-cyber-certification-plan-delays-input-controls-advanced-threats.

[26] Rick Weber, "CISA supply-chain task force briefed by DOD on aggressive schedule for contractor certification," *Inside Defense*, October 28, 2019, https://insidedefense.com/daily-news/cisa-supply-chain-task-force-briefed-dod-aggressive-schedule-contractor-certification.

展，未來一個系統可能有成千上萬的設備互相連接，「邊緣防禦」將無法滿足網路與供應鏈的安全需求，因此必須要有新的安全思維。

2019年7月，美國國防部的諮詢機構「國防創新理事會」（Defense Innovation Board）提出一份白皮書，建議美國國防部以「零信任架構」（ZTA）取代「邊緣防禦」，成為物聯網時代的安全思維。簡單地說，ZTA把系統本身當作是不安全的，對進入系統的每位使用者都不信任，因此，每位使用者都只給予「最低限度存取權限」（least-privilege access），也就是只給予每位使用者及其終端裝置要完成其工作所必須的資料及系統服務，其他不相關的資料及系統服務，該位使用者及其終端裝置沒有權限接觸。[27]此概念就如同一棟公寓有多位住戶，一位特定住戶只會拿到公寓大門鑰匙和自己房間的鑰匙，不會拿到其他住戶房間的鑰匙；因此該名住戶進入公寓後只能進入自己的房間，無法進入其他住戶的房間，如此可以保護整棟公寓的安全。[28]

ZTA是以使用者的「角色」做為核心概念，依據每位使用者的不同角色而給予不同權限。[29]ZTA有三個基本步驟：第一、辨識使用者；第二、辨識其所使用的裝置；第三、根據使用者的任務給予權限。ZTA的重點在於，當同一位使用者的角色發生變化，他在系統內的權限也會隨之擴張或限縮，因此，實施ZTA的先決條件是建立身份及權限的管理機制。ZTA的概念在提出之後，已經受到美國國防部的重視，2019年10月12日，美國國防部下轄的國防資訊系統局（Defense Information Systems Agency, DISA）發布徵求建立身份辨識機制的白皮書；[30]前述在11月8日公布的CMMC第0.6版草案中，對第3級廠商的要求即是ZTA的概念。可以預期，ZTA在未來將會在美國的供應鏈安全規範中逐步落實。

伍、終端市場及安全認證

國防產業的銷售市場端通常以國家為單位，因此從製造到銷售，皆涉及國家利益之維護。發展國防產業所投入的公共預算、產出的經濟溢出效益，又與民生經濟和研發資金息息相關，因此形成了私人資本與公共利益之匯流的循環經濟。然而也正是因為國防產業在資訊、資金、人員的流動上，具有公私混合之特性，且商品規格也異於民用標準，因此在整個國防產業經濟循環末端的「交易對象」以及「交易品項」就成了一國國防工業能力能否持續獲得動能的重要關鍵，特別是有關敏感科技轉移的終端使用者控管與安全認證管理。

---

[27] Justin Doubleday, “DOD seeks white papers on identity technologies foundational to ‘zero-trust’ initiative,” *Inside Defense*, October 16, 2019, https://insidedefense.com/daily-news/dod-seeks-white-papers-identity-technologies-foundational-zero-trust-initiative.

[28] Kurt DelBene, Milo Medin, and Richard Murray, The Road to Zero Trust (Security), *Defense Innovation Board*, July 9, 2019, https://media.defense.gov/2019/Jul/09/2002155219/-1/-1/0/DIB_THE_ROAD_TO_ZERO_TRUST_(SECURITY)_07.08.2019.PDF.

[29] Justin Doubleday, “DOD research and engineering lead pushing ‘zero trust’ approach to cyber, 5G developments,” *Inside Defense*, September 23, 2019, https://insidedefense.com/daily-news/dod-research-and-engineering-lead-pushing-zero-trust-approach-cyber-5g-developments.

[30] Justin Doubleday, “DOD seeks white papers on identity technologies foundational to 'zero-trust' initiative,” *Inside Defense*, October 16, 2019, https://insidedefense.com/daily-news/dod-seeks-white-papers-identity-technologies-foundational-zero-trust-initiative.

一、終端市場風險管理

一國政府通常以頒發「出口許可」（export license）作為管控終端市場風險的方式，管制途徑主要分成「軍民兩用產品」以及「軍用產品」兩大類。凡是被列在管制清單上的類別，都需要依照一些判斷標準加以評估，例如技術特徵（technical characteristics）、目的地（destination）、終端使用者（end user）及最終用途（end use）等。

管制清單依循的國際規範來自包括澳洲集團（Australia Group）、《禁止化學武器公約》（*Chemical Weapons Convention*）、核子供應國集團（Nuclear Suppliers Group）、《飛彈技術管制協議》（*Missile Technology Control Regime*）、《瓦聖納協定》（*Wassenaar Arrangement*）等國際出口管制組織。

在獲得「出口許可」前，出口國政府通常還會要求出口商向國家有關單位出示具有公信力的「終端用戶證明書」（End User Certificate, EUC），證明買方有資格承擔隨交易行為而來之義務。「終端用戶證明書」往往是由進口國政府的經貿或國防單位作為第三方擔保核發，用以證明在國際轉讓行為完成後，國籍買家將是貨品的最終使用者，藉此限制貨品流動性、避免重要軍品或高科技零組件落入敵對國家、禁運國家、迫害反人權之政府或恐怖份子之手，有時也出於保護本國智慧財產與商業利益。

一份較詳盡的「終端用戶證明書」內容除了買賣雙方資訊以外，通常還包括：交易目的與用途、交易內容、交易背景、對現行法規之影響、內文名詞定義、相關政策、交易責任、交易程序等。然而，此類機制需仰賴進出口國政府落實管制機制，甚至是國際監督制衡，才能真正管控風險，否則即使終端使用者為一國之政府，有時也難以保證該義務能確實履行。

我國1994年於《貿易法》中納入相關條文，另訂定《戰略性高科技貨品輸出入管理辦法》以及《戰略性高科技貨品種類、特定戰略性高科技貨品種類及管制地區》等管制措施，由經濟部國際貿易局執行「軍民兩用產品」輸出入管理，參照「歐盟管制清單」（*EU Consolidated List*）作為管制名單主要參考，列管10大類產品，包括核能物質與設施、特殊材料與相關設備、材料加工程序、電子、電腦、電信及資訊安全、感應器與雷射、導航與航空電子、海事、航太與推進系統，廠商皆須申請輸出許可才能出口。[31]2016年我國進一步建立經濟部戰略性高科技貨品管理策略推動小組，納入國防部、外交部等共15個部會局處，組成跨部會的機制推動平台。

在美國，「軍民兩用產品」則由美國商務部工業暨安全局（Bureau of Industry and Security, BIS）依照《出口管理規則》（*Export Administration Regulations*, EAR）管制，[32]該規則下的「商品管制清單」（*Commerce Control List*）當中每種品項均

[31] 《高科技貨品管理》，經濟部國際貿易局，2019 年 10 月 25 日，https://www.trade.gov.tw/Pages/Detail.aspx?nodeID=242&pid=662639。

[32] 主要法源為《出口管制法》(*Export Administration Act*, EAA)。

有一組「出口管制分類編碼」（The Export Control Classification Number, ECCN），由5碼代號所組成，分別代表「商品管制清單種類」、「商品種類」、「管制類型」、「瓦聖納協定軍品管制清單」4種內涵，例如「9A610」代表「軍用航空器及相關商品」，而「9D610」則代表「軍用航空軟體」。部分不在「商品管制清單」上的低技術含量之商品項目，則會被列為「EAR99」，也就是除非輸出對象是被列為禁運名單的終端使用者，否則無須出口許可。

表 4-3、美國出口管制分類編碼表

I、商品管制清單種類 Commerce Control List Categories	
0	核子原料、設施、設備（及相關雜項）
1	材料、化學、微生物與有毒物質
2	材料處理
3	電子用品
4	電腦
5	遠端通訊及資訊安全
6	感應器與雷射
7	導航與航空電子技術
8	海事
9	推進系統、太空載具及有關設備
II、商品種類 Product Groups	
A	系統、設備、零組件
B	測試、檢查、製造設備
C	材料
D	軟體
E	技術
III、管制類型 Type of Control	
0	《瓦聖納協定》之國安管制* 核子供應集團之軍民兩用管制及觸發清單（trigger list）
1	飛彈技術管制
2	核不擴散管制
3	生化武器管制
6	美國國家軍品轉移至商品管制清單之管制
9	非國家及單邊管制（反恐、犯罪管制、區域穩定、短期供應、聯合國制裁等）
IV、《瓦聖納協定》軍品管制清單 Wassenaar Arrangement Munitions List (WAML)	

資料來源：蔡榮峰整理自公開資訊。

*說明：該清單包括核子轉移規範，例如實體保護、保護措施、對敏感技術出口的特別管制、核子材料濃縮設施出口特別安排、對可用於核武器的材料進行管制、對二次轉移之管制以及支援，見“Guidelines for nuclear Transfers,” Nuclear Suppliers Group, https://www.nuclearsuppliersgroup.org/en/guidelines。

「軍用產品」則由美國國務院國防貿易管制處（Directorate of Defense Trade Controls, DDTC）依照《武器貿易管制條例》（*International Traffic in Arms Regulations*, ITAR）、《武器出口管制法》（*Arms Export Control Act*, AECA）及《外國援助法》（*Foreign Assistance Act*, FAA）管理。

美國國防部下轄的國防技術安全局（Defense Technology Security Administration, DTSA）專責檢視國安與科技管制技術規範，協助前述的BIS與DDTC判定出口許可之發放；若遇有部門意見相左時，DTSA也會代表美國國防部進行跨部門協商。當相關法規需要修改時，也是由DTSA協調美國國防部有關單位進行評估。[33]值得注意的是，美國國會於2018年8月13日通過之《出口管制改革法》（*Export Control Reform Act of 2018*, ECRA）第1758條，將由BIS後續公布14項新興科技管制細節後進行審查，以防止關鍵技術流失。此一改變可說對台灣乃至世界科技產業鏈影響深遠，未來發展值得觀察。[34]

除了來自境外的採購，一國國防本身的軍需市場的獨占性特質，對其經濟與科技同樣具有重要影響力。因此如何善用政府採購來扶植國防產業，相當受到各國重視。例如我國於2019年5月31日三讀通過的《國防產業發展條例》，其第11-18條特別列出了獎勵捐助補助、資金技術投資或授權、優先採購、提供融資及優惠利率等獎勵方式，以及外購前應先以「技術轉移」、「研發產製」、「後勤支援」評估國內能量。而考慮到軍用科技的特殊性，戰機、戰車、船艦等一等列管軍品的採購，未來也不再受《政府採購法》及其施行細則內「有關規劃、設計服務的廠商不得參與後續投標、作為決標對象或分包廠商或協助投標廠商」等相關規定的限制，以有利我國重要軍備之全壽期規劃。更重要的是，《國防產業發展條例》第19條將技術輸出入的潛在風險納入考量，管制重要零組件與原物料來源非經許可不得來自中國大陸、香港或澳門背景之法人機構。以法規限制來降低供應鏈風險，除了能夠減少製造或技術依賴性，也能夠透過替代效果扶植我國國內的國防產業。

事實上類似的風險管制，也可見於2018年9月美國國防產業評估報告—《評估與強化美國製造與國防產業基礎與供應鏈韌性》（*Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*）。該報告提出超過280項可能影響美軍軍品與零組件供應的漏洞，並一再點出「中國製造」因素對於美國國防產業基礎（defense industrial base）的

[33] DDTC 負責管制 ITAR，BIS 則負責管制 EAR，見"The U.S. Export Control System and the Export Control Reform Initiative," Congressional Research Service, April 5, 2019, p6, https://fas.org/sgp/crs/natsec/R41916.pdf。

[34] (1)生物奈米與合成技術；(2)人工智慧與機器學習技術；(3) 定位、導航和定時技術；(4)微處理器技術；(5)先進計算技術；(6)大數據分析技術；(7)量子資訊和感應傳輸技術；(8)物流技術；(9)積層製造技術；(10)機器人；(11)腦機介面；(12)極音速；(13)先進材料；(14)先進監控技術，見"Review of Controls for Certain Emerging Technologies," *Federal Register*, November 19, 2018, https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies。

侵蝕性影響。[35]美國《聯邦採購條例》（*Federal Acquisition Regulation,* FAR）規定任何國防與能源的採購案，都必須按照「國防等級與配置系統」分級制度進行。[36]而美國政府也能透過修改該法之下的《國防部補充條例》（*Department of Defense FAR Supplement,* DFARS），來防堵其境內國防產業鏈遭受外國勢力滲透。[37]此外，在美國法律中，被定義為美國國防產業廣義來源地的「國家科技和產業基礎」（National Technology and Industrial Base, NTIB）除美國本身以外，還包括後來納入的3個盟國：加拿大（1994納入）、澳洲（2016納入）和英國（2016納入）。NTIB的擴張、新的威脅和技術環境、私部門逐漸在技術創新上超越公部門，這些新的變化預料將對美國未來國防產業的發展計畫和風險管理帶來新的挑戰。[38]

二、軍規產品安全認證

重要軍用設備的設計與製造往往能夠反映一國的戰略意圖，或是反映其先進工業能力，因此由製造商或第三方來驗證產品安全性，多半視機敏性而定；等級越高的重要軍品例如軍用飛行器製造，就越仰賴掌握獨家技術的製造商提供原廠認證。軍規產品適用之環境條件較民用產品嚴苛，因此其安全認證的標準自然也有所不同，因此除了「製成品」之外，「製程標準」的安全認證更是維繫整個產業鏈上下游的關鍵，而這也是公部門或第三方安全認證能夠在整個國防產業發展過程當中扮演的角色。

拿國防產業技術門檻較高的航太領域來說，波音（Boeing）、空中巴士（Air Bus）、奇異（General Electric）、賽考斯基航空（Sikorsky Aircraft）及龐巴迪（Bombardier）等主要航太製造龍頭，都有針對其下游代工廠商所授予的原廠認證，用以認證一架飛機各階段所需要的上百萬件零組件。當然，一些國家的國防

---

[35] "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," U.S. Department of Defense, September 2018, https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF.

[36] "Federal Acquisition Regulation 52.211-14&15," Aquisition.gov, https://www.acquisition.gov/content/part-52-solicitation-provisions-and-contract-clauses#i1063085.

[37] 1984 年生效、1995 年修正的美國《聯邦採購條例》，其內容闡述該條例希望透過政府採購案達到四個主要目標：（1）在適當的性價比、交件期限下，滿足公部門對特定商品與服務的需求；（2）降低部門行政成本；（3）維護美國國內商務環境的公平、開放、完整性；（4）達成政府公共政策目標。然而，依照美國國防部的採購經驗來看，多半時候「維持對中小企業的採購比例」與「最理想的性價比」往往是兩個互不相容的選項，顯示即便是身為國防產業先發國家，美國為了扶植國內產業，也必須仰賴政策的介入。不過，涉及新創企業的創新科技產品採購案時，較不會發生前述情況，見 Moshe Schwartz, "Social and Economic Public Policy Goals and Their Impacts on Defense Acquisition-A 2019 Update," *Defense Acquisition Research Journal*, July 2019, Vol. 26, No.3, pp.208-228, https://www.dau.edu/training/career-development/logistics/blog/New-Issue-of-Defense-Acquisition-Research-Journal.

[38] William Greenwalt, Leveraging the National Technology Industrial Base to Address Great Power Competition: The Imperative to Integrate Industrial Capabilities of Close Allies, *Atlantic Council*, April 2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/04/Leveraging_the_National_Technology_Industrial_Base_to_Address_Great-Power_Competition.pdf.

部也會以作戰需求與後勤狀況來訂定特有的軍用標準以作驗收之用，例如美國、歐盟、澳洲就有自己的適航認證（airworthiness）標準。

用於後勤維修的零組件，有時會碰到消失性商源的情況，因此需要使用非原廠或非原廠授權代工廠之零組件，這也是「製程標準」發揮功能的主要階段，此時由國家機構所頒定的製程標準認證，可用來檢驗備用商源是否達到堪用標準門檻，例如美國聯邦航空總署（Federal Aviation Administration, FAA）所頒發的技術標準規定認證（*Technical Standard Orders*, TSOs），不過這類認證屬於「製造許可」類的認證，能否使用於特定的飛行器，則需要視廠商合約、相關適航認證許可而定。[39]例如在扣件供應，主要是由美國國防後勤局（Defense Logistics Agency, DLA）核發合格供應商認證，其「合格製造商名單」（*Qualified Suppliers List for Manufacturers*, QSLMs）以及「合格經銷商名單」（*Qualified Suppliers List for Distributors*, QSLDs）兩個主要名單上，就標示了屬於第3級的航太扣件，以及屬於第2級的陸海軍用扣件。[40]

此外，與製造業品質管理息息相關的國際組織「國際標準化組織」（International Organization for Standardization, ISO）也扮演了重要角色，例如航太領域就有ISO9001、AS9100、AS9120。而從產業聯盟演進而來的認證體系，認證範圍更廣，例如致力於規格標準化的美國「汽車工程師學會」（Society of Automobile Engineers, SAE）於1990年創立的「國際航太與國防工業承包商認證體系」（National Aerospace and Defense Contractors Accreditation Program，NADCAP）就涉及品管、製程、產品、相關實驗。近年戮力發展航太產業的台灣，也於2019年8月15日，由國家中山科學研究院、經濟部航空產業發展推動小組、台灣經濟研究院邀集11個單位成立「國機國造檢量測聯盟」，希望能夠藉此協助國內廠商降低嵌入國際供應鏈的門檻，並強化我國國防領域之安全。[41]

不僅軍規產品需要安全認證，就科技創新的先進國家來說，只要有關國防的敏感科技，其轉移過程也需要安全查核。例如美國為了維持20世紀以來的技術優勢，特別針對軍民兩用科技的技術移轉設置了「安全閥」，即1993年頒布實行的《國家工業安全計畫》（*National Industrial Security Program*, NISP）。該計畫主要針對有關國安與國防的敏感科技之技術轉移進行保密管理，由美國國防部長負責、另由資訊安全監督辦公室（The Information Security Oversight Office, ISOO）代表美國國家安全會議監管。[42]根據該計畫所制定的美國《國家工業安全計畫守則》（*National Industrial Security Program Operating Manual*, NISPOM），成為美國政

---

[39] "Technical Standard Orders," *Federal Aviation Administration*, October 11, 2018, https://www.faa.gov/aircraft/air_cert/design_approvals/tso/.

[40] "Engineering and Technical Services - Qualified Suppliers List," *Defense Logistics Agency*, https://www.dla.mil/TroopSupport/IndustrialHardware/Engineering-and-Technical-services/Qualified-Suppliers-List/.

[41] 11 個共同成立的單位包括國家中山科學研究院、台灣區航太工業同業公會、台灣機械工業同業公會、台灣區電機電子工業同業公會、台灣經濟研究院、國家實驗研究院、金屬工業研究發展中心、工業技術研究院、台灣電子檢驗中心、資訊工業策進會、車輛研究測試中心。

[42] ISOO 為美國檔案紀錄管理局（National Archives and Records Administration, NARA）下轄單位。

府跨部會有關單位辦理業務之依循。在執行層面，由美國反情報與安全局（Defense Counterintelligence and Security Agency, DCSA）協調與聯邦政府33個單位的行政作業，並負責美國國防產業鏈上下游國防廠商之招標管理、頒發執照與安全查核。[43]

陸、小結

工業全球化使得產業鏈跨國分工常態化，而這個趨勢同樣也影響到國防產業，甚至先進國家的民用技術創新科技，部分發展速度已超越以往領銜發展的國防機構。該如何透過政府機制來管控技術溢散風險，並於軍民領域間轉換創新動能，逐漸成為各國發展國防工業的重要課題。

從本章的說明可以發現，基於近幾年來外資併購、網路竊取事件頻頻發生，造成美國關鍵科技外流嚴重，因此美國在產業安全的各個面向都在進行改革，制訂新的機制與規範。首先對於外來投資作更嚴謹的審查，不以獲得控制權為前提，而是以投資領域為管制目標，避免外國政府或企業藉由併購獲取關鍵技術。其次是依據廠商的技術能力與專業領域將其分類分級管理，並加強公司內控機制，避免機敏資料由內部流出。更重要的是，因為國防產品之需求與一般商業用途有所不同，所以必須建立國家認證標準來保證國防工業產品的品質，並藉此消弭消失性商源可能帶來的負面影響。最後，國家權責機構依專業機制，建立管理出口許可協同機制來管控終端使用者、保障一國之智慧財產權。

現今的安全思維也面臨典範轉移，從「邊緣防禦」轉變為「零信任架構」。美國新的規範例如「無侵入交付」與「網路安全完善模式認證」的具體措施都正在研擬當中，「網路安全完善模式認證」也已經融入了「零信任架構」的安全思維。我國相關單位應密切注意，這些規範必定有我國可以效法之處，也可以提醒國內廠商注意，以助其打入美國國防供應鏈。

（責任校對：吳宗翰、盧屏淵）

[43] "New to DCSA?" Defense Counterintelligence and Security Agency, https://www.dcsa.mil/; National Industrial Security Program Operating Manual (NISOPM 2006), U.S. government, May 18, 2016, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022M.pdf.

本頁空白

第三篇 未來戰場趨勢與台灣國防產業

本頁空白

第五章　創新作戰

舒孝煌、許智翔*

壹、前言

科技日新月益，也帶動作戰概念轉變。一方面軍事科技的擴散，使潛在敵人也能掌握高科技武器如精準飛彈與無人機等，對手可以使用不對稱手段打擊其敵人，傳統作戰概念已無法適應複雜的現代戰爭，需要更新的觀念來應付挑戰。

另一方面，軍事與非軍事的界限也變得模糊，有些國家意識到，可以使用非軍事手段來對付潛在敵人，減少動用軍事行動的成本與風險，運用非軍事手段，在外部環境或敵人境內創造有利己方的各種政治、經濟、社會甚至軍事條件，「不戰而屈人之兵」，達成己方目標。

在創新的作戰概念上，美國雖然走在其他國家的前端，但其競爭對手也在研究其軍事優勢，並發展克制之道，例如不對稱作戰概念、綜合運用非軍事手段的混合戰方法，因此除發展高科技武器外，更要以比對手更快速、更有效率、更綿密的方式運用新科技，在敵人尚難反應時，結合不同領域的各種手段，即將對手擊敗，因此更快速、整合、有效率的運用不同領域的作戰手段，將是未來戰場獲勝的關鍵。

貳、新型態大國衝突環境與未來戰爭趨勢

美國在 2018 年 1 月 19 日提出的《國防戰略報告摘要》（*Summary of the 2018 National Defense Strategy of The United States of America*）中，已明白指出美國視中國與俄羅斯為目前的主要對手。[1]大國衝突過往並不罕見，直到二次大戰為止，人類歷史上有多場強權、大國間的衝突，兩次大戰的總體戰也將戰爭的規模及影響層面拓展到各種可能的層面，而冷戰時期北約及華約兩大陣營的對峙、先進武器的軍備競賽，及對全面核戰的恐懼，也環繞世界數十年。儘管冷戰未曾造就兩大陣營的全面戰爭，然而各種區域衝突如台海衝突、韓戰、越戰、蘇聯的阿富汗戰爭等，卻成為大國博奕、競爭但避免全面軍事衝突的競合場域。同時，冷戰時期的大國競爭也引發軍事思維與技術的不斷成長，不論是核戰略的轉變、美國的兩次抵銷戰略，還是美軍的空陸戰（Air-Land Battle），或是蘇聯由縱深作戰理論進一步延伸出的作戰機動群（operational maneuver group）作戰概念皆是如此，技

* 舒孝煌，先進科技與作戰概念研究所助理研究員，負責本章第參、肆節；許智翔，先進科技與作戰概念研究所博士後研究，負責本章第壹、貳、伍、陸節。

[1] "Summary of the 2018 National Defense Strategy of The United States of America: Sharpening the American Military's Competitive Edge," U.S. Department of Defense, January 19, 2018, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

術上，先進裝備也因為兩大陣營對峙得到長足發展，不論匿蹤技術、神盾戰系甚至俗稱「星戰計畫」的「戰略防禦機先」（Strategic Defense Initiative）皆是如此。

時至今日，前述的冷戰經驗可能將仍然出現在新形態的大國衝突中，然而技術層面的進步，將使得未來大國衝突中，各種混合性的威脅將更勝以往。根據目前中俄的軍事實力及技術發展來看，可預期未來的大國衝突中，美國將可能遭遇遠較以往強大的綜合性威脅，以下即為幾個可能的狀況：

第一種情況，大量先進拒止武器威脅：針對美國龐大的海空優勢，中俄等國皆運用不對稱途徑以拒止美軍優勢海空實力介入，如大量短程彈道飛彈（SRBM）與中程彈道飛彈（MRBM）、長程巡弋飛彈等長距離打擊武器，整合式防空系統（IADS）等，這些武器均針對美國的可能弱點進行打擊。事實上，冷戰時期蘇聯即已擁有大量各式彈道飛彈瞄準北約各國，並運用 Tu-22M 轟炸機（北約代號「逆火」Backfire）搭配長程反艦飛彈以飽和攻擊「抵銷」美軍航艦戰鬥群，可以說形式上類似。然而技術的進步使飛彈的準確度大幅上升，同時極音速武器及超音速反艦飛彈等裝備，較過去更難進行攔截對抗，對航艦戰鬥群與地面部隊、關鍵設施要點而言，技術進步造成的威脅大幅上升。更進一步來說，在矛與盾的競爭中、當技術進步使攻擊能力遠大防禦時，將使傳統大型載台如美軍的超級航艦等的生存能力，在未來大國衝突戰場上受到嚴峻考驗。就中共而言，彈道飛彈與巡弋飛彈可針對美國在太平洋的海外基地在衝突初期即發動打擊，並可扮演拒止美軍進一步增援的角色，大幅彌補其海空軍實力遠不如美國的弱點。IADS 則是針對美國作為主要打擊力量的空中實力，藉由 S-400 等長程防空飛彈（裝備 40N6 超長程防空飛彈時）在內，多種防空系統與預警系統、戰機及預警機等整合出相當範圍之綿密多層次防空網，以對抗美國壓倒性的空中力量。

第二，先進傳統載台：儘管與中俄相比，美國在先進科技，例如戰機的匿蹤科技、引擎等技術上仍佔據優勢。然而，相較於反恐戰爭、甚至後冷戰初期的時代，在大國戰爭中，美國及西方如同過往在冷戰時期一般，無法佔據技術上的絕對優勢。在最尖端的先進技術領域上，俄羅斯與中國皆具備在技術上與美國競爭的能力，包含極音速、無人載具或導能武器等；儘管美國在此類先進技術上仍擁有優勢，然中俄已在相關技術研發上有所突破，甚至已讓部分先進技術如極音速武器進入服役，以強化其突破美國飛彈防禦的能力。此外，即使是傳統武器載台，大國衝突中美國也將面對實力較為接近的對手，例如中俄已推出 Su-57 及殲-20 等自行製造生產的第五代匿蹤戰機及各種先進載具等。同時，俄羅斯在 2015 年推出的 T-14「阿瑪塔」（Armata）戰車單以概念上而言，甚至已經領先了西方現行的 M1A2「艾布蘭」（Abrams）、「豹 2A7」（Leopard 2A7）等高性能戰車。同時，各種突破性的新科技如導能武器、極音速（hypersonic）武器、無人載具等，在大國衝突間皆可能成為雙方都具備的先進裝備。換言之，可以知道在大國衝突中，相較於以往後冷戰時期面對的各項衝突，過往在後冷戰時期美國憑藉的戰具和技術，已不再具備絕對優勢。

第三種狀況是，火力投射能力的大幅強化：這個現象不僅出現於本節所述的

新形態大國威脅，而是廣泛出現在近年多處戰場的趨勢。從前面兩個新型態大國衝突中可能出現的威脅即可注意到，目前的戰場環境中，技術的進步使得火力的投射能力大幅上升，如大量的長程拒止武器將嚴重威脅美國的海外基地以及航空母艦等。類似的狀況並不僅發生在前述的大型、長程武器上，美國雷神（Raytheon）公司目前正研發的「遊隼」（Peregrine）中程空對空飛彈即為一例，此種飛彈的體積與重量大幅縮小（僅約 1.8 公尺長、68 公斤重，遠小於現有 AIM-120「先進中程空對空飛彈」AMRAAM 的 3.7 公尺長、152 公斤重）[2]，這使得戰機能夠搭載遠較過往為多的彈藥進行作戰，從而強化火力投射的能力，較輕較小的飛彈也更容易裝載於其他較小的載台如直升機甚至無人機等。換言之，由於彈藥技術的進步，可預期未來戰場上，火力投射的能力將是核心關鍵。

第四種可能性則是結合多種軍事及非軍事資源的混合戰：從近年來的衝突中可以發現，中俄等大國在傳統軍事實力外，尚能有效運用各種民間及非軍事資源，如武警、海上民兵等，在不同方面發揮滲透及拒止效果。在新型態的大國衝突中，網路資訊等重要科技也在其混合威脅中扮演重要角色，不僅在軍事層面上，也展現在承平時期的各種灰色地帶行動中。

由這些例子可以發現，大國衝突的本質仍然如同過往一般，各層面的軍事力量都將成為競爭焦點，技術與數量上亦各執牛耳。然而，包括資訊及人工智慧（Artificial Intelligence, AI）等各種技術的逐漸成熟，使得新型態的大國威脅讓西方國家需要重新大規模調整、改革其現有部隊，同時新創環境的變化與混合戰/複合威脅因為科技進步造成的巨大威脅等各方面因素，讓美國在內的西方國家現有的兵力、裝備、軍事結構甚至科研各方面的狀態與準備，皆可能遠不足以應付新形態的大國衝突。

就軍事層面而言，各國將必須針對中俄等大國競爭對手的實力進行改革，並思考未來軍力結構的發展方向。由美國陸軍首先推出的「多領域作戰」（Multi-Domain Operation）正是考量大國衝突環境下，對陸軍角色定位及結構未來發展的再思考；另一個例子則是美國「戰略暨預算評估中心」（Center for Strategic and Budgetary Assessments, CSBA）的分析報告，該智庫在不同的報告中，分別探討在大國衝突需求下，美國海軍應需要如何變更其艦隊、尤其航艦戰鬥群的結構。該報告中認為美軍應另外建立一支較小型（約 40,000~60,000 噸級）的航空母艦部隊，[3]同時也針對艦載機戰力提出質疑：美軍航艦在後冷戰時期逐漸改以超級大黃蜂（F/A-18E/F Super Hornet）多用途戰機的航空聯隊（Carrier air wing/CVW）為主，取代過往有各式專職軍機機隊，使得美軍航艦戰鬥群在面對中國的長程

[2] Jon Lake, "Raytheon Unveils Peregrine Air-to-air Missile," *AIN Online*, September 19, 2019, https://www.ainonline.com/aviation-news/defense/2019-09-19/raytheon-unveils-peregrine-air-air-missile.

[3] Bryan Clark, Peter Haynes, Bryan McGrath, Craig Hooper, Jesse Sloman and Timothy A. Walton, "Restoring American Seapower: A New Fleet Architecture for the United States Navy," Center for Strategic and Budgetary Assessments, February 9, 2017, https://csbaonline.org/research/publications/restoring-american-seapower-a-new-fleet-architecture-for-the-united-states-.

拒止武力及各種大國衝突的威脅時，無法具備足夠的生存及打擊能力而急需革新，並量產包括各種艦上 UAV 及下一代的「F/A-XX」打擊戰鬥機等，使航艦部隊能持續於未來戰場維持其價值。[4]

參、多領域化的未來戰場

跨領域作戰的概念並非新鮮事。由於無法直接與美軍抗衡，俄羅斯、北韓、伊朗、中國均發展其自己的不對稱手段，諸如彈道飛彈、超音速巡弋飛彈等等，挑戰美國傳統武器的優勢。新式的超音速巡弋飛彈可打擊至少 300 公里之外的目標，並可由飛機、水面船艦、潛艦或卡車發射，這些武器未來尚可供外銷，加速其擴散。另外，無人機的部署及使用也日益普遍，或是發展高能微波武器、導能武器、電磁脈衝武器等，有報告指出，中國早已能運用低當量核武創造高能量的瞬間電磁脈衝，同時摧毀方圓 400 公里左右的地面及太空裝備。這也說明單一武器同時拒止多重領域的可能性。[5]

美國的對手也充分研究沙漠風暴（Desert Storm）、伊拉克自由（Iraqi Freedom）、持久自由（Enduring Freedom）等作戰，瞭解美國的作戰方式，諸如聯合作戰、技術優勢、全球武力投射、戰略、作戰、戰術機動、有效的聯合火力（effective joint fires）等等。另外，新的技術如人工智慧、極音速、機器學習（machine learning）、奈米技術及機器人等，隨著這些技術逐漸運用在軍事上，有可能再一次徹底改變戰場的作戰型態。[6]

在未來的衝突中，美國對手如中國、俄羅斯等，除透過整合政治、經濟、非傳統及資訊戰手段、實際動武或威脅動用武力等方法，分化美國的盟友與夥伴外，並在對手間創造政治隔離，導致戰略模糊，降低盟友決策及反應速度；運用多重領域手段，包括海上、空中、陸上、太空及網路空間，尋求擊敗對手，他們相信，這樣可以在低於武裝衝突的門檻下達到目標。這將使美國的聯合作戰部隊失去作戰縱深及攻勢能力。

多領域作戰的中心思想是快速且持續整合所有領域的作戰，以嚇阻並挫敗對手，如果嚇阻失敗，聯合部隊將穿透並瓦解敵人的「反介入／區域拒止」（Anti-Access/Area Denial, A2/AD）能力，挫敗敵人的系統、序列及目標，並實現我方的戰略目標。多領域作戰的三項核心思想包括：結合跨戰略距離機動的能力來調整部隊態勢、具備能力及耐力的多領域編隊，足以跨所有領域對敵人造成多重困境、跨時間、空間及能力快速及持續融合所有能力，以超越敵人。

---

[4] Bryan Clark, Adam Lemon, Peter Haynes, Kyle Libby and Gillian Evans, “Regaining the High Ground at Sea: Transforming the U.S. Navy’s Carrier Air Wing for Great Power Competition,” Center for Strategic and Budgetary Assessments, December 14, 2018, https://csbaonline.org/research/publications/regaining-the-high-ground-at-sea-transforming-the-u.s.-navys-carrier-air-wi.

[5] Jeffrey M Reilly, “Multi-Domain Operations,” *Essay of Joint Air & Space Power Conference 2019*, October 8-10, 2019, https://www.japcc.org/multi-domain-operations/.

[6] US Army, “The U.S. Army in Multi-Domain Operations 2028”, *US Army*, December 6, 2018, https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf.

美國陸軍已在進行「多領域戰鬥」（Multi-Domain Battle）的驗證。「多領域」泛指海上、空中、陸上、太空以及網路 5 個領域。這是美國陸軍與空軍合作發展的概念，延續 1980 年代的「空陸戰」（Air-Land Battle）構想，目的在結合空軍及陸軍的高科技武器抵銷前蘇聯陸軍在歐洲的數量優勢。2018 年時陸軍將「多領域戰鬥」擴充為「多領域作戰」，將概念涵蓋至非戰鬥的行動領域。[7]

美國陸軍正推動多領域作戰的實驗，2017 年時美軍就已在設計及測試多領域任務部隊（Multi-Domain Task Force, MDTF），使前進部署部隊能執行長程聯合精準打擊、飛彈防禦、電子戰、太空、網路等作戰。多領域任務部隊需能提供各軍種及盟國所有領域的能力，以擊敗敵人的反介入／區域拒止戰略。目前美國陸軍太平洋部隊已在 2019 年 1 月建立第一支實驗型「情報、資訊、網路、電子戰及太空」特遣隊（Intelligence, Information, Cyber, Electronic Warfare and Space, I2CEWS），執行多年期聯合及協同實驗計畫，以形塑未來的多領域任務部隊設計，這項實驗結合第 17 野戰砲兵旅、一個指揮單元、一個聯合情報、網路、電子戰及太空單元、以及其他任務單位，以提供實際的部隊資產及作戰能力，並蒐集作戰部隊的回饋，供未來計畫及概念發展之用。

另外，空軍也正在發展多領域指揮管制（Multi-Domain Command and Control, MDC2）概念，成為未來多領域作戰的神經系統。美國空軍正大舉投資在 5G 領域，期能成為數位空軍（Digital Air Force），因為網路不僅重要，更重要的是速度、頻寬及網路延遲時間的縮短。MDC2 目的在使所有軍種、聯盟、夥伴的感測系統在任何情況下，針對任何目標，提供資料給所有使用者。

多領域戰爭可以被視為是一種戰爭的持久特徵，例如「摩擦」或「戰爭迷霧」，這些挑戰使未來的衝突更加複雜。[8]多領域作戰與聯合作戰（Joint Operations）類似，但概念上不同，例如陸戰隊與陸軍地面部隊的協同地面攻勢是聯合作戰，但不是多領域作戰，相反的，水面艦與反潛機的反潛作戰則可視為多領域作戰，但不是聯合作戰。多領域作戰並不新奇，陸上防空作戰屬多領域的一部分，海軍航空也是。新奇的是，過去作戰領域只限於陸地、海上及空中，現在太空及網路空間也屬於作戰領域的一部分。若不建立新軍種在其所能提供的技術領域內作戰，那太空及網路空間就要由陸軍、海軍、空軍或陸戰隊負責。

目前多領域作戰尚未發展成為準則或理論。目前美國陸軍對多領域作戰概念發展最為積極，企圖在衝突或競爭中從多重領域擊敗對手；空軍多領域指揮管制概念中的指揮及管制（Command & Control, C2），將之定義為跨所有領域的指揮及管制，可以保護、允許及增強所有作戰任務的進行，在選擇的時間、地點及進行方法上獲致理想效果。海軍的分散式海上作戰（Distributed Maritime Operations）概念，以及陸戰隊基於分散式殺傷發展的概念，則是透過分散式網路，連結水面艦、潛艦、飛機及衛星，將其感測器、指揮系統及射手連成一氣。

---

[7] US Army, “The U.S. Army in Multi-Domain Operations 2028”, *US Army*, December 6, 2018, https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf.

[8] Will Spears, “A Sailor’s take on Multi-Domain Operations,” *War on the Rocks*, May 21, 2019, https://warontherocks.com/2019/05/a-sailors-take-on-multi-domain-operations/.

由於大國競爭再起，美國各軍種都同意，必須在陸地、海洋、空中、太空及網路等所有領域進行作戰，透過跨越所有領域進行快速及協調的攻擊，以穿透及瓦解敵人反介入及區域拒止戰略的分層結構及網路。[9]然而，雖然各軍種都在朝向各領域，以更分散、更流暢方式同時作戰，但以真正的聯合方式進行多領域作戰的障礙仍然存在，而毫無障礙地運用基於各軍種的作戰能力，仍十分重要。美軍需要一個新的多領域準則，能驅動各軍種以協調一致的方式進行多領域作戰，並確保在指揮、管制、網路及決策等方面進行適當的投資，美國陸軍高階將領承認，雖然持續朝向聯合所有部隊方向發展，但程度仍然不夠。[10]

美國已將多領域作戰視為是未來安全及作戰成功的關鍵，最近數年多領域空間的投資及興趣都會增長。由於作戰雙方都具相同情監偵能力，因此獲勝的一方將是可以讓對方無法跟上的快節奏進行指揮並掌握主動權的一方。未來所有作戰單元都要能從各領域對情勢的改變採取行動及反應。在各領域的節奏，包括採購、性能提升、創新及改變，以及資訊分享都要加快，這是多領域部隊成功的關鍵。

從軍事廠商的觀點來看，多領域作戰也將會影響未來軍事裝備的發展，其需求也會成長，多領域作戰要求在同一平台上偵測、分享及行動，創造分散式指揮及管制的環境。未來戰場的關鍵是由系統至系統間的無縫整合及相容操作性，因為未來已無法在與實力接近的對手的競爭中佔有優勢，因此在各領域的速度是關鍵。真正的多領域作戰，需要能夠在同一平台上結合感測器、共享、行動的技術，從而創造一個分散式的指揮及管制環境，這對所有平台及部隊都是一項巨大的挑戰。[11]

肆、混合戰與非軍事衝突

有些威權或非民主國家，或是政治團體，日益增加對非軍事手段運用以達成其目標，這些常被稱為「灰色地帶」或「灰區」行動（gray zone），其涵蓋面甚廣，包括選舉干預、經濟強制、非傳統力量的模糊運用，這些行動在戰爭水準之下，對美國或其他國家的利益造成挑戰。中國可能使用的手段包括資訊戰（Information Warfare）、經濟強制（Economic Coercion）、運用模棱兩可的武裝力量

[9] Dan Goure, “A New Joint Doctrine for an Era of Multi-Domain Operations,” *Real Clear Defense*, May 24, 2019, https://www.realcleardefense.com/articles/2019/05/24/a_new_joint_doctrine_for_an_era_of_multi-domain_operations_114450.html.

[10] Dan Goure, “A New Joint Doctrine for an Era of Multi-Domain Operations,” *Real Clear Defense*, May 24, 2019, https://www.realcleardefense.com/articles/2019/05/24/a_new_joint_doctrine_for_an_era_of_multi-domain_operations_114450.html.

[11] “A Look Inside Multi-Domain Warfare with Lockheed Martin,” *Global Defence Technology*, October 2018, https://defence.nridigital.com/global_defence_technology_oct18/issue_92.

（ambiguous forces），包括未經指明的軍事力量、島嶼建設、運用代理人等，[12]另外，「影響力作戰」（Influence Operations）也是灰區衝突的一部分。

美國國防部或智庫近期公布的報告，都在關注中國的影響力作戰。美國國防部 2019 年 1 月公布的《評估中國軍力對美國的影響》（*Assessment on U.S. Defense Implications of China's Expanding Global Access*）指出中國過去 10 年來大量投資在駐外及外文媒體上，例如新華社在 2009 至 2011 年間就設了 40 個海外通訊社，至 2020 年預計要達到 200 個。而中國也透過其他手段以圖影響全球公眾意見。[13]

2019 年 6 月公布的《印度太平洋戰略報告：準備、夥伴關係及促進一個區域網絡》（*Indo-Pacific Strategy Report: Preparedness, Partnerships, and Promoting a Networked Region*）則進一步提到中國企圖利用軍事現代化、影響力作戰、經濟掠奪等方式，對他國實施強制行動。中國運用影響力作戰、經濟誘因及懲罰手段，以及暗示軍事威脅，說服其他國家遵守其設定的議程。雖然貿易可讓雙方受惠，但中國利用間諜活動和盜竊來獲取經濟利益，並將獲得的技術轉移至軍事領域，因此仍是其貿易夥伴所需面對的重大經濟及國家安全風險。[14]

「美中經濟安全審查委員會」（U.S. China Economic and Security Review of Commission）2019 年 11 月 15 日公布的《2019 年度報告》（*2019 Report to Congress of the U.S. China Economic and Security Review of Commission*）也指出，中國及俄羅斯的行動雖然有差異，但都分別或合作對抗美國，侵蝕美國在世界的領導地位及其價值觀。中國及俄羅斯使用影響力作戰、網路戰、假訊息等手段，破壞美國及民主世界的穩定，此外，兩國協調一致的軍事活動，也造成新安全挑戰。[15]

中國在海外的影響力行動頗受關注。中國的影響力作戰與俄羅斯不同，俄羅斯傾向直接、有目的的行動，例如干預美國總統大選。相反的，中國偏好長期作戰，他們的行動具有高度針對性、分散，可影響在制定對中政策有重要地位的人士，這與合法的遊說不同，影響力作戰旨在透過強大的商人及公司網路，並透過非正規手段，例如賄賂、資訊扭曲、脅迫等手段，以形塑認知及激勵結構。[16]

影響力作戰是美國對中國一系列行動賦予的名詞，美國國防部 2019 年公布

---

[12] "Competing in the Gray Zone: Countering Competition in the Space between War and Peace," Center for Strategic and International Studies, 2019, https://www.csis.org/features/competing-gray-zone.

[13] US DoD, "Assessment on U.S. Defense Implications of China's Expanding Global Access," U.S. Department of Defense, December, 2018, https://media.defense.gov/2019/Jan/14/2002079292/-1/-1/1/EXPANDING-GLOBAL-ACCESS-REPORT-FINAL.PDF.

[14] "Indo-Pacific Strategy Report: Preparedness, Partnerships, and Promoting a Networked Region," U.S. Department of Defense, June 1, 2019, https://media.defense.gov/2019/Jul/01/2002152311/-1/-1/1/DEPARTMENT-OF-DEFENSE-INDO-PACIFIC-STRATEGY-REPORT-2019.PDF.

[15] "2019 Report to Congress of the U.S. China Economic and Security Review of Commission," U.S. China Economic and Security Review of Commission, November, 2019, https://www.uscc.gov/sites/default/files/2019-11/2019%20Annual%20Report%20to%20Congress.pdf.

[16] Abigail Grace, "China's Influence Operations Are Pinpointing America's Weaknesses," *Foreign Policy*, October 4, 2018, https://foreignpolicy.com/2018/10/04/chinas-influence-operations-are-pinpointing-americas-weaknesses/.

的《中國軍事及安全發展》（*Military and Security Developments Involving the People's Republic of China 2019*）報告中以專題（Special Topic）討論影響力作戰，顯示美國對影響力作戰關切，以及國防部如何思考此一問題。該專題提到，中國至少自 2003 年以來，便使用「三戰」（Three Warfare）的字眼，包括心理戰、輿論戰及法律戰。

在習近平領導下的中國，這種形塑大眾影響力的行動，中國稱其為「統一戰線」（United Front，簡稱統戰），其重要性大幅上升，已成為中國重要政治工具之一。統戰工作部甚至在 2017 年設立 4 個新的局，專事對海外工作。[17]統戰目的在藉秘密、強制的活動，促使外國政府採取有利中國的政策立場，這通常是透過中國僑民、外國境內的附隨組織所進行。

混合戰（hybrid warfare）也是以不對稱，及不公開進行敵對行動的情況下，破壞及削弱對手的行動，這些行動可能游走在戰爭及和平的邊緣。其手段也包括使用假訊息、經濟操、使用代理、叛亂行動、外交壓力，甚至包括軍事行動。影響力作戰、混合戰，或是資訊戰等，都屬於灰區衝突。新的國際局勢使其受到重視，首先是大國競爭重新出現，美國重新關注其地緣政治對手對外國的影響，第二是民族主義再次崛起，賦予其新的動力，威權國家藉民主政治的一系列挫折，鞏固其專制統治及形象；第三是數位革命改變人們通訊方式，也扭曲人們取得訊息的途徑，使得錯誤訊息氾濫到公共領域變得更為容易。[18]

在灰色地帶行動中，行動工具包括：軍事、準軍事或其他國家控制的部隊；代理人；資訊戰，俄羅斯和中共經常使用資訊戰技術，透過社交媒體和其他管道對目標國傳播懷疑、異議和虛假信息，並透過宣傳強化自己論述；直接收買政客，證據顯示中國和俄羅斯正努力直接影響某些國家候選人或政治人物；經濟工具，用以實現政治或其他目的的經濟手段，包括俄羅斯在關鍵時刻有針對性地向附近國家提供能源供應，以及中共對第三世界國家對基礎設施提供投資；塑造公民社會，如中共利用孔子學院和對大學投資以限制反華情緒。[19]

灰色地帶行動不一定會造成戰爭，但也有可能是衝突前的準備行動。中國可能在平時即大量運用灰色地帶行動，例如新聞傳播等，塑造有利中國的政治、經濟情勢，增加目標國政治壓力，塑造有利中國、不利目標國的政治、軍事及經濟情勢。

灰色地帶行動可能獨立發生，也可能是大型軍事行動前的序曲，例如以大量小型準軍事行動做為先期準備，有時是無預警的偶發行動，有時則可能是蓄意引

---

[17] Alex Joske, "Reorganizing the United Front Work Department: New Structures for a New Era of Diaspora and Religious Affairs Work," Jamestown Foundation, May 9, 2019, https://jamestown.org/program/reorganizing-the-united-front-work-department-new-structures-for-a-new-era-of-diaspora-and-religious-affairs-work/.

[18] Carolyn Kenney, Max Bergmann, and James Lamond, "Understanding and Combating Russian and Chinese Influence Operations," Center for American Progress, February 28, 2019, https://www.americanprogress.org/issues/security/reports/2019/02/28/466669/understanding-combating-russian-chinese-influence-operations/.

[19] "What Works: Countering Gray Zone Coercion," Center for Strategic and International Studies, July 16, 2018, https://www.csis.org/analysis/what-works-countering-gray-zone-coercion.

起，目的在挑起事端，因此必需謹慎識別。中國可能以大規模的網路戰、資訊戰與電磁戰，也可能以實體式的恐怖攻擊，如以無人機騷擾機場、潛伏特種部隊破壞電線電纜輸油管等、例如使關鍵基礎設施失能、攻擊政治經濟及社會網路，使目標國陷入緊張狀態，拖延其作戰準備行動、致盲指管通情系統，在戰爭發起前便中和對手反擊行動。

小型衝突也可能是其他事態誘發，如目標國內部政治情勢或社會動盪，對其執政當局造成壓力；國際社會對其對手國的支持行動，例如出售敏感性武器等；或是周邊海域的小型意外誘發衝突；或是某國無預警扣押目標國人員等。

非軍事的小型衝突可能需待後續政治協商或談判以化解爭議，可能不致擴大為武裝衝突，主要焦點在於雙方政治對話或解決爭議，若雙方冷靜、克制，並保持聯繫管道暢通，衝突得以緩解或不會擴大，反之則可能拖延，不利後續的情勢緩和及關係發展，甚且使衝突進一步擴大。

伍、創新思維與不對稱作戰

不對稱作戰（asymmetric warfare）目前在台灣成為國防安全領域上極受重視之概念。從本質上來說，人類史上的戰爭多半帶有相當程度的不對稱成分在內，顯現在包含時間、空間、力量、戰術戰法等不同面向上，而不對稱作戰簡單的說，即為運用此類手段，藉由避實擊虛的手段與方式、達成嚇阻甚至取得衝突中一定優勢的方式。從這個定義出發，可以發現不對稱作戰實際上是一極為廣泛及靈活的概念，並非僅局限於特定項目或方式，也不見得只有實力較弱或較強的一方可以運用不對稱手段打擊對手。而創新思維，則是發展不對稱作戰的核心。由於不對稱概念的廣泛性，本節從台灣與美國兩個案例探討可能的不對稱與創新概念方向。

由於中國在軍事面上，對台灣已形成全面優勢，在兵力的極端不對稱下，包含美國在內，多數的智庫與學者針對台灣面臨的嚴峻軍事威脅，皆視不對稱作戰為台灣未來必須採取的防衛手段，如 2008 年美國海軍戰院（Naval War College）教授莫瑞（William Murray）的「豪豬戰略」（porcupine strategy）即建議台灣採取大量飛彈、武裝直升機及地面部隊等作為防禦手段；[20]美國「戰略暨預算評估中心」2014 年的報告也認為，台灣應以大量小型潛艇、反艦飛彈、機動防空飛彈、機動火砲、多管火箭、地雷等裝備進行不對稱防衛作戰；[21]蘭德公司（Rand Corporation）甚至在一份分析報告中，認為台灣應當僅維持僅 50 架的小規模戰機機隊，並部署大量防空飛彈系統，以確保台灣部隊能在必要時維持局部空優。

[20] William S. Murray, “Revisiting Taiwan ’s Defense Strategy,” *Naval War College Review*, vol.61, Nr.3, 2008, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1814&context=nwc-review.

[21] Jim Thomas, Iskander Rehman, John Stillion, “Hard ROC 2.0: Taiwan and Deterrence Through Protraction,” Center for Strategic and Budgetary Assessments, December 21, 2014, https://csbaonline.org/research/publications/hard-roc-2-0-taiwan-and-deterrence-through-protraction.

[22]另外，喬治梅森大學（George Mason University）的「安全政策研究中心」（Center for Security Policy Studies）也提出台灣應暫緩潛艦、大型艦艇及 F-35 戰機的採購計畫，以強化不對稱防禦系統如無人機、微型潛艦、自動化武器、飛彈，並讓地面部隊搭配小型輪型車輛為主，轉型為能以獨立、小型分散單位行動的部隊等。[23]

綜觀類似的研究分析，多半認為台灣需發展類似莫瑞所建議的「小型、致命、大量、機動」（small, lethal, many, mobile）裝備，[24]以抵銷解放軍的龐大軍力優勢，其分析的重點均在於中國對台灣的全面性軍事威脅及其優勢，使台灣全島在衝突時期即可能因為中國的網路、電子作戰，彈道飛彈及火箭攻擊而使大量的主戰裝備失去效用，同時數量的絕對優勢也使得台灣的高性能裝備將可能無法長期持續支撐作戰即消耗殆盡。因此，需從不對稱的角度出發，藉由目前已發展成熟的大量精準彈藥大量殺傷敵方的人員及擊毀高價載台。同時關於不對稱作戰的分析，也都針對台灣威脅最大的想定，即中國入侵台灣本島進行探討。

面對此種嚴峻形式，不對稱作戰雖是較弱小的國家所能藉「以小搏大」對抗強大對手的方式，然而此種作戰方式仍有其限制與要求，不僅前述提到的各種裝備發展方向外，更需要強調創新思維的重要性。前述包含反艦飛彈、防空飛彈、海上輕快兵力、微型潛艦及水雷、地雷等不對稱作戰裝備儘管預期可在兩岸發生衝突時，較有效的阻止入侵，然而在其餘的可能衝突形式如封鎖，及非戰時的「灰色地帶」行動中較難發揮效果。此外，環境也嚴重影響不對稱作戰的可能形式，如各地地形、海象等，換言之，在各項研究與分析中提及的不對稱作戰裝備如飛彈、水雷等，相較於傳統大型載台而言，可能相對上較不適於在其他情境或威脅下運用，如中國軍機於承平時期繞台甚至越過海峽中線時，台灣可派遣戰機緊急升空監控、驅離，防空飛彈在此時便無法發揮類似作用。然而，由於渡海奪取台灣本島或其他離島確實是兩岸的各種可能衝突狀況中，最直接、也最大的威脅，因此為此全力發展相對應的不對稱武力確有其急迫需要，而如何在有限的國防資源下，對前述在平戰時的不同需求做出合宜分配，可說是發展不對稱作戰一方將可能面臨的困難抉擇。

類似的不對稱思維近年也開始反應在美國的戰略上，由於其國家利益廣布在全球各地，冷戰結束後美國在 1993 年的「通盤檢討」（*Bottom-up Review*）中訂定了「兩場大型區域衝突」（two major regional conflicts, two-MRCs）標準，並在後續的多次《四年期國防總檢討》（*Quadrennial Defense Review*, *QDR*）等各項文

---

[22] Lostumbo, Michael J., David R. Frelinger, James Williams, and Barry Wilson, "Air Defense Options for Taiwan: An Assessment of Relative Costs and Operational Benefits," RAND Corporation, 2016, https://www.rand.org/pubs/research_reports/RR1051.html.

[23] Michael A. Hunzeker, Alexander Lanoszka, Brian Davis, Matthew Fay, Erik Goepner, Joseph Petrucelli and Erica Seng-White, "A QUESTION OF TIME: Enhancing Taiwan's Conventional Deterrence Posture," Center for Security Policy Studies at George Mason University, November 2018, http://csps.gmu.edu/a-question-of-time/.

24 William S. Murray, "Asymmetric options for Taiwan," in Ming-chin Monique Chu and Scott L. Kastner eds., *Globalization and Security Relations Across the Taiwan Strait: In the Shadow of China* (London and New York: Routledge, 2015), p.72.

件中持續討論美軍應有的能力，然而美軍目前實力仍無法滿足 two-MRCs 的需求，[25]特別是目前戰略已轉移到大國衝突的情況下，透過新思維以在大國競爭中取得優勢的必要性更加明顯。因此，美國近年在強化軍力以對抗中俄等強勁對手的需求下，推出「第三次抵銷戰略」（The Third Offset Strategy）。

「創新」正是美國當前抵銷戰略的核心要素。在中俄等強大對手的軍事實力外，「第三次抵銷戰略」的推出更源自於創新環境的日益全球化與商業特性，以及商用技術逐漸廣泛的各種軍事任務應用；美國的對手們已能透過這些技術創造自己的創新作戰概念，並用於挑戰美國及其盟友。為此，美國在技術面上制定了幾個關鍵的創新領域：自主學習系統，人機協同決策，輔助的人員操作（assisted human operations），先進有人—無人系統操作，網路化的自主武器以及高速彈體（high-speed projectiles）等。[26]

針對「創新」這個關鍵要素，美軍採取多項措施使各種新創的研究發展能順利進行，如美國陸軍為其現代化設立了八個跨功能小組（cross-functional team, CFT）以整合採購、需求確認、科學科技、測試評估、資源、合約、成本分析、軍事行動等各方專業，同時也強化跨 CFT 間的橫向整合，以確保其多領域作戰概念與裝備的研發。[27]此外，為了強化技術研發的效率及創新，美軍也在採購流程上採取諸如「其他交易」（Other Transactions, OT）等方式，藉由類似私人商業契約的形式，迴避傳統政府採購的冗長程序，強化與私部門的合作及新創；[28]在適當的運用下，OT 即可透過對特定項目與參與者需求量身訂做的團隊安排，使政府能取得傳統與非傳統國防承包商的最新技術。[29]

然而美國並不僅專注於發展全新的技術，在此次的「抵銷戰略」中，美國藉由與盟國在特定技術項目的合作，並善用盟國的技術強項加強此戰略，美國並偏好在技術上運用現有系統為基礎，形成其所要求的創新作戰概念與戰術戰法核心，同時也強調發展智慧水雷等低成本戰具抵銷中國海軍快速增加的實力。如此美國可在較短的時間內，形成其所要求的創新戰力以抵銷中俄實力；[30]前述借重盟國的成熟技術上以協助美軍快速取得急需戰力，並協助進一步發展所需之裝備的

[25] "An Assessment of U.S. Military Power: Army, Navy, Marine Corps, Nuclear Weapons, Missile Defense," The Heritage Foundation, October 30, 2019, https://www.heritage.org/military-strength/an-assessment-of-us-military-power.

[26] Kathleen H. Hicks, Andrew Philip Hunter and Gabriel Coll, "Assessing the Third Offset Strategy," Center for Strategic and International Studies, March 16, 2017, https://www.csis.org/analysis/assessing-third-offset-strategy.

[27] Maj. Gen. Rodney D.Fogg, "From the Big Five to Cross Functional Teams: Integrating Sustainment into Modernization," *U.S. Army*, September 30, 2019, https://www.army.mil/article/227832/from_the_big_five_to_cross_functional_teams_integrating_sustainment_into_modernization.

[28] 蔡宜臻，〈Other Transaction(OT)於新創政府採購之應用〉，資策會科技法律研究所，2018 年 3 月，https://stli.iii.org.tw/article-detail.aspx?no=64&tp=1&i=176&d=7988&lv2=176。

[29] Office of the Under Secretary of Defense for Acquisition and Sustainment, "Other Transactions Guide," Defense Acquisition University, November 2018, https://www.dau.edu/guidebooks/Shared%20Documents/Other%20Transactions%20(OT)%20Guide.pdf.

[30] Wei-Chieh Huang, 〈真正的超限戰：淺論美國對中國「第三次抵銷戰略」〉，《The News Lens 關鍵評論》，2019 年 7 月 29 日，https://www.thenewslens.com/article/122699。

方式，經常可見於美軍近年的發展中，其中一個例子即是美國陸軍為其「間接砲火防護能力」（Indirect Fire Protection Capability, IFPC）計畫，採購兩套以色列製的「鐵穹」（Iron Dome）防空系統。美軍採購「鐵穹」的目的主要是用以緊急填補作戰能力上的缺口，並且進一步協助發展美軍的 IFPC 系統。[31]儘管美軍認為「鐵穹」系統無法滿足美軍的 IFPC 需求，然而美國的《2019 國防授權法案》（*2019 National Defense Authorization Act, 2019 NDAA*）中同時要求，如美軍在 2023 年以前無法開始運作自行研發的 IFPC 裝備，則需續購「鐵穹」防空系統。[32]

同時，對手運用的不對稱作戰方式，也可能是可以仿效、學習的對象，例如美軍開始加強發展短程戰術飛彈，即為一例證。中國長期將火箭軍作為其對美不對稱作戰的核心武力，火箭軍的大量彈道飛彈與陸射巡弋飛彈在其軍事戰略上，可說同時負責在美國由空軍負責的長程精準打擊，以及對抗美國海軍航艦戰鬥群等任務。美國陸軍目前的六大現代化重點項目（six modernization priorities）之首的「長程精確火力」（Long-Range Precision Fires, LRPF）中，即將彈道飛彈火力作為美軍未來發展的優先項目。

就彈道飛彈而言，儘管美軍擁有大量洲際彈道飛彈如陸基的義勇兵三型（Minuteman III）、潛射的三叉戟二型（Trident II）等，建立了無與倫比的核子保護傘，然而在戰術火力上，美國陸軍目前僅有以 MLRS 及 HIMARS 多管火箭發射之「陸軍戰術飛彈」（Army Tactical Missile System, ATACMS）。LRPF 計畫中的核心項目為「精準打擊飛彈」（Precision Strike Missile, PrSM），原本 PrSM 預期射程因為《中程飛彈條約》（*Intermediate-Range Nuclear Forces Treaty*, INF）限制 500 公里以內，但與原先 ATACMS 約 300 公里的射程，仍大幅增加不少，而在美國 2019 年 8 月 2 日退出 INF 後，預期將可增加射程到至少 700-750 公里，[33]除此之外，美軍更進一步著眼於設成達 1,000 哩（約 1,600 公里）的極音速戰術飛彈，及戰略長程火砲以對抗中俄，[34]並預計在 2019 年底時試射射程約 3,000-4,000 公里的彈道飛彈。[35]透過這樣的方式，美國陸軍不僅可以在大國衝突環境下強化自己的接戰能力，而不需完全依賴海空軍支援之外，更可以透過在西太平洋島鏈部署大量短程彈道飛彈，用同類似中國火箭軍所扮演的 A2/AD 角色，對中國造成防禦上的壓力。

---

[31] Jen Judson, "It's official: US Army inks Iron Dome deal," *Defense News*, August 12, 2019, https://www.defensenews.com/digital-show-dailies/smd/2019/08/12/its-official-us-army-inks-iron-dome-deal/.

[32] Paul Mcleary, "US Army Signals Israel's Iron Dome Isn't the Answer," *Breaking Defense*, October 15, 2019, https://breakingdefense.com/2019/10/us-army-signals-israels-iron-dome-isnt-the-answer/.

[33] Jen Judson, "How far will the Army's precision strike missile fly?" *Defense News*, October 14, 2019, https://www.defensenews.com/digital-show-dailies/ausa/2019/10/14/how-far-will-the-armys-precision-strike-missile-fly/.

[34] Sydney J. Freedberg Jr., "Army Seeks 1,000-Mile Missiles Vs. Russia, China," *Breaking Defense*, September 10, 2018, https://breakingdefense.com/2018/09/army-seeks-1000-mile-missiles-vs-russia-china/.

[35] Aaron Mehta, "Is the US about to test a new ballistic missile?" *Defense News*, November 13, 2019, https://www.defensenews.com/space/2019/11/13/is-the-us-about-to-test-a-new-ballistic-missile/.

圖 5-1、美國陸軍的長程火力

資料來源：舒孝煌攝影。

說明：洛克希德馬丁發展的陸軍長程火力展示模型，由上而下分別是 MLRS 火箭、PrSM 飛彈、ATACMS，右後方為 HIMARS 縮尺模型。

藉由這些例子，可以注意到創新思維與不對稱作戰的思考上，不僅需要透過適合本身環境，以及安全需求發展特定武器裝備外，由現有較成熟技術進一步延伸以加速發展新式裝備、戰術戰法、作戰概念，甚至參考對手的作戰概念並以此發展自己的不對稱戰法等，皆是在靈活概念下所能嘗試思考並發展的概念。同前所述，「創新」將是未來技術發展以及不對稱作戰概念的核心，因此不論在概念上、還是技術層面上建立良好的創新環境、靈活思維激盪，以及進一步的橫向整合，將是未來能在競爭領域取得優勢的關鍵要素。

陸、小結

隨著大國衝突的需求重新浮現，創新作戰以及不對稱作戰概念，已經逐漸成為各國重視的發展方向。然而不論是創新思維的催生還是裝備研發，皆需要合宜組織結構等多方面的改革與轉型，方能創造支持創新的土壤，美國目前採取的諸多措施正是一例。若單從台灣的角度分析，在技術與裝備難以全面追趕中國優勢、而兵力數量又處於絕對劣勢的情況下，在未來的大國衝突戰場上，不對稱代表的更是自我防衛的關鍵。如同前面所分析，飛彈或水雷一類的不對稱裝備確實是防衛作戰的核心概念，然不對稱作戰與創新思維應不僅於此，更包含戰術戰法及組織結構在內、全面的大幅度創新，考量台海兩岸軍力的長期失衡，以及近年中國軍力強化的速度，台灣進行先進裝備投資及組織結構等變革、藉此謀求強化未來的嚇阻能力以面對威脅，是當下十分急迫的需求。

此外，考量未來戰場特性，美軍的先進作戰概念如「分散式殺傷」及「多領域作戰」雖然由於技術與資源的差距，難以直接在台灣複製，然而由於現代火力

投射能力的大幅上升、及資通技術的長足進步，美軍作戰概念的部分原則卻仍有值得參考並發揮之處，尤其如同分散式殺傷般嘗試、藉由高機動載台的靈活運用將火力發揚到最大，將是國軍可以嘗試發展之方向。不過在此前提下，合適的載台及彈藥即是接下來重要的裝備研發或籌獲的方向，而與之搭配的良好通訊、資傳鏈路等各種通資整合、電磁防護、資訊安全方面的能力與裝備，以及電磁環境的掌握與維持，則將可能是遂行此種作戰方式的核心關鍵。

（責任校對：杜貞儀、王綉雯、陳俊良）

第六章 科技趨勢

舒孝煌、許智翔*

壹、前言

由於大國競爭時代來臨，軍事科技發展速度有加快趨勢。近年較受人矚目的發展，包括導能武器如雷射、電磁武器或微波武器等，已逐步邁向實用化，準備開始在艦艇或陸地上進行部署；更遠程、更精準的火力，如長程火砲、極音速武器等，不但遠距的敵人將無所遁形，傳統的防禦手段也將失去效力。

無人載具技術也持續進一步發展，運用範圍更為廣泛，除了大型的無人機與無人艦艇，可執行多元化的作戰任務外，人工智慧運用在無人系統上，也大幅提升無人系統的運用範圍，包括減輕操作者的負擔，使其真正變成「無人化」，並真正成為戰場士兵的隊友，協助執行搬運輜重工作，減輕作戰人員的負荷，或擔任危險的前線偵察等任務，減少士兵曝露在砲火下的危險。

軍事科技發展速度加快的部分原因，是因為武器研發人員及裝備運用者都意識到，不應追求過度高度科幻的先進科技、導致成本過高，期程太長，而且至研發完成的期程太長，而是減少過度的野心，專注於解決當前最急迫問題，先運用現成可行的科技，再逐漸提升其作戰能力。由於大國競爭再起，各國競相發展新軍事科技與新武器，挑戰對手的軍事優勢，使軍備競賽再起，而新軍事科技及備取得管道更為多元化，取得更容易，如無人機及極音速武器等，將促使軍事科技及先進武器更加擴散，對國際秩序及區域安全帶來極大挑戰。

貳、雷射與導能武器

導能武器（direct energy weapon，DEW），意指直接將能量轉換為攻擊敵人的武器，其中包括致命與非致命武器，種類包括雷射、微波武器、電磁武器等，運用領域包括反人員武器、飛彈防禦系統、近迫武器等。過去導能武器被認為是科幻電影的情節，但隨著技術成熟，以及作戰上的迫切需要，使得此一類型武器已逐步邁向實用化，不再僅存在於科幻電影或小說中。

一、美國的雷射武器發展

美國軍方認為，反制火箭、火砲、迫砲與飛彈威脅（counter rocket, artillery, mortar and missile, C-RAMM）是保護前線部隊及基地部署的急迫任務。目前雷射武器發展重點置於可立即投入使用的技術上，逐步提升雷射武器能量。另外，也

* 舒孝煌，先進科技與作戰概念研究所助理研究員，負責本章第壹節、第貳、參節前半與第肆、陸節；許智翔，先進科技與作戰概念研究所博士後研究，負責本章第貳、參節後半、第伍節與第柒節。

開始重視更複雜的太空雷射科技，太空部署雷射的目的將是針對戰略及區域性的飛彈防禦能力。美國國防部計畫從 2020 年開始，進行太空雷射的工程發展。[1]美國海軍正在發展革命性的艦上武器系統，其中包括固態雷射（solid state lasers，SSL）、電磁軌道砲（Electromagnetic Railgun, EMRG）、導引砲彈（Gun-Launched Guided Projectile, GLGP）等。早在 2014 年，海軍即在兩棲船塢登陸艦龐斯號（*USS Ponce*, LPD 15）上進行 AN/SEQ-3 雷射武器系統（Laser Weapons System, LaWS）實驗，用以反制小型無人機、無人快艇，2017 年曾在中東進行實驗性部署。[2]LaWS 用較保守方式發展，應付軍事上的急迫任務，除反制無人機外，還包括海上反恐、獵殺水雷等一系列任務。其功率雖僅 3 萬瓦，但在測試中已足以擊落慢速飛行的無人機。LaWS 基本上是將六具商用焊接雷射「綁」在一起，讓雷射光束聚合在目標上。[3]

美國海軍預計於 2021 年，在勃克級（Arleigh Burke-Class）驅逐艦普雷貝爾號（*USS Preble*, DDG 88）上裝置「高能雷射與整合光學殺傷監視系統」（High Energy Laser and Integrated Optical-dazzler with Surveillance, HELIOS），HELIOS 是海軍雷射武器發展戰略的一部分，[4]能量為 6 萬瓦，未來則提升至 10 至 15 萬瓦。這套系統由洛克希德馬丁公司（Lockheed Martin）發展，部署在勃克級驅逐艦上時，將與神盾作戰系統（Aegis combat system）整合，除作為防禦用武器外，雷射光束也可用來執行長程情監偵任務。

美國陸軍也將雷射、微波、極音速武器視為高度優先計畫。[5]陸軍「快速能力及關鍵計畫辦公室」（Rapid Capabilities & Critical Technologies Office, RCCTO）計畫發展一系列 IFPC 系統，用以保護前線部隊，包括飛彈、雷射、微波武器等，可配備在重型卡車上，或定點部署，保護前進機場、補給節點、指揮中心等關鍵設施，做為陸軍未來中空層的飛彈防禦系統。前進部署則由新的「機動短程空防系統」（Maneuver Short-Range Air Defense, MSHORAD）負責，以史崔克（Stryker）甲車做為載台，搭載機砲、飛彈，以及新的 5 萬瓦雷射，對付數量最多的威脅

[1] Ben Werner, “Pentagon Shifts Focus on Directed Energy Weapons Technology,” *USNI News*, September 5, 2019, https://news.usni.org/2019/09/05/pentagon-shifts-focus-on-directed-energy-weapons-technology.
[2] “Navy Lasers, Railgun, and Gun-Launched Guided Projectile: Background and Issues for Congress,” The Congressional Research Service, May 17, 2019, https://assets.documentcloud.org/documents/6018848/Navy-Lasers-Railgun-and-Gun-Launched-Guided.pdf.
[3] Jason Mick, “LaWS (Laser) "Kills" Boat-Hauled Fuel Tanks, UAV "Bomber" in the Persian Gulf,” *Dailytech*, December 12, 2014, http://www.dailytech.com/LaWS+Laser+Kills+BoatHauled+Fuel+Tanks+UAV+Bomber+in+the+Persian+Gulf/article36994.htm.
[4] Ben Werner, “Pentagon Shifts Focus on Directed Energy Weapons Technology,” *USNI News*, September 5, 2019, https://news.usni.org/2019/09/05/pentagon-shifts-focus-on-directed-energy-weapons-technology.
[5] Theresa Hitchens, “Lasers, Microwaves, Hypersonics & More: Army RCCTO,” *Breaking Defense*, August 7, 2019, https://breakingdefense.com/2019/08/lasers-microwaves-hypersonics-more-army-rccto/.

，如火箭、火砲、迫砲、無人機及直升機等。諾斯洛普格魯曼（Northrop Grumman）及雷神（Raytheon）將競標史崔克甲車的雷射系統。[6]

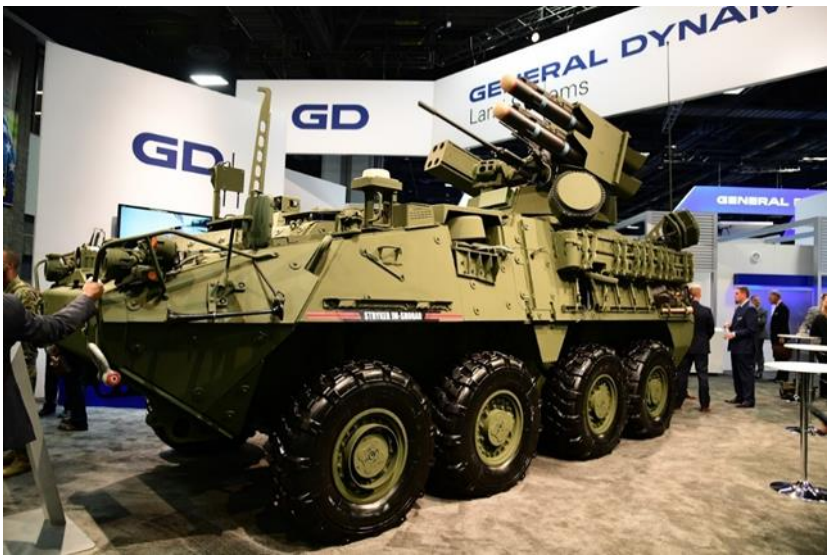


圖 6-1、機動短程防空系統

資料來源：舒孝煌攝影。

說明：通用動力集團在 2019 年美國陸軍年會暨裝備展中展出其發展的機動短程防空系統。

除了 10 萬瓦等級的車載雷射系統外，洛克希德馬丁也計畫自行發展 25 萬至 30 萬瓦的更高能量雷射，預計 2022 年進行展示，2024 年部署，[7]其原型系統稱為「先進測試高能裝備」（Advanced Test High Energy Asset, ATHENA），可用以攻擊大型無人系統、小型無人機、小型快艇、火箭等目標。

美國空軍在 2019 年開始接收第一套高能雷射武器系統（high-energy laser weapon system，HELWS），由雷神公司發展，裝置小型全地形車輛上，使用一套「多光譜目標標定系統」（Multi-spectral Targeting System），由光電及紅外線偵測、辨識及追蹤無人機，再以雷射加以摧毀。充電時可使用 220 伏特電源，供應光電偵蒐系統，並足以供雷射發射數十次。[8]

[6] Jen Judson, “Northrop and Raytheon to compete to build laser weapon for short-range air defense,” *Defense News*, August 1, 2019, https://www.defensenews.com/land/2019/08/01/northrop-and-raytheon-to-compete-to-build-laser-weapon-for-short-range-air-defense/.

[7] Theresa Hitchens, “Lasers, Microwaves, Hypersonics & More: Army RCCTO,” *Breaking Defense*, August 7, 2019, https://breakingdefense.com/2019/08/lasers-microwaves-hypersonics-more-army-rccto/.

[8] “Raytheon announces delivery of first laser counter-UAS system to U.S. Air Force,” *Defence Blog*, October 23, 2019, https://defence-blog.com/news/raytheon-announces-delivery-of-first-laser-counter-uas-system-to-u-s-air-force.html.

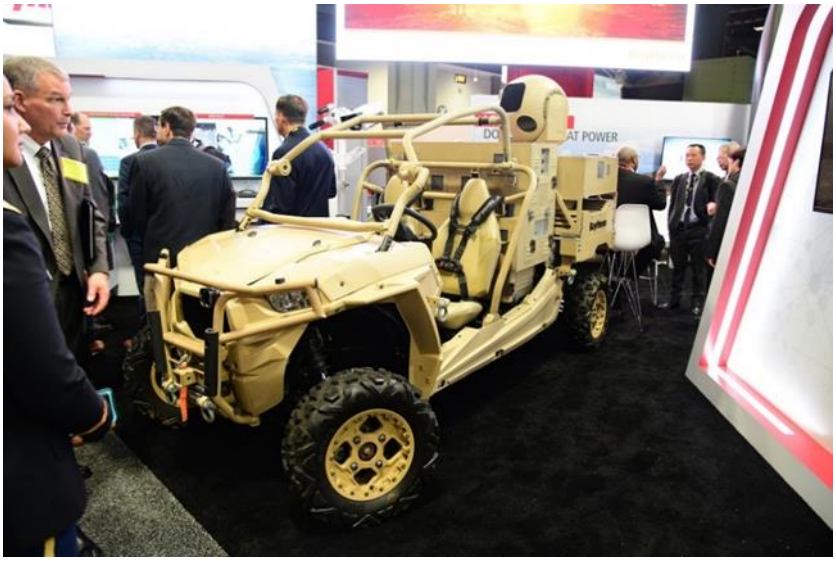


圖 6-2、高能雷射武器系統

資料來源：舒孝煌攝影。

說明：雷神公司發展的高能雷射系統，可由小型全地形車搭載。

二、俄羅斯及歐洲雷射武器

不僅美國，俄羅斯及歐洲國家同樣在雷射武器上投入大量研究，並在近年逐漸得到突破，後者則以德國及英法為甚。2018 年 3 月 1 日，俄國總統普欽（Vladimir Putin）在其國情咨文演講中，提及俄羅斯已在雷射武器上取的顯著進展，俄軍並已自 2017 年開始裝備雷射武器，[9]引起各國注意；2018 年 7 月，俄羅斯軍方公布的影片中揭露了裝置在卡車上的「佩列斯韋特」（Peresvet，14 世紀率兵對抗蒙古軍的俄國僧侶）雷射武器系統，儘管公開資料不足，然推測可能用以對抗巡弋飛彈及無人機，也可能用以「弄瞎」敵方的先進裝備，[10]而此雷射武器也是普欽在其國情咨文中所提及的 6 種關鍵性先進武器之一，另 5 項包括核動力巡弋飛彈、RS-28 洲際彈道飛彈、前衛（Avangard）核彈頭極音速助推滑翔載具、核動力無人水下載具，以及超音速巡弋飛彈。[11]

而在歐洲方面，近十年來德國廠商在相關領域投注相當心力。德國萊茵金屬公司（Rheinmetall AG）與 MBDA 德國分公司（MBDA Germany）皆針對防空用途分別投入陸基與海基的高能雷射（High-Energy Laser, HEL）研發多年。兩家公司皆運用高能光纖（fibre）雷射技術，並已進行多年實驗與測試；萊茵金屬公司將開發重點至於光束疊加（beam-superimposing）技術，並將光譜耦合（spectral

[9] "Presidential Address to the Federal Assembly," *President of Russia*, March 1, 2018, http://en.kremlin.ru/events/president/news/56957.

[10] "Peresvet Combat Laser Complex," Global Security, October 12, 2018, https://www.globalsecurity.org/military/world/russia/vlk.htm.

[11] Joseph Trevithick, "Here's The Six Super Weapons Putin Unveiled During Fiery Address," *the Drive*, March 1, 2018, https://www.thedrive.com/the-war-zone/18906/heres-the-six-super-weapons-putin-unveiled-during-fiery-address.

coupling）技術作為長期選項，而德國 MBDA 自 2008 年開始研發相關系統，並已在測試中成功耦合多個雷射光源。這些系統多半針對 C-RAMM 及反無人機等任務進行測試。[12]2019 年 2 月，萊茵金屬完成機動武器站（mobile weapon station）測試，此武器站具備與該公司之 MANTIS 防空系統密切相關的架構，由雷射光源、帶望遠鏡的光束定向器（beam director）及追蹤器組成，可整合 10 萬瓦以內的雷射光源，並正在研發 2 萬瓦的雷射。[13]

針對雷射武器的發展，德國海軍在 2019 年 2 月時提出要求，希望在 2020-2021 年時整合高能雷射武器的原型到 K130 級巡邏艦（Korvette 130），又稱「布倫瑞克」級（Braunschweig-Klasse）上，並將針對無人機進行最佳化。為此，2019 年 8 月 8 日，萊茵金屬與 MBDA 德國分公司正式宣布將攜手為此計畫進行合作，並將在德國官方宣布進一步的性能需求指標後，決定兩家公司的分工；[14]德軍的雷射武器技術在未來將不只應用在艦艇上，也可能在陸地作戰，例如基地火砲或戰車上應用。[15]

英國與法國在近年也開始了雷射武器的計畫，英國在 2017 年時開始投資「龍火」（Dragonfire）艦載雷射武器，由 MBDA、匡提科（QinetiQ）、李奧納多（Leonardo）、阿爾克（Arke）、貝宜（BAE Systems）、馬歇爾（Marshall）和吉凱恩（GKN）等公司合作發展，並取得 3,000 萬英鎊資金。2019 年 7 月，英國國防部宣布計畫投入 1.62 億美元的資金研發三種不同的雷射武器原型，儘管「龍火」計畫於 2019 年進行測試，新計畫將進一步聚焦於其尺寸、功能性及如何整合於現有載台上；新計畫中包含兩個高能雷射原型，其中一個裝載於船艦上進行防空與平面防禦，另一個裝在地面車輛上，用於短程防空及反監視任務，第三個則是地面車輛用射頻（radio frequency）武器，透過破壞或使對手電子系統喪失作用，以對抗空中無人機及敵人行動，並預計在 2023 年開始測試。[16]

法國也在 2019 年宣布將投入數千萬歐元進行雷射武器的研究，並預期在 2025 年時將能進入測試。此研究項目將使用雷射武器對抗太空及地面系統，如燒毀太陽能板、破壞感測器等方式，使光學或通信衛星失能。[17]值得注意的是，

---

[12] "Raising HEL: The mirage of laser weapons," *Jane's International Defence Review*, 2015, https://www.janes.com/images/assets/736/51736/The_mirage_of_laser_weapons.pdf.

[13] Press Release, "Rheinmetall presses ahead with laser weapon technology: New weapon station successfully tested," *Rheinmetall AG*, February 28, 2019, https://www.rheinmetall-defence.com/en/rheinmetall_defence/public_relations/news/latest_news/index_19392.php.

[14] "Rheinmetall and MBDA to build HELWS demonstrator for German corvette," *Naval Technology*, August 9, 2019, https://www.naval-technology.com/news/rheinmetall-and-mbda-to-build-helws-demonstrator-for-german-corvette/.

[15] Mischa Geörg, "Bundeswehr bereitet sich auf Einsatz von Laserwaffen vor — mit Strahlenkanonen Made in Germany," *Business Insider Deutschland*, June 12, 2019, https://www.businessinsider.de/bundeswehr-bereitet-sich-auf-einsatz-von-laserwaffen-vor-mit-strahlenkanonen-made-in-germany-2019-6.

[16] Andrew Chuter, "UK shoots for new laser weapons against drones, missiles," *Defense News*, July 9, 2019, https://www.defensenews.com/global/europe/2019/07/09/uk-shoots-for-new-laser-weapons-against-drones-missiles/.

[17] Pierre Tran, "French Investments in Laser Weapons: ONERA at the Paris Air Show 2019," *Defense.info*, June 14, 2019, https://defense.info/multi-domain-dynamics/2019/06/french-investments-in-laser-weapons-onera-at-the-paris-air-show-2019/.

歐洲的跨國飛彈大廠 MBDA 同樣參與了法國的雷射武器計畫，成為貫穿英德法三國導能武器發展的核心廠商。MDBA 甚至另外參與了歐盟的「戰術先進雷射光學系統」（Tactical Advanced Laser Optical System, TALOS）計畫，[18]此計畫為歐盟「國防研究準備行動」（Preparatory Action on Defence Research, PADR）中的一環，由歐洲防衛署（European Defence Agency）負責，並由法國雷射公司 CILAS 主導，儘管投入預算僅 5 百餘萬歐元，然 TALOS 計畫將預期為歐盟未來的相關研發計畫提供框架、提供路線圖，並確保戰略自主及供應安全，並預期在未來十年中讓歐盟的高能雷射能整合進軍事應用中。[19]

三、其他國家的雷射武器發展

在美俄與歐洲國家外，中國和以色列等國同樣在投注雷射武器的發展。2018 年 11 月的珠海航展中，中國正式展示其航天三江集團研發的 3 萬瓦等級雷射武器「LW-30 激光防禦武器系統」。根據航展上對此種武器的解釋，中國的 LW-30 與前述多種雷射武器用途相仿，以對抗光電導引系統、無人機及 C-RAMM 等為主要任務目標。

以色列拉斐爾先進防禦系統公司（Rafael Advanced Defense Systems）在 2014 年推出的「鐵光束」（Iron Beam）防禦系統，同樣以防禦 C-RAMM 作為其主要任務，由於以色列經常需與哈馬斯（HAMAS）及真主黨（Hezbollah）等對手交戰，經常遭遇迫砲甚至火箭攻擊，因此以色列發展了包含「鐵穹」（Iron Dome）在內的多種 C-RAMM 武器，「鐵光束」可說是此類武器的進一步發展，針對此類攻擊及日益猖獗的小型無人機，成本較低廉的雷射顯然是較「鐵穹」在內各種飛彈武器更為適宜對抗此類不對稱攻擊。

另一個值得注意的國家是土耳其，2019 年 8 月 3 日，利比亞「民族團結政府」（Government of National Accord, GNA）運用土耳其製的 5 萬瓦雷射防禦系統擊落對手由阿拉伯聯合大公國提供的中國製「翼龍 2 型」（Wing Loong II）軍用無人機，顯示土耳其可能已領先於其他各國，率先將此類武器投入運用，並在北非衝突中進行測試。[20]

---

[18] Pierre Tran, “French Investments in Laser Weapons: ONERA at the Paris Air Show 2019,”.

[19] “Pilot Project and Preparatory Action on Defence Research,“ *European Defence Agency*, July 8, 2019, https://www.eda.europa.eu/what-we-do/activities/activities-search/pilot-project-and-preparatory-action-for-defence-research.

[20] “Libya’s GNA forces shoot down UAE-purchased Chinese drone near Misurata,” *Libya Express*, August 3, 2019, https://www.libyanexpress.com/libyas-gna-forces-shoot-down-uae-purchased-chinese-drone-near-misurata/; “Turkey uses laser weapon technology to shoot down Chinese UAV Wing Loong II in Libya,” Army Recognition, August 12, 2019, https://www.armyrecognition.com/weapons_defence_industry_military_technology_uk/turkey_uses_laser_weapon_technology_to_shoot_down_chinese_uav_wing_loong_ii_in_libya.html.

參、極音速武器與長程打擊武器

極音速一般指以超過音速 5 倍或更快速度在大氣中飛行的載具或武器。[21]除了極音速飛行器外，在武器方面，包括「極音速巡弋飛彈」（Hypersonic Cruise Missile, HCM）及「極音速滑翔載具」（Hypersonic Glide Vehicle, HGV）兩種型式，前者是由地面、飛機或船艦上發射，後者由飛彈或火箭發射，在「彈頭」重返大氣層時藉重力加速度達到高速。

美國發展目標曾經是「傳統迅捷全球打擊」（conventional prompt global strike, CPGS）計畫，但近年研究則聚焦在短程及中程的極音速滑翔載具及極音速巡弋飛彈（hypersonic cruise missile）上，用以應付區域衝突。這是因為中國及俄羅斯也在加速發展極音速武器，並獲得成功，使得美國受到嚴重威脅。

一、中國極音速武器發展

2019 年 10 月 1 日，中國在其建政 70 周年閱兵時展出多種新型號武器，其中極音速武器「東風 17」受到矚目。東風 17 可能是其過去的 WU-14 極音速實驗載具的服役型式，其「彈頭」部分為極音速載具，採乘波體設計，由一具東風 16 飛彈的單級火箭推進，東風 16 射程超過 1,000 公里，東風 17 則約在 1,800 至 2,500 公里左右，屬中程彈道飛彈等級。2017 年 11 月，中國進行 2 次「東風 17」的測試，第一次在內蒙古酒泉發射中心發射，飛行時間 11 分鐘，飛行距離約 1,400 公里，飛行高度約 60 公里，據說目標精度達 10 公尺直徑左右。至於飛行速度，美國認為約 5 馬赫，俄方則估計約 8-10 馬赫。

傳統彈道飛彈將彈頭發射至太空，再依計算的軌跡重返大氣層，藉重力加速度擊中目標，若是中程飛彈，重返大氣層的速度約在 8 馬赫左右，遠程彈道飛彈重返速度則可達 20 馬赫，彈道飛彈的彈頭通常沒有動力，因大氣層有阻力，速度會逐漸衰減。極音速滑翔載具則是用火箭將「彈頭」或載具加速到高超音速，進入太空後結束彈道飛行狀態，在大氣層邊緣以極音速「滑翔」，藉助空氣動力調整與變軌，使其飛行軌道複雜化。此一彈道被稱為「錢學森彈道」（Trajectory of Qian Xuesen），讓彈頭在 20 至 100 公里高度「滑翔」，再進入大氣層，因此又稱助推滑翔彈道。

「東風 17」是世界上第一種進入服役測試的極音速滑翔載具。美國情報單位估計「東風 17」可在 2020 年達到初始戰力。「東風 17」將可加強中國的核嚇阻力量，因為它能穿透美國的飛彈防禦網，美式的飛彈防禦系統是依彈道飛彈的拋物線計算軌跡，錢學森彈道的飛行軌跡無法預測，傳統飛彈防禦系統難以攔截。「東風 17」也被認為可能破壞印太地區的穩定，因為它會使飛彈擊中目標前的反應時間縮短至幾分鐘，大幅壓縮鄰國領導者的決策時間。

[21] Yasmin Tadjdeh, “SPECIAL REPORT: Defense Department Accelerates Hypersonic Weapons Development,” *National Defense Magazine*, July 11, 2019, https://www.nationaldefensemagazine.org/articles/2019/7/11/defense-department-accelerates-hypersonic-weapons-development.

目前中國打擊美國海軍的主要武器是「東風 21D」及「東風 26」，「東風 17」號稱「新航艦殺手」，服役後將使中國反艦彈道飛彈體系更加完整，對西太平洋的美國海軍航艦構成全新威脅。[22]

另外，中國也在 2018 年 8 月成功測試星空 2 號極音速實驗載具，星空 2 號由一具單級火箭推進，獨立飛行時可進行機動，維持 5.5 馬赫速度超過 400 秒，最大速度達到 6 馬赫，約為時速 7,344 公里，有報導認為這可能轉用於搭載核彈頭，但也有媒體指出，這是中國發展極音速飛機的野心之一。[23]

二、俄羅斯極音速武器發展

俄羅斯近年也全力發展極音速武器，外界所知或曾公開過的包括：[24]

（一）Kh-32，已達作戰部署標準，可搭配核彈頭，據報導最大速度達 4 至 5 馬赫，射程約 1,000 公里。

（二）伊斯坎德 M（Iskander-M）及改良型伊斯坎德 M 空射彈道飛彈，已達作戰部署標準，可搭載核彈頭，射程約 700 至 1,000 公里。

（三）Kh-47M2 匕首（Kinzhal）飛彈，被稱為「高精確極音速機載飛彈系統」，目前已達作戰部署標準，可搭載傳統及核彈頭，射程達 2,000 公里。2018 年時俄國防部副部長波里索夫（Yuri Borisov）說匕首飛彈可由 MiG-31 戰機攜帶，塔斯社（TASS）也稱其為空射彈道飛彈，另外該飛彈應也可由 Su-34 打擊戰鬥機，或 Tu-22M 逆火式轟炸機攜帶。

（四）縮小版的匕首飛彈，由 Su-57 戰機攜帶。

（五）前衛（Avangard）極音速洲際彈道飛彈，彈道採推進－滑翔（boost-glide）式，據說在技術上有真正突破，曾在 2018 年試射成功，2019 年已開始部署。

（六）3M22 鋯石（Zircon）極音速巡弋飛彈，射程可達 1,000 公里，速度可達 9 馬赫，另有說法指其射程可達 2,000 公里，數年後可完成作戰部署。

極音速武器極難攔截，主要原因是其速度及機動能力。反飛彈系統的動能攔截器也需要高速及機動力以攔截彈道飛彈，它們必須追蹤彈道飛彈一段時間。普通的彈道飛彈彈道高很多，可以在更長時間以雷達偵測及追蹤，但極音速武器在大氣中飛行的軌跡很低，完全進入大氣飛行時，便難以被固定的地面雷達探測及追蹤，而且它還能躲避追蹤。即使防禦系統的雷達有能力追蹤極音速武器，其可

[22] Jon Lockett & Debbie White, "China unveils terrifying Dongfeng-41 nuke that 'can strike US in 30 minutes with TEN warheads' at 70th anniversary parade," *the Sun*, October 1, 2019, https://www.thesun.co.uk/news/10039105/china-set-*to*-unveil-dongfeng-41-nuke-that-can-strike-us-in-30-minutes-at-70th-anniverary-parade/.

[23] Liu Zhen, "China's hypersonic aircraft, Starry Sky-2, could be used to carry nuclear missiles at six times the speed of sound," *South China Morning Post*, August 6, 2018, https://www.scmp.com/news/china/diplomacy-defence/article/2158524/chinas-hypersonic-aircraft-starry-sky-2-could-be-used.

[24] Mark B. Schneider, "Russian Hypersonic Missiles Have 1 Goal (And They Might Be Unstoppable)," *National Interest,* September 11, 2019, https://nationalinterest.org/blog/buzz/russian-hypersonic-missiles-have-1-goal-and-they-might-be-unstoppable-79591.

防禦區域也會被縮小。這些俄製極音速武器使其可用於突襲美國國家指揮機構，因為它們很少有堅固掩體，使其在面對這種新式突襲手段時顯得脆弱。[25]

有報導指出，俄羅斯正發展 KH-MT 飛彈，採衝壓推進，可由 Tu-95MSM 轟炸機攜帶。9M730 海燕（Burevestnik）飛彈是一種核動力極音速巡弋飛彈，其技術難度較超音速巡弋飛彈更高，而且危險甚高，俄羅斯在 2019 年 8 月的試驗過程中，曾發生工廠爆炸的嚴重意外，5 名工人喪生，且造成輻射污染。核動力飛彈是使用核分裂產生的高熱來產生推力。過去美蘇都發展過核動力飛機，但從未真正使用核動力驅動發動機，因此使用核動力飛彈，不論是否使用核彈頭，即使在承平時期，其核污染的問題仍會受到西方國家關注。[26]

因「大國競爭」再起，冷戰結束後一度被放棄的武器，有可能因而恢復發展，也可能掀起新一波軍備競賽。俄羅斯也加速極音速武器的服役，在 2019 年底之前，前衛極音速飛彈可能會進入服役。[27]俄羅斯海軍也可能首先部署潛射式極音速飛彈，成為第一個擁有潛射極音速武器的國家。[28]

三、美國極音速武器發展

2008 年，美國國防部的國防先進研究計畫署（Defense Advanced Research Projects Agency, DARPA）即已在研究極音速技術，當時目的在發展快速全球打擊能力，但未繼續發展。2010 年，美國空軍實驗室（Air Force Research Laboratory, AFRL）與 DARPA 聯合發展 X-51「乘波者」（WaveRider）極音速載具，採用超音速衝壓發動機技術，藉衝擊波形成壓縮升力，但未能完成測試。2018 年 AFRL 再進行低成本極音速試驗，即 X-60A，預計達到 8 馬赫的高速，但僅供研究。2019 年 5 月海軍航太展覽會（Sea Air Space 2019）上，洛克希德馬丁展出一具極音速飛行器模型，可能是延續 HTV-2 極超音速飛行載具計畫的努力，另外也展出可能供 F-35C 掛載的極音速巡弋飛彈概念。[29]

美國總統川普 2018 年決定退出《中程飛彈條約》(*Intermediate-Range Nuclear Forces Treaty,* INF)，並於 2019 年 8 月正式退出。目前極音速武器已是美國最高優先發展項目，至少有 6 種極音速武器正在發展，其中兩項由空軍主導，兩項由

[25] Mark B. Schneider, "Russian Hypersonic Missiles Have 1 Goal (And They Might Be Unstoppable)," *National Interest*, September 11, 2019, https://nationalinterest.org/blog/buzz/russian-hypersonic-missiles-have-1-goal-and-they-might-be-unstoppable-79591.

[26] Fabian Schmidt "Russia's nuclear-powered cruise missile, fact or fiction?" *Deutsche Welle*, August 08, 2019, https://www.dw.com/en/russias-nuclear-powered-cruise-missile-fact-or-fiction/a-50024689.

[27] Pranz-Stefan Gady, "Russia: Avangard Hypersonic Warhead to Enter Service in Coming Weeks," T*he Diplomat*, November 14, 2019, https://thediplomat.com/2019/11/russia-avangard-hypersonic-warhead-to-enter-service-in-coming-weeks/.

[28] H I Sutton, "Russian Navy To Be First To Field Hypersonic Cruise Missiles On Submarines," *Forbes*, September 15, 2019, https://www.forbes.com/sites/hisutton/2019/09/15/russian-navy-to-be-first-to-field-hypersonic-cruise-missiles-on-submarines/#4e8f0596542c.

[29] Xavier Vavasseur, "SAS 2019: Lockheed Martin's Hypervelocity Missile For F-35C," *Naval News*, May 9, 2019, https://www.navalnews.com/event-news/sas-2019/2019/05/sas-2019-lockheed-martins-hypervelocity-missile-for-f-35c/.

DARPA 與空軍合作，海軍及陸軍各有一項，[30]主要技術包括使用超音速衝壓發動機（Scramjet），由飛機攜帶，在空中發射，以及推進－滑翔技術，將彈頭打至太空，在落下過程中以重力迫使加速打擊目標：[31]

（一）空軍極音速武器計畫：

美國空軍在 2018 年開始推動空射式超音速反艦飛彈的發展，由於極音速發動機技術較困難，藉 2016 會計年度國會授權，先行發展 2 具原型供測試使用。這項合約在 2018 年 4 月由洛克希德馬丁獲得，價值 4 億 8 千萬美元。同年 8 月，空射快速反應武器（air-launched rapid response weapon, ARRW）被賦予 AGM-183A 的編號。2019 年 6 月 12 日，1 架 B-52 轟炸機首次進行 AGM-183 空射實驗。AGM-183 使用超音速衝壓技術，但僅有感測器，且未在試驗中投擲，[32]只用來蒐集飛機操作與環境參數。

圖 6-3、AGM-183 極音速武器

資料來源：舒孝煌攝影。

說明：美國空軍的 AGM-183 飛彈已於 2019 年 6 月首度進行飛行試驗。

另一項計畫是「極音速傳統打擊武器」（Hypersonic Conventional Strike Weapon, HCSW），2018 年 4 月選定洛克希德馬丁發展，負責設計、發展、工程、系統整合、測試、後勤計畫、以及與飛機的整合等，目的在運用已成熟的技術並

[30] Sydney J. Freedberg Jr., "Hypersonics Won't Repeat Mistakes Of F-35," *Multimedia Report: Missile Defense*, March 13, 2019, https://breakingdefense.com/2019/03/hypersonics-wont-repeat-mistakes-of-f-35/; Brian Wang, "First US Hypersonic Interceptor Defense Test Scheduled for 2020," April 17, 2019, *NetBig Future*, https://www.nextbigfuture.com/2019/04/first-us-hypersonic-interceptor-defense-test-scheduled-for-2020.html.

[31] Kyle Mizokami, "The U.S. Air Force Is Pushing for a Hypersonic Strike Weapon," *Popular Mechanics*, Jun 11, 2018, https://www.popularmechanics.com/military/weapons/a21239436/us-air-force-hypersonic-strike-weapon/.

[32] "AGM-183A Air-Launched Rapid Response Weapon - ARRW / Arrow," *GlobalSecurity*, https://www.globalsecurity.org/military/systems/munitions/agm-183.htm.

加以整合，與 ARRW 不同，HCSW 使用固態燃料火箭，具備 GPS 導引能力，[33]將用以打擊高價值及具急迫性目標。空軍計畫在 2021 年試射 HCSW。[34]

在空軍與 DARPA 合作發展的兩項計畫中，其中之一是「戰術助推滑翔」（Tactical Boost Glide, TBG），[35]另一是「極音速進氣武器」（Hypersonic Air-Breathing Weapon, HAWC）。TBG 目的在發展與展示一種空射、戰術層級的極音速助推滑翔系統，由火箭把彈頭推至高速，接著與火箭分離，以無動力方式滑翔打擊目標。TBG 將運用全新概念的推進系統，允許更佳的控制性及可操縱性，預計射程為 500 哩。TBG 包括地面及飛行測試兩階段，主要目標為驗證載具的可行性，包括其氣動力學、氣動熱力性能、可操縱性、操作有效性及可負擔性，[36]新發展合約在 2019 年 5 月由雷神公司獲得。[37]

HAWC 發展合約則由雷神和諾斯洛普格魯曼獲得，總值 2 億美元。TBG 和 HAWC 是兩種不同的極音速推進概念，[38]HAWC 也是空射型，預計也要以 B-52 搭載。[39]目的在發展具備極音速飛行的先進機體結構、碳氫超音速衝壓推進技術。諾斯洛普格魯曼將負責發展超音速衝壓發動機，用以推進雷神生產的彈體。2 家公司已在 2019 年巴黎航展時宣布結盟。[40]極音速衝壓發動機困難之處，在於要將進入發動機的空氣流維持在超音速，這容許載具可以較高速度及高度飛行，因空氣密度降低，也可降低機身磨擦產生的高熱。2019 巴黎航展時波音公司也表示美國空軍新採購的 F-15EX，將可掛載極音速武器。

（二）海軍

海軍「傳統快速打擊武器」（Conventional Prompt Strike, CPS）是延續先前的「傳統快速全球打擊」計畫（Conventional Prompt Global Strike, CPGS），[41]曾包

---

[33] Brian Wang, “First US Hypersonic Interceptor Defense Test Scheduled for 2020,” April 17, 2019, *NetBig Future*, https://www.nextbigfuture.com/2019/04/first-us-hypersonic-interceptor-defense-test-scheduled-for-2020.html.

[34] Valerie Insinna, “Lockheed nabs another big hypersonic weapons contract”, *DefenseNews* August 14, 2018, https://www.defensenews.com/air/2018/08/14/lockheed-nabs-another-big-hypersonic-weapons-contract/.

[35] Yasmin Tadjdeh, “Just In: Two Different DARPA Hypersonic Vehicles 'On Track' to Fly in 2019,” *National Defense*, May 1, 2019, http://www.nationaldefensemagazine.org/articles/2019/5/1/just-in-darpa-hypersonic-vehicle-prototypes-to-fly-in-2019.

[36] Peter Erbland, “Tactical Boost Glide (TBG), Defense Advanced Research Projects Agency, https://www.darpa.mil/program/tactical-boost-glide.

[37] Guy Norris, “Lockheed Hypersonic Missile Unveiled As AGM-183A,” *Aviation Week Network*, August 7, 2018, https://aviationweek.com/air-dominance/lockheed-hypersonic-missile-unveiled-agm-183a.

[38] Yasmin Tadjdeh, “Just In: Two Different DARPA Hypersonic Vehicles 'On Track' to Fly in 2019,” *National Defense*, May 1, 2019, http://www.nationaldefensemagazine.org/articles/2019/5/1/just-in-darpa-hypersonic-vehicle-prototypes-to-fly-in-2019.

[39] Robin Hughes, “Raytheon prepares for first flight of HAWC prototype demonstrator,” *Jane's 360*, June 21, 2019, https://www.janes.com/article/89437/raytheon-prepares-for-first-flight-of-hawc-prototype-demonstrator.

[40] David Szondy, “Northrop Grumman and Raytheon team up to develop air-breathing hypersonic missile”, *New Atlas*, June 19, 2019 https://newatlas.com/raytheon-nrthrop-grumman-hypersonic-air-breathing-missile-agreement/60203/; Robin Hughes, “Raytheon prepares for first flight of HAWC prototype demonstrator,” *Jane's 360*, June 21, 2019, https://www.janes.com/article/89437/raytheon-prepares-for-first-flight-of-hawc-prototype-demonstrator.

[41] Colin Clark, “Army Moves Out on Lasers, Hypersonics: Lt. Gen. Thurgood,” *Breaking Defense*,

括陸軍 AHW、HTV-2 等，2020 年由海軍接手，改成傳統快速打擊武器，海軍曾在 2017 年測試極音速武器成功，由夏威夷發射一枚武器擊中馬紹爾群島的目標區。洛克希德馬丁於 2019 年 4 月再獲得價值 25 億美元的合約，這是在海軍戰略系統計畫（SSP）項下的「中程傳統打擊武器系統」（Intermediate Range Conventional Prompt Strike Weapon System, IRCPS）的早期發展階段，目標在發展一種可在 2025 年服役的極音速滑翔武器。海軍也與陸軍緊密合作，開發數種不同的平台。海軍在 2017 年就曾成功發射一枚極音速滑翔武器擊中目標。[42]

未來海軍的 CPGS 將配備在潛艦及水面艦，為了容納新飛彈，海軍考慮發展新的垂直發射系統，安裝在勃克級驅逐艦上，並結合神盾作戰系統，未來也會配備在新的大型水面艦上。

（三）陸軍

陸軍「陸基極音速飛彈」（Land-Based Hypersonic Missile）計畫，預計在未來 5 年投資 12 億美元，並與海軍及空軍合作，期待在 2023 年進行測試。2012 年陸軍曾成功測試先進極音速武器概念（Advanced Hypersonic Weapon, AHW），速度曾達到 8 馬赫，射程達到 6,000 公里。[43]目前 ATACMS 射程僅約 300 公里，陸基極音速飛彈射程則可達 1,600 公里。[44]陸軍「多領域作戰」概念中，遠程打擊是極重要部分，可使陸軍從傳統陸上作戰角色轉變成長程打擊火力的完全夥伴。陸軍極音速飛彈可與海空軍共用載具，由陸上車輛載運，具陸上機動能力。

四、其他國家的極音速載具發展

由於極音速載具的技術並非全新的獨家概念，因此除了美、俄、中等國具備在此領域中最頂尖的技術外，尚有多個國家投身其中並取得一定成果，如澳洲、印度、法國、德國等，另外日本也在 2018 年時宣布將研發「島嶼防衛用」高速滑空彈等，顯示相關技術逐漸擴散。就近期的武器化發展來說，印度在與俄羅斯合作的 BrahMos II 極音速巡弋飛彈以外，也正在研發自製的類似裝備，並在 2019 年 6 月成功測試 6 馬赫的超燃衝壓發動機；而法國在其 V-max（véhicule manoeuvrant experimental）實驗機動載具計畫下，修改超音速空對地飛彈 ASN4G，使其在 2022 年前能具備極音速飛行能力，[45]預期在 2035 年服役時，成為法國核

May 24, 2019, https://breakingdefense.com/2019/05/army-moves-out-on-lasers-hypersonics-lt-gen-thurgood/.

[42] Sam LaGrone, Lockheed Martin Working $2.5B in Hypersonic Weapon Contracts, *USNI News*, April 23, 2019, https://news.usni.org/2019/04/23/lockheed-martin-working-2-5b-in-hypersonic-weapon-contracts.

[43] Joseph, Trevithick, "Here's What the Army's First Ever Operational Hypersonic Missile Unit Will Look Like," *the Drive*, June 3, 2019, https://www.thedrive.com/the-war-zone/28340/heres-what-the-armys-first-ever-operational-hypersonic-missile-unit-will-look-like.

[44] Colin Clark, "Army Moves Out on Lasers, Hypersonics: Lt. Gen. Thurgood," *Breaking Defense*, May 24, 2019, https://breakingdefense.com/2019/05/army-moves-out-on-lasers-hypersonics-lt-gen-thurgood/.

[45] Kelley M. Sayler, "Hypersonic Weapons: Background and Issues for Congress," *Congressional Research Service*, September 17, 2019, p. 15, https://fas.org/sgp/crs/weapons/R45811.pdf.

子打擊能力未來的重要關鍵。[46]德國雖然曾在 2012 年時成功測試 SHEFEX II 極音速滑翔載具，但目前的武器化計畫卻將重點放在較為「防禦性」的方面，將研發速度能超越 5 馬赫的反戰車飛彈，以對抗日益增強的主動防護系統，並考慮在未來將極音速載具技術投入研發飛彈防禦系統。[47]

日本在 2018 年宣布將研發「島嶼防衛用高速滑空彈」後，更在新版的防衛計畫大綱（又稱「30 大綱」）中更明白宣布，將建立兩個裝備此種極音速武器的大隊（營）。此「高速滑空彈」研發計畫已由 2018 年開始，預期在 2025 年為部隊配備初期型第一批次（Block 1）量產型，隨後的第二批次才裝上「乘波體」彈頭，兩階段的研發顯示了日本希望盡可能運用較成熟的技術，縮短新式裝備服役的時間，並可持續透過自衛隊驗證、改良裝備的技術甚至運用方法等。[48]

肆、人工智慧與無人載具的運用

一、結合人工智慧的忠誠僚機

「忠誠僚機」（Loyal Wingman）目的在使無人機真正與有人機伴隨作戰，減少有人戰機遭受攻擊的威脅，然而這必需結合人工智慧，使其能真正自主飛行。波音公司 2019 年 2 月接受澳洲空軍委託發展忠誠僚機計畫，[49]這被稱為「空權團隊系統」（Airpower Teaming System, ATS），2019 年 11 月 18 日首度完成自主飛行，使該計畫成功邁出一大步。[50]波音使用一種小型的噴射動力實驗機，首次進行半自主式聯合飛行，同時也測試噴射機間安全溝通及協調能力，該 2 架無人噴射機以時速約 186 哩速度飛行，波音並未說明詳細內容，僅表示未來將進行更複雜的機動動作，並增加編隊機數，以及更複雜任務。這是澳洲空軍「空權團隊系統」發展的一部分，其最終目的是要讓有人機與無人機搭配執行任務，並運用新控制架構以自主維持與其他飛機的編隊飛行，並執行任務。

澳洲空軍希望這種無人噴射機可以飛行 2,000 哩，與澳洲空軍各種有人飛機一起執行任務，包括 F-35A、F/A-18E/F、EA-18G、E-7A 預警機及 P-8 巡邏機等。無人機將採模組化設計，容許快速轉換模組並重新配置，以執行各種不同任務。無人機需具備某種程度自主權，其程度多寡取決於系統的搭配、其中角色及工作

[46] "MBDA opens data centre in France for missile development," *Air Force Technology*, April 5, 2019, https://www.airforce-technology.com/news/mbda-data-centre-france-missiles/.

[47] Michael Peck, "Germany Is Now Building Hypersonic Weapons," *National Interest*, June 7, 2019, https://nationalinterest.org/blog/buzz/germany-now-building-hypersonic-weapons-61652.

[48] 〈装備庁の高速滑空弾開発、25 年度には部隊配備へ〉，《WING》，2019 年 11 月 14 日，http://www.jwing.net/news/18912。

[49] "Boeing accelerates 'Loyal Wingman' drone program," *Defense-blog*, August 16, 2019, https://defence-blog.com/army/boeing-accelerates-loyal-wingman-drone-program.html?fbclid=IwAR0fVKv0hzadJWSupUlGHnFxOnYnPJpciipcysCJV2jL46eoNYCKEnZfKGM.

[50] Joseph Trevithick, "Boeing Conducts Flight Test of Surrogate Drones for Australia's Loyal Wingman Program," *the Drive*, November 19, 2019, https://www.thedrive.com/the-war-zone/31104/boeing-conducts-flight-test-of-surrogate-drones-for-australias-loyal-wingman-program.

分配。雖然因運用人工智慧，可將人從決策循環中抽離，但仍需保持控制，其操作程式的某個部分，可以由地面站、製造商，或由戰機上傳。[51]

該計畫的核心是匿蹤無人僚機的發展。AFRL 的 XQ-58 女武神（Valkyrie）已分別在今年 3 月及 6 月成功完成 2 次僚機試飛。空軍打算與洛克希德馬丁及波音合作，使 F-35A Block4 及 F-15EX 都能容納資料鏈及處理器，以便與無人機搭配作戰。

XQ-58 是美國空軍快速發展全翼式匿蹤武裝無人機計畫的努力之一，「天空堡壘」（Skyborg）計畫則是整合有人機及無人機的軟體與硬體。未來空軍戰鬥機的僚機將不再是有人駕駛的隊友，而是無人戰機。美國空軍將以廉價的 XQ-58 與 F-35A 或 F-15EX 聯手，減少空中高價戰機的數量，並降低成本及飛行員要負擔的風險。XQ-58 價值僅數百萬美元，可成為 F-35 的戰力倍增器。該計畫在人工智慧方面投注大量資金及人力，預計在 2023 年達到作戰能力。在天空堡壘計畫下，有人戰機仍是整個作戰網路的中心，XQ-58 無人機則在周邊展開，由人工智慧控制無人機、處理遙測資料、擬訂飛行計畫，並獲取目標。

為發展忠誠僚機計畫，美國空軍第 412 測試聯隊使用特殊的測試手段，在 2019 年進行「複雜環境下自動化操作」（Testing of Autonomy in Complex Environments, TACE）飛行測試，以手持式「褐雨燕」（Swift）小型無人機進行測試，並蒐集測試資料供發展自主化操作的參考。TACE 使用一套自動飛行演算法控制飛機，其中兩項機制，一是自主監控，若在自動飛行過程中違反安全參數，例如接近其他飛機、飛出空域或失去與地面控制站接觸，便會中止自主飛行，回到安全空域巡航。第二是即時虛擬及建構（Live Virtual Constructive, LVC），允許模擬實體與真實飛機互動，將數位化方法、模擬器與真實裝備結合。[52]

這符合美國空軍 2019 年 4 月所發布《科學及技術戰略：強化美國空軍 2030 年及以後之科技》報告（*Science and Technology Strategy: Strengthening USAF Science and Technology for 2030 and Beyond*）的目標，即發展低成本且數量大的平台，藉 AI 與多領域指揮管制等方式，以恢復美國的空中優勢。[53]

美國空軍認為現有無人機系統將很快落伍，傳統情監偵體系也將失去意義。美國空軍要運用更多人工智慧、雲端運算、無人機集群操作等技術，維持美國空權優勢。人工智慧將是無人機核心，可協助操作飛機，並主動識別目標，飛行員不再需要使用肉眼識別目標，所有訊息都會集中在感測器的「網格」（Grid）上。[54]

---

[51] Joseph Trevithick, “Boeing Conducts Flight Test of Surrogate Drones for Australia's Loyal Wingman Program,” *War Zone*, November 19, 2019, https://www.thedrive.com/the-war-zone/31104/boeing-conducts-flight-test-of-surrogate-drones-for-australias-loyal-wingman-program.

[52] William Kucinski, “Air Force tests fully autonomous UAS control system,” *SAE International*, March 12, 2019, https://saemobilus.sae.org/automated-connected/news/2019/03/air-force-tests-fully-autonomous-uas-system.

[53] “Science and Technology Strategy: Strengthening USAF Science and Technology for 2030 and Beyond,” *Air Force Research Laboratory*, April 17, 2019, https://afresearchlab.com/wp-content/uploads/2019/04/Air-Force-Science-and-Technology-Strategy.pdf.

[54] Paul McLeary, “USAF Wants Drone Swarms, AI to Buy Space,” *BreakingDefense*, August 02, 2018,

二、無人機集群技術

DARPA 正在實驗使用自動化操作的集群無人機及機器人協助執行軍事任務，2019 年 6 月於美國喬治亞州進行一項測試，是「攻勢型集群能力戰術」（Offensive Swarm-Enabled Tactics, OFFSET）計畫的一部分，讓小型無人機及地面機器人伴隨一支小規模步兵部隊，在密集的城鎮環境中工作，最終其規模會擴大至 250 架無人機及地面機器人，未來則會持續增加任務的複雜度。

集群式無人機在戰場上可能有許多戰術潛力。個別式無人機雖然有助觀測戰場情況，但要躲藏不被無人機發現並非難事。DARPA 認為大量的集群式無人機可以協助作戰單位對周邊環境的全面性瞭解。

另一個 DARPA 的計畫是「X 班」（Squad X），這是另一項開發「有人－無人」團隊潛力的計畫，即讓現場士兵使用無人機及機器人的人工智慧技術來蒐集周邊環境的大量訊息。美國陸軍近期也開始測試步兵單位使用掌上型無人機的情況，用以傳送影像及其他資訊。[55]

相反的，陸軍同樣也在測試如何消滅敵人的集群式無人機。美國空軍展示使用一種工具，稱為「雷神索爾」（THOR），這是一種微波傳送器，用以清除大量無人機。美國海軍則是在波斯灣使用一種稱為「輕型陸戰隊空防整合系統」（Light Marine Air Defense Integrated System, LMADIS），成功在數千碼距離擊落伊朗無人機。[56]

DARPA 在 2018 年 11 月推動「在拒止環境中協同操作」（Collaborative Operations in Denied Environment, CODE）研究計畫，測試無人機協同實戰測試，[57]目的在驗證高度電子戰環境下，通訊與衛星定位訊號受干擾時，無人機能以高度自動化方式協同運作。[58] CODE 計畫著重改善協調自主能力，由單一人員操作整個集群式無人機群，可持續評估本身情況與作戰環境，並向操作者提供協調行動建議，操作人員則決定是否同意，並指導任務變更。

無人機集群式自動化飛行需彼此協調，避免互撞，自行定位並保持相對位置，每架無人機都不需要操作人員，形成一個整體。具 CODE 能力的無人機將根據既定接戰規則進行接戰。操作人員則進行最少的監督，並配合動態情況如友軍消耗或是應付緊急威脅。

---

https://breakingdefense.com/2018/08/usaf-wants-drone-swarms-ai-to-buy-space.

55 Jay Peters, "Watch DARPA test out a swarm of drones," *the Verge*, August 9, 2019, https://www.theverge.com/2019/8/9/20799148/darpa-drones-robots-swarm-military-test.

56 Ibid.

57 "CODE demonstrates autonomy and collaboration with minimal human commands," *Space Daily*, November 20, 2018, http://www.spacedaily.com/reports/CODE_demonstrates_autonomy_and_collaboration_with_minimal_human_commands_999.html.

58 Patrick Tucker, "The US Military's Drone Swarm Strategy Just Passed a Key Test," *Defense One*, November 21, 2018 https://www.defenseone.com/technology/2018/11/us-militarys-drone-swarm-strategy-just-passed-key-test/153007.

三、無人艦艇

海軍正在進行兵推和原型發展，以便了解無人機及無人水面艦艇將如何適應艦隊，以及濱海作戰艦（Littoral Combat Ship, LCS）如何在全球擴展其存在。目前海軍正持續進行無人戰機及無人艦艇如何與有人駕駛船艦併肩作戰，並為戰鬥做出貢獻的測試。

目前海軍已經擁有 2 艘大型無人艦，即「海獵人」（Sea Hunter），可讓船隻轉移至自主控制系統，目前已完成第一階段測試，確保無人艦可在海上按照航行規則自主航行，另外也確認其船體設計、機械和電子系統能可靠支持海上航行，無需要維修人員隨時待命，確保其完成航行任務。

海軍計畫再採購 2 艘無人艦，持續進行導航等更高階的工作，並搭載海軍的作戰裝備及指管通情系統。海軍為大型無人水面艦（Large USV, LUSV）所進行的測試工作中，有些是已知的技術，例如自主航行工作，主要集中在導航、避碰，及與海上其他船隻互動，並確保 LUSV 本身系統的運作正常。LUSV 也還沒有涉及到自主發射武器的階段。[59]

有關武器交戰的決定，海軍高階官員指出，作戰計劃仍是人為制定的。海軍部署 LUSV 受到關注，基本上海軍希望 LUSV 擔任類似「無人飛彈卡車」的角色。有人操作的神盾戰系驅逐艦會被告知要使用本身的感測系統，向艦艇本身看不到的視距外目標發射武器，LUSV 的運作方式其實大致相同，戰鬥人員仍然會對致命的接戰做出決定，只是他們並不會登上無人艦。

然而，其他操作及運用無人艦的定義仍然缺乏，例如運用無人艦的戰術戰法，以及接戰規則等，無人艦有可能接受其他艦艇指令後發射武器，但還不會自己使用艦上感測器自主發射武器，也不會發射武器進行自衛，這也表示，無人艦目前會緊密跟隨驅逐艦、濱海作戰艦或其他艦艇，擔任保護及必要時犧牲的角色。

海軍官員認為目前無人系統仍處在「提問階段」，建造無人艦的原型並進行實驗，仍是度過這段時間並繼續尋求答案的唯一方法。

四、人工智慧在國防領域的運用與限制

人工智慧是快速發展的領域，可能對國家安全產生重大影響。美國國防部或其他國家都在開發運用人工智慧的一系列技術，以便運用在作戰上，目前人工智慧被運用在情報蒐集及分析、物流，網路及資訊作戰、指揮管制，以及一系列自動及半自動航行等領域。人工智慧已被運用在伊拉克和敘利亞境內的軍事行動中。國會可能進一步干預技術發展，而預算和立法也決定軍事應用的成長及採用的速度。

---

[59] Megan Eckstein, "Unmanned Vehicle Operations, Global LCS Support Informed by Ongoing Wargaming, Prototyping," *USNI News*, November 11, 2019, https://news.usni.org/2019/11/21/unmanned-vehicle-operations-global-lcs-support-informed-by-ongoing-wargaming-prototyping?fbclid=IwAR08IzTAX6H135CzoR9PScX0WrbSu4SQiSEsLIO1-LbBNFV-LDEXG4zPol0.

人工智慧的運用，對軍事整合是一項獨特挑戰。目前人工智慧主要發展仍發生在商業領域。國防採購過程可能需要進行調整以獲取新興技術，人工智慧即是一例。此外，許多商用的人工智慧應用程序也須要先進行重大修改，然後才能運用在軍事用途。文化問題也對人工智慧運用提出挑戰，因為某些資訊產業出於道德考量，不願與國防部合作，甚至在公司內部，也可能存在將人工智慧技術納入現有武器系統和流程的阻力。

人工智慧的潛在國際競爭對手正向美國施加壓力，迫使美國要與對手競爭創新的軍事人工智慧應用。中國是這方面的領導者，曾在 2017 年公布計劃，擬在 2030 年前奪取人工智慧發展的全球領先地位。中國目前主要致力於利用人工智慧做出更快、更明智的決策，還包括發展一系列自動駕駛技術。俄羅斯也積極參與軍用人工智慧的開發，主要側重在機器人技術。

儘管人工智慧能在軍事領域賦予許多優勢，但也會帶來不同的挑戰。例如，人工智慧技術可以促進自主行動，導致更明快的軍事決策，並提高作戰速度和規模。但是，人工智慧也可能是不可預測，或易受獨特形式的操縱而影響。由於這些因素，分析師對人工智慧在未來的作戰行動中將產生怎樣的影響力持有廣泛的看法。不過大多數專家都同意，人工智慧至少會產生革新的影響，即使還不能算是革命。[60]

美國國防部正全力推動人工智慧發展，同時也提出多份文件以指導人工智慧發展，其中 2018 年 11 月公布的《人工智慧戰略摘要：運用人工智慧促進安全及繁榮》（*Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity*），認為人工智慧意指機器在執行通常需要人類智慧的任務，例如認知模式、由經驗中學習並得出結論、做出預測及採取行動，無論這是數位化的過程，或是指自主化系統背後的智慧軟體。[61]報告認為，人工智慧將會改變每個產業，同時也會對國防部內每個領域產生影響，如作戰、訓練、維持、部隊保護、招聘、醫療保健、保護平民及盟友等等，同時也加速作戰節奏。

2018 年 8 月美國國防部發布的另一份「2017 至 2042 會計年度無人化系統整合藍圖」（*Unmanned Systems Integrated Roadmap FY2017-2042*）也指出，機器學習（machine learning）是快速成長的領域，包括指揮管制（C2）、導航，智慧化感測器情況覺知、偵測及迴避障礙物、群體行為及戰術，以及與人類互動等。深度學習（deep learning）則可運用許多圖形處理單元、傳統中央處理器及神經元晶片，從大量資料中學習各種模式。[62]另外，《2018 年美國國防戰略摘要》及《2019

[60] "Artificial Intelligence and National Security," *Congressional Research Service*, November 21, 2019, https://crsreports.congress.gov/product/pdf/R/R45178.

[61] "Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity," U.S. Department of Defense, November 8, 2018, https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.

[62] "Unmanned Systems Integrated Roadmap FY2017-2042," U.S. Department of Defense, November 8, 2018, https://www.defensedaily.com/wp-content/uploads/post_attachment/206477.pdf.

年國防授權法案》都要求各軍種發展、測試與運用自動化和人工智慧系統，顯示美軍對人工智慧的重視。

另外，美國國防部成立「聯合人工智慧中心」(Joint Artificial Intelligence Center, JAIC)，領導人工智慧戰略發展，該中心提供人工智慧相關知識，協助開發技術、知識、相關流程，確保該領域的長期發展及可擴展性。JAIC 的任務之一是藉加速交付及採用人工智慧，擴大其對執行任務的影響，並逐漸改變國防部。[63]

目前人工智慧正逐步擴大在國防上的運用，其中在無人載具的運用上，包括協助分析資料、自動化行駛，並簡化操作程序，另外包括解決自動化操作過程所要面對的問題，如安全航行、避免碰撞、跟隨部隊、與僚機或隊友互動，以及應付天候、地形等障礙，並增加情況覺知能力、強化機動力、保護部隊安全、強化戰力，必要時將能自動接戰。

目前將人工智慧運用在軍用無人載具，主要仍在解決優先問題，即自主航行所要面對的問題，目前能真正面對複雜環境變化的自動化系統仍不存在。軍方需重新審視人工智慧能力的限制因素，重新評估對人工智慧及自動化技術的需求。雖然美軍指揮官對人工智慧尚不能完全信任，但其對手都在全力發展人工智慧，未來有可能因為軍備競賽，導致不成熟的技術被採用，或是無法信任的對手惡意運用，造成無法預測的傷害。

另外，運用人工智慧將不可避免地討論到接戰問題。自主戰鬥無人機是否可以自行觸發扳機？美國，英國和俄羅斯反對聯合國試圖禁止自動殺人機器，顯示各國軍方在此一方向的發展脈絡。隨著自主化系統日益增加，武裝部隊將需面對嚴重的道德問題。一方面，給予無人機自主觸發扳機權力有其意義，F-35 飛行員在進行空戰機動時可能沒有時間發射飛彈。另一方面，人工智慧系統若意外向平民開火，誰該負責？

《人工智慧戰略摘要》中，美國國防部並未提到能獨立思考並作戰的致命武器，目前美軍正在運用的人工智慧技術並不特別，都是專注解決一般問題。不過早在 2012 年，國防部就出版過一分指令，定義自動化武器及如何部署，並明確指出人類仍應保持在此一決策循環內，並詮釋人類需對此類武器保持多少控制。不過完全自主式武器，仍有很長的路要走。另外，人工智慧可能面臨任何意外情況，不是每一個運用軍事力量的對手都能採用同樣的高標準，這是未來要面對的問題。

[63] U.S. Department of Defense Chief Information Officer, Joint Artificial Intelligence Center, https://dodcio.defense.gov/About-DoD-CIO/Organization/JAIC/.

伍、戰場無人系統

一、戰場無人系統

從前述無人載具運用，可以注意到類似裝備的發展將在未來戰場上有效協助士兵進行任務，成為武裝部隊的重要核心，目前包含美國、歐盟多國、俄羅斯等主要大國皆投注心力在發展戰場無人系統上。單以無人航空系統（Unmanned Aerial System, UAS）來說，目前美軍即已在其包含國民兵在內的四個軍種，操作從輕型的 RQ-11「渡鴉」(Raven)到大型的 RQ/MQ-4「全球之鷹/海神之子」(Global Hawk/Triton）等，共約 11,000 架各式 UAS，[64]足見無人飛行載具運用數量之龐大；而無人地面載具（Unmanned Ground Vehicle, UGV）也早在地面部隊中負責拆彈等重要角色，因此可說無人載具在各國軍隊中，早已扮演重要角色。

近年，無人系統在戰場上的重要性也逐漸上升，同時並不僅限於飛行載具，陸海等不同場域運用的無人載具皆十分受到各國矚目，例如俄羅斯軍事工業委員會（Russian Military Industrial Committee）便批准了發展計畫，預期將能在 2030 年時使俄羅斯戰力的 30%由無人遙控與自主的機器人載台組成，[65]以下便從幾個不同層面，藉由近期各領域的無人載具發展，探求未來無人戰場的雛形。

（一）無人飛行載具

「無人飛行載具」(Unmanned Air Vehicle, UAV）仍是目前無人載具領域中，發展最為興盛的方面。目前 UAV 在戰場上的廣泛運用及其未來性，使得各國軍方皆必須發展自己的無人機機隊，並防範敵人各式無人機威脅。

目前 UAV 已廣泛運用於各地戰場，除了美軍在介入各地時大量運用無人機外，中東及北非各地由於美國對外出口無人機的嚴格管制，轉而大量進口中國製的無人機，同樣廣泛運用在衝突之中。事實上，就無人機技術而言，中東戰場可視為一未來戰場雛形，不僅大型軍用無人機在中東及北非皆受到大量運用外，自殺無人機及小型無人機（包含民用改造用作軍事用途等）的大量創意運用，可見其在未來戰場上的重要性。

葉門武裝團體「青年運動」(Houthi）在伊朗支援下，不僅裝備了彈道飛彈，也取得多種無人機加以運用。在面對配備西方先進防空裝備（如愛國者飛彈）的沙烏地阿拉伯及阿拉伯聯合大公國時，「青年運動」仍能運用其 UAV 進行創新的不對稱攻擊，值得注意的是，「青年運動」在 2017 年時已被確認獲得伊朗製的「Qasef-1」自殺無人機，這些廉價的自殺無人機被用以壓制阿拉伯聯軍的愛國者飛彈，以掩護其彈道飛彈攻擊。[66]此外，2019 年 9 月 14 日，沙烏地阿拉伯的石

[64] "Unmanned Aircraft Systems (UAS) DoD: Purpose and Operational Use," U.S. Department of Defense, https://dod.defense.gov/UAS/.

[65] Andrew Feickert, Jennifer K. Elsea, Lawrence Kapp and Laurie A. Harris, "U.S. Ground Forces Robotics and Autonomous Systems (RAS) and Artificial Intelligence (AI): Considerations for Congress," *Congressional Research Service*, p.11, November 20, 2018, https://crsreports.congress.gov/product/pdf/R/R45392.

[66] Tyler Rogoway, "Suicide Drones Have Migrated To The Conflict In Yemen," *The Drive*, March 24,

油設施遭遇無人機與巡弋飛彈的長程打擊，這些攻擊成功穿過愛國者與天兵（Skyguard）防空系統，擊中目標；[67]這些運用不但成功的穿透了先進防空系統，也使人有機會一窺未來戰場上無人機的作戰運用方式。

而北非利比亞戰場則由於土耳其與阿拉伯聯合大公國交付大量無人機給予其代理人，因而成為中國製及土耳其製大量 UAV 的戰場，除了前述中國製「翼龍 2 型」遭到擊落外，各種與 UAV 相關的設施如其機場與指管中心等均成為重要打擊目標，UAV 也成為這些武裝團體的「空軍」。[68]然而，目前的軍用無人機在面對高性能防空系統時，可能仍具相當脆弱性，此可由美軍 RQ-4「全球之鷹」（Global Hawk）無人機在 2019 年 6 月遭到伊朗防空飛彈擊落看出，因此在面對可能的大國衝突戰場時，未來無人機的設計將需進一步針對高強度戰場進行最佳化。

（二）無人地面載具

如同 UAV，UGV 概念同樣早在一次大戰時即已出現，在二戰時德國的「歌利亞」遙控炸彈車即可說是 UGV 的雛形。無人地面載具長時間成為拆彈/爆裂物處理單位的最佳夥伴，而近年更因為技術發展，開始出現具備各種感測器擔任 ISR 任務、甚至搭載各式武裝的戰鬥 UGV。目前無人地面載具的發展仍以俄羅斯及歐美為主。

首先值得注意的是近年俄羅斯在 UGV 上投入的發展，在無人地面載具上投注大量心力，並已發展包含「旋風」（Vikhr，以 BMP-3 步兵戰鬥車改裝而成）、「Uran-9」等多種武裝 UGV 進行測試，這些 UGV 能在數公里外進行遙控（Vikhr 遙控距離可達 10 公里，Uran-9 則可在 3 公里外進行遙控），[69]並能搭載包括 30mm 機砲、反戰車飛彈等各式武裝，「Uran-9」甚至以投入敘利亞在內的戰場進行實驗性運用。俄羅斯在 UGV 發展上，相當重視其作為武器載台的作戰用途，「Uran-9」首要的設計目的即為作戰用途，並強調其作為攻擊矛頭進行突破，以及與一般部隊緊密協同作戰等用途。[70]

相較之下，美國在 2017 年 3 月發佈的《美國陸軍機器人與自主系統戰略》（*The U.S. Army Robotics and Autonomous Systems Strategy*）中對武裝 UGV 採取的態度，在近期內仍較俄羅斯略為保守，在該《戰略》中，美軍詳細定義了對 UGV 在戰場上的主要任務，分別是：1. 強化戰場覺知（situation awareness），2. 減低

2017, https://www.thedrive.com/the-war-zone/8586/suicide-drones-have-migrated-to-the-conflict-in-yemen.

[67] Joseph Trevithick, “Here's All the New Info You Need To Know In The Aftermath Of The Saudi Oil Facilities Attacks,” *the Drive*, September 18, 2019, https://www.thedrive.com/the-war-zone/29918/heres-all-the-new-info-you-need-to-know-in-the-aftermath-of-the-saudi-oil-facilities-attacks.

[68] Peter Brookes and Terre Schroeder, “Game of Drones: Coming to a Military Theater Near You,” The Heritage Foundation, October 8, 2019, https://www.heritage.org/defense/commentary/game-drones-coming-military-theater-near-you.

[69] Ibid., p.12.

[70] Charlie Gao, “Russia vs. America: Which Nation Will Dominate Unmanned Ground Vehicles?” *National Interest*, August 11, 2018, https://nationalinterest.org/blog/buzz/russia-vs-america-which-nation-will-dominate-unmanned-ground-vehicles-28407.

士兵負荷，3. 強化後勤能力維持部隊，4. 強化部隊的運動與機動能力，5. 保護部隊。[71]從該《戰略》中的要求來看，美軍在 UGV 的運用上，仍是著眼於無人載具的機動能力（如在人類無法到達的地方行動）、感測能力、運輸能力等，減輕部隊負擔、並且強化對空間的運用能力及作戰縱深；而在保護部隊上，美軍同樣認為 UGV 能強化作戰縱深，增加部隊對抗敵方編隊、火箭火砲等威脅的遠距（standoff）能力，以保護士兵。在技術層面上，美軍在其《美國陸軍機器人與自主系統戰略》中所規劃的未來藍圖顯示美軍預期能在 2021-2030 時開始引進無人作戰車輛，初期預計具備有人駕駛、遙控及半自主技術，並嘗試在此時期及在人工智慧自主操作上取得突破。[72]

而在目前的發展上，「可置換載人戰鬥車輛」（Optionally Manned Fighting Vehicle, OMFV）計畫，即將前述要求之要素作為其要求之重要性能指標之一。此計畫為美國陸軍目前全力進行之「六大」現代化優先項目（“big six” priorities）中，排名第二的「下一代戰鬥車輛 」（Next Generation Combat Vehicle, NGCV）之重要計畫。OMFV 預期將用以取代 M2「布萊德雷」（Bradley）步兵戰鬥車，除了本身將具備無人操作能力外，OMFV 也預期將搭配美軍未來的 UGV-「機器人作戰載具」（Robotic Combat Vehicle, RCV）進行運用，而「有人—無人組合」（manned-unmanned teaming）正是其 OMFV 在設計時所需考量最重要概念。

在美軍的規劃中，預計與 OMFV 搭配運用之 RCV 將分為輕、中、重型等三種形式，未來將擔負從協助 ISR 任務、強化部隊戰場覺知到裝備重型武器實際參與戰鬥（重型 RCV 預計將裝備戰車砲）等各種任務。針對這項計畫，美國陸軍於 2019 年向軍工大廠發出輕型及中型 RCV 需求，而整個計畫預計在 2020 年時開始進行車輛測試。在 2020 年時，美軍將首先運用由 M113 裝甲運兵車改裝而成的 RCV 搭配由 M2 步兵戰鬥車改裝的控制車輛「任務推進科技驗證載具」（Mission Enabler Technologies-Demonstrators）進行測試，美國陸軍預期在 2021 財年末開始第二階段測試，在此階段除了原先的 4 輛 M113 改裝車外，也將加入各軍工大廠為美軍提供之各 4 輛中型與輕型 RCV；重型 RCV 則將在 2023 財年年中開始的第 3 階段加入測試，這個階段同樣將測試 4 輛 M113 RCV，以及廠商提供之中型與重型 RCV 各 4 輛，預期未來服役的 RCV 將會因為其無人操作，而能以較小的體型、較低的重量提供與現行裝甲車輛同等級的殺傷能力。[73]

2019 年 10 月 21 日，美國陸軍正式選擇德事隆（Textron）與旗下機器人新創公司 Howe&Howe、HDT Global、豪士科（Oshkosh）、匡提科北美分公司與

[71] U.S. Army Training and Doctrine Command and Army capabilities Integration Center, “The U.S. Army Robotic and Autonomous Systems Strategy,” U.S. Army, March 2017, https://www.tradoc.army.mil/Portals/14/Documents/RAS_Strategy.pdf.

[72] U.S. Army Training and Doctrine Command and Army capabilities Integration Center, “The U.S. Army Robotic and Autonomous Systems Strategy,” p.8.

[73] Sean Kimmons and Army News Service, “Soldiers to operate armed robotic vehicles from upgraded Bradleys,” U.S. Army, July 11, 2019, https://www.army.mil/article/224241/soldiers_to_operate_armed_robotic_vehicles_from_upgraded_bradleys.

Pratt&Miller 等四個團隊獲選參與 RCV-L；[74]2019 年 11 月 1 日則宣布通用動力陸上系統（General Dynamics Land Systems）、匡提科北美分公司與德事隆等 3 個團隊獲選得以進一步參與製造 RCV-M 的原型，其中後二者同時參與了 RCV-L 與 RCV-M 兩個計畫。[75]

美俄兩大國以外，歐洲國家也積極參與 UGV 的研發，其中愛沙尼亞米爾倫（Milrem）公司研製的「履帶混合模組化步兵系統」（Tracked Hybrid Modular Infantry System, THeMIS）值得注意，THeMIS 為模組化設計，其中央模組可更換各種用途以負責運輸、後勤、情監偵、消防、掃雷、醫療後送甚至裝置各種武器接戰等各種任務，THeMIS 除可酬載 750 公斤物件外，尚可遙控操縱或自動跟隨駕駛。產品的優異性能使米爾倫很快便與眾多歐美大廠進行合作，並使 THeMIS 能整合各種遙控武器站，甚至反裝甲飛彈與小型無人機，極具任務潛力，並在 2019 年 10 月隨著愛沙尼亞部隊部屬至馬利（Mali）。[76]愛沙尼亞也因此成為歐盟《永久性結構防衛合作協定》（Permanent Structured Cooperation, PESCO）中重要研究項目模組化無人地面系統（Modular Unmanned Ground Systems）的領導者，成為小國軍工發展的典範。

德國萊茵金屬公司則發展了「任務大師」（Mission Master）UGV，同樣高度模組化與自動跟隨駕駛能力，更在 2019 年 9 月波蘭「國際國防工業展」（Międzynarodowy Salon Przemysłu Obronnego）中，展出其整合波蘭製自殺無人機「Warmate」的版本，[77]可預期未來各種武裝將逐漸整合到 UGV 上，使其正式成為主要武器載台。在 2019 年美國陸軍協會（Association of the United States Army）年會中，萊茵金屬更將「任務大師」的技術整合到德國陸軍自 80 年代以來大量運用的「鼬鼠」（Waffenträger Wiesel）輕裝甲車上，[78]與俄羅斯先前以 BMD 空降裝甲車為基礎研發 UGV 相同，可知未來傳統舊式載台將可能藉由持續的改裝、甚至作為無人載具運用，持續在未來戰場活躍。此外，類似美國正在發展的「有人-無人組合」作戰概念，德國與法國剛開始啟動的下一代主戰車「主要地面作戰系統」（Main Ground Combat System, MGCS）計畫中，也將可能具備搭配 UGV 及 UAV 作戰的能力；如同美軍預期淘汰 M1 主戰車的時間點，MGCS 將在 2035

[74] Jen Judson, "The field narrows in US Army's light robotic combat vehicle competition," *Defense News*, October 21, 2019, https://www.defensenews.com/digital-show-dailies/ausa/2019/10/21/the-field-narrows-in-light-robotic-combat-vehicle-competition/.

[75] Jen Judson, "Three teams move on in medium-size robotic vehicle prototype competition," *Defense News*, November 1, 2019, https://www.defensenews.com/land/2019/11/01/three-teams-move-on-in-medium-sized-robotic-vehicle-prototype-competition/.

[76] Harry Lye, "THeMIS UGV makes operational debut on patrol in Mali," *Army-technology*, October 1, 2019, https://www.army-technology.com/news/themis-ugv-operational-debut/.

[77] Nicholas Fiorenza, "MSPO 2019: Rheinmetall presents Mission Master UGV with Warmate loitering munition," *Jane's 360*, September 4, 2019, https://www.janes.com/article/90846/mspo-2019-rheinmetall-presents-mission-master-ugv-with-warmate-loitering-munition.

[78] "AUSA 2019: Rheinmetall proposes next generation solutions to US Army highest priority modernization challenges," *Army Recognition*, October 14, 2019, https://www.armyrecognition.com/ausa_2019_news_show_daily_coverage_report_united_states/ausa_2019_rheinmetall_proposes_next_generation_solutions_to_us_army_highest_priority_modernization_challenges.html.

年左右開始逐步取代現有的「豹 2」(與美軍 M1 推出的時間點相仿)及「雷克勒」(Leclerc)主戰車。[79]

圖 6-4、萊茵金屬「鼬鼠」無人輕裝甲車

資料來源：舒孝煌攝影。

說明：配備「任務大師」的「鼬鼠」無人輕型裝甲車，由萊因金屬公司發展。

在美國與歐陸之外，澳洲目前也正在進行 UGV 測試，澳洲目前建立了一個稱為「信賴自主系統」(trusted autonomous systems)的合作研究中心(cooperative research centre)計畫，其中主要成員之一的貝宜(BAE Systems)公司藉其掌握的無人載具技術，在澳洲同樣改裝了兩輛 M113 AS4 裝甲運兵車投入測試，為澳洲軍方探索未來無人戰場的可能性，[80]可見無人地面載具的研究及概念已逐漸擴散。

不過，UGV 目前在戰場應用上仍有許多需克服的障礙。俄羅斯 UGV 在敘利亞戰場上的實際運用顯示，Uran-9 不僅主武裝 2A72 30mm 機砲運作及感測器的偵測距離出現問題，在都市的複雜環境下，其遙控操作距離也遠短於原先的設計，[81]顯示相關技術在近期內仍有待測試與驗證，值得進一步觀察。

(三)無人水面/水下載具

無人水面載具(Unmanned Surface Vehicles, USV)及無人水下載具(Unmanned underwater vehicle, UUV)的發展由來已久，時至今日已有多個國家具有製造無人水下載具的能力，然以無人作戰艦而言，仍以美俄兩大強權為最主要的技術領航者。美國海軍目前正嘗試尋求一系列的全新平台或升級來加強其無人艦隊，在計畫中，美軍將生產超大型、大型、中型和小型等數種 UUV，並在 2019 年與波音公司簽訂價值高達 2.74 億美元的合約以建造 5 艘「虎鯨」(Orca)式超大型 UUV(XLUUV)原型。美軍也預計在 2020 財年開始徵求大型 UUV(LDUUV)

[79] "Main Ground Combat System – Common Indirect Fire System," *Global Security*, February 21, 2019, https://www.globalsecurity.org/military/world/europe/mgcs.htm.

[80] "BAE Systems partners with Australian Army for autonomous vehicles," *Army Technology*, September 5, 2019, https://www.army-technology.com/news/bae-australia-autonomous-vehicles/.

[81] David Brown, "Russia's Uran-9 robot tank reportedly performed horribly in Syria," *Business Insider*, July 10, 2018, https://www.businessinsider.com/russias-uran-9-robot-tank-performed-horribly-in-syria-2018-7.

「鱧魚」（Snakehead）的投標書，並正在準備中型 UUV 與大型、中型 USV 等不同的研發案，在美國海軍的規劃中，水面的「幽靈艦隊」（Ghost Fleet）計畫將以大型、中型 USV 作為其作戰核心。[82]根據美軍公布的資料，「虎鯨」由波音公司的「回聲巡航者」（Echo Voyager）無人柴電潛艦發展而來，能自主航行並具備 6,500 浬航程而不依賴母船，「虎鯨」的模組化設計使她能用於反制水雷、反潛、反水面艦艇、電子戰以及打擊任務等，[83]可攜帶 Mk.46 輕型魚雷或 Mk.48 重型魚雷，及飛彈等武裝，並可在海床上放置貨物或佈雷，同時「虎鯨」的價格也遠低於各種傳統作戰艦艇，極具作戰效益。[84]

美軍同時也研發了多款較小型的 UUV，如「刀魚」（Knifefish），此種 UUV 為標準 533mm（21 英吋）魚雷直徑，[85]將搭配濱海作戰艦或其他海軍艦艇進行反水雷任務。這種 UUV 經過多年測試實驗，已於 2019 年 8 月 23 日得到美國海軍批准並將進入初始生產階段，美國海軍並宣布一個 4,400 萬美元的合約以採購 39 套「刀魚」系統，其中 24 套將用於 LCS 上。[86]

在 UUV 以外，美國海軍也在 2019 年開始要求廠商提供護衛艦（corvette）大小的 USV 投標書草案，並要求撥款 4 億美元以建造兩艘研發用的 2,000 噸級的大型無人水面載具（LUSV）。儘管 LUSV 及中型 MUSV 的運用概念仍在研發中，美軍預期將透過 USV 的部署提供艦隊更廣泛、龐大的感測器節點，及進一步加強火力投射能力。[87]

美國目前的規劃顯示其對無人作戰艦艇的急迫需求，美軍預期在 2020 財年時開發與採購 LUSV、MUSV 及 XLUUV，並將透過無人作戰艦艇的導入，進行海軍艦隊結構的轉型。美國海軍將提高小型艦艇及無人艦艇的比例，並減少大型水面艦艇如驅逐艦與巡洋艦在整個艦隊中的比重，並透過這些轉型面對來自中國的挑戰。[88]跟隨著美國的腳步，英國也開始投入 XLUUV 的發展。英國國防科技實驗室（Defence Science and Technology Laboratory, DSTL）在 2019 年啟動了 XLUUV 計畫，以協助皇家海軍評估其未來戰場用途。[89]

---

[82] Mandy Mayfield, “Navy Seeking New Technology for Unmanned Boats, Subs,” *National Defense*, October 18, 2019, https://www.nationaldefensemagazine.org/articles/2019/10/18/navy-seeking-new-technology-for-unmanned-boats-subs.

[83] Ben Werner, “Navy Awards Boeing $43 Million to Build Four Orca XLUUVs,” *USNI News*, February 13, 2019, https://news.usni.org/2019/02/13/41119.

[84] Kyle Mizokami, “The Navy Just Ordered the 'Orca,' an Extra-Large Unmanned Submarine by Boeing,” *Popular Mechanics*, February 14, 2019, https://www.popularmechanics.com/military/navy-ships/a26344025/navy-extra-large-unmanned-submarines-boeing/.

[85] “Submarines: Multiplying Mine Finding Robots,” *Strategic Page*, October 16, 2019, https://www.strategypage.com/htmw/htsub/articles/20191016.aspx.

[86] Kyle Kiyokami, “The U.S. Navy’s Mine-Hunting Drone Is Ready to Go,” *Popular Mechanics*, August 27, 2019, https://www.popularmechanics.com/military/navy-ships/a28834032/knifefish-mine-drone/.

[87] Sam LaGrone, “Navy Issues Draft Request for Proposal for Large Unmanned Surface Vehicle,” *USNI News*, August 14, 2019, https://news.usni.org/2019/08/14/navy-issues-draft-request-for-proposal-for-large-unmanned-surface-vehicle#more-68836.

[88] Ronald O’Rourke, “Navy Large Unmanned Surface and Undersea Vehicles: Background and Issues for Congress,” *Congressional Research Service*, September 18, 2019, https://fas.org/sgp/crs/weapons/R45757.pdf.

[89] Jon Rosamond, “U.K. Developing its Own Extra Large UUV for Royal Navy,” *USNI News*, April

另一個在無人作戰艦艇上具備優秀技術，並扮演重要角色的則是俄羅斯。首先值得注意的是「波賽頓」，這種 UUV 最早出現於 2015 年，過往也被稱為「Status-6」及「卡尼翁」（Kanyon），俄羅斯總統普欽在 2019 年 2 月初宣稱已成功研發此型 UUV，並宣稱將於 2019 年夏季開始工廠測試。「波賽頓」可視為一種核子動力的核子魚雷，能跨洲際投射兩百萬噸級的核彈頭。[90]其次則是「大鍵琴-2」（Klavesin-2），這種 UUV 外觀近似潛艇，重約 4 噸並可潛至 6,000 公尺深，「大鍵琴-2」可以攜帶各式感測器、搜索並收集如武器碎片等各種物體，並由特殊改裝的潛艦作為母船進行運用，施放後可操作距離達 50 公里。「大鍵琴-2」在 2018 年時已在克里米亞一帶進行海試，由於海試時已獲得俄軍的正式編號「2R52」，顯示「大鍵琴-2」將可能在海試後進入服役。[91]

此外，中國在 2019 年 10 月 1 日的閱兵中，同樣展出了一種稱為「HSU001」的新式 UUV。相較於美國與俄國的類似系統，HSU001 相對較小，其尺寸與外觀顯示可能不會用於載運大型武器裝備或水雷進行作戰行動，而仍以情監偵等工作為主。[92]儘管中國目前正在進行多種無人船艦，並且可能包含將在下個十年進入服役的超大型 UUV，以及水下基地，[93]但目前推出的系統顯示其可靠性可能仍存在問題，技術上仍需追趕美國與俄羅斯的發展。[94]

陸、未來武器與高科技載台發展趨勢

目前下一代武器載台的發展仍在概念研發階段，目前正處於世代交替階段，，本節先前提過的武器系統，包括雷射、電磁武器、無人機、極音速武器等，未來將成為未來載台的標準或選擇配備，以強化其原有性能或作戰能力，但未來作戰環境也可能賦予新武器載台與現在不同的任務。

一、歐洲六代戰機的跨國整合

歐洲國家正在進行六代戰機概念的驗證及整合。英國貝宜航太首先在 2018 年推出「暴風」（Tempest）戰機全尺寸模型，希望在 2035 年達到初始戰力（initial

17, 2019, https://news.usni.org/2019/04/17/u-k-developing-its-own-xluuv-for-royal-navy.

[90] Matteo Natalucci, “Russia completes testing of ‘Poseidon’ thermonuclear torpedo,” *Jane’s 360*, February 20, 2019, https://www.janes.com/article/86583/russia-completes-testing-of-poseidon-thermonuclear-torpedo.

[91] “Russia Started Sea Trials of Klavesin-2 UUV in Crimea,” *Naval Technology*, May 18, 2018, https://www.navyrecognition.com/index.php/focus-analysis/naval-technology/6234-russia-started-sea-trials-of-klavesin-2-uuv-in-crimea.html.

[92] Ellen Ioanes, “China just unveiled an underwater drone that could one day even the odds against the US and its top allies,” *Business Insider*, October 2, 2019, https://www.businessinsider.com/chinas-underwater-drone-allies-in-pacific-2019-10/

[93] JR Wilson, “Unmanned submarines seen as key to dominating the world’s oceans,” *Military & Aerospace Electronics*, October 15, 2019, https://www.militaryaerospace.com/unmanned/article/14068665/unmanned-underwater-vehicles-uuv-artificial-intelligence.

[94] 歐錫富，〈中國發展水下無人潛航器〉，《國防安全週報》第 73 期，2019 年 11 月 15 日，頁 1-6。

operating capability, IOC），2040 年取代歐洲戰鬥機（Eurofighter），並供應歐洲及國際外銷市場。暴風戰機是一種大型單座雙發動機戰機，採用兩具傾斜式大型垂直尾翼，類似 F-22，可增加其可操縱性，顯示其追求匿蹤能力要更佳，更大的機體也暗示其較佳的航程，以及武器酬載能力。勞斯萊斯的自適應循環渦輪扇發動機的風扇段，將由輕質複合材料製造，具優異的熱管理能力及數位化控制，同時也可透過傳動軸產生大量電力，未來將可驅動雷射武器。

暴風戰機較像是歐洲版的五代半戰機。其先進之處並非外型，而是整體航電及武器設計，以及運用先進生產及後勤技術。「暴風」戰機將運用模組化彈艙，自動化地面支持系統、數位化生產程序及自動化機器人，機體上的各種先進主被動式感測器，可以模組化進行重新設計及安排、以及新一代飛控系統與平衡的高生存性設計、分散式多重光譜感測器下一代反制措施。未來暴風戰機可能會採用極音速武器，並與無人機搭配作戰，這是目前下一代戰機的設計趨勢。座艙最大亮點則是以擴增實境概念取代傳統座艙，飛行員可以看到他自己或他人的座艙，同時可以隨意重新配置，並輕易將資料鏈傳給其他飛機。[95]

「暴風」戰機設計的挑戰，是面對未知的需求時，需有極佳適應性能力。因此在早期設計過程最重要的是先發展任務系統架構，而不是精確的作戰需求，包括概念設計、需要何種技術及如何取得，其關鍵可能是如何提出一種適應性強，能滿足客戶不同需求的戰機。[96]

目前已有數家歐洲集團加入「暴風」戰機團隊，包括義大利李奧納多集團（Leonardo）在 2019 年 9 月 14-17 日的「國際防務與安全裝備展」（Defence & Security Equipment International, DSEI 2019）中宣布加入「暴風」戰機研發陣營，瑞典紳寶（SAAB）集團、歐陸的空中巴士（Airbus）集團、美國洛克希德馬丁也都加入團隊。紳寶將提供發展「獅鷲」E （Gripen E）的經驗，不過瑞典出口法規嚴格，將是一項挑戰。[97]

---

[95] Sebastien Roblin, “Why Britain's Tempest Stealth Fighter May Out-Class the F-35,” *National Interest*, October 31, 2019, https://nationalinterest.org/blog/buzz/why-britains-tempest-stealth-fighter-may-out-class-f-35-92101.

[96] Stew Magnuson, “NEWS FROM DSEI: RAF Puts Development of Tempest Next-Gen Fighter into ‘Hyperdrive,’” *National Defense Magazine*, September 12, 2019, https://www.nationaldefensemagazine.org/articles/2019/9/12/raf-puts-development-of-tempest-next-gen-fighter-into-hyperdrive.

[97] Andrew Chuter, “Sweden to join British ‘Tempest’ next-gen fighter push,” *Defense News*, July 7, 2019, https://www.defensenews.com/global/europe/2019/07/07/sweden-to-join-british-tempest-next-gen-fighter-push.

圖 6-5、英國貝宜航太的「暴風」戰機概念

資料來源：舒孝煌攝影。

法國也與德國及西班牙結盟，在 2019 年 6 月 17 日巴黎航展期間推出六代戰機全尺寸概念，這被稱為「未來空中戰鬥系統」（Future Combat Air System, FCAS），主合約商是法國達梭航空工業公司（Dassault），空中巴士（Airbus）軍用機部門負責發航電系統。FCAS 外型扁平、匿蹤性更佳外，沒有公布太多發動機、航電、結構設計等細節，似是因為對至 2040 年的空中威脅尚無具體看法。

二、美國的六代戰機計畫

美國海空軍在過去數年曾提出未來戰機計畫，美國空軍稱為「下一代空防系統」（Next Generation Air Dominance, NGAD），美國海軍稱為 F/A-XX，不過因兩軍種要求不同，對未來空戰或空中威脅看法尚未整合，但已展開相關技術發展，例如空載雷射武器、空射極超音速飛彈、新一代發動機等。美國空軍《空優 2030 飛行計畫》（*Air Superiority 2030 Flight Plan*），指出未來需要一種「穿透性制空」（Penetrating Counter-Air, PCA）平台，可深入敵境進行致命或非致命打擊，機體需具備多頻譜匿蹤能力，但海軍 F/A-XX 計畫則希望能讓航艦部署在離岸 1,000 至 1,200 浬距離，以遠離敵人飛彈攻擊。六代戰機也應具備系統化或系統家族概念，以便快速升級，因應未來數十年間空中威脅的可能變化。[98]

美國空軍最近對其機隊更新計畫有急迫感。其大部分戰機仍是 1980 年代設計的，其結構損耗至 2020 年將達極限，美國空軍原本規劃的五代戰機中，F-22 僅採購 187 架，F-35 生產仍然遲緩，迫使空軍不得不為 4 代戰機延壽，甚至增購 F-15EX 以為補充。

為快速提升機隊，美國空軍可能大幅改變下一代戰機採購戰略，將要求航空工業在 5 年內設計、發展及生產新戰機，可能延用過去「世紀系列」（Century Series）經驗，不是研發最先進、最昂貴的戰機，而是整合現有科技、採購較少

[98] Jon Harper, "What to Expect from Sixth-Gen Aircraft," *National Defense*, September 16, 2019, https://www.nationaldefensemagazine.org/articles/2019/9/16/what-to-expect-from-sixth-gen-aircraft.

數量，數年後根據新科技再發展下一種戰機，並結合先進的 3D 設計、開放架構、數位工程等技術。[99]

未來六代戰機不會取代五代戰機，而是併肩作戰，採用目前發展中的先進技術，如雷射、無人僚機、人工智慧技術、網路化作戰、智慧化蒙皮、新一代匿蹤技術，如飛機熱能管理，透過感測飛機在飛行中的熱量分佈，重新加熱或冷卻機體表面，使飛機完合融入周邊的大氣環境。另外可能包括極音速飛行等，並引進系統化作戰概念。[100]然而，這些科技都還在發展階段，要能整合在所謂的「第六代」戰機上，目前可能為時尚早。

三、未來水面艦設計趨勢

美國海軍正思考未來水面艦（Future Surface Combatant）發展，除了未來大型水面艦（Large Surface Combatant, LSC）、2021 年開始建造的新巡防艦（FFG(X)）外，尚包括中型及大型無人水面艦，設計理念都著重適應性，將取代現有作戰平台。未來艦艇設計趨勢包括：

（一）匿蹤化

為減少被敵方雷達偵蒐機會，水面艦艇採用匿蹤外型是必然趨勢，然而受限於艦上裝備複雜，以及在設計時需與艦艇水線以上結構達成妥協，包括武器、艦橋、排煙及進氣設備、感測系統、直升庫等結構，難以達成全面且完美的匿蹤要求。不過新一代的匿蹤設計已逐漸成熟，美國的濱海作戰艦與朱瓦特級（Zumwalt）驅逐艦、我國的沱江級巡邏艦、挪威的巡防艦，都採用較革命性的匿蹤外型設計，將使海軍艦艇更進一步減少其被敵雷達發現的可能。

（二）多功能化與彈性化

武器系統彈性化是近年趨勢，使艦上武器可以應付突發狀況及不同作戰環境挑戰，例如標準 3 型飛彈可以攻擊水面目標，戰斧飛彈可用以攻擊水面移動目標，魚叉飛彈則可攻擊陸地目標，而近迫武器則可用以攻擊水面目標或 UAV 等新興的不對稱威脅。艦上感測系統如雷達、光電系統等，則需能發現小型的威脅。另外，艦上可用以部署 UAV 或 USV 等，以增加艦艇的作戰彈性，有時直升機庫甚至可部署攻擊直升機（如 AH-1Z），執行遠距打擊任務。

（三）電力化驅動與高能量武器

因應船艦感測系統逐漸改用電子掃描電達，電力消耗漸漸增加，船艦主機在電力輸出上較過去大幅增加。在電磁軌道砲及固態雷射武器等先進武器逐漸實用化後，船艦的武器系統未來可能有革命性轉變，這些武器會消耗大量電能，因此主機的電力輸出要較過去增加 2 至 3 倍以上。另外驅動方式也由主機經變速箱與大軸直接驅動俥葉，轉變為發電後由電力驅動馬達，馬達再直接傳動俥葉，中間

[99] Valerie Insinna, “The US Air Force’s radical plan for a future fighter could field a jet in 5 years,” *Defense News*, September 9, 2019, https://www.defensenews.com/digital-show-dailies/2019/09/16/the-us-air-forces-radical-plan-for-a-future-fighter-could-field-a-jet-in-5-years.

[100] Kris Osborn, “U.S. Air Force is Prototyping a Replacement for the Stealth F-35,” *National Interest*, September 23, 2019, https://nationalinterest.org/blog/buzz/us-air-force-prototyping-replacement-stealth-f-35-82661.

可減少機械的噪音與動力的消耗，目前新式艦艇已逐漸採用電力馬達驅動，使艦艇動力產生大幅度轉變。

電力驅動與艦上武器系統的革新息息相關。美國海軍電力船舶辦公室（Electric Ships Office, ESO）負責發展海軍的動力及能源系統，主要聚焦在船艦的動力系統與導能武器，或艦上其他需要高能量的任務系統及平台整合，並改善這些組件及次系統的能源效率。由於先進雷達、偵測系統及電磁與導能武器的需要，現代船艦艦上需要的電力及脈衝功率不斷增加，同時仍得維持其他用電系統的穩定，這是設計新一代船艦的挑戰。電力船舶辦公室與海軍研發部門及其他工業界夥伴合作，導入創新科技，引進高效能的動力及能源管理，實現海軍分散式殺傷（distributed lethality）的作戰理念。

另外，為應付殺傷及非殺傷的不對稱威脅，需要新科技解決方案。目前海軍有數種高能量武器及感測器技術，將在未來數年導入服役，其中包括固態雷射，用以取代現有的近迫武器系統（Close-In Weapon System, CIWS）、電磁軌道砲，可發射長程精確武器，增加打擊射程，減少打擊時間、先進感測器，將所有材料、結構、製造技術與感測器、匿蹤等完全加以整合。這些新技術的運用都需要船艦輸出更大的動力，為以可能的最低成本符合作戰需要，由傳統的任務系統及艦艇系統分離，到整合式的電力及能源架構，這種基本的典範轉移有其必要。[101]

ESO 將採用成熟及適當的架構、系統和組件，滿足現有與未來船艦的新興任務的負荷要求，這包括電源轉換模組、發電模組、儲能模組、以及電力控制模組，未來新式的船艦將會運用整合式動力系統，稱為整合動力及能源系統（Integrated Power & Energy System, IPES），其中包括能源庫（Energy Magazine），為模組化、可擴展的動力及能源系統，支援多種系統使用，首套原型已在 2018 年進行測試。IPES 則結合多種多用途分散式能源存儲、先進的能源控制及管理，提供可擴展架構，以支援不同級別船艦的運用。這套系統結合朱瓦特級驅逐艦、馬金島號兩棲突擊艦（USS Makin Island, LHD 8）、英國 45 型驅逐艦等的經驗，IPES 可簡化讓能源穩定共享及管理，可併聯不同額定功率的發電機，毋須保持發電機同步。

（四）網路化與分散式部署

美國海軍發展網路化作戰（Network-Centric Warfare, NCW）多年，如今相關構想更進一步，採「分散式致命」，即艦艇間以網路化連結，網路化部署，艦艇與艦艇間以資料鏈交換訊息，彼此部署距離可能遠達數十浬或近百浬，以 E-2 預警機、直升機、UAV 或衛星交換訊息，減少被敵人攻擊機會，並可增加敵方部署的風險。

[101] "Electric Ships Office," Naval Sea Systems Command, December 2016, https://www.navsea.navy.mil/Home/Team-Ships/PEO-Ships/Electric-Ships-Office/.

柒、小結

藉由前面幾節可以逐漸勾勒出一個未來的戰場圖像。有人與無人的系統搭配作戰將是未來可預見的戰場景象，陸海空的無人僚機將可大幅延伸現有作戰平台的交戰距離、戰場覺知、生存能力以及火力投射能力，而極音速載具與長程打擊武器的大幅增加，則對現有飛彈防禦體系帶來極大衝擊，將使得新世代飛彈防禦系統需求大增。事實上，前一章節所提到的彈藥技術進步，將使得未來載台火力投射的能力更加強化；在這種情況下，包含雷射在內的各種防禦武器，將是未來大型主戰水面艦在對抗逐漸強化的「矛」時，必須採取的手段。

伴隨著大國衝突需求而呈現多領域化的未來戰場，可預見將使兵科、甚至兵種間的藩籬逐漸打破，同時通訊與觀測技術的發展，讓部隊上從指揮官、下到單兵，在未來都可獲得一個完整、共通的戰場圖像，這將使得不同兵種及兵科的整合、甚至將聯兵單位分散以小單位作戰逐漸成為可能。這樣的作戰方式如搭配上複雜地形的運用，對無法與中共進行軍備競賽的台灣來說，無疑是防衛作戰上的重大利基。

然而技術上的限制仍有待解決，就無人自主系統而言，人工智慧以及自主操作系統的發展仍有其限制，特別是在需要面對複雜地面環境的 UGV 而言更是如此，UUV 則將面對通訊及傳輸的問題，特別是水下通訊系統目前仍彼此不相容，換言之不同生產商的產品將可能無法互相通訊，此外，無人系統儘管能省去人命損失的顧慮，然而要真正達到代替人類進行「骯髒、枯燥與危險」環境的工作甚至作戰任務時，仍需要有足夠的數量及可耗損性，換言之其造價也仍需下降，以符合作戰需求。導能武器的功率也仍有待加強，目前的系統雖能破壞感測器或是擊毀無人機，然而面對飛彈等目標時卻仍力有未逮，有待技術上的進一步突破，而矛與盾的競爭也將決定在未來數十年內，傳統的超級航艦一類的大型載台是否能在未來戰場生存的關鍵。

（責任校對：杜貞儀、王綉雯、郭恒孝）

第七章 台灣國防自主前瞻

洪瑞閔*

壹、前言

東亞區域情勢日趨緊張，不僅長期存在的韓半島問題與兩岸關係對立升溫，區域內的多方行為者亦在包括東海、南海等地區，為了相關島礁的主權歸屬問題劍拔弩張。隨之而來的是各國國防開支的不斷增加與追求迅速的軍事現代化，而這反過來又推升情勢。這些特徵使得東亞成為具有爆發軍事衝突的潛在地區之一。

對我國來說，中共自 1949 年以來便是最大的威脅。近二年來，中共戰機多次繞台甚至飛越海峽中線；以遼寧號為首的海軍艦隊也多次繞行台灣本島。這些軍事行動使得台海局勢更加緊繃。面對此一迫切威脅，發展國防自主成為我國的重點策略之一，「國機國造」與「國艦國造」等國防自主項目正如火如荼的展開。

本章將論述國防自主的概念與其對我國的意涵與展望，並分成五個部分進行分析。第一節闡述我國國防自主迄今的發展與國防產業所具備之能力。第二節將從安全與產業等兩大面向探討國防自主對我國之意涵。第三節則綜整其他與台灣背景相似國家的國防自主發展趨勢。第四節指出我國國防自主所將遭遇到的挑戰與機會。

貳、我國國防自主發展趨勢

《中華民國 106 年國防報告書》率先提出「防衛固守，重層嚇阻」作為國家軍事戰略目標。其目的在於「發揮重層聯合戰力，防衛國土安全，嚇阻敵不敢輕啟戰端」，[1]擁有堅強的國防產業能力被視為達成此一目標的必要條件，國防自主成為中華民國國防政策的主軸之一。據此，近年來我國在制度與實務面向上皆有長足的發展。

在制度面向上，2000 年所通過的《國防法》第 22 條揭示結合民間力量發展國防科技工業，獲得武器裝備以自製為優先，對外採購時必須促進技術轉移的國防自主原則。在 2019 年更通過《國防產業發展條例》作為國防產業發展的基礎，希望進一步強化自製能力與減少對外依賴。

在實務面向上，「國機國造」與「國艦國造」已成為台灣國防自主推動的兩大主要計畫。在「國機國造」方面，我國空軍在 2017 年 2 月與漢翔航空工業公司（以下簡稱漢翔公司）與中山科學研究院（以下簡稱中科院）簽署新式高級教

* 洪瑞閔，國防資源與產業研究所博士後研究，負責本章。

1 中華民國 106 年國防報告書編纂委員會，《中華民國 106 年國防報告書》（台北市：國防部，民國 106 年 12 月），頁 55-57。

練機的合約，原型機已於 2019 年 9 月出廠進行地面測試並命名為「勇鷹號」，預計在 2020 年 6 月進行首次試飛，並在 2026 年達成 66 架新式高教機的交機目標。在「國艦國造」方面，2015 年至 2019 年間中華民國海軍分別啟動「潛艦國造」、「兩棲船塢運輸艦」、「高效能艦艇量產」、「快速布雷艇」、「新型救難艦」、「微型飛彈突擊艇」、「新一代飛彈巡防艦」等 7 項造艦計畫。[2]其中又以「潛艦國造」計畫最受注目，中華民國海軍於 2017 年 3 月和中科院及台灣國際造船公司（以下簡稱台船公司）簽署備忘錄，目標建造 8 艘柴電動力潛艦，首艘潛艦預計在 2020 年底開始建造並在 2026 年服役。

在國防產業能力方面，台灣已具備一定程度的國防自主能力。在空軍部分，中科院與漢翔公司是台灣航太產業的龍頭，過去台灣已有「中興號」教練機、「中正號」戰機、「經國號」戰機等多款教練機與戰機的製造經驗。就「勇鷹號」高級教練機而言，自製率約達 55%（見表 7-1），儘管在模擬系統與機體結構部分已具備一定程度的自製能力，但在航電系統與發動機部分仍相當仰賴國外技術的支持。

表 7-1、「勇鷹號」高級教練機組件自製能力情況

技術領域	自製能力
航電系統	大多依賴國外技術
機體結構	自製比例高（起落架除外）
發動機	F124 發動機具 50%產製能力
模擬系統	具備完整產製能力

資料來源：洪瑞閔整理自公開資料。

在海軍部分，中科院與台船公司在台灣國防造艦產業中扮演執牛耳的角色。台灣曾有成功級巡防艦、錦江級近岸巡邏艦、沱江級巡邏艦、磐石號油彈補給艦等各式艦隻的建造經驗，但未有潛艦的建造經驗，因此潛艦國造計畫高度依賴國外技術支援（見下頁表 7-2）。儘管有能力製造螺旋槳與通訊系統等重要組件，但在潛望鏡、聲納與引擎等紅區裝備仍然仰賴歐美大廠的技術支援。

綜上言之，我們可將台灣歸類為「第二級武器生產國家」（second-tier producer-states）[3]。從過去的製造經驗來看，台灣的確具備了一定程度的軍備自製能力，但在重要的先進武器生產上，其尚缺少諸多關鍵性技術的能力，需要有歐美國防大廠的支持，方可進行研發與產製。

[2] 中華民國 108 年國防報告書編纂委員會，《中華民國 108 年國防報告書》（台北市：國防部，民國 108 年 9 月），頁 91-92。

[3] Richard A. Bitzinger, Defense Industries in Asia and the Technonationalist Impulse, *Contemporary Security Policy*, Vol.36, No.3, Summer 2015, p.455.

表 7-2、「潛艦國造」計畫組件自製能力情況

技術領域	自製能力
螺旋槳	高度產製能力
通訊系統	
潛望鏡	主要仰賴外援
聲納	
引擎	

資料來源：洪瑞閔整理自公開資料。

參、國防自主的意義

針對「國防自主」政策，我們可從安全及產業兩層面論述其對台灣的意義。

一、安全層面

（一）戰略建構的基石

近年來有關台灣的國防戰略選擇出現「正規戰略」與「豪豬戰略」（porcupine strategy）兩種邏輯的辯論。正規派的支持者認為，傳統方式從長期來看依舊是建構台灣軍事力量的最佳選擇，台北必須要做好與北京一戰的萬全準備。北京所可能採取的各項軍事行動都必須要被考量在內。在中共尚無能力完全壓制台灣海空戰力的情況下，包括戰機與潛艦在內的各式先進裝備是武器獲得時的優先選擇，[4]同時也是最有效的應對方式。此外，配置精良軍備可使人民具體地感受到國防實力的增強，有助於政府爭取人民的支持與認同。然而，豪豬戰略的支持者反駁此說法。他們主張，考量到台灣有限的國防預算與中共急速的軍事現代化，而應該要專注在包括無人機與水雷等輕巧、高機動性與成本低廉的裝備，透過這些方式以不對稱作戰的方式達到強化自身防衛能力並嚇阻中共的侵略企圖。[5]

儘管戰略選擇的爭辯尚未有定論，但「國防自主」概念無疑已經躍上舞台，將扮演核心角色。無論未來選擇何種戰略，均有賴各項自製研發計畫所獲得關鍵技術與知識做基礎，方能有效建構。

（二）降低對外依賴的脆弱性

毫無疑問地，美國對於中華民國的安全維護扮演了相當重要的角色。在韓戰之後，美軍派出第七艦隊巡邏台灣海峽，使得台海兩岸情勢得以趨向穩定，1954 年的《中美共同防禦條約》（*Sino-American Mutual Defense Treaty*）將雙方關係進一步深化，儘管該條約隨著華盛頓與北京在 1979 年建立外交關係而中止，但台

[4] Michael Mazza, “Assessing the utility of new fighter aircraft for Taiwan’s defense needs,” *Global Taiwan Institute*, March 13, 2019, http://www.aei.org/publication/assessing-the-utility-of-new-fighter-aircraft-for-taiwans-defense-needs/.

[5] Tanner Greer, “Taiwan’s Defense Strategy Doesn’t Make Military Sense,” Foreign Affairs, September 17, 2019, https://www.foreignaffairs.com/articles/taiwan/2019-09-17/taiwans-defense-strategy-doesnt-make-military-sense.

美雙方的緊密關係，依舊以同年美國國會所通過的《台灣關係法》（*Taiwan Relations Act*）的形式繼續維持。

然而，近年來的國際情勢發展使得華盛頓對台北的承諾備受考驗。一方面，美國在 2018 年起對中共發起貿易戰希望能夠藉此維護其在經濟與貿易領域的利益，但在軍事與安全領域中，隨著中共近年來的軍事能力大幅度提升，美中雙方的軍事實力對比已經拉近。倘若未來發生直接軍事衝突，儘管美國依舊佔有相當優勢，但恐將付出相對高昂的代價才能取得勝利。另一方面，孤立主義傳統似乎又成為川普政府外交政策的方向。除了要求北大西洋公約組織（North Atlantic Treaty Organization, NATO）的盟友擔負起更多預算義務以外，阿富汗與敘利亞的撤軍行動都是華盛頓不願再扮演「世界警察」角色的有力證據之一。

在現實主義主導的國際關係中，國家利益始終是一國外交政策的核心考量。對於台灣來說，隨時都可擁有美國的援助是過於天真的想法。因此，在沒有外援的情況下，面對來自中共的威脅，推動「國防自主」是必要手段，唯有「國防自主」所帶來的國防能力能夠作為有力依靠。

（三）提升戰略的自主性

在國際政治中，軍售不只代表著貿易的利益，也是政治與外交的工具。透過軍售所包含的人員訓練、技術轉移與後勤維護等協定，軍備出售國可以藉由此強化其與軍備購買國的雙邊關係。例如，法國便透過出售澳洲海軍 12 艘「短鰭梭魚級」（*Shortfin Barracuda class*）柴電潛艦增強其與印太地區國家的夥伴關係。就台灣而言，美國一直是其最重要的對外武器獲得來源，自卡特（Jimmy Carter）政府與中華民國斷交以來，台灣已先後購入包括 F-16 戰機、派里級（*Perry Class*）巡防艦與 M1A2 主力戰車等各式武器系統。2019 年 8 月 30 日由時任美國國安顧問波頓（John Bolton）所解密，1982 年的雷根（Ronald Reagan）政府備忘錄中確認美國對台軍售的減少將取決於中共是否願意持續信守以和平方式處理兩岸問題的承諾。[6]除了表明出華盛頓對台北長久以來的安全承諾外，透過一系列的軍售案，美台也建立起相當深厚與全面的夥伴關係。

然而，從另一方面來說，軍售也能夠作為強權擴張其權力的工具，用以影響軍備購買國的政策。如美國可使用包括《國際武器貿易條例》（*International Traffic in Arms Regulations,* ITAR）、《1976 年武器出口管理法》（*Arms Export Control Act of 1976,* AECA）與《以制裁反制美國對手法案》（*Countering America's Adversaries Through Sanctions Act,* CAATSA）等法規作為施壓與制裁軍備購買國的方式，迫使後者在特定議題上做出讓步或改變政策。

是以，「國防自主」形同國家主權的象徵。儘管完全的「國防自主」現今除了美國以外沒有國家能夠辦到，然而挑選重要的核心能力自行研發，達成一定的自主性仍是必要的。對國外軍備的高度依賴將使國家主權暴露在危險當中，使其他國家有機會干預其重大政策的決策過程。對台灣而言，「國防自主」可說是一

[6] 侯姿瑩，〈八一七公報不只六項保證 雷根備忘錄解密對台軍售關鍵〉，《中央社》，2019 年 9 月 18 日，https://www.cna.com.tw/news/firstnews/201909180032.aspx。

種避險的必要方式，透過各項自製武器研發計畫提升己身能力，自行生產必要軍事裝備以達成戰略目標而不被其他強權所阻礙，方能為台灣在國際事務中帶來更大的行動自由與斡旋空間。

二、產業層面

（一）就業機會的創造

各項軍備自製計畫可為一國帶來許多就業機會。政府與航太、電子、通訊等多個部門主要承包商簽約，這些主要承包商再將不同的細項合約分包至中小型包商手中，形成一個從設計、建造到維護等不同階段且需要大量人力資源投入的產業鏈。一項軍備自製計畫可以創造出直接、間接與衍生等 3 種層次的就業機會。直接就業機會包括直接涉及合約的主要承包商所帶來的工作機會，間接就業機會包括與主要承包商簽約的中下游轉包商所帶來的工作機會，衍生就業機會則包括為了滿足上述兩種就業機會員工日常生活所需所帶來的工作機會。

就我國的主要軍備國造計畫而言，「勇鷹號」高級教練機將可為中科院創造 500 到 1,000 個工程師職位，同時為其他國內製造商帶來約 400 個工程師職位。[7]整個國艦國造計畫將可在 2017-2025 年間每年創造出 2,645 到 9,340 個工作機會，蔡英文總統則指出至少可創造 8,000 個以上高品質工作機會。[8]

（二）經濟加乘效應

軍備國造計畫可藉由加乘效應帶動國內經濟發展，我們可以將這些計畫視為政府公共投資的一部份，在國防領域的投資支出能夠在後續的經濟活動中帶來超過原先投資額度的經濟效益。如瑞典的「獅鷲」戰機（JAS-39 Gripen）的經濟加乘效應為 4.54，意即該計畫每投入 1 瑞典克朗可帶來 4.54 瑞典克朗的收益。[9]法國彈道飛彈核潛艦計畫的經濟加乘效應為 3.3。[10]

在台灣的主要軍備國造計畫中，「勇鷹號」高級教練機投入的預算為 686 億新台幣，預期可創造的產值為 1,500 億新台幣。[11]因此其所帶來的經濟加乘效應為 2.19。國艦國造的經濟加乘效應則為 2.5，預計在 2016 至 2019 年間投入 171.8 億新台幣，並可帶來約 428.7 億元的經濟效益。[12]

（三）外溢效應

---

[7] 游玉堂，〈國機國造之機會與挑戰〉，國防部資源司科技處，2015 年 7 月 15 日，https://www.mnd.gov.tw/NewUpload/201608/%E5%9C%8B%E6%A9%9F%E5%9C%8B%E9%80%A0%E4%B9%8B%E6%A9%9F%E6%9C%83%E8%88%87%E6%8C%91%E6%88%B0.PDF。

[8] 清華大學人文社會學院，《國艦國造的經濟與就業效益政策說帖》，2017 年 12 月，頁 11；廖禹揚，〈總統：國艦國造帶動國防產業 創 8000 工作機會〉，《中央社》，2019 年 2 月 25 日，https://www.cna.com.tw/news/firstnews/201902250196.aspx。

[9] G. Eliasson, *Public Procurement as Innovation Policy - The Case of the Swedish Multipurpose Combat Aircraft Gripen*, Paper to be presented to the 15th International Joseph A. Schumpeter Conference, Jena, Germany, July 27- 30th, 2014, pp.2-3.

[10] Direction de la communication, *Rapport financier 2017*, Naval Group, 2018, p.95.

[11] 中華民國 108 年國防報告書編纂委員會，《中華民國 108 年國防報告書》（台北市：國防部，民國 108 年 9 月），頁 91。

[12] 中華民國 108 年國防報告書編纂委員會，《中華民國 108 年國防報告書》（台北市：國防部，民國 108 年 9 月），頁 92。

「國防自主」的推動不只能夠保存與提升國防產業的能力，也能帶動國家其他經濟部門的發展。換言之，軍備國造計畫所學習與取得的關鍵科技能夠從軍用轉移至民用領域，為航太、電子與資訊等領域帶來新的應用與發展。例如，「法國原子能和替代能源委員會」（Le Commissariat à l'énergie atomique et aux énergies alternatives, CEA）下轄的「電子暨資訊技術實驗室」（Laboratoire d'electronique et de technologie de l'information, Leti）於 1950 年代中期於格勒諾伯（Grenoble）開始進行有關軍用原子能的研究。在歷經了 60 餘年的發展之後，以 Leti、格勒諾伯大學與相關政府研究單位為核心，格勒諾伯成為法國與歐洲奈米科技與新能源研究的重鎮，由 Leti 出身的研究人員與技術為核心誕生了超過 60 家的新創企業，其中又以由 Leti 的兩位前研究人員所創立的「梭意科技」（Soitec）最具代表性，已成為世界重要的半導體創新材料公司，在法國本土擁有超過 1,000 名員工。[13]

「國防自主」的外溢效應是我國國防部的政策重點。國防科技移轉民間、發展軍民通用科技與資源釋商是政策的三大主軸[14]。過去，有和成衛浴在中科院的支援之下，接下雲豹 8 輪裝甲車抗彈板生產訂單的成功經驗。[15]「勇鷹號」高級教練機與「國艦國造」的外溢效應如表 7-3 與表 7-4（見下頁）所示，均具備相當的發展潛力，可進一步支持國防產業的發展並攤平軍備的研發成本。

表 7-3、「勇鷹號」高級教練機的可能外溢效應領域

軍用技術	民用領域
設計	飛機設計能力
後勤	維修能力
模擬	軌道與娛樂產業
航電系統	通訊與導航

資料來源：洪瑞閔整理自公開資料。

[13] Laurent Gallien, "Cinquante ans pour le CEA-Leti de Grenoble, laboratoire d'innovation," *France Bleu*, Febuary 3, 2017, https://www.francebleu.fr/infos/economie-social/50-ans-pour-le-cea-leti-de-grenoble-laboratoire-d-innovation-1486145270.

[14] 中華民國 106 年國防報告書編纂委員會，《中華民國 106 年國防報告書》（台北市：國防部，民國 106 年 12 月），頁 102-104。

[15] 游凱翔，〈做馬桶也做防彈 台灣企業展現國防自主能量〉，《中央社》，2018 年 7 月 1 日，https://www.cna.com.tw/news/aipl/201807010098.aspx。

表 7-4、「國艦國造」項目的可能外溢效應領域

軍用技術	民用領域
聲納與雷達	醫學超音波檢查
慣性導航系統	大地測量、海洋探測
設計與建造程序	系統工程
結構	材料科學

資料來源：洪瑞閔整理自公開資料。

肆、重要國家的發展經驗

包括美國、英國、法國、德國、義大利與俄羅斯在內的「第一級武器生產國家」（first-tier producer-states）都擁有高技術水平的國防能力，能夠自行或在彼此合作的情況下建造出先進的武器。不過，國防產業能力的提升並非一蹴可幾，而需相當時間的資源投入與政策配合。事實上，此些金字塔頂端國家的經驗對於台灣來說是難以複製的。若要借鏡他國的發展經驗，「第二級武器生產國家」相較於前述先進國家的發展經驗更具參考價值，這些國家擁有規模較小與技術水平較低的「國防產業基礎」(defense industrial base)，出自於不同的動機希望能夠提升國防產業能力。本節將綜整這些中小型國家的發展經驗，指出「第二級武器生產國家」國防自主的發展趨勢。

一、利基生產的發展模式

對於中小型國家來說，它們多數選擇利基生產（niche production）的武器生產模式，強調經濟面向的重要性並尋求在國際軍備出口市場中佔有一席之地，瑞典的「獅鷲」戰機與芬蘭的 AMV 裝甲車可作為代表，具有如下三種特徵：

（一）集中化

在新型武器開發成本日益高漲的情況下，預算與能力皆有限的中小型國家將資源集中在特定武器系統的發展，「獅鷲」戰機與 AMV 裝甲車便分別是瑞典與芬蘭兩國在國際軍售市場與他國產品競爭的主力。

（二）低成本

這些軍備以模組化、國際合作開發、零組件外包等方式盡可能地降低成本以具備價格上的競爭優勢。如瑞典「獅鷲」戰機每架成本僅約 5,500 萬美元，在運作成本上也以每飛行小時平均花費 4,700 美元居各主力戰機之末。此外，芬蘭的 AMV 裝甲車採用輪型而非履帶裝甲車的設計，不但與民用技術相近，在研發與維護成本上也較履帶裝甲車來得便宜，每輛 220 萬美元的價格相當具有國際市場上的競爭力。

（三）差異化

這些國家不追求開發出能夠滿足各種作戰需求的複雜產品，而是看準特定的市場與戰略需求所發展出的特殊產品，儘管這些軍備性能不如「第一級武器生產

國家」所生產的軍備，但出自於不同的戰略與經濟考量，其足以脫穎而出獲得許多軍備購買國家的青睞。如「獅鷲」戰機強調的是保衛國土不受侵犯而非參與高強度的境外作戰，AMV 裝甲車則反應冷戰後歐洲主流軍事需求，著重高機動性、多功能性與海外維和行動的人員保護。這些專門的市場定位使其在與「第一級武器生產國家」的產品競爭時，還能夠保有相當程度的競爭力。

二、重視在地國防企業參與

在無法自行研發製造，必須向外進口的情況下，在地國防企業的參與成為中小型國家在商議合約時重視的條件，主要希望藉由軍購尋求技術轉移的機會，使本國國防產業學習先進國家的關鍵技術並尋求加入全球產業鏈的機會，進而提升自身國防產業能力，土耳其與印度即為代表性之案例：

（一）土耳其

土耳其自 2002 年起便加入美國「F-35 聯合攻擊戰鬥機」（F-35 Joint Strike Fighter）計畫。[16]安卡拉的參與動機除了在於取代舊有的 F-4、F-5 與 F-16 戰機以外，還希望能夠帶動其國內的國防產業發展。目前有 8 家土耳其企業參與 F-35 戰機生產的全球產業鏈，土耳其的主要國防企業包括 Aselsan（世界排名第 55）、Turkish Aerospace Industries（世界排名第 64）、Roketsan（世界排名第 96）、Fokker Elmo、Havelsan、Kale Aerospace 都名列其中，負責中段機身、飛彈系統與武器艙門線路相互聯結系統（Enhanced Electrical Wiring Interconnection Systems, EWIS）等裝備與零組件的開發與製造。

（二）印度

印度在 2016 年 9 月向法國所訂購總價 88 億美元的 36 架「颶風」戰機（Rafale），法國承諾給予印度合約總值 50%（44 億美元）的工業合作（offsets）條款，將由包括達梭航太（Dassault Aviation）、賽峰集團（Safran S.A.）、達雷茲集團（Thales Group）與 MBDA 等 4 個主要國防企業來負責，其中包括印度廠商加入零組件的供應、在印度建設廠房與提供印方人員高技術工作的職業訓練等等。此外發動機製造商賽峰集團也將協助印度國防研究暨發展組織（Defence Research and Development Organisation, DRDO）重啟印度國造發動機「卡維利」（Keveri）的研發計畫。

三、強調國際合作

國際化合作成為近年來也成為中小型國家的國防產業發展趨勢，如芬蘭的派翠亞（Patria）除了由芬蘭政府持有過半股份以外，也不斷在國際上尋找夥伴進行合作。在 2001 年至 2014 年派翠亞曾引入空中巴士（Airbus）的投資藉以打入歐洲與世界市場，現今則強調區域合作，在 2016 年起引入挪威康斯堡防衛及航太

[16] 土耳其自 2019 年 7 月 12 日開始取得俄羅斯製的「S-400 防空飛彈系統」（S-400 missile system），此舉使得美國在 2019 年 7 月 17 日宣布與其他「F-35 聯合攻擊戰鬥機計畫」的夥伴國家一致決定暫停土耳其的參與，是以此處所述為土耳其遭受美方制裁前的參與狀況。

公司（Kongsberg Defence & Aerospace）的資本，藉以強化既有的北歐合作，攜手在國際市場上競爭。

由上述案例看，我們可意識到國防產業的國際化幾乎無法避免。在經濟面向上，屬於高技術範疇的國防產業進入門檻高，需要長期而穩定的大量財政資源的投入，國際合作有助資金的吸引與挹注。在技術面向上，科技的發展促成國防產業中不同部門與企業的合作需求增加，藉由彼此的合作讓產品得以符合最多數買家的需求，開創更多的外銷機會。

伍、台灣國防自主的挑戰與機會

從前述的重要國家發展經驗反思，台灣「國防自主」政策與軍備國造計畫的挑戰與機會主要可從如下兩方面切入：

一、國防產業能力的維持

為了維持國防產業基地的運作，穩定與持續的生產需求是必要的。然而，一國的國內需求往往仍不足以維持軍事裝備生產線的最低運作需求，政府也很難為了生產線的維繫而將預算投入在添購不必要的武器上。如此一來，即使國防企業廠商有意願購置新的廠房與設備進行生產，也會因為僅有少量需求可能使投資血本無歸而卻步。以法國的「颶風」戰機為例，一年需要至少 11 架「颶風」戰機的訂單方可維持 1 條生產線的正常運作，但法國自身需求也無法滿足此一最低標準。[17]

因此，如何維持國防產業基地的永續發展便是「國防自主」的重要課題。台灣在過去已有苦澀的經驗，自 1980 年代開始研發的「經國號」戰機，在 1999 年完成最後 19 架「經國號」戰機後便關閉了生產線，同時研究團隊也遭到解散，部分成員為南韓所雇用發展其自製的 T-50 金鷹式高級教練機，使得台灣航太工業出現了人才與經驗銜接的斷層。「經國號」戰機的案例被視為是台灣航太工業的重大損失。

考量到目前主要的計畫包括 66 架的「勇鷹號」高級教練機與 8 艘的自製柴電潛艦在內的建造數量均有限，使得台灣依舊面對類似的問題，如何在這些計畫結束之後維持國防產業基地的持續運作，以確保關鍵技術能力不致流失，考驗著決策者的智慧。

針對此一挑戰，主要國家如法國便十分強調出口對維持國防產業基地的必要性。根據《2019 年法國軍備出口報告》（*Rapport au Parlement 2019 sur les exportations d'armement de la France*），2018 年法國的軍備出口總額為 91.18 億歐元，與 2017 年相較成長超過 30%，是近 20 年來第三佳的表現，為法國國防產業永續發展注入了一劑強心針，確保了在法國國內約 20 萬的直接就業與 40 萬的間

[17] Ministère des Armées de la France, Rapport au Parlement 2019 sur les exportations d'armement de la France, June 2019, p.18.

接就業機會。[18]因此，出口也是我國國防產業永續發展所必須要考量的重要因素。事實上，我國產製的許多產品已經具有不錯的國際名聲，例如「經國號」戰機與「勇鷹號」高教機使用的 TFE1042-70/F124 發動機，因發展成熟且性能可靠且具成本優勢，已獲國際多種型式教練機採用或作為戰機性能升級的發動機選擇。此外，國造飛彈系統包含天弓三型防空飛彈、天劍二型飛彈、雄風三型飛彈與萬箭彈等也都是極具潛力的外銷產品。然而，考量到我國的艱困的國際處境，台灣的軍備出口可先著重在次系統與代工零組件的出口機會（如閥門與排水馬達），強化在國際市場的能見度以增加出售可能性。

二、關鍵技術的突破

全球軍售市場呈現出寡占的趨勢。就國家而言，如圖 7-1（見下頁）所示，在 2014 年至 2018 年間美國與俄羅斯佔了全球軍售市場的 57%。就企業而言，如表 7-5（見下頁）所示，2018 年全球十大國防企業中，美國籍企業即佔了 50%。這樣的趨勢說明了國防產業的特殊性，相較於其他產業，國防產業的進入門檻較高，其中所使用的尖端技術與所需要投入的研發成本均所費不貲，這使得國防產業中的「先行者優勢」（first-mover advantages）相當明顯，對於後起之秀相對不利，例如由歐洲多國合資設立的空中巴士（Airbus）即是在 1980 年代起在獲得各國政府的財政援助後方能與歷史悠久的美國波音（Boeing）競爭。[19]我國目前主要的軍備國造計畫都需要仰賴歐美國家在關鍵技術領域的支援，由於這些技術都被控制在少數廠商手中，再加上我國特殊的國際處境，將使得技術轉移更加困難與成本高昂。

[18] Michel Cabirol, Exportations d'armes 2018 : la France réalise sa troisième meilleure performance depuis 20 ans," *La Tribune*, April 17, 2019, https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/exportations-d-armes-2018-la-france-realise-sa-troisieme-meilleure-performance-depuis-20-ans-813902.html; Ministère des Armées de la France, *op. cit.*, p.3.

[19] Fanny Coulomb, " L'industrie mondiale de défense, entre mondialisation et politique de puissance des Etats,"*Paix et sécurité européenne et internationale*, Université de Nice Sophia Antipolis, 2018, http://revel.unice.fr/psei/index.html?id=1870.

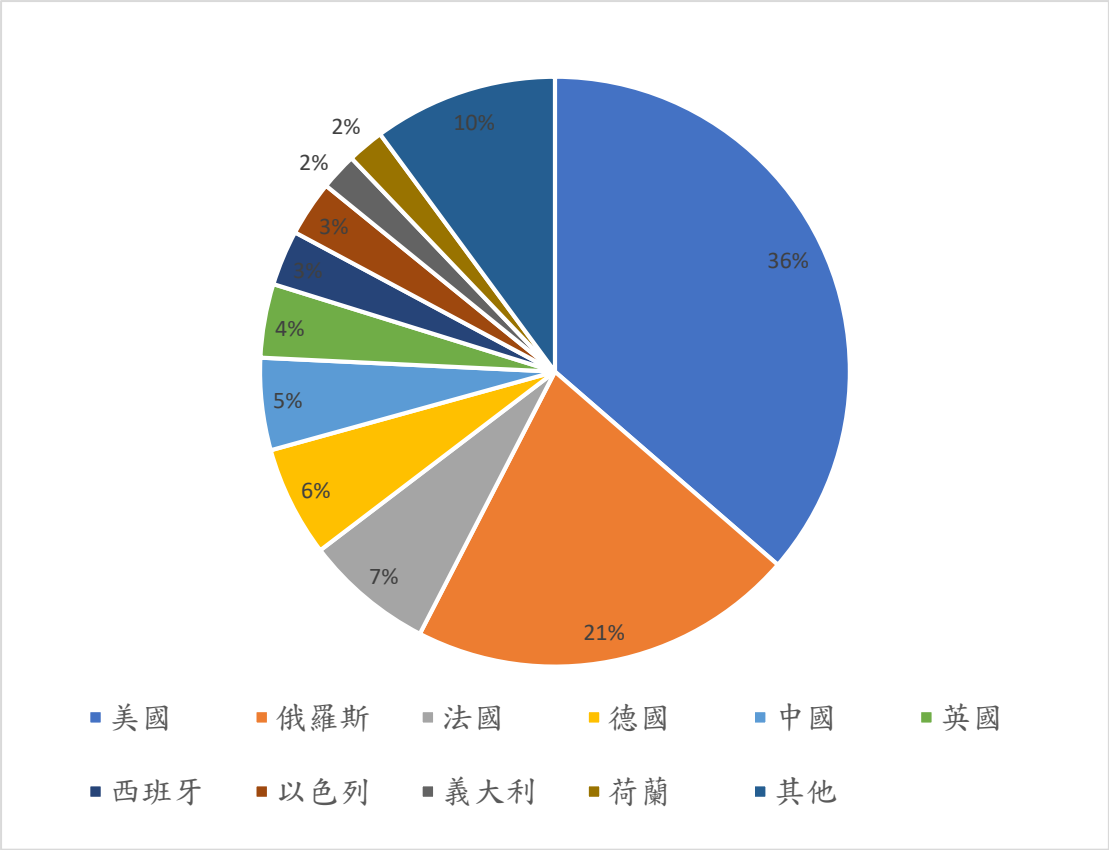


圖 7-1、2014-2018 年全球武器出口市場分布情形

資料來源：斯德哥爾摩國際和平研究所（Stockholm International Peace Research Institute）。

表 7-5、2018 年全球前十大國防企業（單位：百萬美元）

國防企業	國籍	2018 年國防收入
洛克希德馬汀	美國	50,536
波音	美國	34,050
諾斯洛普格魯門	美國	25,300
雷神	美國	25,163
中國航空工業集團	中國大陸	24,902
奇異	美國	24,055
貝宜	英國	22,477
中國兵器工業集團公司	中國大陸	14,777
空中巴士	法國/德國/西班牙	13,063
中國航天科工集團	中國大陸	12,130

資料來源:洪瑞閔整理自公開資料。

面對此一挑戰，土耳其的國防自主經驗可供參考，一方面，土耳其於 1985 年成立年度預算超過 10 億美元的「國防產業援助基金」（Defense Industry Support Fund, SSDF），其財源主要來自各項規費，為各項國防研發計畫提供更多的財政支持。我國已於 2006 年制定「國防工業發展基金設置條例 」的類似機制促進國防工業之發展，同時國防預算在 2020 年達到歷史新高，共計新台幣 3,580 億元，占 GDP 比例 2.3%，惟仍應積極尋找其他的財政來源支持國防產業的發展。

另一方面，自 1980 年代起，土耳其的國防企業便開始與歐美先進國家合作，透過歐美大廠授權生產與成立合資公司等方式來提升自身的技術能力。英國引擎製造商勞斯萊斯（Rolls Royce）、貝宜系統（BAE System）美國發動機製造商普惠公司（Pratt & Whitney）都是土耳其國防企業近年來的合作對象。在美中貿易戰與台商資金回流的背景下，台灣政府若能搭配 2019 年 5 月 31 日所通過的「國防產業發展條例」加速國防產業園區的建構，廣邀國內外相關廠商進駐，爭取參加歐美國家的國防生產計劃以及打入全球產業鏈的機會，將可成為台灣提升關鍵能力與帶動產業發展的契機。

陸、小結

本章討論台灣「國防自主」的發展現況與其未來展望。首先，「國防自主」作為台灣的重要政策之一，「國機國造」與「國艦國造」已經如火如荼進行中。透過新式高教機與潛艦等主要計畫的經驗與進程，可顯示出台灣國防產業已經具備一定自製能力，惟在某些關鍵技術上仍然仰賴歐美國家的技術援助。第二，對於台灣而言，推動「國防自主」具有安全與產業兩方面的意涵，在安全面向上，「國防自主」可作為戰略建構的基石，同時減低對外國的依賴並提升戰略自主性。在產業面向上，「國防自主」可藉由就業機會的創造、經濟加乘效應與外溢效應對國家發展帶來貢獻。第三，從瑞典、芬蘭、印度與土耳其的發展經驗可以得知，利基生產的發展模式、重視在地國防企業的參與和強調國際合作，是與台灣背景相似的中小型國家的發展趨勢，亦是我國國防產業發展應當參考之對象。未來，維持國防產業創新能力與掌握關鍵技術是我國「國防自主」計畫當所努力的方向。尋求擴大對外出口、追求更豐沛與穩定的財源支持以及尋求嵌入全球產業鏈將是台灣國防產業發展機會之所在。

（責任校對：吳宗翰、郭恒孝）

結論

蘇紫雲、吳俊德

對 2019 年國防科技趨勢影響最重大的事件，莫過於從 2018 年 3 月開始，持續延燒至 2019 年底尚未結束的美中貿易戰。表面上，貿易戰是美國樹立關稅壁壘以平衡對中國鉅額的貿易逆差，但實際上有更重要的戰略意涵。中國為躋身世界製造強國之林，以企業購併、駭客入侵、強迫技術轉移等種種方式獲取或竊盜攸關國防與經濟競爭力的關鍵技術。中國在取得這些技術後，近年來大幅提升武器性能，並且不斷擴張軍事力量，成為崛起中的霸權。中國的軍備擴張配合其「一帶一路」倡議威脅到美國在全球的利益，而被美國視為戰略競爭對手。因此，貿易戰的真正目的是反制中國科技滲透、防止美國關鍵技術外流、以及維持美國科技領先優勢，其本質其實是科技戰。在這樣的背景下，敏感科技保護以及國防產業安全成為 2019 年國防科技趨勢的關鍵字，也是本年度評估報告的主軸。

美中科技戰由美國將華為及其相關企業納入出口管制的「實體清單」拉開序幕，資通訊設施尤其是 5G 設備成為科技戰的主要戰場。在美國力求聯合友盟圍堵華為，而華為也極力突破封鎖的態勢下，未來全球可能成為民主科技聯盟與中俄非民主陣營分庭抗禮之局。科技冷戰的兩極體系對台灣來說是機會也是挑戰，一方面，廠商移出中國大陸造成全球生產供應鏈的重組，台灣除迎接台商回流外，更可藉此機會爭取高科技大廠來台投資設廠；隨著台灣在高科技產業供應鏈中重要性的提升，台灣的安全與穩定就更為動見觀瞻。另一方面，台灣將會面臨更多的科技滲透與人才挖角，如何做好資訊安全防護，避免營業秘密和智慧財產權被竊取，將會是政府首要之務。

在中國崛起之後，新興關鍵技術成為未來地緣政治以及全球霸權爭奪的重要因素，其中以高能雷射、極音速打擊技術、人工智慧、與量子運算為各先進國家研發的重點項目。這些技術多屬軍民兩用，許多技術由民間廠商開發，其產品卻可以轉為軍事用途，技術擴散雖然有助於產業發展，卻也可能讓敵對國家取得可轉為軍用的尖端科技產品，因此需要加強科技管制體制。為了防範技術與產品外流，先進國家皆修訂更細膩的法規，對關鍵技術加強外來投資的管制、出口管制、以及對教學研究機構的規範。

以美國為例，美國為因應中國威脅，在 2018 年通過《外來投資風險審查現代化法》改革投資審議體制，自 2018 年底到 2020 年初試行「新前導方案」，只要是涉及關鍵基礎設施、關鍵技術、或是個人敏感資訊，即便是「非控制性投資」也強制要向「美國外來投資審查委員會」通報審查。在廠商管理上，將廠商依技術能力與專業領域分類分級，並加強公司內部安全治理。在供應鏈安全上和資訊安全防護上，美國國防部 2019 年提出「無侵入交付」與「網路安全完善模式認證」的新規範，安全思維也轉為「零信任架構」。最後在產品製造完成後，必須經過認證確保品質，並且以出口許可管制最終使用者的用途。這些規範涵蓋軍民

兩用商品的整個製造、銷售流程，目的是保護智慧財產權以及維護國防產業安全，值得我國效法。

隨著科技日益進步、武器系統推陳出新，作戰概念也為之轉變。未來的戰場將是多領域作戰，並結合非軍事衝突的手段，各國紛紛在戰術戰法上創新，以不對稱作戰思維對抗傳統強權在兵力以及火力上的優勢。台灣亦同，應發展「小型、致命、大量、機動」的裝備，以抵銷共軍龐大軍力的優勢。除了持續投資先進裝備以外，台灣更應配合不對稱作戰的武器配置及戰術戰法進行組織變革，以強化未來的嚇阻能力。

新興關鍵技術運用在武器裝備的發展上，具體而言包括第六代戰機、雷射與導能武器、極音速與長程打擊武器、陸海空無人載具、各式戰場無人系統、以及人工智慧在武器系統上的應用，均為先進國家致力發展的目標。可以預見，未來的戰場景象將是有人與無人系統搭配作戰，而彈藥技術的進步，加上載台火力投射的能力更加強化，防禦性武器如雷射與導能武器、以及能夠抵禦極音速與長程打擊武器的新世代飛彈防禦系統，未來的需求將會大幅提升。

最後，對台灣而言，國防自主具有安全與產業的雙重意涵。一方面，國防自主可以降低對外的依賴並提升戰略自主性；另一方面，國防自主可創造就業機會，並透過加乘效應與外溢效應貢獻經濟發展。台灣的國機國造與國艦國造正積極進行中，台灣應掌握利基生產的模式，並盡量讓本地國防企業參與。台灣國防自主將面臨的挑戰是未來如何維持國防產業能力，以及掌握關鍵技術。因此，尋求對外出口以及協助廠商打入全球國防產業鏈，將會是台灣國防產業發展的關鍵。