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術改革。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（Super-cooling）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 qbite、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 qbite 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%。[6]2018 年 3 月 Google 公布了 72 qbite 處理器「Bristlecone」，在位元總數上超越 2017 年 11 月 IBM 發表的 50 qbite 處理器，也勝過 2018 年 1 月 Intel 發表的 49qbite 處理器「Tangle Lake」。不過，能否其將其 9 qbite 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。

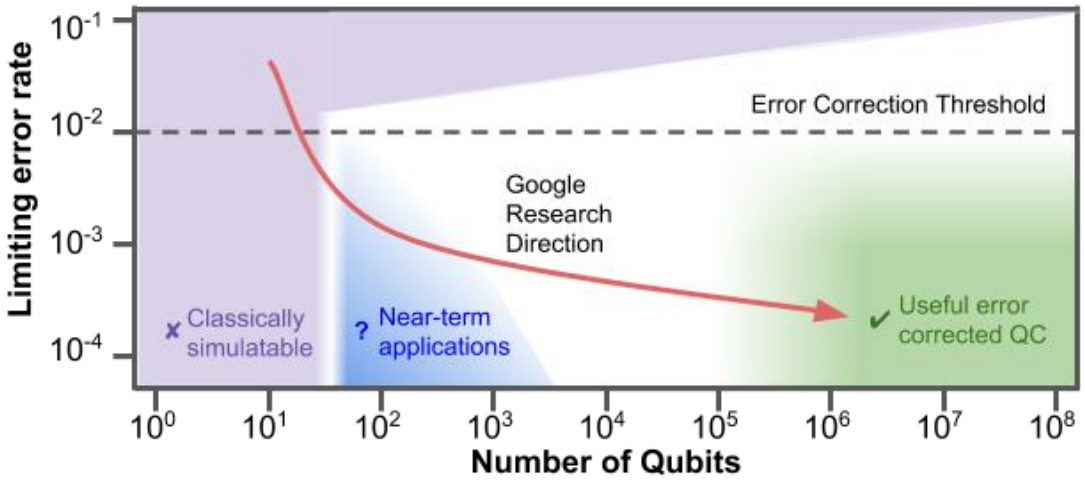

圖 4-1、量子位元與錯誤率之概念圖

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 81qbite、深度 40 層原子（9×9×40）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 10×10×35、11 × 11 × 31 以及 12 × 12 × 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,"*Goolge 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*, August6, 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. 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.bnext.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.cnbc.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] 曾靈，＜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.bnext.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 競賽中最重要的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 ErdalArikan 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-hauwei-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*, January13,2016, 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。