



2018 國防科技趨勢評估報告

主編 蘇紫雲 曾怡碩

財團法人國防安全研究院

2018 年 12 月

2018 國防科技趨勢評估報告

主編 蘇紫雲 曾怡碩



財團法人國防安全研究院

2018 年 12 月

2018 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）

曾怡碩（網路作戰與資訊安全研究所 助理研究員）

作者（依姓氏筆畫順序）

吳俊德（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）

曾怡碩（網路作戰與資訊安全研究所 助理研究員）

舒孝煌（國防資源與產業研究所 助理研究員）

黃恩浩（國防戰略與政策研究所 助理研究員）

劉姝廷（網路作戰與資訊安全研究所 研究助理）

蔡榮峰（國防資源與產業研究所 研究助理）

蘇紫雲（國防資源與產業研究所 副研究員）

摘要

蘇紫雲、曾怡碩

本報告為求系統性評估國防科技趨勢，在分析架構上區分為三大篇：第一篇探討主要國家軍事科技趨勢，並檢視未來戰場特性；第二篇進一步辨識關鍵資通訊科技與關鍵軍事科技發展；第三篇則先分析台灣面對科技挑戰，接著提出因應作為與綜整意見。

在比較分析美國、中國、俄羅斯、北約的軍事科技發展趨勢後，針對未來戰場中，跨領域作戰、網路化分散式作戰、太空競逐、超精準打擊、高密度自動化戰場、模組化作戰形態、混合型作戰模式等七大特性進行梳理，呈現未來戰場的科技需求。進一步則辨識及評估四項關鍵軍事科技與四項關鍵資通訊科技發展，其中，台灣在資通訊科技發展上，具有相當的利基。

台灣關鍵資通訊基礎設施面臨來自中國的太空科技優勢、網路及電戰攻擊、網路心理暨輿論戰之威脅，宜發展不對稱作戰，並可將重心放在以下幾個項目：戰力保存、人力資源有效運用，以及各種新形態的作戰方式與領域等。台灣可著重在發展科技及戰術戰法領域上的不對稱戰力，除承平時期的嚇阻之外，還包括真正面臨衝突時，可發揮實際的戰力加乘效益，可減少台灣在數量上的不對稱劣勢。

同時，美國川普政府對於與中國的貿易戰，有其整體戰略考量，尤其是科技管制出口與管制中國科技產品輸入這兩區塊，是台灣開拓市場的新契機。台灣應投入自身有利基的國防科技發展，進一步打入跨國的國防科技供應鏈，可發揮國防、外交、經濟的綜合效益，強化在國際合作中的地位。舉例來看，除了定向能武器、仿生機器人、主動防禦科技及匿蹤科技之外，台灣在人工智慧、網路安全、立體列印、自駕科技、虛擬科技及無人載具都已具備相當基礎，而這些軍民兩用科技，也將為台灣產業發展與民生福祉，帶來長足的助益。

至於敏感科技管理機制，由於涉及經濟競爭與國家安全，防堵中國科技滲透影響總體安全已成為民主國家的主要議題。美國在 2018 年發佈《評估及強化美國國防工業基礎與供應鏈彈性》中將台灣列為「偽劣電子元件」的主要來源之一，加上具產業代表性的晶圓機台病毒事件、晶圓業者涉及洩密遭美國起訴等案例，突顯我國在產業安全、科技安全的管理仍有極大改善空間。台灣不能成為全球生產供應鏈的缺口，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。這些措施不僅攸關國家安全事宜，對業業者的商譽與競爭力也是關鍵。

面對中國在相關國家造成的資安產品及生產鏈安全問題，台灣的國防產業可以彌補部分供應鏈。例如 F-16、F-18 等 80 年代設計／出廠的戰機與軍備，雖有不同批次的改良，但部分軍規晶片已停產，而台灣業者仍具有相關品項的生產能力，可補充全球數千架戰機機隊的零件替換所需。台灣雖具良好科技基礎，但國際合作關鍵，在於落實敏感科技的管理。鑒於產業界對科技保護的認知不同，未來在溝通時，宜敘明科技研發本身具有「公共性」須受管理，例如傳統的核生化科技外，基因科技、人工智慧所衍生的人類倫理等議題，都是科技與公共性需取得平衡的具體事例，同時輔以貿易戰衍生的產品安全成為市場誘因，較易讓業者理解科技管理的必要性與市場價值，如此得以兼顧台灣在國防安全與經濟的進一步發展。

目錄

摘要.....	v
表目錄.....	ix
圖目錄.....	x
專有名詞中英對照.....	xi
緒論.....	1
第一篇軍事科技趨勢與戰場特性.....	5
第一章主要國家軍事科技發展趨勢.....	6
前言.....	6
壹、美國.....	6
貳、中國.....	15
參、俄羅斯.....	20
肆、北約各國.....	24
小結.....	30
第二章未來戰場特性.....	31
前言.....	31
壹、跨領域作戰.....	31
貳、網路化分散式作戰.....	34
參、太空競逐.....	36
肆、超精準打擊.....	38
伍、高密度自動化戰場.....	43
陸、模組化作戰型態.....	46
柒、混合型作戰模式.....	48
小結.....	50
第二篇關鍵軍用科技的發展.....	51
第三章關鍵軍事科技的發展.....	53
前言.....	53
壹、戰場機器人.....	53
貳、匿蹤科技.....	61
參、極音速載具.....	65
肆、集群式攻擊.....	67
小結.....	70
第四章關鍵資通訊科技的發展.....	71
前言.....	71
壹、量子科技.....	71
貳、人工智慧.....	76
參、網路通訊.....	79

肆、虛擬實境.....	83
小結.....	86
第三篇台灣面對的科技威脅與挑戰機會.....	87
第五章台灣面對之科技挑戰.....	89
前言.....	89
壹、建立制太空權.....	89
貳、台灣資安風險與關鍵資訊基礎設施保護.....	92
參、反制網路輿論心理戰.....	96
小結.....	100
第六章台灣發展不對稱戰力的利基.....	101
前言.....	101
壹、地緣優勢.....	101
貳、台海戰場特性.....	103
參、裝備投資選項.....	105
肆、確保局部科技優勢.....	109
小結.....	113
第七章前瞻台灣國防科技與產業整合.....	114
前言.....	114
壹、美中貿易及科技戰的影響.....	115
貳、值得優先發展之科技.....	117
參、強化科技安全管理.....	124
小結.....	128
結論.....	130

表目錄

表 1-1、三次抵銷戰略	15
表 5-1、台灣人造衛星發展進程	90
表 5-2、國防部所屬民網遭異常偵測、掃描及疑遭攻擊次數統計表 ..	94

圖目錄

圖 1-1、波音公司 MQ-25 概念已獲海軍採用	12
圖 1-2、美國 6 代戰機概念仍待整合	12
圖 1-3、美售給英國的 F-35B 戰機	13
圖 1-4、美國空軍發展中的極音速實驗載具 X-60A	15
圖 1-5、法國達梭公司展出的新一代戰機概念 NGF	27
圖 2-1、美國陸軍在 2018 環太平洋聯合演習中發射海軍打擊飛彈 (NSM)	33
圖 2-2、多領域作戰概念	33
圖 2-3、美國陸軍多領域作戰概念圖	34
圖 2-4、美國空軍 AGM-158 飛彈	40
圖 2-5、英國空軍 MQ-9 無人機	44
圖 3-1、大型機械狗 (BigDog)	56
圖 3-2、「龍行者」機器車 (Dragon Runner)	56
圖 4-1、量子位元與錯誤率之概念圖	73
圖 4-2、美軍採用台灣生產之 VR 裝置	85
圖 5-2、國家太空中心衛星計畫衛星操控地面設施關聯圖	91
圖 5-3、以情報驅動之國家資安聯防架構	95
圖 5-4、建立國家級的資安聯防團隊	96
圖 6-1、我 IDF 警戒伴飛	105
圖 6-2、漢光 30 號演習時空軍幻象進行戰備道起降演練	106
圖 6-3、可執行海上偵搜的 MQ-1 無人機	108
圖 6-4、中科院發展的騰雲大型無人機	110
圖 6-5、中科院發展的陸射劍一及劍二飛彈	111
圖 6-6、中科院發展的雙基雷達	112
圖 7-1、美軍採用之商用移動裝置	118
圖 7-2、具備高度運動能力的軍用仿生機器人原型	123
圖 7-3、配置於龐斯號上的雷射武器	124

專有名詞中英對照

一、報告/計畫/公約

第3代夥伴計畫	3rd Generation Partnership Project
《聯合國特定傳統武器公約》	Conventions on Certain Conventional Weapons, CCW
《禁止或限制使用特定傳統武器公約》	Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects
《俄羅斯聯邦國家安全戰略》	National Security Strategy of Russian Federation
《國家量子資訊科學戰略綱要》(美國)	National Strategic Overview For Quantum Information Science
戰術利用偵察節點計畫	Tactically Exploited Reconnaissance Node, TERN
《俄羅斯聯邦軍事準則》	The Military Doctrine of Russian Federation
《俄羅斯 2018-2027 軍備計畫》	The Russian State Armament Programme 2018 – 2027

二、技術

主動防禦系統	Active Protection Systems, APS
先進極音速武器	Advanced Hypersonic Weapon
先進戰術雷射	Advanced Tactical Laser, ATL
反介入/區域拒止	Anti-Access/Area-Denial, A2/AD
人工智慧	Artificial Intelligence, AI
擴增實境	Augmented Reality, AR
仿生機器人	Biomorphic robotics
指管通電情監偵	C4ISR
分散式殺傷	Distributed Lethality
原生對抗網絡	Generative Adversarial Networks
極音速巡弋飛彈	Hypersonic Cruise Missile, HCM
極音速滑翔載具	Hypersonic Glide Vehicles, HGV
簡易爆炸裝置	Improvised Explosive Devices, IED

情報、監視與偵查	Intelligence, Surveillance and Reconnaissance, ISR
太空智慧組裝機器人系統	Intelligent Space Assembly Robot System, ISAR
戰聯網	Internet of Battle Things, IoBT
殺傷型自主武器系統	Lethal Autonomous Weapon Systems, LAWS
機動重返載具	Maneuverable Re-entry Vehicle, MaRV
混合實境	Mixed Reality, MR
可集群式攻擊戰術	Offensive Swarm-Enable Tactics, OFFSET
迅捷全球打擊	Prompt Global Strike
量子運算	Quantum Computing
雷達截面積	Radar Cross-Section, RCS
雷達波吸收材料	Radar-Absorbing Materials, RAMs
無人戰鬥空中載具	Unmanned Combat Air System, UCAS
垂直發射系統	Vertical Launching System, VLS
虛擬實境	Virtual Reality, VR
乘波體	Waverider
三、部門	
電腦緊急應變團隊	Computer Emergency Response Team, CERT
國防先進研究計畫署	Defense Advanced Research Projects Agency, DARPA
資訊分享與分析中心	Information Sharing and Analysis Center, ISAC
國際電信聯盟	International Telecommunication Union
美國國家科技委員會	National Science & Technology Council, NSTC
國家偵察辦公室	National Reconnaissance Office
資訊安全維運與預警中心	Security Operation Center, SOC

緒論

蘇紫雲、曾怡碩

軍事衝突是人類文明最複雜的行為，涉及政治、經濟、軍事、以及相對科技的總综合能力。科技發展的原始目的在於使人便利，以滿足人類文明的發展，並促進經濟的繁榮與進步，然而軍事的需求則更加速科技發展。例如，網際網路的雛形，是美軍早期發展的軍用網路，用以連結東西岸的美軍進行演習。而每日在道路上拯救人命的 ABS 煞車系統，則是噴射戰機的附帶發明，用以在進場降落後縮短滾行距離。其他如微波爐是源於雷達技術的副產品，抗生素的盤尼西林源於對戰場大規模的軍陣醫療需求，乃至現代刮鬍刀的雛形，就來自於第一次世界大戰對抗毒氣，讓士兵得以快速清除鬍鬚，使防毒面具得與臉部達到氣密效果。

學者克雷派尼維奇(Andrew Krepinevich)定義的「軍事事務革命」(Revolution in Military Affairs, RMA)，其論述的核心就在新技術的運用與軍事系統性的創新。相形之下，人類戰爭由農業時代的冷兵器、人力與獸力的肌肉能，文藝復興時期化學能的火藥，工業時代的蒸汽機與內燃機的機械能，進一步結合機電系統，在第二次世界大戰中，形成第一波的近代軍事科技。現代的軍事科技，除原子科技外，傳統武力則由電子時代揭開序幕，電晶體為主的半導體開始應用於軍事裝備，其後進階為積體電路科技，使作戰裝備的戰場知覺與精準度大為提高。發展到資訊科技的應用之後，隨即展開了整合個別載台與戰場管理的資訊戰時代。

相對的，國際政治衝突也突顯戰爭科技應用的兩面性，一方面是減少「戰爭之霧」(fog of war)，但又製造了「科技之霧」(fog of technology)，也就是對科技倚賴的盲點。本報告描述科技在未來戰場中的可能樣貌，背後原因在於正規戰的勝負，科技可扮演較大角色。但受國際體系新興的非政府武裝組織衝擊，軍事衝突可能混雜非正規戰手段，而網路的應用也涉及更多的政治、人道等非科技因素，例如無人載具是否可擁有發動攻擊的自主權，此將涉及戰爭哲學的本質、以及道德、倫理之問題，不在本報告主要討論範圍，宜另專篇研究。

回顧產業在戰爭中的轉變，過去一世紀以來，工業能力在軍事中的比重愈為增加，技術演變速度越來越快，載台的創新，應用模式也更為多樣。第一次世界大戰揭開工業科技應用於戰場的大舞台，製造工藝趨向規格化的大量生產以及更精密的機械製造。第二次世界大戰則是電子產業參戰的起始點，真空管的應用帶動雷達、無線電、早期電腦、乃至初期型夜視設備的實用化。此後，戰爭的主要科技開始以半導體產業作為核心，而越戰時期的代表產品，即為電晶體及早期的積體電路。第一次波灣戰爭則是類比電子與早期資訊戰的典範，直到20世紀90年

代中期，數位電子逐漸加入戰場，奠定戰場資訊化與數位化的基礎。

廣義來說，當今所流行的「物聯網」(internet of things)，最早即應用在軍隊組織，小從單一載具的各類感測器，大到各載具的相互構聯以及指揮鏈的連動，可說是「即時決策物聯網」，較民間物聯網的應用更加領先。然而，軍用科技雖經常領先民用科技，但卻需承擔高成本，而民用科技的市場需求帶動快速研發，因此軍用科技往往可取自民用科技的現貨市場。軍用科技與民用科技相互援引，並獲得成功的案例甚多，最具代表性的就是戰車。英軍於1916年在索姆河戰役(Battle of the Somme)首次投入戰車，便是將民用的拖拉機結合裝甲防護及越野能力所產生的革命性產品，成功突破「戰壕僵局」，也改變了陸地戰的面貌。因此，在民用產品市場中，發掘出具有軍事價值的技術及裝備，並加以評估與改良，就成為提昇戰力及減少成本的方式。這可說是美國防部國防先進研究計畫署(Defense Advanced Research Projects Agency, DARPA)的政策精神，也是北約提出「智慧國防」(smart defense)的原因。

同時，現有的許多先進作戰裝備，其概念往往在過去就已出現，只是隨著技術的進步使其得以實現或更為成熟。例如現今耳熟能詳的「無人機」(Unmanned Aerial Vehicle, UAV)，最早於一戰時期的1917年3月，便出現世界上第一架無人遙控飛行器原型，其原始設計目的，在於減少飛行員傷亡。而第二次世界大戰時，德軍研製並交付部隊實用的小型遙控履帶車，是現代「地面無人載具」(UGV, unmanned ground vehicle)的鼻祖。此外，同時代由德國推出的Hs-239遙控滑翔炸彈，透過無線電遙控，可以打擊8.5公里外的遠程目標，可說是首次出現的實用化空射遠攻武器，亦即是視距外(stand-off)武器發展的起始，例如現今的「聯合直接攻擊導引彈藥」(Joint Direct Attack Munition, JDAM)，亦採用滑翔導引的方式遂行攻擊。

此外，隨著半導體技術的發展，前瞻未來10年無人載具的運用將更為普及，且明顯的將由偵察與觀測用途，轉向攻擊任務發展。值得注意的是微型飛行器(micro unmaned aerial vehicle)，可說另一分水嶺，其結構不同一般認知的傳統飛行器，而是結合「微機電系統」(Micro-electromechanical Systems, MEMS)科技，包括微型馬達、精密機械的結構設計，可以採用定翼、旋翼、甚至拍翼(flapping)的飛行構型設計。同時，除飛操系統外，其所搭載的技術核心是以積體電路將水平儀、高度計、乃至衛星定位、加速度儀、與微陀螺儀等科技予以整合，以作為飛行姿態控制系統。此一模組化的設計應用如同手機可以拍照；感測姿態、多頻率通話、無線上網，乃至光線感應等多用途整合在不同的晶片模組，同樣的技術整合應用，也見諸於民用的各類無人飛行器，甚至是各類油氣管道的遙控檢測載具，這正是軍民兩用技術的另一實例。

無人載具的發展，也凸顯不對稱作戰概念的發展與落實。將科技應用付諸實

現為具體戰力，不再只是擁有雄厚資源大國專利，務實小國只要善用智慧，也能將科技威脅與挑戰，轉化為發展不對稱因應措施的契機，並轉而挹注於自身國力發展。具體來說，在先進國家所謂的國防預算不再被視為「消耗型」，而應視為「國防經濟」(defense economy)。無論是其從業人員以及裝備生產採購，乃至作業維持等，都被視為國家經濟活動的一環。由於軍用及安全事務是特殊市場，受經濟景氣影響較小，需求也相對穩定，因此具備「戰略經濟」(strategic economy)的價值。有鑒於此，裝備生產的本土化也就更為重要，如此才能實質挹注國家經濟的發展。這就是軍民兩用科技成長、水平擴散整合的主因之一，對國防與經濟發展具有相輔相成的效果。

第一篇 軍事科技趨勢與戰場特性

第一章主要國家軍事科技發展趨勢

美國、中國、俄羅斯、北約

黃恩浩、舒孝煌、許智翔、蔡榮峰¹

前言

軍事科技及國防工業發展，除與其國防安全的需要相關外，也仰賴各國本身經濟實力、科技研發與工業基礎支持，通常一個國防工業大國，本身亦具備雄厚的重工業、高科技產業、材料、金屬、資訊等等產業的基礎。

本章觀察主要國家國防與軍備科技發展趨勢。其中，美國不但具備完整國防工業基礎，並領導世界軍備發展潮流，除先進戰機、艦艇外，尚包括無人機、自動化科技、精準武器、飛彈防禦系統、情報、監視及偵察用電子裝備、各種動力及能源科技等等，並供應盟國武器裝備及技術。

俄羅斯師承過去蘇聯時代的軍事工業發展，在戰機、水面艦及潛艦、戰甲車、飛彈等有豐富發展經驗，雖然因經濟等因素限縮其軍事科技發展，但仍具優勢。中國過去依賴前蘇聯協助建立軍事工業基礎，近年拜經濟起飛之賜，快速發展國防工業，但其模仿、剽竊智財權等行為受到美國等西方國家批評。

北約國家多為中、小規模國家，其國防科技多有其歷史傳承，然因近年因高科技武器發展成本昂貴、技術風險高，因此多採國際合作方式，組成跨國軍事公司，或是由政府出面整合，採用相同標準，發展可供多國使用的共通化武器。

各國國防科技均朝向太空化、無人化、匿蹤化、智慧化與網路化等方面發展，顯示戰爭型態雖日趨多樣化，然高科技戰爭仍會是戰場主流。

壹、美國

美國的國防工業與科技基礎強大，主要來自其國內雄厚的工業基礎及科技實力，另也因為美軍常年在海外作戰，其軍事裝備結合戰場與實地操作經驗，能承受嚴苛戰場操作。美國在二戰時曾有民主國家兵工廠的稱號，並向包括台灣在內的盟國與友邦出售武器裝備，不但擴大市場規模，減低研發成本，同時也協助其友盟國家維護國家安全。

美國是民主國家，為爭取預算、接受國會監督，並讓友盟國家瞭解美國國防政策，每任美國總統一向會在其上任後及任期中出版有關國家安全、國防戰略等

¹ 黃恩浩，國防安全研究院國防戰略與政策研究所助理研究員，負責本章第壹、貳節部分內容；舒孝煌，國防安全研究院國防資源與產業研究所，負責本章第壹、貳節部分內容；許智翔，國防安全研究院先進科技與作戰概念研究所博士後研究，負責本章第肆節；蔡榮峰，國防安全研究院國防資源與產業研究所研究助理，負責本章第參節。

相關文件，因此觀察文件內容，可說明建軍備戰方向。

一、美國的國防政策

2017 年就任的川普總統 (Donald J. Trump)，已在同年 12 月公布《國家安全戰略》(National Security Strategy of the United States)，2018 年則陸續公布《美國國防戰略摘要》(Summary of the 2018 National Defense Strategy of The United States of American)、《核武態勢評估》(Nuclear Posture Review)、《中國軍事與安全發展報告》(Military and Security Developments Involving the People's Republic of China 2018)、《評估及強化美國國防工業基地與供應鏈彈性》(Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States) 等文件，說明川普領導下的美國政府對世界情勢、美國安全威脅、軍事能力等的看法。

(一) 國家安全戰略強調美國優先

2017 年 12 月 19 日推出的《國家安全戰略》，詮釋所謂「美國優先」，主要在於軍事及科技領域，其中包括確保軍事力量現代化、確保美軍取得最精良及創新之裝備、修正裁減聯合作戰部隊之決策並促使現代化及確保戰備能力、強化軍力整備具備全方位作戰能力、發展新的作戰構想，確保面對非傳統軍事衝突或無法完全掌握空、海、太空及網路優勢時仍能勝利、具備對抗非正規戰爭能力。

另外，報告還提到健全國防工業體系，並批評過去 20 年來，美國國防工業弱化，產品仰賴國內單一來源或是國外供應，若無法完全自製產品，美國會在高科技、網路安全及航太領域等基礎弱化。相關作為包括評估美國軍工業，確保國安重要物資來源穩定、供應鏈的脆弱點，並掌握未來科技；鼓勵國內產業投資，加強關鍵科技及製造能力，改善美製武器出口流程及規定，保護關鍵技術。美國也要維持核武優勢、確保核武存量、核武設施現代化，以保持穩定嚇阻力。美國應確保太空領域的自由使用，以保障通訊、金融、軍事、情蒐、氣候及航行安全。許多國家已獲得反衛星的不對稱能力，美國優先包括確保在太空領域領先，成立國家太空委員會，更新遠程探索目標，透過鬆綁及更新法規，促進商業太空活動；在太空探索維持領導地位，探索太陽系，加強公私部門及夥伴合作。

(二) 國防戰略摘要強調美軍需防範中俄

2018 年 1 月 19 日《國防戰略摘要》對美國國際安全環境與挑戰作整體評估，將中國和俄羅斯列為最重要的對手，指出它們對美軍構成的威脅已經超過恐怖主義。該報告認為，中國和俄羅斯的軍事發展已削弱美國在全球的軍事優勢，為因應對這一趨勢，美國必須增加國防支出，以使美軍能保持更強大、敏捷，以及維持在隨時應戰狀態。該報告強調美軍仍將持續從事反恐，但現在國家安全最主要焦點是大國競爭，也就是說美軍亦將盡全力防範與應對中俄兩國國際擴張。²

² “Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the

該報告認為未來美軍要做到以下幾點才能保持軍事優勢，包括：1、將核武器現代化。2、投資太空和網路空間，並把這兩個領域當成戰爭領域。3、加大在電腦、通訊、情報和監控系統的投資。4、部署更多的飛彈防禦系統保護美國軍隊和美國本土。5、打造更具殺傷力的戰鬥部隊，有能力襲擊敵方的空中和導彈防禦系統。6、投資海、陸、空和太空部隊，使其遭遇到襲擊也仍然可以作戰並重聚軍力。7、在世界重要的戰略地點儲存重要的戰鬥武器和其他軍需物資。該報告還提到，美軍應該迅速將商業科技用於軍事，藉以提高人工智能和機器學習技術來確保美軍在世界上的優勢地位。

《國防戰略摘要》提到美國「將維持世界一流軍事力量、確保對美國有利之權力平衡、促進有利美國安全與繁榮之國際秩序」。這五項威脅可分為兩個層次，前者為中俄所構成之「大國戰略競爭」，後者則是不斷製造事端，影響區域穩定與安全之行為者。針對中俄兩個修正主義大國，更明指其「企圖推動快速軍隊現代化，以擊敗美國武力，並挑戰美國經濟領導地位」，以及「妄圖撼動北約安全體系」，必將成為未來最大的戰略競爭對手。³

《國防戰略摘要》明白提到，中俄都在利用其體制內的利益，破壞國際秩序，企圖創造一個與其獨裁模式相同的世界秩序。中國是以掠奪性經濟來威懾鄰國，同時在南中國海進行軍事化，影響航行自由；而俄羅斯是以侵犯鄰國的邊界，藉控制鄰國的經濟、外交和安全面向並造成威脅。另外，在流氓政權方面，北韓和伊朗堅持採取威脅地區乃至全球穩定的非法行動，並壓榨人民、破壞人權。在恐怖主義方面，例如：伊斯蘭國，黎巴嫩真主黨或基地組織等暴力極端主義，仍繼續在世界各地散播仇恨、破壞和平。⁴

在「因應戰略環境」、「強化聯盟關係」與「精進國防科技武器發展與獲得」之前提下，美國國防政策之對內目標在於，試圖擺脫目前美國戰略縮減現象，並重建軍隊優勢。這軍事戰略方向可視為美國軍事事務再革新；對外目標則在於驅使盟國共同承擔責任，讓美國領導下的國際安全體系得以繼續運行。為了因應未來從陸海空、太空與網路所有領域競爭，積極發展高階運算電腦、大數據分析工具、人工智慧、自主科技、機械人、雷射武器、高超音速武器和生物科技。預見前述科技趨勢已成為打贏未來各類型戰爭的必要條件，美國國防計劃將從三個戰略方向著手：

- 1、建立更精實的軍力：建立靈活的聯合部隊，再配合核打擊與網路作戰等能力，構成系統性的全面軍力。
- 2、強化同盟連結並建立新的夥伴關係：擬繼續在印度洋、太平洋地區努力打造盟友關係，強化建立一個自由、開放、包容和繁榮的印太地區的願景。

American Military's Competitive Edge, U.S. Department of Defense, 19 January, 2018, <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>。

³ <美國防戰略適應新興安全環境>，《青年日報》，2018年1月24日，<https://www.ydn.com.tw/News/274584>。

⁴ 同註1。

3、落實軍工複合體整合：結合民間，將美國的高科技與技術創新能量注入國防，這就表示美軍將推展更多的軍工複合體機制。

（三）改善採購流程以獲致加快獲致新裝備速度

美國國會已同意增加國防預算因應新戰略，包括網路安全、指管通情監偵（C4ISR）、飛彈防禦、核武、極音速武器、高能雷射、電子戰、太空，這些領域都是急迫需求。美國廠商已準備因應挑戰，發展相關新技術，包括：人工智慧、積層製造（Additive Manufacturing，即 3D 列印）、奈米科技（Nanotechnology）等。這些技術都已發展超過 10 年，現在開始運用在國防工業，並進入部隊開始服役。另外，國防產業也與非傳統國防夥伴聯合，將商用技術運用在國防工業，並由新創公司、小型產業及矽谷學習科技創新的速度。另外，美國要和盟邦保持合作，工業界則在國外尋找創意及靈感，強化創新及競爭力。

過去 5 年來，美國防部啟動數項重要武器計畫，但美國國防工業並未滿足期待。過去國防部投資在研究發展，特別是其需要的武器裝備，並與國防合約商緊密合作。但今日則是國防部尋求夥伴，包括傳統及非傳統公司，投資在新技術及以更快且更便宜的方式交貨。這意味國防工業要改變其投資及發展新產品方式，取代過去依賴年度性計畫循環以創造財務預測的模式，並需採取更精準的途徑進行評估。應依據精準評估做出戰略性投資選擇，避免依賴過度採購來彌補創新及成長的不足，同時也制定一連串戰略，形塑承擔風險以及創新的文化。⁵

新的安全挑戰使美國防部無法再循過去官僚途徑，等待多年以獲取新技術。美國國防部要工業界儘快發展新的技術，以反應轉變中的威脅。與其等待國防部投資計畫，這些傳統參與者應自我投資新系統，並面對其不確定性、提升舊系統性能。目前進行中計畫包括：席瑞亞內華達集團（Sierra Nevada）發展 A-29 輕型攻擊機，參與美國空軍「非發展輕型攻擊機平台」能力評估；波音公司（Boeing）與瑞典 SAAB 集團合作，以自有資源發展並生產 T-X 教練機的原型機；另外如洛克希德馬汀公司（Lockheed Martin），也聚焦於自動化系統及機器人等長程戰略性投資。

二、美國軍事科技趨勢

美國一向自詡擁有並掌握世界上最先進科技，藉投資實驗室、國防先進研究計畫署（Defense Advanced Research Projects Agency, DARPA）及國防工業公司，⁶以秘密驅動創新技術，例如第二次抵銷戰略（Second Offset Strategy），包括：匿蹤戰機、精準武器及資訊化指揮管制系統。美國前國防部助理部長渥克（Robert O. Work）所稱第三次抵銷戰略（Third Offset Strategy），則包括：先進極音速武器、直接能武器（雷射）、AI 人工智慧等。為因應高科技戰爭趨勢，美國國防科

⁵ “Can Aerospace and Defense Companies Meet Their Great Expectations?” *Strategy+Business*, February 1, 2018, <https://www.strategy-business.com/article/Can-Aerospace-and-Defense-Companies-Meet-Their-Great-Expectations?gko=1ec59>。

⁶ “Defense Advanced Research Projects Agency,” DARPA, <https://www.darpa.mil/>。

技正朝向太空化、無人化、匿蹤化、智慧化與網路化方面發展，以下舉其要者說明發展趨勢。

（一）太空武器與太空戰

美國仰賴太空的程度高於其他國家，主要是部署各型氣象、導航及定位、通訊、光學或雷達影像偵察（Optical or Radar Imaging Reconnaissance）、電子情報蒐集（ELINT）、飛彈預警、監視、衛星追蹤以及科學研究等。過去也曾發展太空武器，1980 年代美國即已發展空射反衛星飛彈技術，曾以 F-15 戰機發射 ASM-135 反衛星飛彈（ASAT），摧毀一枚軌道高度 555 公里的衛星。2008 年，美國海軍以一枚標準 3 型飛彈（Standard 3）擊毀一枚失效的間諜衛星。目前美國除以擊落失效衛星避免落在人口稠密區為理由，並未特別運用太空進行部署。目前主要發展重心在彈道飛彈防禦科技，除強化對太空觀測能力，追蹤俄、中可能的殺手衛星發展外，也曾計畫在太空中部署雷射，用以對付彈道飛彈。

美國三個軍種都有自己的太空資源，美國空軍在 1982 年成立太空司令部，川普總統已下令成立太空軍（United States Space Force, USSF），美國防部已開始進行初步規劃。目前許多太空武器仍在概念化階段，包括仍在測試階段的 X-37B 無人太空梭、可重返太氣層的極音速飛機、太空無人機、雷射武器等；另外，新一代美國衛星也將思考可能在太空中遭遇敵方威脅，必需有自我保護能力，這是美國目前思考方向。⁷

（二）先進無人載具

美國在無人載具的發展及軍事運用，無疑地居於世界領先地位，其技術亦是世界最先進。美國無人機已在中東戰場上執行任務有 10 年以上，包括 MQ-9「死神」（Reaper）、MQ-1 掠奪者（Predator）等，結合偵打一體、透過衛星遠端控制、以及綿密的情監偵體系，對恐怖組織造成嚴重打擊，並減少人員及有人戰機的消耗，在反恐戰爭中居於重要角色。無人機且可進行長時間廣範圍的空域與海域偵察及監視任務，以及地球資源探勘、災害勘察等，耐航時間可長達 10 餘小時、甚至 24 小時以上毋需落地，透過資料鏈將資料下傳至地面站，減輕人力負擔，未來無人機角色將進一步發展。美國已嘗試運用無人機進行空中攔截任務，⁸海軍已決定發展 MQ-25 艦載無人空中加油機，增加艦載機作戰範圍、減少艦上機隊調度負擔，未來也可能衍伸為匿蹤無人打擊機，與有人戰機搭配執行任務。MQ-25 採用原來 X-47B 成熟的自動著艦技術，可以透過機對艦的雙向資料鏈偵測航行中航空母艦的位置，不斷修正著艦點，以便自動著艦。MQ-25 雖為加油機，但美國海軍已放棄原來發展「無人艦載空中監視打擊」飛機（UCLASS）的計

⁷ “US military prepares for the next frontier: Space war,” *CNN*, November 29, 2016, <https://edition.cnn.com/2016/11/28/politics/space-war-us-military-preparations/index.html>。

⁸ “MQ-9 Gets First Air-to-Air Kill in Training Exercise, Air Force Official Says,” *Military.com*, September 19, 2018, <https://www.military.com/daily-news/2018/09/19/mq-9-gets-first-air-air-kill-training-exercise-air-force-official-says.html>。

畫，而獲選的波音 MQ-25 設計擁有極佳的匿蹤外型，故未來仍有衍生為無人打擊機的空間。

除大型無人機外，地面部隊已廣泛運用小型無人機執行戰場偵察等任務。美軍也嘗試運用集群式攻擊 (Swarm) 技術，使用大量小型無人機進行攻擊敵人的「自殺」任務。美軍也嘗試在飛機上施放小型無人機，例如 2017 年 1 月時，國防部戰略能力辦公室 (Strategic Capabilities Office) 與麻省理工 (MIT) 的林肯實驗室合作發展，以 F/A-18 戰機施放林肯實驗室發展的 Perdix 小型無人機，投放後自動化操作，可實施集群式攻擊等任務。⁹國防先進研究計畫署也在 2018 年 4 月以 C-130 運輸機，施放較大的「小精靈」(Gremlins) 無人機，由運輸機貨艙內施放，在視距外對敵境執行任務，飛行時間達 24 小時，並可回收再使用。¹⁰

海軍也運用艦載小型無人機，例如 MQ-8「火斥候」(Fire Scout) 無人直升機，可在驅逐艦或巡防艦等級的直升機甲板上起降，擔任偵察任務。另外也在發展其他型式的大型無人機，例如應用傾斜旋翼概念的貝爾 (Bell) V-247，衍生自較早期的「鷹眼」(Eagle Eye)；國防先進研究計畫署與海軍研究辦公室 (Office of Naval Research, ONR) 的「戰術利用偵察節點計畫」(Tactically Exploited Reconnaissance Node, TERN)，¹¹是一種更小型的無人機，讓所有不同型式的水面艦都可成為情報、監視、偵察與戰鬥用途的無人機母艦，搭載能在中高度持續飛行的無人機，增加海軍作戰能力。

海上獵殺者 (Sea Hunter) 也是由國防先進研究計畫署與雷神公司合作發展的無人水面載具，被稱為無人潛艦獵殺者。因許多國家都發展難以偵測的潛艦，威脅美國海軍水面艦部署，為防範水下威脅，美國海軍決定發展這種無人載具，現已進行海洋測試，未來可能進行作戰測試。¹²

⁹ “F-18 Fighter Jets and UAVs Join Forces in Air Force Test,” *Engineering*, January 14, 2017, <https://www.engineering.com/DesignerEdge/DesignerEdgeArticles/ArticleID/14092/F-18-Fighter-Jets-and-UAVs-Join-Forces-in-Air-Force-Test.aspx>。

¹⁰ “This Is Our First Glimpse of a DARPA Gremlins Drone Being Launched or Recovered From A C-130,” *thedrive*, April 11, 2018, <http://www.thedrive.com/the-war-zone/20058/this-is-our-first-glimpse-of-a-darpa-gremlins-drone-being-launched-or-recovered-from-a-c-130>。

¹¹ “DARPA asks Northrop Grumman to build second TERN prototype UAV to fly from small surface ships,” *Military & Aerospace Electronics*, June 20, 2016, <https://www.militaryaerospace.com/articles/2016/06/uavs-small-surface-ships.html>。

¹² “Sea Hunter: inside the US Navy’s autonomous submarine tracking vessel,” *Naval Technology*, May 3, 2018, <https://www.naval-technology.com/features/sea-hunter-inside-us-navys-autonomous-submarine-tracking-vessel/>。



圖 1-1、波音公司 MQ-25 概念已獲海軍採用
資料來源：舒孝煌攝。

(三) 新一代空戰平台

美國在匿蹤技術運用上領先世界，未來第 6 代戰機將有比現在更先進的匿蹤外型，雷達截面積較現在的第 5 代戰機更低。目前諾斯洛普格魯門正在發展新一代匿蹤轟炸機，即 B-21，將會擁有全翼構形，攜帶現有重型及長程武器，進行長程飛行，用以取代已經老舊的 B-52 及 B-1 轟炸機。

美國 6 代戰機的發展可能還言之過早。美國空軍「穿透性制空」(Penetrating Counter-Air) 及海軍 FA-XX 兩項計畫仍有待整合，但已開始發展未來關鍵科技，例如先進的多重可變循環發動機、機載雷射武器等。此外，美國空軍先進行現有戰機的性能提升，除決定為 F-22 進行性能升級，也考慮為 F-35 配備雷射武器。發動機大廠普萊特惠特尼 (Pratt & Whitney, PW) 計畫提升 F135 發動機推力，被稱為成長選項 2.0 (Growth Option 2.0, GO2)。這與未來在 F-35 配備直接能武器密切相關，美軍亦考慮為 F-35 配備極音速飛彈。



圖 1-2、美國 6 代戰機概念仍待整合
資料來源：波音公司。



圖 1-3、美售給英國的 F-35B 戰機

資料來源：舒孝煌攝。

（四）直接能（Direct energy）與電磁能（Electromagnetic）武器

雷射與電磁武器概念雖非新穎，確遲未實戰化。然不久的未來，這些武器將會實用化並開始部署。美國空軍曾將一架波音 747 客機改裝，改稱 YAL-1，做為空載雷射反飛彈系統的實驗平台，曾在 2010 年進行雷射測試，後因成本因素被取消。後來也曾在 AC-130 砲艇機上測試以雷射攻擊地面目標，稱為先進戰術雷射（Advanced Tactical Laser, ATL）。YAL-1 使用化學能雷射，國防先進研究計畫署與波音（Boeing）公司合作開發的雷射武器系統已經試射成功，將開始在船艦及軍用車輛上部署，正式名稱是「雷射武器系統」（Laser Weapon System, LaWS），曾於 2014 年在兩棲運輸艦龐斯號（USS Ponce）上配備雷射武器進行實驗。洛克希德馬汀公司的「高能雷射及整合監視及眩光器」（High Energy Laser and Integrated Optical-dazzler with Surveillance, HELIOS）則結合致命及非致命雷射，將可在 2020 年部署於海軍艦艇上。¹³

此外，美國防部也在發展可部署在陸地車輛上的固態雷射武器，包括波音的「高能雷射機動展示平台」（High-Energy Laser Mobile Demonstrator, HELMD）。未來雷射系統可更為緊緻化，搭載在史崔克輪型裝甲車上，機動性更佳。洛馬及雷神公司的團隊，目前聚焦於發展 100 千瓦的雷射，¹⁴其目的是用於對付「非對稱性威脅目標」，例如大批武裝無人機或快艇，造價便宜卻具有威脅性，若用導彈等高價武器對付這些威脅，付出的代價將過於昂貴。

¹³ “Star Wars At Sea: Navy’s Laser Gets Real,” *Breaking Defense*, December 10, 2014, <https://breakingdefense.com/2014/12/star-wars-at-sea-navys-laser-gets-real/>; “First Combat Laser For Navy Warship: Lockheed HELIOS,” *Breaking Defense*, March 1, 2018, <https://breakingdefense.com/2018/03/first-combat-laser-for-navy-warship-lockheed-helios/>。

¹⁴ “Lockheed-Dynetics team and Raytheon locked in battle to build 100-kilowatt laser for US Army,” *Defense News*, August 8, 2018, <https://www.defensenews.com/digital-show-dailies/smd/2018/08/07/lockheed-dynetics-team-and-raytheon-locked-in-battle-to-build-100-kilowatt-laser-for-us-army/>。

美國海軍在 2015 年就發展電磁軌道砲 (electromagnetic railgun) 成功，使用與單極馬達原理類似的電磁軌道裝置推動「砲彈」，不需使用火藥，射速可達音速 7 倍，射程可提高至 100 公里以上，除穿透能力驚人外，砲彈成本還相對便宜，若未來船艦動力系統能解決電力供應問題，將可能實用化。

(五) 極音速武器及長程打擊武器

由於擔心在極音速武器競賽中落後，美國空軍已將其置於最高優先。¹⁵美國過去曾發展數種設計，包括「極音速技術載具-2」(Hypersonic Technology Vehicle 2, HTV-2)、「先進極音速武器」(Advanced Hypersonic Weapon, AHW)，用以進行其全球打擊計畫。相較於俄、中，美國發展時程雖已落後，但可以採不對稱途徑，如整合導引極音速武器的感測器技術，以維持優勢。

為了加速推進極音速武器發展，美國國防部在 2018 年增加極音速技術投資，包括美國空軍的 2,000 萬美元，預計在 2020 年進行「極音速傳統打擊空射滑翔武器 (Hypersonic Conventional Strike Weapon, HCSW) 飛行測試，以及 6,500 萬美元發展陸基型武器。2018 年 4 月，美國空軍授予洛克希德馬汀 (Lockheed Martin) 10 億美元合約，進行 HCSW 的設計、整合及工程支援，8 月 14 日再獲一筆 4 億 8400 萬美元合約，發展另一型「空射快速反應武器」(Air Launched Rapid Response Weapon, ARRW)。¹⁶

另外，美國空軍、國防先進研究計畫署及雷神公司 (Raytheon) 也合作推動戰術推進滑翔 (Tactical Boost Glide, TBG) 計畫，預計在 2023 年發展出原型。為推動極音速載具研究計畫，2018 年 10 月 4 日，美國空軍賦予空軍實驗室 GOLancher1 (GO1) 極音速載具 X-60A 的實驗機編號，這是一枚空射式液態燃料火箭，用以研究在極音速飛行時衝壓推進發動機 (scramjet)、耐高溫材料及自動控制等技術。¹⁷

¹⁵ “Russia and China are 'aggressively developing' hypersonic weapons — here's what they are and why the US can't defend against them,” *CNBC*, March 21, 2018.

¹⁶ “Lockheed Martin gets a second hypersonic weapons contract, this time for \$480 million, as the US tries to keep pace with Russia and China,” *CNBC*, August 14, 2018.

¹⁷ “U.S. Air Force Designates GO1 Hypersonic Flight Research Vehicle as X-60A,” *88th Air Base Wing Public Affairs*, October 4, 2018, <https://www.wpafb.af.mil/News/Article-Display/Article/1653238/us-air-force-designates-go1-hypersonic-flight-research-vehicle-as-x-60a/>。



圖 1-4、美國空軍發展中的極音速實驗載具 X-60A

資料來源：USAF。

表 1-1、三次抵銷戰略

	年代	背景	重點項目
第一次抵銷戰略	1950s	艾森豪總統時代，透過美國核嚇阻能力，反制前蘇聯傳統武力的數量優勢。	核武
第二次抵銷戰略	1970s	時任國防部長布朗（Harold Brown）要求發展高科技武器，對抗華約部隊在歐洲的部署。	精準武器、匿蹤科技、情監偵系統。
第三次抵銷戰略	2016~	時任國防部長卡特撥款 36 億美元進行先進科技及創新作戰概念研究。	極音速武器、直接能或電磁武器、AI 人工智慧等。

資料來源：舒孝煌整理自 NDU Press，<http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-82/Article/793224/securing-the-third-offset-strategy-priorities-for-the-next-secretary-of-defense/>。

貳、中國

中國目前的大戰略是「強調國家利益的國際性，強調中國崛起背景下國家利益拓展的重要意義；強調主動性，要求把握在國家實力基礎之上的戰略主動權，為國家戰略利益的擴展服務。」¹⁸ 國際環境對中國的崛起相當重要，就建構中國國際安全環境而言，北京認為目前國際形勢正在演變，包括：國際實力對比、全

¹⁸ 王昆義，〈中國的國際戰略與一帶一路的形成〉，《台灣國際研究季刊》，第 12 卷第 3 期（2016 年秋季號），頁 24，<http://www.tisanet.org/quarterly/12-3-2.pdf>。

球治理體系結構、亞太地緣戰略局勢和國際經濟、科技、軍事競爭等，都正在轉變中。在可預見的未來，發生世界大戰的可能性不高，國際和平情勢仍會持續維持。然而，北京認為，美國霸權主義、強權政治和新干涉主義將會持續發展，各種國際權力和權益的再分配會趨於更競爭。此外，恐怖主義活動猖獗，民族宗教矛盾、邊界領土爭端復雜多變，小衝突不斷、危機頻繁仍是一些地區的常態，國際局勢依然面臨現實和潛在局部戰爭的危機。因此，確保國防與軍隊現代化乃是中國國防戰略的重要目標。

在 2017 年 10 月 18 日，習近平在中國十九大報告中指出，中國的國防與軍隊建設在面對國家安全環境的變化，和面對強國強軍的時代要求，必須全面貫徹新時代強軍思想，貫徹新形勢下軍事戰略方針，建設強大的現代化陸軍、海軍、空軍、火箭軍和戰略支援部隊，打造堅強高效的戰區合作指揮機構，建構中國特色的現代作戰體系。¹⁹該報告亦指出，為適應世界新軍事革命發展趨勢與國家安全需求，中國將提高軍隊建設的質量與效益，預計在 2020 年先基本實現機械化與信息化，以提升戰略能力；預計到 2035 年全面實現國防與軍隊的現代化，並成為世界一流軍隊。為了提升軍隊的質量，中國不僅將深化國防工業科技改革，也將強化軍民科技合作，建構一體化的國家戰略體系與能力。²⁰

一、中國的國防政策

中國所有武裝力量是由中央軍事委員會所指揮，採「黨指揮槍」的軍事領導體系，在國家安全和發展戰略全局中具有重要地位和作用。中國主要奉行防禦性的國防政策，而「積極防禦」主要中國的傳統軍事戰略的重要思想，由毛澤東所創，但在不同時期，積極防禦軍事戰略方針的內容有所不同，而且根據形勢的變化而不斷發展。²¹在 2015 年的《中國的軍事戰略》白皮書，中國提出了「新形勢下積極防禦軍事戰略方針」作為中國的軍事戰略方針。其戰略重點是：立足打贏「信息化局部戰爭」，創新基本作戰思想，優化軍事戰略布局，堅持戰略指導原則。²²

根據 2015 年《中國的軍事戰略》白皮書內容，中國國防的方針包括有下列幾項：²³第一、服從服務於國家戰略目標，貫徹總體國家安全觀，加強軍事鬥爭

¹⁹ <習近平：決勝全面建成小康社會，奪取新時代中國特色社會主義偉大勝利——在中國共產黨第十九次全國代表大會上的報告>，《新華社》，2017 年 10 月 27 日，
http://www.gov.cn/zhuanti/2017-10/27/content_5234876.htm。

²⁰ 同註 18。

²¹ “Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2018,” Office of the Secretary of Defense, May 16, 2018. p. 46-47.
<https://media.defense.gov/2018/Aug/16/2001955282/-1/-1/1/2018-CHINA-MILITARY-POWER-REPORT.PDF>。

²² “Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2018,” Office of the Secretary of Defense, May 16, 2018. pp. 2, 45-46, 73.
<https://media.defense.gov/2018/Aug/16/2001955282/-1/-1/1/2018-CHINA-MILITARY-POWER-REPORT.PDF>。

²³ 中國國務院新聞辦公室，《中國的軍事戰略》，2015 年 5 月 26 日，
www.scio.gov.cn/zfbps/ndhf/2015/Document/1435161/1435161.htm。

準備，預防危機、遏制戰爭、打贏戰爭。第二、營造有利於國家和平發展的戰略態勢，堅持防禦性國防政策，堅持政治、軍事、經濟、外交等領域鬥爭密切配合，積極應對可能面臨的綜合威脅。第三、保持維權維穩平衡，統籌維權和維穩兩個大局，維護國家領土主權和海洋權益，維護周邊安全穩定；努力爭取軍事鬥爭戰略主動，積極運籌謀劃各方向各領域軍事鬥爭，抓住機遇加快推進軍隊建設、改革和發展。第四、運用靈活機動的戰略戰術，發揮聯合作戰整體效能，集中優勢力量，綜合運用戰法手段；立足應對最複雜最困難情況，堅持底線思維，紮實做好各項準備工作。第五、充分發揮人民軍隊特有的政治優勢，堅持黨對軍隊的絕對領導，重視戰鬥精神培育，嚴格部隊組織紀律性，純潔鞏固部隊，密切軍政軍民關係，鼓舞軍心士氣。第六、發揮人民戰爭的整體威力，堅持把人民戰爭作為克敵制勝的思維，拓展人民戰爭的內容和方式方法，推動戰爭動員以人力動員為主向以科技動員為主轉變。第七、積極拓展軍事安全合作空間，深化與大國、周邊、開發中國家的軍事關係，促進建立地區安全和合作架構。

2015年9月習近平宣布裁軍30萬，吹響軍改號角，11月在「中央軍委改革工作會議」上強調，深化國防及軍隊改革是實現「中國夢」、「強軍夢」的時代要求，其後軍改正式展開，目的在「實施領導管理體制、聯作戰指揮體制改革」，以及「實施軍隊規模和作戰力量體系、院校、武警部隊改革，基本完成階段性改革任務」。

習近平軍改的目的包括政治上的「擴權」及軍事上的「強軍」，前者是要軍隊「聽黨指揮」，拔除舊體系，強化共黨對軍隊的控制，後者是要軍隊「能打勝仗」，強化解放軍的作戰能力，除裁撤4總部、建立陸軍指揮機構、裁撤原7軍區，建立5大戰區，以簡化指揮層級、擴建新式軍兵種及專業部隊，如火箭軍與戰略支援部隊，強化聯合作戰及快速反應能力、縮短指揮鏈、由軍委直接指導戰區，戰區再指揮麾下軍種協同作戰，將有助提升其作戰效能。

二、中國軍事科技趨勢

在中國國防戰略的指導下，中國軍事武器裝備走向遠程精確化、智能化、隱身化、無人化特色之趨勢相當明顯，太空和網路領域已經成為各方戰略競爭的新高地，現代戰爭形態也已經朝向信息化發展。世界主要國家正積極調整國家安全戰略和國防政策，加速推進軍事轉型並重建軍事力量體系。這些尖端軍事技術和戰爭形態的變化，對國際政治與軍事發展產生重大影響，對中國軍事安全而言是全新的嚴峻挑戰。為打造世界級軍隊，中國國防部在2018年1月25日正式頒發《新軍事訓練大綱》²⁴，軍隊將致力於打造「實戰化、聯合化、科學化、規範化的訓練內容體系和相關制度機制」，在實現國防和軍隊現代化目標下，中國計畫在未來20年內將軍隊建設成世界一流軍隊。近期中國重要軍事科技發展趨勢如下列所示：

²⁴ 馮人恭、曹昆，〈首批新軍事訓練大綱正式頒發〉，《人民網》，2018年01月26日，<http://military.people.com.cn/n1/2018/0126/c1011-29787749.html>。

(一) 極音速滑翔飛行器

中國號稱發展世界上第一種實戰型極音速武器，其所採用的方式是「推進—滑翔」方式，其載具進入大氣層以極音速飛行時是無動力，即所謂「極音速滑翔飛行器」(Hypersonic Glide Vehicle, HGV)。其新一代彈道飛彈東風 17，射程可達 2,500 公里，若搭載此類彈頭，將大幅提升中國對於周邊地區軍事目標的打擊能力，同時西方飛彈防禦系統將很難攔截。2017 年時曾進行兩次試射，均成功命中目標。若擴展到更長程的東風 31/41 洲際彈道飛彈，就有可能將目標延伸至美、歐洲大陸。

(二) 先進飛彈系統

中國致力於長程、精準打擊武器發展，除戰略嚇阻能力，尚擁有傳統飛彈武力，包括東風 15 (CSS-6)、東風 11 (CSS-7)、東風 16 (CSS-11) 等短程飛彈；東風 21 (CSS-5) 中程飛彈，以及東風 26、東風 31 及 41 等遠程或洲際彈道飛彈，以及各種長程巡弋飛彈。更具代表性的是如東風 21D、東風 26 等可打擊海上大型目標如航空母艦的反艦彈道飛彈，雖然其效能仍被懷疑。此外，中國亦以終端彈道機動、匿蹤等方式，強化其飛彈彈頭生存性，使其更難攔截。在攻陸巡弋飛彈 (LACM)，包括鷹擊 63、長劍 20 (長劍 10 的空射型，射程達 1,500 公里)、攻地 88 等空射巡弋飛彈，數量約 200 至 300 枚。中國可能在開發更長程的巡弋飛彈的同時，也發展各型對地攻擊及砲兵精準武器。

(三) 反潛監測

中國近年不但建造新一代傳統柴電動力潛艦及核動力潛艦，也建立所謂「水下長城」，即在主要海域如南海及渤海灣等海域，以及第一島鏈重要海域部署「水下聲音監測系統」，被稱為中國版的「反潛聲納陣列系統」(Sound Surveillance System, SOSUS)。這套系統曾在 2016 年時「十二五科技創新成就展」展出，顯示其構建水下監測網的企圖，其目的毫無疑問是要偵測美國海軍潛艦在西太平洋的活動，除讓美軍在中國周邊的潛艦行動將會無所遁形，藉此保護其航空母艦戰鬥群及戰略飛彈潛艦在近海航行安全。

(四) 太空與反衛星作戰

中國正強化運用太空，其戰略支援部隊任務之一即為太空。2017 年中國在西昌衛星發射中心以長征二號丙火箭發射「遙感 30 號」第 3 組衛星，將遙感 30 衛星網組建完成，共有 13 枚衛星組成星群，類似美國海軍的海洋監視衛星系統，可透過電磁與光學等相關技術對美軍的全球行動進行嚴密監視，掌握美軍主要艦艇位置。遙感 30 號 01 及 02 組衛星也由長征 2 號丙運載火箭，均在 2017 年發射成功，²⁵分別由中國科學院微小衛星創新研究院和中國運載火箭技術研究院研

²⁵ <遙感三十號 03 組衛星發射 可監視美艦介入台海>，《聯合報》，2017 年 12 月 26 日，

製，測控任務由西安衛星測控中心、中國衛星海上測控部和北京航天飛行控制中心共同完成。

反衛星作戰是不對稱作戰的一種模式，中國已經部署了兩套公路機動反衛星飛彈系統，可能是 KT-1 和 KT-2A 固體燃料火箭，搭載 DN-1/2/3 彈頭，為一種動能殺傷攔截器（Kinetic Kill Vehicle, KKV），具備反衛星能力，覆蓋低中高三種軌道，因採用固體燃料，可機動部署及應急發射。中國也發展新一代運載火箭，可能為長征 9 號，可舉升 25 噸物體進入登月軌道，或舉升 70 噸物體進入近地軌道。

（五）直接能及電磁武器

中國在直接能武器發展上正加快速度，2017 年中國科學院上海光機所「超強超短雷射」實驗裝置實現 10 拍瓦（Petawatt）輸出，可創造超強電磁場及超高能量，²⁶並計畫建造 100 拍瓦的設施。此一高能量的強雷射輸出，表面來看是為科學研究，但其技術也可轉用於軍事，並說明中國雷射裝置發展已有相當水準。中國也發展電磁軌道砲，並裝在 072III 型戰車登陸艦的前甲板上進行試驗，在此試驗上似領先美國。然而該武器顯然並非使用船艦本身主機提供電力，若中國未來水面艦艇主機能解決大量電力供應問題，就能實現艦砲反飛彈和超遠程水面精確打擊。

（六）匿蹤戰機及轟炸機

中國在作戰飛機上有快速發展，成都飛機公司研發的殲 20 戰機已開始少量生產及服役，可能仍在進行小規模修改與驗證。該機採用前翼設計，具優異匿蹤外型，具有三個彈艙，可能使用中國自製的電子掃瞄雷達。另一瀋陽飛機公司負責發展殲 11B、殲 16，以及海軍的殲 15，其 FC-31 目前僅 2 架原型機，有報導指出解放軍對殲 15 不滿，可能另選艦載機。但 FC-31 目前並未被解放軍接受，仍僅是瀋飛所自行發展。²⁷中國自製戰機最大問題為發動機，不但限制其性能，甚至影響飛安。中國另發展運 20 運輸機，與 IL-76 類似，若順利服役，將提升中國武力投射能力，另外中國也傳聞在發展轟 20 大型匿蹤轟炸機，外型可能接近美國 B-2 轟炸機或是 X-47B 實驗機的放大版，亦可增加中國將打擊力量投射至西太平洋，不過技術挑戰必然甚高。

（七）海軍新航空母艦、驅逐艦、兩棲突擊艦

中國海軍近年朝向藍水發展，除持續派遣艦艇遠赴亞丁灣參與護航行動，獲取遠洋作戰經驗外，也發展新式大型水面艦艇 055 型，配備垂直發射系統及大型相位陣列雷達，未來除獨自進行作戰外，可做為海軍航空母艦戰鬥群的護航艦使

<https://udn.com/news/story/7331/2895627>。

²⁶ <上海“超強超短激光”實現 10 拍瓦放大輸出>，《新華網》，2017 年 10 月 28 日，
http://big5.xinhuanet.com/gate/big5/www.xinhuanet.com/mrdx/2017-10/28/c_136711400.htm。

²⁷ <殲 15 事故頻日媒曝艦載機缺陷>，《青年日報》，2018 年 7 月 8 日，
<https://www.ydn.com.tw/News/296002>。

用。中國自行建造的國產航艦已經下水，並已進行達3次海試，但似尚未有艦載機起降跡象。中國已在葫蘆島興城基地進行陸上彈射起飛試驗，顯示中國下一艘航艦有可能採用彈射系統，增加航艦作戰效率。但目前最大問題是艦載機，殲15戰機仿自俄Su-33，性能仍不可靠。若不能解決艦載機問題，航艦將無法發揮作戰效率。另中國正建造075兩棲突擊艦，搭載約30架直升機，具直通式泛水甲板，可搭載氣墊登陸艇，排水量達4萬噸，建造數量可能為3艘。若建造完成，將對其兩棲登陸作戰模式造成極大改變。²⁸

（八）無人機發展

中國無人機已有長足化發展，並出售給中東國家。除軍用外，中國也已是民用無人機最大輸出國，其無人機型別多元，且可執行各種不同任務。在2018年11月於廣東珠海舉辦的「中國國際航空航天博覽會」（一般稱為珠海航展）展出多種無人機及無人飛彈快艇，另有「彩虹7」匿蹤無人機，具極佳全翼匿蹤外型，據稱可用以穿透敵防空網，打擊高價值目標。其外型類似美X-47B，日本媒體批評該機一望即知是盜竊智財權的成果。中國另也展出各種不同型式的集群式無人機系統。其中較大型的「蜂群」無人機系統，有大型的MR-150及小型的MR-40兩種，均為4軸式無人機，搭載反戰車火箭，可用以對敵地面目標進行集群式攻擊。另外也有具匿蹤外型的JY-300無人預警機，與彩虹4型大小相當，可進行長時間對空偵測及預警。除此之外，尚有多型具類似傾斜旋翼設計的無人機，應可供在船艦上操作。除此之外，中國已有多型大型無人機，如翔龍無人機，具有菱形機翼，可用於長程中繼目標標定；利劍無人機，亦採匿蹤外型，與彩虹7型外觀近似；多種中型無人機如彩虹3、彩虹91、92、901、刀鋒、ASN系列等多種型式，可能多達數十種，甚上百種以上，然種類雖多，未必表示能如美軍中東戰場那般順利遂行作戰任務。

參、俄羅斯

俄羅斯受其地緣條件影響，國防向來將擴大防衛縱深，視為保護其國界安全之重要基礎，針對周邊各國採取不同策略來謀取其國家安全利益。在與北約對峙的西界，須防止接壤的烏克蘭、白俄羅斯倒向西方。在南方則交好土耳其與伊朗，並干涉敘利亞，同時透過政軍經合作維持在中亞之影響力。在遠東，持續以北韓無核化與北方四島等議題作為對日籌碼、藉由軍演與共同開發合作案來聯合中國對抗美日，同時也不忘維持對蒙古、北韓之雙邊關係牽制北京。

俄羅斯在冷戰後與美國之間的戰略制約基礎，不斷受到美國所開發之反飛彈防禦系統侵蝕，而北約東擴與中國軍事現代化，以及俄國自身戰略武器老舊，都為其防務帶來挑戰。再者，2014年俄國占領克里米亞遭西方經濟制裁以來，俄國

²⁸ <可變身輕航母陸075兩棲攻擊艦年底亮相>，《中時電子報》，2017年10月25日，
<https://www.chinatimes.com/realtimenews/20171025002814-260417>。

經濟動能趨緩，在投入資源受到限縮的情況之下，實現軍民兩用的戰略性武器現代化，發展「創新不對稱」能力成為當前最重要的課題。

一、俄羅斯國防政策

俄羅斯並沒有發表國防白皮書之慣例，然其與之功能相近的官方報告書，為不定期對外發布的《俄羅斯聯邦國家安全戰略》(National Security Strategy of Russian Federation)以及《俄羅斯聯邦軍事準則》(The Military Doctrine of Russian Federation)，同樣具有戰略方向擬定、指導國防建設方向之功能。兩者目前最新版本分別為《2014年俄羅斯聯邦軍事準則》²⁹以及《2015年俄羅斯聯邦國家安全戰略》。³⁰

《2014年俄羅斯聯邦軍事準則》將北約東擴視俄國主要的外部軍事威脅，尤其是外國部隊、反彈道飛彈系統之部署持續近逼其邊界，已成為首要考量。如何防止外部因素導致俄國社會與軍隊失序、確保戰略核武優勢，儼然成為軍備重點。《2015年俄羅斯聯邦國家安全戰略》明確點名美國及其盟國企圖干預俄羅斯內政與外交的獨立性，試圖藉著在政治、經濟、軍事、資訊四個方面圍堵俄國來維持西方對全球事務的主導權。俄國自認所處安全環境，正因大國對於天然資源的爭奪持續惡化，並特別指出北極為競爭重要區域。³¹此外，由於衛星裝備老化與火箭發射問題，2014-2015年俄羅斯長程彈道飛彈太空預警能力曾出現近一整年的缺口，一度被認為是重大國防危機。³²

為突破西方2014年以來在經濟與安全上的包圍態勢，俄羅斯未來國防資源的挹注將有兩大重點：一為以軍事工業發展帶動工業現代化與科技創新、注重軍民兩用之科技，並重振軍火出口。³³二於「戰略核三角」(nuclear triad)持續投入能量，為確保北約無法削弱其戰略打擊能力。

二、俄國軍事科技趨勢

2018年2月則通過《俄羅斯2018-2027武器綱要》(The Russian State Armament

²⁹ 2014年12月25日俄羅斯總統普丁簽署通過，俄文版參見

http://64.mchs.gov.ru/upload/site53/document_text/002/534/218/ihgiu.rtf。英文版參見 <https://rusemb.org.uk/press/2029>。

³⁰ 2015年12月31日俄羅斯總統普丁簽署通過，原版參見

<http://static.kremlin.ru/media/events/files/ru/l8iXkR8XLAtxeilX7JK3XXy6Y0AsHD5v.pdf>。

³¹ 呼應2013年2月20日俄羅斯總統普丁簽署通過的《2020年前俄聯邦北極地區發展戰略與國家安全保障戰略》(The Development Strategy of the Arctic Zone of Russian Federation and National Security for the Period Up to 2020)。英文版參見

<http://www.iecca.ru/en/legislation/strategies/item/99-the-development-strategy-of-the-arctic-zone-of-the-russian-federation>。

³² “Russia's Satellite Nuclear Warning System Down Until November,” *The Moscow Times*, June 30, 2015, viewed September 30, 2018, <https://themoscowtimes.com/articles/russias-satellite-nuclear-warning-system-down-until-november-47799>。

³³ 俄國2013-17年軍火出口相較於2008-12年，大幅衰退7.1%，參見“Trends in international arms transfers, 2017,” *SIPRI*, viewed March, 2018, viewed September 29, 2018 https://www.sipri.org/sites/default/files/2018-03/fssipri_at2017_0.pdf。

Programme 2018 – 2027)，³⁴該報告具體指出未來 10 年俄國軍備發展趨勢。³⁵俄國未來 10 年將投入 19.3 兆盧布（約 3570 億美元），按照《俄羅斯 2018-2027 武器綱要》來建設國防資源；其中除約 1 兆盧布用於建設軍事基礎設施，其餘全數投入研發採購與後勤維修。³⁶其中，戰略武器、極音速武器、戰略預警系統，更是重中之重。

（一）戰略武器

水下部分，「亞森」級（Yasen-class）與「北風之神」級（Borei-class 995A/995B）戰略核子潛艦將陸續服役。2025 年將可搭載 32 枚巡弋飛彈的 885 型「亞森」級（Yasen-class）多用途攻擊核潛艦，從現有的 1 艘增加至 7 艘。2024 年後，「北風之神」A 型（995A）與「北風之神」B 型（995B）戰略核子潛艦將從現有 3 艘提升到 8 艘，每艘搭載 16 枚「布拉瓦」潛射洲際彈道飛彈（Bulava，北約代號：SS-N-32）；單枚布拉瓦飛彈可攜帶威力達 150 千噸黃色炸藥的多目標核彈頭或 10 枚極音速彈頭，也就是說每艘北風之神潛艦將能發射 160 枚高超音速武器，確保美國飛彈防禦系統無法攔截；其中一半或將部署在太平洋艦隊。

空中部分，未來 10 年將量產 Tu-160 轟炸機來維持戰略投射能力。原本備受矚目的匿蹤轟炸機 PAK-DA 受限於預算，其量產將延至 2027 年後。此外，30 架服役中的 Tu-22 M3 逆火式（Backfire）超音速轟炸機，也將於 2020 年前升級為 Tu-22 M3M。Tu-95MS 熊式（Bear）戰略轟炸機以及 Tu-160 海盜旗（Blackjack）戰略轟炸機，則將進行發動機、電戰系統與武器裝備升級，並配備彩虹設計局（Raduga）發展的，具匿蹤外型的新式 Kh-101/ Kh-102 巡弋飛彈。

長程巡弋飛彈方面，主要是以射程 4,500 至 5,500 公里的 Kh-101 巡弋飛彈逐漸汰換射程 3,000 公里的舊型 Kh-55 巡弋飛彈，能夠搭載核彈頭的版本 Kh-102，也將取代原有的 Kh-555。

洲際彈道飛彈方面，可攜帶 3-6 枚核彈頭的「亞爾斯」洲際彈道飛彈（Yars/RS-24），最遠射程可達 11,000 公里，目前 73 枚已陸續服役，預計將在下一個十年完全取代「白楊」（Topol）與「白楊 M」（Topol-M）洲際彈道飛彈。而原本倍受矚目、以陸基鐵路系統發射的「邊界」洲際彈道飛彈（Rubezh/RS-26）研發計畫，則因經費遭「先鋒」極音速飛彈排擠，遭延後至 2027 年。³⁷第五代重型液態燃料

³⁴ Арматы, “Сарматы' и 'Цирконы': каковы приоритеты госпрограммы вооружения до 2027 года,” TASS, January 30, 2018, viewed September 30, <https://tass.ru/armiya-i-opk/4911274>。

³⁵ 根據儘管掌管國防工業的俄羅斯副總理羅戈辛（Dmitry Rogozin）的說法，這份每 5 年出版一次的報告，原訂於 2016 年完成，礙於 2014 年俄羅斯遭西方經濟制裁、石油價格下跌等因素影響，遲至今年才出版，參見“‘What froze Russia-NATO council and how a missile dispute impacts sanctions,’” TASS, 2018 February 26, viewed September 29, <http://tass.com/pressreview/991544> 以及“‘Putin signs new State Armaments Programme,’” Jane’s 360, 2018 February 28, viewed September 29, <https://www.janes.com/article/78235/putin-signs-new-state-armaments-programme>。

³⁶ “The Russian State Armament Programme 2018 – 2027,” NATO Defense College, May 3, 2018, viewed 2018 September 29, <http://www.ndc.nato.int/news/news.php?icode=1167>。

³⁷ “Avangard hypersonic missiles replace Rubezh ICBMs in Russia’s armament plan through 2027,”

戰略飛彈「薩爾馬特」(Sarmat/RS-28)，重 200 噸，投射重量 10 噸。³⁸2017 年 12 月完成首次試射、2018 年進行多次發射實驗，預計最遲 2021 年服役。2018 年 3 月 1 日普丁在國情咨文中，即曾提到「薩爾馬特」飛彈。³⁹

(二) 先進極音速武器

莫斯科企圖將極音速飛彈類型與數量多元化，來抵銷美國近年來藉飛彈攔截系統所帶來之戰略優勢。對於各國現有防空系統來說，大氣飛行速度 20 馬赫的「先鋒」先進極音速飛彈 (Avangard)、10 馬赫的「匕首」先進極音速飛彈 (Kinzhal/KH-47M2)、8 馬赫的「鋁石」先進極音速反艦飛彈 (Zircon)，⁴⁰皆難即時防禦。俄國宣稱「先鋒」不僅能躲避戰略衛星偵測，還能實施精準打擊。⁴¹

(三) 戰略預警系統

目前服役中的「聶伯」(Dnepr) 飛彈預警雷達共設置於四處：西伯利亞的伊爾庫斯克 (Irkutsk)、哈薩克的巴爾喀什 (Balkhash)，北極圈內的莫曼斯克 (Murmansk) 和克里米亞的塞凡堡 (Sevastopol)，其中塞凡堡一處年久失修。俄羅斯當局改設新型「沃羅涅日」長程飛彈預警高頻雷達系統 (Voronezh-SM)，偵測高度達 8000 公里，偵測範圍最遠 6000 公里，可加強防衛縱深。俄羅斯全境「沃羅涅日」雷達的部署數量由 2017 年的 4 具提高到 2018 年底的 10 具，算是完成「沃羅涅日」雷達網之初步建置。未來隨著部署地點增加，俄國本土的長程飛彈預警系統將更加完備。⁴²

在未來十年內，俄國下一代全球長程彈道飛彈預警衛星網「統一太空系統」衛星系統 (ESK Satellite System，以下簡稱 ESK 衛星系統) 能否順利取代陸續退役的「眼睛」衛星系統 (Oko Satellite System)，將是莫斯科所關心的國防重點項目。⁴³由俄「彗星中央科學研究院」(TsNIKOMeta) 研製的 ESK 衛星，屬於「凍原軌道衛星」(Tundra Orbit)，⁴⁴能在敵方彈道飛彈起飛後迅速偵測，並預先計算

TASS, March 22, 2018, viewed 2018 September 30, <http://tass.com/defense/995628>。

³⁸ “Russia preparing Plesetsk spaceport infrastructure for Sarmat ICBM flight tests,” TASS, July 20, 2018, viewed September 30, 2018, <http://tass.com/defense/1014234>。

³⁹ 《俄國防部完成洲際彈道導彈「薩爾馬特」的系列彈射試驗》，《俄羅斯衛星通訊社》，2018 年 7 月 18 日，<http://big5.sputniknews.cn/military/201807181025912696/>。

⁴⁰ “Russia’s hypersonic Zircon anti-ship missile reaches eight times speed of sound,” TASS, April 15, 2017, viewed September 30, 2018, <http://tass.com/defense/941559>。

⁴¹ “US intelligence reports: Russia’s new hypersonic weapon will likely be ready for war by 2020,” CNBC, May 15, 2018, viewed September 30, 2018, <https://www.cnbc.com/2018/05/15/russia-hypersonic-weapon-likely-ready-for-war-by-2020-us-intel.html>。

⁴² “Ideal Place’: Russia to Deploy Next Gen Missile Warning Radar in Crimea,” *Sputnik International*, August 19, 2017, viewed September 30, 2018, <https://sputniknews.com/russia/201708191056602007-russia-crimea-radar/>。

⁴³ ESK 為俄文「ЕдинаяКосмическаяСистема」之縮寫，意思為「統一太空系統」。

⁴⁴ 凍原軌道衛星有著較高傾角、高橢圓的地球同步軌道，軌道周期為一個恆星日 (Sidereal Day)，具有「遠地點駐留」(apogee dwell) 的特性，參見 <http://www.americaspace.com/2013/10/18/sirius-rising-proton-m-ready-to-launch-digital-radio-satellite-into-orbit/>。

其飛行軌跡參數與打擊地點，並同時透過戰鬥指令傳輸系統，將反擊命令迅速發布給負責防禦的反彈道飛彈部署基地，爭取有效反制之時間。⁴⁵2012 至 2017 年間，北約已知俄羅斯發射的軍事衛星共有 55 枚，其中多半是汰舊換新。俄國第一顆 ESK 衛星於 2015 年 11 月被送入軌道，俄國官方宣布將在 2021 年完成至少 10 枚 ESK 衛星發射，完成 ESK 衛星系統初步建置。然而北約觀察，由於發射進度落後，建成時間點可能延後。⁴⁶

（四）新一代作戰飛機

俄羅斯空軍作戰飛機發展已落後美國，甚至中國。其新一代戰機已命名為 Su-57，已進行多次試飛，具有一定程度匿蹤設計，並具有機腹彈艙。但與美國的 F-22、F-35 或是中國的殲 20 戰機相較，顯然在減少雷達反射截面積設計上較不出色。目前俄羅斯僅小規模採購，有報導指俄羅斯官方承認該型機失敗，不確定該機是否會進入量產。⁴⁷俄羅斯仍在採購 Su-30SM，其數量甚至較 Su-35 多，可能反映其預算不足窘況。不過也有報導稱，俄正尋求建造新航空母艦，並發展新戰鬥機，有可能類似 F-35，具備垂直／短場起降技術。⁴⁸

肆、北約各國

自蘇聯解體以來，原先以對抗蘇聯華約集團為其核心使命的北大西洋公約組織(North Atlantic Treaty Organization, NATO)之定位開始轉變，其所處的安全環境變得極為多元且複雜。不論是在巴爾幹地區及阿富汗的維和工作，還是 911 事件等，皆顯示當前北約面對的安全環境不同於以往。

冷戰結束後北約的戰略思想經歷三次轉變，1991 年時開始透過與過去對手的合作擴大與改善歐洲的安全，並減少核武運用；1999 年時的戰略構想則藉由廣泛的安全定義，重視政治、經濟、社會與環境等層面，面對後冷戰時期包含恐怖主義、種族、人權、經濟及大規模毀滅性武器的擴散等新時代威脅。911 事件之後，恐怖主義與大規模毀滅性的威脅成為重中之重，北約再次調整其結構與能力。2010 年里斯本峰會中提出的「主動接觸、現代國防」(Active Engagement, Modern Defence)，為目前北約的核心戰略概念，並延伸出三大核心任務「集體防衛」(collective defence)、「危機管理」(crisis management) 及「合作性安全」(cooperative security)。

近年包含敘利亞內戰及烏克蘭危機等事件影響，西方與俄羅斯的關係日趨惡

⁴⁵ “Russia’s Soyuz launches EKS Missile Warning Satellite, ends Year-Long Military Launch Gap,” *Space Flight 101*, May 25, 2017, viewed September 30, 2018, <http://spaceflight101.com/soyuz-successfully-launches-second-eks-satellite/>。

⁴⁶ “The Russian State Armament Programme 2018 – 2027,” p.5, NATO Defense College, May 3, 2018, viewed September 29, 2018, <http://www.ndc.nato.int/news/news.php?icode=1167>。

⁴⁷ “Russia Basically Just Admitted Its Next-Generation Stealth Fighter Is A Failure,” *Business Insider*, July 13, 2018, <https://taskandpurpose.com/su-57-stealth-fighter-failure/>。

⁴⁸ “Russia Wants New Aircraft Carriers and a New Fighter Jet That Has Something in Common with the F-35,” *National Interest*, September 14, 2018, <https://nationalinterest.org/blog/buzz/russia-wants-new-aircraft-carriers-and-new-fighter-jet-has-something-common-f-35-31247>。

化，然而在歐洲長時間裁軍與縮減國防預算情況下，美國開始敦促歐洲各國增加軍費支出。在 2014 年的北約威爾斯高峰會中，各國達成設立快反部隊「高度戰備聯合特遣隊」(Very High Readiness Joint Task Force, VJTF) 及各國將逐步提高國防預算至 GDP 的 2%，其中 20% 費用投入主要裝備投資等各項協議以應對當前問題。然而在軍事投資上各國的進展不一，美國川普總統上任後更對此加強施壓，如於 2018 年 7 月的北約布魯塞爾高峰會上要求盟國將軍費提高到該國 GDP 的 4%，並引發內部的不和諧。然而在內外的不同壓力之下，北約各國在軍事科技上仍各擅勝場，持續推出新技術與優異裝備，本報告將近期美國以外北約國家的軍事科技發展集中於此節呈現。

一、北約防衛政策

北約透過諸如個人自由、民主、人權、法制等共同價值觀為基礎，確保其成員國之安全；除了捍衛領土之外，在必要時投射價值至外部，管理與預防危機，穩定衝突結束後之情勢並支援重建。然而其安全政策必須隨著當前複雜的安全形勢不斷變化；如同前述 2010 年的戰略原則，北約目前的三個核心任務主軸仍將傳統的集體防衛放在首位，這項任務在近年北約與俄羅斯關係惡化後更形重要。集體防衛代表當對其中一個盟友的攻擊等於對所有成員國的攻擊，這項原則載於北約成立的「華盛頓條約」(Washington Treaty，又稱「北大西洋公約」North Atlantic Treaty) 第五條，該條文並在 911 事件後首次被援用。除此之外，北約在後冷戰時期有過多次集體防禦行動，並在 2014 年針對俄羅斯兼并克里米亞及因應伊斯蘭國等威脅加強集體防禦，增設多國快反部隊並前進部屬至波羅地海國家及羅馬尼亞等地；2016 年之後更將網路防禦視為其新的任務場域之一。

二、北約的軍事科技趨勢

北約近期的軍事科技發展，除具有歐洲特殊的地緣政治需求、也反映歐洲的國防需要。另外，由於對未來戰場的預測有其相似性，並需考量與美國的協同作戰，北約各國在軍事科技上的發展也可尋得與美俄等強權接近的脈絡。近期歐洲國家科技的若干趨勢如下：

(一) 下一代戰機

當前歐洲「六代戰機」的概念已逐漸地浮上檯面。若干軍事工業公司或集團，例如：貝宜集團(BAE System)與瑞典 SAAB，及法德兩國的航空工業等目前皆有類似構想，強調整合的「未來空中戰鬥系統」(future combat air system, FCAS)概念。2018 年 7 月在英國法茵堡航空展 (Farnborough Airshow) 所展出由貝宜聯合多家廠商推出的「暴風」戰鬥機概念即是一最佳範例，運用無人駕駛、人工智慧控制、與機器學習打擊目標、甚至與無人機系統等聯合等最新科技趨勢，讓未來的戰機不再僅是單一戰機，而是融合包括有人與無人等裝備在內的「系統」。貝宜的設計保留雙垂直尾翼，主翼則採用類似三角翼的概念，機翼後緣有雙重後掠

角，並採用雙發動機。若干軍事武器科技評論其比較類似歐洲版的五代半戰機。

然而，該戰機的先進之處不在於它的外型，而是其整體航電及武器設計，以及生產與後勤補給等。貝宜公司便指出，其未來戰鬥機的概念應該包括先進動力及推進系統、自動化地面支持系統、數位化生產程序及自動化機器人等設計與元素。在機體上則是先進無線射頻感測器、新一代飛控系統、平衡的可生存性設計、分散式多重光譜感測器、整合式感測器及下一代反制措施、以及擴增實境（Augmented Reality）座艙等等。

英國是接著法國與德國的計畫與合作發展新戰機之後，第二個提出新一代戰機的歐洲國家。近年英法開始共同開發 FCAS，然由於英國在 2016 年決定脫歐而無以為繼，法國與德國因此決定共同開發下一代戰機；⁴⁹而英國和義大利曾經在龍捲風戰鬥機、颱風戰鬥機、及 F-35 戰鬥機等計畫上有過緊密的合作，許多軍事科技公司與集團認為貝宜公司這樣的合作發展構想，應該可以獲得歐盟的支持，推出暴風式戰機，並認為可能爭取到包含瑞典、日本、土耳其等其他盟國支持計畫。貝宜的暴風戰機研發團隊包括 MBDA 所提供空載雷射武器概念，李奧納多在蘇格蘭的研究工廠除進行雷射研究之外，也投注發展無人機控制的技術，勞斯萊斯則準備發展下一代的動力系統。而法德方面的 FCAS 則在 2018 年 4 月柏林航展上正式簽署協議由法國達梭（Dassault）與德國方面的空中巴士集團合作進行，並由法德國內多家航空、電子與發動機等企業參加進行合作；⁵⁰然法德合作的計畫目前仍不若貝宜的暴風機計畫般，已展出等比例的概念模型。保守來看，這些北約國家所計畫合作研發的第六代戰機仍須十餘年以上的研發、測試才可能實際進入量產服役，故而各計畫的合作與構形仍可能在未來經歷多次變更。

相較於著眼未來戰場的第六代戰機計畫，同屬北約國家的土耳其的第五代匿蹤戰機 TFX 計畫案已開始多年。從目前公佈外型看，為具有相當程度匿蹤設計之雙發重型戰鬥機，土耳其方面於 2018 年 10 月 31 日並決定採用美國通用電氣（General Electric）的 F110 引擎。⁵¹

⁴⁹ Pierre Tran, "France and Germany agree to jointly build new generation fighter jet," *Defense News*, July 14, 2017, <https://www.defensenews.com/air/2017/07/14/france-and-germany-agree-to-jointly-build-new-generation-fighter-jet/>。

⁵⁰ "Dassault Aviation and Airbus join forces on Future Combat Air System," Dassault Aviation, April 25, 2018, <https://www.dassault-aviation.com/en/group/press/press-kits/dassault-aviation-airbus-join-forces-future-combat-air-system/>。

⁵¹ BurakEgeBekdil, "General Electric beats Rolls-Royce to power Turkey's indigenous fighter jet," *Defense News*, October 31, 2018, <https://www.defensenews.com/industry/2018/10/31/general-electric-beats-rolls-royce-to-power-turkeys-indigenous-fighter-jet/>。



圖 1-5、法國達梭公司展出的新一代戰機概念 NGF

資料來源：Dassault，

<https://www.dassault-aviation.com/en/group/news/euronaval-2018/>。

（二）強化傳統裝甲部隊

近年由於來自俄羅斯的威脅增加，加以俄國新式的 T-14 Armata 戰車的研發，使得北約歐陸各國雖然擁有如豹 II (Leopard 2)，雷勒克 (Leclerc) 等高性能主力戰車，裝甲部隊仍有提升的必要。德國克勞斯—馬費—威格曼 (Krauss-MaffeiWegmann, KMW) 與法國 NEXTER (原 GIAT 地面武器工業集團) 兩大地面武器公司所合組的 KNDS (KMW+Nexter Defense Systems) 在 2015 年成立，以開發德法下一代主力戰車為目標。雖然在 2018 年歐洲防務展 (EuroSatory 2018) 中曾展出以豹 II 車體結合雷勒克砲塔的混合戰車，然此款車僅為概念，而非實際產品。⁵²同時德國萊茵金屬 (Rheinmetall) 公司亦於 2016 年時宣布其正在研發下一代 130 公厘滑膛戰車砲，預估其發射穿甲彈的穿甲能力比現有 120 公厘/55 倍徑戰車砲多出 50%，能有效對抗俄國的新式主戰車。⁵³此外，北約各國目前亦有多種主動防禦系統 (Active Protection Systems, APS) 推出，以對抗現代戰場極度發達的反戰車武器。

除了重達 60-70 噸的西方高性能主戰車外，北約各國近來亦持續有廠商研發重量較輕的戰車，以因應可能難以操作主力戰車的作戰地形。除早先瑞典 CV-90 衍生之搭載戰車砲的版本外，2018 年歐洲防務展中與奧地利、西班牙合作研製的 ASCOD 等步兵戰鬥車亦推出衍生之中戰車，土耳其 Otokar 也推出一搭載 105mm 戰車砲、可使用砲射飛彈的 TULPAR 輕戰車。⁵⁴另外，萊茵金屬公司針

⁵² Nicholas Fiorenza, "EuroSatory 2018: KNDS presents joint Franco-German tank demonstrator," *Jane's 360*, June 13, 2018, <https://www.janes.com/article/80889/eurosatory-2018-knds-presents-joint-franco-german-tank-demonstrator>。

⁵³ "EuroSatory 2016: Gun for future tanks," *Jane's 360*, June 13, 2016, <https://www.janes.com/article/61205/gun-for-future-tanks-es2016d1>。

⁵⁴ "EuroSatory 2018: Latest innovations in tracked and wheeled armored vehicles," *Army Recognition*, June 21, 2018, https://www.armyrecognition.com/eurosatory_2018_official_news_online/eurosatory_2018_latest_in

對機械化步兵市場需求推出了該公司宣稱第一款針對未來戰場設計的步兵戰鬥車 KF-41 Lynx，在設計時就納入高度模組化概念，以針對不同的需求更換其裝備，同時在防禦面上亦考量對簡易爆炸裝置（Improvised Explosive Devices, IED）等武器的防禦，以及搭配主動防禦系統等設備。該公司正以此積極參與美國正在進行的下一代戰鬥車輛（Next-Generation Combat Vehicle, NGCV）計畫。

（三）歐洲無人載具與反無人機技術

歐洲在小型無人機上有一定發展之外，在大型飛行無人機方面，當前值得注意的已發展一段時日的大型匿蹤戰鬥無人機，如法國達梭公司過去開發的 Neuron 及英國的 Taranis 等，並持續與各國廠商合作發展下一代無人戰鬥空中載具（Unmanned Combat Air System, UCAS）。2018 年 10 月下旬該公司在歐洲海事防務展（Euronaval 2018）中除了展出下一代戰機 NGF 外，亦表明無人空戰系統將可能與有人戰機連結；⁵⁵空中巴士（Airbus）集團亦於 2018 年 9 月測試無人機與有人飛機的整合。⁵⁶除了航空系統之外，地面無人載具 UGV（unmanned ground vehicle, UGV）亦是當前積極發展的領域之一，其中包含愛沙尼亞 Milrem 自行研製以及其與歐洲各國廠商共同研發的系統在內，目前已可見到多種無人地面載具產品，並能涵蓋偵、監、後勤，甚至搭載武裝與敵人交戰等任務。雖目前對於無人機、甚至 AI 操控無人機搭載武器攻擊等領域仍有道德與倫理上的疑慮與討論，然目前此領域的發展仍然十分蓬勃。

與無人載具相對的，則是反無人機技術。由於當前各種高價精密以及小型廉價的無人機受到大量採用，已可預見其將成為未來戰場上的其中一支主角之一。其中小型無人機具隱密性、廉價，如能發展集群式攻擊技術，則除了能進行精密複雜的任務外，龐大數量與其低廉造價，將使得以防空飛彈攻擊在成本效益上極度不划算。萊茵金屬公司的 Skyranger 防砲車以及 MBDA 的 CAMM（Common Anti-Air Modular Missile）飛彈即考量了對抗小型無人機的需求。但除此之外，目前已有各種專門對抗無人機的方式出爐，例如藉由「干擾槍」以發送干擾訊號、切斷無人機與控制機構的連線；除了以切斷敵對無人機控制訊號的方式進行干擾外，亦有廠商開發專門用於捕捉無人機之無人機系統。

（四）歐洲下一代海上作戰系統

除了陸空裝備外，北約主要國家的海上裝備目前也正開始進行下一階段裝備更新。當前焦點為英國的「全球作戰艦」（Global Combat Ship）⁵⁷，「全球作戰艦」由貝宜公司發展，為一高度模組化、具多任務彈性及升級空間的大型巡防艦，並

novations_in_tracked_and_wheeled_armored_vehicles.html。

⁵⁵ “Dasault Aviation Presents Rafale Successor Concept At Euronaval Exhibition,” *Defense World*, October 24, 2018. <http://www.defenseworld.net/news/23559#.W-Pq25MzaUk>。

⁵⁶ “Airbus conducts MUT test flights,” *Shephard Media*, October 4, 2018, <https://www.shephardmedia.com/news/uv-online/airbus-conducts-mut-test-flights/>。

⁵⁷ 英國海軍給予其所採用的版本 Type 26 級巡防艦之型號名稱。

已獲澳洲及加拿大青睞。除此之外，英國海軍尚在計畫另一較小型的 Type 31e 型巡防艦，然其仍在接受各方初期投標之階段，仍有極高不確定性。

法國除近年與義大利合作的 FREMM 巡防艦外，目前正在進行 FTI 中尺寸巡防艦的研發，此約 4000 噸級的模組化多功能巡防艦預計，將取代剩餘的拉法葉級 (Classe La Fayette)。2018 年 10 月的歐洲海事防務展展出的 FTI 巡防艦已重新設計外型增加匿蹤能力，並將高度數位化，藉各種先進的智慧模組及感測器為核心，設置數位戰中心遂行系統管理及內部保護。⁵⁸法國在該展會場也宣布開始新式航艦計畫的研究階段，此艦未來將搭配目前研發中的次代戰機，用以取代目前服役中之戴高樂號航艦 (Charles de Gaulle)，然而此型艦艇的雛形仍待法國方面研究。⁵⁹德國當前也正在進行下一代多用途作戰艦艇 MKS 180 的競標工作，預計將可能造出較現有薩克森級 (F124 Sachsen Klasse) 巡防艦更大型的主戰艦艇，並預計加強網路安全等考量。但由於先前 F125 級巡防艦的建造問題，使德國海軍宣布其造船巨擘蒂森·克魯伯海洋系統 (Thyssen Krupp Marine Systems) 與呂森 (Lürssen) 必須退出競標，為其他可能的歐洲各地競爭者敞開大門。⁶⁰

此外，如同日本將在接下來的新型柴電潛艦中使用鋰電池一般，法國海軍集團 (Naval Group) 於 2018 年 10 月下旬宣布研發成功高性能與高安全性，可供傳統柴電潛艦運用的鋰離子 (Lithium-ion) 電池，提供兩倍的能量以及更短的充電時間。潛艦用鋰離子電池技術如發展成熟，將能透過更長的操作時間以加強其隱蔽能力與作戰範圍，大幅增加柴電潛艦戰力。⁶¹該集團並推出十分前衛的 SMX31 電力驅動潛艦概念艦，該艦由鋰電池供電，取消帆罩、擁有一獨特、受抹香鯨外型影響而設計的船體，將槳葉置於船的兩側，並搭配大量武裝及無人載具，然其構想與設計在實際發展及操作上的效益仍有待驗證，短期內難以成為實際服役的作戰系統。⁶²

⁵⁸ Luca Peruzzi, "Naval Group details FTI capabilities and programme development," *European defence review*, October 28, 2018, <https://www.edrmagazine.eu/naval-group-details-fti-capabilities-and-programme-development>。

⁵⁹ Xavier Vasseur, "Euronaval 2018: France Officially Launches Aircraft Carrier Renewal Program," *Navy Recognition*, October 23, 2018, <https://www.navyrecognition.com/index.php/news/naval-exhibitions/2018/euronaval-2018/6594-euronaval-2018-france-officially-launches-aircraft-carrier-renewal-program.html>。

⁶⁰ "Thyssenkrupp und Lürssen gehen bei Bundeswehrauftrag leer aus," *Spiegel Online*, March 2, 2018, <http://www.spiegel.de/wirtschaft/soziales/kampfschiff-mks-180-thyssenkrupp-erhaelt-keinen-bundeswehr-auftrag-a-1196136.html>。

⁶¹ "Introducing Naval Group's new Lithium-ion batteries system for submarines," *Navy Recognition*, Oct. 24, 2018, <http://www.navyrecognition.com/index.php/news/naval-exhibitions/2018/euronaval-2018/6625-introducing-naval-group-s-new-lithium-ion-batteries-system-for-submarines.html>。

⁶² H I Sutton, "SMX-31 future submarine concept: 'The Electric,'" *Covert Shores*, October 31, 2018, <http://www.hisutton.com/SMX-31.html?fbclid=IwAR0Z6Nhr5hNc30Ozt43EtmRPCKLFaGNSqNuLWK1oJ3FXE9vO1mzi3lCyyEc>。

小結

本章介紹世界各主要國家，包括美國、中國、俄羅斯以及北約軍事科技發展趨勢。其中，美國仍是世界軍事科技最先進國家，美國也是民主國家兵工廠，其武器、裝備、彈藥或是軍事技術，多輸出其盟國及友邦。其中，台灣也以美製武器為主要作戰裝備。川普總統上任後強調發展軍備，確立「美國優先」，以因應中國及俄羅斯挑戰。因此，具備先進科技的武器裝備發展有復甦之勢。然而，美國也在改革國防採購體系，以加快採購速度，並減低成本，目的亦是強化軍備。

其他國家科技亦不容忽視，各國均針對其戰略環境及作戰需要，運用適當技術，發展適合其國情的武器系統。中國、俄羅斯傳統武器載台技術如飛機、水面艦等仍然落後美國，雖有創新概念，部分科技仍受限制，主戰裝備發展尚無法挑戰美國。因此，研發武器裝備主要方向，在於創造對美國及西方精良武器備的不對稱優勢，如彈道飛彈、巡弋飛彈及先進極音速武器，這已構成對美國及其盟國的挑戰。

第二章未來戰場特性

舒孝煌¹

前言

未來戰爭型態將較現在更趨多樣化、複雜化。一方面，武器系統日益精準、效能提升，摧毀及殺傷面積更小，戰爭朝向小型、精準、外科手術式發展；另一方面，非殺傷式作戰，例如網路戰、輿論戰、破壞攸關國家社會運作及人民日常生活的關鍵基礎設施等等非傳統戰法，則可能對國計民生造成重大影響，間接影響國家軍事反擊的能力。

當今敵人不僅擁有高科技武器，如匿蹤戰機、長程精準飛彈、極音速武器、無人載具等，還有其他非軍事手段可運用於作戰，例如網路戰、電子戰、心理戰、游擊戰或恐怖攻擊等，使作戰發起可能非常早，甚至在部隊集結或啟程前即已發生。敵人的「反介入／區域拒止」(Anti Access/Area Denial, A2/AD) 能力使海、空軍無法保證一定能準時抵達戰場掩護地面部隊，更別提資訊或網路戰可能在戰爭開打前早已先形塑戰場，這使作戰場域大為擴張。

非傳統式戰具如小型 UAV、自動化機器人等在作戰中的運用日益增加，不僅增進部隊情監偵、作戰與後勤等能力，也讓敵人可能在戰爭發起前，即以網路戰、電磁戰等技術，使傳統戰具減少或失去其作戰效能。換言之，戰爭在大規模部隊動員、兵力集結前即已發起，前方和後方的傳統意義也不再存在。

壹、跨領域作戰

為因應快速多變的戰場環境，近期美軍提出的創新作戰構想，可以勾勒出未來高科技作戰的樣貌。設想中的多領域作戰 (Multi Domain Battle)，將戰場由前方至後方劃分為 7 區，反應戰場的擴大及作戰領域的增加，各區彼此重疊，「開火」(Fire) 意義不僅是具體的武器如火砲及飛彈，也包括無形的網路及電子戰。

一、5 大領域支援 7 區域作戰

美國陸軍規劃中的多領域作戰包括 7 區域：(一) 戰略支援區 (Strategic

¹ 舒孝煌，國防安全研究院國防資源與產業研究所助理研究員，負責本章內容。

Support Area);(二)作戰支援區(Operational Support Area);(三)支援區(Close Area);(四)接近區(Close Area);(五)深入機動區(Deep Maneuver Area);(六)作戰深入火力區(Operational Deep Fires Area);(七)戰略深入火力區(Strategic Deep Fires Area),所有5大作戰領域:太空、網路、空中、陸地、海洋,都可涵蓋以上7區域作戰。

在多領域作戰概念下,各軍種的角色較過去大幅擴展,因此美國陸軍要進行大幅度的現代化,6項目標包括1、長程精確火力(Long-Range Precision Fires, LRPF),2、下一代戰鬥車輛,3、未來垂直舉升平台,4、陸軍自己的網路化作戰,包括網路化指管通情、定位、導航及即時情報,5、防空及彈道飛彈防禦,6、單兵殺傷力的提升。

「多領域作戰」概念除了減少對空軍的依賴,強化對敵打擊戰機、短程彈道飛彈及巡弋飛彈威脅的防禦。在未來衝突中,陸軍需有能力保護自己免受空中威脅,因此機動短程防空(Maneuver Short-Range Air Defense, MSHORAD)成為最急迫項目之一。另外,陸軍也恢復過去曾擁有過的長程精確打擊能力,發展新式長程飛彈取代現有 ATACMS,體積更小,射程達500公里,可打擊固定目標。但如果配備新式尋標器,將可打擊陸地及海面的移動目標,可用以部署在太平洋,對付海上艦艇。²

二、多領域作戰打破軍種隔閡

在多領域作戰的構想下,各軍種都可能扮演主動角色協助其他軍種,例如陸軍可以長程火力協助友軍,使用 UAV 發現及標定目標,以火炮或長程火力摧毀敵方防空陣地,讓空軍戰機得以深入敵境打擊目標。除精準飛彈外,如果新火炮使用更先進彈頭,如極音速或衝壓推進彈頭,射程還可以延長至100公里,多管火箭也可延伸至150公里。其實長程砲兵火箭早在俄羅斯、中國或其他國家服役,只是美國現在也考慮發展自己的長程打擊能力。

陸軍同樣也考慮運用先進武器,包括電磁軌道武器,可將「投射物」(彈頭)以7馬赫速度投射,目前該領域由海軍領先;發展M109自走榴砲自動裝填系統,使射速提升至每分鐘6至10發。過去美國陸軍要依賴海空軍提供空中保護,才能在陸上作戰,現在陸軍則尋求在多領域(陸上、空中、海上、太空、網路)協同攻擊,不僅是支援地面部隊,且是協助海、空軍及陸戰隊,摧毀敵戰機及水面艦,成為海、空軍的搭檔。多領域作戰概念進一步發展,將成為跨領域作戰(Cross Domain Battle),使傳統的軍種角色更為模糊,由於網路化作戰的發展,在最高指揮階層的統一指揮管制可能進一步聯合化、自動化,由聯戰指揮機制依

² “CSA Milley Bets On ‘Radical’ Tech, Promises No More FCS”, *Breaking News*, January 17, 2018, <https://breakingdefense.com/2018/01/csa-milley-bets-on-radical-tech-promises-no-more-fcs/>。



圖 2-3、美國陸軍多領域作戰概念圖

資料來源：US ARMY。

貳、網路化分散式作戰

美國海軍同樣也對其所面對的威脅，發展因應之道。因其在太平洋上的潛在敵人，擁有長程反艦彈道飛彈或巡弋飛彈，號稱可以在企圖破壞美軍的行動自由，並威脅美軍的前沿部署。

一、網路化作戰

由於網路化作戰的廣泛運用，使作戰平台的部署不再需要集中於一處，而是可以大幅分散至所有區域，並使所有艦上及空中的感測器、防空、反艦與攻陸火力得以充分發揮。因武器發射載台和感測器可以相距數百公里，將使敵方更難以打擊。

美國海軍的「分散式致命」(Distributed Lethality) 概念，意在指使更多的敵人在更寬廣的地理範圍蒙受更大風險，並且使所有的水面部隊更為「致命」(Lethality)。除一般作戰艦艇外，尚納入支援艦艇，讓艦隊或聯合作戰指揮官具備更多的攻勢性選項，並強化傳統嚇阻的態勢，限制敵人的作戰選項，甚至將敵人限制在港灣內無法行動。³

³ “Distributed Lethality and Beyond: The U.S. Navy's Surface Fleet Is Evolving Right Before Our Eyes,” *National Interest*, November 1, 2016, <http://nationalinterest.org/blog/the-buzz/distributed->

二、海上部署新思維

到 2030 年，美國海軍作戰艦艇可能不會有太多突破性變化，但卻會採取完全不同的作戰思維，⁴例如配備相位陣列雷達的巡洋艦和驅逐艦，原本其任務是擔負區域防空角色，保護航艦戰鬥群，防止敵海軍攻擊航空母艦，現在則成為防禦彈道飛彈攻擊的平台。此外，為確保海上作戰行動順暢，海軍尚需維持一支數量龐大的兩棲與後勤支援艦艇。這些艦艇不具作戰能力，但在「分散式致命」概念下，所有海軍艦艇都可以在維持制海權上扮演一定角色。

未來美國海軍及陸戰隊兩棲艦的部署將與現在不同，所有船艦都要廣泛分布在海洋上，不再是圍繞在航空母艦周圍。因此，兩棲艦艇要配備無人空中預警機，具備空中早期警戒的能力，不需受到 E-2D 作戰範圍的限制。⁵

分散性部署的關鍵是「海軍整合射控—制空」(Naval Integrated Fire Control-Counter Air, NIFC-CA) 網路，未來所有水面艦、飛機都能整合在此一網路中，延伸海軍標定、分析及攔截目標的範圍。在此架構下，其核心是 E-2D 空中預警機，使用其協同接戰能力 (Cooperative Engagement Capability) 將目標資料以 Link 16 鏈傳至遠方艦艇，由其發射標準 6 型飛彈攔截空中目標。水面目標則暫時需依賴 P-8 巡邏機或 RQ-4 無人巡邏機，以 Link16 鏈傳目標資料。未來感測器可以擴展至 F-35，使其與 NIFC-CA 網路結合。⁶

三、分散式防禦概念

如同陸軍的「多領域作戰」一般，此一概念可以加以擴大，成為「分散式防禦」。美智庫「戰略暨國際研究中心」(CSIS) 在 2018 年 1 月推出一分報告《分散式防禦：整合式空防及飛彈防禦的新作戰概念》(Distributed Defense: New Operational Concepts for Integrated Air and Missile Defense)，⁷提及「任何感測器、更佳射手」、「任何飛彈、任何目標」、「任何發射器、任何地區」等概念，其核心包括：1、網路中心化，2、要素分散化，3、混合酬載，4、結合攻勢及守勢的發射單元，5、多任務射手，6、容器化發射器，7、被動式防禦（欺敵以增加敵情監偵困難及攻擊成本）。這些概念並非新穎，許多已運用在美軍或其他國家的軍事部署上，然而需要武器平台有更多的運用彈性，同時可讓感測器資訊在作戰網

lethality-beyond-the-us-navy-evolving-right-18251?page=show。

⁴ 同註 3。

⁵ “Marines Won’t Need a Carrier for High-End Fight With MUX Unmanned System”, *USNI*, June 6, 2018, <https://news.usni.org/2018/06/06/marines-wont-need-carrier-high-end-fight-mux-unmanned-system>。

⁶ “Navy Expanding NIFC-CA To Include Anti-Surface Weapons, F-35 Sensors,” *USNI*, June 22, 2016, <https://news.usni.org/2016/06/22/nifcca-expands-sm6-f35>。

⁷ “Distributed Defense New Operational Concepts for Integrated Air and Missile Defense”, CSIS, January 25, 2018, <https://www.csis.org/analysis/distributed-defense-0>。

路上迅速分享。

參、太空競逐

太空早已是軍事部署的重鎮，美軍在波斯灣戰爭獲致勝利，主要是高科技武器發揮效能。然而其精準導引武器發揮效能，需依賴太空中部署的衛星，可以說美國的軍事強權，幾乎完全要依賴在太空的部署。

一、美國軍事霸權依賴太空

1991 年第一次波斯灣戰爭前，美國發射達 50 枚衛星，擔負衛星定位、導航、通訊、飛彈預警及偵察等任務。偵察衛星可提供敵方軍事部署及動態的廣域、即時偵察，通訊衛星提供指揮部與作戰單位的遠距離通訊及目標資料的快速鏈傳，衛星定位則可提供目標座標，導引武器精確命中目標。2001 年 911 事件後，美國在中東進行反恐戰爭，並在伊拉克、阿富汗等國境內以 UAV 打擊恐怖分子與游擊隊，其 UAV 亦依賴衛星進行遠距控制。

美國部署在太空中的軍用衛星，主要功能包括氣象、導航及定位、通訊、光學或雷達影像偵察 (Optical or Radar Imaging Reconnaissance)、電子情報蒐集 (ELINT)、飛彈預警、監視、衛星追蹤以及科學研究等等，操作衛星的單位除美國空軍旗下如太空司令部、第 50 太空聯隊、空軍實驗室、太空系統研究中心外，尚包括國防部、海軍、國家偵察辦公室 (National Reconnaissance Office)、飛彈防禦署、國家航空太空總署、國家科學基金會等單位。除衛星外，雖然太空梭已退役，但美國仍在進行重返大氣層載具的測試，例如屬實驗性質的美國空軍 X-37B 「軌道測試載具」(Orbital Test Vehicle, OTV) 由火箭發射，以滑翔方式重返地面，雖然其任務多為科學研究性質，仍其真正功能仍未被外界所悉。

二、太空軍事化

除部署衛星外，為維持太空優勢，美國考慮在太空中部署武器，如高能量雷射、粒子束武器 (Particle beam)，以擊落彈道飛彈或是太空中的衛星。⁸在反衛星武器方面，美國早在 1985 年即嘗試以 F-15 戰機發射反衛星飛彈 (ASAT)，摧毀一枚軌道高度 555 公里的衛星；2008 年，美國海軍以一枚標準 3 型飛彈成功摧毀一枚衛星。

為了監視中國及俄羅斯太空活動，美國從 2010 年開始推動的「太空監視系統」(Space-Based Surveillance System, SBSS)，目的在強化對太空感知及監視能

⁸ “How Space Wars Will Work,” *How Stuff Works*, 2018, <https://science.howstuffworks.com/space-war.htm>。

力。美國軍用通訊在戰時可能會遭敵方干擾，目前僅有 7% 的軍用頻寬有能力抗干擾。2018 年，美國發展先進極高頻衛星 (AEHF)，使用相位陣列天線，可自動偵測未被干擾波段，並能向地面發射多重波束以傳遞訊息，即使發生核戰，也能維持軍事通訊能力，目前已有 4 枚在運作中，另外也投資發展新一代可抗干擾的 GPS 衛星。

除干擾外，反衛星是對太空衛星的另一項威脅，AEHF 衛星在地球同步軌道運行 (geostationary orbit)，軌道高度達 22,500 哩。目前主要反衛星技術都針對低軌道衛星，高度僅 1,200 哩。但未來太空武器有可能打到更高目標，將是此類衛星的威脅。

美國仍是太空強權，目前運行中的衛星達 859 枚，其他國家如俄、中也在運用太空進行軍事部署，中國約擁有 250 枚衛星，超過俄羅斯的 146 枚，這三大太空強權擁有衛星數量佔所有運行中衛星的 66%。除美國外，中國在通訊、導航、情監偵等領域的快速發展值得重視。⁹

三、未來戰爭將從太空展開

俄羅斯與中國已嘗試在太空中進行作戰任務，設法削弱對手的太空能力。俄羅斯學者有所謂「第六代戰爭」說法，指未來若大國之間發生戰爭，將會從太空展開。首先是中國以改良的彈道飛彈攔截美國低軌道偵察衛星，並以殺手衛星撞毀高軌道衛星；美國則攻擊中國的衛星發射基地，阻止其發射衛星，雙方並干擾對方衛星定位、導航、通訊能力。¹⁰雖然其言論頗有爭議，但美方也有專家警告美國可能遭遇「太空珍珠港」般的突襲，¹¹亦預示太空戰的來臨。

美國的挑戰者包括中國及俄羅斯。中國也擴張運用太空能力，在 2015 年實施軍事改革後，成立戰略支援部隊，負責統籌太空任務。中國衛星包括資源探測、氣象、通訊、導航、海洋、遙測等。中國自主發展的北斗衛星導航系統尚在建置中，至 2012 年已覆蓋亞太大部分地區，2020 年將以 35 枚衛星實現全球導航服務能力。¹²

除發射各種不同用途的軍用衛星外，中國也進行反衛星武器試射，曾在 2007 年成功摧毀一枚失效衛星，使用的是類似美國彈道飛彈防禦系統的外大氣層擊殺

⁹ "UCS Satellite Database," *Union of Concerned Scientists*, April 30, 2018, <https://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database#.W-ezEtUzapo>。

¹⁰ <外媒：中國在軌衛星數超俄正準備第六代戰爭>，《環球網》，2016 年 8 月 3 日，<http://military.people.com.cn/BIG5/n1/2016/0803/c1011-28607364.html>。

¹¹ "Rumsfeld Commission Warns Against "Space Pearl Harbor"," *Spacedaily*, January 11, 2001, <http://www.spacedaily.com/news/bmdo-01b.html>。

¹² <譚述森：認識北斗>，《北斗衛星導航系統網站》，2011 年 3 月 28 日，<https://web.archive.org/web/20130324195344/http://www.beidou.gov.cn/2011/03/31/201103318928b0d1cfb44598a98ead9fdbbf6e33.html>。

載具(Exoatmospheric Kill Vehicle)。另中國可能進行多次測試,但皆無明確證據,但有報導指出中國在2013年發射一枚實驗火箭,展示達到地球同步軌道的能力,唯該火箭並無酬載物。¹³前蘇聯很早就發展「殺手衛星」,即以火箭將裝置彈頭的攔截器發射至接近目標衛星的軌道,火箭上裝置雷達以偵測目標,攔截器重達1,400公斤,足以在1公里外摧毀目標。美國情報單位也證實,近年俄羅斯持續測試反衛星飛彈,不過可能並未模擬攻擊目標,僅是展示發射入軌能力。¹⁴

由於大國持續擴張對太空的運用,甚至開始部署武器,未來除洲際武器經由太空重返地球攻擊目標外,也可能對敵方衛星進行攻擊,使太空變成戰場。未來美俄中等太空強權可能投入「太空快速反應作戰」(Operational Responsive Space, ORS),以低成本、快速部署取得太空戰場優勢,軍事衛星可能朝「微/小型化」與「星系式」部署,發射載具則使用固態燃料火箭,以便快速發射、即時反應,這將是太空反速反應作戰的趨勢。

肆、超精準打擊

美國在波斯灣戰爭中運用精準打擊武器,獲得優異戰果。精準武器反映的是國家整體國防能力的強大,精準武器的建立需滿足武器本體、導引系統及偵蒐單元、以及搭載以上系統的智慧平台等要求。未來無論空戰、海戰或地面戰,都需要有效的精準打擊武器性統作支撐。未來趨勢則為結合區域網絡及智慧武器系統,取代各自獨立的武器平台。然而建立一套精準化打擊平台花費龐大,並非所有國家均能負擔,鮮少有國家能建立類似美國的龐大C4ISR能力。近年歐洲國家在中東及北非執行反恐作戰時,亦仰賴美國的C4ISR支援。

一、精準武器改變作戰方式

經歷1991年第一次波斯灣戰爭(沙漠風暴作戰)、1999年科索沃空襲、2001年阿富汗的持久自由作戰、2003年第二次波斯灣戰爭(伊拉克自由作戰)的成功,使美國空軍作戰概念產生極大變化。新型態的作戰概念被稱為「效能作戰」(Effective-Based Operation)。¹⁵過去空權論者主張空軍執行戰略轟炸可以贏得戰爭勝利,但戰略轟炸會造成大量附加損傷及平民傷亡,己方執行任務的作戰單位也會付出極大代價的損失。結合資訊科技的精確導引技術出現後,因為空中打擊可以精準命中目標,不需為了增加擊殺率而擴大投彈數量,不會傷及平民或非軍事設施。過去需派遣大規模轟炸機隊投擲數百噸彈藥的作戰方式,現在只需數架

¹³ “Doomsday Satellites and the Space Wars To Come,” *Popular Mechanics*, February 16, 2018, <https://www.popularmechanics.com/military/research/a18194748/ahf-doomsday-satellites/>。

¹⁴ “Sources: Russia tests anti-satellite weapon,” *CNN*, December 21, 2016, <https://edition.cnn.com/2016/12/21/politics/russia-satellite-weapon-test/index.html>。

¹⁵ 「效能作戰」為國軍軍語,坊間出版品譯為「基於效果作戰」或「效基作戰」,見98年版國軍軍語辭典,138頁「Effect-based operation」條目。

戰機，投擲數枚雷射或衛星定位武器便能達成摧毀效果。

由於技術變革使作戰效能大幅提升，以精準攻擊取代大規模戰略轟炸，力量的浪費變成力量的節約，空權運用方式也隨之轉變。1991 年波斯灣戰爭前，美國空軍約翰沃登上校制定一套戰略空中計畫，¹⁶分階段對敵人施加武力，以產生特定效果，不需要完全摧毀敵人目標。2001 年 10 月持久自由行動，以及 2003 年的伊拉克自由行動，精準打擊技術更為成熟，戰場指揮管制、情報偵蒐等技術的大幅進步、無人機的投入戰場，戰損評估技術的精進，使精準打擊效能及速度較 1991 年倍增。更具革命性的運用當屬匿蹤戰機的出現，使我方飛機不易被敵防空雷達查覺，可以省略投注在防空制壓作戰的兵力，攻擊其他更關鍵的目標，使得空襲行動的效益大幅提升。

美國在中東進行反恐戰爭時，因掌握制空權，戰機執行任務時並無敵情顧慮，因此依賴的是短程精準武器，包括聯合直接攻擊炸彈（Joint Direct Attack Munition, JDAM），是一系列具有全天候精確投擲能力的低成本通用炸彈，以及鋪路系列（Paveway, 其中 PAVE 是「精確航電導引裝備」Precision Avionics Vectoring Equipment 的縮寫）雷射導引炸彈，由地面或空中導引莢艙發射雷射光源導引炸彈攻擊目標。

不論射程多長或多精準，最大考驗都是目標獲得。固定目標如機場、設施可依賴衛星或空中偵照，但移動目標如機動部署的飛彈發射車、突然出現的恐怖分子車隊，若無強大指管通情監偵（C4ISR）體系，無法支持對機動性、機會性目標的打擊。目前除美國及北約依賴精準武器外，俄羅斯及中國則較依賴各種新式的彈道飛彈，如可變軌、機動式的彈道飛彈，或甚至使用極音速載具，而非戰機搭載的直攻彈藥，顯示對其奪取制空權以及對攻擊目標的 C4ISR 能力上仍不具信心，然而其對地攻擊能力則日益精準，且號稱能使用反艦彈道飛彈對海上移動船艦進行打擊，雖然並無實際驗證紀錄，不過其精準打擊能力仍不容忽視。

二、新一代遙攻精準武器

若遭遇空防能力強大的對手，美國的精準打擊能力能否如此有效，就難以定論。在反恐戰爭暫告尾聲之際，美國開始關注在亞太或中東等地的新威脅，為反制敵人的 A2/AD 能力，因此開始研發長程的精準武器，目前已開發並服役，然仍持續改良精進的新一代長程武器包括：

（一）AGM-158 聯合空對地視距外飛彈（Joint Air-to-Surface Standoff Missile, JASSM）：

這是一種 1,000 公斤級的飛彈，攜帶 450 公斤級的彈頭，採用 GPS/INS 導

¹⁶ John T. Correll, "The Strategy of Desert Storm", *Air Force Magazine*, January, 2006, pp26-33, from <http://www.washingtonpost.com/wp-srv/inatl/longterm/fogofwar/wargoals.htm>。

引，彈體具匿蹤外型，可穿透現代防空系統，並裝置彈翼以提高巡航效率，將射程提升到 460 公里以上。AGM-158 除使用 GPS/INS 導引，終端另使用影像式紅外線尋標器導引，具備自動識別目標功能。AGM-158A 導入雙向通訊鏈結及「人在迴路」(Man in the loop) 導引納入，增加飛行中改變攻擊路徑及目標功能，並強化 GPS 接收器抗干擾能力。AGM-158B 延程型 (JASSM-ER) 除攻擊固定及機動陸上目標，尚增添攻擊船艦能力。

(二) AGM-154 聯合視距外武器 (Joint Stand-Off Weapon, JSOW)

由美國海空軍聯合發展，也採用 GPS/INS 導引，基本型不具動力，精確度可達到 10 公尺以內，滑翔距離 40 哩，可配單一彈頭或次彈械撒布器，攻擊較大範圍目標。除 GPS/INS 導引外，AGM-154C (JSOW-C1) 終端也增加影像式紅外線尋標器，增加 Link-16 數據鏈功能，具備攻擊陸上及海上目標能力。JSOW-ER 正測試 TJ-150 小型渦輪噴射發動機，航程可增至 560 公里。

(三) AGM-84 衍生型：

由魚叉 (Harpoon) 反艦飛彈衍生發展而來的 AGM-84H/K 距外陸攻飛彈 (Standoff Land Attack Missile, SLAM/SLAMER)，主要為海軍及空軍戰機攜掛，具備攻艦及攻陸雙模式，射程則延伸至 270 公里，可在飛行中重新給予指令，標定其他目標。



圖 2-4、美國空軍 AGM-158 飛彈

資料來源：舒孝煌攝。

三、未來發展趨勢

精準導引武器仍持續發展中，除上述武器外，目前有數種發展趨勢：

(一) 多模式導引

不同導引模式間可互相切換，因炸彈可能受天候、環境因素干擾，如煙霧、沙塵會使雷射導引炸彈失去作用，GPS 導引炸彈只能用以攻擊固定目標。因此，美國將兩種導引模式結合為一，發展雙模式導引武器。

雙模式可增加運用彈性，改善任務效率。運用雷射導引模式時需以雷射照射目標直到擊中，不過若使用衛星定位／慣性導航（GPS/INS）模式時，飛行員在射程範圍內投彈後即可脫離。小尺寸 II 炸彈（SDB II）更使用三波段（毫米波雷達、非致冷式影像紅外線、半主動雷射）尋標器，可因應不同時間、天候及目標加以切換。目前遙攻武器多具自主導引能力，毋需使用雷射光源輔助導引。

（二）長時間滯空

可在目標區上空盤旋數小時，結合 UAV 的廉價、小型化、可長時間滯空，等待機動目標出現時發動突襲；或將無人機改為配備終端導引系統及彈頭部的「自殺」式無人機，一架戰機可攜帶較多數量，以增加獵殺量。波音的小直徑炸彈（SDB）為 250 磅級，使用慣性及 GPS 導引，衍生型更可增加尋標頭以提升對付機動目標能力。洛馬的監視微型巡弋飛彈（SMACM）滯空能力達一小時，航程可達 450 哩，另一種新的區域支配炸彈（ADM）更可滯空達數天之久，甚至可由無人機攜帶。目前 UAV 已可被當成精準武器實施攻擊，因小型 UAV 的多樣化，如長時間滯空、垂直起降，目前已有許多國家以小型 UAV 搭載武器，可針對隱藏在樹林或建物後的小規模地面部隊，遂行自殺攻擊，達成超精準打擊。

（三）快速、長距離

未來長程打擊武器可以打擊全球範圍內的即時目標。美國早在計畫將全球打擊能力朝向精準武器發展，原本計畫發展傳統迅捷全球精確打擊（Conventional Prompt Global Strike, CPGS）計畫，目的是在一個小時內精確打擊世界上任何一個角落。其候選方案包括數種不同型式的極音速武器，如美國空軍的傳統打擊飛彈（Conventional Strike Missile, CSM）、國防先進研究計畫署及空軍合作的「極音速技術載具 2」（HTV-2），以及美國陸軍的先進極音速武器（AHW）。這些計畫雖然進展不太順利，不過美國 2018 年持續撥款發展極音速概念，已如第一章所述，實際目的在於確保發展優勢，避免落後俄羅斯及中國。另外，在 2017 年 4 月進行一次無彈頭的義勇兵 3 型飛彈試射，目的是確保核武部隊的運作正常，未來可能會為彈道飛彈改配傳統彈頭。若能成功，義勇兵飛彈有可能成為 CPGS 的選項。¹⁷

¹⁷ “The US Continues with Conventional Prompt Global Strike (CPGS),” Ankara Center For Crisis and Policy Studies, June 5, 2018, <https://ankasam.org/en/us-continues-conventional-prompt-global->

（四）載台及武器分散化

未來美國情監偵體系可能進一步發展，支持其全球快速精準打擊，並達成分散性部署，使所有作戰單位都能網路化、分享共同圖像，上網擷取其執行任務的必要情資，並藉由網路分配任務，快速打擊目標。美國海軍測試中的 NIFC-CA 網路，容許發射載具在未獲得目標情資下發射飛彈，再藉由戰機等進行目標資訊鏈傳協助導引，可用以打擊移動目標。在 NIFC-CA 架構下，E-2D 空中預警機可當成資料傳輸的節點，由匿蹤戰機如 F-35 擔任穿透敵堅強防空網，EA-18G 電戰機則進入擔任防空制壓角色，當空域安全後，不具匿蹤能力的 F/A-18 以最大酬載進入目標區進行精準打擊。即使沒有掛載武器，戰機也可導控遠處潛艦或水面艦發射的長程巡弋飛彈，將目標以資訊鏈傳給飛彈，以導引其擊中目標。美國海軍已在 2015 年測試由 F/A-18 導引一枚戰斧巡弋飛彈攻擊移動中的靶船，也驗證海軍網路化作戰的可行性。¹⁸

其他的發展尚包括：制壓打擊目標多模式化，除上述武器具備攻艦及攻陸模式外，尚包括標準 6 型飛彈除防空外，尚可攻擊陸地及海上目標；網路共享聯合作戰，以中繼機或衛星雙向資料鏈，對臨機（time critical）目標進行動態即時打擊；模組化多功能酬載，彈頭可視情況轉換成智慧型散撒次彈械、脈衝彈、感爆雷、石墨彈、跑道破壞武器、阻絕雷等；模組化電戰酬載，可擔負誘標或電子干擾任務；增加終端影像導引能力及自動識別目標技術，提升打擊精度；「人在迴路」，以在飛行途中由人力介入改變路徑及目標；複合式被動雷達尋標器（ESM IIR+ATR）。

四、精準武器有賴強大 C4ISR 能力

不論射程多長或多精準，最大考驗都是目標獲得，固定目標如機場、設施可依賴衛星或空中偵照，但移動目標如機動部署的飛彈發射車、突然出現的恐怖分子車隊，若無強大指管通情監偵（C4ISR）體系，無法支持對機動性、機會性目標的打擊。目前除美國及北約依賴精準武器外，俄羅斯及中國則較依賴各種新式的彈道飛彈，如可變軌、機動式的彈道飛彈，或甚至使用極音速載具，而非戰機搭載的直攻彈藥，顯示對其奪取制空權以及對攻擊目標的 C4ISR 能力上仍不具信心，然而其對地攻擊能力則日益精準，且號稱能使用反艦彈道飛彈對海上移動船艦進行打擊，雖然並無實際驗證紀錄，不過其精準打擊能力仍不容忽視。

strike-cpgs/。

¹⁸ “Watch a Tomahawk Missile Guided By an F/A-18 Strike a Ship,” *Popular Mechanics*, February 11, 2015, <https://www.popularmechanics.com/military/weapons/a14024/tomahawk-missile-f-a-18-video/>。

伍、高密度自動化戰場

無人載具及自動化機器人將是未來戰爭的主角，且使用密度將日益增加。自動化裝備早已運用在軍事上，例如：火炮採用自動裝填，可節省人力；船艦上採用自動化近迫武器系統，可自動偵測並迎擊來襲飛彈，減少反應時間；軍機可以自動偵測附近有無其他飛行物靠近，或偵測地形地物障礙，並由電腦控制自動避碰；無人機除遠端有人操作外，也可以程式依設定航線自動飛行，進行長時間巡弋與偵察；戰場上也早已在運用所謂「機器人」，即無人駕駛載具，用以進行拆解爆裂物、除雷、偵察等任務。

一、無人載具

無人機(UAV 或 Drone, 美軍正式說法為 RPA, 即「遠距操作飛機」〔Remotely Piloted Aircraft〕) 也已大量運用在戰場上，例如美軍的 MQ-1 及 MQ-9，雖然在執行打擊任務時由人員控制，但可以依自動設定的航路返航。較大型的 RQ-4 全球之鷹(Global Hawk) 則可自動飛行，進行長時間的空中偵察及監視任務；較小型的無人機則是發射後在空中盤旋，當偵測到目標時，自動歸向予以擊毀。

UAV 可算是戰場自動化裝備一種，雖仍是有人操作，但操作者位於遠離戰場的操作站台，透過衛星將控制訊號傳至 UAV，UAV 則將感測器獲得資訊回傳至控制站，讓操控者決定是否發動攻擊。美軍反恐戰爭中極為依賴 UAV，結合偵打一體、情監偵，使美軍獲得即時攻擊時效性目標的利器，而且節省自己的人力及機隊成本。現在 UAV 仍在持續發展，未來可能結合有人與無人機，由機上飛行員操控，執行危險穿透敵境任務。小型 UAV 執行自殺攻擊任務；可自動飛行的運輸型 UAV 以及戰場機器人，則代替人力進入危險的戰區，執行後勤補給物資的重物或重型武器運送任務。水面無人載具 USV 或水下無人載具 UUV，干擾敵登陸船團、掃布雷艦或執行封鎖等任務之艦艇。發展特定用途之大型 UUV，執行襲擊大型艦艇或敵港口之特種任務。UAV 結合 AI(人工智慧)，可自行執行耗時耗力的巡邏任務，依程式設計自行決定是否發動攻擊，其自動化程度進一步提升。



圖 2-5、英國空軍 MQ-9 無人機

資料來源：舒孝煌攝。

二、自動化機器人

軍方考慮更進一步在後勤等方面運用自動化機器人，包括使用微型機器人偵測及修復複雜的機械，例如噴射發動機。英國發動機製造商勞斯萊斯（Rolls Royce）正與大學合作，運用其微型機器人技術進入發動機內平常檢修程序難以接觸之處進行檢查，甚至實施修補。使用送貨無人機或機器人進行工廠運輸或自動物流的概念，也可運用在戰場上。民間物流公司開始嘗試運用大型四軸或多軸式 UAV 做快遞使用，能垂直起降並運送重貨。若在技術上能普及，也有可能供軍事運用，用以向前線運送補給品、燃料、彈藥等，減少因交通線被截斷或後勤兵源不足之困擾；或向前方戰況吃緊地區運補，減少人員曝露在敵火下的危險；或運送不易由人力搬運的重型貨物，如火砲及彈藥。民間廠商發展的「機器狗」（robot dog），具有四隻機器腳，可模仿真實動物的行動，可用於在歧嶇地面進行重貨運輸，¹⁹商用市場上的「機器狗」發展已經成熟，可以自主移動，越過不平整地面，可自動穩定，自動繞過或迴避障礙物，並有機器手臂可以進行簡單動作，如撿拾物品、開關門等。²⁰

三、未來無人系統發展

UAV 可依據衛星定位進行自動飛行，已是普遍的技術，然在戰場上運用的

¹⁹ “Marines Are Testing A Robot Dog For War,” *Popular Science*, September 23, 2015, <https://www.popsci.com/marines-test-robot-dog-for-war>。

²⁰ “Boston Dynamics Is Gearing Up to Produce Thousands of Robot Dogs,” *Fortune*, July 21, 2018, <http://fortune.com/2018/07/21/boston-dynamics-spotmini-robot-dog/>。

無人載具，例如地面無人載具（UGV），基本上仍是有人在遠端遙控，並非完全無人操作。軍事單位恐暫時無法接受自動駕駛的想法，不過未來若技術成熟，也有可能改變。美國廠商如 Boston Dynamic 已研究可為陸軍運送裝備的機器人或是無人運輸機，已將研發成品交給陸軍進行測試及分析，並研發無人戰車，與有人車輛搭配作戰。²¹ 微型 UAV 或小型機器人，可藉由群組模式發動攻擊或是協調作戰，因其體積小、數量多，可個別擔負偵蒐及攻擊任務，也可由戰機或地面車輛加以投放，使用彈性極廣。

機器人也會被用在操作某些危險或需長時間工作的任務，例如太空。美國與日本的航太工業計畫使用機器人執行太空任務；全日空（ANA）與日本宇宙航空研究開發機構（JAXA）合作進行一項稱為「阿凡達 X」（AVATAR X）的太空計畫，運用遠端操作機器人來解決太空任務難題。²²

美國海軍正在發展中的 MQ-25 空中無人加油機，以及其前身 X-47B 實驗機，是空中無人載具自動化操作的先聲，然而其所運用的技術仍是雙向 GPS 定位鏈傳，以修正降落定位點，距離人工智慧仍然很遠。國防先進研究計畫署正研究新一代人工智慧（AINext），包括新的演算法及應用，並增加其推理能力，有可能運用在未來的自動化裝備上，使其可以自主操作。

四、有人部隊及無人載具的整合

雖然戰場機器人的運用仍在發展中，但軍隊已要思考如何讓機器人與真人士兵搭配作戰，並在軍隊中運用更多自動化裝備、人工智慧以及無人系統。²³ 同時軍隊應擬定一套戰略，增加運用自動化裝備，例如美國陸軍希望未來的自動化裝備能增加情況覺知能力，減輕士兵的身體及認知上的負擔，幫助部隊在戰場上的運動能力，並保護士兵免受戰場威脅。為了提升對機器人的運用，需強化自動化、人工智慧以及共同控制的技術。²⁴

另外，目前美國在中東反恐作戰所使用之 UAV，在打擊目標時仍有人操作，船艦上使用之近迫武器系統亦是自動化操作，然機器人在戰場上殺人，將造成道德問題。1980 年 12 月聯合國已通過《禁止或限制使用特定常規武器公約》

²¹ “Four companies advance to build Army’s equipment transport ground robot,” *Defense News*, December 14, 2017, <https://www.defensenews.com/land/2017/12/14/four-companies-advance-to-build-armys-equipment-transport-ground-robot/>。

²² <全日空聯手 JAXA 展開「AVATAR X」計畫，要用機器人化身執行太空任務>，《科技新報》，2018 年 9 月 20 日，<https://technews.tw/2018/09/20/avatar-x-program/>。

²³ “US Army to Demo Robotic Wingman Vehicles in 2017,” *Defense News*, December 28, 2016, <https://www.defensenews.com/land/2016/12/28/us-army-to-demo-robotic-wingman-vehicles-in-2017/>。

²⁴ “Army Details Draft Robotics and Autonomous Systems Strategy At AUSA,” *Defense News*, October 4, 2016, <https://www.defensenews.com/digital-show-dailies/ausa/2016/10/04/army-details-draft-robotics-and-autonomous-systems-strategy-at-ausa/>。

(Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects)，有關機器人是否能用在戰場的問題，早在 2014 年聯合國已辯論過，也有許多國家與人工智慧專家呼籲禁止開發全自動化殺人武器，2018 年 9 月，歐盟也呼籲禁止開發生產相關武器，並在 11 月聯合國大會提出，26 國政府已表態。²⁵然因美、英、俄、中國都在開發自動化武器，未來能否通過仍充滿挑戰。

陸、模組化作戰型態

現代戰爭型態日益多樣化，威脅型態快速改變，使傳統的軍事組織及作戰平台難以應付多變的作戰場景。因此，各先進國家依其作戰經驗及教訓，調整組織編裝，以因應不同的作戰，並增加靈活反應的能力。各國軍事體系都有類似困境，即「官僚盛行、山頭林立」，既得利益者抗拒改革，使得軍隊組織難以創新。然而若軍隊面臨一次重大慘敗，就有可能使其得到教訓，不得不改變。

一、作戰體系的變革

美軍在越戰得到教訓，於是在 1970 年代推動「軍事事務革新」(Revolution of Military Affairs, RMA)。2000 年後，又繼續推動「國防轉型」，首先修改國防戰略重心，因應新型態危機、並為不確定的未來做好準備，美軍需保持高度戰備，並具備打贏 2 場可能同時發生戰爭的能力。2001 年發生 911 事件，助長美國國防轉型。由於未來軍事威脅極不確定，作戰型態也變得複雜而多樣化，美軍改變冷戰時期鎖定蘇聯的「基於威脅」建軍思維，轉為「基於能力」(Capabilities-Based Approach) 的建軍思維，全方位提升作戰能力，既要能夠因應大規模毀滅性的戰爭，又要能夠對付游擊式的不對稱威脅，有些衝突則不需動用大規模部隊，僅是制裁對手。

二、彈性的編制

在多變的威脅環境下，軍隊組織自需彈性調整，以因應戰況的變化。模組化的作戰編制可使部隊結構多樣化，靈活性增強。以陸軍為例，過去鈍重的師級編制已無法應付新作戰型態，而且陸軍需要跟其他軍種進行更良好的搭配。1976 年美國空軍上校鮑依德 (John Boyd) 提出「衝突的型式」(Patterns of Conflict) 報告，²⁶對如何擊敗敵人提出新構想，即所謂「觀察、定向、決策、行動」循環 (observation-orientation-decision-action loop, or OODA loop)，這發展出一套反敵

²⁵ <影/AI 勿濫用！歐盟也呼籲各國簽署禁開發「全自動化殺人武器」>，《智慧機器人網》，2018 年 9 月 19 日，<https://www.limitlessiq.com/news/post/view/id/6702/>。

²⁶ John Boyd, "Patterns of Conflict", *AirPower Australia*, 1986, <http://www.ausairpower.net/JRB/poc.pdf>。

人閃電戰的新構想。1982年美國陸軍提出「空陸戰」(AirLand Battle)，以在歐陸應付華約國家的陸上威脅，其中強調空軍及陸軍的緊密協調，以及要求前線作戰單位與後方指揮體系需同步連線，並即時決策，這有賴部隊達成資訊化，這是托佛勒所謂的「第三波戰爭」，在1991年波斯灣戰爭大獲成功。

資訊化打破過去鈍重的官僚體系及複雜的決策系統，改變作戰指揮體系及部隊結構。接著是部隊的「聯合」作戰，未來的武器，不論是載台或是武器本身，不再僅強調個別性能，而是強調其「網路化」特性，每一個平台都可以透過網路，彼此分享情資、實施目標標定及導引、並進行管制與指揮作戰，扁平化、蜂窩化的組織取代過去的金字塔式組織。²⁷

在美國戰略重心轉向亞太後，為因應亞太地區廣大海域的作戰特性，2010年提出「空海戰」(AirSea Battle)構想，在西太平洋地區強化美國海空軍合作，為可能到來的美中衝突做準備，以對抗中國的A2/AD戰略。2015年1月宣布創立「全球公域聯合介入及機動」概念(Joint Concept for Access and Maneuver in the Global Commons, JAM-GC)，取代空海整體戰，將陸上武力納入更廣泛的概念中，即如何將陸軍及陸戰隊介入衝突區域，協助美國部隊重獲介入能力。雖然用詞有所變動，其意義均在於進一步打破軍種間藩籬，更進一步強化聯合作戰。

三、模組化作戰編組

美國空軍已在1990年代末期進行組織改造，將指揮體系加以扁平化，取消戰略空軍及戰術空軍之間的差異，成立空戰司令部(Air Combat Command)。同時成立「遠征軍」(Air Expeditionary Force)編組，因美國中央司令部並未指派部隊，其概念是將美國空軍各不同任務的作戰中隊加以編組，依任務在作戰時指派給不同的遠征軍，加入特定的區域司令部，執行聯合作戰任務。這些中隊可能來自空軍作戰司令部，也可能是預備役部隊或是州國民兵，單位包括空優、對地打擊、偵察、預警、空中加油、戰略轟炸等不同性質中隊，它們仍屬原建制聯隊，但作戰時則編入遠征聯隊。

美國陸軍也在反恐戰爭後的2004年開始進行模組化改革，因傳統師級作戰單位過於龐大，難以適應不同規模作戰需要，特別是因應小規模的衝突時，彈性調度有其必要。另外，師的分工太細，有裝甲師、機械化師、步兵師、空降師等，編制太過僵化，難實施彈性調度。模組化改革是將師級單位虛級化，作戰單位改以旅級戰鬥隊(Brigade combat team, BCT)為主體，部隊規模變小，更容易戰略機動，編制變靈活，可以彈性組成聯合特遣部隊。此外，偵察及火力特支援單位下放至旅，更強化其獨立作戰能力。過去在反恐戰爭中對重型裝備需求較低，2018

²⁷ 陳宗逸，〈第四波戰爭從投石器到機器人的革命〉，《多維新聞》，2017年，第20期，<https://duoweicn.dwnnews.com/CN-2017%E5%B9%B420%E6%9C%9F/10003879.html>。

年美國陸軍持續調整旅級戰鬥隊，強化重裝火力，以聚焦更戰力更強的對手。²⁸美國海軍過去以特遣艦隊作為任務派遣的主力，但二戰開始已有以航艦為主力的作戰部隊。在 1990 年代正式以航空母艦戰鬥群（Carrier Battle Group, CVBG）為名，將海軍航空及水面作戰兵力進行更有彈性的整合，由艦載機聯隊、巡洋艦、驅逐艦、巡防艦、以及核動力攻擊潛艦構成。2004 年宣布將過去的重組為航艦打擊群（Carrier Strike Group），另外遠征打擊群則由兩棲突擊艦（LHD）與船塢登陸艦（LSD）、兩棲運輸艦（LPD）組成，主要由垂直起降戰機、直升機組成，此一編組更注重海軍的由海向陸武力投射能力。

四、軍種角色模糊化

在未來戰爭中，部隊的任務會更為多樣化；傳統陸、海、空軍等軍種的角色將更為模糊。在聯合作戰中，指揮階層視任務特性指派最適當的作戰單位，例如防空制壓作戰，有可能是陸軍 AH-64 攻擊直升機以低空穿透執行，或是特戰部隊，而不是空軍戰機。在守勢國家，除了海上及空中部隊保衛本身的制海及制空權外，因地面載具可以分散及彈性化部署，依賴地形地物掩護，搭配新的科技如多基雷達、網路化防空系統等等，可有效取得局部空優，或避免敵人取得空優，搭配新式機動化攻艦武器，也可取得由岸向海的局部制海優勢，可以較低成本遂行有效防衛。因此，在海軍的兵力投射、空權的火力打擊之外，地面部隊也可成為任務多工化的主要軍種。

現代戰爭中，一支搭配適當作戰單元的輕型反速反應部隊，可擔負應急機動作戰任務，包括國境反擊作戰、先遣及哨戒、反恐維穩等任務。輕型快反部隊可依不同任務需要，編組不同模組，在最短時間內編組不同的部隊，快速準確採取有效行動。模組化可以實現各軍、兵種的專業合成化，適應資訊化聯合作戰要求，以一致的作戰原則指導各模組的作戰任務，指揮層級扁平化，各模組間可以資訊交流，作戰任務上相互補充，以發揮彈性用兵的最大效果。

柒、混合型作戰模式

冷戰結束後，戰爭型態也有極大變化。國與國戰爭仍是學者研究衝突理論時主要關心的焦點，但全球化日益普及，也使衝突以不同型式擴散。傳統上戰爭被簡單分為「大型及傳統戰爭」以及「小型及非正規戰爭」，但霍夫曼（Frank Hoffman）認為現代敵人會將不同型式戰爭加以結合運用。²⁹非國家角色偏好運用

²⁸ <美陸軍 2 旅級戰鬥隊 火力升級>，《青年日報》，2018 年 9 月 23 日，
<https://www.ydn.com.tw/News/306176>。

²⁹ Frank G. Hoffman, "Conflict in the 21st Century: The Rise of Hybrid Wars," Potomac Institute, December, 2007,
http://www.potomac institute.org/images/stories/publications/potomac_hybridwar_0108.pdf。

非正規型式的戰爭，但可能是在傳統戰爭中被引發或用以支持其原有戰爭目的；國家也可能在傳統戰爭中運用非傳統手段以達到目的。因此國家應準備應付一系列全光譜衝突。

一、衝突的擴散

混合式戰爭（hybrid warfare）是近年北約提出的新概念，指國家或非國家對手採用正規戰、非正規戰、武裝民兵、偽裝平民等方式，也可能包括其他可能對敵產生影響的方式，如心理戰、網路戰、法律戰，甚至包括恐怖攻擊或非法行動等，對國家安全造成威脅。這可能由不同的組織發起，也可能由相同的組織同時發起不同的行動。在戰略層級，許多戰爭均結合傳統及非傳統要素，但常發生在不同戰區或不同場景，在混合戰爭中，則有可能同時在同一戰場上發生。

911 事件後美國在中東發動反恐戰爭，打擊神學士組織，雖然幾乎使其瓦解，但也在伊拉克境內造成權力真空。2014 年時，伊斯蘭國（ISIS）在伊拉克境內推進，伊斯蘭國使用混合戰術對付傳統伊拉克部隊，據有伊拉克大片領土，以及油田與煉油廠等據點用以獲取資金，支持其恐怖行動。以美國為首的西方國家，繼續與伊斯蘭國作戰，也幾乎將其擊敗。然而恐怖組織化整為零向歐洲國家等滲透並發動恐怖攻擊，造成歐洲國家安全及社會安定的困擾。

另外，混合戰爭有可能導致國與國間真正的戰爭。北約已認知混合戰爭對其成員國造成的安全威脅，因此認為採取適當手段有其必要，俄羅斯以類似手法在其周邊前蘇聯共和國併吞領土，北約認為會員國受到來自國家及非國家角色的挑戰已日益增長，並警告俄羅斯有可能對北約成員國使用類似手法。這些混合戰爭手段很可能違反公約第 5 條，即對任何成員國攻擊視同對所有國家攻擊，這將使北約認定混合戰爭是一次真正的武裝攻擊行動，要以防禦及嚇阻手段加以反制。這也表示，北約讓全世界注意到，混合戰爭可能引起更廣泛的戰爭行動。³⁰但混合戰爭的型態恐難以傳統方式加以嚇阻，例如俄羅斯以假新聞干預北約成員國選舉，此事本身即難論定，更遑論加以反制。北約亦聲稱要建立「反制混合支援團隊」，由跨北約的專家及資源組成，反應對北約機構及設施的威脅。

二、混合戰爭的先制條件

俄式的混合戰爭容易識別，其效用以軍事設施為主，包括在邊界部署不合理的部隊，以進攻性質為主的大規模演習，在國際海空域進行挑釁式演習，另包括網路攻擊、激進式的媒體攻擊，以及其他活動。否定式的媒體宣傳是其主要模式，

³⁰ “Now NATO Says Russian “Hybrid Warfare” Could Start a Real War,” *Popular Mechanics*, July 13, 2018, <https://www.popularmechanics.com/military/a22140482/nato-russia-hybrid-warfare-start-a-war/>。

以烏克蘭—俄羅斯邊界衝突為例，俄運用宣傳攻勢，不斷在國際媒體聲稱「俄並未部署軍隊在烏克蘭境內」、「俄絕未提供武器給分離主義份子」，在其目標群眾及國際社會中製造混淆。

混合戰爭有其先制條件，在俄烏衝突的情況下，成功實施混合戰略至少有 5 個關鍵先決條件。首先，俄方具備軍事優勢。二，其中一方中央權力被削弱，或是其安全結構失調。三，一方境內有與另一方同質性高的俄語少數民族，成為侵略者聲稱的目標。四，兩方都有強大媒體存在，允許大規模的宣傳活動。最後，邊防安全的脆弱。這些要素缺一不可，因為全頻譜的混合戰爭無法孤立運作。³¹

靈活及適應性是其混合戰模式的關鍵，不會有兩場完全相同的混合戰爭。西方國家也不能免於混合戰爭的威脅，這些威脅可能輕易而迅速地演變為混合戰爭，如果沒有得到妥善解決和反擊，有可能會演變成傳統戰爭。混合戰爭並不是新鮮事，而且可以有不同的型式，而且會隨時間推移改變及適應，現代國防及國家安全體系應認真對待混合式的威脅。

小結

本章討論未來戰場特性，包括技術及非技術領域，以及高科技及非科技手段，或是兩者的結合。在未來作戰中，各軍種的角色將大幅擴展，界限也日益模糊，太空的角色會更形重要；而在戰場上，因少子化及募兵已是世界趨勢，採用自動化操作的戰場機器人和無人載具的角色會日益重要，不但取代人力負荷搬運彈藥等沉重工作，減少士兵的負擔，也可因使用機器人在敵火下作業，可減少人員的傷亡。無人載具也可代替執行長時間海、空域監視等耗時耗力的枯燥工作，若結合人工智慧，在平時及戰時的運用將日益寬廣。

由於戰爭型態多樣化，不僅武器系統、作戰編組也要彈性化，以模組化方式因應任務的不同需要。然而，除戰場上的短兵相接外，混合型的作戰模式，結合輿論、網路、心理、媒體、恐怖攻擊等等不同方式的非正規作戰，在高科技的時代，因資訊傳播的快速，反而更發揮其作用，也成為未來戰場作戰的特性之一。

³¹ “Hybrid Warfare: A Known Unknown?” *Foreign Policy Blogs*, July 18, 2016, <http://foreignpolicyblogs.com/2016/07/18/hybrid-warfare-known-unknown/>。

第二篇 關鍵軍用科技的發展

第三章關鍵軍事科技的發展

許智翔、蔡榮峰¹

前言

古今戰史上總能找到科技差距成為戰爭勝敗決定性因素的例子，而最近的明顯例子，正是 1990 年代初期的波灣戰爭。該役展示在世人面前的，是美軍為主的聯軍在科技優勢之下以懸殊的比例，消滅了當時擁有強大陸空軍力的伊拉克軍隊，證明軍事科技維持優勢的重要性。在 21 世紀已經過了接近二十年的現在，各種軍事技術的發展又再次到了關鍵節點，當前發展的技術很可能在不久的未來大幅改變戰場的樣貌，甚至戰爭的形式。

壹、戰場機器人

不同於一般機器學習 (machine learning) 多處於封閉或半封閉式環境，變幻莫測的戰場屬於開放式環境，即使對於搭載人工智慧 (Artificial Intelligence, AI) 的機器人來說，仍然是一大挑戰。世界各國現階段尚未有任何全自動武器系統，能夠將戰術目標誤判機率維持在人類士兵同等水準，並在沒有人工涉入的狀態下，自動完成從偵測、追蹤、辨識、獨立接戰等戰場及時應處，大多仍處於人工遙控的階段。最先進的技術也僅能在相對單純的戰術環境下，完成自主偵測與殲敵任務，且無法完全脫離人工監控。

戰場機器人的性能評估共有四大面向：火力 (firepower)、機動性 (mobility)、續航力 (endurance)、通訊技術 (communications)。當前大部分的戰場機器人研發，主要目標擺在人機協同作戰，因此輔助性質多於單兵作戰，大多研究聚焦維持續航力，以及整合戰情資訊兩方面。²戰場機器人依其戰術自主程度，可分為以下三種等級：

「人工控制」(human-in-the-loop weapons)：目標選擇與火力射控皆由人類下指令。

「人工監控」(human-on-the-loop weapons)：機器人可在人類監視下，自主完成目標選擇與火力射控，必要時以人工指令介入程序。

「無人工涉入」(human-out-of-the-loop weapons)：自主完成目標選擇與火力射控，過程無須任何人機互動。³

戰場機器人與工業機器人最大的差別在於，前者需要在複雜環境當中擁有判

¹ 許智翔，國防安全研究院先進科技與作戰概念研究所博士後研究，負責本章第貳、參、肆節；蔡榮峰，國防安全研究院國防資源與產業研究所研究助理，負責本章第壹節。

² Horowitz, Michael C., "Military Robotics, Autonomous Systems, and the Future of Military Effectiveness," in *The Sword's Other Edge*, Cambridge University Press, 2017, pp. 161–96.

³ Docherty, B., "Losing Humanity: The Case Against Killer Robots," *Human Rights Watch & International Human Rights Clinic*, November 19, 2017, p. 2, https://www.hrw.org/sites/default/files/reports/arms1112_ForUpload.pdf。

別敵方單位的能力。若接戰所需的關鍵技術未達門檻，戰場機器人戰術誤判的風險，很可能導致戰略失敗而失去其運用價值。因此戰場機器人發展初期階段，可能率先投入實戰的，集中於無人載具技術與穿戴型兩大類，而是否導入支援人機協同作戰的AI與配備何種先進控制技術，則將決定下一代戰場機器人性能優劣。

一、最新發展

美國國防部 2018 年 8 月 28 日公布《2017-2042 無人系統整合藍圖》(Unmanned Systems Integrated Roadmap 2017-2042)，針對 2035 年為止，美軍應具備之「機器人與自動化系統」(Robotic and Autonomous Systems, RAS) 能力水準，提出了戰術整合概念，作為未來 20 年技術推進目標，主要內涵有以下 8 項指標。

「具有學習能力」(ability to learn)：RAS 能夠透過自動學習如何與戰鬥人員互動或適應環境。

「擴大戰況覺察」(greater situational awareness)：RAS 能夠在日趨複雜的戰場上，搜集跨領域資訊、分析整合並依重要性排序，供戰術決策使用；

「超越人類的勤務表現」(enable higher performance)：環境耐受度、持久性與資訊處理速度能優於人工控制系統。

「提升戰場效率與效能」(improve efficiency and effectiveness)：RAS 能應用的戰場類型多元化，可大幅提升部隊作戰表現。

「裝備相容更有彈性」(provide greater flexibility)：RAS 軟硬體更新與支援將更有彈性，以便配合聯合作戰部隊 (Joint Forces)。

「加快機器運轉節奏」(increase tempo by operating at machine speed)：RAS 能夠運用情報監視偵查系統 (Intelligence, Surveillance and Reconnaissance Systems) 現場資訊，進行大數據運算，搶先敵方自動部署至戰術有利位置。

「提供量產潛力」(provide potential to generate mass)：有別於現階段聯合作戰部隊使用的武器大多昂貴精密且難以短時間大量製造，RAS 較有機會以相對低廉之價格量產。

「有利分散式戰術行動」(enable distributed and dispersed operations)：考量到敵方科技發展屆時精準度與範圍已有所提升，過度集中容易遭敵實施重點打擊，透過 RAS 進行分散式戰術行動能降低任務失敗風險。⁴

依照上述 8 項指標，以下選出 5 種即將邁入實用化以及研發中的戰場機器人先進科技：

(一) 無人地面載具

無人地面載具 (Unmanned Ground Vehicle, UGV) 本質上是一種地面機器人載台，目前大多屬於遠程控制，搭載 AI 後可部分自主行動。被認為可用來克服

⁴ “Unmanned Systems Integrated Roadmap 2017-2042,” U.S. Department of Defense, August 28, 2018.

戰場環境的枯燥 (dull)、危險 (dangerous)、骯髒 (dirty) 的「3D 問題」。UGV 能夠長時間監視與偵查，協助提高地面作戰單位的「戰況覺知」(situational awareness)、減輕兵員荷重來提高戰場效能與機動性、強化第一線後勤補給能力。搭載火力的 UGV 還能掩護部隊移動、擴大有效縱深及擴張接戰距離。⁵UGV 的類型與尺寸也能針對不同地形與戰術需求來設計，例如體積小、具機器單臂、專門用於偵察的機器車「龍行者」(Dragon Runner)。⁶或是屬於「仿生機器人」(biomorphic robot)、能夠負重 182 公斤達 32 公里之遠的「LS-3」，⁷或是能夠負重 150 公斤、時速 10 公里、能爬 35 度角坡度、專門用在後勤支援的大型機器狗「BigDog」。⁸

美國陸軍「次世代戰鬥車輛跨職掌團隊」(Next Generation Combat Vehicle Cross Functional Team) 負責人卡夫曼准將 (Brig. Gen. Richard Coffman) 表示，下一代幾乎所有戰鬥車輛都會具備不同程度的無人自主功能或是搭載機器人，如「可置換載人戰鬥車」(Optionally Manned Fighting Vehicle, OMFV) 未來將取代「布萊德雷型戰鬥車」(Bradley fighting vehicle, BFV)，作為下一代重裝部隊運輸車。「M113 裝甲人員運輸車」將被「武裝多功能車」(The Armored Multi-Purpose Vehicle, AMPV) 取代。美國陸軍也打算發展支援空中部隊或輕裝步兵的「機動掩護火力 (Mobile Protected Firepower, MPF) 輕型坦克」、機器人戰鬥車 (Robotic Combat Vehicle, RCV)，以及足以取代現有 M1 主戰坦克 (M1 Abrams main battle tank) 之無人坦克系統。⁹

除了美國之外，俄羅斯軍工企業卡拉什尼科夫 (Kalashnikov) 也於 2018 年 1 月宣布該公司的 7 噸輕量無人坦克「Soratnik」進入實測階段，遙控有效範圍 10 公里，時速達 40 公里，除了火力之外，還可負責偵察巡邏及排除地雷。¹⁰已經列裝的多功能機器坦克「Uran-9」與「Uran-6」則首次於 5 月 8 日勝利日閱兵亮相，俄國軍方進一步表示擬研發 BMP-3 及 T-72B3 型無人坦克，¹¹中國解放軍的「59 式遠程控制無人坦克」也傳出進入驗證階段。¹²

⁵ “U.S. Department of the Army,” *The U.S. Army Robotic and Autonomous Systems Strategy*, March 2017.

⁶ “Dragon Runner,” *Qinetiq North America*, <https://qinetiq-na.com/products/unmanned-systems/dragon-runner/>。

⁷ “LS-3,” *Boston Dynamics*, <https://www.bostondynamics.com/ls3>。

⁸ “BigDog,” *Boston Dynamics*, <https://www.bostondynamics.com/bigdog>。

⁹ “Robot Aircraft For Robot Tanks: GD & AeroVironment Team Up,” *Breaking Defense*, October 9, 2018, <https://breakingdefense.com/2018/10/robot-aircraft-for-robot-tanks-gd-and-aerovironment-team-up/>。

¹⁰ “Russia tests robotic strike vehicle in conditions close to real combat,” *TASS*, January 19, 2018, <http://tass.com/defense/985821>。

¹¹ “УВЗ начал работу над танком-роботом на альтернативном «Армате» шасси Т-72,” *РБК*, August 8, 2018, <https://www.rbc.ru/politics/08/08/2018/5b62d8979a794742d5e293fd>。

¹² <俄專家：中國測試無人駕駛坦克，是新聞但並不轟動>，《俄羅斯衛星通訊社》，2018 年 3 月 30 日，<http://big5.sputniknews.cn/opinion/201803301025044263/>。



圖 3-1、大型機械狗 (BigDog)

資料來源：Boston Dynamics。



圖 3-2、「龍行者」機器車 (Dragon Runner)

資料來源：QinetiQ North America。

(二) 外骨骼

「市街戰」(urban warfare) 作為未來戰爭的主要型態之一，複雜的都市環境

以及建築障礙物，使正規部隊大規模火力受到限制，如何提高步兵單位的偵察裝備與輕兵器的效率、提高近距離戰術能力，逐漸受到重視。此外，提高士兵生存率，也有助於降低民主政府的決策風險。「外骨骼」(Exoskeleton) 穿戴式人體載具，即為此趨勢而生，這種先進單兵戰鬥系統，整合了人體載具與新式裝甲的複合功能，可提供單一士兵具備更強的負重能力與抗彈性能，提高單兵戰術價值，源起於 2008 年美國國防部的「陸地戰士」(Land Warrior) 系統，其主要目的在於整合步兵的指揮、管制、通訊、觀測，使其具備完整的戰場管理能力、提高主動作戰能力。同時，負重及抗彈等被動防護能力也獲得提升。對於攻堅部隊來說，可作為輔助裝備，增加瞬間打擊力；在守勢作戰、場站後勤的搬運用途等不需長時間倚賴補給的情況，將可立即發揮效益。¹³

俄國「中央精密機械研究所」(TsNiiTochMash) 於 2018 年 8 月底公布「Ratnik-3」戰術外骨骼系統，美軍的「ONYX」以及「TALOS」系統也預計在 2021 年前陸續投入實戰。¹⁴不過，外骨骼裝備的應用現階段受限於續航力，使得實際應用價值大打折扣；俄國的「Ratnik-3」電池續航力低於 4 小時，而美國的「ONYX」測試也僅有 8 小時，無法滿足野戰部隊的需求。如何改良電池技術以及尺寸小型化，成了目前美俄兩國在外骨骼開發上的競爭重點。¹⁵

(三) 非侵入性腦機介面系統

借重神經科學所發展出來的義肢控制技術，已經能夠用腦波做為輸入訊號，然而這類技術控制訊號精確程度有限，易受外在環境干擾，也離不開醫學手術，並不完全適用於肢體健全、在複雜環境移動的操縱者。

美國「國防先進研究計畫署」(Defense Advanced Research Projects Agency, DARPA) 在「Neuro-FAST」侵入性腦神經研究專案 (Neuro Function, Activity, Structure, and Technology) 於 2018 年暫告一段落後，¹⁶同時開啟了「次世代非手術神經科技計畫」(Next-Generation Nonsurgical Neurotechnology program)，又被稱為「N³」計畫，希望利用接下來 4 年的時間，發展出一套雙向 (bidirectional)、即時 (real-time)、非侵入性 (noninvasive) 的腦機介面系統 (brain-computer interfacesystem)。

結合生醫工程學、神經科學、合成生物學以及奈米技術，「N³」系統將研發目標設定為為可攜式、零手術、高解析度的大腦訊息讀取與輸入系統。利用機器學習能力，「N³」系統將能自動校正不同操控者生理差異，自動對接大腦訊號與

¹³ 蘇紫雲，《外骨骼載具的科技競爭與分析》，《國防安全週報》，第 12 期，國防安全研究院，2018 年 9 月 7 日。

¹⁴ “This Army unit will be first to test an exoskeleton that lightens combat load,” *Army Times*, June 5, 2018, <https://www.armytimes.com/news/your-army/2018/06/05/this-army-unit-will-be-first-to-test-an-exoskeleton-that-lightens-combat-load/>。

¹⁵ Patrick Tucker, “Russia, US are in a military exoskeleton race,” *Defense One*, August 30, 2018, <https://www.defenseone.com/technology/2018/08/russia-us-are-military-exoskeleton-race/150939/>。

¹⁶ “Neuro Function, Activity, Structure, and Technology (Neuro-FAST),” DARPA, <https://www.darpa.mil/program/neuro-function-activity-structure-and-technology>。

操作訊號。如何克服外部環境以及人類身體組織對大腦訊息的干擾，預料將是「N³」系統所面對的首要難題。¹⁷

(四) 戰聯網

伴隨著戰場機器人功能的多樣化，有些可能外觀像人類，有些可能體積小如昆蟲，海、陸、空、太空、網路五大領域的戰場機器人，該透過何種戰術控制系統來進行虛實整合將成為一大考驗。讓機器人彼此之間能進行即時戰況交流、協助人機與多機協同作戰的「戰聯網」(Internet of Battle Things, IoBT)，正悄悄進入各國國防部的視野，例如美國國防部就與產學單位成立「協作研究聯盟」(Collaborative Research Alliance, CRA)，¹⁸擴增研發能量，並推出「分散式協同情資系統與技術」(Distributed and Collaborative Intelligent Systems and Technology, DCIST) 研究計畫希望加速戰聯網投入實際應用。¹⁹

雖然戰聯網仍然還在發展初期，不過在架構上起碼必須具備以下能力，才算是邁入實用門檻：

「情報分發」(intelligence distribution)：能即時判斷那些戰情該送給那些協作單元，並且能依照重要性而非時間排序傳送；

「異團體控制」(heterogeneous group control)：指令下達能夠因為次團體戰術任務之差異而有所不同，自動拆解成細部單元指令，達成化整為零之目標；

「分析彈性」(analytical resilience)：複雜戰場環境的訊息來源繁雜，必須能夠將接收戰情標準化以利決策，AI 戰場機器人必須要能考慮「整體」戰術目標，適時調整與環境的互動方式；

「多重介面相容性」(multi-interface compatibility)：戰聯網的升級與配備相容性需要特別設計，以符合國防工業產業生態之特性，並且在人機互動介面需要顧慮人類與機器人資訊處理速度之差異。

目前，戰聯網面臨的主要挑戰在於機器學習的戰場反應仍無法跟上人類士兵的水準，因此情資分送與分析彈性程度有限、網路攻擊抵抗能力不足、人機溝通介面無法滿足實際戰況需要。未來這三個面向，將是戰聯網建置需要克服的重點項目。

(五) 太空衛星組建能力

美國海軍學院(USNA)研發中的「智慧太空組裝機器系統」(Intelligent Space Assembly Robot System, ISAR)，目標是在衛星軌道上高速移動的情況下組建衛星。第一台 ISAR 機器人名為「RSat」，是一顆 3 單位立方衛星機器人(30 cm x 10

¹⁷ “Nonsurgical Neural Interfaces Could Significantly Expand Use of Neurotechnology,” DARPA, March 16, 2018, <https://www.darpa.mil/news-events/2018-03-16>。

¹⁸ “Internet of Battlefield Things (IoBT) Collaborative Research Alliance (CRA),” Duke University, May 8, 2017, <https://researchfunding.duke.edu/internet-battlefield-things-iobt-collaborative-research-alliance-cra>

¹⁹ “Distributed and Collaborative Intelligent Systems and Technology (DCIST),” United States Army Research, Development and Engineering Command (RDECOM), <https://www.dcist.org/wp-content/uploads/2018/07/DCIST-CRA-Introduction-1.pdf>。

cm x 10 cm)，擁有一台 3D 攝影機與環境感測器，以及兩隻長度 60 公分、4 個關節、最大移動角度 7 度的機器手臂，皆配備零後座力馬達以及前端 2D 攝影機。

「RSat」預計 2018 年 12 月在紐西蘭與 NASA ELaNa XIX 立方衛星一起，由 Rocket Lab 公司承包發射升空。「RSat」機器人輕巧的體積，將有利修復細部破損，或是建造立方衛星。²⁰而 NASA 的「蜻蜓軌道衛星組建計畫」(Dragonfly On-Orbit Satellite Assembly Program) 則是注重在機器手臂的功能多樣化，能夠修理目前已經運作的各式太空基礎建設。²¹

希望開發近地軌道衛星低成本開發技術的國防先進研究計畫署「鳳凰計畫」(Phoenix program)，2017 年 10 月則是直接從國際太空站施放了 6 枚「HISat」微衛星 (Hyper-Integrated Satlets)，於 2018 年啟動「eXCITE」實驗計畫評估其施放成效與運作情況；「鳳凰」計畫採取的策略則是將微衛星結構模組化，提高衛星的替代性。²²

二、應用

戰場機器人科技涉及 AI、機器人學 (Robotics)、控制理論 (Control Theory) 三大領域。因此具有軍民兩用特性，相關技術能夠轉入民生、厚實工業，使得各國競相發展。當前投入最多資源發展戰場機器人的前 11 大國，正好也是全球武器輸出占比最高的國家。²³然而同時，也因為戰場機器人被歸類為「致命自主武器系統」(Lethal Autonomous Weapon Systems, LAWS)，諸多技術應用議題牽涉到戰爭倫理問題，國際輿論、非政府組織、AI 專家近年來紛紛疾呼，國際間應該比照大規模毀滅性武器，將機器人軍事化的風險管控，納入國際條約體系。如何降低風險，可說是戰場機器人開發近年來遇到的一大難題。

《聯合國特定常規武器公約》(Conventions on Certain Conventional Weapons, CCW) 123 個締約國已同意，各國政府自 2017 年起針對包括機器人與無人機技術在內的 LAWS，定期召開討論會議，邀集政府專家與非政府組織共商監管機制；參與國家包括美國、中國、俄羅斯等戰場機器人主要開發國家。然而 2017 年 11 月、2018 年 4 月及 8 月三場會議以來，各方意見仍然有待整合。²⁴

²⁰ Dakota L. Wenberg, Thomas L. Lai, and Jin S. Kang, “Miniaturizing the Robotic Assembly of Spacecraft: ISAR Development and On-Orbit Demonstration,” United States Naval Academy, SpaceOps Conferences Paper, January 1, 2018, <https://arc.aiaa.org/doi/10.2514/6.2018-2704>。

²¹ “NASA Awards SSL Next Phase Funding for Dragonfly On-Orbit Assembly Program, Demonstrates Confidence in Public Private Partnership for Space Robotics,” *SSL*, September 11, 2017, <https://www.sslmda.com/html/pressreleases/2017-09-11-NASA-Awards-SSL-Next-Phase-Funding-for-Dragonfly-On-Orbit-Assembly-Program-Demonstrates%20Confidence-in-Public-Private-Partnership.php>。

²² “On-Orbit Assembly of Space Assets: A Path to Affordable and Adaptable Space Infrastructure,” The Aerospace Corporation, February 2018, https://aerospace.org/sites/default/files/2018-05/OnOrbitAssembly_0.pdf。

²³ 美國、英國、俄羅斯、法國、義大利、日本、以色列、韓國、德國、印度、中國（未按軍火出口占比順序），參見“Mapping the Development of Autonomy in Weapon Systems,” *SIPRI*, November 2017.

²⁴ “2018 Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS),” UNOG, [https://www.unog.ch/80256EE600585943/\(httpPages\)/7C335E71DFCB29D1C1258243003E](https://www.unog.ch/80256EE600585943/(httpPages)/7C335E71DFCB29D1C1258243003E)

考慮到快速浮出的國際法爭議，預料率先投入實戰之戰場機器人相關科技，將首先處理如何優化人機協同作戰的問題，以及在尚未成為人類士兵戰場的太空爭奪制太空權以防止遭到敵方剝奪軍事偵察能力。

（一）人機一體控制系統

非侵入性腦機介面系統的發展，也預示人機一體的時代即將到來。一旦如波士頓動力公司（Boston Dynamics）的 Atlas 系列等人型機器人技術成熟之後，除了能自主思考的 AI 戰場機器人之外，由士兵腦控的「阿凡達」（avatar）戰場代理機器人，將成為另一種「避免道德困境」的研製選項。當然，過渡階段也可能發展出由單兵阿凡達帶領一群 AI 機器人的戰術戰法。

此外，這類腦機控制系統也能將戰聯網「微觀調控」的特性，導入戰鬥人員與其操作的武器系統之間，如飛行員頭盔能在戰機高速飛行的狀況下，逆向輸入訊號穩定飛行員大腦。又或是狙擊手頭盔能在潛伏時保持大腦清醒、狙擊時提高專注能力並且能透過腦波校正槍枝瞄準等等。除了武器裝備與人型機器人以外，各類遙控無人機的操作介面也可能更加「隨心所欲」。未來人機一體控制系統外溢效應更可能促使外骨骼技術向「巨大化」、「多功能化」的方向發展。

（二）讀心戰情指揮系統

搭載 AI 的戰聯網，未來將能夠做到透過戰場資訊即時蒐集，預先分析敵方可能採取的下一步動作，若能取得敵方指揮官各種人際互動資料，甚至可能做到透過演算法預測出未來可能採取的策略選項有哪些，提供戰情指揮決策者使用。暫且可以將其想像為目前網路社群商業 AI 運用模式轉化為國防用途。此外，戰聯網也能夠用來分析敵方戰聯網如何預測我方下一步，以利人類指揮官發動不對稱戰術或奇襲。

值得注意的是，戰聯網搭配人機一體控制系統之後，理論上將使得目前由單人指揮的機器人數量上升到戰場規模，種類還可能同時橫跨陸海空、網路及太空，在 AI 的協助下，它們將表現得像是協同作戰的士兵，而且十分「善解人意」。真實戰場指揮將與策略性電玩操作產生趨同現象，在人類參與較少的戰場上，電子兵推的準確度也會大幅提升，其結果進而對各國領導人之戰爭決策產生，影響層面將遠遠超越軍事範疇。

（三）衛星軌道戰術運用

軍事衛星在戰情指揮以及戰略武器攻防上的應用價值，以及難以取代的精密特性，使其容易成為敵方重點打擊目標。當前的太空機器人科技受制於現有衛星技術的特性所影響，側重「遠端控制」（remote control）以及「一次性打擊」（one-off destruction）。不過隨著太空軍事化的趨勢逐漸白熱化，可重複利用的火箭系統、低成本的立方衛星（CubSat-Class satellite）逐漸普及，衛星防護策略開始從

原有的「本體防護」轉向「撒豆成兵」，藉由模擬核武平台多樣化來保證太空戰略優勢；只不過與海中的核子潛艦不同，未來的太空戰略將不再以衛星匿蹤能力為主軸，而是以韌性（resilience）為核心，意即原有衛星遭摧毀後，能迅速藉由其他衛星的替補來恢復運作。

太空基礎建設出現微型化趨勢，具有相同功能的衛星體積正快速縮小，進入立方衛星的時代，而擁有微衛星模組化技術，意味著敵方反衛星能力失去其作用，進而影響到其區域拒止的太空打擊效用。更有甚者，發展初期只用來修復的太空組裝機器人，一旦技術成熟，將可在衛星軌道上以「無發射建造」方式，來部署己方衛星，或是寄生、撞擊敵方衛星。不僅對於地球上的戰況產生作用，在本世紀的月球資源探勘競爭上，應用潛力不容小覷。

貳、匿蹤科技

自 1991 年波灣戰爭中美軍 F-117A 匿蹤戰機成功穿透伊拉克防空網、一戰成名以來，對抗雷達偵測的匿蹤技術成為各大國技術單位於軍方最高度注意之技術項目之一，而近年來對抗各式偵測手段的技術皆得到大力發展及應用。

匿蹤（stealth），又稱「低觀測度」（low observability），為透過設計、特殊材料、塗料等方式，減少透過可見光、雷達、紅外線、聲納等媒介偵測到載具之技術。其中尤以降低雷達截面積（Radar Cross-Section, RCS）為目前對匿蹤一詞最常見的含意，並成為現今戰機設計最重要的指標之一。此種針對雷達偵測之匿蹤技術近年來可於飛行器、船舶、飛彈在內等多種武器系統上見到其運用，船艦雖然同樣可運用匿蹤技術降低其可偵測性，然而其本身即極為龐大的體積與海面雜訊等使其在運用匿蹤設計上運用仍然相對有限。由於匿蹤的高技術門檻，使得當今實際操作匿蹤戰機的國家仍然有限，僅美國已有大量具高度匿蹤性能的戰機服役運用，中國與俄羅斯則緊追在後、研發具相當匿蹤性能之戰機。

一、當前發展與軍事應用

就武器系統而言，當前最受矚目的即是包括美國 F-22、F-35、B-2 在內的匿蹤航空器，以及匿蹤船艦如美國朱瓦特級（Zumwalt class）驅逐艦等，而台灣海軍所操作之法製康定級巡防艦與沱江級巡邏艦，亦是在設計之初即考慮匿蹤性的艦艇。以下以當前最具發展之降低雷達 RCS 匿蹤技術為主，簡要提及紅外線訊號匿蹤技術，並對當前發展進行評估。

（一）降低 RCS

目前減低 RCS 主要的手段有二，包含透過運用材料以減少雷達波反射，與匿蹤外型設計。前者包含了機身材料與雷達波吸收材料二者；早期先由降低雷達波反射材料打造機身開始，延伸到以雷達波吸收材料（radar-absorbing materials, RAMs）作為材料及塗層，以減少遭到雷達發現的機率。最重要的則是藉由載具本身的外型設計，盡可能降低雷達反射面數量減少低雷達回波，其方式包括採用

：減少垂直面，邊緣平行，鋸齒狀結構，蛇行進氣道，將武器內置於彈倉中等各種方式，以減少外掛武器在匿蹤上的不利影響。藉由三者（外型設計、機身材料與塗料）相互配合，達成高度匿蹤。隨著匿蹤技術的進展，匿蹤戰機早已不再需要如同早年美國 F-117A 戰機一般極具特色的稜角幾何外觀、而出現更為流線，較能兼顧氣動力與空戰機動的設計。

當前最新式戰機的設計方向有二，首先是追求更佳匿蹤性能，如 2018 年英國宣布之下一代戰機「暴風」(Tempest) 以及德法將共同發展的未來空戰系統 (Future Combat Air System) 等，皆走向透過如過往美國 ATF 計畫中落敗的 YF-23 一般，多以融合水平尾翼與垂直尾翼為一體等方式，進一步嘗試加強其匿蹤性。但戰機設計需考量其空戰機動性能，因此匿蹤外型設計仍需與氣動力構型互相妥協。此外，目前亦有多種新式戰機設計相當程度運用匿蹤設計，但有相當程度妥協，例如維持傳統外掛武器方式，以尋求較低的技術門檻與成本，以求加速研發，如韓國 KF-X 戰機計畫，這種戰機預計在第二批次 (Block 2) 才追加內部武器艙。²⁵ 土耳其的 TFX 戰機計畫也選擇了傳統的通用電器 F110 發動機，亦可視為一種妥協。²⁶ 事實上，對於技術與資源較少的國家而言，後者亦是可能之途徑，以減少與擁有先進匿蹤戰機的國家之技術及與之造成的軍事劣勢。此外，日本近年亦曾投注大量資源研發、驗證 X-2「心神」驗證機，然在技術驗證完成後即因龐大經費負擔而停止發展，未進一步發展為實際服役之武器系統。²⁷

就目前其他國家實際服役及較有進展的研發計畫來看，中國殲 20 戰機的外型包含其前翼等設計仍可看出其為氣動力妥協之處。俄羅斯研製之 Su-57 匿蹤戰機雖在外型設計上較符合匿蹤設計之概念，然目前仍缺乏良好匿蹤塗料與之配合。因此，目前可說美國在匿蹤技術上仍佔據絕對優勢。在美國匿蹤戰機開始服役後，匿蹤技術包含設計以及塗料等亦開始應用在傳統第四代戰機上，以降低其 RCS，如 F/A-18E/F 超級大黃蜂戰機設計上，即已考量一些匿蹤要素，而大量運用匿蹤塗料，也有效幫助第四代戰機有效降低其 RCS。目前台灣 F-16 戰機升級為 F-16V 的升級案，即包含美軍的 Have Glass 匿蹤技術。在上述的匿蹤重點項目之外，俄羅斯已研發多年的「電漿匿蹤」是另一途徑。透過注入電漿流以吸收雷達波、並減低反射，如研發成功，或可因此不需考量外型之匿蹤設計，然此項概念目前仍未能順利實用化。

在船艦上，則因前述包含船艦本身體積與海面雜波、船舶的尾流等各種因素都會使得匿蹤設計更加複雜，並且其應用亦不若在飛機上發達。當前的許多主力船艦如我國康定級 (法國拉法葉級)、英國 45 級驅逐艦及美國目前主力的柏克級

²⁵ Defense Industry Daily staff, "KF-X Fighter: Korea's Future Homegrown Jet," *Defense Industry Daily*, October 23, 2018, <https://www.defenseindustrydaily.com/kf-x-paper-pushing-or-peer-fighter-program-010647/>。

²⁶ Burak Ege Bekdil, "General Electric beats Rolls-Royce to power Turkey's indigenous fighter jet," *Defense News*, October 31, 2018, <https://www.defensenews.com/industry/2018/10/31/general-electric-beats-rolls-royce-to-power-turkeys-indigenous-fighter-jet/>。

²⁷ "空自の F 2 後継機、F 3 5 など既存機ベースに共同開発案＝関係者," *Reuters*, March 8, 2018, <https://jp.reuters.com/article/jasdf-replacement-f2-idJPKCN1GK05S>。

(Arleigh Burke Class) 神盾驅逐艦等船隻，皆在設計時已將匿蹤外型加入其設計考量中。除此之外，台灣自製的沱江級巡邏艦也是匿蹤外型的作戰艦艇。許多匿蹤船艦同樣運用塗料以降低雷達反射。

目前最值得注意的匿蹤主力艦艇則是美國海軍朱瓦特級驅逐艦，該級驅逐艦除了達到 14000 噸等級的巨大排水量並搭載先進火炮系統(Advanced Gun System, AGS) 155mm 先進艦砲與 80 組垂直發射系統(VLS) 等強大火力外，其獨特的匿蹤外觀亦是此級艦的一大亮點。朱瓦特級的匿蹤設計超越以往船隻、能降低因海面雜波加強的雷達反射；據稱，其匿蹤設計能使該級艦的 RCS 降到僅為美國目前主力柏克級神盾驅逐艦的 1/50。接下來觀察美國於船艦上運用匿蹤技術的重點，在於其戰力核心的航空母艦在雷達上是極度顯眼的巨大目標，因此如何進一步運用更好的匿蹤技術於船艦上，以及類似技術是否會大量應用在美國下一代巡洋艦 CG(X)、甚至下一代巡防艦 FFG(X)上，而且又要能夠配合整體航艦戰鬥群之運用。就目前所能接觸的消息來看，朱瓦特級的匿蹤船體設計正是 CG(X)計畫所可能採用的方案之一，但後續之發展則仍待觀察。另外，由於海面雜波在雷達偵測上的巨大影響，各種干擾手段如干擾絲與主動干擾系統等，透過干擾甚至「製造」海面雜波以提高自身匿蹤效果，這對各種艦艇匿蹤的重要性，有時候可能更高於外型上的匿蹤設計考量。

在車輛運用上，針對紅外線軌跡與聲音等其他方面的匿蹤，可能較降低雷達 RCS 的設計更加重要。但近年仍能注意到幾款包涵匿蹤考量的地面裝備。過往最值得注意的可能是波蘭於 2013 年所推出之 PL-01 匿蹤輕戰車，其設計概念中，就包含了考量匿蹤的外型與雷達波吸收材料。

最後，這些降低 RCS 的匿蹤技術目前儘管大放異彩、特別在空戰更是如此，但仍有對抗匿蹤的雷達偵測手段。傳統上低頻雷達即是能偵測匿蹤戰機的一個手段，惟其精度有限、目前仍難以導引攻擊匿蹤戰機。當前包含中國及俄羅斯在內可能面對美國高性能匿蹤戰機威脅的國家，都在研發新技術如量子雷達(quantum radar)等，以求與之對抗。2016 年 9 月，中國方面宣稱其量子雷達已經研發完成，並能在 100 公里的範圍內有效偵測匿蹤戰機。²⁸加拿大滑鐵盧大學也在 2018 年 4 月宣布其正在研發新式的量子雷達，而俄羅斯也在 2018 年 7 月宣稱其正在研發一無線電光子雷達(radio-photonic radar)，並可能成為匿蹤戰機殺手等。²⁹然而，即使此類技術能有效對抗匿蹤戰機，仍然需要相當程度的研發之後，才可能在戰場上大規模部屬運用，對雷達的匿蹤技術仍在相當時間內難以遭到反制。包含中俄在內各國目前研發中的新一代戰機計畫，都仍然將匿蹤技術作為其中之重要部分，顯見其在未來仍將持續扮演重要角色。

²⁸ 瓦西里·卡申，〈俄專家：中國量子雷達或致美現代戰機失去存在意義〉，《俄羅斯衛星通訊社》，2016 年 9 月 26 日。http://big5.sputniknews.cn/military/201609261020833490/。

²⁹ Dave Majumdar, "Stealth Killer? Russia's Sixth-Generation Fighter Might Have a "Radio-Photonic Radar"," *National Interest*, July 9, 2018, https://nationalinterest.org/blog/buzz/stealth-killer-russias-sixth-generation-fighter-might-have-radio-photonic-radar-25361。

（二）降低紅外線訊號

針對紅外線訊號的匿蹤技術，不僅對飛機等航空器至關重要，也影響車輛、船艦、甚至人員等。紅外線訊號根據其波長可分為近紅外線、短波長、中波長、長波長以及遠紅外線等不同種類。在軍事應用上紅外線訊號根據其波長不同，分別可應用在夜視鏡、熱顯像儀，甚至到空戰中運用的紅外線導引飛彈（又稱熱導引或追熱飛彈）等各種不同領域。就戰機設計而言，目前為止減少熱紅外線訊號主要透過設計，使熱與冷卻空氣結合，藉排氣尾管的形狀設計以減少其截面積，透過內部油箱分布減少電子設備發熱，使用碳複合材料減低紅外線訊號，或是採用更高旁通比的引擎等方式進行。此外，一些雷達波吸收塗料同樣提供了一定程度減少紅外線訊號的能力。

近來特定材料科學的研究，或許為降低紅外線訊號作為未來的關鍵方向。2018年6月報導顯示，美國威斯康辛麥迪遜大學(University of Wisconsin-Madison)正在研發一基於半導體材料「黑矽」(Black Silicon)的降紅外線訊號材料，有極小的厚度、並可隔絕約94%的紅外線。這種材料在面對各種透過熱顯像進行的偵測系統、甚至紅外線導引武器時，皆可能達到高度匿蹤，極具應用潛力。不過目前這項技術仍在研究初期，有待進一步研發。³⁰

就陸上裝備如車輛及人員而言，降低紅外線訊號同樣十分重要。除了類似飛行器的設計方式外，亦使用具減少紅外線訊號功能的偽裝網或是人員野戰服加強效果。貝宜近年開發的ADAPTIV迷彩系統則是透過輕量、六角形的片材遍佈在載具上，改變溫度影響其紅外線訊號，並可以偽裝成如民用車輛，甚至岩石的熱訊號以欺騙對手。

然而，在陸戰中所需顧慮的並不僅只有紅外線訊號問題，尚包括可見光在內的各種偵測手段。因此，不少當前發展的類似產品不僅止於針對紅外線訊號，同樣包含了對可見光、雷達波偵測等多重頻譜的匿蹤能力。

（三）多頻譜與可見光匿蹤

如前節所述，多頻譜的匿蹤技術的目的為抵擋包含可見光、雷達波等多重偵測手段而生，近年來亦成為西方各國重視的項目，並紛紛開始測試或是採用，如瑞典紳寶梭子魚(Saab Barracuda)公司生產的移動偽裝系統(Mobile Camouflage System)等設備。這種新式偽裝網除了傳統視覺偽裝功能外，對多種光譜皆能遮蔽，包括能有效減少紅外線訊號、雷達波反射與視覺偽裝等功效。³¹

除了前面提到的各種設計及技術外，透過各種材料嘗試減低肉眼的可辨識性同樣是當前正在努力的目標。除了傳統迷彩服持續發展之外，俄羅斯 Rostec 集

³⁰ Sam Million-Weaver, “‘Stealth’ material hides hot objects from infrared eyes,” University of Wisconsin-Madison, June 21, 2018, <https://news.wisc.edu/stealth-material-hides-hot-objects-from-infrared-eyes/>。

³¹ “Germany’s KMW Orders Saab’s Mobile Camouflage System For Leopard 2 Tanks,” *Defense World*, December 20, 2017, http://www.defenseworld.net/news/21568/Germany___s_KMW_Orders_Saab___s_Mobile_Camouflage_System_For_Leopard_2_Tanks#.W-jYsJMzaUk。

團在 2018 年 8 月展出了一款新式迷彩材料，宣稱其電子操作 (electrically-operated) 塗料能使其隨著環境改變色彩、強化偽裝能力，惟目前仍未實際展示與驗證其功能。³²類似技術並不只有俄羅斯正在致力開發，以色列本古里安大學 (Ben-Gurion University) 的研究團隊亦宣稱設計出一種能偏轉光線使人能隱身的方式，但仍需嘗試做出原型。³³儘管這些概念及構想在未來戰場上可能發揮極大作用，然而進一步的發展與驗證皆仍待進行，可以推估各種構想仍須相當時日才能實際進入應用

參、極音速載具

此項技術為軍民兩用，主要應用在武器、航空器以及太空飛行器 (Spacecraft) 等三種方式。當用於軍事用途時，現有主要的兩種極音速載具發展為：透過火箭加入推進至高層大氣 (但較傳統彈道飛彈為低) 並釋放之極音速滑翔載具 HGV，及透過超燃衝壓發動機使其達到 5 馬赫以上速度之極音速巡航飛彈 (hypersonic cruise missile, HCM)。

極音速載具之技術相關概念在數十年前即已提出發展，近年則有長足進步。美國在 2001 年開始測試之 X-43 在 2004 年創下 9.68 馬赫的飛行速度計錄；2010 年開始，並至 2013 年為止共進行四度測試之 X-51 HCM 即採用「乘波體」(Waverider) 設計，使其能藉由飛行產生衝擊波為其自身提供升力；武器化用途亦曾有配合其「迅速全球打擊」(prompt global strike) 概念之「先進極音速武器」(Advanced Hypersonic Weapon) 實驗、及國防先進研究計畫署與洛馬公司合作之 HTV-2 極音速滑翔載具 (hypersonic glide vehicles, HGV) 實驗等。美國並在 2013-2016 年及 2016-2017 年間分別與多家軍火巨擘合作，進行不同的極音速武器研究計畫。然近年來俄羅斯與中國在此技術及其軍事化上，亦受到世人矚目，美國也因而在相關的武器系統研發加緊腳步。

一、當前發展

目前致力於發展此項科技的主要為美、俄、中三國。除此之外，包含日、澳、印及歐洲國家等在內，多項相關技術之研究計畫正在進行。然仍以前述三個國家為主要的技術領先者，其餘國家如印度、法國、澳洲等各國之極音速研究計畫，仍多仰賴與美俄等國進行國際合作。在民用載具方面，包括美國的波音公司與歐盟之空中巴士集團等航空巨擘皆正在進行民用極音速載具之研究，然當前最受到矚目的則屬其軍事用途。

就武器裝備上目前的發展而言，俄羅斯在 2018 年 3 月 1 日宣布了射程 2000

³² Daniel Brown, "Russia just showed off new stealth camouflage that supposedly can change colors rapidly to conceal troops," *Business Insider*, August 21, 2018, <https://www.businessinsider.com/russia-shows-off-new-stealth-camouflage-but-it-appeared-to-be-static-2018-8>。

³³ Shoshanna Solomon, "Israeli researchers develop invisibility cloak – but you can't see it, yet," *Times of Israel*, November 14, 2017, <https://www.timesofisrael.com/israeli-researchers-develop-invisibility-cloak-in-theory/>。

公里、10 馬赫高速之「匕首」(Kh-47M2 Kinzhal) 空射極音速飛彈，可裝置在 MIG-31 戰機及 Tu-22M3 轟炸機上。根據俄方宣稱、此型武器由後者裝載將使其威脅半徑達到 3000 公里之遠。此外，俄羅斯另外亦有一 Project 4202 極音速滑翔武器計畫，預計在將來搭配新型洲際彈道飛彈 RS-28 Sarmat 上，負責搭載核子彈頭，突穿對手的彈道飛彈防禦系統。匕首飛彈應為 9K270 伊斯坎達 (Iskandar) 陸基短程彈道飛彈的空射型，然根據美方估計，其在 2020 年才能完成戰備。³⁴Project 4202 如研發順利，將在 2020-2025 年之間服役。³⁵值得一提的是，相較於美俄兩國，中國在相關領域為較晚進的參與者，但透過大力投資發展，近年積極進行極音速載具研究，並於 2018 年 8 月進行「星空二號」HGV 相關測試。中國在「星空二號」上，如同美國的 X-51 極音速飛行器一般，採用「乘波體」設計。2018 年 9 月 21 日，中國在酒泉衛星發射中心，對三種不同的極音速載具設計之縮尺模型，進行設計驗證技術細節。³⁶中國也曾研發代號為 WU-14 的 HGV，整體來說已經累積相當研發經驗與能量。除三個技術領先的國家之外，印法亦透過與俄羅斯的合作取得極音速武器之相當進展，如印度與俄羅斯共同研發之 BrahMos II 型 HCM 等，在相關武器系統發展上領先美俄中之外的其他國家。

由於各方極音速武器仍需數年研發時間才有可能服役及實際形成戰力，而美國在極音速技術上仍具有相當領先實力，為因應俄中在將其武器化的作為，美國於 2018 年開始加速發展極音速武器，以避免在極音速武器的技術上產生落後，並陷入戰略劣勢。美國在 2018 年與洛馬公司簽約，開始全力投入「極音速傳統打擊武器」(Hypersonic Conventional Strike Weapon) 等計畫。³⁷在這些國家之外，日本亦宣布研發其稱為「高速滑空彈」之 HGV，並預計在 2025-26 年投入運用，並於 2028 年的第二批次 (Block 2) 性能提升型上，加上「乘波體」設計。³⁸

二、軍事應用

蘭德公司在 2017 年報告中指出，極音速技術應用在武器上具有改變當前世界「遊戲規則」的能力；HGV 可在武器系統許可的範圍內、在飛行中更新其攻擊目標，並且能以難以預測之軌跡滑翔。換言之，過往用以攔截彈道飛彈之系統、包含能對抗機動重返載具 (maneuverable re-entry vehicle, MaRV) 之飛彈防禦系統，皆無法反制 HGV 攻擊。HCM 則透過其高速與可操作性同樣大幅壓縮防

³⁴ Dave Majumdar, "Russia: New Kinzhal Aero-Ballistic Missile Has 3,000 km Range if Fired from Supersonic Bomber," *National Interest*, July 18, 2018, <https://nationalinterest.org/blog/buzz/russia-new-kinzhal-aero-ballistic-missile-has-3000-km-range-if-fired-supersonic-bomber>。

³⁵ "Objekt 4202 / Yu-71 / Yu-74," *Global Security*, March 4, 2018, <https://www.globalsecurity.org/wmd/world/russia/objekt-4202.htm>。

³⁶ "China tests three hypersonic missiles at one go," *The Economic Times*, September 30, 2018, <https://economictimes.indiatimes.com/news/defence/china-tests-three-hypersonic-missiles-at-one-go/articleshow/66014665.cms>。

³⁷ Joseph Trevithick, "American Hypersonic Weapons Could Shower Their Targets In Deadly Fragments," *The Drive*, October 30, 2018, <http://www.thedrive.com/the-war-zone/24582/american-hypersonic-weapons-could-shower-their-targets-in-deadly-fragments>。

³⁸ "防衛省、滑空弾研究ブロック化、25年に早期装備型," *JWING*, November 9, 2018, <http://www.jwing.net/news/6855>。

禦系統的對抗能力。需注意的是 HGV 與傳統彈道飛彈概念不同，由於其在較低的高度上持續飛行，因此需強化其飛行能力、設計上須考量低阻力與高升力，並可藉此持續機動。

除了目前攔截系統幾乎無法與之對抗的特性外，極音速武器另外的戰略意義是其大幅縮短決策與反應的時間。因此除了對現有飛彈防禦系統能力的挑戰外，此類型的武器同樣對傳統的決策組織帶來巨大挑戰。其目前仍無法被攔截之特性，使得目前在武器化發展上著墨較多的俄羅斯相當重視透過 HGV 投射戰略核武，藉以擊敗美國當前領先的飛彈防禦技術。美國則因為俄羅斯原本即擁有大量搭配核彈頭的洲際彈道飛彈緣故，認為極音速武器用於核武投射上，並無法對整體戰略情況產生較大衝擊，故更著重於其作為戰術上之運用價值。其對美軍過往所提倡的「迅速全球打擊」概念上扮演極關鍵角色。然而，雖然此種極具威力的武器能夠提供使美國在進行第一擊或是針對關鍵目標發動攻擊時，能取得極大優勢，並在戰略上提供核武以外的另一選項，但面對擁有核子武器的對手，特別是俄中等同樣具有戰略核武打擊能力的國家時，使用此類武器仍須考量對手可能的激烈反應使衝突升級。此外，投射 HGV 時，由於對手難以判斷是否遭遇核子攻擊，因此可能立即遭到核報復。然而，對美軍而言，此類武器在全球海外介入以及遭遇反介入情況時，仍然極具價值。

就 HCM 類型武器而言，進行常規作戰時的用處即非常高。不論是面對陸上高價值目標、或是攻擊海軍艦隊等，皆因其無法防禦之特性，具有極高價值。衝壓發動機用於極音速武器上時的技術難度，也遠高於一般超音速飛彈。因此，當前能發展之國家同樣有限。不過，2018 年 6 月時，以色列展示其能以 F-16 戰機發射、源自於「EXTRA」砲兵火箭之空射型音速飛彈「Rampage」。³⁹此飛彈雖非宣稱為極音速武器，但這種類似俄羅斯將 9K270 伊斯坎達爾飛彈修改為空射極音速飛彈的方式，將可能是其餘國家進入極音速武器研發領域的一可能方式。相較於伊斯坎達爾飛彈需由 MIG-31 等重型戰機，甚至 Tu-22 轟炸機才能掛載的重型武器，以色列的方式或許更適合缺乏重型戰機的國家發展。台灣身為少數有完整衝壓引擎開發經驗的國家之一，進一步研發超燃衝壓引擎，或許是可能之發展方向。極音速武器無法防禦的特性，使其在戰術及戰略上皆能對未來戰場環境產生根本性的影響，因此在可預見的將來，將會使其成為主要大國禁止武器技術擴散的重要對象之一。

肆、集群式攻擊

「集群式攻擊」一詞原用以敘述自然界中集體合作行為，故又稱為「蜂群」。這種概念與無人機結合，使小無人機群在民間運用及軍事行動上皆創造極多的可能性，並能因此進行各種複雜工作。

³⁹ Judah Ari Gross, "Israel says new 'Rampage' rocket will break bunkers, but not the bank," *Times of Israel*, June 14, 2018, <https://www.timesofisrael.com/israel-says-new-rocket-will-break-bunkers-but-not-the-bank/>。

「集群式攻擊」為當前無人機領域重要之發展方向之一，並能在未來軍事應用上扮演重要角色。從非國家行為者藉由較原始的方式，以大量小型無人機發動攻擊，到先進國家以高科技操縱無人機群進行複雜工作，甚至伴隨未來戰鬥機系統執行任務等皆是。就後者來說，無人機群的操作基於自動化與資訊共享，透過軟體建立體系以針對「集體系統」進行操作、並達成單一無人機所無法達成之工作。無人機群組應用上包含二重要特性：「分散式運算」及「系統重構性」。前者意味著無固定長機的無人機群將各自單獨運算，即時交換訊息並各自操作；後者則意味著集群式攻擊整體的運算能隨著外力對結構改變，而立即重新建構，以持續任務進行。

一、當前發展

以國家行為者來說，美俄中歐是目前在無人機領域上發展較為進步的主要國家。無人機技術具有高度的軍民兩用特性，其技術發展帶來的功能多半可同時用於民用與軍用等雙重用途。因此，當前所發展之技術與用途，皆可說是或多或少帶有軍事上的意涵。在 2018 年 2 月南韓的平昌冬季奧運開幕式中，英特爾公司展示了其在 2017 年 12 月所預錄，以 1218 架迷你四軸無人機同時升空快速編隊，排出滑雪選手比賽及奧運會五環標誌等圖像，顯示出無人機群組的巨大潛力。

在操作上較為困難的固定翼無人機上，美國與中國則仍在激烈競爭中。中國不斷嘗試刷新其同時操控的固定翼無人機數量，2018 年 5 月中國宣稱已經成功完成 200 架固定翼無人機的群集飛行。與有人戰機的合作運用更可回顧到 2016 年 10 月，美軍當時以 3 架 F/A-18E/F 超級大黃蜂戰機成功投放 103 架小型 Perdix 無人機群。⁴⁰針對美國在有人戰機與無人機群整合方面的技術優勢，空中巴士（Airbus）於 2018 年 9 月在德國波羅地海沿岸的軍方測試場，進行無人機群與有人飛機的協同操作測試，希望在此美國已經領先的領域上迎頭趕上。⁴¹

此外，英國勞斯萊斯公司在 2018 年 7 月於法茵堡（Farnborough）航空展上，宣布了維修用微型機器人群組之研發計畫，並將透過此項技術、以這些「無人機群組」進入飛機引擎結構內部，深入各縫隙部位檢測。操作人員可以藉此對其受損部位進行修補，顯示出無人機群組技術在戰鬥或監視、偵查等用途之外的新可能性。

二、軍事應用

蓬勃發展使得其軍事應用逐漸分化為小型無人機集群式攻擊與高價、極端複雜、匿蹤之大型無人機兩種截然不同的方向。瑞典 SIPRI 在其報告中指出，目前的技術使無人機群組在軍事上的運用可分為幾種主要用途：協調機動，使陸上、空中或海上的系統能協調進行編隊移動，不論作為長機引導或是僚機；在大型區

⁴⁰ Chris Baraniuk, "US military tests swarm of mini-drones launched from jets," *BBC*, January 10, 2017, <https://www.bbc.com/news/technology-38569027>。

⁴¹ "Airbus conducts MUT test flights," *Shephard Media*, October 4, 2018, <https://www.shephardmedia.com/news/uv-online/airbus-conducts-mut-test-flights/>。

域內協調進行情報、監視與偵查 (intelligence, surveillance and reconnaissance, ISR)；反介入/區域拒止 (A2/AD) 調度及分散式殺傷 (Distributed Lethality)。

嚴格說來，小型無人機集群式攻擊在軍事應用上仍在實驗發展階段，然目前已能透過各種資訊推敲其發展與運用。無人機集群式攻擊由於使用小型廉價（小型無人機在造價上遠較大型精密的高性能無人機便宜）的機型，故而在數量上極為龐大，可以透過群體工作的方式完成各種細微縝密的工作，從監視偵查、到前述維修引擎皆有可能。其龐大的數量亦使其在作戰任務中有較好耐戰損的能力，敵方亦不容易消滅數量龐大的小型無人機群。因此，在戰術運用上衍生出與高價的大型精密無人機不同的運用方式。例如美國國防先進研究計畫署提出的「攻勢集群式戰術」(Offensive Swarm-Enable Tactics, OFFSET)，就規劃讓步兵單位配合超過小型 250 個無人飛行/地面載具，以執行在複雜城市環境中的任務、快速部署與部署突破能力等。⁴²在複雜的城市環境中，各種包括地下道等各式複雜地形，同樣能交由小型無人機進行偵查與地圖繪製。同時，單就攻擊來說，小型無人機群較難以發現，如能有效運用，則可收奇襲之效。除了中國方面媒體宣稱其可藉此對美軍航空母艦在內的大型艦艇進行打擊外，小型無人機群組對各戰略要點、重要設施包括防空系統與雷達，甚至要人等，皆可能透過奇襲方式取得戰果，在整體作戰上取得優勢地位。2018 年 7 月，綠色和平組織在網路上發佈一短片，片中赫然見到其操作小型無人機，衝撞法國核廢料儲存設施，以顯示此類設施對類似攻擊的無力與無防備的嚴重程度。但此短片亦顯示出小型無人機難以被發現的特性，使其在攻擊行動中，可能造成奇襲效果。

在各國軍方的規劃中，將來無人機集群式攻擊除了地面及海上發射使用外，也能從戰機等飛行器中投放，並與之成為整合作戰系統。在空戰中，小型無人機的用途上並不限於偵查、監視與攻擊，無人機同樣可以保護有人戰機、執行防禦任務。從前面提到的發展可知，美國在此方面仍有較領先之技術。但環顧美俄中歐（包含英國的暴風式戰機與德法的未來空戰系統）等各項對未來戰機的規劃與計畫，皆有意將無人機與有人戰機整合為全面性之系統，足見此技術的重要性，及其在未來戰場上的地位。未來以微型機器人集群式維修引擎的技術，亦或可為飛行器在必要時提供應急修理，在民間及軍事上皆可能有極大用途。

在高科技的無人機集群式攻擊作戰之外，如同前面所提到的非國家行為者同樣嘗試以較簡單的方式，進行類似集群式攻擊的作戰方法。2018 年 1 月，俄軍在敘利亞遭到敵對武裝份子以 13 架簡易無人機進行攻擊，成功造成俄方人員傷亡及停放在機場的多架俄國軍機受損。雖然俄羅斯軍方宣稱其捕獲三架無人機，同時防空砲火擊落另外兩架，⁴³其造成的損失單就價值上來說，遠超過這些小型無人機群。可見得小型無人機在非國家行為者的使用上，甚至遭到恐怖分子運用

⁴² Dr. Timothy Chung, "OFFensive Swarm-Enabled Tactics (OFFSET)," *Defense advanced Research Projects Agency*, <https://www.darpa.mil/program/offensive-swarm-enabled-tactics>。

⁴³ Neil MacFarquhar, "Russia Says Its Syria Bases Beat Back an Attack by 13 Drones," *New York Times*, January 8, 2018, <https://www.nytimes.com/2018/01/08/world/middleeast/syria-russia-drones.html>。

時，同樣可能造成嚴重損害。最簡單的例子，就是台灣目前在機場旁設立禁航區。其禁止範圍同樣包括民用的各種小型無人機，因其可能造成重大飛安事故，危及旅客生命財產安全。

事實上，小型無人機進行簡易改裝後成為自殺炸彈等攻擊方式，早已被 ISIS 採用。雖然前述 2018 年初俄軍所遭受的攻擊事件，由於實際上操作方式仍十分原始，故不應輕易以集群式攻擊稱之，然而各武裝團體對小型無人機的廣泛應用，使得各國國土確實存在將來遭到小型無人機群組攻擊的可能性。更進一步來說，非國家行為者如武裝團體藉由小型無人機和簡易程度的技術，能達到如此攻擊效果，當實際面對具備高度無人機技術及集群式攻擊能力的對手時，一旦遭遇此類奇襲、受到的損傷可能將會遠高於此。

就反制上來說，不少軍工大廠皆針對小型無人機的威脅進行研究，或者提出能與之對抗的方案。如雷神（Raytheon）公司的郊狼（Coyote）反無人機系統，幾乎可說是「以無人機擊落無人機」；萊茵金屬（Rheinmetall）公司研發的 Skyranger 防砲系統，其中一個重點對抗的目標，就包含小型四軸無人機。在這些「硬殺」手段之外，透過各種干擾裝置，切斷其與控制單元的訊號，以對抗小型無人機的「軟殺」方法，亦是當前對抗無人機及集群式攻擊的重要方式。

小結

本章節錄當前幾個重要的技術領域，雖然在簡短篇幅中難以詳細介紹技術概念及目前所有的發展計畫，然而綜觀這些領域的目前技術進展，可以發現這些在未來十年內可能會實現的技術，皆能改變未來的戰爭樣貌。戰場機器人，包含 AI 等相關技術的應用，即使不直接用於交戰上，也將使得從前線戰士、後方勤務到指揮官決策等各種方面的任務效率，都大幅提升。匿蹤技術的持續發展，同樣將使戰場上具備強大匿蹤技術所佔的優勢更加巨大，尤以空戰為甚。極音速載具幾乎不可防禦的特性，則使各掌握技術的大國，如同管制核武器般避免其擴散，但這同樣成為小國對抗大鯨魚的關鍵兵器。最後，無人機集群式攻擊能使操作者不論在空中、地面還是海上，皆有執行各種複雜任務的彈性與能力，並且在民用領域上亦有巨大潛力。最重要的是，台灣在不同領域上，皆已有一定程度的科技研發能量與基礎，如何進一步發展，以達成技術上的不對稱優勢，正是當務之急。

第四章關鍵資通訊科技的發展

吳俊德、蔡榮峰、劉姝廷¹

前言

隨著電腦運算技術的進步，全球先進國家正迎來工業 4.0 的大數據時代，能夠對各種控制單元進行微觀調控，預料也將為軍事指管系統帶來新一波的技术改革。藉由量子科技與人工智慧的發展，人類正邁向一個「智力替代」的新時代，大幅度改變決策環境。下一代的 5G 網路通訊技術，則猶如神經迴路，用以支撐為數龐大的控制單元間所需之訊息流量。虛擬實境則協助整合線上與線下，為數位資訊與實際環境提供介面混和機制，擴大前述各項科技所帶來的效應。

壹、量子科技

量子為光子、中子、質子等基本粒子之總稱，應用其量子物理學特性的技術即為量子科技。目前各國政府大力投入發展的面向，聚焦於「量子運算」(Quantum Computing)。主流電子通訊系統所使用的電子位元，受限於傳統物理學，單一最小單位 bite 只能存在 0 或 1 兩個狀態，需要許多並列 CPU 來執行運算。而奠基於量子力學範疇的量子位元(qbite)則具有「量子疊加態」(Quantum Superposition)的優勢，即無限多種狀態分布三維的布洛赫球面 (Bloch Sphere) 上，同時加之「量子糾纏」(Quantum Entanglement) 現象之應用，²量子運算能夠執行巨量平行運算，達到傳統電腦無法企及的運算速度。量子運算可以推進分子構成研究、深化機器學習，若能導入密碼轉譯、光學校正、機械控制、材料科學、戰情系統，將為一國軍事能力之提升帶來巨大綜效。

建構量子等級系統之技術，也能用來強化下一代國防工業所需的各種偵測感應器以及衛星遙測能力，大幅提升精準打擊能力。而能否實際投入應用，則必須視量子網路 (Quantum Networking) 的建構能力而定。規模小至晶面表面陣列，大至覆蓋全球太空至深海的戰情資訊系統。量子時代的科技國力，將可能因為組件量子網路能力之優劣重新洗牌。

2018 年 9 月 24 日美國國家科技委員會(National Science & Technology Council,

¹ 吳俊德，國防安全研究院網路作戰與資訊安全研究所助理研究員，負責本章第貳、參節；蔡榮峰，國防安全研究院國防資源與產業研究所研究助理，負責本章第壹節；劉姝廷，國防安全研究院網路作戰與資訊安全研究所研究助理，負責本章第肆節。

² 愛因斯坦稱其為「鬼魅般的超距作用」，大意是量子系統中，2 個相互糾纏的粒子，其物理性質如動量、自旋、偏振等呈現相對性；測量其中一個粒子，另一個粒子同時能「感知」測量動作的發生並產生相應影響之結果，且此作用不受宏觀物理距離之影響。

簡稱 NSTC) 發佈《國家量子資訊科學戰略綱要》(National Strategic Overview For Quantum Information Science), 並宣布投入 13 億美元, 與美國科技大廠如 IBM、Google、Intel、Microsoft 合作開發量子技術, 維持美國的領先地位。³ 中國在 2016 年 8 月發射世界首顆量子通訊實驗衛星「墨子號」後, 2017 年喊出合肥「量子信息國家實驗室園區」五年計畫。2018 年 9 月 19 日阿里巴巴集團也宣佈將研發量子運算系統。日本文部科學省宣佈 2018 年開始製造量子電腦, 而韓國科學技術研究所 (Korea Institute of Science and Technology, 簡稱 KIST) 則希望在關鍵的量子通訊密鑰技術上取得優勢。歐盟 2018 年也啟動量子技術旗艦計畫 (European Quantum Technologies Flagship Programme)。⁴ 台灣的科技部則是於 2018 年 4 月啟動量子電腦專案計畫, 計畫每年經費 7000 萬元, 約 3 至 5 年時間, 希望促成每年 3 到 5 個團隊投入量子電腦研發。⁵

一、最新發展

現階段的量子網路技術限制, 在於量子疊加態只要受到外界測量的擾動, 即可能崩潰成一個狀態, 而失去應用價值; 再者, 透過量子位元交換訊息, 也意味必須仰賴原子之間的交互作用, 更增加操作的複雜性。量子科技的進步基礎建立在模擬實驗、測量結果與運算試驗之上, 尤其量子處理器仰賴超冷卻 (Supercooling) 與隔絕技術, 所需設備資金門檻極相當高, 因此當下量子科技之發展, 聚焦在各國政府與產業界領導企業之間的競爭。

(一) 迫近「量子霸權」門檻

2012 年加州理工學院物理學家普瑞斯基爾 (John Preskill) 指出, 如果一部具有 50 量子位元的量子處理器, 若其運算錯誤率能夠低過一個特定門檻, 則當運算定義良好的問題時, 速度將遠遠超過世界上任何一台奠基於傳統物理學基礎的超級電腦, 解答傳統電腦無法計算之問題; 而這個門檻的概念, 就被稱為「量子霸權」(Quantum Supremacy)。如何提高量子處理器的量子位元數、降低其錯誤率, 成為兩個主要的競爭力指標。

目前量子處理器硬體製造方面由美國領先。根據「Google 量子 AI 實驗室」(Google Quantum AI Lab) 最新實驗結果, 量子位元數目只要達到 49 qbit、電路深度 40 層原子、雙量子位元匣錯誤率低於 0.5%, 就已經具有明顯的「量子霸權」優勢。

³ “AP Explains: The US push to boost ‘quantum computing,’” *Washington Post*, September 24, 2018, https://www.washingtonpost.com/business/technology/ap-explains-the-us-push-to-boost-quantum-computing/2018/09/24/99d17034-c004-11e8-9f4f-a1b7af255aa5_story.html?noredirect=on&utm_term=.dff215f8b335。

⁴ <探索量子電腦的秘密 科技部啟動量子電腦研發專案>, 科技部, 2018 年 4 月 27 日, https://www.most.gov.tw/folksonomy/detail?subSite=main&article_uid=b11cef32-5cbd-4f1a-819f-c835e1492a62&menu_id=9aa56881-8df0-4eb6-a5a7-32a2f72826ff&l=CH。

⁵ <科技部拚量子電腦年砸 7 千萬輔導團隊研發>, 《中央社》, 2018 年 4 月 10 日, <http://www.cna.com.tw/news/ait/201804100089.aspx>。

Google 目前在 9 qbit 一維陣列量子電路，已經能達到讀取錯誤率 1%，且單位元閘（single-qubit gates）錯誤率 0.1%、低雙位元閘（two-qubit gates）錯誤率 0.6%。⁶2018 年 3 月 Google 公布了 72 qbit 處理器「Bristlecone」，在位元總數上超越 2017 年 11 月 IBM 發表的 50 qbit 處理器，也勝過 2018 年 1 月 Intel 發表的 49qbit 處理器「Tangle Lake」。不過，能否其將其 9 qbit 一維陣列模組的實驗參數成功應用到更大規模的量子系統，將是未來幾年值得觀察之重點。

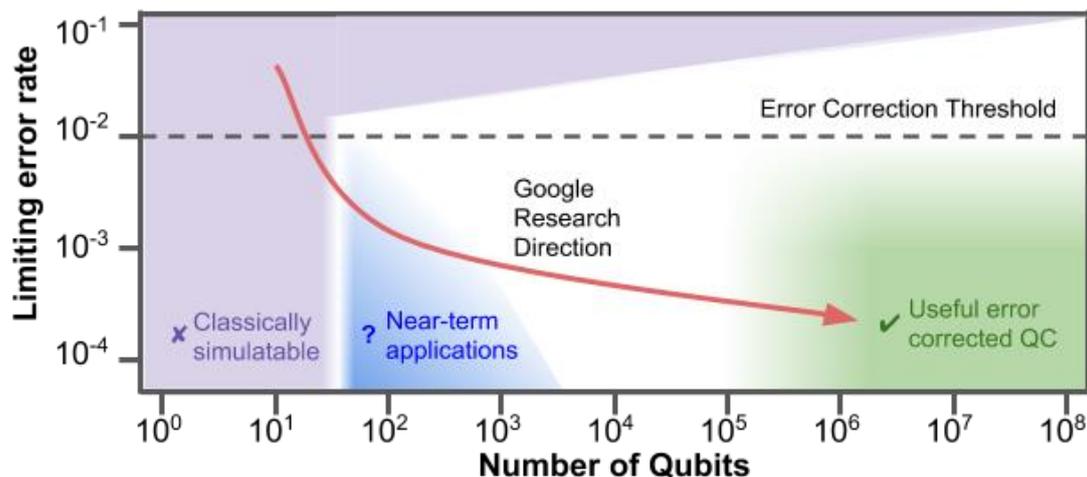


圖 4-1、量子位元與錯誤率之概念圖

資料來源：Google AI Blog，

<https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html>。

（二）雲端運算模擬量子處理器

中國欲利用改良演算法結合傳統運算的變通方式，創造出模擬的量子處理器，企圖以變通方式跨入量子霸權門檻。其主要有兩種方式，一是運用現有紀錄的量子態資料庫進行模擬，二是在超級電腦上，運用千兆位元組（Petabyte）等級之記憶體傳統處理器，來運算隨機量子態。

2018 年 5 月 8 日，阿里巴巴量子實驗室施堯耘團隊發表一篇論文，宣布改以雲端運算，建立可進行隨機量子態運算的模擬量子處理器「太章」，成功模擬 81qbit、深度 40 層原子（ $9 \times 9 \times 40$ ）的量子電路，宣稱只運用了 14% 的網路節點資源，以及兩分鐘的時間，並分別成功模擬了 $10 \times 10 \times 35$ 、 $11 \times 11 \times 31$ 以及 $12 \times 12 \times 27$ 共四種規模的量子電路。⁷「繞道而行」的想法並非中國獨創，越來越多科技大廠預測，在實體量子處理器推進到量子霸權階段之前，模擬量子處理器可能就會率先普及，成為各類應用科學的量子等級研究之催化劑，例如看好此一趨勢的 Microsoft，於 2018 年 9 月就正式推出量子運算開發程式。⁸

⁶ “A Preview of Bristlecone, Google’s New Quantum Processor,” *Google AI Blog*, March 5, 2018, <https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html>。

⁷ Chen, J., Zhang, F., Huang, C., Newman, M. & Shi, Y., “Classical Simulation of Intermediate-Size Quantum Circuits,” May 3, 2018, <https://arxiv.org/abs/1805.01450>。

⁸ 請參見 <https://www.microsoft.com/en-us/quantum/development-kit>。

(三) 量子位元缺陷檢測

量子霸權概念提出者普瑞斯基爾 (John Preskill) 2018 年 8 月撰文指出量子運算即將進入「噪聲過渡期量子」(Noisy Intermediate Stage Quantum, 簡稱 NISQ) 技術的時代, 即跨過量子霸權門檻後, 量子處理器普遍達到 50 至幾百個量子位元。然而, 此階段人類尚無法完美操控量子等級的粒子, 因而干擾量子運算效能的擾動「噪音」, 將大大限制量子處理器發展速度。⁹如何降低「噪音」, 成為 NISQ 時代量子處理器硬體製造的重要關鍵。

2018 年 9 月 4 日, Google 量子 AI 團隊證實量子運算性能不穩定的因素, 來自材料缺陷形成的局部量子系統, 其與其他量子位元間若產生共振, 造成了性能波動的現象。該實驗也展示了如何利用量子位元來改善量子處理器的製造。¹⁰以色列 Weizmann 科學研究所稍早於 8 月則成功利用微米級的二氧化矽諧振器, 使原子與光子的量子位元訊息耦合, 進行訊息交換。將光子做為媒介量子的交換閘, 有利於建構量子等級的「超大型積體電路」(Very-Large-Scale Integrated, 簡稱 VLSI)。¹¹

二、應用

各種涉及次原子等級之應用, 基本上都被歸類為量子技術。然而這也隱含了其各項軍事應用的發展進程, 將取決於以何種工業技術作為基礎。量子運算受限於超導體製程與超冷卻等關鍵技術, 而運用光子與電子的相關量子技術, 則可能因為光電技術早已廣泛應用, 率先取得初步實用化的成果。以下選出 4 項可能因量子研究突破而產生之軍用技術:

(一) 量子運算及加密演算法防禦

工研院指出, 目前普遍被認為安全性較高的虛擬貨幣之公鑰與私鑰, 解密私鑰約要需耗費傳統電腦 1,092 億年來運算, 而一部 100qbite 的量子電腦只需要 3 個小時。¹²若使用跨入量子霸權門檻的量子電腦來攻擊現有的密碼系統, 勢必衝擊各國既有國安基礎。連目前被認為安全程度較高的「RSA 非對稱加密演算法」遭破解時間也將大幅縮短。因此, 美日等國政府已經開始著手開發「後量子密碼演算法」(Post-Quantum Cryptography, PQC) 安全協定之網路通訊應用, 以因應量子電腦問世之破密衝擊。此外, 量子運算預料將成為人工智慧發展的加速器, 並用來精進戰情指揮系統、協助戰場決策、提升飛彈打擊精準度、模擬武器與相

⁹ Preskill, J., "Quantum Computing in the NISQ era and beyond," *Quantum*, August 6, 2018, vol. 2, pp. 79.

¹⁰ Klimov, P.K. et al., "Fluctuations of Energy-Relaxation Times in Superconducting Qubits," *Physical Review Letters*, September 4, 2018, vol. 121, issue 9, <https://arxiv.org/ftp/arxiv/papers/1809/1809.01043.pdf>。

¹¹ Bechleret, O. et al., "A passive photon-atom qubit swap operation," *Nature Physics*, August 13, 2018, vol. 14, pp. 996-1000。

¹² <全面取代傳統電腦, 人類該害怕量子電腦嗎?>, 《數位時代》, 2018 年 2 月 6 日, <https://www.bnnext.com.tw/article/48091/why-we-should-be-afraid-of-quantum-computing>。

關系統測試、協助研發量子等級結構的創新材料等。

(二) 量子密鑰分配技術

「量子密鑰分配」(Quantum Key Distribution, QKD) 技術乃基於量子特性製作，以解決密鑰傳送安全上的問題。一旦遭到第三方攔截，量子疊加態必然改變或崩塌，原有資訊將無法被破譯。與受到「量子霸權」限制的量子運算不同，以光子基礎的量子密鑰分配的傳輸技術已逐漸邁入實用化階段。美國、中國、歐盟都開始出現運用案例，唯目前受限於技術，必須在傳播地之間鋪設上百公里的光纖作為傳輸介面。

2017 年 9 月中國與奧地利兩國合作，利用「墨子號」量子實驗衛星，對靜止、相距 7600 公里的兩地，進行了太空量子密鑰分配實驗。該實驗由配置量子糾纏態發射器的人造衛星，建立衛星與地面的量子密鑰分配系統，屬於檢驗太空尺度量子力學完備性之研究。雖然該實驗報告宣稱，中國科學院和奧地利科學院之間，進行了 75 分鐘的洲際量子加密視訊會議。¹³不過事實上其通訊加密與一般電波通信方法並無二致，唯其加密密鑰採用了 QKD 技術，並透過人造衛星傳送，距離真正的自由空間量子通訊 (Free Space Quantum Communication) 仍有一段距離。量子密鑰以人造衛星傳送時，必須解決傳輸效率如何提高的技術性問題，因此需仰賴量子位元原缺陷檢測技術，如同傳統通信工程所謂的誤碼糾錯。自由空間量子通訊技術一旦實用化，勢必大幅提高軍事通訊保密性。

(三) 量子雷達

當前產業界自駕車關鍵感測技術相當依賴的雷射車用防撞器，以及應用廣泛的脈波雷射測距，皆屬於光學雷達 (Light Detection and Ranging, LiDAR) 技術，也就是利用光波進行探測。若將量子技術運用於雷達領域，可突破光學雷達在感測和成像的技術極限。透過利用單一光子的量子特性來進行探測，除了具有更強的抗干擾和抗隱形能力外，其靈敏度可輕易偵測任何未使用量子隱形塗料之匿蹤飛機。¹⁴不過，現階段各國量子雷達實測多半集中於可見光頻段，而在微波頻段方面，理論架構與關鍵元組件皆處於研究階段，尚無法克服單光子能量過低的限制。簡言之，各國軍方普遍將量子技術視為突破現有光電技術限制之關鍵，一旦能夠建立量子等級的導航偵測系統，不僅能提升精準打擊能力，反隱形與反潛能力也可望大幅提升。

(四) 量子材料

利用量子微觀結構以及量子特性所製造出的量子等級軍事材料，可提升軍用

¹³ Liao, S. et al., "Satellite-relayed intercontinental quantum network," *Physical Review Letters*, January 19, 2018, vol.120, <https://arxiv.org/ftp/arxiv/papers/1801/1801.04418.pdf>。

¹⁴ "Quantum radar will expose stealth aircraft," *Phys.org*, April 23, 2018, <https://phys.org/news/2018-04-quantum-radar-expose-stealth-aircraft.html>。

設備抵抗傳統物理干擾之能力。量子網路結構建構技術可用以增加武器裝備對作戰環境干擾因素之韌性 (resilience)，提高系統性能穩定性。量子塗層技術可用於抗電磁波攻擊。量子隱身材料能實現真正意義上的隱形，不僅肉眼難以察覺，且能夠躲避傳統光學、熱力學設備的追蹤，對於各種戰場的環境也有較高的抗干擾能力。而先進量子材料科學研究，例如拓撲絕緣體 (topological insulators)、石墨烯等材質與量子霍爾效應之應用息息相關，其導電、導熱特性，未來在軍事領域技術的微電子學 (Microelectronics)、光電子 (Photoelectron) 研究中，具極高潛在應用價值。

將「量子糾纏」運用在「物理特性共享」機制，則能創造出顛覆常識的材料，如量子電池。當量子位元越多，量子糾纏現象擴大，反而使整體充電過程加速，變成越多電池一起充電，反而節省更多時間。未來若能結合無線充電技術研製軍用量子電池，或許有機會改變如反坦克飛彈等傳統武器系統的動力供需方式。不過，目前量子電池的製造技術，仍然與量子處理器一樣，受限於超冷卻技術與隔絕材質，尚處於實驗階段。澳洲阿德萊德大學 James Quach 博士的研究團隊表示，他們企圖製造出的全球第一款量子電池，可能將於 2019 年問世。¹⁵

貳、人工智慧

人工智慧即是賦予機器認知 (cognitive) 能力，讓機器變得聰明，能夠自行決定應該採取何種行動以達成既定目標。人工智慧的原理是讓機器藉由演算法從資料中學習，進而找出解決問題的最佳方案。具有人工智慧的系統就如同有了「大腦」，可以在沒有人類的操縱、控制之下自動完成工作。人工智慧最大的優勢在於可以用飛快的速度處理大量的資料，不論是找出資料所呈現出的型態及資料中的離群值 (anomaly)、預測未來趨勢、整合大量資訊以做出決策，其速度與效率是人類無法企及的。另外，機器可以持久運作，不會產生疲勞，也不會有情緒或是偏見的問題，決策較為穩定可靠，這些都是人工智慧的優點。

在過去的第一次及第二次工業革命中，人類發明機器來幫助完成需要勞力的工作；如今，人類發展人工智慧讓機器幫助完成需要認知能力的工作，人工智慧因此被認為將掀起第三次工業革命。具有人工智慧技術的國家能夠創造新的財富來源，並大幅提昇經濟競爭力與軍事力量，因此，這項科技的發展將會影響一個國家的國家安全，甚至會改變國際間的權力平衡。由於人工智慧是一國未來國力之所繫，世界主要國家無不投入大量資源全力發展，以期在這項競賽中取得優勢。

然而，人工智慧的發展也引起許多爭議，由於其可以被應用的範圍非常廣泛，首先引起關注的便是將會有許多原本由人類所執行的工作被機器取代，造成嚴重的失業問題。另一個引發激烈爭辯的層面則是軍事應用，當武器系統導入人工智慧，其威脅性與殺傷力將更加強大。人工智慧是否應該用來殺人？人工智慧武器

¹⁵ “Want to charge your iPhone instantly? A world-first 'super battery' could make it possible,” ABC, July 21, 2018, <http://www.abc.net.au/news/2018-07-21/new-technology-could-help-to-charge-your-iphone-instantly/10021086>。

的發展是否能夠加以規範？規範是否能發生作用？還是反而讓遵守規範的國家落居劣勢？這些問題在倫理道德、國際政治、產業、法律等各個領域都引起熱議，但也未有定論，成為未來亟需解決的問題。

一、現況發展

機器學習 (machine learning) 是讓機器獲取人工智慧最主要的途徑，其原理是將大量的資料輸入機器，讓機器的演算法從大量資料當中，依人類的需求去學習並歸納出規則。現今機器學習已經發展出多種不同方法，目前較為熱門的幾類演算法如下：非監督學習 (unsupervised learning)、深度學習 (deep learning)、加強學習 (reinforcement learning)、以及生成對抗網絡 (generative adversarial networks)。¹⁶

非監督學習：此種方法是將同類型但無標記 (label) 的訓練資料輸入至機器，例如輸入蘋果的圖片，但這些圖片並沒有標示為「蘋果」。在機器大量接收蘋果的圖片後，演算法便可以辨識出蘋果的特徵，此時若輸入狗的圖片，機器會知道這不是蘋果，就不會將其和蘋果歸為同一群 (cluster)。此法讓機器透過觀察、解析結構將資料分門別類，可以找出資料中的離群值或預測未來行為，應用範圍非常廣泛。非監督學習被認為是未來研究的趨勢，但此法正確率低，僅能用在不強調正確率的特定系統。

深度學習：此種方法是用類似人類神經網絡 (neural networks) 的方式來讓機器學習，其原理是在輸入端與輸出端之間建構多層由相互連結的端點形成的網絡，每一個端點都可以單獨處理資訊，如同一個人工的神經元 (neuron)。當資料輸入時，會被拆解成細微的單位 (例如將相片拆解為畫素) 流經各個端點，機器透過端點之間的連結學習到資料特性，最後在輸出端將資料歸類並標記。此法可以用來辨識影像或預測醫療結果，在軍事上有許多應用。

加強學習：此種方法是以深度學習為基礎，讓機器從環境所回饋的訊息 (feedback) 中學習。機器每採取一個行動，會產生一個後果，這些後果量化為分數傳回給機器，機器就會知道採取某個行動會得到什麼分數。當機器在不同的情況下去嘗試各種可能的行動，機器會學到在何種情況採取什麼行動會得到較高的分數。加強學習主要應用在鬥智的遊戲或比賽，例如下棋，人工智慧系統在此領域的表現已經勝過人類。

生成對抗網絡：此法是機器學習的最新技術，亦為深度學習的應用，由 Ian Goodfellow 在 2014 年所提出。生成對抗網絡由兩個相互對抗的神經網絡所組成，其中一個網絡 (generator, 生成器) 先隨機生成資料，另一個網絡 (discriminator, 分類器) 再分辨資料是真實還是仿造。生成器與分類器一直互相對抗，一方仿造資料，一方辨識資料，並根據對抗結果不斷調整演算法參數，每一次的對抗都讓

¹⁶ Paul Scharre and Michael C. Horowitz, "Artificial Intelligence: What Every Policymaker Needs to Know," Center for a New American Security, June 19, 2018, <https://www.cnas.org/publications/reports/artificial-intelligence-what-every-policymaker-needs-to-know>。

兩個系統更進步。如此反覆對抗下去，生成器仿造的資料會越來越接近真實，分類器辨識的能力也越來越強。此法可以大幅減少用來訓練機器的資料量，節省許多成本；也可以大幅提升機器學習的速度，而且一次可訓練兩個系統，效率倍增，因而成為當前人工智慧的發展趨勢。

目前人工智慧所能賦予機器的智慧相當於人類三歲的程度，尚不具備常識及推理能力，因此在重複性高以及勞力密集的產業，可以將機器智慧化以取代人工作業。另外，人工智慧系統的問題在於當機器學會執行一項任務之後，如果再去學習一項新的任務，機器會「忘記」原本的任務要如何去執行，因此人工智慧系統只能執行單一任務。如何讓機器在學習新任務的同時不會失去舊有的知識，而能夠執行多重任務，是當前人工智慧發展的重點之一。

人工智慧發展的另一個重點，是要讓系統有能力處理多方即時（real-time）互動。人工智慧目前在處理回合制的雙方互動（例如下棋，一方下完再換另外一方）上，表現已經遠遠超過人類，但是尚無能力處理多位行為者在開放環境中同時進行互動的複雜情況（例如即時戰略遊戲）。任何一個國家能夠開發出具有此種能力的人工智慧系統，就能獲得在戰場上的優勢，等同大幅提升其軍事力量。

二、軍事科技的應用

人工智慧在軍事科技的應用非常廣泛，從決策管理、戰場指揮、作戰能力、到後勤維修都可以派上用場。在決策管理方面，北約要以人工智慧協助該組織的營運決策以及軍事管理。¹⁷在戰場指揮方面，人工智慧發展的方向在於自動偵測敵軍動向並產生情報資料，在快速分析複雜情資之後產生威脅評估，並且衡量我軍部隊與裝備相互合作的能力，以利戰場決策的制訂。

在作戰能力方面，主要是裝備自動化。在地面防護系統方面，整合紅外線與攝影機以辨識在警戒區內的不明物體，一旦確認敵意，除警示我軍外，也會自動對來襲的敵人開火射擊，以色列的哨兵科技系統（Sentry Tech）與南韓的超級庇護系統（Super aEgi）皆屬此類。在空對面或面對面的精確武器中，如挪威與美國合作的海軍打擊飛彈（Naval Strike Missile, NSM）與聯合打擊飛彈（Joint Strike Missile, JSM）都無須瞄準目標再發射，只要指定目標區域，飛彈就可以自動找到目標加以攻擊。¹⁸

在後勤維修方面，人工智慧可以讓系統長時間監測自身狀況，例如是否需要加油或充電、故障檢測、甚至進行簡單的自我維修。美國海軍的「智慧維保後勤系統」（Paladium）與「機器人前支維修系統」（JARVIS），即是運用人工智慧軟體，來進行故障檢測、料件更換、及零件產製，除了大幅減少時間以外，還可以

¹⁷ Nyshka Chandran, “How NATO Wants to Use Artificial Intelligence in Decision Making,” *CNBC*, June 4, 2018, <https://www.cnb.com/2017/06/04/how-nato-wants-to-use-artificial-intelligence-in-decision-making.html>。

¹⁸ 寧博，〈淺論 AI 於軍事領域運用與發展〉，《青年日報》，2018 年 10 月 12 日，<https://www.ydn.com.tw/News/308780>。

將人為錯誤降至最低。¹⁹

值得注意的是，雖然人工智慧在軍事層面上的應用很廣，目前只能做到「自動化系統」(automated system)，尚無法達到「自發性系統」(autonomous system)的程度。「自動化系統」指的是系統依據規則執行任務，輸入相同的資料，系統會產生相同的結果。「自發性系統」則不然，它會隨時更新資訊並進行推論，每當輸入一筆資料，它會計算出最佳的行動方案，因此輸入相同的資料，系統未必會產生相同的結果。

在軍事科技上，系統智慧化的程度仍然很低，以發展最快的無人機為例，目前還無法自行處理包括氣象資料、飛行路線、維持高度、油料及機械等所有狀況，仍然要仰賴操作員發出指令，才能操控飛機執行任務。²⁰以目前的科技而言，要達到真正的「自發性系統」，還有很長的一段路要走，然而，人類會慢慢接近這個目標，應該要趁著這段時間，將前述人工智慧應用在軍事科技所產生的爭議予以釐清與解決，才能確立未來人工智慧發展的方向。

參、網路通訊

網路通訊即將進入 5G 時代，5G 不只是為了滿足人的需求，更是為了滿足物的需求，讓各個裝置皆可以在網路上連結。5G 是針對未來所設計的通訊技術，它不只是 4G 技術的提升，而是一項推動各項產業轉型的變革，²¹因此，5G 技術的發展成為世界主要國家兵家必爭之地，5G 競賽也已經如火如荼地展開。

一、5G 應用情境

5G 在技術上的提升有三個主要的應用情境：增強型行動寬頻通訊(Enhanced Mobile Broadband, eMBB)、超可靠度和低延遲通訊(Ultra-reliable and Low Latency Communications, URLLC)、大規模機器型通訊(Massive Machine Type Communications, mMTC)，分述如下。

增強型行動寬頻通訊：5G 首要之務是提升資料傳輸的效能，其傳輸速度最快可達到下載每秒 20Gbit、上傳每秒 10Gbit，是 4G 的 100 倍，也就是下載一部 8GB 的影片只需要 6 秒。唯有達到這樣的資料傳輸速度，智慧城市、無人駕駛、遠距醫療、以及虛擬實境(virtual reality, VR)的娛樂體驗才不再是遙不可及的夢想。

超可靠度和低延遲通訊：除了傳輸速度以外，有一些網路通訊服務對於資料傳輸的正確性以及從輸出端到接收端的時間落差有非常嚴格的要求。以無人駕駛為例，在正確性上，對於路況資訊如前方路口交通燈號的資料傳輸絕對不能出錯；在時間落差上，對於周圍車輛動態的資訊必須即時接收到才能立即做出反應。若

¹⁹ 社論，〈AI 軍事應用改變下世代戰爭型態〉，《青年日報》，2018 年 9 月 25 日，
<https://www.ydn.com.tw/News/306517>。

²⁰ 同註 18。

²¹ 曾毅，〈為未來設計的網路——5G 掀起全新戰場〉，《數位時代》，2018 年 3 月 30 日，
<https://www.bnnext.com.tw/article/48674/5g-future>。

是資料傳輸過程會發生錯誤，或是資料從輸出端到接收端有時間上的延遲，無人駕駛就無法確保安全。因此，5G 技術在資料傳輸的正確性及時間延遲訂定非常高的標準，其錯誤率要低於 10 的負 5 次方，也就是正確率接近 100%；時間延遲要低於 1 毫秒（millisecond，簡稱 ms，即千分之一秒），比 4G 提高 10 倍。²²

大規模機器型通訊：未來將是物聯網（Internet of Things, IoT）的時代，透過網路通訊，萬物皆可互聯。在各個機器設備能夠相互連線的情況下，智慧家庭及智慧城市就有可能出現，人類的的生活也將更為便利。為了達成這個理想，5G 必須要能滿足非常大量終端裝置的通訊需求，因此其要求每平方公里內要能夠讓至少一百萬個裝置連接上網路，這是 4G 的 100 倍。

二、標準規格競爭

由於 5G 將改變未來人類生活的樣貌，又是帶動國內產業轉型的關鍵，不但商機無限，更會影響一國的國力，世界主要國家無不支持國內主要通訊廠商全力發展，以求在 5G 競賽中領先。5G 有許多相關技術，包括編碼（coding）、多輸入多輸出（Multi-input Multi-output, MIMO）、毫米波（millimeter wave）、網路切片（slicing）、以及邊緣計算（edge computing）等。對通訊廠商來說，在 5G 競賽中最重要不是設備製造能力或商用能力，而是有多少項技術成為標準。一旦成為業界唯一的標準規格，全世界所有廠商都要按照該規格來生產設備、組織網路、以及接入終端裝置。

掌握技術規格的廠商除了在產業鏈具有先發優勢以外，關鍵在於其他廠商都必須向其獲取專利授權。有些也擁有核心專利的廠商，可以用互相開放的方式來獲取；沒有核心專利可供交換的廠商，就只能花錢購買。專利授權費用是一筆非常龐大的利潤，因此各大通訊廠商無不致力於開發技術規格，希望自身的技術能夠成為標準，以下以 5G 頻道編碼技術的競爭為例來說明。

第三代伙伴計畫（3rd Generation Partnership Project，以下簡稱 3GPP）是規劃與制訂 5G 通訊標準的國際組織，5G 的技術規格皆要在此組織獲得通過，再提案到國際電信聯盟（International Telecommunication Union, ITU）認可。3GPP 達成決議的方式是採取共識決而非多數決，一項標準規格要能通過除了技術本身夠好、夠成熟以外，關鍵在於沒有其他廠商反對，尤其是具有話語權的大廠。在這樣的遊戲規則下，廠商之間必須談判斡旋，甚至妥協讓步，任何一項提案都是經過不斷地修正，才能讓大廠一致通過。

行動通訊的頻道大致可分為兩種，控制頻道（control channel）傳送操作網路設備的指令，資料頻道（data channel）則傳送資訊。不論是指令或是資訊，都必須先經過編碼處理才能傳送，因此頻道編碼是無線通訊的重要基礎技術。在 5G 之前，編碼的標準規格是由歐、美廠商所壟斷，3G 以及 4G 採用歐洲廠商愛立信

²² 簡均哲、汪海瀚，〈eMBB/URLLC/mMTC 鼎立 5G 標準制定全面啟動〉，《新通訊》，2017 年 10 月 16 日，<https://www.2cm.com.tw/2cm/zh-tw/magazine/-Technology/F20D9109E8FC4D34B9CC25B24A786283>。

(Ericsson) 主導的 Turbo 碼；無線網路 (Wireless Fidelity, Wi-Fi) 則是廣泛應用美國廠商高通 (Qualcomm) 主導的低密度同位檢查碼 (low-density parity-check code, 以下簡稱 LDPC 碼)。

頻道編碼技術有三大陣營在競爭成為標準規格, 分別是 Turbo 碼、LDPC 碼、以及中國廠商華為主導的極化碼 (polar code)。²³ 在 2016 年 10 月, 3GPP 進行 5G 新空中介面 (New Radio, NR) 的標準評選, 讓增強型行動寬頻通訊 (eMBB) 的服務可以先做準備。在此次會議中, LDPC 碼先獲選為 5G eMBB 資料頻道長碼的編碼方案; 隨後在該年 11 月, LDPC 碼又獲選為 5G eMBB 資料頻道短碼的編碼方案; 最後在控制頻道, 則是由極化碼獲選。²⁴

雖然 5G 的頻道編碼是由高通佔上風, 但華為以極化碼為基礎所開發的技術, 讓高通無法壟斷 5G 編碼; 更重要的是, 華為藉由極化碼拿下一項標準, 就在 5G 的技術標準取得話語權。5G 完整的通訊標準預計首次提案將在 2019 年 7 月前完成, 最終提案則是在 2020 年 2 月前完成, 在中國廠商取得話語權之後, 未來 5G 通訊標準的競爭將會更加激烈。

三、軍事科技的應用

網路通訊在軍事科技上最大的應用是以物聯網技術結合至指管通資情監偵系統 (C4ISR), 可以提高指揮效率, 發揮戰場上戰力倍增的效果, 成為現代軍隊的神經中樞。在指管通資情監偵系統之下, 由監視系統和偵察系統所獲得的情報資料, 藉由通信系統傳入作戰指揮中心, 經過分析之後指揮官做出決策, 命令便直接送達下屬單位。

指管通資情監偵系統是否能發揮作用, 關鍵在於資訊與通信技術。戰場的情境複雜且變化快速, 若是關於地形地物、敵我雙方位置、速度、運動情況等資訊無法有效取得並即時傳遞, 便無法在第一時間判斷出敵人的意圖及能力、並做出適當的回應, 在戰場上就會落居劣勢。當網路通訊的能力愈強大, 指管通資情監偵系統的運作就愈順暢, 即時性也愈佳, 就愈有可能在隨時需要更新資訊的戰場情境中獲得優勢。

網路通訊在軍事科技上另一個重要應用是火力控制系統 (fire-control system), 藉由在端點部署的感測器即時傳送資訊, 在面臨威脅時, 配合人工智慧可以做出自動回應, 一個明顯的例子是精準打擊 (precision strike) 武器。精準打擊武器例如追蹤飛彈, 藉由連線到衛星做全球 GPS 定位, 可以自動搜尋, 甚至是追蹤在移動中的目標, 在飛行過程中, 需要不斷更新資訊以修正飛行路線, 才能準確命中目標。若是沒有強大的網路通訊能力, 這樣的任務是不可能完成的, 無人機也是相同的情況。因此, 5G 通訊技術的發展, 將使火力控制系統威力更能夠發揮。

²³ 極化碼是由土耳其教授 Erdal Arıkan 在 2008 年提出, 此法是第一個被證明可以逼近頻道容量上限的編碼方式, 應用在 5G 技術上, 可以提高編碼性能、降低解碼複雜度、以及減少功率損耗。華為從 2010 年開始研究極化碼, 並開發出原創的編碼技術。

²⁴ 資料頻道的編碼有長碼與短碼的區別, 控制頻道則只有短碼, 沒有長碼。

在未來的戰場上，也會有許多的物件可以在網路上相互連結，包括感測器、軍需品、武器、載具、個人攜行裝備，因而形成「戰聯網」(Internet of Battle Things, IoBT)。²⁵在戰聯網中，各個物件皆能蒐集、處理、傳遞、分享資訊給在戰鬥中的士兵以利其決定行動，也就是說，每一名士兵自己就是一個自動化指揮系統，這將會改變未來作戰方式，也是網路通訊在軍事科技應用的發展方向。

四、中國製網路通訊產品與服務引發安全疑慮

5G通訊技術會為人類生活帶來莫大的便利，但同時也會帶來比以前更多在資訊安全方面的隱憂。5G的資訊安全風險主要來自於物聯網，在物聯網之下，機器設備以及終端設施皆可透過網路相互連線，這是過去3G與4G無法達到的。但是當萬物互聯，卻也表示萬物皆可能成為網路攻擊的途徑，這會讓駭客有更多的管道可以入侵一個系統。在3G與4G時代，能夠相互連線的機器數目不多，但是在5G時代，一個物聯網的系統會有少則上百，多則成千上萬個設備相連，只要一台相連的機器沒有做好安全防護形成漏洞，一旦被駭客發現利用這個漏洞入侵，就可能導致相連的所有機器都受到影響，後果會比3G與4G時代嚴重許多。因此，5G有著比3G與4G更高的潛在資訊安全風險，在5G時代，資訊安全的防護必須要更嚴密，涵蓋範圍也更廣泛。

在軍事上，指管通資情監偵系統即是物聯網的應用，也會面臨相同的資訊安全威脅。除此之外，國家的關鍵基礎設施(critical infrastructure)以及重要資料庫未來也都是物聯網的一環，而且可能是由民間業者提供雲端服務，若是資訊安全發生漏洞，後果將會不堪設想。因此，在享受5G帶來的便利之餘，資訊安全防護更是要格外小心注意的。

當前台灣網路通訊的安全威脅有很大一部份來自於中國，在台灣2018年手機銷售排行榜的前10名中，中國品牌手機就佔了4名，而且排名有逐漸上升的趨勢；在2018年9月，中國品牌手機在台灣的市佔率達到23%，這些數據都說明中國手機在台灣頗受歡迎。²⁶然而，中國品牌的通訊產品一向有安全上的疑慮，因此被一些國家提出警告，甚至是將中國廠商排除在該國國內的5G基礎建設之外。

在2012年的一場駭客會議上，與會者揭露中國廠商華為所製造的路由器(router)有嚴重的安全漏洞，其韌體(firmware)²⁷可被駭客經由網路在遠端操縱，進而控制整個路由器。²⁸在2016年11月，美國一家資訊安全公司發現，部分安卓(Android)系統的手機有中國廣升公司編寫的程式，該程式會將簡訊內容、聯絡人名單、通話記錄、位置等資訊傳送到位於上海的伺服器，這個程式內建在

²⁵ Alexander Kott, Ananthram Swami, and Bruce J. West, "The Internet of Battle Things," *Computer* 49.12 (2016): 70-75.

²⁶ 周若敏，〈中國華為的5G發展與安全疑慮〉，《國防安全週報》，第20期，2018年11月2日。

²⁷ 韌體是嵌入在硬體裝置中的程式，硬體可透過韌體的更新來提升其效能與可靠性。

²⁸ Lucian Constantin, "Hackers Reveal Critical Vulnerabilities in Huawei Routers at Defcon," *Computer World*, June 30, 2012, <https://www.computerworld.com/article/2505191/malware-vulnerabilities/hackers-reveal-critical-vulnerabilities-in-huawei-routers-at-defcon.html>。

手機裏，但沒有向手機用戶揭露有這種監視功能。廣升公司設計此程式是為了幫助中國手機製造商監視用戶行為，而廣升提供程式的客戶包括華為與中興。²⁹在2018年11月，澳洲情報單位一份機密報告指出，中國情報機構會向中國通訊產品製造商（華為）施壓，以取得密碼進入其所製造的網路設備，中國情報機構已經以此法入侵過他國網路。³⁰

由於類似事件時有所聞，加上中國在2017年通過的《國家情報法》中第七條規定：「任何組織和公民都應當依法支持、協助、和配合國家情報工作，保守所知悉的國家情報工作秘密。」除了中國通訊產品本來就有安全疑問之外，中國通訊廠商也需要配合中國情報機構，這讓一些國家對中國通訊產品及廠商產生很大的安全顧慮。在2018年2月，美國六位情報首長在一場聽證會上告訴參議院情報委員會，他們不會建議美國民眾使用華為的產品或服務；³¹澳洲更是在今年8月禁止中國廠商華為與中興參與其5G網路建設。³²

當其他國家開始對中國通訊產品及廠商提出警告甚至是管制，以中國手機在台灣逐漸受到歡迎，兼以台灣受到中國網路威脅的程度，對於中國通訊產品及廠商對資訊安全可能造成的風險，是台灣必須要更為謹慎應對的。

肆、虛擬實境

自1935年美國科幻小說家開啟虛擬實境的想像，經過數十年來軟體技術與硬體設備的進步與變革，虛擬實境將朝向更多元廣泛的應用。然而，虛擬實境受限於軟體開發與硬體設備昂貴等因素，在市場應用上尚未普及，是目前虛擬實境技術欲思突破的瓶頸。

虛擬實境技術（Virtual Reality, VR）是指在使用者的現實世界中，透過電腦整合圖形的運算、感應和顯示，及藉由網路與人工智慧等數位創建方式，模擬出高度真實感的虛擬空間，在封閉的虛擬環境中，營造出使用者身處於現實中的錯覺，並配合相關配備裝置，讓使用者獲得身歷其境的感受。

擴增實境技術（Augmented Reality, AR）則是將虛擬資訊擴增到現實空間中的一種技術。它強調的不是取代現實的空間，而是在現實空間中添加一個虛擬物件，利用攝影機的辨識技術與電腦程式的結合，使原本的目標能夠被清楚標示，或是在螢幕上產生虛擬圖示，使虛擬與現實進行同步互動。

²⁹ Matt Apuzzo and Michael S. Schmidt, “Secret Back Door in Some U.S. Phones Sent Data to China, Analysts Say,” *The New York Times*, November 15, 2016, https://www.nytimes.com/2016/11/16/us/politics/china-phones-software-security.html?_ga=2.13797235.516978498.1541660397-84974788.1541066456。

³⁰ Paul Maley, “China Used Huawei to Hack Network, Says Secret Report,” *The Australian*, November 3, 2018, <https://www.theaustralian.com.au/national-affairs/national-security/china-used-huawei-to-hack-network-says-secret-report/news-story/510d3b17c2791cbcac18f047c64ab9d8>。

³¹ Sara Salinas, “Six Top US Intelligence Chiefs Caution against Buying Huawei Phones,” *CNBC*, February 15, 2018, <https://www.cnbc.com/2018/02/13/chinas-huawei-top-us-intelligence-chiefs-caution-americans-away.html>。

³² Catherine Shu, “Australia Bans Huawei and ZTE from Supplying Technology for its 5G,” *TechCrunch*, August 23, 2018, <https://techcrunch.com/2018/08/22/australia-bans-huawei-and-zte-from-supplying-technology-for-its-5g-network/>。

混合實境技術 (Mixed Reality, MR) 是結合虛擬實境與擴增實境的技術。它將虛擬場景與現實世界進行高程度的結合，建立出一個新的環境及符合一般視覺上所認知的虛擬影像，讓現實世界裡的物件能夠與數位世界裡的物件並存，並且即時產生互動，創造出似真似假的使用體驗。

一、現況發展

虛擬實境技術、擴增實境技術與混合實境技術，在科技發展趨勢上具有多元應用之潛力。根據美國高盛投資銀行 (Goldman Sachs) 的研究報告，虛擬實境技術、擴增實境技術與混合實境技術產業規模，預估在 2025 年將達到 800 億美元，其中數位遊戲、醫療保健與工業應用是核心應用領域。³³

數位遊戲產業是目前虛擬實境技術與擴增實境技術主要發展的領域，虛擬實境與擴增實境技術帶動著遊戲產業硬體與軟體的市場發展。例如手機遊戲「精靈寶可夢」(Pokemon Go)，運用擴增實境技術，讓玩家可在日常生活中與各種虛擬角色進行互動，並配合手機中 GPS 定位功能，加強玩家與遊戲的連結。

醫療保健是虛擬實境與擴增實境技術未來潛力發展的產業。虛擬實境技術可藉由非侵入性的方式，完整呈現患者體內身體構造，以便醫生準備與調整治療方案。此外，擴增實境技術亦可應用於醫療手術，例如以色列開發商「Augmedics」，透過擴增實境技術研發出「ViZOR」系統，有助於脊椎外科手術的進行。

在工業生產製造方面，以擴增實境技術為基礎，發展出智慧眼鏡工業應用解決方案，讓員工在工廠內配戴智慧眼鏡，將生產組裝指示或產品訊息，疊加在真實環境上，取代傳統指導手冊、平面藍圖或教育訓練方式，以此保障作業人員工作安全，提升工作生產的效率。

二、軍事科技的應用

根據北約出版的報告，虛擬實境技術早在 2003 年已進行軍事應用。³⁴ 虛擬實境憑藉擬真體感的特性，在有限的國防資源及戰場多元變化的情況下，能夠有效節省戰前訓練的花費，並提供多元虛擬戰場的訓練模式。擴增實境技術的應用，在作戰時可結合各方的資訊，並傳送至士兵所配戴的顯示器中，以增強士兵對作戰地情形的掌握。

(一) 模擬訓練與軍事演習

將虛擬實境技術與擴增實境技術導入國軍模擬訓練與軍事演習中，加強部隊實戰能力。例如挪威海軍潛艇模擬系統，藉由虛擬實境技術，增添士兵在潛艇內的真實作戰情境；利用虛擬作戰系統為軍隊訓練提供新方法，加強戰術訓練；透

³³ “Virtual & Augmented Reality: The Next Big Computing Platform?”, *Goldman Sachs*, January 13, 2016, <https://www.goldmansachs.com/insights/pages/technology-driving-innovation-folder/virtual-and-augmented-reality/report.pdf>。

³⁴ “Virtual Reality: State of Military Research and Applications in Member Countries”, NATO, February, 2003, <http://www.dtic.mil/dtic/tr/fulltext/u2/a411978.pdf>。

過虛擬戰場，使各軍兵種身處異地，亦能同時參與戰術演練，促進部隊之間的合作，提高軍事訓練的效率，並降低戰鬥模擬預算成本。



圖 4-2、美軍採用台灣生產之 VR 裝置

資料來源：U.S. Air Force。

（二）裝備研發與技術維修

連結民用領域中虛擬實境技術與擴增實境技術的先進科技與創新概念，以此強化軍事裝備的研發生產與維修工作，提升部隊的戰鬥實力。例如英國 BAE Systems 運用擴增實境技術，結合台灣 HTC 技術，打造出虛擬駕駛座艙，增強戰機戰鬥實力。運用擴增實境技術或混合實境技術，研發戰鬥機飛行員或坦克車車長頭盔顯示器，即時呈現戰場情況，協助處理戰爭工作；此外，透過擴增實境技術，能夠清楚看到軍事設備的輔助性說明，特別於戰時，以易操作、高效率的維修方式，可為作戰人員節省寶貴時間。

（三）軍事指揮與作戰輔助

透過虛擬實境技術與擴增實境技術，成立行動式指揮中心，隨時隨地發號施令，即時流通戰場訊息，例如美國曾運用擴增實境技術，研發軍用智能眼鏡，指揮官可隨時將地圖及訊息傳送給士兵，以迅速掌握最新戰地情況。另一方面，擴增實境技術除可展現真實的戰場環境，亦能透過增加虛擬物件，突顯肉眼無法觀測的環境訊息，以及敵我雙方的隱藏力量，指揮官與戰鬥人員以此做全盤完整評估，並調整作戰策略，達到擴增實境技術作為戰鬥輔助的優勢效果。

小結

本章討論目前重要的資訊科技發展趨勢，特別選出具有工業 4.0 時代特徵之革新技術，並檢視其對軍事領域可能帶來之變革。無論在哪一項技術獲得突破，其外溢效應可能都會為一國軍事能力帶來相當可觀的相對性優勢。量子科技可用以強化通訊、偵測、衛星遙測能力，提升精準打擊效能，不僅在數位運算方面為電腦科技後發國家，提供突破傳統運算製程困境的機會，更可能在密碼學領域投下震撼彈。運用人工智慧可加快資訊處理速度，取代許多原本要由人力執行的工作，減輕人員負擔，人工智慧機器學習模式的演進，使得「仿生智力」的替代性將大幅提升，除人工智慧機器人對產業與社會產生前所未有之衝擊，在軍事層面的戰略、戰術應用上，也可能出現顛覆性創新，並對既存的國際法體系帶來挑戰，未來的國防決策者將無可避免，需將「非人類智慧」此一變數，納入整體考量。5G 網路通訊提升現有網路效能，增進資訊交換速度，5G 網路規格標準化之競爭，則是對未來即將深入智慧城市各個角落的物聯網建置影響深遠。虛擬實境則改變軍隊訓練方式，提高作戰效率，由此看來，資訊科技的發展，在軍事上的應用，不僅增進人與軍事武器間的連結，也強化了操作武器及遂行作戰的效能。

第三篇 台灣面對的科技威脅與 挑戰機會

第五章台灣面對之科技挑戰

曾怡碩¹

前言

軍民兩用科技對台灣造成的挑戰，主要來自敵意國家或其資助團體以新興科技優勢，壓制及打擊台灣。本報告第二篇提及之匿蹤戰機、超精準武器、極音速載具，均為中國積極發展之未來科技項目，但均非台灣力所能及。目前著眼之因應作為，是以加強戰力保存為未來主要防禦手段，這在下一章將有所著墨。台灣資源有限，必須發展足以形成不對稱戰力之科技，以因應現存最顯著的科技威脅。這類威脅目前主要來自中國解放軍於 2016 年將電戰部隊、太空軍、網軍、心理戰部隊組建之戰略支援部隊。其中，台灣在電戰方面，因長期與中國交手，並能與時俱進，故未讓中國佔到優勢。在太空戰方面，雖然台灣力有未逮，但基於通訊傳輸需求，仍有建構制太空權之必要，這對台灣形成重大挑戰。此外，中國仍在網路作戰以及網路輿論心理戰層面構成之威脅，對台灣資訊安全與關鍵資訊基礎設施保護以及反制網路輿論心理戰，形成重大挑戰。因此本章分別檢視台灣在這三大層面軍民兩用科技所面對的挑戰，並在小結呈現國軍秉持不對稱作戰思維之因應作為。

壹、建立制太空權

前蘇聯在 1957 年發射第一個進入軌道的人造衛星史波尼克（Sputnik 1），開啟了美蘇太空競賽。現代高科技戰爭或非戰爭軍事行動已與太空科技緊密結合。太空科技提供陸、海、空軍即時偵察、通信、氣象、導航、定位等作戰支援任務，不論是對敵軍之軍事及戰略目標實施精準打擊，還是藉由遙測影像進行災害防救，太空科技力量已成遂行軍事任務的要角。因此，除爭奪制空權、制海權、制陸權、制資訊權之外，制太空權已成為軍事行動致勝關鍵。

不論是採取攻勢還是守勢，一國要取得制太空權，必須發展與部署太空硬體設施、信號傳輸鏈結、指揮管制站暨使用單位三大部分的太空科技。太空科技的發展是一國整體科技與產業實力的體現，涵蓋系統工程、機械材料、推進控制、資訊系統、通信電子及遙測導航等科技範疇，發展成果往往具軍民兩用性質，對民生和國防等工業之推動，具有重大影響。然而，不論是在國防軍事用途或與民生相關的經濟應用的太空科技發展，皆須挹注大量人力與資金，由於所需經費與基礎工程過於龐大，有心發展太空科技的國家，也會在獨立自主發展路線之外，採取跨國策略合作方式，希望能取節省經費、截長補短之利，及早實現目標。

¹ 曾怡碩，國防安全研究院網路作戰與資訊安全研究所助理研究員，負責本章內容。

因應中國積極部署發展太空軍力，並於 2016 年將太空軍力納入其戰略支援部隊，台灣持續發展與建置因應措施，逐步形成制太空權戰力。然而，台灣雖積極發展與部署太空科技，仍囿於資源與技術限制，且於尋求國際技術合作時，常面臨國際政治現實面制約。因此短期內，台灣仍需與友好國家維持密切合作，以維繫初步的制太空權。

台灣的制太空權乃專注於防禦中國的太空軍力對於台灣的威脅，台灣目前面對中國太空戰力最大威脅，在於戰時通信與導航系統遭受破壞或干擾。中國北斗全球定位系統將提供「一帶一路」沿線國家服務，落實《推動共建一帶一路的願景與行動》有關「完善空中（衛星）資訊通道」指導，積極建構「天基絲路」，將有利於中國對台軍事監偵。下一部分將呈現台灣太空科技發展現況。

一、太空硬體設施

太空硬體設施係指置於地球軌道上之火箭、人造衛星或其他可執行任務之裝置。台灣探空火箭計畫分別由國家太空中心統籌系統整合與任務規劃，中科院負責火箭推進系統，國內學術研究單位提出科學研究及酬載儀器研製計畫，於 1997 年至 2014 年間總共發射了 10 枚。台灣探空火箭計畫對於低緯度電離層研究量測、提供大氣觀測飛行路徑即時精密數據、衛星用反應式控制系統的功能測試、推進系統控制能力及回收艙系統能力測試，可用於未來發展衛星的通信、定位、推進、控制及回收艙。

台灣由國家太空中心發展人造衛星，自 1999 年開始，台灣從衛星接收國成為衛星發送國，成為全球第 33 個擁有衛星的國家。國家太空中心發展的福爾摩沙（福衛）人造衛星，已發送福衛一號、二號、三號、五號。其中福衛一號與二號已經除役，而福衛三號在 2018 年 11 月時，已服役超過 12 年，國家太空中心將以發送福衛七號取代三號，詳見圖 5-1。

通常探空火箭計畫是做為大型火箭發射衛星進入地球軌道的先行指標，福衛六號原規劃為第一個由台灣自行發射升空的人造衛星。2009 年國科會（科技部前身）界定台灣太空科技發展以科學研究為目標，決定取消原訂 2012 年自行發射衛星計畫，回歸原發展模式，委託國外火箭公司執行發射任務。

表 5-1、台灣人造衛星發展進程

福爾摩沙衛星	一號 原名：中華衛星一號	二號 原名：中華衛星二號	三號 6顆微衛星組成	五號	七號
總經費 (NTD)	61.14 億元	46.02 億元	30.23 億元	56.59 億元	32億元 (台灣出資)
升空時間	1999 年 1 月 27 日	2004 年 5 月 20 日	2006 年 4 月 15 日	2017 年 8 月 25 日	今年底或明年
除役時間	2004 年 6 月 17 日	2016 年 8 月 20 日	服役中	升空之後 5 年	升空之後 5 年
運載火箭	雅典娜一型	陶洛斯	美樂達	獵鷹 9 號	獵鷹重型運載
繞行地球一周時間	96 分鐘	103 分鐘	100 分鐘	99 分鐘	97 分鐘
主要任務	科學實驗 1. 電離層特性研究 2. 海洋水色研究 3. Ka 頻段通訊實驗	全球陸地及海域 遙測 科學實驗研究及 救災	觀測全球大氣層 及電離層 建立全球大氣量 測網	1. 自行研發台灣衛星 關鍵技術 2. 全球陸地及海域 遙測	1. 接續福衛 3 號 2. 密集提供中、 低緯度電離層 觀測資料

資料來源：中央社，2018 年 8 月 3 日。

二、 信號傳輸鏈結

國家太空中心專家在 2018 年 2 月出版的《科學發展》中指出，台灣位於近赤道的低緯度地區，上空受「赤道電漿噴泉效應」的影響，電離層活動較活躍且形成電離層的「赤道異常區」。這區域的電漿濃度特別高，其擾動現象對於全球定位系統（GPS）使用者，以及其他與衛星通訊相關的民生和國防應用，都可能產生很大的影響。

前述台灣探空火箭計畫與衛星計畫中，多次使用更精進的電漿量測儀器，配合地面設備持續研究台灣上空「電離層不規則體」的產生機制，並實現三方對照成果，具有精進通訊與定位上的功能。此外，2004 年除役的福衛一號，在 Ka 頻段通訊實驗方面，進行 Ka 頻段低速率、高速率及雨衰減通訊實驗，並且進一步做安全通訊實驗，以增強台灣的通訊系統能力。後來取消的福衛六號計畫，主要搭載的儀器將以遙測及導航定位為主，如果當初計畫實現，可算是台灣第一個自主開發的通訊定位衛星。至於地面的衛星操控中心及外部地面設施的資料傳輸，則仰賴地面通訊網路。位於新竹科學園區的衛星操控中心以台灣高品質的學術研究網路連接位於桃園中央大學及台南成功大學的 S 頻段遙傳追蹤指令站，而與海外發射場及海外支援站之間的資料傳輸通訊，則以 VPN (Visual Private Network) 線路進行連結。

三、 衛星指揮管制站及資料接收站

國家太空中心負責衛星的操控，主要工作是以衛星操控中心、S 頻遙傳追蹤與指令地面站、X 頻遙測影像資料接收站及海外支援地面站等設施，進行指令傳送、狀態擷取、衛星追蹤、軌道控制、酬載資料及遙測影像接收等之全程任務操作，如圖 5-2 所示：



圖 5-1、國家太空中心衛星計畫衛星操控地面設施關聯圖

資料來源：國家太空中心。

衛星指揮管制站及資料接收站需有重複配置，冀能發揮緊急備援之效。國家太空中心分別於桃園中央大學及台南成功大學歸仁校區設立 S 頻段遙傳追蹤指令站，負責衛星指令發送及遙傳資料接收，而桃園中央大學站則同時兼具有任務操控中心的功能，作為衛星操作控制中心的緊急備援中心。X 頻遙測影像資料接收站建置於新竹科學園區，接收遙測影像資料後，傳送至新竹科學園區的遙測影像處理中心。此外，台南成功大學歸仁校區 S 頻段遙傳追蹤指令站於 2013 年升級為 S/X 雙頻衛星地面站，作為竹科園區 X 遙測影像資料接收站的備援站。

貳、台灣資安風險與關鍵資訊基礎設施保護

隨著物聯網、社群媒體等新興資訊技術服務快速擴展，軍、民資訊系統不論在虛擬網路世界，還是在實體硬體設備，遭受惡意入侵的威脅隨之俱增。台灣面對的資安威脅，是每月高達數千萬次網路攻擊。這些惡意攻擊背後，不乏國家政府資助的駭客團隊，以台灣為其實驗場域，對關鍵基礎設施、廠房企業、個人帳戶進行惡意入侵、竊取資料或擴散，造成國家安全威脅、商業利益損害與隱私人權侵害。

為因應資安威脅，我國政府於 2016 年 8 月即擬定「資安即國安」策略方針。蔡英文總統並在 2017 年的總統府資安週活動中，宣示了三項國安級的資安目標：第一、打造國家資安機制，確保數位國家安全；第二、建立國家資安體系，加速數位經濟發展；第三、推動國防資安自主研發，提升產業成長。有別於中國所強調的網路主權，並汲取中國及其他國家政府侵犯人民數位隱私權的爭議教訓，台灣採取資通安全治理途徑，以政府機關組織、私部門產業、非政府行為者、以及國際組織或建制為多方利害攸關者，共同因應資安威脅，以兼顧數位主權、人權與安全。

國軍保衛國家安全、守護數位國土有責，理應為多方利害攸關者資通安全治理中的重要角色。國防部遂於 2017 年成立資通電軍指揮部，依照 2018 年 5 月立法院通過的「資安管理法」與 2018 年 9 月國家安全會議發布的《國家資通安全戰略報告》，加入資通安全治理的行列。「資安管理法」與《國家資通安全戰略報告》均將國防部列為國家層級資安聯防團隊中的國安國防機制，實質上等於接受國安會指令，平時與各相關機關搭建構伙伴關係，俾利於必要時協同執行任務，包括協同國土安全辦公室及國營事業，以抵禦消弭關鍵基礎設施面臨之資安威脅。

隨著關鍵基礎設施的資訊聯網已成趨勢，遭駭客入侵風險也遽增。著眼於此，「資安管理法」與《國家資通安全戰略報告》均將關鍵資訊基礎設施保護列為要項，接下來除了處理一般資安風險，將以專節闡述台灣關鍵資訊基礎設施保護措施。

一、資安威脅現況

根據行政院資通安全會報技術服務中心於 2018 年 3 月指出，全球面臨的資

安威脅，主要類型不外乎：進階持續威脅（APT）攻擊竊取機密資料、分散式阻斷服務（DDoS）癱瘓網路運作、物聯網設備資安弱點威脅升高、網路與經濟罪犯影響電子商務與金融運作及資訊供應商持續遭駭影響供應鏈安全，關鍵資訊基礎設施資安風險倍增。

事實上，台灣不論是政府、企業所面臨的資安威脅，上述這些一樣都少不了。首先，根據行政院資安處於 2018 年 10 月表示，APT 與組織型駭客試圖竊取公務與商業機密威脅持續增高，且潛伏期拉長到五百多天，而分散式阻斷攻擊頻率與規模仍維持高量，並未減緩。其次，由於暗網惡意程式地下經濟猖獗，台灣金融業不只一次遭遇勒索惡意程式或駭客入侵自動提款機。

智慧城市物聯網的鋪設建置，讓物聯網元件設備未改密碼而維持一樣的原始碼的便宜行事陋習，不僅讓智慧城市資安蒙上陰影，也成為關鍵資訊基礎設施網路串聯後的噩夢。最後，美國與歐洲多國關注中國資訊產品資安問題，也讓資訊廠商供應鏈的軟硬體資安問題成為眾所矚目焦點，台灣資訊廠商因此面臨供應鏈可能須考慮遷出中國的機會與挑戰。

台灣政府或企業也面臨類似的資安難題。個人攜帶行動裝置至辦公場合處理公務以及微型裝置察覺日益困難導致管理不易、技術更迭與惡意攻擊模式不斷翻新以致應變不易、社交工程防不勝防導致認知警覺不足、資安人才短缺以致資安自主能力不足及協力廠商或者分支機構管理不易造成資安漏洞。

台灣月達數千萬次的網路攻擊，光是國防部各單位每月就承受近兩千萬次網攻。根據 2018 年 7 月國防部公布資料（如表 5-1），在 2013 年，國防部各單位遭受網攻 868 萬次，2014 年大幅增為 7 億 2686 萬次，2016 年降為 3 億 932 萬次，2017 年國防部各單位遭受網攻次數卻進一步降為 2 億 466 萬次，但共軍對於國防部貫徹募兵制最重要的國軍人才招募中心遂行網攻也創下 3 千 196 萬次，是有史以來最高紀錄。

雖然資安攻擊事件往往難以追究確認發動來源，仍然可經資安鑑識與行為模式辨識，確認許多攻擊來源是來自中國。行政院資安處簡宏偉處長警告，中國網軍攻擊的頻率在降低，但成功率卻上升，特別是具有高度影響性的攻擊（第三級資安事件），從 2015 年僅成功 4 件，到 2017 年成功 12 件，成長 3 倍之多。²

² 資安事件影響等級分為四級：一.符合下列任一情形者，屬 4 級事件：(1)國家機密資料遭洩漏（機密性衝擊）。(2)國家重要資訊基礎建設系統或資料遭竄改（完整性衝擊）。(3)國家重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作（可用性衝擊）。二.符合下列任一情形者，屬 3 級事件：(1)密級或敏感公務資料遭洩漏（機密性衝擊）。(2)核心業務系統或資料遭嚴重竄改（完整性衝擊）。(3)核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作（可用性衝擊）。三.符合下列任一情形者，屬 2 級事件：(1)非屬密級或敏感之核心業務資料遭洩漏（機密性衝擊）。(2)核心業務系統或資料遭輕微竄改（完整性衝擊）。(3)核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作（可用性衝擊）。四.符合下列任一情形者，屬 1 級事件：(1)非核心業務資料遭洩漏（機密性衝擊）。(2)非核心業務系統或資料遭竄改（完整性衝擊）。(3)非核心業務運作遭影響或短暫停頓（可用性衝擊）。

中國網軍採取新的技術來隱匿他們的行為，讓網路攻擊更難被察覺，例如透過搜尋引擎或部落格，讓資訊安全部門以為這只是一般網路平台，而忽略其行動。另外，也有許多的攻擊是繞道經由其他國家發動，使其難以被追蹤。專家表示，雖然台灣有良好的網路防禦與調查能力，但是要達到百分之百的防範是很困難。前揭顯示中國網軍在改變其網路攻擊型態，從原本大量進攻調整為精準打擊，一旦攻擊成功，後果將更形嚴重。

表 5-2、國防部所屬民網遭異常偵測、掃描及疑遭攻擊次數統計表

年度 單位	102 年	103 年	104 年	105 年	106 年
國防部網站 (政務辦公室)	713,778	1,001,142	1,153,275	4,120,552	9,552,884
國防大學	9,405	877,450	995,312	219,522	198,469
人才招募中心 網站(人次室)	804,092	4,309,186	4,931,321	28,522,275	31,968,975
軍醫局(所屬 國軍軍醫院)	4,557,186	720,542,371	561,312,118	276,271,708	162,453,979
政戰資訊服務 網、青年日報 社、軍聞社、 全民國防署戰 營網站(政治 作戰局)	2,597,760	133,587	856,889	194,621	492,549
總計	8,682,221	726,863,736	569,248,915	309,328,678	204,666,856

資料來源：《國軍資安防護機制書面報告》，國防部通資次長室對立法院第 9 屆第 5 會期外交及國防委員會第 14 次會議關係文書，2018 年 7 月。

二、台灣關鍵資訊基礎設施保護

台灣將政府、高科技園區、能源、水資源、通訊、交通、銀行與金融、緊急救援與醫院列為八大關鍵基礎設施，而關鍵資訊基礎設施（Critical Information Infrastructure, CII）指的就是用來維運這些關鍵基礎設施所需的資訊網路系統，或調度控制系統（Supervisory Control and Data Acquisition, SCADA）。關鍵資訊基礎設施一旦遭受網路攻擊破壞，將威脅人民性命安全，亦即虛擬世界攻擊將造成實體世界傷亡，其嚴重程度等同於未達戰爭標準的暴力衝突。

為強化關鍵資訊基礎設施的資安防護(Critical Information Infrastructure Protection, CIIP)、風險評估機制及資安事件復原能力，特串接國家層級、關鍵資訊基礎設施領域層級以及關鍵資訊基礎設施提供者層級之三級電腦緊急應變團隊(Computer Emergency Response Team, CERT)、資安資訊分享與分析中心(Information Sharing and Analysis Center, ISAC)及資訊安全維運與預警中心(Security Operation Center, SOC)，建構完整的資安情報區動架構（如圖 5-3）。

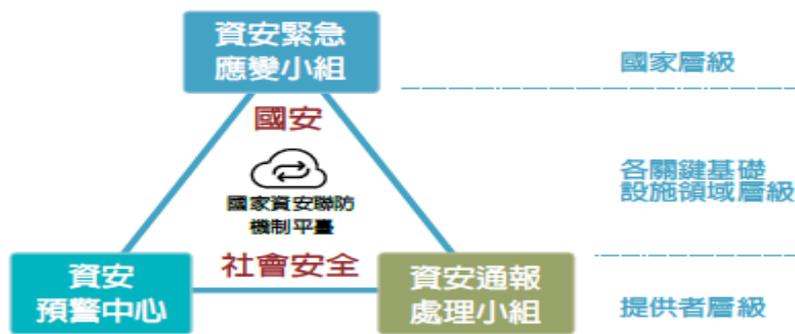


圖 5-2、以情報驅動之國家資安聯防架構

資料來源：國家安全會議，《國家資通安全戰略報告》。

關鍵基礎設施防護的權責分為國家、關鍵領域與設施提供者三層。國家層級由行政院資安處負責召集，主要實施跨領域演練、制定資安防護建議等工作。領域階層由八大領域的中央主管機關負責，例如金融領域是金管會，能源與水資源就歸屬經濟部。第三層則是關鍵設施提供者，金融設施就是銀行、證券機構，能源提供者就像台電、中油等單位（如圖 5-4）。

在關鍵設施提供者層級，必須注意工控系統（SCADA 屬於工控系統的一種）的資安。超過 80% 的關鍵基礎設施是依賴工控系統來執行自動化作業，因此工控系統的安全可說關係到國家的戰略安全。早期設計時都是在封閉環境中使用，並未預想會以網路互聯，所以較少考量安全上的防護。根據 IBM 於 2018 年 10 月發布的《工控系統安全攻擊報告》，對工控系統的網路攻擊，可透過人工或在工控系統感染病毒，經控制主機植入未經授權的控制程式，再對工控系統網段通訊封包動手腳。因為工控系統的控制協議不具備加密機制，讓攻擊者乘機控制工控系統。2018 年 8 月台積電不慎讓病毒在科學園區廠房擴散，生產線被迫停機檢測數日，估計損失達新台幣數十億元之譜。此次事件直接的肇事原因，指向廠區安裝人員沒有按照 SOP 執行病毒檢測，就把新機台接上廠區內部網路，造成病毒擴散。

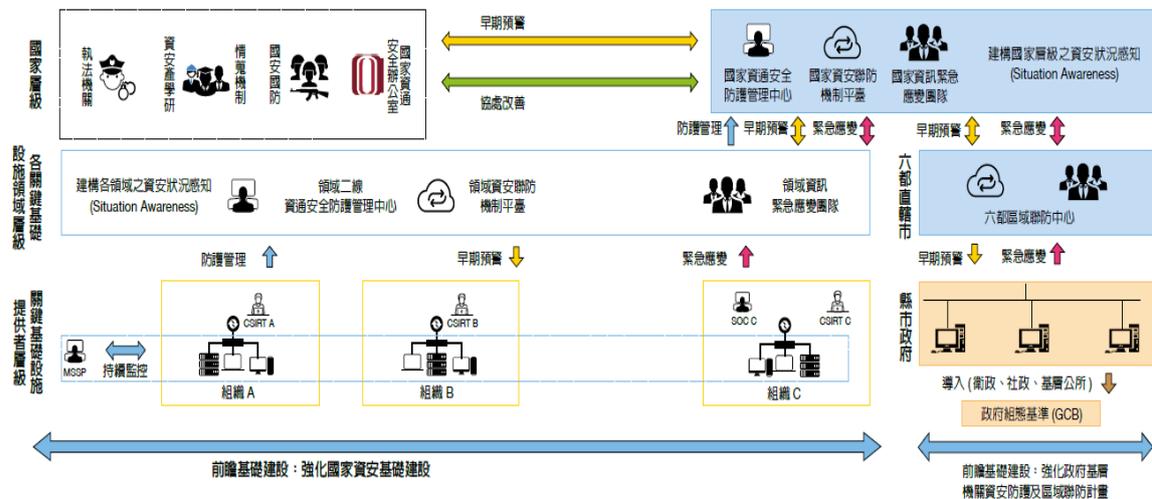


圖 5-3、建立國家級的資安聯防團隊

資料來源：國家安全會議，《國家資通安全戰略報告》。

參、反制網路輿論心理戰

中國一向擅長運用統一聯合戰線，亦即統戰，對台灣進行分化，並進一步對台灣實施三戰，其中即包含輿論戰與心理戰，亦即國軍所界定的政治作戰。中國如今將這些傳統政治作戰，轉化進入網路虛擬世界，形成所謂的影響力攻勢，但有別於傳統宣傳與當代軟實力，中國這類網路影響力攻勢因仍具備統戰的隱匿性、腐敗性及強迫性，因此被美國民主基金會在 2017 年歸類為與俄羅斯以網路干預美國 2016 年選舉一樣行徑的銳實力。

俄羅斯於 2016 年藉由社交工程釣魚郵件侵入美國民主黨系統，竊取機密資料後散佈於網路空間，並於社群軟體發布假消息以及發動謾罵，形成同溫層效應後，進一步分化美國原已對立的分裂社會，造成美國社會分歧，直接影響美國的國家安全。俄羅斯後來對歐洲國家選舉以及 2018 年美國期中選舉，一再重施故技，進行俄羅斯眼中所謂的資訊戰。

由於俄羅斯成功地讓美國淪為被干預內政的國家，中國有意效法俄羅斯，運用網路散布假消息、發動網軍帶風向，對台灣 2018 年地方選舉與 2020 年總統大選進行干預。更重要的，中國是希望能夠嫻熟運用現代網路媒體，先以台灣為實驗場域，進行網路空間的輿論戰與心理戰，日後再用以對付美國，冀能在美中新冷戰後，對美實行政治干預。

一、發展現況

大致上，傳統的輿論戰與心理戰都能套用到網路世界。謠言耳語即假消息、造勢即組成五毛黨網路洗版及收編/分化或分而治之即為網路同溫層效應的不斷延伸。除了假消息之外，利用社群媒體散佈仇恨言論，以達到動員暴力行為的目的，也讓網路虛擬言論造成實體世界性命傷害。社群媒體是現今資訊傳遞的重要

媒介，挾著這股新興網路傳播力量，針對如宗教、人種、性別、族群或性取向等特定群體，散佈具有煽動、貶抑或威嚇的仇恨言論，正蔓延全球國家社會，挑起社會對立衝突，衝擊社會和諧，成為政府亟需正視的安全議題。

網路空間要實施輿論戰與心理戰，就是利用網路假消息與仇恨言論，藉著社群媒體演算法的缺陷，散播貼文速度與方向取決於按讚或否定的數量，達成其動員、煽動目的。查核假消息所面臨的爭議，在於「誰能判定消息真偽」。若政府介入主導，可能因執行內容審查，淪於言論檢查爭議，徒生箝制言論自由的疑慮。目前作法，是採多方利害攸關者共同查核通報機制，由社群媒體業者、第三方查核人士以及政府共同面對與處理假消息。

西方民主國家面對仇恨言論引發的安全威脅，仍存有爭議。對於主張加以限制的國家而言，其著眼點在於避免仇恨言論所帶來的影響與傷害，即「第三人效果」傳播理論觀點，因預期傳播訊息對他人會產生高度影響效果，進而促使其採取預防及因應行動。例如德國於 2017 年通過《社交網路強制法》，規定社群媒體必須在接受使用者通報後的 24 小時內，撤除明顯違反德國刑法的仇恨言論，這項立法使德國成為打擊社群媒體仇恨言論最為積極與嚴厲的西方民主國家。

目前對待假消息與仇恨言論，多要求網路平台業者與媒體自律，對於一向捍衛言論自由的美國來說，限制社群媒體仇恨言論的作法，被視為嚴重侵害言論自由的思想控制，並給予社群媒體過分的權力進行內容審查。美國最高法院主張應保障憲法所言的言論自由為首要之務，國家不應過分介入社群媒體言論的價值判斷，否則恐因產生偏見與歧視。因此，美國採取相對寬容的立場，面對仇恨言論的管制。

台灣主要是由國家通訊傳播委員會因應網路假消息與仇恨言論問題。國家通訊傳播委員會與國安會資安辦以及行政院資通安全處，並列為資安鐵三角，對於網路通訊關鍵基礎設施的資訊安全維護，將強化早期預警、持續控管與維運、通報應變及協處改善等四大面向。國家通訊傳播委員會立場是認為，媒體報導應注意事實查證及公平原則，搭配事業建立之自律機制，如製播新聞違反事實查證原則，致損害公共利益或妨害公共秩序，現行廣播電視法或衛星廣播電視法早於 105 年即訂有違反者最高可核處新台幣 200 萬，並得令其停止播送該節目或採取必要之更正措施。事實上，行政院數位政委唐鳳與通訊傳播委員會都認為，事實查核必須以不侵害言論自由為原則，除網民應該要有意識地查證事實，網路平台必須有自律機制，兼得求證於第三方公正之媒體消息查證團體。

二、軍事發展應用

網路自律牽涉內容識別技術，目前除網路爬蟲兼大數據分析之外，也會以人工智慧偵測假消息與仇恨言論。對於社群媒體假消息的偵測技術，最早來自大數據分析。在 Express Scripts 擔任首席資料長(Chief Data Officer, CDO)的 Inderpal Bhandari 於 2013 年在波士頓舉辦的大數據創新高峰會演講中，提出資料真實性

(veracity) 的概念，認為大數據分析中應該加入資料辨識真偽的考慮，分析並過濾資料有偏差、偽造、異常的部分，防止這些「髒資料」(dirty data) 損害到資料系統的完整跟正確性，進而影響決策。

偵測假消息的技術規格，須能辨識文字與圖或影像，經前後文分析，分辨內容真偽，並透過大數據分析比對，追蹤來源真實性以及圖或影像是否經加工修飾。目前科技已進展到利用人工智慧偵測假消息，透過「自然語言處理」辨識文本內容及「視覺性質識別」辨識圖片與影像，經由「監督式深度學習」，運用「循環神經網絡」，對照前後句、前後段落與其他文本進行比較分析，藉以辨識其真實性。

假消息來源經多方利害攸關者交叉確認，就會由演算法列入通報名單，俾利辨識並阻斷假消息的散播。人工智慧不僅是辨識假消息的有力工具，同時也是製造與散播假消息的利器。人工智慧透過先前累積資料，可以鎖定大量特定社群媒體用戶，目前已被用於假消息的自動化散播。另一方面，若經由跨領域專門知識背景的演算法驅動，以及對於語言、文化以及各類知識的大量快速吸收與學習，加上反覆試誤、修正與練習，人工智慧未來也能成為製造挑撥分化性質假消息的來源。此外，人工智慧演算法的設定，必然存有人為決策思維的偏見(bias)。因此，以人工智慧處理假消息，依然要面對「誰能判定消息真偽」的根本議題。於此同時，在辨識假消息來源時，人工智慧「深度學習」可藉由辨識出演算法中偏見的特質與權重，可以分類及標示人工智慧製造之假消息。

處理仇恨言論就更加複雜，除經由監督式深度學習與運用「循環神經網絡」架構中「長短期記憶—支持向量機器」(LSTM-SVM) 網絡模型，對照前後句、前後段落與其他文本，還要進一步進行情緒分析，將內容區分為「非侵犯性-侵犯性-仇恨性」，則可鑑別仇恨言論。由於仇恨言論定義模糊，導致現有人工智慧偵測系統對仇恨言論的操作型定義不一致。一旦檢視的內容超出訓練範疇或字句被刻意動手腳，如故意打錯字、添增不相關字眼或改變字距間隔，便可能輕易瞞騙過偵測體系。因此，目前技術若欲達成全自動化偵測仇恨言論，仍有相當差距。以目前 Facebook 與 Instagram 所採用的「Rosetta」技術為例，即使該系統足以同時處理超過 10 億件不同語言的附圖或影像文字內容，仍需人工進行篩選決策，Facebook 便聘僱兩萬人進行線上檢查。

偵測仇恨內容與偵測假新聞技術要求規格不盡相同，雖皆為辨識文字與圖或影像，前者經前後文分析，著重情緒辨識與侵犯性分級；後者則注重分辨內容真偽，透過大數據分析比對，追蹤來源真實性以及圖或影像是否經加工修飾。此外，一經辨識確認，處理仇恨言論與假新聞的方式也大相逕庭。仇恨言論多經網路平台予以刪除，而假新聞則按不同性質，可以有刪除、降階(demotion)、威懾，或運用充足的資訊對誤導性內容進行平衡、淡化、轉移(distraction)。因此，若有心人士或團體刻意編織假新聞以製造仇恨言論，即使沒有挑釁或侵犯性字眼，也能以肉搜曝光的個資或羅織的文字或圖像，蓄意煽動實體世界的暴力行為。由於此類網路仇恨言論可能不含挑釁或侵犯性字眼或圖像，僅呈現出羅織編造的

文字、圖或影像，因而將大幅增加人工智慧偵測仇恨言論的難度。

社群媒體業者須具備細緻豐富的語言與歷史、社會、文化知識背景，方能同時追查假新聞及審視仇恨言論。以羅興亞遭受種族清洗為例，由於緬甸軍方領袖利用 Facebook 散佈煽動暴力的仇恨言論與假消息，Facebook 坐視不理頻遭指責，雖然 Facebook 在 2018 年 7 月宣示要移除刻意煽動仇恨暴力的假新聞，但卻沒有具體動作，直到聯合國於 8 月發布報告，指責緬甸軍方對穆斯林少數民族羅興亞人犯下戰爭罪行，Facebook 才在 8 月 27 日移除 18 個臉書帳戶和 52 個臉書專頁，包括緬甸武裝部隊總司令敏昂萊（Min Aung Hlaing）和軍方 Myawady 電視台的專頁。

值得注意的是，中國加強對「一帶一路」戰略的同時，勢必對這些國家加緊輸出資通訊基礎建設，以利資料大量蒐集與傳回，遂行網路監控與情蒐，俾利為其實施政治干預做好準備。輸出的規格也可能視該國發展程度或對中國依賴程度而不一。對於低度開發國家或者極權國家，中國可能整廠輸出智慧城市，但必要時，得要先支援水、電、電信、交通運輸基礎建設，才能將監視器與感測設施內建並串接物聯網，達到全面監控情蒐的目標。對於諸如馬來西亞、白俄羅斯等開發中國家，中國則可能藉由爭取特定項目基礎建設，像是中國原先極力促成，後來遭馬來西亞政府取消的馬來西亞的「東海岸銜接鐵道」計畫，以及白俄羅斯的科學園區計畫，然後再將內建資通訊設備經由合法串接或者是非法手段駭進當地國資通訊關鍵基礎設施，以達成情資蒐集佈建的目標。中國未來勢必以「一帶一路」沿線國家作為精進網路輿論干預的試驗場域，藉此試行、實驗以人工智慧輔助的網路輿論量身製作(含假消息)、即時反應帶風向、網路水軍洗版等手法，除可壓制「一帶一路」沿線國家內對中國的不友善言論，也能進一步演練「混合式威脅」中的網路輿論干預他國內政手法，藉此精進其「銳實力」。

為因應中國於網路空間對台施行輿論戰與心理戰，蔡英文總統於 2018 年國慶致詞禮指出，必須阻止外來勢力對國內進行滲透破壞，確保民主制度及社會經濟正常運作。對於製造散布假消息以及企圖用各種方式介入選舉及干擾政治運作的行為，只要罪證確鑿，一定嚴辦到底。針對系統性、來自特定國家背景的假消息傳播，台灣也將加強跨國合作。未來要建立查核和通報機制，共同來因應這些假消息對各國的社會穩定，所帶來的破壞和衝擊。

中國正藉由台灣 2018 年選舉，作為其利用假消息施行政治干預的試驗場域，並可能於兩年後，將人工智慧「深度學習」的成果，套用在干預 2020 年美國總統大選，並進一步染指印太區域民主體制。因此，台美合作反制中國假消息，實為迫切的安全需求。然而，辨識與追查假新聞所需要的，是細緻豐富的語言與歷史、社會、文化知識背景。因此，台灣憑藉著語言與文化等知識上的優勢，以及對於人工智慧科技的積極研發應用，勢將成為印太區域反制中國假消息的國際陣營中，不可或缺的要角。

小結

台灣太空科技發展為科學研究用途，其中可應用於軍事、並形成制太空權的相關技術，除基本衛星部署與遙測影像之外，也對通訊傳輸環境進行研析，未來將藉福衛七號初步建置通訊定位系統。對於指揮管制部分，則包括衛星操控中心所建置的衛星操控系統，藉分析衛星下傳的 GPS 資料及地面站收集的天線追蹤數據，以掌握衛星的飛行動態，並進行衛星軌道轉換，已經成功地操控福衛一號、二號及三號衛星，初步具備不對稱反衛星能力。

除了太空科技發展，台灣的關鍵資訊基礎設施以及通信設施，同時面臨中國火箭軍以飛彈或電偵部隊以無人機、空軍以反輻射飛彈攻擊之威脅。此外，中國也可能以電戰部隊發動干擾。台灣除加強防空與反干擾戰力，面臨中國發展反衛星戰力之威脅，若要發展可直接打擊衛星的武器，則有資源上的限制。國軍未來可持續發展無人載具、增購機動化雷達系統、機動干擾器（中科院正積極研發「單兵導航衛星干擾系統」、「衛星導航干擾系統」、「合成孔徑雷達衛星反制系統」）、整合預警系統及強化反飛彈能力等作法，削弱中國在衛星的軍事運用，以創造制太空權不對稱能力。可持續發展無人載具、增購機動化雷達系統、機動干擾器、整合預警系統及強化反飛彈能力等作法，削弱中國在衛星的軍事運用，以創造制太空權不對稱能力。³

目前各國對於軍隊在資安治理中的角色，其實尚無明確界定。國安會於 2018 年藉由發布《國家資通安全戰略報告》，將國軍界定在資安人才培育與資安產業發展的促進角色，並與其他政府部門一同參與國家資安聯防體系，對於資安風險診斷、關鍵資訊基礎設施保護及國際情報分享等，國軍參與的角色及途徑仍待進一步釐清。

在平時獲得授權，被動受要求支援的情形之下，國軍可以秉持「超前部署，預置兵力」原則，參與平時資安聯防，發揮專業人力與設備能量，對於關鍵資訊基礎設施實施資安風險診斷，俾利實現關鍵資訊基礎設施保護之國土防衛，並可進一步實現與國際理念相近國家遂行國際資安聯防與情資交換，並進一步合作組成資安虛擬聯防體系。

最後，國軍面對具高度政治性的假消息與仇恨言論，必須謹慎處理。另一方面，防禦中國輿論戰與心理戰，乃國軍職責所在。因此，國軍必須拿捏投入此一政治作戰的分寸與界限，才不至於淪於政治不中立的批評。就此，建議國軍政治作戰專業應結合第三方公正事實查核團體或個人，並輔以人工智慧技術發展，遂行假消息與仇恨言論之查察，俾利反制中國對台之輿論戰與心理戰。

³ 林柏州，〈從美國升級 GPS 看全球導航系統發展〉，《國防安全週報》第 18 期，國防安全研究院：2018 年 10 月 19 日，第 15-16 頁。

第六章台灣發展不對稱戰力的利基

舒孝煌、許智翔¹

前言

21世紀初期以來，伴隨中國經濟成長，解放軍戰力快速提升。中國增加軍事投資，雙方的軍力差距持續加大，軍事平衡已嚴重傾斜。對於物資經濟實力與人力皆難以單獨與中國抗衡的台灣而言，藉由不對稱作戰方式抵銷與中國間龐大的實力差距，是今後的必然考量方向。

台海兩岸有海峽天險阻隔，中國軍隊快速高科技化下可能造成弱點，台灣則具備某些技術能力優勢，在各種不同先天、後天條件之下，台灣確實擁有發展強大不對稱作戰的優勢與利基。不對稱戰力與基本戰力如能適當取得平衡，不但在實際面臨衝突時能發揮作用，同樣也是嚇阻以避免戰事發生的重要籌碼。因此，在依國防部「防衛固守、重層嚇阻」戰略指導原則下，持續精進國防戰力的同時，不對稱戰力應視為整體國防軍事戰略的重要一環，由戰略、科技、國防經濟等不同面向，持續進行研究及投資。

壹、地緣優勢

一、台灣地理的優勢及劣勢

台灣地處西太平洋，四面環海，為一島嶼地形，東臨西太平洋、西濱台灣海峽，北靠東海、南倚巴士海峽，陸地總面積約為36,000平方公里，東西窄、南北長，全島2/3面積分佈高山林地，其他則為丘陵、台地、海岸平原及盆地所構成。主要山脈皆為南北走向，中央山脈由北到南縱貫全島，玉山山脈主峰接近4,000公尺，為東北亞第一高峰，3,000公尺以上山峰超過200座。山地地形佔全島54%，加上河川多為東西走向，將整體地理環境切割成多塊，造成台灣特殊地理景觀。

台灣陸地不大，東西寬僅144公里，縱深過短，但加上台灣海峽，可以擴展為12萬平方公里，再加上其他海域，「海洋腹地」面積更可以大幅增加。此外，台灣尚控制台海數個外島，如金門、馬祖、澎湖，更增加我軍事部署上的彈性。

台灣海峽是隔開台灣與大陸的天險，西距離大陸最近為新竹至平潭，約130公里，西南部距廣東省海岸則為300公里，平均寬約180公里，南北長約300公里。平均水深雖不足50公尺，實則差異甚大，有水深超過1,000公尺的大陸坡，

¹ 舒孝煌，國防安全研究院國防資源與產業研究所助理研究員，負責本章內容；許智翔，國防安全研究院先進科技及作戰概念研究所博士後研究，負責本章第三節部分內容。

也有不足 30 公尺的淺灘，因此極不利潛艦活動，但卻可運用距岸水淺特性，實施防禦部署，增加登陸部隊的困難。

台灣海峽屬亞洲大陸外東亞島弧的一部分，北從千島群島、日本諸島、琉球群島，經台灣至菲律賓，冷戰時期成為以美國為首的西方世界圍堵共產世界的第一道前線，故又被稱為第一島鏈（First Island Chain）。台灣居於第一島鏈的中央位置，由東海至南海，不論海空交通，都需通過台灣。

二、台灣周邊航運

在海運上，東南亞至東北亞是最重要的海運航線之一，其中一條經由台灣海峽至台灣或中國港口，往北則到日本及韓國；另一條經巴士海峽後再北上，直接前往日、韓或駛往太平洋。除台灣外，日本、韓國乃至中國，其石油及天然氣消耗，幾乎都依賴進口，東海、台灣海峽、巴士海峽、南海是能源運輸必經之地，可見台灣周邊航道與鄰近國家經濟安全密切相關。

在航空方面，由東北亞至東南亞也是全球空中航班最密集區域，Routesonline 2018 年公布全球百大繁忙航線，桃園至香港名列第 8，2017 年旅客人數達 671 萬人次，飛航航班達 28,881 班，若在國際航線則排名第 1，²另外，桃園至東京成田 12,787 班居第 74、桃園至關西 14,211 班名列第 82。³

從國防安全角度，台灣地理環境地理特性同時具有劣勢及優勢，劣勢是台灣腹地甚小，在現代戰爭中幾無戰略縱深可言；現代軍事講究快速打擊，本島若遭敵突擊，防禦作戰部署將失去彈性及先機。優勢則是有台灣海峽天險阻隔，加上地理環境上的複雜度，使台灣安全上的最大挑戰者—中國，在計畫任何軍事行動時，即使能跨越台海天險，也將面對島嶼陸地的複雜及破碎。

台灣縱深雖短，但因中央山脈將東西部阻隔，使得東西部無法經由陸路直接穿越，需繞經南北端始可抵達，這無形中增加台灣部署的彈性，以及敵登陸作戰的困難。外敵對台作戰時，需同時考慮西部及東部兩個面向，國軍可以增加東部部署作為備用選項，保存重要戰力，減少西部重要軍事設施遭摧毀時，失去軍事反擊能力。惟若對手海空武力投射能力進一步擴展，能由海空加以繞越，則將使東部反面臨敵人精準打擊能力的挑戰。

² “Busiest passenger air routes in the world revealed,” *Routesonline*, September 16, 2018, <https://www.routesonline.com/news/29/breaking-news/280477/busiest-passenger-air-routes-in-the-world-revealed/>。

³ “These are the top 100 busiest routes on earth,” *Routesonline*, September 16, 2018, <https://www.routesonline.com/news/29/breaking-news/280568/these-are-the-top-100-busiest-routes-on-earth/>。

貳、台海戰場特性

一、威脅多樣化

由於戰爭型態轉變，如果台海情勢惡化，中國顯將運用多種手段對台施加威脅，台灣未來將面臨的戰爭型態，將更趨多樣化、複雜化。中國軍事科技也隨著世界趨勢發展，武器系統日益精準，可先使用遙攻武器如飛彈等，先行穿透台灣綿密防空網，以精準打擊摧毀關鍵軍事設施，先行瓦解台灣的偵測及即時反擊能力。然而，也可能使用非正規方式。未來戰爭的殺傷面積更小，戰爭朝向小型、精準、外科手術式發展。另一方面，非殺傷式作戰，例如電磁戰、網路戰、輿論戰、心理戰等，以及破壞攸關國家社會運作及人民日常生活的關鍵基礎設施等等非傳統戰法，則可能對國計民生造成重大影響，間接影響國家軍事反擊的能力。

在軍事戰方面，非傳統式戰具如小型 UAV、自動化機器人等，在作戰中的運用日益增加，不僅增進部隊情監偵、作戰與後勤等能力，卻也使敵人可能在戰爭發起前，即以網路戰、電磁戰等技術，讓傳統戰具減少或喪失其作戰效能。換言之，戰爭在大規模部隊動員、兵力集結前即已發起，前方和後方的傳統意義也不再存在。

二、遠程打擊為最大威脅

由於台海天險阻隔，在現代戰爭中，掌握制海及制空權為獲得戰場優勢的先決條件。因此，任何對台軍事上的首波攻擊必先來自海上及空中。當敵人掌握制空及制海權後，才能進行渡海登陸作戰。中國過去海空軍發展速度緩慢，對台威脅需依賴長程武器。但早期飛彈也缺乏有效打擊台灣軍事目標的能力，如 1995-96 年台海飛彈危機中，中國飛彈主要目的，只是對台發揮威嚇效果。

中國軍力經歷 20 年發展，並在 2015 年實施軍改，將各軍種賦予平等發展地位，並提升火箭軍，不論傳統陸、海、空軍，或長程火力投射方面已有長足發展，強化其「反介入／區域拒止」(A2/AD) 能力，對台軍事威脅自亦大幅提升。中國對台當面部署 1,000 餘枚彈道飛彈，其中主要為先進的短程彈道飛彈(SRBM)，如東風 11、東風 15 及東風 16，其精準度較早期不具精準打擊能力的飛彈為佳，可精準擊中台灣軍事目標。此外，中國還部署遠程多管火箭、巡弋飛彈、大型無人機。⁴與彈道飛彈不同的是，巡弋飛彈以超低空飛行，無人機飛行速度雖慢，但更為靈活，均難以攔截。遠程多管火箭則是較廉價的武器，可以進行多波次打擊，

⁴《國防部 107 年中國軍力報告書》，中華民國國防部，2018 年 9 月 1 日；“Able Archers: Taiwan Defense Strategy in an Age of Precision Strike,” *Project 2049 Institute*, September 22, 2014, <https://project2049.net/2014/09/22/able-archers-taiwan-defense-strategy-in-an-age-of-precision-strike/>。

增添國軍在防衛作戰上的困難。

美國國防部公布之《中國軍事與安全發展報告》(Military and Security Developments Involving the People's Republic of China 2018)指出，中國運用先進軍事能力脅迫台灣，並逐漸強化入侵能力，對台灣安全構成主要挑戰。中國從未放棄使用武力，持續發展先進能力以因應可能的軍事衝突。中國近期陸、海、空軍之發展雖強化武力投射能力，不過兩棲作戰風險仍相當高，新近擴張之陸戰隊發展方向尚不明確。隨著軍事能力擴張，中國對台用兵選項也趨於多樣化，包括海空封鎖、有限兵力或脅迫 (coercive) 行動、空中及飛彈打擊及入侵台灣。⁵

我國防部《中國軍力報告》亦指出，中國現階段若對台用武，可能行動包括聯合軍事威懾、聯合封鎖作戰、聯合火力打擊、聯合登島作戰等，在取得「三權」(除制空及制海權外，尚包括制電磁權)，並癱瘓國軍大部分戰力後，結合其火箭軍及三軍部隊，三棲進犯本島，力求速戰速決。

三、武力投射能力跨越地理限制

上述兩分報告均持類似看法，即中國尚無大量建造兩棲艦艇跡象，目前登陸載具及後勤能力仍不足，暫無發動全面犯台之正規作戰能力。對傳統大規模登陸作戰而言，由於台灣本島在原本地理環境限制，以及都市化發展，可供大型登陸部隊運用的地點實為有限。就西部海岸來說，海岸附近緊連著大大小小的都市及鄉鎮，對進攻方而言同樣造成極大困擾。另由於中央山脈限制，台灣東西岸互相聯繫的陸上通道亦相對有限，同樣成為不對稱作戰在地形上可藉之屏障。

惟中國仍有計畫建造大型兩棲艦、運輸及攻擊直升機有長足發展，且擁有大型氣墊登陸艇，且新型運 20 運輸機已開始量產，其對外武力投射能力發展正持續強化。由中國持續實施轟 6 或運 8 電戰機、以及遼寧號航艦編隊刻意繞行台灣周邊海空域、赴西太平洋訓練、或由東部通過，顯然拜其海空作戰平台進步之賜，軍事行動選項大幅增加，不但台海天險不復存在，甚至對叢山阻隔的東部也造成重大威脅。遼寧號航艦雖空中作戰能力有限，然其仍可藉殲 15 作戰半徑優勢，在我方攻擊距離外發射攻陸武器，也可以其有限空優能力形成防空網，掩護由內陸出海進入西太平洋之轟 6 轟炸機，發射反艦或攻陸飛彈，強化其對東部威脅。

由其軍事演訓可知，中國持續對台保持相當之軍事壓力，且未放棄武力犯台想法，不能輕視其武力投射能力提升的幅度及方向，同時應視其軍事威脅的方向，適時調整島上防務規劃的重心。

⁵ "Military and Security Developments Involving the People's Republic of China 2018," US DoD, August 16, 2018, <https://media.defense.gov/2018/Aug/16/2001955282/-1/-1/1/2018-CHINA-MILITARY-POWER-REPORT.PDF>。



圖 6-1、我 IDF 警戒伴飛

資料來源：中華民國空軍司令部。

參、裝備投資選項

中國傳統武器載台技術，如飛機、水面艦等技術仍不斷提升，並持續發展其 A2/AD 或不對稱作戰，除已成為美國及其盟國的挑戰，對我國更是嚴重威脅。台灣軍備規劃，應該包括基本戰力及不對稱戰力兩個面向，基本戰力包括傳統陸、海、空兵力，不對稱戰力則包含傳統與非傳統戰爭手段，以我方之強點，針對敵方特定弱點，實施出其不易攻擊，削弱其力量、並創造有利我方態勢。以下分析基本及不對稱戰力之建軍備戰方向。

一、強化關鍵設施及戰力保存

首先檢討強化戰力保存，如何增進戰時空軍戰機起降可用跑道選項：例如持續強化、增進空軍基地之跑道、副跑道、滑行道、連絡道與延伸停機坪之運用，以便戰機緊急起降。除檢討其他民用機場在戰時之運用，包括桃園國際機場、小港機場、恆春機場、豐年機場等，並思考持續運用國道及省道戰備道，增加空軍備降運用空間。軍用船艦亦可運用全台周邊各小型漁港進行疏散，以避免遭封鎖。

另外，共軍規劃藉由二砲飛彈多次齊射，或使用搭配跑道穿透子母彈及人員殺傷彈的混合彈種，或者使用延時引爆子母彈等方式，來殺傷、瓦解我機場工程單位，遲滯、癱瘓機場跑道搶修作業。因此，需要強化跑道、港口及關鍵指管設施的偽裝、搶修與恢復，強化跑道搶修小組在敵火威脅下作業及對延時引爆彈藥處置之能力，以帆布等偽裝設施覆蓋已修復或受損跑道，達「能而示之不能，不能而示之能」的偽裝、欺敵之效。

重要軍事設施之保護措施應加以強化，如增加部署陸劍 2 等短程防空飛彈、增加機動雷達部署，於機場周邊進行電子干擾，防止 UAV 偵測；重視分散式部署，強化指管與偵搜備援能力，確保萬一遭攻擊，個別防空作戰單位（如防空飛

彈、空軍各作戰隊等) 仍具有獨立作戰及反制敵後續軍事行動之能力。此外，應強化對重要目標偽裝，並阻止敵進行戰場偵照及損壞評估。



圖 6-2、漢光 30 號演習時空軍幻象進行戰備道起降演練
資料來源：舒孝煌攝。

二、發展彈性化之無人、非傳統打擊能力

發展具較長程打擊能力之 UCAV，用以攻擊敵海上集結之登陸船團及敵當面戰略及軍事目標，並減少對空軍主力戰機之依賴，減輕戰時戰機任務負擔，亦可作為誘餌以消耗敵防空飛彈。UAV 可使用一般道路起降，部署容易，敵難以發現與反制。其武器可使用地獄火飛彈、或發展適合 UAV 使用之多功能精準武器，如反艦飛彈或子母彈撒布器，對敵船艦、港口、機場、飛彈陣地等進行再反擊，阻止或遲滯敵軍事行動，使其作戰想定複雜化。

依「固安作戰計畫」，外島雖需「獨立固守」。然現今武器科技及載具已呈彈性及多樣化發展，外島除可配備視距外防空及反艦武器外，亦可部署 UAV，削弱射程範圍之敵空中、海上載具，阻滯敵戰力並增加敵部署與投射武力困擾。

三、發展具備不對稱優勢之防空武器

不論歐美或中國軍方都在發展雷射武器，美智庫也關切雷射武器發展現況及其不對稱作戰之優勢。⁶美國雷射武器原著眼於因應急迫性威脅，並運用商用市場可取得之工業用高能雷射，用以保護船艦或基礎設施等，對抗導引火箭、火炮、迫砲、飛彈、UAV 等急迫性威脅，並且減少反制敵先進 A2/AD 武器之成本。現

⁶ “Changing the Game: The Promise of Directed-Energy Weapons” CSBA, April 19, 2012, <https://csbaonline.org/research/publications/changing-the-game-the-promise-of-directed-energy-weapons/>; “The Next U.S. Asymmetric Advantage: Maritime Lasers to Counter the A2/AD Challenge”, Lexington Institute, March 2014, <https://www.lexingtoninstitute.org/the-next-u-s-asymmetric-advantage-maritime-lasers-to-counter-the-a2ad-challenge/>。

在雷射武器逐漸發展成熟，並朝向高能量發展。⁷目前美國海軍及陸軍已對型發展中雷射系統進行測試，空軍亦提出未來雷射系統需求。此外，如美國空軍實驗室、國防先進研究計畫署及各主要軍事公司如波音、洛克希德馬汀（Lockheed Martin），歐洲之萊茵金屬公司（天兵防空系統生產廠奧立崗 Oerlikon 的母公司），均在發展雷射武器系統。美國陸軍並成功在歐洲展示在史崔克裝甲車（Stryker）上裝置雷射，這說明雷射武器已經漸趨成熟並邁向實際部署。⁸我國可參考美國與歐洲目前發展雷射武器之經驗，發展適合我軍防衛作戰需要之雷射，減少我防空武器發展及部署成本，強化對基礎設施及作戰單位之保護，並增加敵空中突襲成功之不確定性與成本。

四、強化制空制海戰力

除持續國機國造及國艦國造外，我仍應向美爭取出售關鍵裝備，如具短場起降能力之第 5 代戰機、以及國艦國造或潛艦國造之關鍵紅區裝備。若暫時無法獲得，即因思考其他替代方案或過渡時期選項，如以高教機附帶掛載武器能力，以填補部分空軍作戰任務。未來即使可獲得 F-35B，因其價格昂貴、系統複雜、對空地勤均為負擔，應思考採高一低性能混搭方式，搭配國造新型戰機，以減輕預算及後勤負擔。

五、強化地面戰力

雖然海空防禦能力是台海防禦主軸，但地面戰力如適當發展，仍能在新戰略中發揮作用，強化不對稱作戰優勢，例如從小型機動到長程，考量不同火力發揚方式、加強單兵火力、以及強化生存性。前者包含智慧型先進迫擊砲及可裝置於輕型車輛的機動火炮系統；後者則是可以是新式的長程火炮。類似裝備可在美國陸軍當前提倡的多領域戰鬥中發現，如美國正在研發的新式 58 倍徑 155mm 榴砲預估可將射程提升至 70 公里之遠，而搭配衝壓引擎助推的砲彈，甚至可能攻擊 100 公里外之目標，再搭配陸軍戰術飛彈如美國當前的 ATACMS 或是正在研發中的 PrSM 戰術飛彈，提供 100 公里外之火力。藉由地面的多層次火力投射，一方面使得陸軍除能更進一步契合當前「重層嚇阻」概念，也能分擔海空軍的防衛重擔，甚至偕同海空軍，對戰術飛彈射程內的重要設施目標發動打擊。

台灣西部地狹人稠，不論對手在哪一個點登岸，除了在灘頭交戰之外，很可能也會進入住民地戰鬥。因此。做為陸軍骨幹的步兵單位有需要加強其包括迫擊砲、反戰車武器在內的各種火力投射能力。

當前各式武器精密高價化，同時加上長時間以來的少子化，使得將來從兵員到載具的數量，都將遠於過往。因此，強化防護能力與生存性至關重要。從載具來說，最明顯的方式即例如為戰車強化防禦能力，包括裝甲（例如為可能將採購

⁷ “Lockheed-Dynetics team and Raytheon locked in battle to build 100-kilowatt laser for US Army”, *Defense News*, August 7, 2018. <https://www.defensenews.com/digital-show-dailies/smd/2018/08/07/lockheed-dynetics-team-and-raytheon-locked-in-battle-to-build-100-kilowatt-laser-for-us-army/>。

⁸ “US Army successfully demos laser weapon on Stryker in Europe,” *Defense News*, March, 21, 2018, <https://www.defensenews.com/land/2018/03/21/us-army-successfully-demos-laser-weapon-on-stryker-in-europe/>。

的 M1A2 戰車搭配 TUSK 附加裝甲套件，以及現有戰車防護力的升級）與主動防護系統（APS）等，同時兵員的人身防護裝備同樣需要更新，而野戰醫療能力同樣必須加以重視，以求盡力減少交戰時的損害。

六、強化電磁干擾能力

干擾/反制敵方精密導引與電子系統之設備。中國解放軍在長期的現代化投資後，亦開始慢慢轉型為如西方國家部隊般運用各種高科技裝備的先進軍隊。因此，投資相關裝備以強化干擾及反制的能力，包括對 GPS/北斗系統，甚至是空中預警機等裝備，亦成為當前須更重視的項目。

七、強化運用無人及智慧化系統

募兵制及少子化使得兵員數量銳減，有限人力需做更有效率運用，應強化國軍運用自動化及無人化操作系統之運用。例如使用大型無人機執行長時間任務，如海域及空域監視任務，一架無人機滯空時間可長達 10 餘小時甚至 20 小時以上，透過資料鏈將監視資料下傳至接收站，即可減少派遣空中預警機之負擔。火炮、工兵、特種部隊則可使用機器人協助搬運重型貨物如彈藥及裝備，減輕士兵負荷。另外，強化火力單位的自動化（如雷達偵搜、火炮採自動裝填等），同樣減輕人力負擔及增進效率，透過其他前方、後方，如鎊重、補給、保修等各種領域，運用無人以及智慧化、自動化系統，可節省寶貴人力。



圖 6-3、可執行海上偵搜的 MQ-1 無人機

資源來源：舒孝煌攝。

八、強化通資安全

依國安會《2018 國家資通安全戰略報告》，資安威脅可分為國家支持型、犯罪組織型、理念宣傳型、恐怖主義型等類別，我國可能遭侵駭對象包括政府體系、關鍵資訊基礎設施，如電信、金融、醫療、能源、水資源、交通與科學園區等，以及關鍵民間產業如擁有智財權、商業機密、影響產業數位化的關鍵企業，以及

國防工業等。目前資通安全主管機關為行政院國家資通安全會報，下設有資通安全處。我應強化國家整體通訊及資訊安全，目前國內 8 大關鍵資訊基礎設施防護包括政府、高科技園區、能源、水資源、通訊、交通、銀行與金融、緊急救援與醫院八大關鍵資訊基礎設施。其中，通訊網路是以上 8 大領域關鍵持續運作的骨幹，通訊基礎設施的資安防護由國家通訊傳播委員會負責，將強化早期預警、持續控管與維運、通報應變及協處改善。另外，也應整合國防、外交等單位，強化國安層面的資通安全防護。⁹

肆、確保局部科技優勢

國防是國家實力的資產而非負債，國防預算不應視為是「消耗型」預算，而是「國防經濟」(defense economy)，即國家整體經濟及科技實力的一環，無論是國防科技人員、各種類型的裝備研發、生產及採購，武器系統的作業維持、壽期維護及性能提升，都是國家整體經濟活動的一環。軍用與安全事務是特殊市場，受經濟景氣影響較小，具備「戰略經濟」(strategic economy) 的價值，對國家經濟發展更形重要。

在既有之國機國造、國艦國造基礎上，我應結合軍方及民間科技力量，投注於潛力之未來國防科技發展，並將民間發展科技之創新能力與活力，運用於建軍備戰，創造我基本戰力及不對稱戰力優勢。

一、多樣化無人與自動化載具

除傳統武器平台如下一代匿蹤戰機、潛艦外，應置下一階段國防自主重心於發展各種型式之 UAV，包括其動力系統、感測器、遙控能力、自主操作能力等，支持國軍各階段作戰，例如：

- (一) 能偵打一體的中大型 UAV，不但可在海上進行搜索，並可對低速、防空能力薄弱的艦艇如給油艦、兩棲艦等進行打擊。
- (二) 自殺型 UAV，於作戰時大量部署於台海，本身載有作戰部如高爆炸藥或次彈械，能在空中依設定航線巡航，發現目標時即予摧毀。
- (三) 迷你型 UAV，如群集式攻擊的小型 UAV，可用以干擾敵空中作戰、偵搜系統如飛彈的雷達尋標器，以及飛行器的飛行等，或者本身搭載炸彈，用以攻擊敵方登陸船團等。
- (四) 運輸型 UAV，為大型四軸或多軸式 UAV，能垂直起降並運送重貨，用以

⁹ 《2018 國家資通安全戰略報告》，國家安全會議，2018 年 9 月，
<https://www.president.gov.tw/File/Doc/588f1a08-5ea7-41df-b0d0-482a00b45322>。

向前線運送補給品、燃料、彈藥等，減少因交通線被截斷或後勤兵源不足之困擾。

- (五) 水面無人載具 USV 或水下無人載具 UUV，干擾敵登陸船團、掃布雷艦或執行封鎖等任務之艦艇；發展特定用途之大型 UUV，執行襲擊大型艦艇或敵港口之特種任務。



圖 6-4、中科院發展的騰雲大型無人機

資料來源：舒孝煌攝。

二、可攔截小型低空目標之彈性化火力與發射系統

敵方的小型、低飛目標如迷你 UAV，我方現有防空系統未必能搜獲並接戰，即使偵獲，大型長射程防空飛彈雖可以爆炸時之破片或衝擊波擊落小型 UAV 或使其失效，但高價、數量有限之長程防空飛彈攔截廉價的小型 UAV，不符成本效益。另外，小型 UAV 本身無法飛越台海，可能由其他載具如飛機或火箭加以投送，至本島低空執行任務，若以大型飛彈攔截，則有傷及我方人員及民間設施危險。

(一) 強化對小型或戰術目標的彈性攔截能力

應確保我方彈性因應敵方各種不同的作戰行動，並保留適當戰備彈留供後續階段作戰使用，同時可以因應突發戰況或即時目標立即反應。例如未來的天弓飛彈同時具備反地面目標或反艦能力，陸射天箭或是反戰車飛彈也能攔截小型 UAV，並射擊地面或近程的海上目標。

(二) 強化對小型目標偵搜與干擾能力

應強化對小型 UAV 的干擾及偵搜能力。目前中科院發展之蜂眼雷達具對小

型目標偵搜能力，其他小型雷達亦具偵搜小型 UAV 能力。小型 UAV 依賴無線電訊號協助操作，在一定距離內，一個功能強大的干擾器，或是電子掃瞄雷達（AESA），亦可使 UAV 失效。



圖 6-5、中科院發展的陸射劍一及劍二飛彈

資料來源：舒孝煌攝。

三、網狀化作戰

能分散指揮體系，確保備援系統在主系統被摧毀時仍能持續運作。同時各軍種的指管通情體系能進一步分散，提供所有軍種的所有作戰單位分享，使各作戰單位都能獲得台海戰場的單一圖像，俾利迅速進行反應，且打破軍種間藩籬。指揮官可以就目標情況立刻下令附近的作戰單位，不論是在空機、海上艦艇或是陸軍火炮進行反擊。

四、彈性化的制空制海及制陸武器

包括對地、對海與對艦之彈性化長程武器。發展新一代彈性制壓武器，平衡敵我雙方長程打擊能力之差距，並解決目獲與中繼導引等問題。發展能夠威脅敵方大型艦艇的長程反艦武器，或是耐航性佳，有偵搜系統的大型自殺式 UAV，或是在智慧化武器上加裝動力及彈翼，增加其制空時間，在作戰時令其在戰場空中盤旋，自行發現目標並伺機加以攻擊。發展長程陸射及海射制空武器，可遠距攻擊敵方大型高價空中目標，如預警機、加油機或電偵機。以現有天弓、天劍、雄三等飛彈為基礎，發展彈性化的反制武器，同時可攻擊陸上、海上或空中目標。

五、資訊戰、網路戰與電磁武器

強化我電子戰能力，確保能夠致盲敵方的情監偵系統、干擾遙控操作的 UAV 使其失效或墜毀。敵方一定會對台發起網路戰、資訊戰，我方則需提相應之道，除國軍內部培育專業資訊戰單位外，也可與政府部門、民間資安公司、大學資訊系所合作，在非機敏領域培養相關人力，厚植資訊戰力。

六、反制匿蹤空中武力發展

中國殲 20 戰機已少量服役，傳聞具備與美國 B-2 相同匿蹤能力之轟 20 亦將推出，遲早成為我會面對之威脅。中國目前在短程的直攻武器 (DAM) 上運用極少，較依賴長程的距外武器 (SOW)，主因為中國空軍不具如美國一般的穿透敵防空網能力，其精準度較差。但在其匿蹤空中武力成熟後，也會開始廣泛運用美式的精準打擊。另外，我空軍面對威脅將大增，與匿蹤敵機交戰時將居於弱勢。我過去曾發展匿蹤塗料等技術，地面載具除利用隱蔽，也需遮蓋紅外線跡訊以藏匿行蹤。下一代戰機及水面艦均應考慮運用匿蹤設計，如藉由外型設計偏向反射雷達波、並運用電磁吸收材料消耗、吸收電磁波能量，並大量運用複合材料，強化吸波能力。同時也可發展雙基或低頻雷達 (lower-frequency, directed anti-stealth radar)，以偵測敵匿蹤飛機。



圖 6-6、中科院發展的雙基雷達

資料來源：舒孝煌攝。

七、發展自動化器械與人工智慧用於傳統軍備

因應少子化、人力不足之募兵窘境，與民間廠商合作，發展適合軍事用途之

「仿生機器人」(Biomorphic robotics)，以模仿人類或動物之機器人，克服對地形限制，協助搬運重物、運送重物或補給、或運用在災害救助與人道援助，減少對人力負擔。其他傳統戰具與裝備則強化自動化，例如火砲改採自動裝填，使用自動化運送車運送砲彈，並採用自動化照準系統，增加命中精準度，減少發射次數。另外，也與民間廠商探討如何將新資訊技術運用於國防，舉例而言，近期提出歐洲 6 代戰機概念之一的英國貝宜航太 (BAE Systems)，其所使用的「擴增實境」座艙概念，即是結合台灣的 HTC 技術。

八、智慧型水下攻擊武器

中國水面艦快速發展，已成我海洋交通線最大威脅。其航空母艦兵力也在擴張中，可能威脅我東部防禦，並打破東亞戰略平衡。我為海島型國家，阻滯敵最大優勢就是海洋。我可發展智慧型水面或水下攻擊武器，運用戰機、直升機、快速巡邏艦、無人載具、火箭等武器實施布放，中科院已有智慧水雷研發能量，並可發展遠海「攻勢布雷」作戰，阻滯中國海上威脅。

九、匿蹤技術

匿蹤技術已是未來軍事裝備設計的標準，國內應建立對匿蹤技術的基礎能量及研發能力，例如材料、塗料、外型，針對不同特性偵測系統的匿蹤需求，研發匿蹤技術的基本科學理論，運用在下一代戰機、水面艦、無人機、彈藥等領域。

十、其他局部科技優勢

依國內科技能量及國軍戰略指導，發展適合我防禦需求的武器系統，並育能量於民間。例如反匿蹤科技、遠距制壓武器、整合式防空及制海科技、可用於國防領域的 AI 人工智慧科技、水下相關科技、快速佈雷技術、導能武器如結合現有防空系統的雷射武器、微衛星與衛星反制技術、電子戰、網路戰相關技術。

小結

綜合本章節之分析，台灣在發展不對稱作戰的方面顯然可以將重心放在以下幾個項目：戰力保存、人力資源有效運用，以及各種新形態的作戰方式與領域等為主，並主要著重於技術及戰術戰法領域上的不對稱。除了承平時期的嚇阻之外，還包括真正面臨衝突時、其對台灣戰力的實際加乘效果，並減低雙方在數量不對稱上對台灣帶來的劣勢。現今國際間各國高度互賴、經濟高度發展，曠日廢時的長期戰爭對國家帶來的傷害更勝於以往，對手因需短期結束戰事，將面臨更大的時間壓力，故在提高前述各方面不對稱能力同時，我方防衛固守的能力也能因此得到加強，台灣也更能強化平時的嚇阻能力。

第七章前瞻台灣國防科技與產業整合

蘇紫雲¹

前言

台灣發展國防科技產業，可以讓國防預算的投入發揮經濟效益，成為正向循環。要達成此一目標就必須先衡量自身產業的利基，並掌握國際的國防產業環境，以辨識發展項目之優先次序，找出台灣國防科技與產業整合的最佳途徑。本章先剖析美中貿易及科技戰影響，以及台灣進入產業供應鏈的優勢，冀能標定台灣科技與產業的機會，並進一步盤點值得發展的科技，尋求務實可行的科技與產業整合途徑。

國防產業經常會涉及兩用科技與產品，廣義而言係指可用於商業市場，同時也可用於軍事戰場，甚至用作製造用於核武、飛彈、化武、生物戰劑等大規模毀滅武器。以美國為例，類似產品或技術在出口之前都需要獲得相關輸出許可，然而，兩用技術擴散後，軍民兩用產品可利用特定方式迴避輸出許可，或偽造獲得輸出許可，甚至使用空頭公司以及摺客的名義購買，以掩護真正的最終用途。

而具威脅性的敏感技術也由前述的核生化擴大至看似無關的資訊科技領域，例如現正熱議的網路戰、資訊安全等議題。因此，美國早在 2011 年也訂出未來指導的網路政策「五大戰略」，正式將網路空間列為等同海、陸、空和太空的「作戰領域」，但為避免國際關係變得複雜，策略「主守」不「主攻」。未來型態的網路戰，將由衛星、網路的虛擬空間，橫跨到金融、交通、生產、電力控制等各個領域，最極端的現象將導致機具的實際破壞呈現「複合型」的實體攻擊。²

當前，美國川普政府對中國的貿易戰，可說有總體考量，尤其是管制敏感科技出口以及中國科技產品的使用，台灣應該掌握的契機，積極投入對自身有利的國防科技發展，藉此進一步打入國際的國防產業供應鏈，鞏固在國際合作國防科技產業的地位。而符合我國工業水準且具發展潛力的科技，包括定向能武器、仿生機器人、主動防禦科技及匿蹤科技之外，台灣在人工智慧、網路安全、立體列印、自駕科技、虛擬科技及無人載具都已具備相當基礎，這些軍民兩用科技，也將為台灣產業發展與民生福祉，帶來長足的助益。

¹ 蘇紫雲，國防安全研究院國防資源與產業研究所副研究員，負責本章內容。

² “International Strategy for Cyberspace”, (Washington, D. C.: White House, 2011), pp. 10- 11.

壹、美中貿易及科技戰的影響

美中的貿易戰由美國川普總統於 2018 年 3 月 22 日簽署備忘錄揭開序幕，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財權(intellectual property)的狀況進行聽證與調查。⁴並隨即於 2018 年 7 月 6 日正式啟動第一波行動，對價值 500 億美元的商品加徵關稅，緊接著於同年 9 月 24 日起美國再對貿易規模達 2,000 億美元的商品課徵 10% 關稅，發動第二波的關稅攻勢。⁵華盛頓並表示若中國方面無法與美國達成有意義的解決方案，不排除於 2019 年開始再對其他 2,670 億美元的商品開徵 25% 的進口關稅，若第三波貿易戰啟動，將等同對中國進口商品全面加稅。而 2018 年 12 月 1 日美中雙方元首在「20 國集團」(或謂 G20 峰會)會面舉行的「川習會」，在中方釋出部分善意並表達願意協商的情況下，美方決議前述 25% 關稅的調整政策給予 90 日的緩衝期。⁶看似有所轉機，但實際上要美方全面停止貿易戰卻仍困難重重。

依照美國普查統計局(Census Bureau)結算，在 2017 年美國對中的逆差已達 3,750 億美元，同時再對照中國商務部 2017 年公布的資料，等同北京年外貿順差的 86 % 以及 GDP 的 3% 都仰賴美國單一市場，中國的此種高度倚賴形同戰略弱點。進一步來看，一方面美國對中的鉅額貿易逆差固然使川普總統亟思平衡，另一方面北京對美的鉅大貿易順差來自美國單一市場，也使中國 GDP 的成長過度依賴美方，對北京而言更是真正的軟肋。因此決定美中兩大國的真正核心利益，是國內的經濟發展與就業率，急迫性與重要性高過軍事對抗、北韓、南海，乃至「一中政策」等議題，也使得美中貿易戰無可避免。⁷

必須特別指出並注意的是，早在在 2018 年貿易戰開打之前一年的 2017 年 7 月，川普總統簽署 13806 號行政命令(Executive Order 13806)，直接下令國防部對美國國防產業的安全性進行評估，⁸一年後的 2018 年 10 月 5 日，美國國防部公佈名為《評估並強化美國國防產業的製造基礎與供應鏈韌性》(Assessing and

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 Documents*, 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 Yen Nee Lee, "It's not over: The US- China trade war is still on despite 90- day tariff ceasefire, experts say." *CNBC*. Dec.2, 2018. <https://www.cnbc.com/2018/12/03/us-china-trade-war-still-on-despite-trump-xi-90-days-truce-experts.html>

⁷ <美中台 2017 / 兵棋推演之三，蘇紫雲：關鍵變數在中美貿易戰>，《中國時報》。<https://opinion.chinatimes.com/20170119005374-262105>。

⁸ "Presidential Executive Order on Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States", *White House*, July 21, 2017, <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-assessing-strengthening-manufacturing-defense-industrial-base-supply-chain-resiliency-united-states/>。

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》)，該報告提出明確警訊，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。同時，中國的經濟發展促進軍事力量的快速發展、並以侵略型的經濟擴張、軟實力戰略、以及隱藏性的軍事研發經費支應科技合作，甚至文化性的滲透對美國造成全面威脅。實際上，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經濟與軍事崛起的最大推手。⁹此皆清楚指出中國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威脅模式完全不同。

至於對美國防產業構成的威脅，該報告列舉之事項可歸類為下列幾項：

(1)定調中國壟斷關鍵原物料。報告特別提到了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。中國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。¹⁰(2)認定中國掠奪性製造。中國以各種竊取科技的方式進而發展掠奪性的製造業，目前已生產全球 70% 的太陽光板、24% 的電力、28% 的汽車、41% 的船隻、50% 的冰箱、60% 的電視、80% 冷氣空調、以及 90% 的行動電話。¹¹(3)指控中國以經濟為戰略工具。北京最近對斯里蘭卡發動的「攻擊性經濟戰」(aggressive economic warfare)，在近年同樣用於對付南韓佈署 THAAD 事件、菲律賓的南海爭議、日本的釣魚台爭議、以及用於威嚇台灣。可以預見，若中國持續坐大，未來也將威脅美國。

以上足見在貿易戰開打前，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，並可能已決定對北京進行全面的戰略壓制。

前述的貿易與科技戰，也可視為印太區域的安全情勢呈現嶄新架構的戰略背景，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)，作為美國正式回應中國的戰略手段。事實上，美中的關鍵矛盾在於價值觀的異質性，貿易摩擦、地緣政治等問題。「中國威脅論」更有了新面貌，不只軍事崛起、經濟壯大，強調威權治國更為有效的「中國模式」顛覆西方價值體系，成為民主國家的最大挑戰。另一戰略意義，則肇因於中國過度賴美國單一市場，形同華府擁有對中的經濟核彈。凡此都促使雙方的競逐白熱化。

美中貿易戰表面上係美國不滿對中國長期處於逆差，因此發動三波的關稅調整。但由《國防授權法 2019》、副總統彭斯(Mike Pence)在「哈德森研究所」(Hudson

⁹ “Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States,” *US DoD*, (Washington D. C.: DoD, 2018), p. 44.

¹⁰ *Ibid.*, p.37.

¹¹ *Op.*, cit., p. 36.

Institute) 的演說、以及《強化美國防產業》等官方文件與態度觀察，美國貿易戰的同時也著重科技安全以及未來的經濟競爭。同時，美國貿易戰的進行將有助劃清美商對中投資的界線，減少科技外流風險，確保未來競爭力。並可對中國的經濟發揮戰略打擊效果，使其軍事投資、內部政經穩定性的受到重大衝擊，間接減弱其對外部的威脅。

宏觀來說美國新的印太政策與戰略，整體而言對台灣相對有利，美國除力求經濟貿易的平衡外，更進一步壓制中國的全面擴張，此或可視為台灣的戰略機遇期。台灣良好且健全的製造業可有效取代中國既有的供應鏈，重點包括零組件、次系統、以及工規符合軍事需求的成品件。這將是美台國防產業發揮互補效應的良好模式，可兼顧防衛需求與經濟的發展。

貳、值得優先發展之科技

台灣資源有限，在投入資源發展國防科技之前，必須明確認知適合自身研發或尋求國際合作共同開發之項目，以下區科技經濟與軍民通用潛力兩類，並於後者檢視 10 項科技發展項目。

一、科技經濟的整合

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. economics)，亦即是超越科技製造業的範疇，進一步成為經濟發展的主軸。以發展中的 5G 通訊為例，涉及包括物聯網、自駕車、高解析度影像等在內的服務，也是未來經濟的主要驅動力，而這些服務應用都倚賴 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。因此，相關科技的發展也就決定國家競爭力的關鍵。

同時，軍民兩用科技(dual-use technologies)的重要性也愈為重要，主因除了前文所述及的軍事科技史的發展外，在 21 世紀的今日，由於資訊、通訊科技的高速發展，機電的深度整合，部分民用科技也具備軍用潛力，尤其是民用通資訊產品往往轉為軍用，或提升部分性能後成為軍用規格，例如筆電、甚至手機等多有轉為軍用的實際案例。

而傳統的大型軍備，軍機、軍用艦艇、潛艦、資訊安全皆盡可能採國造化，除追求國防自主的同時力圖推動產業發展，為台灣經濟注入活水。事實而言，在先進國家所謂的國防預算不再被視為「消耗型」，而是被視為「國防經濟」(defense economics)，無論是從業人員所能創造的就業機會、以及裝備生產採購、乃至作業維持等創造的經濟產值與產業升級，都應被視為國家經濟活動的一環。同時，由於軍用、安全事務是特殊市場，受經濟景氣影響較小，可提供相關業者穩定的供需環境，因此對台灣而言更具備「戰略經濟」(strategic economics)的價值。基於此特性，裝備生產的本土化也就更為重要，才能實質挹注國家經濟的發展。



圖 7-1、美軍採用之商用移動裝置

資料來源：US Army。

二、軍民通用的潛力科技

前瞻未來 10 年中短期的科技趨勢，科技對戰場的滲透將更為全面，甚至無人載具或自動化控制裝備將以「自主」模式參與戰鬥。其與民間的自駕車、高速無線網路等科技的發展都息息相關。戰場上的兵火力之結構將重行調適，作戰單位的編裝也必定出現新的面貌。由科技發展的軌跡，我們可以合理預估在未來可能具備改變戰場潛力的科技，而審視我國的產業特點，亟具發展潛力的科技主要包括：

（一）高科技傳產的應用

台灣若干具備軍民兩用價值的產業，既有基礎可說極為雄厚，雖屬非作戰裝備，但可快速獲得以增強整體戰力，並快速為民間創造經濟產值。這些產業包括：(1)機能紡織，可用於被服、金屬絲偽裝網、甚至抗彈材料等。(2)軍規筆電，具有較佳的防水、耐震、耐摔等特性，符合軍規(MIL-STD 810G)規範，可適用於戰場環境。台灣生產之軍規筆電具有價格優勢，且資訊安全可受信賴，具有高度市場潛力。(3)資安產業，此為台灣的強項之一，可有效強化資安防護與反制，且台灣最重要的資產為軟體工程的人力，可有效的爭取全球公務部門的資安市場。(4)軍用綠能，目前推行最力的為美軍，除大型基地裝置太陽能發電系統外，包括戰機、車輛、船艦等都已成功測試生質燃料的使用，並計劃推行油電混合動力載具。台灣在太陽光電、動力電池的電極材料、以及驅動馬達具有極佳優勢，此為綠能的核心技術，若與高價值的軍規需求結合，將具有極佳的市場潛力。(5)食品加工，軍用口糧(MRE)的製作，亦可說是高科技產業，結合食品加工與保存，工藝水準極高。可廣泛用於軍用口糧乃至特殊需求的醫療、戶外運動、乃至航太食品。前述列舉項目僅為台灣既有的產業優勢之一，若能加以推廣，不僅可

快速改善國軍野戰佈署所需，亦可爭取外銷，促進經濟效益。

(二)網路通訊與資訊安全

台灣的網通及資安產業極具代表性，甚至應用於國外的軍網防護。主要應用於商業市場的網路科技，特別是資安防護的科技可說與網路戰(cyber warfare)、資訊戰(information warfare)高度相關，技術相互涵蓋面向廣泛，因此可區分為硬體、軟體兩大類別。硬體最重要的演變除隨著半導體技術進步而提昇運算速度外，將是持續無線化並深度倚賴安全技術。同時，包括頻寬、穩定性、射頻設備的技術與成本等都會獲得長足進步，其衍生的意義就是涵蓋的區域、使用人口都大幅增加，而目前全球網路的規模，包括桌機、筆電、以及行動網路的使用數量約達30億的人口，¹²隨著無線通訊科技進步，頻寬流量與軟體的成本都可以降低，因此網路涵蓋率將快速增加。另一方面，軟體工程的發展則是高階語言持續發展，符合人類語言的直覺性語法、或是圖型化指令等揭有利於軟體工程的普及，並使程式設計的門檻降低，可使「程式設計師」不再僅限於工程背景為主，可有更多元背景的人力來源，未來網路戰的程式的架構、策略、應用範圍、參與的成員都會持續擴大。

可能的面貌就是網路戰的形式、攻擊對象將更為複雜而多元，其連鎖效應的深度與廣度可達網路架構的深層，以「開放式通訊系統互連參考模型」(Open System Interconnection Reference Model)為例，此一模型共分為7層架構，未來網路對抗的戰場隨著技術擴散可能將滲透到基礎結構的第二層也就是「資料連結層」(Data Link Layer)，其在電腦系統的運作介於軟體與硬體規範的層級，不僅可能導致硬體的失能甚至可造成實體損壞。網路科技的此一特性對於IT產業發達的台灣而言，具有深化發展的利基。

(三)影像處理及立體列印

影像處理科技也是台灣的產業強項之一，原先的發展主要是基於娛樂產業需求而擴大發展，而在軍事應用面的特色主要可分為虛擬實境(Virtual Reality, VR)、擴增實境(Augmented Reality, AR)、以及全像投影(hologram)等。VR是指電腦以三維座標進行向量圖型演算，模擬出的三度空間，再整合電腦圖型、顯示、網路、以及人工智慧等技術，讓使用者具有真實的臨場體驗，目前以頭戴的VR眼鏡為主要的顯影配置。

AR則是在實際的環境影像中加入特定的物件，同步呈現在使用者的載具影像，主要用途是讓使用者可體驗虛擬與實際場景的結合，例如全球流行的手機遊戲「寶可夢」(Pokemon)，就是成功的商業運用。而在其他用途，則可結合地圖導航、軍事目標標定等使用。

至於全像投影則是將影像直接投射在現實環境中，只需肉眼就可看到，不再

¹² 陳曉莉，〈Mecker 網路趨勢報告：全球網路人口突破 30 億，印度超越美國成第二大網路市場〉，《ITHome》，2016 年 6 月 2 日，<http://www.ithome.com.tw/news/106353>。

透過影像載具。其中，全像立體投影最具應用潛力與佈署彈性，目前的全像投影主要倚賴煙幕、透光片等之影像反射作業，但以雷射直接投射在空氣中的影像技術已出現原型機，¹³目前主要是用於各種特殊場合，如音樂會等，未來隨著投影技術的進步，軍事運用的潛力即為廣泛，包括誘餌、偽裝、指管地圖的立體顯示等都是極具價值的應用。

台灣的掃瞄器、印表機技術極為成熟，加上精密步進馬達、多軸加工機的精密機械產業，立體列印亦為台灣可發展之強項。由於材料科學的進步，發源於1980年代的立體列印技術，在21世紀才真正受到重視，並號稱新工業革命的動力，使得立體列印的原料具有更高的成品實用性，因此才使其應用潛力展現。目前的立體列印材料已可達到耐溫、耐壓的物理特性。主要缺點在於立體列印的速度較慢，例如整體列印一輛機車虛耗時一個月，¹⁴產量不具備經濟效益，因此主要的應用在於原型建造成本的大幅減少，或是客製化的零組件生產。

但可以合理的預估，隨著列印噴嘴、雷射光源技術、射出材料的改良，特別是金屬列印的進步，將逐步開始運用於國防產業。¹⁵因此可預見的未來，戰場的後勤維修將有機會出現革命性的運作模式，維修保養單位除部分另組件外，只需攜帶各類液態、粉態的列印材料，就可在前線列印各類零組件，對損傷的裝備進行一定程度的修護使其再次投入戰場。如此，可大幅減少零附件攜帶的數量，及其所佔據的運輸空間。無形中減少後勤尾巴的長度與負擔，而戰鬥部隊的裝備妥善率也可獲得提昇，對戰鬥力的維持與發揮將產生重大助益。同時，也可運用於太空環境或各類偏遠據點，使得遠距維修成為可能。

(四) 人工智慧

台灣有若干實力堅強的人工智慧(Artificial Intelligence, AI)研發中心與團隊。且相關科技的發展近年突飛猛進，先是屢次在人機對抗的圍棋賽中擊敗職業棋手，「堆牌」(DeepStack)此一AI軟體更在撲克大賽中，大勝職業牌手更顯不易。因為較諸圍棋賽事、棋盤上的資訊透明公開，而撲克比賽的主要難度在於「不對稱資訊的賽局」，軟體無法依賴計算，而是必須仰賴「思考直覺」¹⁶因此此對人工智慧的發展可說具備重大意義。此種「思考直覺」的能力若用於控制作戰載具，由於具有取代戰鬥員、操作員的能力，在硬體的結構設計上可節約載具的乘員空間，外型尺寸也得以縮減，使載具設計可有更大的酬載或防護力，而酬載則可用於火力配置，發揮最大的殺傷性。

同時必須注意的是，由於人工智慧的應用是否會超越人類所賦予的限制，或既

¹³ 如 Holovect, Kino-mo 等公司的系統利用雷射解離空氣形成光線折射，目前可顯示簡單圖型。

¹⁴ 謝明珊，〈Zortrax 以3D 列印 Triumph 機車測試印表機能力兼精簡製造流程〉，
《Digitimes》，2017年3月31日，

http://www.digitimes.com.tw/iot/article.asp?cat=158&id=0000497577_5rx4ch6i8apkby6o4i7pq。

¹⁵ 黃晶琳，〈震旦日攻3D 金屬列印〉，《經濟日報》，2017年3月7日，
<https://money.udn.com/money/story/5710/2324743>。

¹⁶ 〈電腦再度勝人腦，直覺思考 AI 攻下德州撲克〉，《蘋果日報》，2017年3月3日，
<http://www.appledaily.com.tw/realtimenews/article/new/20170303/1068051/>。

有的法律、倫理規範，甚至對安全層面都有極大的不確定性，例如後文所提的自駕車，在遭遇危險時將面臨犧牲車輛乘員、或是其他道路使用人的道德兩難。而軍用無人航空器若由系統取得開火的自主權，其風險誠如美國前國防部長卡特所言「人工智慧就如同 1940 年代的核武發展恐將失控。¹⁷」然而，由於其具有極大的軍事應用潛力，未來在戰場上絕對不會缺席。最基本、且無道德風險的應用，將是飛彈導引、以及預置佈署裝置，例如水雷、自主防禦系統等被動的殺傷裝置，用以提高防護效能。

（五）無人載具與自駕科技

台灣擁有世界級的遙控飛行器企業、以及前述的茲通訊科技業，此都為發展無人載具的良好基礎。如前文所述，無人飛行器(UAV, Unmanned Aerial Vehicle)的概念出現於一次大戰末期，由英國發展出的原型機在1917年3月進行試飛，目的降低飛行員傷亡，同時減少飛行員的需求與培訓成本。而無人載具實用化投入戰場則是在二戰時期，1940年德軍佔領法國後，將攫奪的技術改良研制，推出稱為「哥利亞」(Goliath)的遙控小型履帶車，德軍的戰術構想是利用其搭載炸藥，藉有線遙控方式遠距攻擊敵人的堅強據點或戰車，除可發揮精準打擊效果外，更可降低士兵傷亡，可說是現代「地面無人載具」(UGV, unmanned ground vehicle)的濫觴。而最先實戰化加入戰場「距外」(stand-off)彈藥同樣由德國推出，亨謝爾(Henschel)公司研發出 HS-239遙控滑翔炸彈，藉由無線電遙控，可由轟炸機投射遙控導引打擊8公里外的目標。而美軍在越戰時期投入 BQM-34A「火蜂」(fire bee)無人偵察機開始參與實戰，另外的重要分水嶺則是以色列在以阿戰爭期間以無人機進行更多作戰任務，藉由偵測、干擾等戰術手段，成功癱瘓埃及防空系統。至1991、2003兩次波灣戰爭，各級別無人機更涵蓋戰場高中低空的全空域運用，其後無人機首次擔任攻擊任務，搭配反戰車飛彈成功擊恐怖份子的高階人員，無人機的軍事用途與任務選項已大致齊備，所剩下的僅為道德、倫理的議題。

而前瞻未來 10 年，無人載具的運用將更為普及，且明顯的將由主要的偵察、觀測用途，轉為發展攻擊任務。在這些趨勢中，必須特別注意的是「微型無人載具」(Micro UAV)的發展與應用，不同一般認知的傳統飛機造型，微型無人載具是整合 MEMS (微機電系統) 科技的產物，類似微型感知器等模組元件的整合，應用於飛行主要是以積體電路整合的水平儀、高度計、磁場感測器、加速度計、微陀螺儀等，飛行控制系統中的微型空速計、微型舵機等。同時，在「微型無人載具」上搭載的微型攝影機、控制、影音傳遞所需的微型通訊系統等，都需要 MEMS 技術的支援，以減少體積和重量，改善飛行器的性能，同時其飛行構造除定翼、旋翼設定外，也可採用「拍翼」(flopping wings)設計，仿生物的飛行模式使其具備更靈活的飛行包絡線，可在複雜障礙物中穿梭飛行，得以在茂密的植被、建築等複雜空間中慢速而靈活的運作。且因體積甚小便於攜行，未來在成本降

¹⁷ Lucas Ward, "Former Defense Secretary Discusses Military Innovation," *The Harvard Crimson*, <http://www.thecrimson.com/article/2017/3/29/ash-carter-military-innovation-talk/>。

低後可以大量佈署，具有極高的戰術運用彈性，降低士兵傷亡風險。¹⁸承平時且可肆應救災、複雜管線等基礎設施檢查等非軍事任務的應用，可說極具價值。

自駕科技或自主控制的無人載具，其技術的整合已逐漸成熟。台灣的起步較晚，但已有企業投資「光達」(LIDAR)的技術發展，並力圖降價的同時使其輕量化、小型化，加上前述的影像科技整合，使台灣有極佳的發展潛力。在無人機的自主控制方面，技術面的評估目前仍以美軍的 X-47系列為代表性系統，其機電與飛操系統的整合，可使其在狹小且起伏的航艦甲板精準降落。而地面載具方面，則是以歷經大量實際道路里程行駛的美方企業所研發之自主駕駛車輛最成熟，事實上，由於地景環境與障礙物較複雜、且其他活動物件也造成干擾，因此地面自駕科技的難度往往高於無人飛行器。一般來說，此類自主無人載具，需整合各種感測器、控制元件、決策系統，在無外界人為資訊輸入和控制的情況，可以自主判斷、並獨立完成特定任務。其主要運用的科技包括視覺/雷射測量系統、決策支援系統，依照所在環境、以及自身的姿態進行高速運算，並即時回饋，以對應動態環境變化，包括各類隨機出現的障礙物如其他車輛、人員、動物等。

特別的是，此種自主控制能力不僅可用於避開碰撞，相對也可使其進行「有計劃的協調碰撞」，也就是群組 (swarming) 行動以完成任務。此一運用更進一步結合人工智慧、以及「物聯網」(Internet of Things, IOT) 技術，可令複數的自主控制物件相互交換資訊，意即是多個無人載具、或機器人可以在無人操控狀態下同時採取組織性的行動。在此一系統性的組織行動中，它們彼此間必須避免相互碰撞，又必須彼此協調，以合作方式達成任務，更進一步是，此一技術可對人員、車隊、船隊等集合式目標，進行協調性的分別攻擊，此種特性與動物或昆蟲的集群攻擊相當類似，例如狼群、蜂群、蟻群等，這類特性讓智慧載具在戰區或救援勤務中尤其具有價值，SWARM 控制技術也為 DARPA 列為研發專案之一。¹⁹

(六) 步行機器載具

台灣已有成功開發外骨骼(exoskeleton)載具的資訊科技業者、以及動力電池的正極材料產業，這都給步行機器載具的發展打下良好根基。廣義的機器人在製造業為主的生產線早已成熟運用，並逐步滲透服務業的第一線，包括旅館、車站、甚至航站等擔任詢問服務的輔助角色。另一方面，機器人也已漸次加入戰場，逐漸成為武裝部隊的生力軍，最常見的為爆裂物處理裝備，以降低人員處理的風險。同時，這對少子化、高齡化的個先進國家而言，可說是關鍵科技。

而在戰場上的運用，預估先是擔任各類輔助勤務，例如偵察搜索，以降低士兵遭到伏擊的風險，之後則可能攜掛武器以執行攻擊任務，正式加入戰鬥序列。若狹義之定義，仿生機器人 (Biomorphic robotics) 是指模仿動物手足行動的機器系統，或可稱為「步行機器載具」，其結合機械設計、環境感知、姿態感知器、

¹⁸ 蘇紫雲，〈機器人戰爭來臨，台灣務缺席〉，《新社會政策》，2014年35期，頁48。

¹⁹ “OFFensive Swarm Enabled Tactics (OFFSET),” DARPA, February 15, 2017, https://www.fbo.gov/index?s=opportunity&mode=form&id=01149a8a61316a0f94d92088157b3c89&tab=core&_cview=0。

電力控制等精密技術。由於採用足肢步行系統，可以克服地形障礙，降低戰場空間的限制，使其戰術運用彈性發揮到最大。

具里程碑意義的是 2014 年 8 月的環太平洋軍演 (Rim of Pacific 2014)，運載用的步行機器首次加入軍事演習，²⁰最具代表性的應是「仿生機器驢」(robotic mule) 正式與美軍陸戰隊地面部隊編組測試，此一機器驢作為後勤補給使用，伴隨步兵單位運動可克服 80% 的地形，其表現令參與評估的官兵感到滿意。²¹但目前主要的限制是電池儲能技術使其續航力受限，若搭載內燃機發電操作則噪音過大，使其戰場投入的時間推延。但此類仿生機器人除在戰場應用外，相同的技術更可用於工業、防救災、乃至於醫療、老年照護的用途，可說是極具潛力的軍民兩用技術，市場發展潛力不容小覷。進一步觀察全球機器人科技居領導地位的美國及日本，發展側略可分為兩大領域，一是戶外耐候、可負重、具高度障礙克服性能為主的美國機器人產業，著重戰場與工業場所的運用，而日本機器人產業的設計概念則趨向細緻、靈巧取向，更適合作為精細勞力的輔助，例如前述的醫療照護、服務業的應用。而現階段最接近市場化的以美國 Boston Dynamic 公司的系列原型產品，可以靈巧的搬運、上下樓層、甚至跳躍等方式避開障礙物，期推出的 Spot 四足機械人已實際投入日本市場測試，擔任建築工地的安全巡邏警戒。²²預估未來 10 年內，類似的步行機器在電池技術更為成熟後將正式編入武裝部隊。



圖 7-2、具備高度運動能力的軍用仿生機器人原型

資料來源：Boston Dynamics。

(七) 防衛型定向能武器

台灣的雷射科技研發與應用實力堅強，包括前述的立體列印（光雕）也是

²⁰ <中國軍方派四艦艇參加「環太平洋」聯合軍演>，《BBC 中文網》，2014 年 6 月 9 日，
http://www.bbc.co.uk/zhongwen/trad/china/2014/06/140609_china_army_us.shtml。

²¹ Sara Dietz, “Meeting LS3,” *Hawaii Marine*. July 18, 2014, Vol. 45, No. 29, A5. 另見蘇紫雲，〈機器人戰爭來臨，台灣務缺席〉，前揭書，頁 47-48。

²² Eric Chan, <Spot 四足機器犬在工地上班的情況>，《engadget》，2018 年 10 月 12 日。
<https://chinese.engadget.com/2018/10/12/boston-dynamics-spot-construction-demo/>。

雷射的應用之一，若能強化雷射源研發以及避免重複投資，或將成為台灣國防裝備的明日之星。先進國家定向能武器（direct energy weapon）的原型已臻於成熟，主要是指高能雷射、微波、乃至音波等能量的運用，將其集中於一定方向，使目標產生高溫、輻射、或共振而造成物理性破壞。目前仍以美軍居於領先地位，除空載雷射外，實際上已在海軍「彭斯」號（Ponce）運輸艦進行測試性佈署。進一步分析此類武器的最大優點，是其能量以接近光速前進（不含音波武器），因此在有效射程範圍內，敵意目標的偵獲與擊滅幾乎沒有時間差，這將創造出極大的戰術價值，傳統的偵測系統與火控電腦的解算能力相對可以增加，也就意味著接戰能力的增加。缺點則是受到物理限制，其發出的光電能量易受大氣遮蔽、濕度的折射影響，能量擊中目標的穿透力將減損。同時，現階段發射所需的消耗電力龐大、等同發射間隔較大，連續射擊的能力受到制約。

然而，在超級電容、電池技術快速進步後，未來在戰場佈署的實用性將趨於完善。預估此類武器在未來戰場的主要用途，以擔任飛彈防禦的潛力最大，除可發揮以快制快的優勢外，更在於來襲的彈道飛彈，其彈道屬高拋射角，因此接戰系統的動作屬於海平面與大氣層垂直面攔截特性，可避開地球曲面的物理制約，此一高射角的戰術特性可使定向能武器得到最佳的性能發揮，並使得濕度、大氣折射的影響減到最低。同時，能量武器光速前進的物理特性使得各式高速彈道飛彈的終端速度失去突穿優勢，甚至所謂的極音速載具也相對成為「慢速」，因此定向能武器在飛彈防禦的應用具有極佳的戰術乃至戰略價值，值得遭受大量飛彈威脅的國家評估發展。



圖 7-3、配置於龐斯號上的雷射武器

資料來源：US Navy。

(八) 匿蹤與主動防護科技

匿蹤科技雖早已應用，但隨著科技的改善，台灣的利基在於結合紡織與複材技術，特別是地面載具、裝具的應用，可結合地形地物增加匿蹤效果，因此應用層面仍在持續擴大，且具有高度發展潛力。在民間方面，大量使用的隔熱塗料、

電輻射遮蔽/能量吸收就是匿蹤技術的基礎。而在軍事上，最早的匿蹤技術是可見光的「迷彩」塗裝，而大規模運用首見於一次大戰的海軍，將船體的幾何外型藉明暗線條組合，用以迷惑攻擊者的測向以及測距，降低火炮、魚雷的命中率。其後在 1940 年代開始出現的電子匿蹤應用，則是著重降低、干擾雷達反射，以減少被發現的機率、或被偵測的距離，實務運用包括潛艦呼吸管設計、鋁箔薄條、電波干擾等手段。簡單說，匿蹤科技可歸納為兩大類，可見光與不可見光的電磁頻譜。在可預見的未來 10 年，光學頻譜的匿蹤科技，可見光部分主要是隱形披風(invisible uniform)，其原理為折射周邊光線，使欲隱蔽的目標呈現模擬的「透明」效果，²³另一可能的應用方式則是結合可變顯示薄膜，或塗料覆蓋在被保護目標物的表面，使其可用電力改變色彩，以適應戰場環境的改變。而電磁頻譜的隱蔽，目前主要運用於戰機、船艦，藉由外型設計讓雷達回波偏向、並同時用電磁吸收材料消耗、吸收電磁波的能量，以降低雷達回波。相對必須注意的是，面對新式「低頻雷達」(lower-frequency, directed anti-stealth radar)，則可能降低其匿蹤效果。電磁頻譜的隱匿，未來主要著眼在材料科學的進步，以作為匿蹤科技的核心。例如「主動選頻表材」(Active Frequency Selecting Surface, AFSS)，可適應廣域電磁頻譜的特性，將是未來匿蹤科技的潛力技術之一。²⁴

藉由射頻技術以電波偵測來襲射彈並予以攔截的主動防護科技，目前主要用於海軍艦艇，包括各類防空、近迫武器系統，用以攔截來襲的飛彈。台灣目前也發展出船用的近迫防衛系統，至於空軍戰機與陸軍載具則依賴各種主被動的干擾技術，原因除造價昂貴外，主要的挑戰在於主動攔截裝備需具備精準的偵測、火控雷達，其重量難以配置於航空器、地面車輛。²⁵

但隨著電子元件的進步，主動反制系統的總體夠行在體積與重量已經大為縮小，此一趨勢使地面車輛也有機會可以應用相關技術，以有效攔截來襲的目標。值得注意的是，即使防護力強大的主戰車，也陸續採用此一科技，以增加在城鎮、複雜地形等近接作戰中的存活能力。例如目前較成熟的車載主動防護科技，可使作戰車輛在傳統的被動防護能力包括裝甲、偽裝、遮蔽煙幕等防護手段外，增加更進一步的防護能力，包括以色列的「聖杯」(trophy)型車載主動防護系統可偵測來襲的射彈，並予以擊落或引爆，衍生型也應用於美國 M1 戰車。俄國則推出的「阿富汗石」(Afghanit)車載主動攔截系統等，其主要功能都是用以反制反戰車飛彈、火箭的攻擊，並大幅提昇主裝甲的防護效果。

由於其可跳脫傳統裝甲防護的重量與雜動力的兩難課題，徹底擺脫戰車與反戰車的軍備競賽困境，因此未來可能大幅應用於地面主戰車，甚至可使各類輕裝車輛得到等同以往重裝甲的防護能力，大幅增加戰場存活率。

²³ 目前最具代表性的產品，為加拿大 Hyper Stealth 公司所提出的原型。

²⁴ Collin Jeffrey, "New stealth material could defeat latest radar systems," *New Atlas*, November 3, 2015, <http://newatlas.com/stealth-material-radar-systems/40380/>。

²⁵ 大型航空器，仍有搭載主動防禦系統的實例，例如 B52 轟炸機早期型，於機尾搭載雷達控制的機砲，用於防護。並曾於越戰時創下擊落米格機的紀錄。

參、強化科技安全管理

一、中國規格威脅民主國家

「中國製造 2025」的核心理念，是中國產業升級與轉型，脫離廉價代工的產業結構。深入分析其目的是讓「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，主因為規格的專利若具效能優勢與壟斷性，則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。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。

中國對此自不會放過，只不過這多屬於戰術性質。戰略性質的網路戰，則從承平時就開始佈局，藉由植入後門程式、木馬等軟體做為，到就由工業、商業流程在對手國硬體植入晶片，平時休眠，戰時啟動。中國資訊、手機大廠之一的「中興手機」，便被發現銷往美國的 Score 型智慧手機暗中植入後門。²⁶早在 2013 年 2 月美國麥迪安網路安全公司（Mandiant Corporation）發佈報告，總結 141 個主要駭客攻擊的反跟蹤分析，辨識出位於其實際地理位置是駐紮在上海的一座大樓的「六一三九八」部隊，²⁷隸屬於總參謀部三部二局。²⁸此凸顯國家整體研發與生產供應鏈的重要性，應建立機制由源頭進行風險評估與管控。

二、科技的擴散與穿透

2011 年突尼西亞爆發「茉莉花革命」(Jasmine Revolution)，²⁹並引發後續埃及、利比亞等國一連串的武裝革命運動，就是透過網路社群串連，因此又被稱為「推特革命」(Twitter Revolution)或「社群網站革命」(Social Network Revolution)。可見網路具備獨力推翻主體國家的潛力工具，在軍事意義上就如同空權獨力擊敗南斯拉夫一般。

這主要是科技的穿透性。新的科技同樣可用於舊載具，使其發揮新的作戰效益。在以往，這類改裝主要是以機械性能為主，且每一型式的載具都有獨特性，例如單一機種機械性能的提升、零組件無法用於另一機種，電子裝備受限於尺寸、重量也可能無法用於另一機種。但未來由於電子裝備微型化，其可能適配的載具將更加自由，類似「隨插即用」(plug-in)的特性。反應在戰場上，將出現類似「舊瓶裝新酒」，舊式載具卻具備全新作戰能力的面貌，兵力的質量與數量此一

²⁶ <中興手機出包 A+H 股跌>，《世界新聞》，2012 年 5 月 22 日。

²⁷ <《紐約時報》：中國軍方是黑客襲擊者>，《BBC 中文網》，2013 年 2 月 19 日，

http://www.bbc.co.uk/zhongwen/trad/press_review/2013/02/130219_china_hacking_report.shtml。

²⁸ <共軍網路駭客、總參三部二局>，《中央社》，2013 年 2 月 20 日。

²⁹ "Tunisia's 'Jasmine Revolution' jolts Arab world," *AFP*, January 15, 2011.

老問題，可能將向質量方向傾斜。

由於技術擴散，非正規軍在都市、山區、叢林等地形也可能擁有高強度的戰力。此種由國家支持的武裝勢力，也可能配合正規軍事行動，被美軍認定為「複合戰爭」(hybrid war)，³⁰「混雜著傳統作戰、武裝反叛勢力、以及網路攻擊」。³¹實際上，未來除了正規戰場外，非正規軍事力量可能混雜的部分高科技裝備，將使以往的游擊隊武力升級，這也是軍民兩用科技所造成的另一後遺症。任何非正規軍力，都享有更大的自由發動突襲，這些被美軍描述為「高強度民兵」(potentially high densities of civilians)，³²的確會成為戰場的新勢力，混雜在平民之中極難對付。這也是德國國防部提倡「民-軍司令部」(civil-military headquarter)的主因，目的應該就在於藉民間部門的彈性，增加防衛的廣度與深度。

值得注意的是，由於國際製造業的垂直與水平整合，此種科技的穿透性也可能影響生產線與供應鏈。依照美國防部的說法，中國是美國製造業「偽劣電子元件」(counterfeit electronics)的最大來源，而台灣也名列第三大，這些元件不僅影響美國相關設備的安全，也常帶有「木馬」(Trojan)程式或病毒，滲透美國的軍用系統。³³此突顯我國工業與生產部門對零組件的安全控管仍有改善空間。

三、迅速彌補科技管制漏洞

美國「國家核能安全署」(National Nuclear Security Administration, NNSA)於2018年9月24日宣布，將建立類似「指紋技術」(fingerprinting technique)的方式，防止大規模毀滅武器 (weapons of mass destruction, WMD) 的設備與裝置流入非正確買家或戰略對手。

儘管美國有嚴格的敏感產品、軟體、技術(sensitive equipment, software and technology)出口管制，但仍存在許多漏洞。除了前述的利用偽造的空頭公司、掮客等方式外，尚有偽造「最終使用者」(end user)的方式騙取出口許可。同時，特別是來自中國對敏感科技研發的投資，往往令相關的技術出口變成管制的灰色地帶，造成國家利益的損失。

中國對其他國家的科技滲透極為嚴重，澳洲國安顧問包貝吉(Ross Babbage)也向澳洲政府提出警告，中國正向澳洲的大學研究室進行滲透，企圖以民用名義向中國出口量子(quantum)電腦、超視距雷達(或稱越地平線)等技術。³⁴這都造成敏感科技控管的漏洞。

³⁰ 複合戰爭，北約另稱「複合作戰」(Hybrid Warfare)，德國另稱「複合威脅」(Hybrid Threat)。

³¹ Helene Cooper, "The War of the Future? Picture Big Armies and Many Fronts," *The New York Times*, June 10, 2016, https://www.nytimes.com/2016/06/11/us/the-war-of-the-future-picture-big-armies-and-many-fronts.html?_r=0。

³² 同註 28。

³³ "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," US DoD, op. cit., pp. 28-9.

³⁴ Primose Riordan, "Naive Australia open to China's tech thieves, experts warn," *The Australian*, October 2, 2018, <https://goo.gl/shg5WY>。

舉例而言，美國核安署基於目前的稽核漏洞，透過學者、專家的產官學合作方式，計劃建立相關產品的完整資料庫，以利商務部、海關得以完整比對、追蹤產品流向，以確保兩用產品與技術的安全，同時得以使合法的貿易得以不受干擾的持續進行。具體作法為增加相關產品的相關辨識資料。例如用於測量鈾純度的「壓力計」產品，與測量汽車輪胎的胎壓計使用同一產品條碼，往往造成出口時的管制漏洞。但是兩者的價位、單批銷售數量差距達千倍，因此藉由多重資料的辨別，可有效讓出口查驗的標的更為精確，避免大量人力浪費且能有效防止管制品混雜出關。同時，美國也考慮動用「國家緊急法令」(National Emergency Law)禁止中國投資參與敏感科技的研發並取得相關科技。³⁵

小結

前述核生化管制案例，重點在於管制機制，由於涉及經濟競爭與國家安全，防堵中國科技滲透已成為西方國家的主要議題。台灣於前述的《美國防產業報告》中被列為「偽劣電子元件」的第三大供應商，加上具代表性產業的晶圓機台中毒事件，突顯我國在工業安全、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。

同樣重要的是，5G 通訊能力帶來的新價值將創造出新的經濟模式與產值，因此在前述的美國官方文件中皆提及相關通訊技術安全的重要性，並直接點名華為、中興等中國通訊廠商的安全威脅。因此，我國的「5G 國家隊」在面對美中為主的5G 規格競爭時，除價格外，更應考量價值，落實供應商管控、機房建置與防護、資料鏈內容防護等整體規劃並融入國家政策。避免成為「中國隊」的一員，危及國家安全並可能遭到民主國家市場排擠之風險。

台灣具有良好國防工業基礎，可以彌補部分供應鏈，與美國防產業具有互補與合作之機會。舉例而言 F-15、F-16、F-18等80年代設計/出廠的戰機與其他武器裝備，部分軍規晶片已停產，但台灣若干晶圓廠舊式8吋晶圓機台，可發揮其閒置的生產能力，可補充前述戰機全球數千架機隊的零件替換所需，特別是產量達4,500架左右的 F-16機隊。此可作為台美國防工業合作之選項，生產高價軍規晶片，並兼顧安全合作的雙贏效應。

相形之下，台灣具良好科技基礎可填補中國在市場空缺，關鍵在於落實敏感科技的管制，但產業界對科技保護的認知不足，甚至消極抵制的態度。與其溝通除以國家安全角度切入外，敘明科技研發本身除智財權外，並具有「公共性」需受管理，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其接受，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

³⁵ Dan Mangan, "US reportedly considers using existing emergency law to bar Chinese investment in sensitive tech," *CNBC*, March 27, 2018, <https://goo.gl/RWKvtR>。

場價值，建立包括資安防護的敵我意識、人員安全管理、以及實體防護等整體規劃，如此則可兼顧台灣國家安全與經濟的進一步發展。

結 論

蘇紫雲、曾怡碩

本報告系統性評估國防科技趨勢，分析台灣為因應威脅所需面臨的科技挑戰，並進而評估台灣本身條件及資源優劣勢後，辨識出台灣發展不對稱戰力之利基以及可足以形成局部優勢之科技發展項目。第一篇綜整主要國家軍事科技發展趨勢以及未來戰場特性，嵌合第二篇各項關鍵通用科技發展，進而在第三篇提出台灣面對挑戰暨建議因應措施。臚列台灣可投入發展之科技項目，並以戰略經濟及科技安全為考量，為台灣國防產業發展與國際合作方向，尋求明確的定位。以下將依序呈現系統性評估所產出的研究成果。

主要國家軍事科技發展趨勢與未來戰場特性

美國領導世界軍備發展潮流，除先進戰機、艦艇外，尚包括無人機、自動化科技、精準武器、飛彈防禦系統、情報、監視及偵察用電子裝備、各種動力及能源科技等等，並供應盟國武器裝備及技術，深度結合軍民兩用科技發展。俄羅斯師承過去蘇聯時代的軍事工業發展，在戰機、水面艦及潛艦、戰甲車、飛彈等有豐富發展經驗，雖然因經濟等因素限縮其軍事科技發展，但仍掌握部分優勢，特別是新式的地對地飛彈技術。中國過去依賴前蘇聯協助建立軍事工業基礎，近年仰賴經濟起飛，快速發展國防工業，但其模仿、剽竊智財權等行為受到美國等西方民主國家批評與防範。北約國家近年因高科技武器發展成本昂貴、技術風險高，因此多採國際合作方式，組成跨國軍事公司，或是由政府出面整合，採用相同標準，發展可供多國使用的共通化武器。

進一步來說，美國、中國、俄羅斯、北約雖擁有較豐富的國防資源，但都投入研發先進無人載具以及匿蹤戰機，以降低人員作戰風險。美國、中國與俄羅斯更積極發展極音速武器以及太空戰，美國與中國皆發展電磁武器。中國與俄羅斯傳統武器載台技術如飛機、水面艦等雖有創新概念，部分科技仍受限制，主戰裝備的效能尚無法挑戰美國，因此研發武器裝備的主要方向，在於創造不對稱優勢，如具備更精準導引與運動性能的新式彈道飛彈與巡弋飛彈，對美國及民主盟國造成挑戰。

實際上美國之所以能夠主導趨勢，除美國政府與國會持續以「風險投資」的觀念支持廠商研發，使新技術得以迅速投入部隊服役，國防產業也與非傳統國防夥伴聯合，將具潛力的商用技術導入軍事用途，並藉由新創公司、小型產業及矽谷產業聚落，加快科技創新的速度。美國更與盟邦進行科技合作，業界則在國外，尤其是歐洲國家尋找創意及靈感，強化創新及競爭力。北約國家的國防廠商也有跨國合作共識，單打獨鬥不僅要冒重大風險，且以歐陸國家規模，更難承擔其巨大發展成本，因此國防產業的跨國水平分工、垂直整合也成為

創新模式，但需要有完整的科技安全管理機制作為合作平台的基礎。

前瞻未來戰爭型態，將更趨多樣化、複雜化，一方面武器系統日益精準、效能提升，摧毀及殺傷面積更小，戰爭朝向小型、精準、「微創手術」的方向發展。另一方面，非殺傷式作戰，例如網路戰、輿論戰，破壞攸關國家政治秩序、社會運作、乃至人民日常生活的關鍵基礎設施等等非傳統戰法，則可能對國安與民生造成重大影響，間接影響國家軍事防衛的能力。而在作戰層級，各軍種的角色將大幅擴展，界限也日益模糊。由於戰爭型態多樣化，不僅武器系統、作戰編組也趨向彈性化，以模組化方式因應任務的不同需要。然而，除戰場上的短兵相接外，混合型的作戰模式，結合輿論、網路、心理、媒體、恐怖攻擊等等不同方式的非正規作戰，在高科技的時代，因資訊傳播的快速，反而更發揮其作用，也成為未來戰場作戰的特性之一。

軍備發展方面，非傳統式戰具如小型 UAV、自動化機器人等在作戰中的運用日益增加，不僅增進部隊情監偵、作戰與後勤等能力，敵方也可能在戰爭發起前，即以網路戰、電磁頻譜管控遮蔽等科技手段，使傳統戰具減少或失去其作戰效能。換言之，戰爭在大規模部隊動員、兵力集結前即已發起，前方和後方的傳統意義也不再存在。此也影響作戰概念的轉變，舉例來看，美軍「多領域作戰」主要概念是減少對空軍的依賴，強化對敵方打擊機、短程彈道飛彈及巡弋飛彈威脅的整合防空能力，在未來衝突中，地面部隊需有能力保護自己免受空中威脅。另外，在多領域作戰的構想下，各軍種都可能扮演主動角色以協助其他軍種。進一步說，多領域作戰概念將成為跨領域作戰，使傳統的軍種角色更具彈性。由於網路化作戰的發展，在最高指揮階層的統一指揮管制可能進一步聯合化、自動化，由聯戰指揮機制依其能力統籌調度指揮，並分配任務，各軍、兵種變成各種各類的武器載台與工具。

關鍵通用科技發展趨勢

在關鍵軍用科技發展方面，戰場機器人功能的多樣化，有些可能外觀像人類，有些可能體積小如昆蟲，海、陸、空、太空、網路五大領域的戰場機器人，該透過何種戰術控制系統來進行虛實跨境整合將成為一大考驗。讓機器人彼此之間能進行即時戰況交流、協助人機與多機協同作戰的「戰聯網」，正悄悄進入各國國防部的視野。在人工智慧的協助下，它們將如同集群式攻擊協同作戰的戰士。另一方面，由於科技含量與密集化，真實戰場指揮將與策略性電玩操作產生趨同現象，而在特定的作戰領域，電腦兵推的準確度也會大幅提升，對各國決策菁英之戰爭決策的影響層面將遠遠超越純軍事範疇。

在新的作戰工具方面，美國、俄羅斯、中國與歐洲國家目前在無人機領域上發展較為進步，甚至可用於集群攻擊。以美國而言，無人機技術雖仍居於領先地位，但實際面對同樣具備高度無人機技術及集群式攻擊能力的對手時，仍可能受到高強度威脅。因此就反制手段來說，若干國防大廠皆針對小型無人機的威脅進

行研究、提出能低成本的有效反制方案。除「硬殺」手段之外，透過各種干擾裝置切斷其與控制單元的訊號以對抗小型無人機的「軟殺」方法，亦是當前對抗無人機及集群式攻擊的重要方式。

此外，隨著資訊科技發展，量子科技現階段的運用主要在保密及運算，可用於強化通訊、偵測、衛星遙測能力，提升精準打擊效能，運用人工智慧可加快資訊處理速度，取代許多原本需由人力執行的工作，減輕人員負擔與成本。5G 網路通訊提升現有網路效能，增進資訊交換速度，虛擬實境則改變訓練方式，提高作戰效率。資訊科技領域的發展運用在軍事上，不但大幅提升武器系統的效能，也增進人與武器間的連結，強化操作武器及遂行作戰的節奏。

台灣面臨的科技挑戰與因應

中國在太空作戰、網路作戰以及網路輿論心理戰層面，對中華民國的區部制太空權、資訊安全與關鍵資訊基礎設施保護以及反制網路輿論心理戰，形成重大挑戰。台灣太空科技發展以科學研究為主，但具防衛的應用潛力，建構區部制太空權的相關科技，除基本衛星部署與遙測影像之外，也包含通訊傳輸的維持，未來將藉福衛七號初步建置通訊定位系統。而指揮管制部分，則包括衛星操控中心所建置的衛星操控系統，藉分析衛星下傳的 GPS 資料及地面站蒐集的天線追蹤數據，以掌握衛星的飛行動態，並進行衛星軌道轉換，已經成功地操控福衛一號、二號及三號衛星，初步具備基礎的衛星網。其他包括小型運載火箭、微衛星的製造與部署能力，將是我國極具潛力的發展選項。

在資安方面，國安會於 2018 年藉由發布《國家資通安全戰略報告》，將國軍界定在資安人才培育與資安產業發展的促進角色，並與其他政府部門一同參與國家資安聯防體系，對於資安風險診斷、關鍵資訊基礎設施保護及國際情報分享等，國軍參與的角色及途徑，仍待進一步定位。基於憲政體制的政軍分離原則，武裝部隊在平時需獲得授權，被動接受要求支援的情形之下，國軍可以秉持「超前部署，預置兵力」原則，參與平時資安聯防，發揮專業人力與設備能量，對關鍵資訊基礎設施實施資安風險診斷，俾利實現關鍵資訊基礎設施保護之數位國土防衛，進而實現與國際理念相近國家遂行國際資安聯防與情資交換，進一步合作組成資安虛擬聯防體系。

同時，我國與其他民主國家面對高強度的政治性的假消息與仇恨言論，必須謹慎處理，避免淪於政治不中立的疑慮。就此，相關單位宜參考美、日、歐盟等民主國家處理網路媒體假訊息之立法案例，結合第三方公正事實查核團體或個人，並輔以人工智慧技術發展，遂行假消息與仇恨言論之查察，俾利反制中國對台之輿論戰與心理戰。

台灣宜發展不對稱戰力與科技安全管理

在台海兩岸之間包含戰場地緣、中國軍隊高科技化的相對弱點，及台灣具備的技術能量等各種不同先天、後天條件之下，台灣確實擁有發展強大不對稱作戰

的優勢與利基。由於中國持續實施轟 6 或運 8 電戰機、以及遼寧號航艦編隊刻意繞行台灣周邊海空域、赴西太平洋訓練、或由東部通過，其海空作戰平台的進步使軍事行動選項大幅增加，台海天險不復存在，甚至對群山阻隔的東部也造成重大威脅。遼寧號航艦雖空中作戰能力有限，然其仍可藉攔 15 作戰半徑優勢，以其有限空優能力形成局部的艦隊防空網，掩護由中國內陸出海進入西太平洋之轟 6 轟炸機，投射反艦或攻陸飛彈，強化其對東部威脅的能力。

在各方面強化國防戰力的同時，不對稱作戰的原則應當成為整體軍事戰略的重要一環加以考量，並進一步結合戰史與未來科技進行研究、驗證及投資。台灣同時須強化關鍵設施及戰力保存、發展彈性化之無人及非傳統打擊能力。發展具備不對稱優勢之防衛能力，重點包括機動防空系統、強化制空制海戰力、確保地面戰力、電磁反制及資通安全、善用無人及智慧化系統。此外，可依資源投入選定優先順序，藉由研發多樣化無人與自動化載具、可攔截小型低空目標之彈性化火力與發射系統、網狀化作戰、彈性化的制空制海及制陸武器、網路戰與電磁武器、反制匿蹤空中武力發展，並發展自動化器械與人工智慧用於傳統軍備、智慧型水下攻擊武器及匿蹤技術，以取得局部科技優勢。最後，除了以各種新形態的作戰方式與領域等為主，並應著重於技術及戰術戰法領域的不對稱。除了承平時期的嚇阻之外，還包括真正面臨衝突時，其對台灣戰力的實際加乘效果，以不對稱的質量優勢，降低在數量居劣勢的風險。

特別須注意的是，防堵中國科技滲透已成為西方國家的主要議題。台灣於前述的《評估及強化美國國防工業基礎與供應鏈彈性》中，被列為「偽劣電子元件」的來源之一，加上具代表性產業的晶圓機台中毒事件以及晶圓業者竊密遭美方起訴等事件，突顯我國在產業安全、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，亟須法令以及新管理觀念的導入。這不僅攸關國家安全事宜，對國防產業的業者本身商譽與競爭力也是關鍵。

台灣的國防產業宜落實供應商管控、機房建置與防護、資料鏈內容防護等整體規劃並融入國家政策，避免因危及國家安全，而可能衍生遭民主國家排擠之市場風險。台灣具有良好國防產業基礎，除可與西方民主國家共同形成全球供應鏈，也與美國防產業具有互補與合作之機會。關鍵在於落實敏感科技的管制，但產業界對科技保護的認知不同，甚至有消極抵制的態度。建議與產業界溝通時，除國家安全角度切入，應敘明科技研發除智財權保護外，同時兼有「公共性」需受管理。此外，可以提供類似手機無線頻譜的分配、生物科技的倫理、基因科技的安全等實際案例，較易為產業界理解與接受。若同時輔以貿易戰的實質市場需要及誘因，對於讓產業界接受科技管理的必要性與市場價值，將更具說服力，進而建立包括資安防護的敵我意識、人員安全管理、以及實體防護等整體規劃。在顧及業者權益、公共性、市場前景的原則下，科技的管理將可產生正面效益，促進中華民國的國防安全與經濟的共同成長與發展。

