

行動通信導入國軍通資平臺之初探

作者／張堯銘中校

提要

- 一、國軍通資平臺戰時易遭敵鎖定破壞、且受限於無線電波方向性、機動中傳輸頻寬低及頻率資源等因素，使得國軍在作戰任務中易失去即時傳輸能力。
- 二、本文旨在探討民間行動通信最新技術發展與應用，運用涵蓋綿密且具可攜性及機動性高之民用行動網路系統作為國軍通資備援，並分析其可行性。
- 三、本研究運用各種既存網路公開資料、官方書籍及學者著作、專欄等，輔以政府部門的相關研究報告，研討各國發展現況，並比較及歸納國軍現有裝備介接整合能力及人力資源成本等指標，來確認行動通信可用度與支援度，並在通資安全政策規範的前提下，確保其通聯保密之要求，期未來能提供國軍決策者及相關單位在建構整合國軍行動通信平臺之參考。

關鍵詞：第五代行動通信、行動網路資安、混合實境

前言

因應通訊技術的快速發展，智慧型終端設備所開發的各項行動運用已大幅改變人們的生活習慣和工作，軍事單位亦隨此資訊潮流逐步改變內部資訊化作業方式，第五代行動通信技術(5G)是目前在市場上備受矚目的新一代行動無線寬頻技術，它可以讓服務供應商透過較為經濟的方式提供無線寬頻服務，並超越現今第四代(4G)無線網路的效能，帶來更優異的表現，未來的通訊產品能提供「超高頻寬」、「超大連結」及「超高可靠度與低延遲」之服務。

國軍目前通資平臺傳輸骨幹以資通電軍光纖固定站臺為主，並以機動性站臺如載微波機動車、無線電中繼臺、衛星系統及區域通信系統等為輔助通資備援，然上述通資平臺戰時易遭敵鎖定破壞，現有無線電波設備因傳波的方向性、機動中傳輸頻寬低及頻率資源等因素，使得國軍在作戰任務中失去即時傳輸能力而受限制，故瞭解民間行動通訊最新技術發展與應用，運用本島涵蓋綿密且具可攜性及機動性高之民間電信無線網路系統作為備援，來傳輸情報、監視、偵察等資料，通報戰場即時資訊、作戰指令、傷患救助、物資補充需求或敵軍戰場現況等研究，實為國軍發展之重要議題。

目前民營行動通信系統雖可提供即時數據傳輸與連網服務，但卻因業者考量成本，大量使用大陸製造產品，一旦運用民間與國軍網路系統介接，勢必衝擊到國軍資訊網路的實體安全，國軍運用行動網路始終是以資訊安全確保為優先考量，相關資安措施，必須更詳加擬訂。

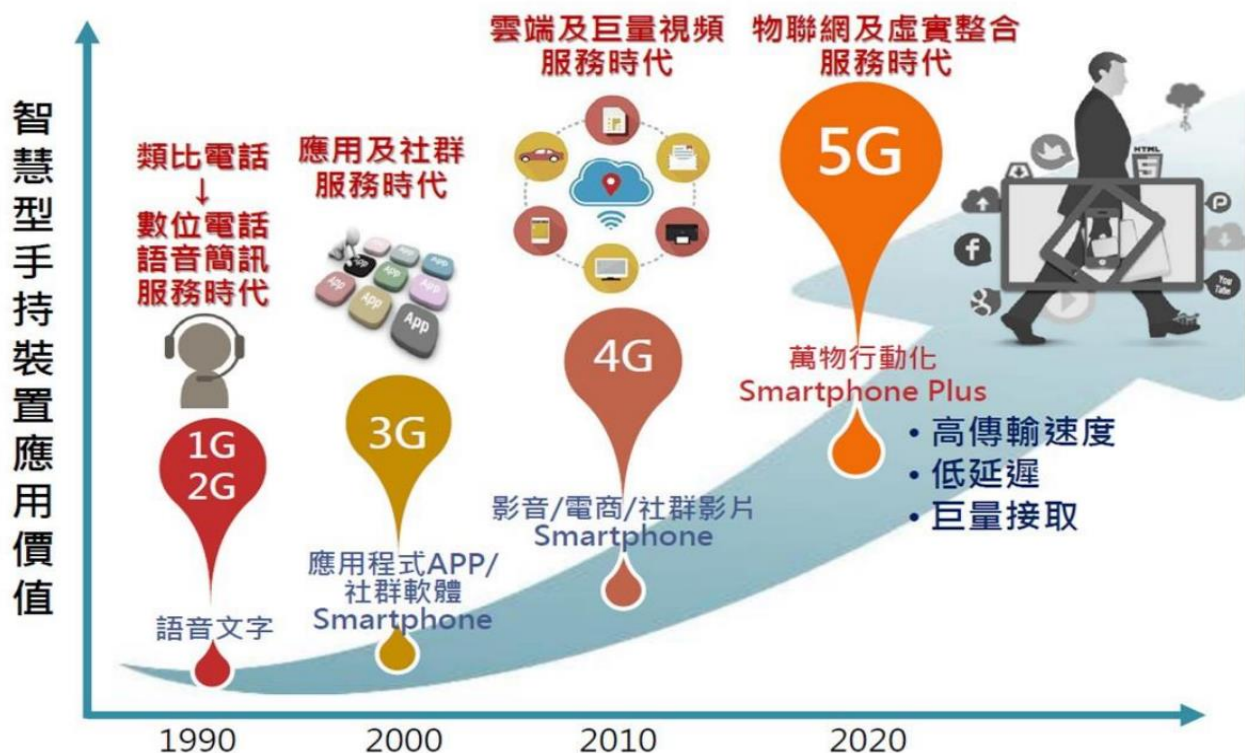
本研究分析國軍導人民間第五代行動通信後之可行性，以提供國軍運用新一代行動通信技術之參考。未來，將有可能進一步地發展具保密功能之軍用作戰雲端系統及個人可攜式智

慧型傳輸裝置，實現數位戰士概念之可能。

行動通信發展現況

行動通信從最初第一、二代(1G、2G)類比、語音簡訊之服務，經第三代(3G)應用程式及社群軟體等資訊運用發展，至第四代(4G)雲端影音巨量視頻服務，技術漸已成熟，多項應用通訊、社群及影音軟體廣為人們所用，為迎接物聯網及虛實整合服務快速發展，以及因應用戶更高資料量的傳輸需求，下一個世代(5G)的行動通信發展，必須解決頻寬及連網速度之問題，以滿足現今時代使用者運用需求(如附圖1)。

附圖1 各世代行動通信發展應用



資料來源：〈臺灣5G行動計畫(2019-2022年)〉《臺北：行政院，民國108年5月》，頁1。

第五代行動通信概述

一、5G意涵與優點

第五代行動通訊(5G)已於2020年進入全球商用階段，具備超高頻寬(Enhanced Mobile Broadband Access, eMBB)、超大連結(Massive Machine Type Communication, mMTC)、超高可靠度與低延遲(Ultra-Reliability and Low Latency Communication, uRLLC)等三大優良特性，除了可提供超寬頻無線上網服務外，還能帶動包括高品質視聽娛樂、智慧物聯網、智慧工廠、無人車、無人飛機、智慧城市等各種創新垂直應用的蓬勃發展，帶來龐大商機；5G國際標準技術規範已於2018年6月起陸續制訂完成，目前已成為世界各國的重點發展項目之一，包括美

國、日本、韓國、中國、歐洲各國等，都積極展開5G的技術研發及應用實證，除了希望藉此帶動產業發展、搶佔市場先機外，並希望5G能帶動各項創新應用服務、驅動產業創新升級，引導典範移轉及社會成長(如附圖2)。

附圖2 5G多樣化之應用服務



資料來源：〈臺灣5G行動計畫(2019-2022年)〉《臺北：行政院，民國108年5月》，頁2。

二、5G技術及頻譜運用

為了提供5G超高頻寬、超大連結、超高可靠度與低延遲的功能目標，技術面的挑戰包括新型調變編碼、多天線存取(Multiple-Input Multiple-Output)、毫米波傳輸、載波聚合(Carrier Aggregation)、新多址技術(New Multiple Access)、高密度組網(Highly Coordinated Ultra Dense Networks)、網路切片(Network Slicing)、邊緣運算(Edge Computing)、軟體定義網路(Software-Defined Networking, SDN)、網路功能虛擬化(Network Functions Virtualization, NFV)、控制承載分流(Bearer Offload Handling)及網路功能重構(Network Refactoring)等；隨著各國國際大廠積極投入研發，5G關鍵技術已有所突破，使5G成為可實現的網路系統。5G潛在商用頻譜大致可分為6GHz以下的中低頻頻段，以及6GHz以上的高頻毫米波頻段，6GHz以下中低頻頻段因其傳輸技術較為成熟、且涵蓋範圍較廣，是各國第一波釋出5G頻譜的重點，其中3300-4200MHz為國際上較具共識的釋出範圍；而因應5G超高速寬頻傳輸需求，6GHz以上的高頻頻段亦為5G頻譜的潛在開放標的，但因其傳輸與元件技術相對之下較不成熟，目前多處於技術研發或場域試驗的階段，各國高頻段5G頻譜釋出範圍參考(如附表1)。

三、5G資通安全需求

為全面發展5G資安防禦能量，政府自2018起已推動跨機關之分工合作，因應5G網路在開放架構及軟體層面將帶來新興資安威脅與挑戰，完成行動寬頻業務管理規則與系統審驗技術規範，以及資安議題法規整備工作；因5G網路將與4G網路共存共構一段時間，亦預先研析5G發展各階段可能面臨之資安議題。另一方面優先發展具產業需求的5G資安技術項目、並研議可實現之應用情境與商轉營運模式，滿足未來5G商用網路及特定5G場域垂直應用之需求。以精進5G資安技術、打造5G產品資安防護機制，並強化關鍵基礎設施及營運資安防護能力，帶動我國資安產業及資安檢測服務的發展。另外2018年11月訂頒「資安產業發展行動計畫(2018-2025)」聚焦於我國資安產業利基市場，透過資安人才培育、提供試煉場域及協助國際拓銷等策略，推升我國資安產業自主能量，未來亦將此行動計畫中循序推動5G資安產業發展。

5G可乘載未來智慧物聯多元應用服務，與人們的生活將更緊密結合，其資安的議題也更顯重要；與現有的4G網路相較，5G網路因其服務導向的系統架構及多元應用，更需要防範資安威脅所帶來的風險，例如5G接取網路與核心網路納入許多軟體功能模組或使用開源軟體，易受資安攻擊。為維持高速與低延遲性，部分應用伺服器會建置在接取網路邊緣，未受核心網路保護，亦容易受到攻擊。5G將帶動各種創新應用服務，並開放多種接取介面，資安防禦需往上延伸到應用領域，其所帶來新型態的資安威脅與挑戰，在安全、隱私及資安防禦面的重要性不言可喻。¹

附表1 世界各國5G頻譜規劃狀況

國家/地區	1GHz 以下 低頻段 (MHz)	1-6GHz 中頻段 (MHz)	6GHz 以上高頻段 (GHz)
美國		2500, 3500, 3700-4200	24.25-24.45, 24.75-25.25, 27.5-28.35, 37, 39, 47
英國		3410-3480, 3500-3580	
愛爾蘭		3410-3435, 3475-3800	
芬蘭		3410-3800	
德國		1920-1980, 2110-2170, 3400-3700, 3700-3800	26
義大利		3600-3800	26.5-27.5
西班牙	694-790	1452-1492, 3600-3800	
日本		3600-4100, 4500-4600, 4600-4900	27-28.2, 28.2-29.1, 29.1- 29.5
韓國		3420-3700	26.5-28.9
中國		3300-3600	24.25-27.5, 37-42.5
香港		3300-3400, 4830-4930	24.25-27.5, 27.5-28.35
新加坡		3400-3600	24.25-29.5

資料來源：〈臺灣5G行動計畫(2019-2022年)〉《臺北：行政院，民國108年5月》，頁4。

¹ 臺灣5G行動計畫(2019-2022年)〉《行政院108年5月10日院臺科會字第1080170031號函核定(台北)，2019，頁1、4、37、38。

國軍通資基礎架構

一、國軍通資基礎建設

國軍地面通資基礎傳輸設備主要有數位微波及光纖通信系統構連至本外島各基地，提供國軍各部隊語音、中繼、數據、專線、資訊、視訊、作戰情報指管等各類型通資電網路傳輸，其中除構建實體傳輸環路及無線微波多重備援保護外，並利用非同步傳輸模式交換設備(Asynchronous Transfer Mode, ATM)之SPVC(Soft Permanent Circuit)電路自動尋徑功能(Auto rerouting)提供系統傳輸多重保護運用，以建構成為全網路化(All IP Network)之通資傳輸骨幹。

二、國軍通資系統架構

(一)國軍電話交換網路

國軍電話交換機區分固定式數位電子式交換機及野戰數位式電話交換機，各交換機間與公眾電話網路及行動通信網路整合，提供了綿密通達的電話交換網，成為國軍主要行政通連方式，目前網路電話(Voice Over IP, VOIP)應用日趨普遍，國軍已依現行裝備壽期辦理新式IP化電話交換系統汰換作業。固定電話交換網路主要建置於固定營區，作戰部隊戰術指揮所使用之有線電話，以機動微波、展頻微波、無線電多波道、戰術區域通信系統或運用民營業者充沛的既設線路等方式，銜接至固定站臺或鄰近電話交換中心，構成穩定可靠之電話網路。

(二)國軍骨幹電路

未來將以「國軍通資系統網路」為骨幹，整合作戰區及國軍直屬機構等所需交換電路，規劃國軍通資網管中心、雲端交換中心及地區交換中心架構，以IP Trunk交換網路替代傳統TDM(Time-Division-Multiplexing，包含T1、E1、CO、EM)電路，降低彙接風險及電路頻寬浪費，增加電路資源彈性，並符合國際電信標準聯盟(ITU-T)所規範之新世代(Next Generation Network, NGN)電信網路架構，具有雲端服務、視訊會議系統、影像電話、網路電話等功能，以及行動辦公室及無線網路通話系統等擴充介面，提升下一代民用通信系統之備援整合能力。

(三)國軍資訊網路

國軍資訊網路建構在國軍通資傳輸骨幹網路上，主要是以ATM(Asynchronous Transfer Mode)交換器收容國軍各單位資訊區域、廣域網路交換器、路由器等，資訊網路依網路機敏性、用途等區分為：行政資訊網路、作戰指管網路、情監偵等專屬虛擬電路(Permanent Virtual Circuit, PVC)，網路間彼此是互相隔離，不得串接的，以確保資訊安全。國軍資訊網路以虛擬電路區分作戰指管類網路、機敏性網路、戰備類、一般行政類等資訊網路，各網均隔離運用，確保資傳安全，軍網無法支援處則以專屬公民營線路管控銜接國軍網路，另可結合機動通信裝備到達任務地後以網路介面搭接國軍骨幹網路。

三、國軍資訊安全政策

國防資訊系統網路之建置，以通資安全、經濟效益與作戰支援等原則為考量重點；亦就是除了傳統之軍用通資專屬系統外，另考量在安全無慮的情況下，運用民間的網路資源，配

合國軍通資系統的運作，以最有效的投資，滿足未來國軍在建軍備戰上的通資需求。目前國軍刻正研擬適法性問題調整相關政策，擴大運用民間通資資源，將民間通資資源及網路資安整體防禦納入戰時管制運用之具體方案，在有效利用國家資源的原則下，整合國軍與民間之通資資源。為因應未來中共對我可能實施之各類型資訊作戰，國軍資訊系統的發展，應以通資安全為首要之考量。也就是必須依據敵情威脅，整備通資系統之安全防護。因此，國軍在通資安全的技術研發、管制機能及教育訓練上，須前瞻規劃並分階段落實，以奠定通資安全基礎能量。目前國軍正結合國內產官學研各界，著手電腦網路防禦之相關研究與建置，希望在「主動防禦」的理念下，使敵無任何可乘之機。除了運用入侵我方電腦網路系統散播電腦病毒之「軟殺」手段外，國軍亦密切注意敵運用各種「硬殺」手段對我方指管機制所做之實體破壞。²

各國軍事行動通信發展應用

行動通訊目前已成為世界各國發展重點項目之一，包括中國、美國、日本、韓國、歐洲等國家，都積極開發相關技術及應用服務，相對於各國軍方，也都將其技術運用於各項軍事用途，以下就以與我國關係較密切之美軍及中共等國家，說明其行動通信發展應用情況：

一、共軍

(一)軍民融合戰略發展

中共軍方表示，5G 行動通信將改變未來戰爭形態，自曝外國使用華為產品的風險，5G 是中共的軍民融合戰略，難以排除中國企業在 5G 上被共軍「所用」，更將改變未來戰爭形態，無人偵察、無人駕駛、無人打擊等新作戰樣式的使用，都將依賴 5G 的超高速資訊傳輸。共軍的發言正好加強了其他國家對中國 5G 產品的安全疑慮。中國企業華為和中興通訊不僅是中國國內 5G 設備供應商，更可能是共軍 5G 設備的唯二供應商。同時，華為和中興也躋身全球提供 5G 基礎設施設備的主要公司。華盛頓智庫「美國新安全中心」技術和國家安全部門的兼職研究員卡尼亞(Elsa B. Kania)曾在「防衛一號」(DefenseOne)網站撰文說，對北京而言，5G 競爭一直與該國的「軍民融合」戰略有關。「5G 競爭已成為美中關係競爭的新前線」，「華為、中興等公司技術進步除了可以帶來經濟優勢，5G 的軍民雙重用途和軍事潛力更賦予其另一個地緣戰略意義，這也是中共軍事和國防工業正在熱衷探索的領域。」早在 2018 年 11 月，中國 5G 行業的主要參與者，包括中興、聯通和中國航天科工集團，就成立了 5G 技術軍民融合應用產業聯盟。夥伴關係旨在促進三方合作、發展 5G 的軍事和民用發展，同時促進 5G 的國防和商業應用。中國航天科工集團第一研究院特別關注 5G 在航空領域的應用。此外，中國的 5G 議程還跟國家和國防「資訊化」戰略聯繫在一起，包括中國軍隊發展 C4ISR(Command Control Communications Computers Intelligence Surveillance and

²林勤經，〈如何建構國軍完善通資體系與強化資訊戰能力〉，《第八屆國防管理學術季實務研討會論文》(台北)，2003，561-566頁。

Reconnaissance)能力，5G 快速及穩定的資訊傳輸，將改善戰場通信、提高資訊的及時性和整合性，除了應用於戰場上，如此迫不及待要步入 5G 時代，更是為了軍事效益，這種軍民融合技術使共軍從民用經濟和基礎設施中受益，可以提供比美國或其他潛在對手更顯著的資源優勢。³

(二)5G應用智慧化

5G 可以提供在軍事上發揮物聯網和人工智慧(Artificial Intelligence, AI)潛力所需的快速傳輸和頻寬，幫助實現軍事智慧化，中共軍方一直試圖提高人工智慧技術應用在軍事上的可能性，中共的 5G 進程和國防「信息化」戰略聯繫起來，包括共軍指揮自動化系統的能力，可通過更快、更穩定的信息傳輸，改善戰場通訊，增強信息的及時性和整合性，並提供快速傳輸和頻寬，將人工智慧技術應用於軍事領域，滿足戰場上實現網際網路和人工智慧的潛力，實現軍事智慧化。

(三)5G整合前瞻佈局

中共推動 5G 有助於軍事創新，在未來軍事競爭中勝出，以滿足未來作戰的資訊支援、強化資料分享、指管機制、增進系統架構等需求，迅速整合資訊與改良通信的潛能，提供戰場覺知的關鍵戰力；從中共意圖橫跨太空與陸基系統，建立整合資訊與通信架構的檢視，即看出 5G 的必要性。例如，中共整合 5G 和北斗衛星導航系統，以提升定位、導航與即時能力；在戰場外，5G 布局有助於中共的防衛動員，提供更智慧選項，協調資源和後勤支援，滿足戰時應變所需。中共未來推廣開發的 5G 技術標準，削弱全球競爭對手，推進科技戰略極權目標，而 5G 技術的發展也提高其未來的軍事優勢，尤其是世界各國對單一供應商的主要依賴，不僅增加對該供應商的潛在風險和後果，還加劇弱點或漏洞的潛在後果，威脅者可能利用的弱點，特別是在依賴關係存在高度風險的狀況。⁴

二、美軍

(一)軍規手機驗測與軟體發展

美國陸軍已測試 iPhone、Android 手機和平板電腦的作戰使用性能，於新墨西哥州的白沙導彈靶場(White Sands Missile Range)與德克薩斯州的布利斯堡(Fort Bliss)檢驗 iPhone、Android 手機和平板電腦的作戰性能。驗證這些設備是否能夠承受惡劣的沙漠氣候，透過這些設備的應用程式，可幫助部隊了解更多來自於戰場前線的數據，或是觀看遠方監視攝影機拍攝的實況視訊。其中一款名為「士兵之眼」(SoldierEyes)的應用程式，能夠將智慧型手機變成戰場導航儀器，不但能夠顯示電子地圖，甚至能夠透過設備的攝影鏡頭掃描地平線，然後銀幕上就會顯示數字符號，表示敵方目標在戰場上的方位與距離。而生物識別技術也可能被應

³ 〈5G將改變戰爭型態中共自曝華為隱患〉《大紀元》<http://www.epochtimes.com/b5/19/2/28/n11080193.htm/amp>，檢索日期：民國110年5月14日

⁴ 〈中共布局5G戰略威脅全球安全〉《青年日報兩岸論壇》<https://www.ydn.com.tw/news/newsInsidePage?chapterID=1231767&type=%E8%AB%96%E5%A3%87>，檢索日期：民國110年5月14日。

用，利用相片、指紋、視網膜掃描等來辨識伊拉克和阿富汗的可疑分子。這些設備都在幾百元美元的價格範圍內，比起專業器材動輒須耗費千元以上的高價位來說，相對較低成本。⁵

美海軍運用行動通信系統，作為艦艇內部、艦艇之間、艦艇至直昇機之行動寬頻通訊，並整合軍用無線電、無線網路及衛星通訊等，完成手持式機動部隊管制系統，提供應急救援、具備地理符號之白板、聊天及即時訊息等功能進行即時合作、協調與指揮所需共同圖像。

GD公司研發軍規智慧型手機(型號Itronix GD300)，安裝聯合戰鬥指管(Joint Battle Command-Platform, JBC-P)及整合戰術地面報告(Tactical Ground Reporting system, TIGR)等應用軟體，其中JBC-P已規劃為下一代旅級以下戰術指管系統(Force XXI Battle Command Brigade and Below, FBCB2)。另智慧型手機連接具戰士無線電波形(Soldier RadioWaveform, SRW)之聯合戰術無線電系統(Joint Tactical Radio System, JTRS)，並運用頭盔等穿戴裝置，透由行動通信傳輸平臺，可獲取戰場即時情資，進行遠距醫療等運用。(如附圖3、4)。⁶

附圖3 美軍智慧型手機軟體程式運用

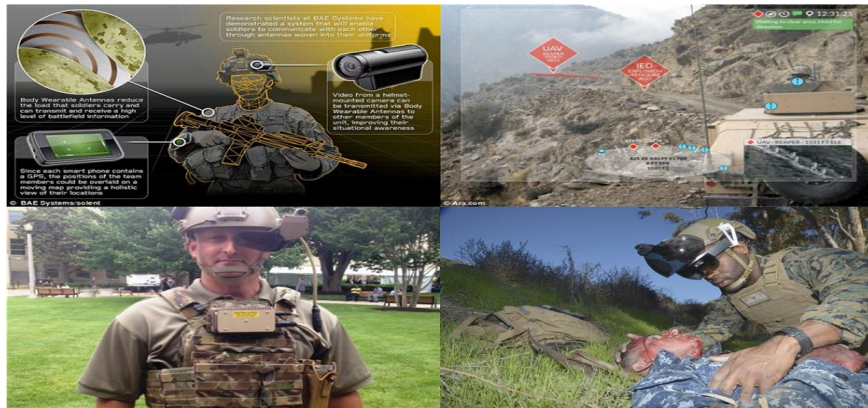


資料來源：〈Oceus Networks Demonstrates Proven Mobile 4G LTE Network at Army〉
《4G-Portal.com》，<http://4g-portal.com/>，檢索日期：民國110年1月28日。

⁵ iPhone參戰?美軍沙漠測試作戰性能〉《Newtalk新聞》<https://newtalk.tw/news/view/amp/2011-06-03/14899>，檢索日期：民國110年5月14日。

⁶ Advancing and integrating 4G LTE technology is a significant priority within the U.S Army programs <http://4g-portal.com/advancing-and-integrating-4g-lte-technology-is-a-significant-priority-within-the-u-s-army-programs>，檢索日期：民國110年1月28日。

附圖4 美軍視訊頭盔及軟體運用



資料來源：〈Oceus Networks Demonstrates Proven Mobile 4G LTE Network at Army〉，
《4G-Portal.com》，<http://4g-portal.com/>，檢索日期：民國110年1月28日。

(二)佈建行動網路雲端服務

美軍已開始運用智慧型行動裝置，平時以訓練或災防為主，戰時則可支援作戰任務；然而就軍方龐大且分散的資訊量來看，藉由雲端運算技術來重整資料中心(Data Center)外，亦可分散式儲存與運算巨量資料，因此雲端運算之重要性不言而喻，例如美國陸軍已從早期地面戰士(Land Warrior)至現在推展之網際戰士(Net Warrior)，均由訓練及準則司令部執行「戰士推向數位化應用(Connecting Soldiers Digital Application, CSDA)計畫」，充分運用智慧型手機及應用軟體。⁷

洛克希德馬汀公司研發「Monax 夜鷹行動通信系統」，協助美軍於阿富汗境外戰場佈建移動式基地臺，可運用智慧型手機之群組聊天功能，精確地進行火力協同射擊或回報需醫療後送之確切位置，並利用照相或攝影功能，將戰場實況立即回傳給指揮所。⁸

美國防部國防資訊系統局執行全球資訊網絡提昇計畫(GIG Convergence Master Plan, GCMP)，將雲端化(Cloud-based GIG)，規劃在非機敏與機敏防衛資訊系統網路上建置私有雲，以達成資訊共享之聯盟作戰及自動化目標；同時美國陸軍開始建置第二階段之專屬私有雲(Army Private Cloud, APC2)，屬一個地面作戰網，除降低應用程式植入與維護管理成本及整併現有資料中心之建置目標外，另採用可攜且軍規等級之行動資料中心，可強化大量資料蒐集、處理與儲存之資訊計算能力，提供所需支援及資訊安全。

美軍已將所有空中與陸地之情監偵情資，如無人飛行載具(Unmanned Aerial Vehicle, UAV)、聯合監偵目標攻擊雷達系統(Joint Surveillance and Target Attack Radar System, JSTARS)、電子情報(Electronic Intelligence, ELINT)等，匯集至戰鬥雲端，以提供戰場管理、目標資訊及搜救輔助等系統使用基於情資即時且直接傳送至戰場前線作戰單兵之需求，規劃建構移動型戰鬥雲端(Mobile Tactical Cloud)，系統組成包含智慧型行動裝置、專屬行動通訊戰鬥網、行動

⁷王岳吉，〈智慧型行動裝置軍用發展及安全〉，《陸軍通資半年刊第119期》(桃園)，102年4月。

⁸Advancing and integrating 4G LTE technology is a significant priority within the U.S Army programs <http://4g-portal.com/advancing-and-integrating-4g-lte-technology-is-a-ignificant-priority-within-the-u-s-army-pro-grams>，檢索日期：民國110年1月28日。

資料中心及衛星通訊系統等，透過行動運算、服務導向(Service-Oriented Architecture, SOA)運算與雲端運算等，提供隨需、即時、精確、高價值資訊的服務，包含計算與視覺分析、巨量資料處理、大量儲存空間及可擴充性等項目，將所有高耗運算資源的工作全部在雲端來計算，而非行動裝置，最後再將運算結果傳遞至行動裝置運用。⁹

(三)行動網路憑證安全

美國海軍透過公開金鑰基礎建設(Public Key Infrastructure, PKI)機制，運用共通存取智慧卡(Common Access Card, CAC)憑證作為智慧型手機連接至國防部專屬軟體商店「U.S. ARMY Marketplace」網頁之身分認證，下載獲得所需應用軟體，同時並對智慧型手機進行資安與資產檢測。另外智慧型手機透過行動寬頻通訊網，鏈結美國防部全球資訊網格(Global Information Grid, GIG)，可登錄作戰指揮中心之指管系統，查看地圖、傳遞作戰命令及戰地情報，並能讀取「掠食者」UAV 無人偵察機之即時偵蒐影像，供單兵情報運用。

(四)混合實境網路整合

美軍於 2020 年起，即運用微軟混合實境 Hololens 頭戴裝備開發各項訓練產品與課程，與波音公司透由 5G 行動通信分享器實施空軍各型機之維保課程，以提高維修人員實作課程時數，增加實作經驗；另亦將敵情、我軍部署狀況、氣候、地形、水文等資訊納入伺服器，依任務之不同調整相關參數，輔以頭戴式裝置顯像實施沙盤推演，俾磨練幹部指管能力；步槍射手亦透由 Hololens 頭戴裝置模擬作戰場景與敵目標，並由裝置顯示所提供之各參數實施射擊校正。(如附圖 5)

附圖5 美軍微軟混合實境Hololens頭戴裝備結合5G運用



資料來源：〈Optimising augmentation systems on the battlefield〉《軍備局詹氏年鑑》，
http://10.22.155.203:8081/Display/Viewer?id=fg_3203720-idr-2020，檢索日期：民國110年1月28日。

⁹A.R.Hartman, M.J.Beacken, D.J.Bishop, and K.L.Kelly, 〈4G LTE Wireless Solutions for DoD System〉, IEEE., 2014, P1-10。

國軍行動通信發展願景與建議

一、發展願景

國軍近年來在救災、通資備援等軍事運用上，行動通信已是不可或缺的工具，平時它能加速業務的聯繫協調，提升工作效率，並作為有線電網路的備援；戰時它能維持指管順暢，以利指揮部隊移動、掌握動態。國軍在未來數位化戰場，若能完全整合第五代行動通信，就能滿足C4ISR運作構想，達到戰力整合、靈活指揮、集中運用之目標。臺灣具有高科技資訊軟、硬體生產能力，且行動通信已有相當規模及成熟之技術，除供民眾平時使用外，若未適當導入軍事用途，實為可惜，尤其國軍經常仰賴國外軍購，關鍵技術受限於國外，造成本土技術人才流失，對於國軍未來建軍作戰影響甚鉅，本研究基於此理念，希望利用國內已有之行動通信技術資源，以最低成本之方式加以整合運用，轉換成國軍可用之通訊資源，充分發揮其可用價值，以下幾點為未來發展重點：

(一)軍事通信備援目前已有線電為主，無線電為輔，在可供備援之無線電資源有限之下，必須結合民間現有無線電行動網路資源，作為軍事通訊備援手段，而行動通信技術及資源，將是有利於國軍多重備援解決方案之一。

(二)固定式通信設施戰時容易遭受破壞，提高網路節點戰場存活率，建置可移動之無線電通信平臺，運用民間無線網路資源，結合民間固定及行動基地臺，可確保戰場存活率，維持國軍指管暢通。

(三)發展國軍雲端專屬科技及開發用戶端軟體APP，從政治戰略、軍事戰略與戰鬥角度，以及情報、作戰、訓練與後勤補給等方面研發相關軟、硬體，建構一個具戰場知覺、數據鏈路、資訊傳輸、敵我識別、導航定位、視訊會議、數位地圖、模式模擬與數據中心等雲端作業系統，創新未來作戰模式。

(四)以專線構接系統業者機房至國軍光纖資訊網路之間，先透過系統業者設定MDVPN(Mobile Data Virtual Private Network)安全群組，管控專屬SIM卡之IP位址、門號，可將智慧型行動裝置序號(如IMEI)與SIM卡序號(如IMSI)配對並加以綁定，以防止使用者更換私人SIM卡，以連接至網際網路。於智慧型行動裝置至資訊網路入口閘道端自行建立VPN(Virtual Private Network)安全通道，運用符合國際標準規範FIPS 140-2及國安局認證之保密裝備，並輔以資安防護機制，如PKI憑證及存取權限管控等，以確保傳輸及通信安全。

(五)國軍須先期培訓Android、IOS及雲端運算軟體開發人才，奠定指管系統雲端化之開發關鍵技術能量，並導入美軍DoDAF(Department of Defense Architecture Framework)分析模式，從作戰架構(Operational View, OV)、系統服務架構(Systems/Services View, SV)至技術架構(Technical Standards View, TV)，確實掌握作戰需求。

(六)為適應戰場環境需求，運用軍、工規等級智慧型行動裝置，以達防水(塵)、耐溫(摔)等功能，安裝自行研製之指管或災防應用軟體，結合其GPS、照相、數位羅盤及陀螺儀等感測功能，並機動架設專屬行動寬頻通訊戰鬥網，運用符合國際標準規範FIPS140-2及國安局認

證之保密裝備，確保戰時存活率及通信安全，以鏈結雲端架構下之虛擬化指管系統，可動態派送數位圖資，提供地面部隊所需偵蒐、導航、觀測、火協、災防、陸航及射擊輔助等功能。

(七)整體規劃智慧型行動裝置與雲端運算所需資安防護技術能量，如資安中央監控系統、應用軟體安全檢測及應用軟體商店管理等，確保資訊安全。

(八)配合我國政府行動裝置核心技術提升與「政府有感雲」雲端產業政策，在國防部通資電整體規劃下，依地面部隊作戰需求，完善「智慧型行動裝置結合戰鬥雲端」之軍用發展與安全，奠定軟硬體研製與系統整合等技術能量，建構國軍「小而精、小而強、小而巧」的現代化勁旅。¹⁰

(九)國軍考量資安政策及實體隔離安全，現行國軍與民營行動通信系統整合，仍以救災通資整備為主，運用智慧型手機、可攜式電腦及平板等用戶終端設備，透由中華電信基地臺設備，構成災防區之通聯，以肆應複合式災害防救任務，未來將視資訊安全管控強度，並參考各國建置發展情形，逐步建構國軍行動通信通資平臺，達成通資多重路徑、複式備援之通資要求。另國軍具軟體開發能力，未來配合行動通信終端設備，完成行政勤務管理、情資後傳、遠端監控、作戰指管、位置標定、後勤補保、醫療網路、資料加解密等相關軟體開發，俾發揮國軍行動通資平臺之最佳效益。¹¹

二、建議

因個人研究時間與知識有限，故本研究以探討國軍資訊網路銜接軍規或商規設備分析比較為主，國內各家業者刻正建置的行動寬頻網路，系統建置無法即期提出軍方相關服務，其系統網路及行動網路可否運用在國軍資訊網路，安全機制將是首當其衝的議題，國內民營行動寬頻網路建設，刻正大力建構，尤其國軍對資訊安全的重視與要求，民營業者網路透過VPN與MDVPN等技術，尚需搭配哪些資訊安全系統管控機制方可導入運用，可在往後依民營業者行動寬頻網路架構實際探討，並納入後續實際測試與驗證。

國軍現已全面開放使用智慧型手機，在通資安全基礎下，未來可參考美軍網際戰士，建立數位化國軍，以支援作戰、救災與駐地訓練，相關建議如后：

(一)在作戰運用部分：

為適應戰場環境需求，客製化開發軍規智慧型手機或平板，可達防水(塵)、耐溫、耐摔等功能，開發並安裝指管應用軟體，結合其GPS、照相、電子羅盤及陀螺儀等感測功能，並依地面部隊戰術位置或紅色海灘附近之高山站臺，機動架設專屬行動寬頻通訊網，如機動通信車及行動基地臺，確保訊號涵蓋範圍，並可自行掌握傳輸頻寬與安全，提供地面部隊偵察單兵、戰鬥單兵、前觀單兵、陸航部隊及射擊單兵所需偵蒐、導航、觀測、飛航及射擊輔助等功能；另以智慧型手機結合VHF手持式寬頻通信機，形成機動型數位化戰鬥網，透過地

¹⁰王岳吉、郭立言，〈次世代資通系統之軍用發展與安全－以智慧型行動裝置結合戰鬥雲端為例〉，《新新季刊第四十一卷第四期》(桃園)，2013年10月，52頁。

¹¹柯偉震博士，〈結合中華電信通資網路資源有效支援地面防衛作戰之具體作為〉(台北)，2019，2-33頁。

面網路介接 UAV 地面導控站，使智慧型手機可讀取 UAV 偵蒐即時影像，同步掌握 UAV 偵蒐情資，或運用智慧型手機遙控 UAV 與武裝機器人，減少人員傷亡。另運用平板或智慧型手機，採行動網路方式連結指管伺服器，顯示共同作戰圖像，遂行指管情傳作業，依現行民用電信無線安全防護技術，將資訊安全隔離作為納入考量，以海、空情擷取器，接收海、空情資，滿足共同圖像顯示功能。

(二)在災防運用部分

除智慧型手機之語音通話功能外，可安裝災防應用軟體，藉由內嵌第五代行動通訊系統能力，透過系統業者提供數據服務與連接網際網路功能，可連接行政院災防會或消防署災害防救中心等網頁，獲得各部會彙整之最新災情狀況，以提供國軍救災部隊即時掌握災情，另可將結合智慧型手機之 GPS、照相、電子羅盤及陀螺儀等感測功能，將救災部隊位置、即時影像回報至災害應變中心之數位地理圖資系統，供指揮官即時掌握部隊座標、災情與下達指管決策。

(三)在駐地訓練部分

智慧型手機或平板可結合穿戴式裝置，即時監控並紀錄官兵生理表徵與狀態，因人施訓提升訓練成效，並消弭危安因素。另可建置雲端數位教學平臺，運用智慧型手機多媒體影音播放功能，以裝備類 AR(Augmented Reality)虛擬實境軟體，實施數位化教學及電子化準則參考，減少紙本教材耗費，提供官兵自我進修工具，提升本職學能，後續若能結合第五代行動通信連網能力，獲取更多雲端服務，將發揮更多元化之效能與運用。(如附圖 6)

(四)其他建議事項：

1.第五代行動通信因頻率特性，穿透效應較差、對金屬建築、結構干擾及多路徑繞射、折射更嚴重，故更需分析計算基地臺涵蓋範圍，除運用現有基地臺架構，應以行動基地臺彌補涵蓋不佳地區，構成綿密之行動通信網。

2.依照國軍網路分級管理運用機制，作戰指管的機敏網路規劃運用軍規行動通訊設備，設置專用 VPN 之網路平臺，並加裝國安局認證之保密器，商規設備運用在一般行政網路，以貫徹現行資安政策。

3.野戰軍規寬頻傳輸設備規劃配賦應適度調整降低，以挹注地面主戰部隊(如戰略部隊、飛彈、戰砲甲車、電戰部隊等)或以各作戰區區域重點配置，以降低建置成本及頻譜資源有效運用，勤務支援部隊及後備動員部隊可考量建構開放頻段商規行動通訊設備及運用充沛民營業者系統網路資源。

4.考量國內頻譜資源運用與電磁環境日益複雜，國軍如建置軍規行動通訊設備，應儘速完成建案規劃與頻率需求規劃協調國家通訊傳播委員會(NCC)作業，並加強掌握國際及國家頻譜規劃運用政策，建立與國家通訊傳播委員會(NCC)頻譜管理運用協調機制，掌握國內頻譜規劃運用趨勢，適時將國軍系統規劃頻譜需求，納入整體頻率資源運用規劃。

5.配合政府推動行動通訊產業政策，將國軍軍規需求標準規範，委由中科院或國內生產製造商研發生產，一方面滿足國軍建置軍規專屬行動寬頻設備，又可扶植國內產業，提升產業國際行銷競爭力。

6.行動通訊商業設備的發展運用，可否導入國軍建軍備戰，國軍應就相關技術運用與發展適時研析評估，並訂定相關機制與規範。

7.國軍運用之資訊設備均為商業設備，相關軟硬體、系統與網路安全管制與防範作為，應明確訂頒俾利遵循，以兼顧安全與便利性。¹²(如附表 2)

附圖6 國軍智慧平板虛擬實境軟體教學運用



資料來源：作者自行製作。

¹²王岳吉，〈美國政府無線網路安全政策簡介、軍用無線網路安全發展〉，《資訊通信期刊》(桃園)，2005，12-15 頁。

附表2 行動通信導入國軍相關建議一覽表

作戰運用	規劃專屬行動寬頻網路備援，連結指管伺服器，顯示共同作戰圖像，提供地面部隊指管通情監偵能力；客製化軍規智慧型手機或平板，達防水(塵)、耐溫、耐摔等級，開發相關應用軟體，結合其GPS、照相、電子羅盤及陀螺儀等感測功能，另設置專用VPN之行動通信通資平臺，運用現有民用固定基地臺及行動基地臺架構彌補涵蓋不佳地區，構成綿密之行動通信網，提供部隊運用。
災防運用	連接災害防救中心網頁，獲得各部會彙整之最新災情狀況，以提供國軍救災部隊即時掌握災情，另可將結合智慧型手機之GPS、照相、電子羅盤及陀螺儀等感測功能，將前線救災部隊位置、即時影像等情資回報至災害應變中心之數位地理圖資系統，供指揮官即時掌握部隊座標、災情與下達決策。
駐地訓練	結合穿戴式裝置，即時監控並紀錄官兵生理狀態，因人施訓提升訓練成效，並消弭危安因素；建置雲端數位教學平臺，運用智慧型手機多媒體影音播放功能，以裝備類AR虛擬實境軟體，實施數位化教學及電子化準則參考，減少紙本教材耗費，並提供官兵自我進修工具及管道，提升本職學能。
其他建議	一、加裝國安局認證之保密器，貫徹現行資安政策。 二、勤務支援及後備動員部隊考量開放行動通訊設備運用。 三、與國家通訊傳播委員會(NCC)完成頻率作業需求及建案規劃。 四、掌握國際頻譜規劃運用趨勢，納入頻率資源整體運用。 五、配合政府行動通訊產業政策，規範國軍軍規需求研發生產。 六、適時研析評估相關技術運用與發展，並訂定相關機制與規範。 七、明確訂頒行動網路資安管制規範，兼顧安全與便利。

資料來源：作者自行整理

結論

近期美軍與共軍先後提出下一代軍事通訊手段，將以行動通訊技術為基礎，建構新一代網狀化網路，以肆應未來的戰爭型態，反觀國軍應結合政府政策，運用臺灣行動通訊產業鏈一體化之優勢，全力發展行動通訊無線寬頻網路，建構網狀化作戰模式之基礎，達到國防自主能力，進而深植全民國防理念。本文研討軍方有關裝備軍售投資建案之評估，以作戰需求為藍本，來建構通資指管架構，後續應考量其裝備系統能力、與國軍現有裝備介接整合之能力及人力資源成本等指標，來確認其建案可用度與支援度，以及其相關預算成本之估算，並在通資安全政策規範的前提下，確保其通聯保密之要求，期未來能提供國軍決策者及相關建置單位在建構國軍行動通信平臺之參考。

參考文獻

- 一、臺灣 5G 行動計畫(2019-2022 年)〉《行政院 108 年 5 月 10 日院臺科會字第 1080170031 號函核定(臺北)，2019。
- 二、林勤經，〈如何建構國軍完善通資體系與強化資訊戰能力〉，《第八屆國防管理學術季實務

研討會論文》(臺北)，2003。

- 三、王岳吉、郭立言，〈次世代資通系統之軍用發展與安全－以智慧型行動裝置結合戰鬥雲端為例〉，《新新季刊第四十一卷第四期》(桃園)，102 年 10 月。
- 四、柯偉震博士，〈結合中華電信通資網路資源有效支援地面防衛作戰之具體作為〉(臺北)，2019。
- 五、王岳吉，〈美國政府無線網路安全政策簡介、軍用無線網路安全發展〉，《資訊通信期刊》(桃園)，2005。
- 六、王岳吉，〈智慧型行動裝置軍用發展及安全〉，《陸軍通資半年刊第 119 期》(桃園)，2013。
- 七、〈iPhone 參戰?美軍沙漠測試作戰性能〉《Newtalk 新聞》<https://newtalk.tw/news/view/amp/2011-06-03/14899>，檢索日期：民國 110 年 5 月 14 日。
- 八、〈Optimising augmentation systems on the battlefield〉《軍備局詹氏年鑑》，http://10.22.155.203:8081/Display/Viewer?id=fg_3203720-idr-2020(檢索日期：民國 110 年 1 月 28 日)。
- 九、〈5G 將改變戰爭型態 中共自曝華為隱患〉《大紀元》<http://www.epochtimes.com/b5/19/2/28/n11080193.htm/amp>，(檢索日期：民國 110 年 5 月 14 日)。
- 十、〈中共布局 5G 戰略 威脅全球安全〉《青年日報兩岸論壇》<https://www.ydn.com.tw/news/newsInsidePage?chapterID=1231767&type=%E8%AB%96%E5%A3%87>，(檢索日期：民國 110 年 5 月 14 日)。
- 十一、Advancing and intergrating 4G LTE technology is a significant priority within the U. S Army programs<http://4g-portal.com/advancing-and-intergrating-4g-lte-technology-is-a-ignificant-priority-within-the-u-s-army-pro-grams/2021/1/28>。
- 十二、〈Oceus Networks Demonstrates Proven Mobile 4G LTE Network at Army，〉《4G-Portal.com》，<http://4g-portal.com/oceus-networks-demonstrates-proven-mobi-le-4g-lte-network-at-army/2021/1/28>。
- 十三、Advancing and intergrating 4G LTE technology is a significant priority within the U. S Army programs<http://4g-portal.com/advancing-and-intergrating-4g-lte-technology-is-a-ignificant-priority-within-the-u-s-army-pro-grams/2021/1/28>。
- 十四、A.R.Hartman，M.J.Beacken，D.J.Bishop，and K.L.Kelly，〈4G LTE Wireless Solutions forDoD System〉，IEEE.，2014，P1-10。

作者簡介

張堯銘中校，國防大學管理學院資訊管理碩士、空軍航空技術學院電子戰正規班。曾任連長、人事官、後參官、營參謀主任、通參官、電戰官、資參官、主任教官，現任陸軍通信電子資訊訓練中心網路作戰組組長。