數位發展部
Ministry of Digital Affairs

跨領域應用規劃計畫期末報告

計畫編號：Y111-F2

計畫期程：111/2/18-111/12/31

執行單位：財團法人工業技術研究院

版別：第3.0版

技資編號：521B10037

目錄

圖目錄

表目錄

壹、 計畫執行成果摘要

計畫名稱	跨領域應用規劃計畫 6G Industry development and advance planning Programme
計畫經費	36,000 仟元
計畫期程	111/2/18-111/12/31
執行成果摘要(中)	**1.研究緣起**：為布局我國 6G 自主技術能量，使臺灣成為全球主流系統重要策略夥伴，本計畫將先期投入 6G 產業發展規劃相關重要工作，除了通訊系統之外，相關的數位科技應用技術、標準、智財也是兵家必爭之地，其中又以人工智慧、資安隱私兩項數位科技應用最為關鍵，故將以涵蓋應用端以應用情境導向整合人工智慧應用與 6G 通訊特性，以及資安與隱私防護的需求，對未來 6G 商轉可能遭遇的問題與技術需求進行規劃與初期驗證。其中包含成立公部門連結小組，針對 6G 發展各項議題，進行跨部會協商與意見整合。 **2.計畫年度重點成果與建議：** (1)**通訊整合增強型人工智慧協作規劃**： A. 統整 6G 的需求指標 KPI 及能實現關鍵性能指標的必要技術，融合聯合學習與模型剪枝的技術來克服邊緣裝置計算效能不足問題。實驗結果顯示在修剪接近一半的參數量下，正確率幾乎與不修剪相同，符合預期成效。 B. 聯合學習將機器學習帶到網路邊緣運算，利用分散的資料集和參與者的計算資源來開發通用機器學習模型，解決資料通訊增加及損害資料隱私等問題，為 6G 網路應用中的關鍵技術。 C. 6G 大規模且複雜的移動網路將具有大量不同條件的異構設備(heterogeneous devices)，聯合學習除了要能布署在不同平台，還需設計同步機制使異質節點能共同參與訓練，並以 Class/Continue Incremental learning 的方式解決新增類別的問題。 (2)**安全可靠與受信賴的分散式運算規劃**： A. 探討以區塊鏈結合聯合學習在 6G 行動網路上建立一個安全可靠與受信賴的分散式運算環

境，允許在無信任關係的各方共享資料，保護用戶通訊的安全及隱私，運用區塊鏈建立各方平等且公開的信任關係，以保障平等且公開的信任。

B. 建立實驗環境測試，得出分散式運算環境所產生的延遲時間比傳統中央式的運算環境小，同時可維持原有效能。

C. 建議電信業者以區塊鏈結合聯合學習建立資料共享平台，讓用戶在可信任的環境下，以模型參數取代原始資料上傳平台並有相對報酬，而業者將有足夠的資料，建立 AI 決策工具以滿足 6G 關鍵效能指標，避免成為單純的傳輸管道。

(3)**跨領域應用情境研析**：

A. 彙整規劃各領域對 6G 環境預測之白皮書，以資安、人工智慧以及感知應用探討跨領域應用發展與技術方向，可提供政府將來規劃推動 6G 跨領域應用趨勢參考。

B. 國際上各單位對於 6G 環境下跨領域應用之建議及預測皆架構於資安、人工智慧以及感知應用三個面向的基礎技術之上，結合各種應用獨特應用技術，以建構各種新興網路服務。

C. 世界趨勢皆認為完善的資安是 6G 網路普及的基本條件，建議應建構所謂零信任基礎環境，相關應用也應考量資安需求，如以聯合學習建構具備個資防護的 AI 的應用，以提供兼具效能、安全及便利的網路服務。

(4)**6G 資安偵測與防護研析**：

A. 以 Open RAN 為參考架構對「Pre-6G Core Network, Pre-6GC」、「Pre-6th Generation Mobile Network, Pre-6G 開放式無線接取網路」、「假基地台」、「人工智慧與機器學習」等 4 種情境下的技術與威脅進行研析。

B. 可信任的 Pre-6G 網路軟硬體設備供應鏈管理以及對應資安防護，將是其資安技術發展最重要的關鍵議題。

C. 建議：為驗證開放式無線接取網路下基地臺產品開發的強健性與安全性，建議業者及早依潛在客戶需求導入產品資安確保標準、滲透測試、開源軟體元件分析及機器學習資料毒害等相關資安測試，以提升產品競爭力。

(5)**6G 網元及通訊資安檢測研析**：

A. 依照臺灣產業的發展與觀察，延伸「無人機」、「低軌衛星」、「遠距醫療」之 6G 應用，進行資安威脅與降低資安威脅方法做進一步的研析。

B. 6G 安全性和隱私性將延續採用 5G 網通環境特性，針對 5G/6G 仍持續發展的新興技術，如：AI/ML、區塊鏈等，大部分網路攻擊手法步驟大多相同，為偵搜、武裝、派送、弱點攻擊，在進入系統做提權操作或橫向感染，於 5G 存在的智慧化攻擊威脅，將在 6G 更加深入發揮。

C. 建議：產品與應用業者可搭配 MITRE ATT&CK 攻擊手法框架，透過對應情境規劃設計檢測工具，並藉由模擬完整攻擊鏈行為(如 UNC1945，電信 APT 攻擊等)跟驗證防禦機制，對未來 6G 場域進行驗測。

(6)**6G 跨產業資安聯防生態探索研究**：

A. 以「晶片資安」、「網路資安」、「應用結合專網與公網兩種情境」進行探索。並邀請 54 家公協會、電信產業、系統整合商/資安廠商進行訪談，整合產、學、研意見及提供之相關議題，擬定我國 6G 應用情境之未來發展方向。

B. 6G 發展技術將依 3GPP 等國際標準研提方向展開，並根據技術探索相關生態，其資安防護層面更加複雜與多元，單一產業或是業者的資安意識以及偵防手法將無法有效全面性保護，亟需採取多層次聯防措施。

C. 建議：依現有 5G/6G 相關產業生態，我國業者可在白牌伺服器及終端設備具備相對優勢，建議及早導入相關資安議題，如 6G 網路各節點介面設置資安防護機制、或終端設備導入

SSDLC 等建議作法，並加強跨產業體聯防意識，以協助我國廠商提升資安防護能力。

(7)**公部門連結小組**：

A. 完成籌組：111 年 8 月 23 日完成公部門連結小組籌備會議，分為「雛型系統與國際布局工作組」、「國際連結暨產業應用工作組」、「頻譜整備暨跨域發展工作組」及「部會合作與協調推進工作組」等 4 個工作組進行運作。

B. 協調連結：透過每季公部門連結小組會議的召開，對 6G 發展各項議題進行跨部會協商與意見整合，因應議題需求邀請相關專家顧問與會參與討論，做為跨部會及公私部門協調平台，以有效進行計畫滾動修正，並協助電信業者國際參與，促使政府政策與產業需求有效鏈結。

C. 持續推進：建議持續維運公部門連結小組，並建立資源共享平台，讓公部門相關計畫間的資訊更為通透，整合國內的能量，一起參與國際盛會，進而帶動新興應用服務及系統整合發展。

3.後續推動規劃：

(1)本計畫預計藉由探討 6G 在跨領域應用服務上的情境與需求，透過對照現有的 ICT 技術，並鏈結主計畫分項一的通訊技術研發，協助國內推動 6G 發展的技術儲備，跨領域應用在目前 6G 通訊系統的 KPI 中，並無直接對應的量化 KPI，如超大規模同時連網(10M 個/每平方公里)、超低功耗與成本(5G 的 1/10)等項目，但在如 Hexa-X 提到的與 5G 不同的人工智慧、資安與隱私、服務可用性與多樣化、分散式應用等新能力上(對應 D5.1 的規劃)，以及南韓納入的「可信賴、隨時資安」以及日本從 B5G 推進的未來人工智慧、超安全可信賴、分散式架構上，逐步探討可能的技術選項並進行評估與技術實證，預計在 2026 年 6G 標準制定前(本計畫執行至 2026)，達成上述相關的評估與規劃實證。

(2)預計 2023 始規劃具備零信任能力的服務架構技術，2024 可展延快速部署之跨領域應用服務，2025 達到受信賴且具備資安整合能力的服務架

	構，2026 實現未來 6G 跨領域應用的情境雛形展示。
執行成果摘要(英)	**1. General Background Information:** The programme first invests in important work related to 6G industry development planning, including communication systems, related technology application, artificial intelligence, security, privacy, standards, intellectual property rights, etc. We will introduce the integration of 6G, artificial intelligence, cyber security and privacy protection with application scenarios. Then plan and verify the problems and technical requirements that may be encountered in future 6G commercial use. At the same time, we sep up the Pre-6G Inter-ministerial Cooperation Working Group for cross-functional communication on 6G issues. **2. Key achievements of the Programme include:** **(1) The planning report for communication integrate enhanced artificial intelligence collaboration.** **A.** Summarize the necessary technologies to achieve 6G KPIs. Experimental results show that federated learning approach with pruning can find a desired model size that can achieve a similar prediction accuracy as the model without pruning and also solve the problem of insufficient computing power of edge device. The view was expressed that the expected accomplishments fully met the requirements. **B.** Federated Learning as a key technology for 6G. Federated learning allows the training of ML models on mobile edge networks from local data collected by edge devices while preserving data privacy and communication resources, which has wide applicability to various applications of machine leaning. **C.** 6G make the network more massive-scale, complex and heterogeneous. Federated learning will be deployed on different devices, and a synchronous communication mechanism needs to be designed for model training due to the

	heterogeneity devices. We will develop class/continue incremental learning in the FL field to learn new classes continually while maintaining knowledge on previous classes. **(2) Secure, reliable and trusted distributed computing planning reports.** **A.** We explore the method of integrating blockchain into FL to build a distributed model training and sharing platform, where distributed mobile devices execute local model training. a Blockchain-based, Zero-trust Security-enabled distributed computing to address user privacy and data provenance requirements. The proposed method also supports the requirements of 6G networks. **B.** The experimental results show that the distributed computing environment experience lower latency than a traditional centralized environment and can achieve a similar prediction performance. **C.** It is recommended that the service provider establish a data sharing platform by integrating blockchain and federated learning. The method can record and reward federated learning contributions with blockchain. Users can upload gradients instead of their privacy data. The service provider can get the data to build the AI models. The method can satisfy the 6G KPIs to improve the use of applications and related services over the internet **(3) Cross-domain application** **A.** Summarize the development and technical points of 6G white paper from different perspectives such as cyber security, AI and applications in machine perception. Such information would provide references to the Government to plan and promote 6G cross-domain application trends in the future. **B.** International organizations believe cyber security, AI and applications in machine perception are basic technologies of 6G. The integration of these 3 technologies to various applications can construct various emerging network services.

C. The popularization of 6g technology is based on perfect cyber security. Federated learning is an approach for collaborative computing services in a zero-trust environment. It is suggested that using federated learning for developing AI applications to provide network services that are both efficient, safe, and convenient.

(4) Study Report for 6G Threat Detection and Defense

A. Taking Open RAN as reference architecture, research in technology and threats in situations such as in Pre-6G Core Network, Pre-6G Open Radio Access Network, fake base station, AI and machine learning.

B. Trusted Pre-6G network software and hardware equipment supply chain management and corresponding cyber protection will be the most important key issues for Pre-6G development.

C. In order to enhance product competitiveness, it is recommended that service provider perform security testing such as penetration testing, open-source vulnerability and poisoning attack in machine learning and meet the information and cyber security standards to verify the robustness and security of O-RAN base stations.

(5) Study Report for 6G Network Element and Communication Cyber Security Detection

A. According to the Industrial Development in Taiwan, analyze the cyber security threats in the extend 6G applications such as drone, low-orbit satellite and telemedicine and methods to reduce security threats.

B. 6G security and privacy will presumably adopt many features from 5G. The cyber threats based on AI, ML and blockchain in 5G can lead to privilege escalation or horizontal infection through attack methods such as reconnaissance, weaponization, delivery, and exploitation. There would be constantly evolving and highly sophisticated cyber threats in 6G.

C. In order to build trust and security for 6G Networks, it is proposed to test the 6G application

	by using MITRE ATT&CK to build the test and verification tool and simulating an advanced persistent threat in information and communication systems. **(6) 6G cross-industry cybersecurity ecosystem exploration report** **A.** To give direction to Taiwan's future 6G development, we visite 54 associations, service provider, system integrators and cybersecurity companies and discuss the topics in chip security, network security, and combining application with private network and public network. **B.** The set of technology specifications that will eventually be known as 6G will begin to emerge in a 3GPP Release. There will be more security requirements and challenges of 6G technologies and applications. Related companies should adopt the multi-layered defense policy to improve cyber protection. **C.** In order to improve the cybersecurity capacity of related companies, it is proposed to set up protection mechanisms on each node of 6G network or implement the secure software development life cycle (SSDLC) approach to terminal equipment. **(7) Pre-6G Inter-ministerial Cooperation Working Group** **A.** We held a meeting of the Pre-6G Inter-ministerial Cooperation Working Group on 8/23/2022 to divide the group into 4 working group: prototype system and international arrangement working group, international connecting and application development working group, spectrum planning and cross-domain joint development working group and inter-ministry cooperation and 6 G promotion work Group. **B.** The Pre-6G Inter-ministerial Cooperation Working Group meets regularly to discuss issues and challenges from all aspects of 6G. We establish and support the service providers to participate in the topics for making the effective

	connection between government policy and industry needs. **C.** It is recommended to continue to maintain the Pre-6G Inter-ministerial Cooperation Working Group, so that the information between related projects in the public sector will be more transparent, thereby driving the development of emerging application services. **3. Follow-up:** **(1)** The programme is expected to support the country to promote the technical reserve of 6G development by discussing the situation and demand of 6G in cross-domain application services. There is no corresponding quantitative metric for cross-domain application in the KPI of the current 6G communication system. However, European Union, South Korean authorities and Japanese authorities promote future artificial intelligence, ultra-safe and reliable, and decentralized architecture. We will explore possible technical options and conduct evaluation and technical verification. It is expected that before the 6G standard is formulated in 2026 (this program will be implemented until 2026), the above-mentioned relevant evaluation and planning verification will be achieved. **(2)** In 2023, planning service architecture technology with zero trust. In 2024, cross-domain application services can be expanded and quickly deployed. In 2025, archiving a trusted service architecture with cyber security integration. In 2026, realizing the prototype of future 6G cross-domain application scenarios.
關鍵字(中)	跨領域應用；資安偵測防護；公部門連結小組
關鍵字(英)	Cross-domain application, Cyber Security for Threat Detection and Defense, Pre-6G Inter-ministerial Cooperation Working Group

貳、 計畫進度甘特圖及計畫查核點說明

本計畫規劃進度如表1甘特圖，查核點說明詳見表2，均已依規劃完成所有查核點。

表1、計畫進度甘特圖

月份 / 執行進度	1	2	3	4	5	6	7	8	9	10	11	12
一、跨領域應用規劃												
(一)應用情境研析與驗證												
A-1 ・通訊整合增強型人工智慧協作設計與驗證規劃 ・安全可靠與受信賴的分散式運算設計與驗證規劃												
A-2 ・通訊整合增強型人工智慧協作規劃 ・安全可靠與受信賴的分散式運算規劃 ・跨領域應用情境研析												
(二)資安偵測防護與推動												
A-3 ・6G 資安偵測與防護研析 ・6G 網元及通訊資安檢測研析 ・6G 跨產業資安聯防生態探索研究												

月份 / 執行進度	1	2	3	4	5	6	7	8	9	10	11	12
A-4 ・ 6G 資安偵測與防護研析 ・ 6G 網元及通訊資安檢測研析 ・ 6G 跨產業資安聯防生態探索研究								■	■	■	■	■
二、成立公部門連結小組												
B-1 公部門連結小組籌組							■	■				
B-2 公部門連結小組會議							■	■	■	■	■	■
進度百分比%	25%			50%			75%			100%		

資料來源：本計畫

表2、計畫查核點說明

查核點編號	預定完成期間	查核點概述	執行成果
A-1	111/09	1. 通訊整合增強型人工智慧協作設計與驗證規劃書 1 份 2. 安全可靠與受信賴的分散式運算設計與驗證規劃書 1 份	已於 9 月 30 日前完成「通訊整合增強型人工智慧(Artificial Intelligence, AI)協作設計與驗證規劃書」及「安全可靠與受信賴的分散式運算設計與驗證規劃書」各 1 份，達成情形說明如下： 1. 通訊整合增強型人工智慧協作設計與驗證規劃書：本規劃書首先統整 6G 的需求指標及能實現關鍵性能指標的必要技術，並彙總包括工業和研究機構在內的不同國家

查核點編號	預定完成期間	查核點概述	執行成果
			的研究活動；再來介紹聯合學習的基本概念、架構和相關技術，並探討聯合學習對 6G 應用的核心挑戰。最終藉由實驗設計與規劃，說明如何改進聯合學習技術，克服計算效能不足問題。 2. 安全可靠與受信賴的分散式運算設計與驗證規劃書：本規劃書首先統整各主要發展國家的 6G 要求指標，再對 Federated Learning(FL)及 BlockChained FL 進行全面的文獻調查，發現 FL 直接用於第六代行動通訊系統將有延遲，通訊成本及隱私方面的問題。最後，由系統整合的角度研究出區塊鏈（Blockchain，BC）整合到 FL 的方法來解決上述問題。
A-2	111/12	1. 通訊整合增強型人工智慧協作規劃報告 1 份 2. 安全可靠與受信賴的分散式運算規劃報告 1 份 3. 跨領域應用情境研析報告 1 份	已於 12 月 15 日完成「通訊整合增強型人工智慧協作規劃報告」、「安全可靠與受信賴的分散式運算規劃報告」、「跨領域應用情境研析報告」各 1 份，達成情形說明如下： 1. 通訊整合增強型人工智慧協作規劃報告：本報告首先統整 6G 的需求指標及能實現關鍵性能指標的必要技術，並彙總包括工業和研究機構

查核點編號	預定完成期間	查核點概述	執行成果
			在內的不同國家的研究活動；再來介紹聯合學習的基本概念、架構和相關技術，並探討聯合學習對 6G 應用的核心挑戰。融合聯合學習與模型剪枝的技術來克服邊緣裝置計算效能不足問題，藉此達成 6G 關鍵性能指標之一「超大規模同時連網」。實驗結果顯示在修剪接近一半的參數量下，正確率幾乎與不修剪相同，符合預期成效。 2. 安全可靠與受信賴的分散式運算規劃報告:AI 原生的 6G 行動網路需要用戶分享資料以建立更有效率的資源分配決策工具，滿足 6G 行動網路的需求，本計畫探討以區塊鏈結合聯合學習在 6G 行動網路上建立一個安全可靠與受信賴的分散式運算環境，允許在沒有預先建立信任關係的各方共享資料，可滿足 AI 技術需要大量資料訓練，另一方面也可保護用戶通訊的安全及隱私，並有機制可提供獎勵給分享資料的用戶。此環境以區塊鏈建立各方平等且公開的信任關係，用戶以聯合學習訓練本

查核點編號	預定完成期間	查核點概述	執行成果
			地資料，分享模型至區塊鏈並由區塊鏈得到獎勵，此流程的每個步驟都會記錄在區塊鏈，以保障平等且公開的信任。為此，計畫建立實驗環境測試，發現分散式運算環境所產生的延遲時間比傳統中央式的運算環境小，同時可維持原有效能。 3. 跨領域應用情境研析報告：面對未來 6G 在網路技術、應用的趨勢，本跨領域應用研析報告參酌世界各國研發單位及企業思考 6G 環境的可能性所發布之白皮書，整理、分析國際上對於 6G 環境下相關應用趨勢之見解，藉以觀察 6G 無線通訊技術發展，思考各種跨領域之應用情境，瞭解大部分意見認為 6G 網路應用環境中資安、人工智慧以及感知應用三個面向技術是跨領域應用的重要基礎，未來應是三種技術交互融合，建構兼具效能、安全及便利的網路服務，此部分發現期可提供政府將來規劃推動 6G 跨領域應用趨勢參考。
A-3	111/09	1. 6G 資安偵測與防護研析期中	已於 9 月 30 日前完成「6G 資安偵測與防護研析期中報告」、

查核點編號	預定完成期間	查核點概述	執行成果
		報告 1 份 2. 6G 網元及通訊資安檢測研析期中報告 1 份 3. 6G 跨產業資安聯防生態探索研究期中報告 1 份	「6G 網元及通訊資安檢測研析期中報告」及「6G 跨產業資安聯防生態探索研究期中報告」各 1 份，達成情形說明如下： 1. 6G 資安偵測與防護研析：臺灣已有工業電腦與伺服器廠商以及小型基地臺製造商積極投入開放式架構網通設備的市場。本報告以開放式無線接取網路(Open RAN)架構下之 5G/B5G 獨立布建核心網路、5G/B5G 開放式無線接取網路、人工智慧與機器學習以及量子電腦運算等 4 種情境下的技術與威脅進行研析。 2. 6G 網元及通訊資安檢測研析：本報告以 6G 無線網路潛在相關技術與資安議題為主，針對國際相關應用情境進行研析，盤點 6G 相關的資安威脅攻擊，並進一步延伸至無人機以及低軌衛星 2 類產品，進行資安威脅與降低資安威脅方法做進一步的研析。 3. 6G 跨產業資安聯防生態探索研究：研析未來 6G 行動通訊可能之技術型態、應用情境，同時描繪出應用情境

查核點編號	預定完成期間	查核點概述	執行成果
			可能涉及的產業別，以及情境可能需求的資安防護，與防護的對應生態，並於9/14(三)辦理 6G 資安產業座談活動，邀請 6 位資安相關企業與專家進行 6G 相關議題的需求訪談。
A-4	111/12	1. 6G 資安偵測與防護研析報告 1 份 2. 6G 網元及通訊資安檢測研析報告 1 份 3. 6G 跨產業資安聯防生態探索研究報告 1 份	已於 12 月 15 日完成「6G 資安偵測與防護研析報告」、「6G 網元及通訊資安檢測研析報告」及「6G 跨產業資安聯防生態探索研究報告」各 1 份，達成情形說明如下： 1. 6G 資安偵測與防護研析報告：本報告以開放式無線接取網路（Open RAN）架構下之第六代行動通訊先期技術核心網路（Pre-6G Core Network, Pre-6GC）、第六代行動通訊先期技術（Pre-6th Generation Mobile Network, Pre-6G）開放式無線接取網路、假基地台以及人工智慧與機器學習等 4 種情境下的技術與威脅進行研析，彙整第六代行動通訊先期技術系統架構的安全議題，期望能協助國內廠商與檢測實驗室建立開放式無線接取網路的資安能量，相關的資安議題

查核點編號	預定完成期間	查核點概述	執行成果
			與建議如下： (1) Pre-6GC 為 3GPP 中定義的 Pre-6G 網組組成之一，可為網路功能虛擬化及多接取邊緣運算提供較完善的網路架構，而 Per-6G 提供垂直應用程序的通用服務平台，於專網布建時與電信業者整合，實現視訊分析、無人車、智慧製造、健康醫療或企業服務等不同類型的技術服務。 (2) 假基地台會干擾與封鎖電信業者訊號，監測到行動通訊過程中的各種訊息，容易造成入侵、監聽與資料被竊取的風險，根據此安全威脅，透過誘騙終端用戶的實驗，作為假基地台的威脅偵測機制，保護 Pre-6G 終端用戶的隱私安全性。 (3) 在 Pre-6G 的應用中，為提供最佳化的網路性能與用戶體驗，因此需運用 AI 與 ML 技術來實現無線訊號智能化與網路巢狀層次的自動化。有

查核點編號	預定完成期間	查核點概述	執行成果
			鑑於此類技術為了大規模部署的效率與成本考量，很大程度仰賴於調整模型，帶來可能造成訊息洩漏或模型損害以致改變決策等風險。因此，端到端自動化網路服務管理與安全防護將會是重點考量的項目。 2. 6G 網元及通訊資安檢測研析報告：本報告以 6G 無線網路潛在相關技術與資安議題為主，針對國際相關應用情境進行研析，盤點 6G 相關的資安威脅攻擊，並依照台灣產業的發展與觀察，進一步延伸至無人機、低軌衛星、遠距醫療此三類產品之 6G 應用，進行資安威脅與降低資安威脅方法做進一步的研析，相關建議如下： (1) HAPS 載體於 6G 無人機上的應用也是國際組織與產業落地的重要項目之一，對於台灣而言無人機上游的零組件廠商打入國際市場與電信業者商轉有巨大的幫助，且未來在自然災害等緊急狀況下等救助，

查核點編號	預定完成期間	查核點概述	執行成果
			無人機可作為無線通信領域的新示範。 (2) 低軌衛星具備低延遲與廣覆蓋率之優點，亦為6G發展之關鍵技術，隨著全球網路覆蓋與高速通訊的需求增加，各國積極投入發展的情況下，我國在通訊設備供應鏈中也佔有重要角色。 (3) 由於目前全球人口平均年齡增加以及近年來慢性病患者數量遽增，未來的醫療保健系統也形成新的挑戰。 3. 6G 跨產業資安聯防生態探索研究報告：本研究報告盤點未來 6G 行動通訊可能之技術型態、應用情境，同時擘繪未來應用情境所需要的資安防護技術。未來應用情境主要可分成晶片資安、網路資安及應用三層，而相關生態未來可分為專網與公網兩種情境，進而針對提高日常生活品質及符合聯合國 SDGs 之 6G 應用、醫療保健、製造、農業等關鍵領域進行情境探索。在建立跨產業之資安聯防合作部

查核點編號	預定完成期間	查核點概述	執行成果
			分，透過辦理 4 場 6G 資安產業活動座談會、問卷調查等方式，邀請包含資訊經理人協會、中華電信、喬立成資安等 54 家跨公協會、電信產業、系統整合商/資安廠商進行訪談，整合集結國內外產、學、研意見及提供之相關議題，擬定我國 6G 應用情境之未來發展方向，依現有 5G/6G 相關產業生態，我國業者可在白牌伺服器及終端設備具備相對優勢，建議及早導入相關資安議題，如 6G 網路各節點介面設置資安防護機制、或終端設備導入 SSDLC 等建議作法，並加強跨產業體聯防意識，以協助我國廠商提升資安防護能力。
B-1	111/07	完成公部門連結小組籌組	基於行政院科發基金管理會遲於 111 年 6 月始與通傳會簽定補助合約，本計畫於 6 月 21 日始完成計畫書暨合約簽定，爰相關「公部門連結小組」未能及於 7 月底完成籌組，在本計畫團隊的努力下，已於 111 年 8 月 23 日完成公部門連結小組籌備會議，本小組分為「雛型系統與國際布局工作組」、「國際連結暨產業應用工作組」、「頻譜整

查核點編號	預定完成期間	查核點概述	執行成果
			備暨跨域發展工作組」及「部會合作與協調推進工作組」等 4 個工作組，規劃架構與分工、運作、年度討論議題等依籌備會議內容執行，後續視實際執行狀況滾動修正。
B-2	111/12	辦理公部門連結小組會議 2 場	已於 9 月 23 日辦理公部門連結小組第一次會議、12 月 7 日辦理第二次會議，針對 6G 發展各項議題進行跨部會協商與意見整合，因應議題需求邀請相關專家顧問與會參與討論，做為跨部會及公私部門協調平台，以有效進行計畫滾動修正，並協助電信業者國際參與，促使政府政策與產業需求有效鏈結。

資料來源：本計畫

參、 計畫背景與架構

一. 計畫背景

第六代行動通訊技術(6th generation mobile networks, 6G)對於數據安全性、用戶隱私和可持續能源等方面更加完備，成為全新通信系統之關鍵，而不僅是一個更好的第五代行動通訊技術(5th generation mobile networks, 5G)而已。由於6G 仍在極前期階段，對應資安攻防端也將設想新的資安攻擊與防禦情境，如量子電腦的量子位元(Qbit)數持續增加，將可輕易破解現行大宗使用的非對稱密碼系統，對此推測必須引入後量子密碼(Post-Quantum Cryptography, PQC)或量子密鑰分發(Quantum Key Distribution, QKD)等防護技術。根據趨勢科技於2021年12月發表一份未來願景報告：《2030專案》，描繪出十年後的世界模樣，以及人類生活將如何演變並衍生新式的網路犯罪。其中因應未來6G世界的來臨，無遠弗屆的萬物連網以及萬物皆服務(Everything as a Service)的結果，將引來各種針對製造、物流、運輸、醫療、教育、零售及家用環境的破壞和勒索攻擊，使得駭客攻擊更加精密，因此必須要有極高的安全等級，以滿足工業和高端用戶的極高要求，提前因應6G 產業發展與應用需求進行規劃布署也更顯迫切。

由於6G 技術與應用的新穎性、整合人工智慧(Artificial Intelligence, AI)應用的多樣性，加上資安威脅也將有新樣態，以致現行資安防護技術難以因應，故以應用情境研析與驗證、資安防護與偵測兩大主軸，涵蓋應用端以應用情境導向整合人工智慧應用與6G 通訊特性，以及資安與隱私防護的需求，對未來6G 實現商轉可能遭遇的問題與技術需求進行規劃與初期驗證。期透過提前整備、布署，使各方能更順暢地推助6G 發展，加速新便利時代的到臨。

在6G 時代更積極的技術/應用特性需求指標下，本計畫將觀測6G 無線通訊技術發展與應用趨勢相關的國際生態系議題動向，例如探索各國產學研界開展6G 先期研究的項目，研析6G 在頻率提升、傳輸速度增加、覆蓋範圍與連網數量的需求上，從射頻無線端、基頻、通訊次系統到網路端的技術發展瓶頸。期望藉由分析國際產學研界對於6G 通訊技術與應用趨勢之見解，據此掌握各組織/政府與產業對於6G 技術與新應用發展布局，並考量我國技術服務發展進程，追蹤可因應未來6G 世代衍生的諸多創新且多元應用可能伴隨之技術門檻，協助我國規劃先期研究布局、研擬相關政策推動發展之參考。

二. 計畫架構

為布局我國6G 自主技術能量，使臺灣成為全球主流系統重要策略夥伴，本計畫將先期投入6G 產業發展規劃相關重要工作，除了通訊系統之外，相關的數位科技應用技術、標準、智財也是兵家必爭之地，其中又以人工智慧、資安隱私兩項數位科技應用最為關鍵，故將以涵蓋應用端以應用情境導向整合人工智慧應用與6G 通訊特性，以及資安與隱私防護的需求，對未來6G 商轉可能遭遇的問題與技術需求進行規劃與初期驗證。其中包含成立公部門連結小組，針對6G 發展各項議題，進行跨部會協商與意見整合。

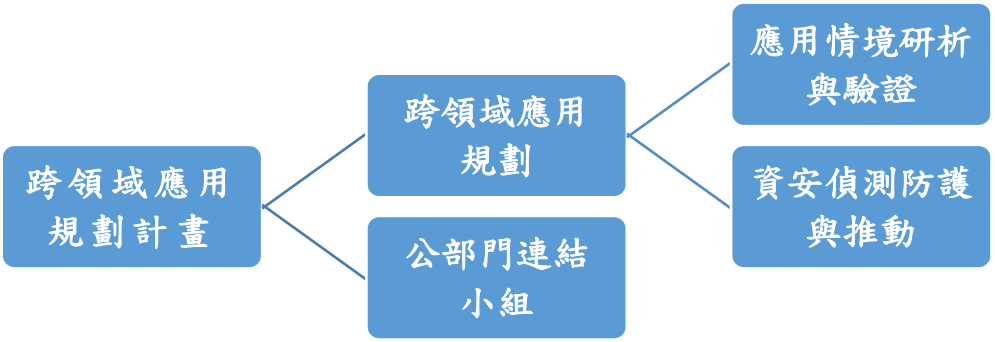


圖1、計畫架構表

資料來源：本計畫

(一) 跨領域應用規劃

1. 應用情境研析與驗證

6G 將更為確立融合通訊系統與數位科技應用的架構，在面對未來更大量的異質裝置與網路的整合，預計達到高效率、

低延遲的應用整合體驗，本計畫預計收集產業相關意見與未來發展方向，對可能遇到的問題，進行研究並對相關技術進行可行性評估與雛型研發驗證，並將推動與現有電信業者在基礎AI技術整合通訊網路框架上，對未來銜接6G 標準進行討論與驗證測試，以期在初期對6G-機器學習(Machine Learning, ML)標準架構參與相關標準制定與討論，中期可提前融合相關技術進行整備，最後在6G 商轉時可快速拓展相關6G 特色應用服務的展開。

2. 資安偵測防護與推動

為使計畫有效達成預期目標，擬以超越第五代行動通訊技術(Beyond 5th Generation Mobile Networks, B5G)、第六代行動通訊先期網路技術(Pre 6th Generation Mobile Network, Pre-6G)、6G 等通訊技術為核心，規劃對應資安防護機制，產業服務所需之資安方案能量，以及推動未來產業生態協作體系等方向進行策略推動：

(1) 規劃 B5G/Pre-6G/6G 資安技術研發方向：結合過往第四代行動通訊技術(4th Generation Mobile Networks, 4G)/5G 自主資安技術研發成果之基礎，因應未來6G 相

關技術發展趨勢，研提6G 通訊層和服務層威脅研析，包含相關威脅攻擊與其應對偵防技術。6G 產業業者可透過此報告事先針對待解決的資安議題與挑戰進行跨產業合作與技術研發，亦可透過本報告建議尋求/發展解決方案，提高安全強度，提升國產產品資安防護能力與國際競爭力。

(2) 規劃6G 產品資安防護機制：研析6G 資安偵防系統所需之技術與環境規格/規範，結合國內外相關場域試煉實證經驗，導入相關資安防護機制，透過新型攻擊手法研提，由外而內建置完善6G 資安偵防系統發展建議。

(3) 推動6G 資安產業與生態體系發展並促進未來6G 應用場域實驗建立：落實法人研發與產業合作，結合國內資安業者、系統整合商、網通設備廠商與專網業者合作，進行6G 產業變遷預測、服務發想規劃、在地專網資安解決方案與服務框架研析，協助國內資安檢測服務業者超前部署6G 資安檢測能量，提升國際競爭力。

(二) 公部門連結小組

以行政院科技會報辦公室(111年7月27日更名為國科會科技辦公室)為指導單位，針對6G 發展各項議題，進行跨部會協商與意見整合。公部門連結小組整合4個工作組，包含雛型系統與國際布局工作組、國際連結暨產業應用工作組、頻譜整備暨跨域發展工作組及部會合作與協調推進工作組，定期收集相關意見並協助各工作小組間的資源需求整合。

公部門連結小組以「公部門」為主體，另有經濟部計畫下之6G產業諮詢小組係以「產業」為主體，我國6G 產業發展相關議題與產業相關者，以6G 產業諮詢小組為主要溝通協調平台，而經濟部議題須協調者則以公部門連結小組為溝通協調平台，若產業發展需要政府部會協調時，則由經濟部將議題提至公部門連結小組進行協調，並將協調結果回覆6G 產業諮詢小組；同理，若公部門連結小組討論議題中有需要聽取產業建議者，則請6G 產業諮詢小組協助協調，並將協調結果回覆公部門連結小組，透過公部門連結小組與產業諮詢小組資訊交流，以確認產業議題於公部門連結與協調。

肆、 工作實際執行情形說明

本計畫今年度的工作均依規劃確實執行，相關執行情形詳列如後，將先就第一部分跨領域應用的產業現況與國際趨勢進行分析說明，第二部分的計畫執行情形再依前述分析結果進行相關的議題探討，包含「跨領域應用情境研析」、「6G 資安偵測與防護研析」、「6G 網元及通訊資安檢測研析」及「6G 跨產業資安聯防生態探索研究」，接著針對「通訊整合增強型人工智慧協作設計與驗證」、「安全可靠與受信賴的分散式運算設計與驗證」進行實證方式與結果說明，最後則說明「公部門連結小組」的年度推動成果。

首先，就跨領域的產業現況與國際趨勢進行分析說明：

一. 跨領域應用產業現況與國際趨勢研析

為因應未來 6G 各類新興應用所需之技術特性以及現階段 5G/B5G/Pre-6G 等相關標準與大廠之規劃，本計畫將觀測並掌握 6G 國際生態系在 6G 無線通訊技術發展與應用趨勢相關議題動向，例如相關的國際標準組織，以及探索各國主要機構之 6G 先期研究的項目，期望藉由梳理國際產學研界對於 6G 通訊技術與應用趨勢之見解，據此掌握各組織/政府與產業廠商對於 6G 技術與新應用發展布局，並考量我國技術服務發展進程，追蹤可因

應未來 6G 世代衍生的諸多創新且多元應用可能伴隨之技術門檻，協助我國規劃先期研究布局、研擬相關政策推動發展之參考。

以下將對應 6G 潛在威脅與防護先期研究、網通資安生態系解析、6G 系統與新興應用服務推動等背景展開重點研析，並配合國際組織之規範與相關產業與技術發展現況與進行說明。

(一)6G 通訊系統的演進

第六代行動通訊提供了真正自治網路的願景，6G 將能夠支持超過 1Tbps 的速度，比 5G 快 50 倍，而延遲預計為 10-100μs，目前 5G 還在發展中，推估 6G 無線網路將在 2030 年進行商業部署，而 6G 基礎建設範圍預設該標準將從 5G 傳統的覆蓋區域(地面基礎設施) 擴大到 3D 覆蓋範圍(地-空-海三方面建設無線接入網基礎設施)，實現 3D 聯網，伴隨著覆蓋範圍和網路異構性的大幅增加，人們嚴重擔心 6G 的安全性和隱私性可能會比前幾代更差。然而針對 6G 網路的安全和隱私問題的研究仍處於早期階段，現有的研究主要是針對物聯網(Internet of Things, IoT)網路、5G 網路以及像是人工智慧和機器學習或 6G 可能衍生的特定技術進行初步的探索，因此 6G 網路的許多基本組件在很大程度上仍未定義。

然而，觀察先前幾代網路的演進(從 4G 到 5G)表明，每一代網路都傾向於使用多年。對於資本支出和投資回報優化，許多網路供應商傾向於推出新一代網路，同時仍增強現有基礎設施的技術。此外，向後兼容對於維持已部署設備的連接性是必要的，作為繼承的基礎，6G 的安全性和隱私性會基於 5G 的特性進一步做延伸。基於當前 5G 的基礎上去預想 6G 網路架構暫定的威脅形勢，對 6G 使用的新技術做攻擊分類和相應的解決方案。

自 1980 年代 1G 無線網路問世以來，幾乎每十年就會推出新一代通訊技術，從一代到另一代的轉移改進了服務品質(Quality of Services, QoS)指標，包括新服務，並提供新功能。

1. 第一代行動通訊技術(1G)：為類比式行動電話系統，使用類比調變，分頻多重進接(Frequency Division Multiple Access , FDMA)，僅限語音的傳送，使用蜂巢式基地台架構，缺點是此時通話品質並不好且訊號不穩定、同時能連線的數量少、保密性低。
2. 第二代行動通訊技術(2G)：2G 行動通訊系統對語音係以數位化方式傳輸，除具有通話功能外，某些系統並引入了簡訊(Short Message Services , SMS)功能。其中 2G 最重要的標

準就是全球行動通訊系統(Global System for Mobile Communications, GSM)，透過數位的方式強化「蜂巢式網路」架構，更容易延伸和擴充，包含室內都可以通。還可以國際漫遊。使用者身分模組(Subscriber Identity Module, SIM)卡也跟隨的 GSM 標準誕生，可讓使用者透過換裝 SIM 卡的方式換裝置，更可以儲存個人資料和發送文字簡訊。

3. 第三代行動通訊技術(3G)：3G 為將無線通訊與網際網路等多媒體通訊結合的新一代行動通訊系統。能夠處理圖像、音樂、視訊形式，提供網頁瀏覽、電話會議、電子商務資訊服務。3G 規格是由國際電信聯盟(International Telecommunication Union, ITU)所制定的 IMT-2000 規格的最終發展結果。目前 3G 存在四種標準：W-CDMA、CDMA2000、TD-SCDMA、WiMAX。

4. 第四代行動通訊技術(4G)：是 3G 之後的延伸，由歐、日、韓產業巨頭一起組成的第三代合作夥伴計劃(3rd Generation Partnership Project, 3GPP)，提出以分離複頻調變技術(Orthogonal frequency-division multiplexing, OFDM)為基礎的長期演進技術(Long Term Evolution, LTE)。一方面要更多

連線數，更快的速度，更長的通信距離，而且可以和 3G 通道共存，這可以說是 2G 至 4G 的技術的總集合。從技術標準的角度看，按照 ITU 的定義，靜態資料傳輸速率達到 1Gbps，使用者在高速行動狀態下可以達到 100Mbps，就可以作為 4G 的技術之一。

5. 第五代行動通訊技術(5G)：為 4G(LTE-A、WiMAX-A、LTE)系統後的演進。5G 的效能目標是高資料速率、減少延遲、節省能源、降低成本、提高系統容量和大規模裝置連接。在 ITU-R 已經定義了 5G 的增強功能三個主要的應用領域指標。分別是增強型移動寬頻(Enhanced Mobile Broad-Band, eMBB)、超高可靠低延遲通訊(Ultra-Reliable Low-Latency Communications, uRLLC)和大規模機器類互聯(Massive Machine-Type Communications, mMTC)。

依據 3GPP 定義的規格，5G 分為 2 個大頻段，第一個是以 6GHz 頻段為界線，6GHz 以下的 Sub-6 頻段，範圍在 450MHz 至 6GHz 之間，而毫米波(mmWave)頻段，則是屬於高頻段，範圍在 24GHz 至 52GHz 之間。以下將針對兩個頻段進行說明與比較：

(1) Sub-6 頻段(450MHz-6GHz)

屬於 5G 的低頻段，與 4G LTE 技術相近，差別為 Sub-6 增加頻寬(通道寬度)以提升傳輸速度，但是頻率並沒有提升，被稱為是初階的 5G 技術。由於 Sub-6 的產業技術已經非常成熟，可以用現有的 4G 技術繼續向下發展跟強化，所以 Sub-6 的基地台容易部署，且傳訊距離長、覆蓋範圍廣，讓它成為許多國家的 5G 主要發展方向。缺點是 Sub-6 所涵蓋的頻段多數已被占用，因此使用的資源變得相當有限，也有不少國家捨棄飽和的 Sub-6，完全轉向 mmWave 毫米波發展 5G 頻段。

(2) mmWave 頻段(24GHz-52GHz)

毫米波通訊技術屬於 5G 的高頻段，無線通訊技術提升頻段至 24GHz 以上，傳輸速率快、低延遲、頻寬更大，被稱為是進階的 5G 技術，為待突破開發，降低限制條件的下一階段目標技術，目前已知美國同步進行 Sub-6 和 mmWave 毫米波的開發，優點有頻率高、頻寬大，且鮮少被使用，讓它能支援高速大容量的資料傳輸，也因此才能達到 5G 的「高速度、低延遲」特性。缺點是 mmWave 毫

米波的波長短、穿透力弱，也就是它很容易受到地形限制，如果要在所有地方都能夠維持高速上網，必須要建構大量的基地台，短時間難以普及。

表3、5G Sub-6和 mmWave 差異表

頻段	Sub-6	mmWave 毫米波
傳輸速率	最高 1Gbps	最高 10Gbps
頻寬	最大 100MHz	最大 400MHz
延遲	0.5 毫秒	0.125 毫秒
優點	1.訊號射程長 2.穿透率高 3.建置成本低	1.傳輸速率快 2.頻寬較大 3.低延遲 4.裝置體積小、易安裝
缺點	1.與 4G LTE 技術相近，無法真正快速傳輸 2.於都市等高需求區域，因傳輸量限制不敷使用	1.訊號射程短容易被阻擋 2.覆蓋範圍小致使需廣設基地台增加網路覆蓋，建置成本相對較高

資料來源：本計畫整理

3GPP 於 2018 年通過第 15 版(Release15)規格，對 5G 新無線電(5G New Radio, 5G NR)，以 6GHz 為界，區分第一型頻率範圍(Frequency Ranges 1, FR1)與第二型頻率範圍(Frequency Ranges2, FR2)，FR1 頻段範圍為 450-6000MHz，FR2 頻段範圍為 24250-52600MHz，整理如表 4 及圖 2、圖 3：

表4、5G NR 頻段劃分表

頻率範圍名稱	相應的頻率範圍
FR1	450-6000MHz
FR2	24250-52600MHz

資料來源：本計畫整理

NR 運作頻段	上行頻率	下行頻率	多工模式
n1	1920-1980 MHz	2110-2170 MHz	FDD
n2	1850-1910 MHz	1930-1990 MHz	FDD
n3	1710-1785 MHz	1805-1880 MHz	FDD
n5	824-849 MHz	869-894 MHz	FDD
n7	2500-2570 MHz	2620-2690 MHz	FDD
n8	880-915 MHz	925-960 MHz	FDD
n12	699-716 MHz	729-746 MHz	FDD
n20	832-862 MHz	791-821 MHz	FDD
n25	1850-1915 MHz	1930-1995 MHz	FDD
n28	703-748 MHz	758-803 MHz	FDD
n34	2010-2025 MHz	2010-2025 MHz	TDD
n38	2570-2620 MHz	2570-2620 MHz	TDD
n39	1880-1920 MHz	1880-1920 MHz	TDD
n40	2300-2400 MHz	2300-2400 MHz	TDD
n41	2469-2690 MHz	2469-2690 MHz	TDD
n51	1427-1432 MHz	1427-1432 MHz	TDD
n66	1710-1780 MHz	2110-2200 MHz	FDD
n70	1695-1710 MHz	1995-2020 MHz	FDD
n71	663-698 MHz	617-652 MHz	FDD
n75	n/a	1432-1517 MHz	SDL
n76	n/a	1427-1432 MHz	SDL
n77	3300-4200 MHz	3300-4200 MHz	TDD
n78	3300-3800 MHz	3300-3800 MHz	TDD
n79	4400-5000 MHz	4400-5000 MHz	TDD
n80	1710-1785 MHz		SUL
n81	880-915 MHz		SUL
n82	832-862 MHz		SUL
n83	703-748 MHz		SUL
n84	1920-1980 MHz		SUL
n86	1710-1780 MHz		SUL

圖2、3GPP 5G NR FR1頻段配置方式

資料來源：3rd Generation Partnership Project, 3GPP

NR 運作頻段	上行頻率與下行頻率	多工模式
n257	26500-29500 MHz	TDD
n258	24250-27500 MHz	TDD
n260	37000-40000 MHz	TDD
n261	27500-28350 MHz	TDD

圖3、3GPP 5G NR FR2頻段配置方式
資料來源：3rd Generation Partnership Project, 3GPP

6. 第 6 代行動通訊技術(6G)：第六代行動通訊技術是 5G 系統後的延伸，目前仍在開發階段，3GPP 的 6G 標準工作小組尚未開始制定相關事項。

B5G 和 6G 的目標是各自的能力比上一代移動升級提升 10-100 倍。在過去十年中，由於智慧設備和機器對機器通訊的引入，移動數據流量大幅增長，預計到 2030 年全球移動流量將比 2010 年增長 670 倍，到 2030 年底，ITU 預測所有移動數據流量將超過每月 5ZB，移動用戶數量將達到 171 億，而 2010 年為 53.2 億。

6G 通訊系統演進背後的幾個關鍵驅動趨勢如下：高比特率、高可靠性、低時延、高能效、高頻譜效率、新頻譜、綠色通信、智慧網路、網路可用性、通訊融合、定位、計算、控制和傳感，6G 將是一個全數位連接的世界。

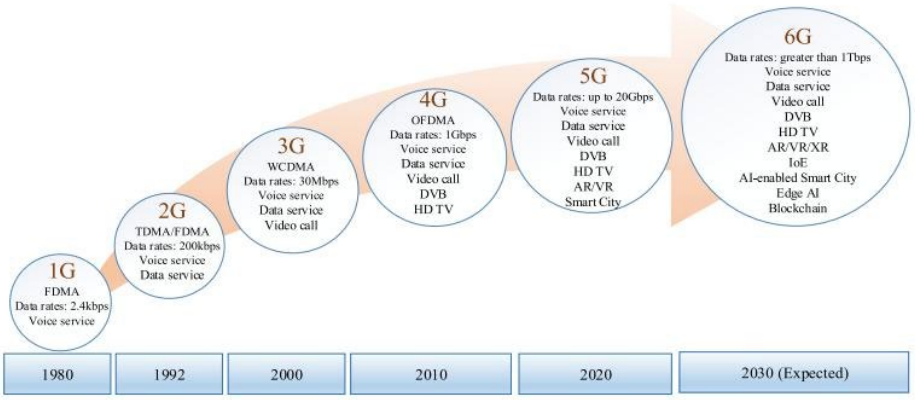


圖4、行動通訊系統演進(1G to 6G)

資料來源：6G Wireless Systems: A Vision, Architectural Elements, and Future Directions, IEEE

(二)通訊技術產業現況

1. 5G 毫米波頻段使用現況

隨著 5G 在全世界大規模商轉，很快就會用盡 6GHz 以下(sub-6 GHz)頻段的頻譜資源。

電信事業為了實現更好的用戶體驗(Quality of Experience, QoE)，其營運的 5G 系統就需要支援 3GPP 定義之第二型頻率，也就是 24GHz 頻率以上的毫米波(millimeter wave, mmWave)，以支援密集區域的部署，如大型體育館與展演場域等高訊務服務熱點等行動寬頻場景。由於使用毫米波讓 5G 系統具備高頻寬、大容量以及超低延遲等多項優勢，有助於推動超低延遲的工業物聯網(Industry Internet-of-Things, IIoT)與智慧製造，同時實現大頻寬和高傳輸率的雲端運算產業，提升擴增實境(Augmented

Reality, AR)和虛擬實境(Virtual Reality, VR)線上遊戲體驗，加速 5G 在元宇宙(Metaverse)的發展。

臺灣的 5G 毫米波正在起步階段，臺灣的電信事業龍頭中華電信與全球最大的手機晶片供應商聯發科技於新竹的聯發科技研發總部打造 5G 毫米波晶片測試環境，其建置的 5G 技術非獨立組網(Non-Standalone, NSA)訊號包含 3.5GHz 中頻(頻寬 90 兆赫茲)及 28GHz 毫米波高頻頻段(頻寬 600 兆赫茲)。聯發科技的 5G mmWave 陸續搶攻美日市場以完整的布局到大眾市場的全系列產品。

此外，為了因應日益蓬勃的 5G 企業專網終端設備需求，聯發科技提供晶片給國內外廠商開發專屬 5G 終端設備，並搭配於中華電信推廣之企業專網服務場域使用，引領臺灣 5G 產業升級與轉型，導入各產業垂直應用鏈，滿足各項智慧生活應用的傳輸需求。中華電信攜手國際晶片大廠高通(Qualcomm)及臺灣手機品牌華碩、雲端遊戲開發商 Gamestream 打造由 5G mmWave 驅動的 5G 垂直領域應用 4K 超高畫質電視(Ultra High Definition Television, UHDTV)遊戲展示場域，以 5G mmWave 在手機上展現優異 4K 畫質雲端遊戲串流技術。日月光預計自行投資約四千

萬建構企業 5G mmWave 專網試煉場域，協助國產廠商進行建構毫米波專網網路設備與國際5G 專網服務的整合架構設計與驗證。日月光將採用高通開發的 Snapdragon X65 5G 數據機射頻系統，並於高雄智慧工廠中導入 5G 獨立組網毫米波雙連線(New Radio Dual Connectivity, NR-DC)通訊技術。

部署 5G 獨立組網毫米波網路與裝置可以不使用 6GHz 以下(sub-6 GHz)頻段，大幅突破 5G 上行傳輸瓶頸，滿足半導體高階製程所需擴展性，以更有彈性地提供具有數千兆位元速度和超低延遲的無線光纖寬頻網路加速智慧製造應用。

2. 5G 開放式無線接取網路發展現況

臺灣現有工業電腦與伺服器廠商以及小型基地臺製造商，積極投入 5G 開放式無線接取網路(Open Radio Access Network, O-RAN)架構以及邊緣運算(Edge Computing, EC)平台網通設備的市場，而且電信事業為了節流，切割標單、分開採購，直接向品質佳的第三方設備供應商購買，網通設備「白牌化」商機應運而生。

當企業欲建立起 Pre-6G 專網環境時，可透過租用電信營運商的 Pre-6G 網路達成，但礙於企業的資訊需要保密，故需要將

EC 平台部署於企業網路中。同時為了實現低延遲率與高可靠度以及高傳輸速率的垂直領域應用服務，需將 Pre-6G 專網多接取邊緣運算與電信業者無線接取網路及核心網路的通訊設備緊密整合，所以 Pre-6G 專網多接取邊緣運算是未來部署 Pre-6G 企業專網的關鍵。

(三)各國國際安全標準化組織

2015 年 2 月 3 日經濟部成立「臺灣資通產業標準協會」(Taiwan Association of Information and Communication Standards, TAICS)，是國內唯一協助資通訊產業標準發展之非營利組織，由資通產業各領域關鍵廠商參與組織運作，會員已超過 100 家，包含產業界、法人、研究單位及政府單位，TAICS 為官方認可與國際標準發展接軌的標準發展組織，與國際及區域標準組織連結的窗口。現已與多家標準組織/聯盟，包括電機電子工程師學會(Institute of Electrical and Electronics Engineers, IEEE)、歐洲電信標準協會(European Telecommunications Standards Institute, ETSI)、中國通信標準化協會(China Communications Standards Association, CCSA)、次世代行動網路聯盟(Next Generation Mobile Networks, NGMN)等建立連結管道。

以當前 5G 網路標準舉例，國際電信聯盟 ITU 作為聯合國專門機構，所發布的標準在國際上有著高度認同，而國際電信聯盟無線電通信部門(ITU Radiocommunication Sector, ITU-R)在工作組會議上，批准了 3GPP 5G 技術，將其作為 2020 年第五代行動通訊技術(International Mobile Telecommunications 2020, IMT-2020)標準，各國將依照這標準在世界各地部屬 5G 網路，臺灣目前是以歐洲電信標準協會 ETSI 會員方式參與 3GPP 無線通訊標準的會議討論，學術界的陽明交大、台北大學跟研究單位的工研院、資策會，業界的聯發科、中華電信，皆都是以 ETSI 會員身分參與。

我國在全球通訊產業中扮演網通設備的主要供應國，而在無線網路標準的發展過程中，臺灣產業一直都是於通訊標準底定後，才投入產品與服務，故一直無法搶得先機，如今 5G 國際標準制定上，我國開始緊跟國際標準趨勢發展，積極參與國際標準會議，期許於標準制定後第一時間，推出具競爭力之產品。

以下針對各國國際安全標準組織做簡單介紹，更多的應用與技術分析將在「三、計畫執行情形-跨領域應用情境研析」做詳細說明：

1. 歐洲電信標準協會 ETSI

ETSI 是在歐洲的一個獨立的、不以營利為目的的電信行業(裝置製造商和網路業者)標準化組織，於 1988 年由歐洲郵電管理委員會(Confederation of European Posts and Telecommunications, CEPT)建立，並得到了歐洲聯盟執委會和歐洲自由貿易協會(European Free Trade Association, EFTA)秘書處的正式認可，總部設在法國索菲亞科技園，已被歐盟正式承認為歐洲標準化組織，在全球擁有 900 多家會員組織，遍佈五大洲 64 個國家。其多元化的會員組織由各種規模的私人公司、研究機構、學術界、政府和公共組織組成，影響力輻射全球。ETSI 為會員提供了開放且包容的環境，制定適用於全球的資訊科技與通信技術(Information and Communications Technology, ICT)標準，包括固定、移動、無線電、融合、廣播和網際網路技術，這些標準涉及各行各業和社會各界領域。

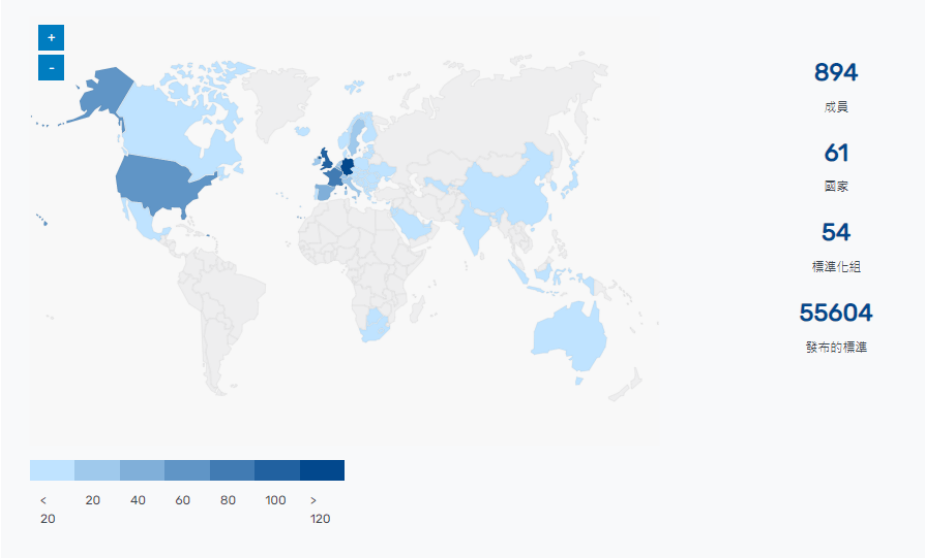


圖5、歐洲電信標準協會_ 全球會員分佈
資料來源：European Telecommunications Standards Institute, ETSI

如圖 5 所示，ETSI 同時也是 3GPP 國際標準組織的成員跟合作夥伴，和日本的一般社團法人電波產業會(Association of Radio Industries and Businesses, ARIB)與日本情報通訊技術委員會(Telecommunication Technology Committee, TTC)、韓國的電信技術協會(Telecommunications Technology Association, TTA)、中國通訊標準化協會(China Communications Standards Association, CCSA)、印度電信標準發展協會(Telecommunications Standards Development Society, India, TSDSI)和美國的電信產業標準聯盟(Alliance for Telecommunications Industry Solutions, ATIS)共同參與 3GPP 技術規格制定，目的為制定無線網路全球通用標準，另外 ETSI 也是

全球機器對機器合作項目 (one Machine-to-Machine, oneM2M)的成員，該組織的目標是根據其成員提出的要求，為機器對機器和物聯網技術的架構、API 規範、安全和註冊解決方案創建一個具備互操作性的全球技術標準。

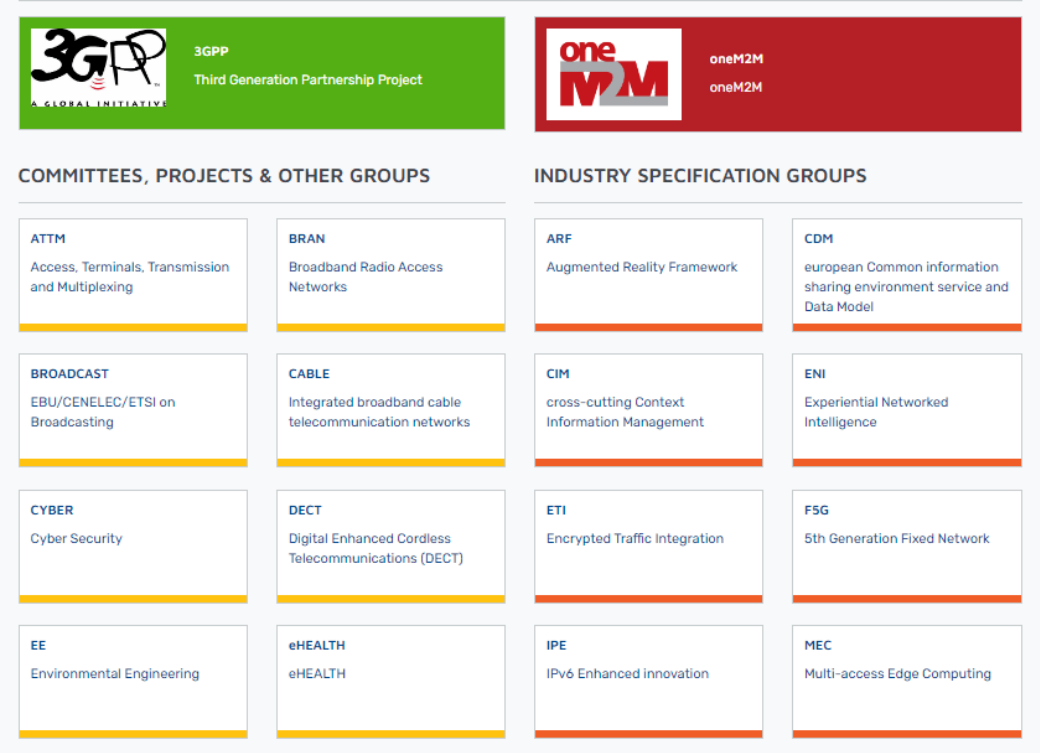


圖6、ETSI_3GPP&oneM2M 合作項目
資料來源：European Telecommunications Standards Institute,ETSI

ETSI 推出了多個行業規範組(Industry Specification Groups, ISG)來檢查 5G 組件技術，包括網路功能虛擬化(Network Functions Virtualisation, NFV)、安全人工智慧行業規範小組(Securing Artificial Intelligence, SAI)、體驗式智慧網路工作組(Experiential Networked Intelligence Industry, ENI)和零接觸和服

務管理小組(Zero touch network & Service Management, ZSM)負責處理網路自動化相關。NFV-SEC 是 ISG NFV 下的一個工作小組，負責制定與 NFV 技術安全相關的行業規範。

2. 國際電信聯盟電信標準化部門(Telecommunication Standardization Sector, ITU-T)

此部門是國際電信聯盟管理下的專門制定遠端通信相關國際標準的組織。1865 年成立國際電報電話諮詢委員會(Comité Consultatif International Téléphonique et Télégraphique, CCITT)，總部在瑞士日內瓦，並於 1993 年改名為 ITU-T，該機構一直在推動以貢獻為主導、基於共識的標準制定方法，在這種方法中，所有國家和公司，無論大小，都被賦予平等的權利來影響 ITU-T 建議書的製定，從作為國際電報交換標準化機構開始，到其在電信領域的形成以及在當今融合的 ICT 生態系統中，ITU-T 為全球標準化界提供世界上最好的設施，並且仍然是世界唯一真正的全球 ICT 標準機構。

3. 第三代合作夥伴計劃 3GPP

3GPP 於 1998 年 12 月成立，最初的工作範圍是第三代行動電話系統制定全球適用的技術規範和技術報告，之後 3GPP 工作範圍改進增加對通用陸面無線接取(Universal Terrestrial Radio Access, UTRA)長期演進系統和 5G NR 的研究和標準制定，成員包括七個電信標準開發組織，歐洲的 ETSI、日本的 ARIB 與 TTC、韓國的 TTA、中國的 CCSA、印度的 TSDSI 和美國的 ATIS，稱為「組織合作夥伴」，一起參與 3GPP 技術規格訂定，其技術規格涵蓋 2G 至 5G 技術，包含 GSM、全球行動通訊系統 (Universal Mobile Telecommunication System, UMTS) 和長期演進技術 LTE。目前獨立成員超過 550 個，並包含電信技術發展產業聯盟 (TD Industry Alliance, TDIA)、 時分同步碼多重進接 (Time Division - Synchronous Code Division Multiple Access, TD-SCDMA)論壇、分碼多重進接(Code Division Multiple Access, CDMA)發展組織(Communications Data Group, CDG)等 13 個市場夥伴(MRP)，全球會員分布情況如圖 7 所示。

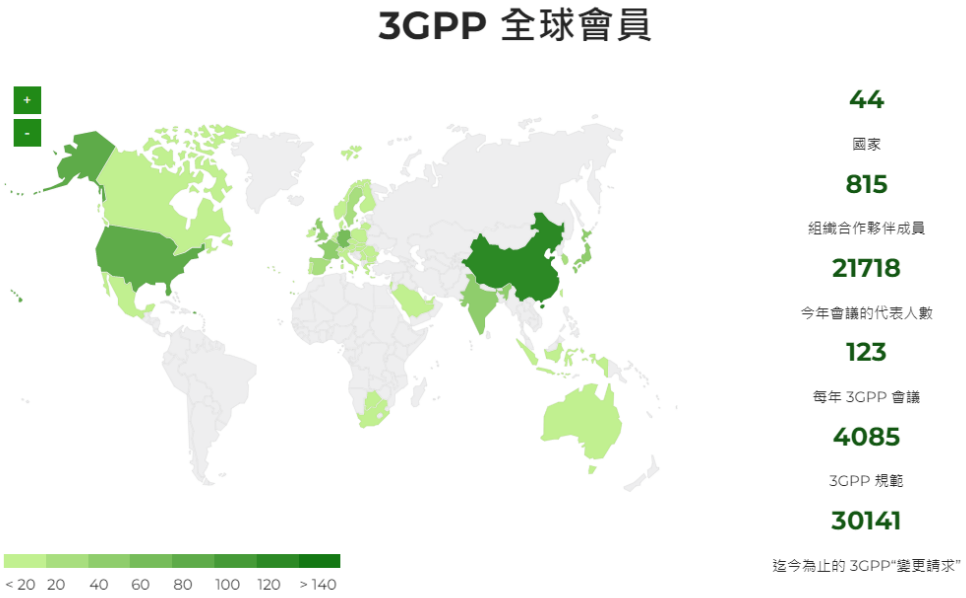


圖7、3GPP_全球會員分佈
資料來源：3rd Generation Partnership Project, 3GPP

3GPP 組織結構中，技術方面的工作由技術規範組(Technology Standards Group, TSG)完成，目前包含 3 個 TSG，分別負責不同的部分：

(1)無線接取網路(Radio Access Network, RAN)：制定無線介面技術演進的標準。

(2)終端與核心網路(Core Network and Terminal, CT)：制定終端與核心網路的技術演進的標準。

(3)服務與系統方面(Service and System Aspects, SA)：指整個系統架構以及系統提供服務模型。

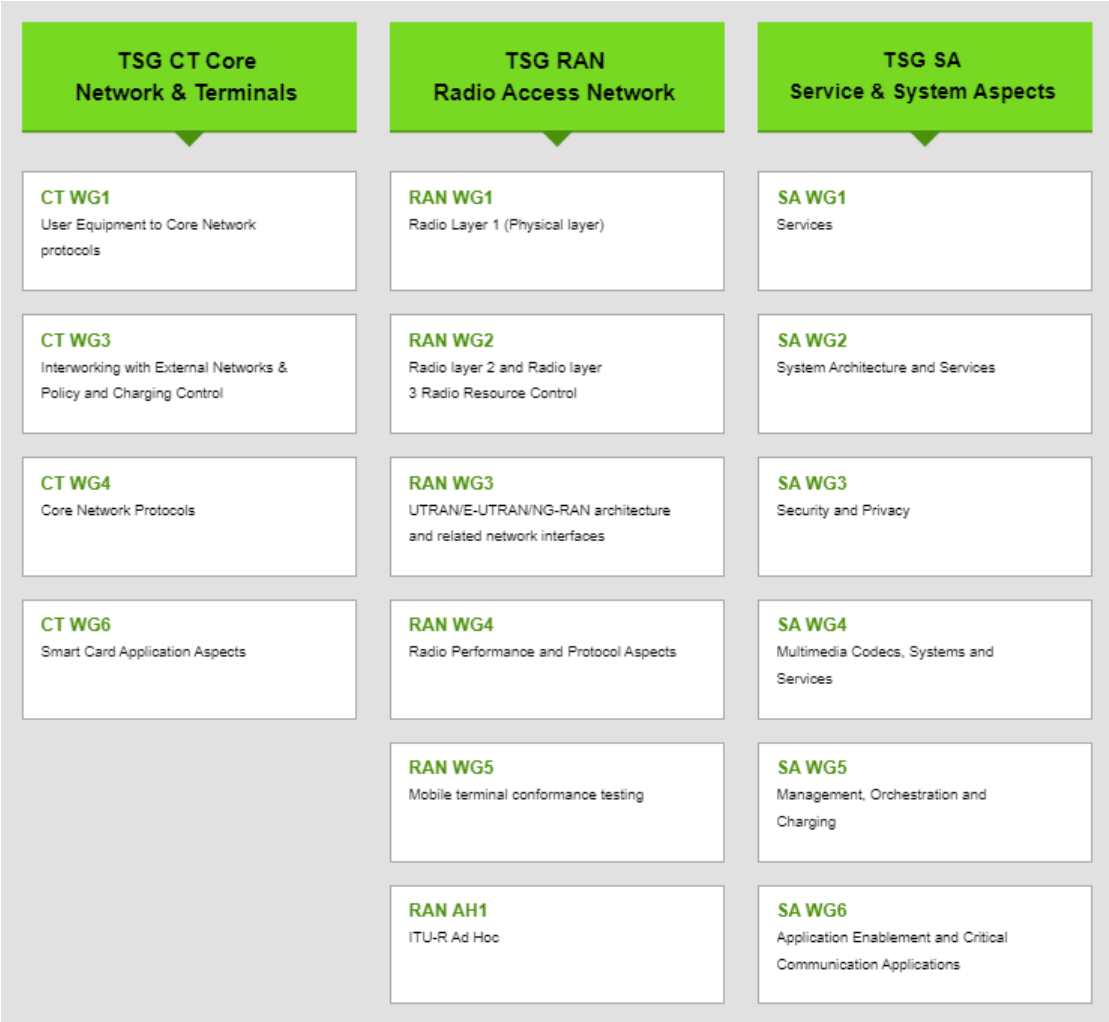


圖8、3GPP_技術規範組
資料來源：3rd Generation Partnership Project, 3GPP

3GPP 制定的標準以 Release 作為版本進行管理，可以將 Release 視為一個工作規劃，實際工作時按照預定的規劃進行工作， 並且會有好幾個 Release 並行工作(例如：完善 5G 網路標準的同時，開始 6G 網路研究)，每個 Release 的工作重點都不一樣，下面介紹最近幾個 Release 的重點內容：

(1)Release16(R16)

2020 年 6 月已凍結，為 5G 第二版涉及各種主題：多媒體優先服務、車聯網應用層服務、5G 衛星接入、5G 中的局域網支持、用於 5G 的無線和有線融合、終端定位和定位、垂直域通信以及網路自動化和新型無線電技術。正在研究的其他項目包括安全、編解碼器和流媒體服務、局域網互通、網路切片和物聯網。

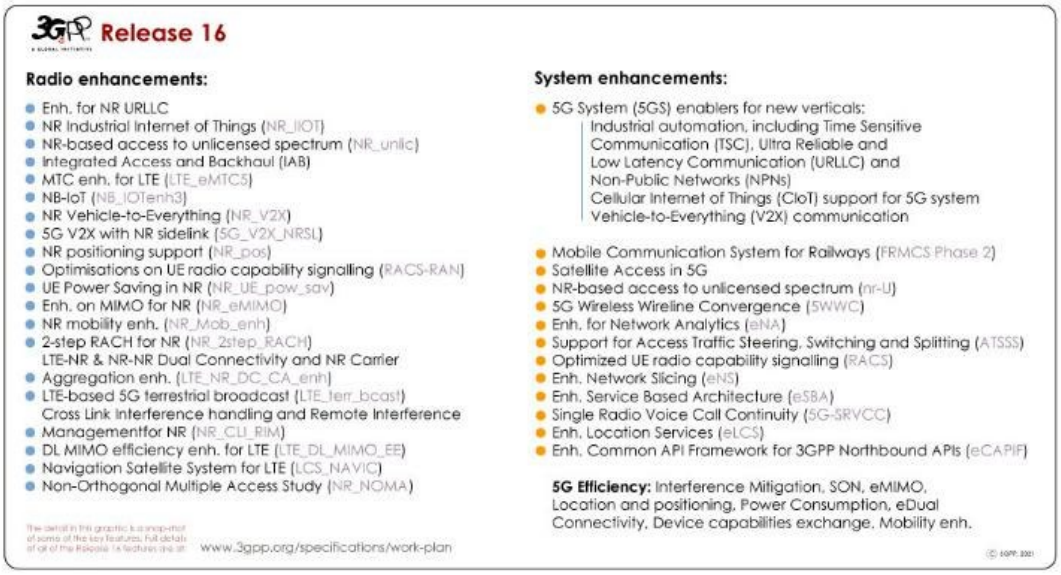


圖9、3GPP_Release16標準規範

資料來源：3rd Generation Partnership Project, 3GPP

(2)Release17(R17)

2022 年 6 月已凍結，3GPP R17 進一步增強 5G 系統功能，如容量、涵蓋範圍、能源消耗、延遲與移動性等，關鍵改善領域包含進一步增強巨量天線(further enhanced massive MIMO)、涵蓋增強、設備節能、頻譜擴充、增強型整合接取/後端網路

(Integrated Access/Backhaul, IAB)和簡單中繼器、進一步強化超低延遲 URLLC、專用網路等。而 3GPP R17 擴展 5G 的新設備與應用，如輕量化(Reduced capability, RedCap 或 NR-Light)終端裝置、非地面網路(Non-terrestrial networks, NTN)、側鏈路(sidelink)擴充、增強精準定位、廣播／群播擴充(broadcast/multicast expansion)、無邊界延展實境(Boundless Extended Reality, Boundless XR)等。此外，其他增強 5G 系統的項目包含多無線電雙連結(multi-radio dual connectivity)、多 SIM 卡支援(multi-SIM support)、小資料傳輸、體驗品質、無線電接取網路切片(RAN slicing)。

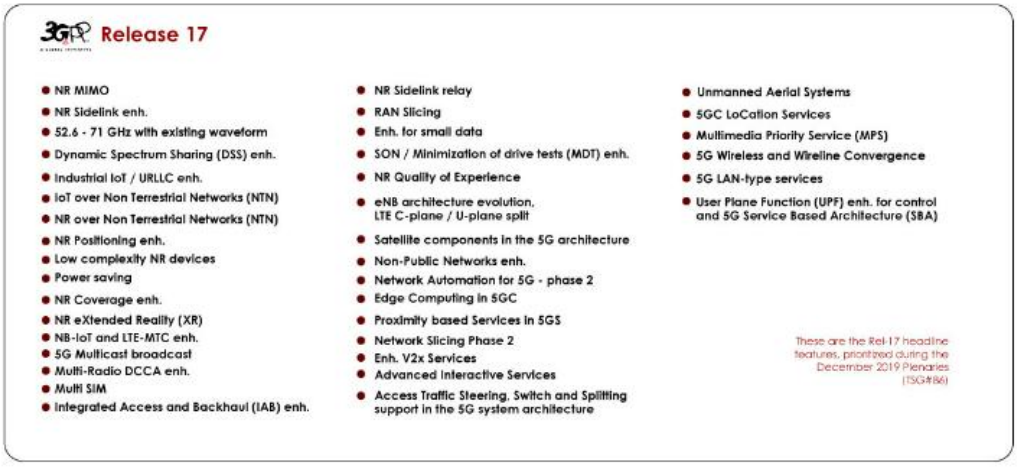


圖10、3GPP_Release17標準規範

資料來源：3rd Generation Partnership Project, 3GPP

(3)Release18(R18)

R18 於 2022 年開始進行，新版本將大幅提升 eMBB 性能、普及 XR 等沉浸式新服務、滿足行業大規模數位化、實現萬物聯網等多個目標，始能提升 5G，產生更大的社會和經濟價值。3GPP 已列出 R18 版本的早期工作項目如：網路切片接入和支持增强、5G 時序彈性系統、基於測距的服務、工業物聯網場景低功耗高精度定位、鐵路智慧車站服務配套、鐵路網外 Off-Network for Rail、支持觸覺和多模式通信服務、車載繼電器、5G 智慧能源與基礎設施、住宅 5G 的增強功能、個人物聯網網路、5GS 中 AI/ML 模型遷移的流量特性和性能要求。

圖11、3GPP_Release18標準規範

資料來源：3rd Generation Partnership Project, 3GPP

2022 年 3GPP 的 5G 標準已經進入到 R18 階段了，目前尚未有任何 6G 標準的項目發展，從 2022 年印度 ITU-APT 展示的 3GPP 時間軸來看，推估 6G 可能在 2024-2025 年間定義需求，規劃在 2025-2026 年創建研究項目。

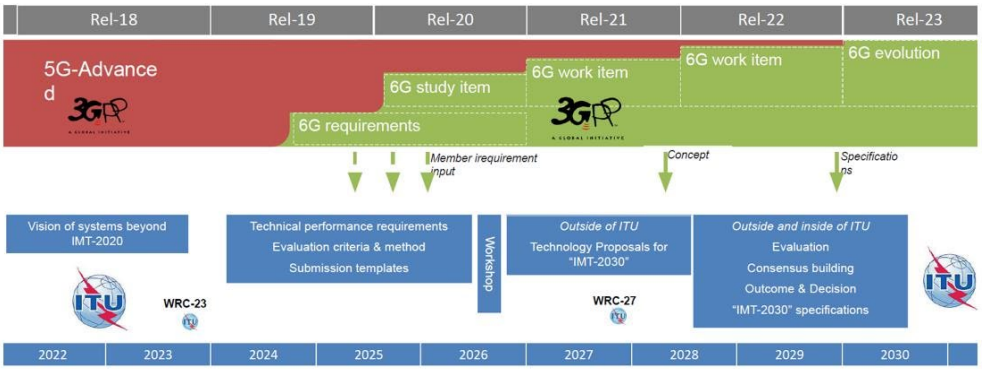


圖12、3GPP_6G 發展 Timelines
資料來源：印度 ITU-APT

4. 網際網路工程任務組(Internet Engineering Task Force, IETF)

IETF 成立於 1986 年，是一個開放的標準組織，負責開發和推廣自願網際網路標準，特別是構成網際互聯通信協議(Transmission Control Protocol/ Internet Protocol, TCP/IP)的標準。它沒有正式的會員資格或會員資格要求，所有參與者和經理都是志願者。IETF 最初是作為一項由美國聯邦政府支援的活動開始的，但自 1993 年以來，它在網際網路協會(Internet Society, ISoc)的支援下作為標準制定職能運作。

IETF 定義了安全自動化和持續監控架構(Security Automation and Continuous Monitoring, SACM)，支持基於實體或組件的協作 SACM 生態系統，這些實體或組件通過共享訊息進行通信。一個或多個組件是給定流中訊息的消費者，而一些組件是訊息的提供者。一個關鍵組件是一個協調器，它有助於實現各

種功能的自動化，例如 SACM 組件的配置、協調和管理。還可以有各種存儲庫，例如策略存儲庫、漏洞定義數據存儲庫和安全訊息存儲庫。

5. 5G 公私聯盟協會(The 5G Infrastructure Public-Private Partnership, 5G-PPP)

5G-PPP 是歐盟委員會和歐洲 ICT 行業(ICT 製造商、電信事業、服務提供商、中小企業和研究機構)之間的聯合倡議。5G-PPP 目前處於第三階段，許多新項目於 2018 年 6 月在布魯塞爾啟動。5G-PPP 將為未來十年無處不在的下一代通信基礎設施提供解決方案、架構、技術和標準。5G-PPP 面臨的挑戰，是確保歐洲在強大或有潛力創造新市場的特定領域的領導地位，例如智慧城市、電子醫療、智慧交通、教育或娛樂與媒體。5G-PPP 倡議將加強歐洲產業在全球市場上的成功競爭，並開闢新的創新機會，它將打開一個平台，以實現維護和加強全球技術領先地位的共同目標。

5G-PPP 成立了 5G-PPP 安全工作組，共同應對 5G 安全風險和挑戰，並提供對 5G 安全以及應如何解決的見解。它詳細闡述了 5G 安全架構及其與 3GPP 架構的契合度、訪問控制、隱私、信任、安全監控和管理以及 5G 安全的標準化。儘管它專注

於 5G，但該小組的成果對智慧網路安全、安全關鍵績效指標(Key Performance Indicators, KPI)、新興風險、威脅和對策等超越 5G 網路具有直接影響。

6. 電機電子工程師學會 IEEE

IEEE 前身是成立於 1884 年的美國電氣工程師協會(Aggregation-induced emission enhancement, AIEE)和成立於 1912 年的無線電工程師協會(Institute of Radio Engineers, IRE)。前者主要致力於有線通訊、光學以及動力系統的研究，而後者則是國際無線電領域不斷擴大的產物。20 世紀 30 年代，「電子學」這個詞開始進入工程學詞典。雖然許多工程師都同時是 AIEE 和 IRE 兩個協會的會員，但是新入行的電子工程師們還是更傾向於加入無線電工程師協會。兩個協會之間激烈的競爭的結果，造就雙方的合作與合併。1963 年 AIEE 和 IRE 宣布合併，IEEE 正式成立。

作為全球最大的專業技術組織，在電氣及電子工程、計算機及其他技術領域中，IEEE 出版了近三分之一的技術文獻，其中包括每年出版的 200 本期刊和雜誌，IEEEXplore 數字圖書館文

獻已超過 500 萬篇。配合各專業技術領域的學術交流活動，IEEE 還提供學報、技術通訊、會議論文集和會刊等出版物。

如今，隨著電子訊息和其他相關技術的不斷發展和演進，以及會員職業範圍的擴大和技術興趣的不斷增長，IEEE 也將其關注點不斷擴充至其他新興領域。IEEE 將努力幫助其會員跟上並引領新技術發展步伐，制定國際和行業標準，激勵新一代專業技術人員架構並融入全球技術協作團隊。更重要的是，隨著會員所在地域範圍的擴大，IEEE 已經日趨全球化，並在航空航天、生物科技、計算機工程、新能源、地理訊息系統、神經網路、無線通信等高科技領域的技術發展上，有卓著領先。

IEEE P1915.1 軟體定義網路(Software-Defined Networking, SDN)和網路功能虛擬化(Network Functions Virtualization, NFV)安全標準致力於提供一個框架來構建和運行安全的SDN/NFV環境。

它針對不同的利益相關者，例如最終用戶、網路電信事業和服務/內容提供商，指定了一個具有相關係統模型、分析和要求的安全框架。同樣，IEEE P1917.1 軟體定義網路和網路功能虛擬

化可靠性標準側重於可靠性要求，並為可靠的 SDN/NFV 服務交付基礎設施開發框架。

對於量子通信，軟體定義量子通信(Software Defined Quantum Communication, SDQC)的 IEEE P1913.1(草案)標準定義了 SDQC 協議，該協議支持在通信網路中配置量子端點。它允許在軟體定義的設置中動態新增、修改或刪除量子協議或應用程序。這可以通過定義明確的量子通信設備接口的可用性來實現，該接口可以重新配置以實現各種協議和測量。SDQC 協議在應用層起作用並通過 TCP/IP 進行通信，協議設計考慮未來與網路的集成軟體化相關標準。

(四)6G 技術應用型態的演化與各國主張

雖 6G 仍屬於初始階段，各國組織皆紛紛提出相關的 6G 技術應用的主張並逐步展開布局，為因應未來 6G 相關技術發展趨勢，將於下面章節研析 6G 應用技術型態的演化，並盤點各國主要機構之主張，了解國際動態，以利後續 6G 技術應用情境評估挑選、服務驗證評估以及合宜場域選取等相關推動。

1. 應用技術型態的演化

欲了解 6G 可能的發展應用及技術方向，必須觀察現有 5G 行動通訊標準的主責制訂機構 3GPP 中主要技術提案業者的展望看法。全面網路通訊協定(Internet Protocol, IP)化是 4G 行動通訊的一大特點。4G 由於傳輸率已大幅提升，不僅能滿足寬頻上網需求，甚至允許即時傳遞影音內容，故 4G 不再與 3G 相同只強調行動寬頻，而是強調「三網合一」(Triple Play)，亦即 4G 可以同時傳輸語音、寬頻以及視訊。Triple Play 為 4G 的初步應用主張，到了中後期也開始衍生出其他主張，例如過往以來行動通訊都重視在戶外、郊外通訊，畢竟行動通話多是在室外發生。但隨著寬頻上網日益普及後，在室內使用行動通訊的機會也增加，然原有的設計較不適合於室內用，為了強化室內通訊的能力，故提出「LTE 熱點/室內」LTE-Hi(Hotspot/indoor)的技術提案。

再者，LTE 亦提出「LTE 設備間就近型服務」LTE-D2D(Device-to-Device, D2D)，亦即讓行動電話對基地台發訊，基地台再廣播給相同覆蓋區內的鄰近區域，以此達到互助互利效果。例如某人暈倒了，需要醫護人員立即救助，此時附近的人可以上傳呼救訊息，基地台會立刻廣播給附近所有的人手機，讓鄰

近的醫護專業人員快速前往急救。同時 LTE-D2D 亦允許臨時拋售演唱會的票，或者就近找球友，或其他的就近型服務。LTE-D2D 之後也稱為「LTE 直接交談」(LTE-Direct)，因為 LTE-D2D 在上傳廣播訊息後，有意思進一步聯繫的人，是允許 LTE 手機與 LTE 手機直接交談，不再需要透過 LTE 基地台，因而得稱。

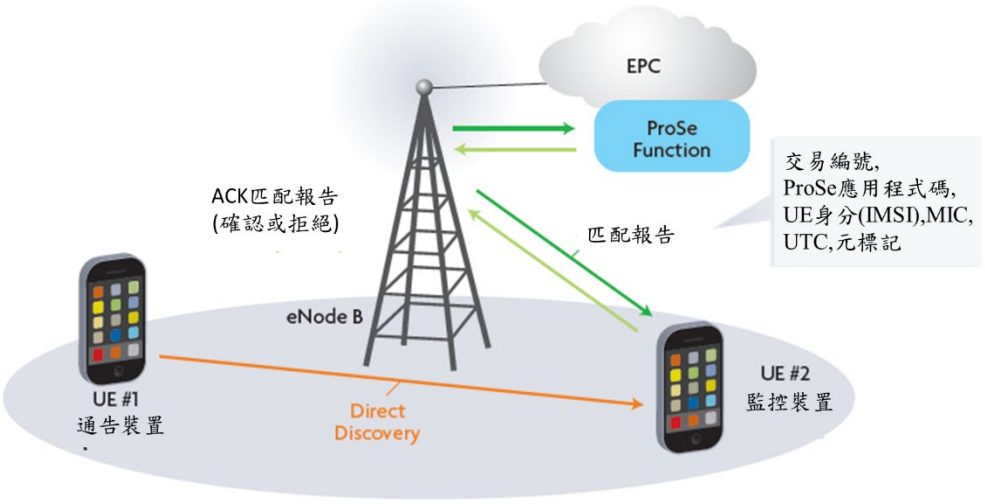


圖13、LTE-Direct 原理示意圖

資料來源：Device-to-Device Communications and Heterogeneous Structures in LTE networks,SRG

雖然 LTE-D2D/Direct 立意良善，功能也已經實現，但卻鮮少有電信營運商運用與開通此項服務，至多以關鍵要緊的緊急呼救為主，且非營利。

除了 LTE-Hi、LTE-Direct 外，還有所謂的 LTE-U(LTE-Unlicensed，Unlicensed 是指如 Wi-Fi 般使用不需要授權的頻段、波段)，主要是用來統合異質網路(Heterogeneous Networks,

HetNet)，例如控制信號的傳遞仍使用 LTE 基地台，但使用者的傳輸資料則改用短距、快速的 Wi-Fi 來傳遞，初期以下載資料為主，之後無論下載或上載均可運用 Wi-Fi 實現。此外 LTE-U 也有不同的運作模式，詳見圖 14：

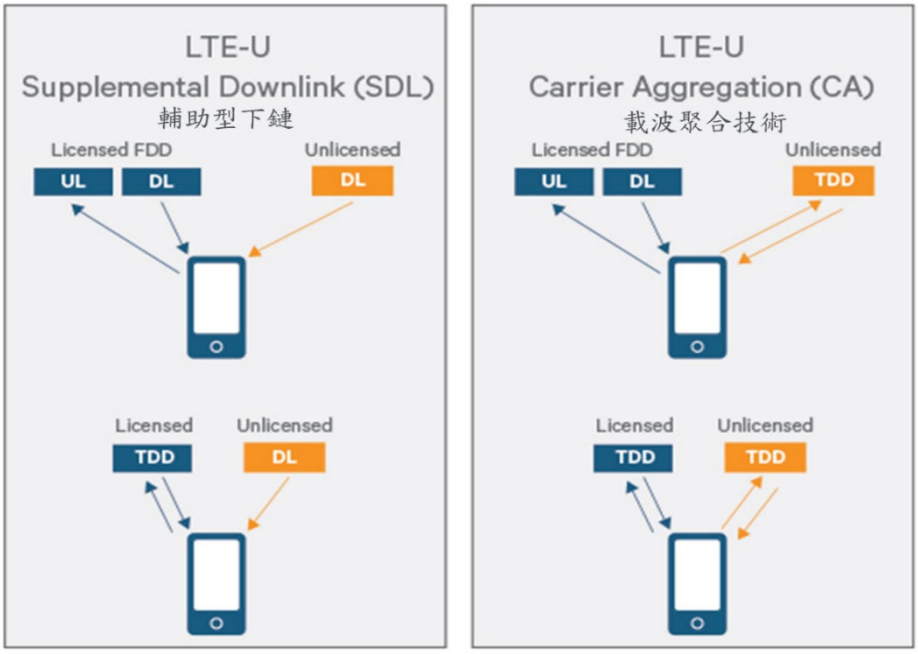


圖14、兩種 LTE-U 運作模式
資料來源：LTE in Unlicensed Spectrum Research，Qualcomm

無論是 LTE-Hi、LTE-Direct、LTE-U 等，都是以人們的手持式行動裝置為主要應用設想，但 LTE 中後期的另一項發展更為重要，即為機器型態通訊(Machine Type Communication, MTC)，稱為 LTE-MTC。

LTE-MTC 就其技術本質即為物聯網 IoT，亦即不是人們手持的裝置來與基地台互通，而是裝設在用品、物品、設備上的通訊裝

置來與基地台互通，例如智慧抄錶、智慧照明等，由電錶、電燈與 LTE 基地台通訊。

對於 LTE 的 MTC 技術，在發展初期即有兩種規劃，一種是在以相同覆蓋區內可以大量布建，但通訊裝置盡可能低功耗運作、盡可能長電池時間(battery life)運作，而不重視傳輸率、傳輸資料量、傳輸延遲，甚至不重視傳輸的正確性。此稱之為 Massive MTC。

另一種則是不重視相同面積的布建數量，也不重視資料傳輸量，但非常重視傳輸的即時性、傳輸正確性，用在非常重要的控制場合中，例如下令操作機器手臂、操控工控系統、無人搬運車(Automated Guided Vehicle, AGV)、多軸無人機等，或者是醫療設備、車聯網等應用，此一取向也被稱為 Critical MTC，詳如圖 15：

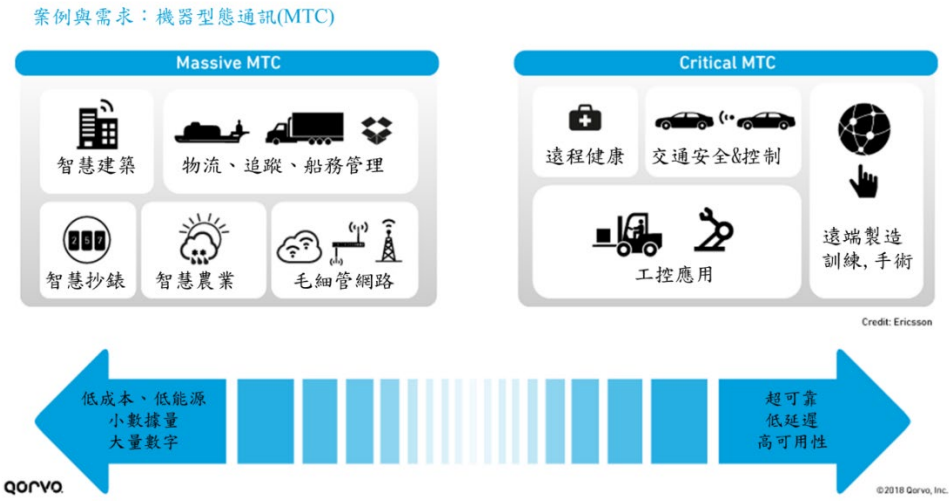


圖15、兩種不同型態的 LTE-MTC

資料來源：How NB-IoT and LTE-M Fit into the IoT Ecosystem: The Future of Cellular IoT，qorvo

了解 LTE-MTC 的兩大取向相當重要，因為 4G 之後的 5G，即是以原有的 3G、4G 以來的行動寬頻為基礎，再加上 4G 的兩種取向 MTC 所構成，成為 5G 的三大支柱。

原有的行動寬頻在 5G 時改稱為「增強型行動寬頻通訊」eMBB，其中 e 即為 enhanced 強化之意，有部分資料則認定為 extreme 極致或 evolved 進化，以便有別於原有的 4G/LTE 所言的「行動寬頻通訊」(Mobile Broadband, MBB)；而 Massive MTC 則不變，並縮寫成 eMTC；至於 Critical MTC 則改名為「超可靠低延遲通信」URLLC。

所謂的超可靠是指傳輸的資料高度講究正確性，一旦傳輸的資料有誤，不僅必須能夠偵測出錯誤，還必須能自行更正錯誤，若無法自行更正錯誤，則必須能對發送發要求重新傳遞內容。同時錯誤率(error-rate)也必須盡可能降低，目標為 10 的負 9 次方，亦即每 10 億次只能有 1 次出錯。

而所謂的超低延遲即在於要求傳輸的時效，此方面依據不同的應用也有不同的時效要求，例如無人搬運車允許 15mS～20mS(毫秒，意指千分之一秒)的傳輸延遲；智慧電網(Smart Grid)則較嚴苛，

只允許 3mS～5mS 的延遲；至於工廠自動化則只允許 1mS 內的延遲。有關 5G 三大支柱詳如圖 16：

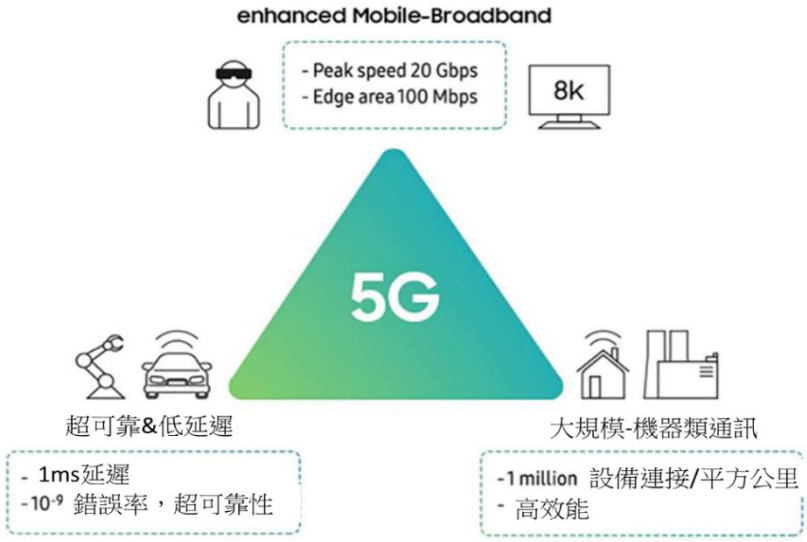


圖16、5G 行動通訊的三大支柱
資料來源： 5G Is Now, Part 1: 2018, the Year of 5G，Samsung

2. 新的應用技術型態的主張

5G 確定三大取向的通訊型態後，更後續的 B5G、Pre-6G 以及 6G 等，將以 5G 為基礎持續擴展延伸，畢竟 3G 時代大體維持單一型態，4G 時代區分出 MTC 的另一種型態，5G 成為三足鼎立的形態，B5G/Pre-6G/6G 持續增加新型態自屬必然。不過，新的擴展延伸方向目前尚未有共識，而是各業者各有主張，以下舉數種常見的主張提案。

一是電子通信研究院(Electronics and Telecommunications Research Institute, ETRI)的看法，主張後續發展應持續與三大支

柱為基礎，沿線持續開展新的技術應用型態，例如在 mMTC 與 eMBB 間應當可以為智慧城市的攝影機再設立一種技術應用型態，或者在 URLLC 與 eMBB 間也可以再設立若干種技術應用型態，如產業與載具自動化，或增強實境/擴增實境等，詳見圖 17：

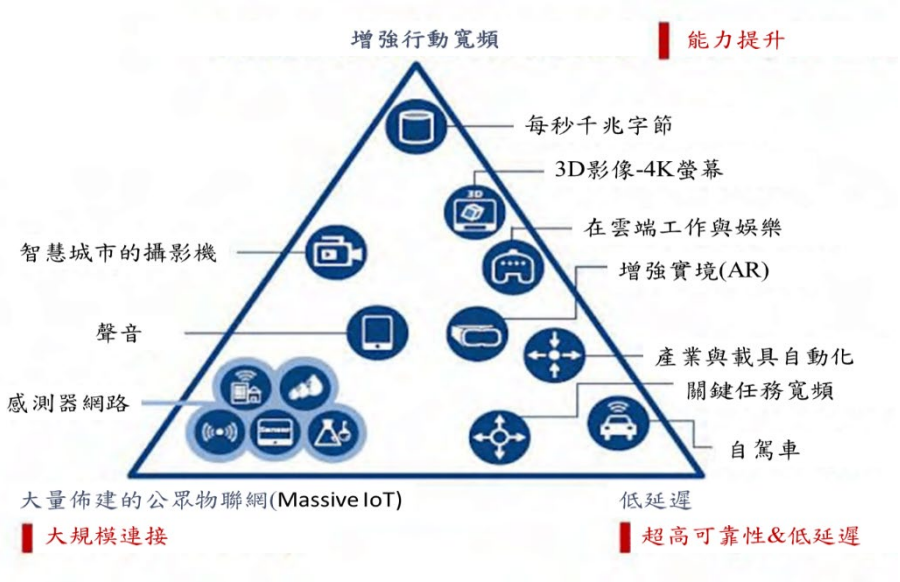


圖17、5G 三大支柱衍生新技術應用型態
資料來源：5G Technology and Its Applications to Music Education，ETRI

二是華為(Huawei)在 2020 年提出的 5.5G(或可認定為 B5G)構想，以原有 5G 三角為基礎再展開另三個角，成為六角形，新增的三類型分別為寬頻即時通訊(Real-Time Broadband Communication, RTBC)、上行超寬頻(Uplink Centric Broadband Communication, UCBC)以及感知定位(Harmonized Communication and Sensing, HCS)。

加入的三要素也分別有其特性訴求，例如 UCBC 重視高清晰度視訊影像的上傳以及機器視覺等應用，HCS 則更重視車聯網以及定位應用。此外也加入兩項重點訴求，一是加入人工智慧，另一則是運作的波段頻譜超過 100GHz，詳見圖 18：

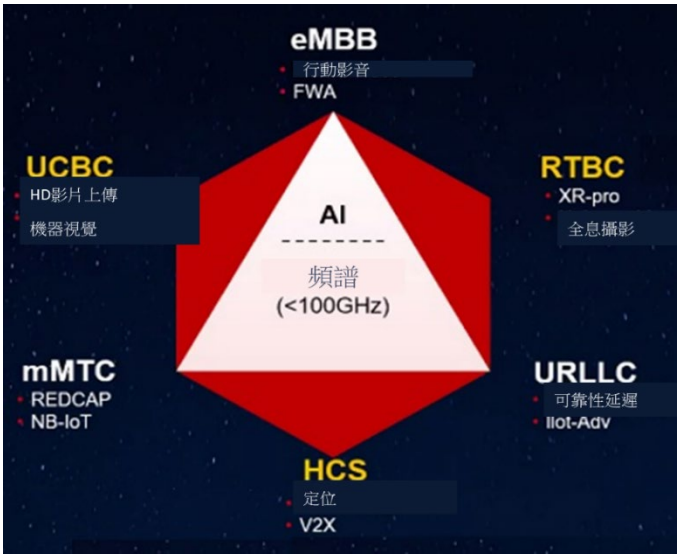


圖18、華為主張5.5G 的六大支柱
資料來源：2020 MBBF，華為，本計畫整理

三是阿布都拉國王科技大學(King Abdullah University of Science and Technology)所提出，該大學為沙烏地阿拉伯的研究型大學，該大學於 2019 年 11 月發表一篇名為《What should 6G be?》的專文中提到五種6G技術型態，同樣是以原有三大支柱衍生而成，詳見圖 19：

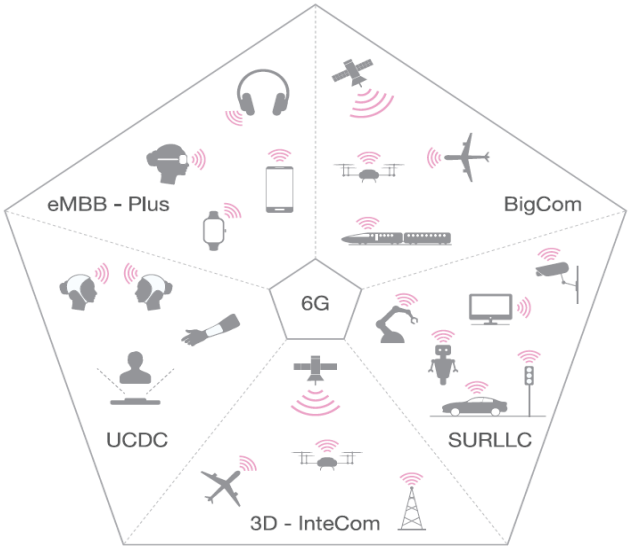


圖19、五種6G 技術應用型態的主張
資料來源：What should 6G be?，阿布都拉國王科技大學

阿布都拉國王科技大學認為 eMBB 與 URLLC 應持續擴充，成為 eMBB - Plus 與 SURLLC(此處的 S 為安全防護 Secure 之意)，但 mMTC 則進行更細部的分拆，例如有更針對穿戴式需求的「非常規數據通訊」(Unconventional Data Communications, UCDC)，或是更高遠快速移動需要的「大型通訊」(Big Communications，BigCom)，或是以三維通訊維設想的「三維整合通訊」(Three-Dimensional Integrated Communications, 3D- InteCom)。

四是日本知名行動通訊營運商 NTT DOCOMO(前身為日本國營企業的日本電信電話株式會社，類同於我國中華電信)，NTT DOCOMO 於 2020 年發表的白皮書《5G Evolution and 6G》中主張，6G 技術應用型態當以 5G 三大支柱為基礎展開，但不需要限

制其發展維度，而是向各維度開展，依據各種實務與特定應用需求更加深強化，從而成為新的確立型態，詳見圖 20：

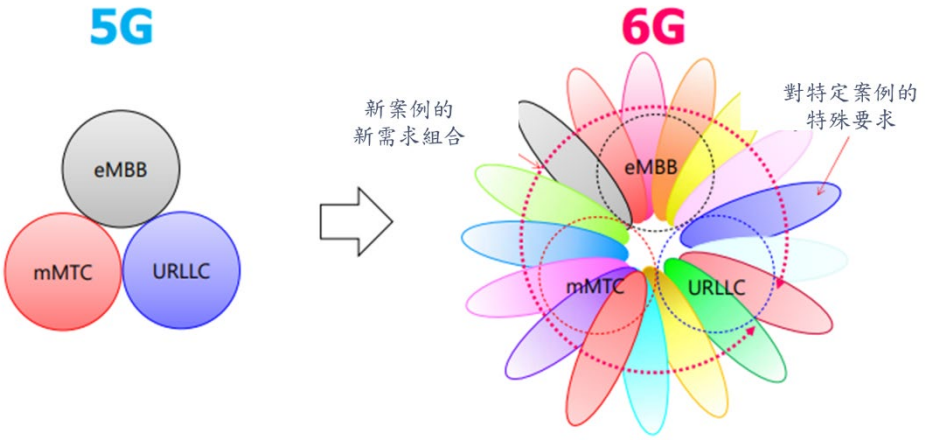


圖20、6G 應全向位開展技術型態的主張
資料來源：5G Evolution and 6G White Paper，NTT DOCOMO

五是華為於 2021 年提出其 6G 主張，有別於此前 5.5G 的六角形主張，改為金字塔型態的立體五主張，原有 5G 中的 eMBB、mMTC、ULRRC 於 6G 統統保留，但從三端點變成四端點，再加入感測 Sensing，而後再加入一個更高位階的人工智慧 AI，形成其主張的連接智慧，詳見圖 21：

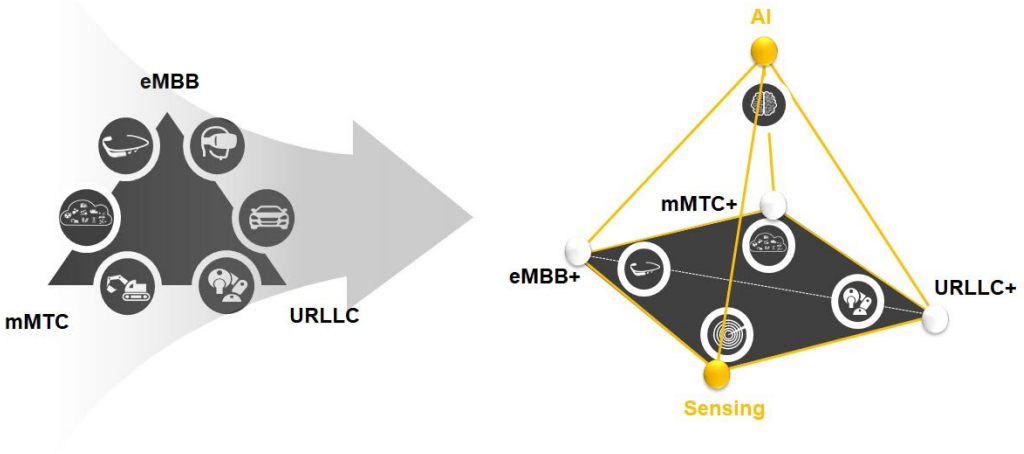


圖21、華為6G 技術型態主張
資料來源：《6G：無限通信新征程》新書發布，華為

六是同屬 ETRI 轄下的未來行動通訊研究部的 6G 無線傳輸研究科的總監 Young-Jo Ko(南韓人)博士於 2020 年所提，他認為 mMTC、eMBB、URLLC 該轉化成六個使用要素(usage element)，分別是 Ultra broadband、Ultra large coverage、Ultra massive connectivity、Ultra low energy、Ultra high precision 以及 Ultra high mobility 等。

然後同樣以立體方式加入一個共通要點，稱為無所不在的智慧(Ubiquitous Intelligence)，此類似呼應華為提出的 AI 頂點主張，差別在於華為對 5G 三要素不進行改動，而是追加，但此一主張傾向對原有三支柱進行更多的要素分拆，詳見圖 22：

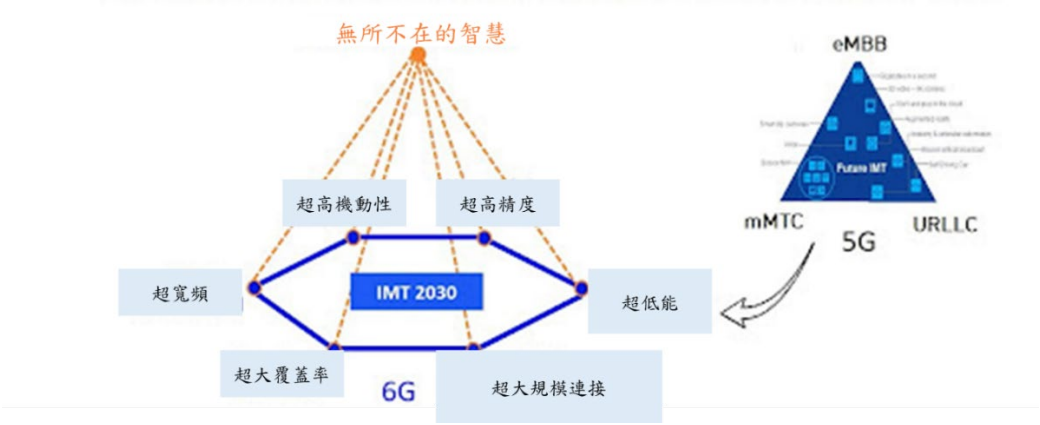


圖22、Young-Jo Ko 博士的6G 技術型態主張
資料來源：ETRI，本計畫整理

此外，2021 年 IEEE 專文《6G Ecosystem: Current Status and Future Perspective》，除保留 URLLC 外，原有的 eMBB、mMTC 將有更多延伸或拆解，例如 feUMBB、uHEE、uHDD、uHSLo、uHS、uHUx 等，而後也有相互重疊處，如 uHRS、uLLRS，以及 uHRUx 等，同時也將人工智慧列入不可或缺的要項，雖然在描繪上人工智慧並非如華為、Young-Jo Ko 博士般將人工智慧至於立體性的頂點位置，但卻週遍在所有的技術型態要項上，也等同於頂點位置，詳見圖 23：

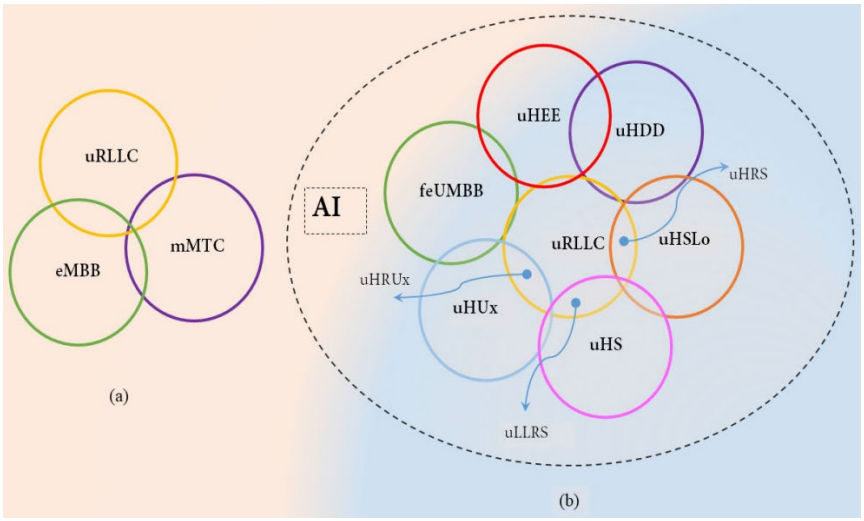


圖23、自5G 的三要項(a)擴展成6G 的多要項(b)
資料來源：6G Ecosystem: Current Status and Future Perspective，IEEE

3. 主要機構之應用主張

由於 6G 仍在前期階段，諸多機構對 6G 應用有各自的看法與主張，如量測儀器業者羅德史瓦茲(Rohde & Schwarz, R&S)認為 6G 將使 5G 的全像投影提升為大規模、高傳真度的全像投影，或者有運用能量採集(或稱能源收割)或無線電力傳輸運作的超低功率通訊，或可安裝於衣物布料內，或可嵌入到塑膠或玻璃中運用。

我國聯發科技(MediaTek)於 2022 年 1 月提出的《6G 願景白皮書》中提到極致的全息影像通訊(holographic communication)、觸覺通訊、數位分身(digital twin、avatar)、進階的遠距臨場技術(telepresence)等。

無獨有偶的，美國維吉尼亞理工學院與州立大學與芬蘭奧盧(Oulu)大學、普林斯頓大學的共同學術文章中所提的多感官體驗(Multisensory XR)、連接機器人與自主系統(Connected Robotics and Autonomous Systems, CRAS)、無線腦機互動(wireless Brain-Computer Interactions, BCI)、區塊鏈與分散式帳本技術(blockchain and Distributed Ledger Technologies, DLT)等，詳見圖 24「6G：推動應用」部分。

圖24、6G 願景：應用、趨勢及技術
資料來源：維吉尼亞大學，本計畫整理

除此之外，電機電子工程師學會 IEEE 的多名院士於 2021 年 7 月共同發表的研究專文《6G Wireless Systems: Vision, Requirements, Challenges, Insights, and Opportunities》提及十餘項應用，詳如圖 25：

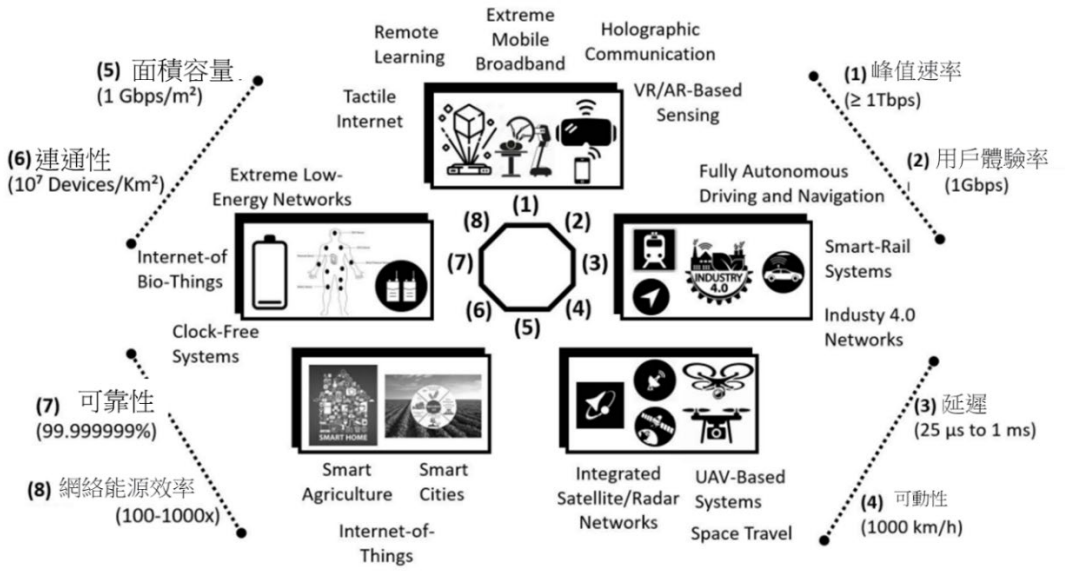


圖25、6G 系統及其發展中的應用等願景

資料來源：IEEE，本計畫整理

圖 25 外側 8 點是 6G 的通訊特性，內則是各種可能的應用，分別為：觸覺網路、遠端學習、極致的行動寬頻、全像通訊、虛擬實境 VR/增強現實 AR 為基礎的感測、智慧軌道系統、工業 4.0 網路、無人機為基礎的系統、整合衛星/雷達網路、整合衛星/雷達網路、太空旅遊、智慧城市、智慧農業、物聯網、免時脈系統、生物連網、極致低能源網路等。

以下便針對全球各主要機構提出的 6G 主張做說明：

(1)美國-次世代聯盟(NextG Alliance)

美國電信產業標準聯盟 ATIS 擁有 150 家成員公司，其會員包括各種電信服務提供商、設備製造商和供應商，如亞馬遜、蘋果、愛立信、Meta、思科系統、Google、三星等名大廠商。該組

織包括眾多的委員會和論壇，討論有關網路安全、網路可靠性、技術互操作性、緊急服務、計費等主題的指南和網路功能虛擬化等相關議題。

2020 年 10 月由美國電信產業標準聯盟結合了北美主要電信業者、國際系統設備大廠成立 Next G 聯盟。其成立之目的，是在未來 6G 的發展過程中，確保北美在塑造新一代無線通訊技術研發、標準化、網路架構、系統設備及其最終應用部署等，取得全球性的領導地位。Next G 聯盟匯集了北美各產業界、學術界和政府等重要廠商及單位，共同製定 6G 願景和藍圖。

有關 Next G 所規劃的6G 願景分別為「強化安全性防護」、「實現多重感官體驗」、「更具成本效益的網路架構」、「虛擬化技術應用」、「人工智慧原生」及「環保議題」六個面向，以下針對上述六個面向進行說明：

A. 強化安全性防護：6G 將強化網路的信任、安全性、隱私保護和彈性各方面的的效益，讓民眾、企業和政府可以完全的信任。而 Next G 此一議題提出四個關鍵目標：

a. 服務可用性：6G 系統和未來的系統設計應在工業和社會中負起重要的角色。

b. 安全和隱私：5G Advanced 和6G 之間的一個顯著區別將是網路中用戶可程式(User-Programable)行為的可用性，專有或個人訊息可能暴露給底層計算系統。

c. 資料保護：不僅要保護傳輸中的資料，還要保護靜止和使用中的資料。

d. 網路和服務的彈性：服務需要創新的方法來從各種試圖破壞網路的可用性、完整性或安全性的干擾以及阻斷服務(Denial of Service, DoS)攻擊甚至因設備故障或操作錯誤所引起的作業失敗和錯誤中恢復。

B. 實現多重感官體驗：未來由多種感官體驗(multi-sensory experiences)組成的增強型數位世界，實現新型的協作形式，以及人機交互和機器交互，這些變革將可以提升生活的品質，創造更多新的經濟價值。

其中，數位世界體驗(Digital World Experience, DWE)包含各種改變人類互動的多感官體驗，跨越實體、數位和生物世界，創新的人機界面和機器間通信產生的協同作用，是更具表現力的數位世界體驗交互互動。人際應用程序數位世界體驗可以提高日常生活質量(如在

朋友或家人互動中實現情感交流)、體驗質量(如增強多用戶遊戲組中的共享體驗)。通過利用混合實境顯示，數位世界體驗可以在讓人們以他們選擇的任何方式隨時隨地出現。

另一個提高生活質量或關鍵角色的數位世界體驗的例子，是將遙感、觸覺反饋和驅動相結合，以實現與遠處或難以接近的物體的延展實境互動。其使用情境可能發生在遠端手術的情況下或工業技術人員無法獲得到場動手修理故障機器的狀況下。

C. 更具成本效益的網路架構：在設備、無線連接、基地台、整體分佈和能源消耗等網路架構議題提出更具有成本效益的解決方案，以因應包括城市、農村和郊區等未來各種使用環境中可提供適當服務，同時在未來網路服務還支援更高的資料傳輸速度。

D. 虛擬化技術應用：基於虛擬化技術構建分散式雲和通信系統，提高應用提供靈活性、性能和彈性，可支援如混合實境(Mixed Reality, MR)、互動性遊戲和多感官應用程序等關鍵應用。

E. 人工智慧原生：6G 需要一個人工智慧原生(AI-native)網路，以因應更多樣化的流量類型、超密集部署的網路拓撲和更具挑戰性的頻譜情況。6G 中所謂的人工智慧原生系統將利用各種人工智慧技術，如機器學習 Machine Learning、深度學習 Deep Learning、類神經網路等來設計、部署、管理和操作各種6G 網路和設備功能。在人工智慧的技術協助下，可以提高系統穩健性、性能和效率，從而帶來龐大的經濟效益及影響。

F. 環保議題：通訊的能源效率和環境保護應用需達到所謂IMT 2040年碳中和目標。因應全球氣候變遷的挑戰和減少碳足跡的需要，6G 網路架構應該最節能的技術、減少對不可再生能源的依賴，儘量使用再生能源和環境能源。

Next G 所規劃的 6G 願景每個大項中，有更細項的具體應用，圖 26 即為多感知延伸現實應用的情境之一，更詳盡的應用說明可參閱「三、計畫執行情形-跨領域應用情境研析」之「6G 跨領域應用關鍵技術」章節。

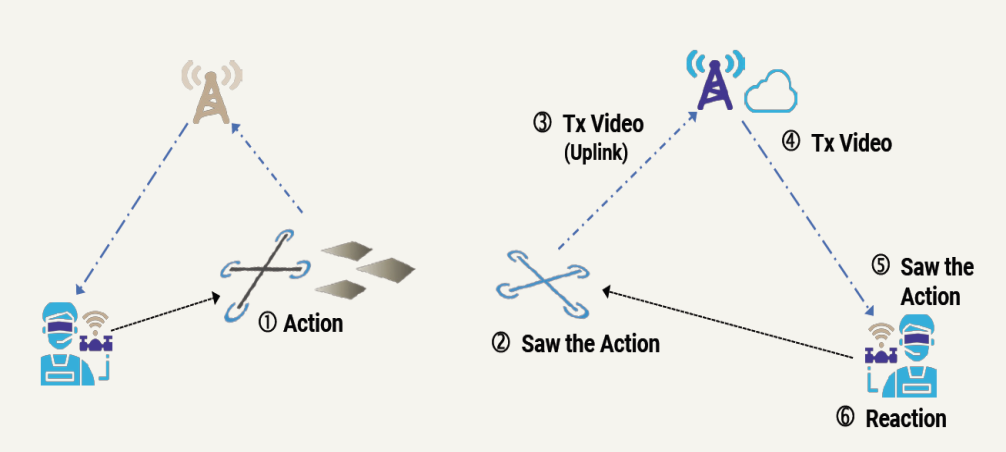


圖26、多感知延伸現實應用-無人機超現實互動情境
資料來源：Next G Alliance

(2) NGMN 聯盟(NGMN Alliance)

以各國行動通訊營運商為主所構成的 NGMN 聯盟，在 2022 年 2 月發布的 1.0 版《6G Use Cases and Analysis》中將 6G 應用分成四大類別，分別是強化的人類通訊(Enhanced Human Communication)、強化的機器通訊(Enhanced Machine Communication)、啟動服務(Enabling Services)、網路演化(Network Evolution)，各大類中也細分出多項潛在的一般性應用例子，詳如圖 27：

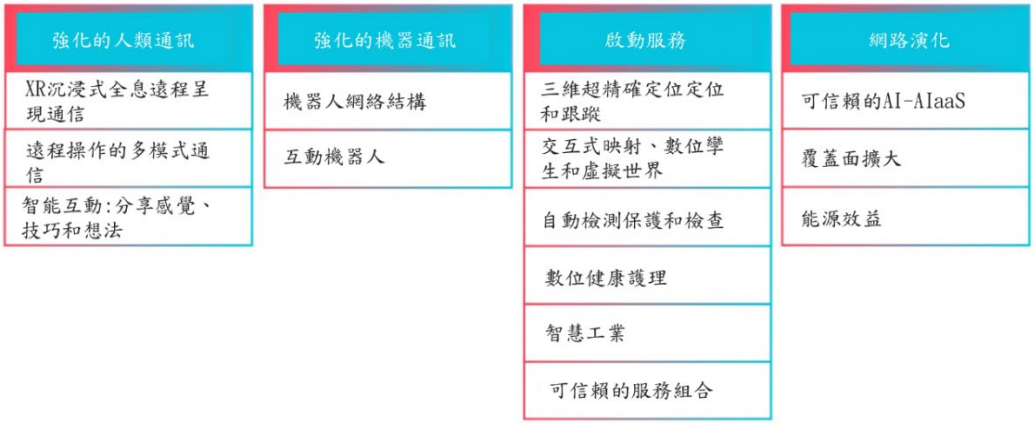


圖27、NGMN 主張的6G 應用類別與潛在應用案例
資料來源：NGMN Alliance，本計畫整理

(3) 歐盟 Hexa-X 計畫

歐盟執委會 EC 於 2021 年 1 月 1 日正式啟動 Hexa-X 計畫，該計畫包含多項 6G 發展內容，如找尋 6G 發展的主要趨力、6G 發展的技術挑戰等，同時也包含 6G 新應用的探索。

Hexa-X 計畫也獲得 Horizon 2020 的資助。Hexa-X 計畫的成員多數為歐洲業者，如芬蘭諾基亞(Nokia)、瑞典愛立信(Ericsson)、法國電信營運商 Orange、德國西門子(Siemens)等，然英特爾(Intel)也在列。

Hexa-X 對於應用情境有 5 大主張，並在各主張下分別舉出 3～7 個應用案例，5 大主張分別為永續發展(Sustainable development)、大量雙生結對(Massive twinning)、遙傳至現場(Telepresence，更早先的文件稱為強化互動的沉浸式遙傳至現

場 Immersive telepresence for enhanced interactions)、機器人到協作機器人(Robots to cobots)，以及在地信任地帶(Local Trust Zones)。Hexa-X 計畫期待可以達成「加速和促進 6G 研究，並推動歐洲在 6G 時代的領先地位」。

歐盟委員會目前也已宣布創建 Hexa-X-II 計畫，為歐洲 6G 旗艦計劃的第二階段。此一新階段將把 原本 Hexa-X 合作夥伴名單擴大到 44 個組織，這些成員領域包含網路供應商和通訊服務提供商，進而到技術提供商以及歐洲通信研究機構。這些組織的任務是預先創建標準化的平台和系統規劃，這將為未來 6G 標準化的許多投入奠定基礎。

(4)德國-諾基亞貝爾實驗室

諾基亞貝爾實驗室正在領導由德國資助的 6G-ANNA 計畫，旨在從德國和歐洲的角度推動 6G 網路技術的全球預備研究和標準化工作。「德國 6G 平台(6G Platform German)」的資金來自德國聯邦教育及研究部(Bundesministerium für Bildung und Forschung, BMBF)。諾基亞表示，將與其他各方密切合作，包括 Vodafone、Siemens、Ericsson、Bosch，以及眾多小型供應商、

研究機構和大學。其願景是認為 6G 將即時連結數位世界、實際世界與生物世界。

諾基亞貝爾實驗室除了提出奠定 6G 無線系統技術基礎的六大挑戰，包含「智慧連結(Connecting Intelligence)」、「網路中的網路(Network of Networks)」、「永續性(Sustainability)」、「全球服務涵蓋(Global Service Coverage)」、「極致體驗(Extreme Experience)」及「可信任度 (Trustworthiness)」，亦認為有六項技術將會成為未來 6G 網路的重要組成技術，分別為「AI 與機器學習」、「利用新頻譜」、「定位精度」、「逼近網路極限」、「新型網路架構」以及「資安、隱私與信任」。

(5)芬蘭-奧盧 Oulu 大學 6G 旗艦(6G Flagship)

2018 年 4 月芬蘭 Oulu 大學首先以「支持 6G 的無線智慧社會與生態系統(6Genesis)」為主題，成為芬蘭科學院國家研究資助計畫中的旗艦研究項目，獲得 8 年 2.5 億歐元的研究資金(2018-2026)，同年 5 月正式啟動 6G 旗艦研究計畫。目前已有至少 75 家產、學、研機構參與研究，而其中主要合作夥伴為阿爾托大學、奧盧應用科學大學、諾基亞和芬蘭 VTT 技術研究中

心和 InterDigital。他們所期 2030 年願景：「未來社會是數據驅動，通過近乎無限的無線連接實現」。

其所提的戰略研究領域，包括無線連結、元件與半導體技術、分散式運算(含增強型人工智慧協作)、新興應用服務等四大領域。

該計畫於 2019 年 9 月由 75 名專家合作，發表全球第一版 6G 白皮書：「Key Drivers and Research Challenges for 6G Ubiquitous Wireless Intelligence」，該 6G 白皮書七大主題分列如下：

A. 6G 社會與商業驅動力

B. 6G 使用案例與新設備形式

C. 6G 頻譜與 KPI 目標

D. 無線網路硬體的進步與挑戰

E. 物理層與無線系統

F. 6G 網際網路

G. 新服務啟用

有關 6G 關鍵績效指標之設定，在技術和生產力驅動的關鍵績效主要有：延遲率、時基誤差、鏈路預算、擴展範圍/覆蓋範圍

(包含衛星)、3D 投影準確度、基於既有 5G 指標調整的 KPIs(包含行動寬頻)、位置精度與更新率、成本及能源。

而另一層面有關非技術之可持續發展和社會驅動的關鍵績效指標，主要為在技術要求與標準化的定義裡頭將垂直參與者納入其中、透明度 KPIs (如與 AI 相關)、隱私/安全/信任、面向全球用例的 APIs、 受聯合國可持續發展目標(UN SDG)啟發之 KPIs、一切可開源、針對倫理道德的 KPI。

2019 年 11 月，芬蘭 Oulu 大學廣泛討論使 6G 得以實現所需且最受期待的技術元件組合，設定了 12 項特定領域，分別為：

A. 6G 的驅動因素和聯合國可持續發展的目標(6G Drivers and the UN SDGs)
B. 針對2030年垂直產業的驗證及試驗(Validation and Trials for Verticals towards to 2030's)
C. 無線網路上的機器學習(Machine Learning on Wireless Communication Network)
D. 聯網(Networking)
E. 6G 中的寬頻聯接(Broadband on Connectivity in 6G)
F. 射頻與頻譜(RF & Spectrum)
G. 偏遠地區互聯互通(Connectivity on Remote Areas)
H. 6G 商用(Bussiness on 6G)

I. 邊緣智能(Edge Intelligence)

J. 信任、安全和隱私的研究挑戰(Research Challenges for Trust,Security and Privacy)

K. 針對6G 的關鍵和大規模機器通信(Critical and Massive Machne Type Communication toward 6G)

L. 定位與感知(Localization and Sensing)

Oulu 大學對於未來 6G 的應用服務使用情境，認為智慧型手機雖然已是生活中不可或缺的一部分，但是根據預測新的顯示技術、感知和成像設備以及低功耗專用處理器的快速發展，正在開創一個新興應用服務時代，使用者的設備將與感官和運動控制無縫聚合在一起。

VR、AR 和 MR 技術正在融入 XR 的技術中，其中包括可創建和維持感知的可穿戴顯示器機制。增強用戶使用媒體、搜索網際網路、探索現實和虛擬世界、在工作項目上協同作業、與家人和朋友聯繫以及參與各種活動的能力。

(6)南韓-科學技術情報通信部

南韓科學技術情報通信部(Ministry of Science and ICT., MSIT)於 2018 年 9 月啟動「6G 核心技術項目」的初步可行性研究。主要透過蒐集來自產、學、研等機構的 100 名專家之意見，

且舉辦公開聽證會瞭解各方意見，確定 6G 技術項目的基本方向與後續關鍵任務。

南韓於 2019 年 4 月開始 6G 布局，南韓通信與資訊科學研究院首先召開 6G 論壇，開始研究並組建了 6G 研究小組，以開發 6G 核心技術並定義 6G 應用場景。隨後，7 月南韓科學技術情報通信部規劃在 2020 年正式提出「6G 研發初步可行性研究計畫」，由韓國科技規劃評價院負責。

2020 年 8 月 6 日南韓政府舉辦第十二屆科技部長會議中，敲定「引領 6G 時代的未來移動通信研發促進戰略」，並以成為「6G 時代的領先者」為願景、將「達成 6G 全球商用首發，確保核心技術、完備主導 6G 全球市場的基礎」策略目標，規劃南韓於 2026 年進行 6G 試驗，並於 2028 年或 2030 年開始推動 6G 商用化服務。為此，南韓政府初期規劃在 2021 年起 5 年間投入至少 2,000 億韓元，以支持 6G 技術的研發以及關聯產業生態系統之建構。

(7)南韓三星

南韓三星發表一份「全民下一代超連結體驗」的 6G 白皮書，勾勒其對於 6G 通訊技術及場景未來的願景，期待將下一個超連

結體驗帶入生活的每個角落。該份白皮書涵蓋 6G 的各項層面，包括技術與社會趨勢、創新服務、規範、候選技術以及標準化的預定時程。

在該份白皮書中，預估 6G 網路最快將於 2028 年完成標準制定與商業化，並於 2030 年起實現大規模商轉，屆時不單單是人類，還包含機器都將成為 6G 網路的主要使用者，進而實現一系列的前瞻服務。

三星認為要成功實現 6G 服務，須同時滿足效能、架構與可靠性三大需求。而該白皮書中提及「真正的沈浸式延展實境」、「高度逼真的行動顯示」、「數位複製」3 種應用將在「三. 計畫執行情形-跨領域應用情境研析」之「(二)6G 跨領域應用關鍵技術」章節做更詳細的說明。

(8) 中國大陸 IMT-2030(6G)推進組

IMT-2030(6G)推進組於 2019 年 6 月由中國工業和信息化部推動成立，組織架構源自於 IMT-2020(5G)推進組，成員包括中國主要的 5G 相關產業的電信事業、製造商、大學和研究機構。推進組是聚合產官學研相關單位的能量，推動中國大陸第六代行動通訊技術研究，並開展國際交流與合作的主要平台。

IMT-2030(6G)於 2021 年 6 月推出了「6G 總體願景與潛在關鍵技術白皮書」，內容提到對於 2030 年及未來的願景，人類社會變化趨勢將進入智慧化時代，社會服務均衡化、高端化，社會治理科學化、精準化，社會發展綠色化、節能化。

網路資訊的應用將從行動互聯，到萬物互聯，再演進至萬物智聯，而 6G 將實現從服務於人、人與物，到支持智慧個體高效聯接的變動。未來在數學、物理、材料、生物等多類基礎學科的創新驅動下，6G 將與先進計算、巨量資料、人工智慧、區塊鏈等資訊技術交叉融合，實現通訊與感知、計算、控制的深度結合，成為服務生活、智能生產、綠色發展的基本要素。

6G 將實現網路全球式無縫覆蓋的境界，隨時隨地滿足安全可靠的「人、機、物」無限連接的需求。也將提供完全沉浸式交互場景，支持精確的空間互動，滿足人類在多重感官、甚至情感和意識層面的聯通交互，也將協助實現真實環境中實體的數位化和智慧化的成型，最大化的提升資訊通訊服務的品質。此一環境將可構建人機物智慧互聯、智慧體高效互通的新型態網路，在大幅提升網路能力的基礎上，具備人工智慧原生、多維感知、數位分身、安全內生等新功能。

《6G 總體願景與潛在關鍵技術白皮書》提及應用的 3 項特性(智慧化、沉浸化、全域化)及 8 種應用，如下所列：

A. 沉浸式雲端延伸現實：虛擬空間的廣闊天地

B. 全息通信：身臨其境的極致體驗

C. 感官互聯：多維感官的交融回應

D. 智慧交互：情感思維的互通互動

E. 通信感知：融合通信的功能拓展

F. 普惠智能：無處不在的智慧內核

G. 數字分身：物理世界的數位鏡像

H. 全域覆蓋：無縫立體的超級連接

圖28、6G 潛在業務應用場景
資料來源：6G 總體願景與潛在關鍵技術白皮書

(9)中國大陸-中國移動

中國移動在 2022 年發布「中國移動 6G 網絡架構技術白皮書」，強調所謂 6G 網路是通信技術、資訊技術、大數據技術、人工智慧技術、控制技術深度融合的新一代行動通訊系統，其特徵表現為跨學科、跨領域的應用。其內容描述提到 6G 網路架構設計理念，建議有 10 項狀況需要考量，包含：

A. 雲端化/服務化/開放協定是5G 架構的精神。

B. 支援天地一體、元宇宙等新技術和新場景。

C. 需要更好地服務產業互聯網的確定性、服務級別協定(service-level agreement, SLA)保障等需求。

D. 6G 架構不僅僅是通訊架構，而是通訊、感知、計算等的融合架構。

E. 連接密度、流量等需求將指數增長。

F. 分佈更廣、更加開放的網路內呈現非信任關係。

G. 網路領域複雜，網路規模巨大，網路流量豐富。

H. 6G 網路將涉及更多領域，引入更多能量，以提供更強的性能。

I. 2/3G 的逐步退出，將為6G 網路設計提供更簡潔的環境和基礎。

J. 接入網的集中化、服務化和核心網的分佈化為領域間融合提供了契機。

(10) 中國大陸-賽迪智庫無線電管理研究所

賽迪智庫是中國工業和資訊化領域的智庫，直屬於國家工業和資訊化部中國電子資訊產業發展研究院。該智庫於 2020 年 3 月發布「6G 概念及願景白皮書」，從網路聯結的方式看，6G 將會是包含多樣化的網路，如行動蜂巢網路、衛星通訊、無人機通訊、高空平台、可見光通訊等多種網路連接方式。從網路覆蓋範圍看，6G 的願景下期可構建跨地域、跨空域、跨海域的全球無縫覆蓋網路。從網路性能指標看，6G 無論是傳輸速率、點到點延遲、可靠性、連接數密度、頻譜效率、網路能效等方面都會有大的提升，從而滿足各種垂直行業多樣化的網路需求。

就網路智慧化的程度觀之，6G 願景下網路和使用者將整合為一體，人工智慧內嵌於 6G 網路核心，可深入挖掘用戶的智能的需求，每個使用者都將經由 AI 助理提升使用者的體驗。從網路服務的邊界看，6G 的服務對象將從實際世界的人、機、物拓展至虛擬世界的「境」，透過實際世界和虛擬世界的連結，實現人、機、物、境的協作，滿足人類精神和物質層面的全方位需求。

(11) 日本-NTT DoCoMo

日本知名行動通訊營運商 NTT DOCOMO 已多次發表「6G 白皮書」，以 2022 年 1 月的最新版 4.0 為例，在章節 4.4 中提及 6G 時代的潛在應用案例，例如讓虛擬與現實無縫接軌(Seamless Real and Virtual)、時間限制的擺脫(Freed from location and time constraints)等，詳如圖 29：

圖29、NTT DOCOMO 6G 白皮書主張的應用案例
資料來源：NTT DOCOMO，本計畫整理

日本政府計畫以與民間廠商共同合作的方式，規劃在2030年實現比5G 通訊速度快10倍以上的「後5G」(6G)技術的綜合戰略。其應用上的目標是期待6G 能夠扮演連接虛擬空間和實體空間的神經系統，進而實現超智能的社會。

(12) 其他潛在應用推演

其他與 6G 相關的產業聯盟，如無線世界研究論壇(Wireless World Research Forum, WWRF)、高海拔平台站(High Altitude Platform Stations, HAPS)聯盟、日本 Beyond 5G 推廣協會、one6G 協會等，也多對 6G 應用發表其看法與主張。

例如 one6G 協會於 2022 年 6 月發表的 6G 垂直應用白皮書「one6G white paper, 6G Vertical Use Cases」中即列舉了 25 個應用例子，並將其歸納統整為 6 個產業領域，包含 7 個製造業案例、5 個汽車業案例、5 個醫療業案例、4 個通訊業案例、3 個農業案例，以及 1 個運輸業案例。

二. 計畫執行情形

近幾年來 5G/B5G/Pre-6G 等相關標準與大廠已開始啟動規劃與推動，本計畫因應現階段之發展現況、未來規劃以及產品/服務建置推動等訊息，就各項產業可能建構之應用情境下所衍生之已知或未知的資安威脅、攻擊/防護實證技術、風險評估、可能漏洞及對應攻擊手法進行解析與推動規劃，因此主要關鍵因素即為基於現有 5G 發展推動經驗、6G 新興技術與應用觀測，以及國內外 6G 推動指標業者的動態觀測與回饋，並展開跨領域應用情境、

6G 資安偵測與防護、6G 網元及通訊資安檢測以及 6G 跨產業資安聯防生態探索等四個構面進行彙整與解析，接下來的執行情形將依前述「跨領域應用情境研析」、「6G 資安偵測與防護研析」、「6G 網元及通訊資安檢測研析」及「6G 跨產業資安聯防生態探索研究」四個構面做說明，接著針對「通訊整合增強型人工智慧協作設計與驗證」、「安全可靠與受信賴的分散式運算設計與驗證」進行實證方式與結果說明，最後則說明「公部門連結小組」的年度推動成果。

三. 計畫執行情形-跨領域應用情境研析

觀察行動通訊從 1G 到 4G 發展，從 1980 年到 2010 年間，行動通訊的應用著重在「人與人的溝通」，讓民眾可以隨時隨地的通話、發布訊息與分享各種數位內容，形塑一個跨越傳統國家概念的大型社群網路。而自 5G 時代開始之後，行動通訊應用的發展重點轉向「人與物的溝通」，偏重在各行業的商業應用，如智慧工廠、自動駕駛、遠距醫療等，實現模擬人類反應的關鍵工作，透過 5G 的普及帶動產業應用提升。

到了 6G，預期會有很大程度的優化並改善現有 5G 效能，按照過往行動通訊技術約每十年會更新一代的演進歷程，預估在 2030 年 6G 將可實現商用化。

5G 已方興未艾，但對於 6G 相關議題已甚囂塵上，全球主要國家政府、學研單位，甚至相關資通訊產業已經多已嚴陣以待，了解相關技術需求，提前準備以搶食商機。而在亞洲地區，至少有中國大陸、日本與南韓三國積極討論，已從政府層面思考，並徵詢產、學、研界意見，研擬開展 6G 通訊技術發展的戰略計畫。歐美地區也積極的討論 6G 通訊技術，依據 6G 的無線網路場域可能的使用情境需求，規劃 6G 必要的通訊基礎技術。各國皆期望能在此下一世代通訊技術發展中，無論在核心關鍵技術或是標準上，甚至專利的量與質，可以搶得先機佔有一席之地，故要藉此整備產研能量，欲在 6G 世代資通訊軟、硬體和應用市場中掌握先趨優勢。

雖然目前 3GPP 尚未啟動有關 6G 行動網路技術的規格研制工作，然而包含美國、歐盟、中國、日本、韓國等通訊技術發展先進國家及相關廠商，對於其 6G 發展相關的產、官、學、研等單位，近年來紛紛發表針對 6G 白皮書，描述各單位心目中想像

未來 6G 環境的願景，開啟下一世代通訊標準化的前哨戰。

本計畫參酌全球各界所提出之白皮書，藉以觀測 6G 無線通訊技術發展、思考各種跨領域之應用情境，對應各種需求之相關主流應用技術趨勢，以及相關的技術生態議題之動向，目前根據各國、廠商所闡述的 6G 願景，可以比較明確預期未來 6G 基礎建設的發展將涉及超高速(Extreme High Data Rate)、超覆蓋(Extreme Coverage)、超節能(Extreme Low Energy)、超低延遲(Extreme Low Latency)、超信賴(Extreme High Reliability)、超連結(Extreme Massive Connectivity)等未來面向需求。

期望藉由分析國際對於 6G 通訊技術與相關應用趨勢之見解，藉此了解世界各組織、政府與產業對於跨領域應用之發展布局。此外，考量我國技術服務發展進程，並因應未來 6G 環境下創新且多元的跨領域應用技術門檻，提出適合本國環境的建言，協助政府先期規劃研發布局，研擬相關政策推動發展之參考。

以下針對 6G 發展下跨領域新興應用服務的轉變、6G 跨領域應用關鍵技術研析內容進行說明：

(一)6G 發展下跨領域新興應用服務的轉變

目前5G 網路已經在全球多數地區完成部署，從這些已部署的商用網路營運中，可以從實證經驗學習到各種實作的狀況，將會有助於後續調整精進6G 網路的規劃及發展。透過瞭解新興的垂直產業案例，持續發展5G 網路需求，促使3GPP 開啟了5G Advanced 系統相關的標準化工作，間接地奠定6G 網路系統的重要基石，藉此實現5G 與6G 的銜接，並作為建構跨領域應用的基礎環境。

所謂跨領域應用情境，是指基於未來6G 將建構強大的通訊、基礎資訊、計算能量三大服務，考量應用服務將從現階段人與人連接的應用服務，延伸至設備與設備、人與設備之間的連接。雲端服務整合廠商博弘雲端科技引用 Statista 研究報告指出[3.14]，預計到2030年全球 IoT 裝置將有至少500億台設備連接上網路，可以想像在未來6G 無線網路環境，更多具效率、便利的設計、創造、服務等新創應用，都可以在數位世界中的完成。

✓ 3.14 “雲端物聯網新紀元 Part 1：AWS IoT 服務與架構”，博弘雲端，https://www.nextlink.cloud/news/aws-iot-info/

基於對6G 行動網路系統認知的跨領域應用，本計畫分析國際上各政府、國際組織、產業界之技術趨勢，透過研析各單位所發布之白皮書等相關文件，解析各國際機構及指標廠商在6G 發展的跨領域新興應用觀點及相應策略，可以期待在6G 發展的跨領域新興應用，將會擴大市場商機，改變社會運作和各行業現行作業型態，進一步改變人們的生活、工作、娛樂、教育等互動模式。各面向影響的相關特徵如下：

1. 日常生活：

6G 應用將有助於提高一般民眾的日常生活品質，如服務機器人可以提供醫療保健、護理、室內、本地送貨服務幫助。在6G 環境下普設感知器和智慧網路結構的高度整合，人們在此6G 服務環境下的終端用戶將可以透過環境智能於日常居住環境或旅行中獲得提高生活質量的益處。甚至面對目前老年化社會的問題，也可以透過各種架構於6G 環境而新興的照護服務獲得緩解。

2. 互動體驗：

動態和擴展的6G 應用將有助於改善客戶體驗和技術介面。從語音助手到服務機器人等增強功能會擴展人與設備的互動體驗，並提供豐富的沉浸式體驗的系統。這些應用功能可支援延展實境娛樂、人機互動、身體和心理醫療保健支援、具有實際溝通的即時互動式的遊戲等。

3. 社會目標：

6G 應用將促進實現高層次的社會目標並提高公共安全，這些目標範圍極廣泛，涵蓋社會、環境和經濟問題的各個面向。而6G 將可為社會和經濟提供可實現的應用、服務關鍵價值。如建立數位公平以降低數位落差，包含成本效率、可負擔性和社會可持續性。

目前在解決數位公平和社會可持續性方面已有長足進步，但預計6G 的應用環境將提高相關工作協作的流暢度，同時將服務擴展到偏遠或數位落差大的地區。此外，6G 將在網路架構設計階段就考量以減少二氧化碳排放並提高能源效率為目標，超長壽命電池、零能耗設備和自供電感知器等元素，都是有助於實現某些可持續發展目標的技術。

4. 關鍵角色：

未來6G 技術的進展將可以提供新興應用服務上更優質的服務基礎，如醫療保健、製造、農業、交通和公共安全等領域，可預見會在服務品質上扮演更關鍵性的功能。

在6G 技術、網路和應用程序的共同加持下，人類與機器之間的互動應更自然順暢，可以提高生產力並維持基本操作。這些應用服務可能使用數位分身技術，人類在數位空間中與機器人自然互動，以在實際世界中執行動作或任務。相關應用案例包括遠程手術、治療和監控。

(二) 6G 跨領域應用關鍵技術

在本計畫研析目前國際上各政府、國際組織、產業界等對6G 行動網路系統的觀點及相應策略後，彙整各機構認知中的跨領域應用情境相關內容、基於6G 行動網路環境提出的跨領域應用服務，分析各應用應該具備那些關鍵技術，相關對應技術詳如表5。

表5、各單位對於6G 跨領域應用及對應技術表

項次	單位名稱	跨領域應用	關鍵技術
1.	美國 ATIS-Next G 聯盟	聯網機器人和自主系統	資安技術(隱私保護) 人工智慧
		多感官延展實境	延展實境
		分散式感知和通訊	人工智慧 分散式雲與通訊系統 資安技術(隱私保護) 延展實境

項次	單位名稱	跨領域應用	關鍵技術
			感知應用技術
		個人化用戶體驗	人工智慧 分散式雲與通訊系統 資安技術(隱私保護) 延展實境 感知應用技術
2.	歐盟 Hexa-X 計畫	XR 技術	延展實境 定位 感知應用技術 人工智慧
		全息呈現	延展實境 資安技術
		數位分身	人工智慧 感知應用技術 資安技術(隱私保護)
		聯網機器人	人工智慧 感知應用技術
		遠端醫療、教育	資安技術(隱私保護)
		遠端保健	資安技術(隱私保護) 感知應用技術
3.	德國-諾基亞貝爾實驗室	AR	延展實境
		遙現	延展實境 感知應用技術
		集群機器人/無人機	人工智慧 感知應用技術
		分散式運算/自動化	人工智慧 感知應用技術 資安技術
		數位分身/虛擬世界	人工智慧 感知應用技術 資安技術(隱私保護)
		身體感知	感知應用技術 資安技術(隱私保護)
4.	芬蘭-Oulu 大學	XR 體驗輕型眼鏡	延展實境 定位

項次	單位名稱	跨領域應用	關鍵技術
			感知應用技術 人工智慧
		遙現	延展實境 感知應用技術
		自主系統和機器人	人工智慧 感知應用技術
		資料市場	資安技術(隱私保護)
5.	南韓-科學技術情報通信部	數位醫療	資安技術(隱私保護) 延展實境 人工智慧
		體感內容	感知應用技術 人工智慧
		自駕車	感知應用技術 人工智慧 資安技術(隱私保護)
		智慧城市	感知應用技術 人工智慧 資安技術(隱私保護) 延展實境
		智慧工廠	感知應用技術 人工智慧 延展實境
6.	南韓-三星	真正的沈浸式延展實境	延展實境
		高度逼真的行動顯示	人工智慧 感知應用技術
		數位複製	人工智慧 感知應用技術
7.	中國大陸-IMT-2030(6G)推進組	沉浸式雲 XR	延展實境 人工智慧
		全息通訊	延展實境 資安技術
		感官互聯	感知應用技術 資安技術(隱私保護)

項次	單位名稱	跨領域應用	關鍵技術
			人工智慧(聯合學習) 延展實境
		智慧互動	人工智慧 腦機互動
		通訊感知	人工智慧 感知應用技術
		普惠智能	感知應用技術 人工智慧 定位
		數位分身	人工智慧 感知應用技術 資安技術(隱私保護)
8.	中國大陸-中國移動	沉浸式多媒體應用	延展實境 人工智慧 資安技術(隱私保護) 區塊鏈技術
		通感互聯	人工智慧 感知應用技術
		泛在覆蓋	超低功耗 人工智慧
9.	中國大陸-賽迪智庫無線電管理研究所	人體數位分身	人工智慧 感知應用技術 資安技術(隱私保護)
		基於全息通訊的XR	延展實境 人工智慧
		新型智慧城市群	人工智慧 資安技術(隱私保護)
		全域緊急通訊搶險	感知應用技術
		智能工廠	人工智慧 區塊鏈 資安技術
		連接機器人與自主系統	人工智慧 感知應用技術
10.	日本-NTT DoCoMo	人體增強	延展實境 人工智慧

項次	單位名稱	跨領域應用	關鍵技術
		大腦技術	腦機互動 人工智慧
		感知共享	感知應用技

資料來源：本計畫整理

有關各組織的相關介紹，已在前述工作實際執行情形說明的「一、跨領域應用產業現況與國際趨勢」之「 (四)6G 技術應用型態的演化與各國主張」做了相關說明，以下分別就全球各單位對於跨領域的應用面做詳細解析：

1. 美國 ATIS-Next G 聯盟

在 Next G 所發布的6G 的應用及使用案例報告 「Next G Alliance Report: 6G Applications and Use Cases」中，說明了針對未來6G 環境下可能產生的新興應用服務，對於規劃未來架構於6G 環境下技術方向及應用服務有相當的參考價值。

以下針對 Next G 所發布的6G 應用及使用案例報告中的「聯網機器人和自主系統 (Networked-Enabled Robotic and Autonomous Systems)」、「多感官延展實境 (Multi-Sensory Extended Reality)」、「分散式感知和通信 (Distributed Sensing and Communications)」及「個人化用戶體驗(Personalized User experiences)」等四個面向，提出各種應用情境案例分析：

(1) 聯網機器人和自主系統：6G 無線通信技術的最新進展，將擴充至空中3D 網路的潛在新穎功能，特別是機器人應用，可能會對於強化工業自動化並改善日常生活有極大的影響。

A. 案例一，一組服務機器人之間的在線協同操作(Online Cooperative Operation among a Group of Service Robots)：多台服務機器人協同合作一起完成某些任務，通常稱為多代理場景/模型。用到的技術對應到 Next G 所規劃的6G 目標為可信任、安全、彈性、數位世界體驗以及人工智慧原生。

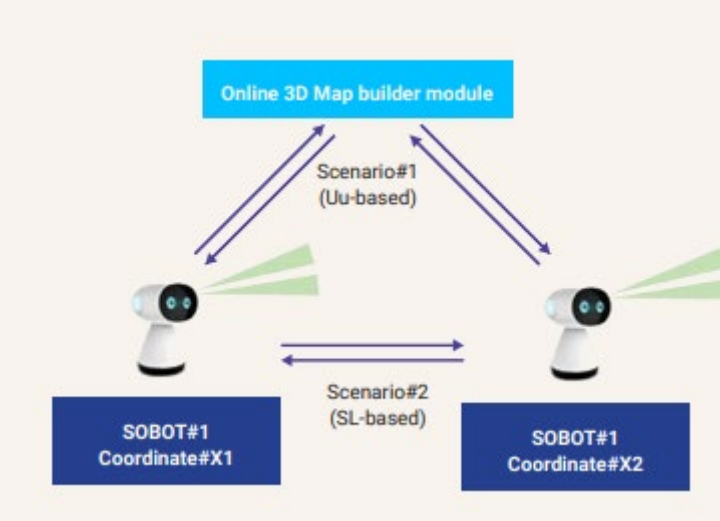


圖30、服務機器人群共同合作作業示意圖
資料來源：Next G Alliance Report: 6G Applications and Use Cases

B. 案例二，用於危險環境的現場機器人(Field Robots for Hazardous Environments)：現場機器人可以在偏遠或難以到達工作場所進行檢查或維護。此外，它們可以被使

用來執行對人類工人來說比較危險或太費力的任務。野外機器人的具備準確性和可靠性的優點，使它們成為執行關鍵任務的最佳選擇。此案例使用到的技術對應到 Next G 所規劃的6G 目標為可信任、安全、彈性以及人工智慧原生。

(2) 多感官延展實境：多感官延展實境是包括 AR 和 VR 在內的沉浸式技術集合的總集成。

A. 案例一，超現實互動運動-無人機競速(Ultra-Realistic Interactive Sport – Drone Racing)：無人機競速的重點之一是畫質，包括辨識率和時間延遲，此一品質好壞的因素很大程度上取決於網路能力。飛行員以目視方式駕駛無人機，因此該案例相當程度依賴於網路提供足夠即時的影像，網路中有限的傳輸數據速率和延遲可能會限制影像刷新率。6G 系統將具有 Tera-bps 等級的峰值，提供更快的資料傳輸速率、更低的延遲，並提供新的網路計算結構。有望通過實現吞吐量達數千兆位/秒範圍的全3D 成像傳輸，可以推動相關行業的發展。此案例使用到的技術對應到 Next G 的6G 目標為數位世界體驗。

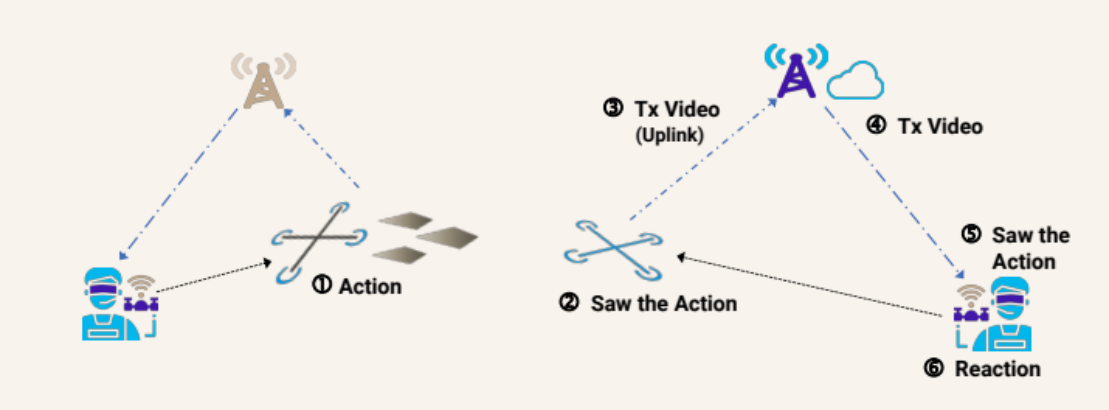


圖31、超現實交互式無人機場景示意圖
資料來源：Next G Alliance Report: 6G Applications and Use Cases

B. 案例二，身臨其境的遊戲/娛樂(Immersive Gaming/Entertainment)：所謂身臨其境的遊戲是一種創新性的體驗，相關研究顯示很可能是未來遊戲的新趨勢。身臨其境的遊戲玩家在遊戲中發現自己，渴望獲得更多的延展實境娛樂，玩家願意為良好的體驗品質投資設備和支付更高的成本。5G 雖然提供了高速率、低延遲、更精確的沉浸式體驗(如遊戲)的連接性，但它無法同時支持大量沉浸式遊戲玩家，所以6G 是實現這一趨勢所必需的基礎建設。藉由6G 的特性，地理上分離的玩家可以體驗無縫式參與更高級的同步、低延遲，並超越人類感官的限制。除了無處不在的連接、卓越的頻寬和擁塞控制之外，可靠性、體驗品質 QoE 和延展實境遊戲至關重要。

其中 QoE 由多個因素決定，包括用戶、上下文和網路方面。而 QoE 的網路面向是一個涵蓋連接方面的保護傘，如抖動、低延遲、所需頻寬、擁塞控制等，以提供高精度網路和近乎即時的交互。6G 可以在應用程式、設備、邊緣服務器和網路之間提供即時的回饋，以提供最高水平的 QoE。此案例使用到的技術對應到 Next G 所規劃的6G 目標為數位世界體驗。

C. 案例三，混合現實協同設計(Mixed Reality Co-Design)：所謂混合實境 MR 協同設計是遠程或同地協作和「原型製作前的體驗」，這是混合實境融合真實世界和虛擬世界的概念。而混合實境協同設計系統可以讓設計師創造新的產品，並將它們組合在虛-實的環境中。混合實境現實協同設計將捕捉動作、情緒和臉部表情。通過使用新形式的人機交互，混合實境協同設計將捕獲更多重要的人體測量值。預計到2030年，混合實境協同設計過程將包括各種設計師的行為和重要參數，藉由人工智慧，混合實境協同設計使用案例的功能將非常出色。更高級使用者設備與可穿戴設備相結合，將改變下一代工業物聯網。

此案例使用到的技術對應到 Next G 所規劃的6G 目標為數位世界體驗。

圖32、遠端合作體驗示意圖
資料來源：Next G Alliance Report: 6G Applications and Use Cases

D. 案例四，混合現實遙現(Mixed Reality Telepresence)：混合實境和3D 功能將成為工作和社交互動的新規格、功能，可以讓人們在身處不同地點時看起來好像在某個地點(如在車中時看起來像是在辦公室)。混合實境遙現體驗需搭配各種可穿戴的各種設備，如耳機和嵌入衣服中的設備，讓每個人都擁有多個可無縫協作，並具有自然、直觀界面的可穿戴設備，對著用來完成工作的設備做手勢和說話進行輸入。而使用的設備將可以有所感知，網路在預測需求方面將變得越來越複雜，這種情境感知與新的人機界面相結合，將使遠程呈現交互更加直觀和高

效。此案例使用到的技術對應到 Next G 所規劃的6G 目標為數位世界體。

E. 案例五，6G 的沉浸式教育(Immersive Education with 6G)：教育是社會發展最重要的驅動力之一，每個人都應該廣泛平等地接受高質量的教育。然而，教育的可觸及性和教育質量目前仍面臨著諸如缺乏基礎設施、高成本、過時等挑戰。例如在嚴重特殊傳染性肺炎(Coronavirus disease 2019, COVID-19)大流行期間，遠端教學缺乏學生與學生/學生與教師之間的互動、難以在遠端教學的環境下使用傳統教育工具、缺乏合適的學習環境，以及低質量的網際網路連接等挑戰。結合多感官延展實境和人工智慧/機器學習等新技術，6G 可以幫助產生完全沉浸式的教育體驗。在沉浸式教室中，一群配備混合實境耳機、運動感知器等設備的學生在網路實體空間中參加教育課程，即使師生可能在實際上彼此相距很遠，教室的沉浸式特性將使即時的、人為控制成為可能，學生可以參與語音和影音等傳統應用的小組活動。使用數位分身技術，以感知器取代實驗室設備、樂器等物理工具，降

低教育各種相關的成本，感知器還可用於通過辨識個體的手勢和身體各種動作來改善課堂體驗。立體和全息視訊等的數位內容可以取代傳統的教學方法，從而增強學習體驗和學生參與度。對流動性的支持還將提供範圍更廣的教育內容，如讓博物館實地觀察的學習質量更加提高。遠端沉浸式教育也可用於為有身體障礙和學習障礙的學生提供更優質和無障礙的教育環境。此案例使用到的技術對應到 Next G 的6G 目標為數位世界體驗。

F. 案例六，用於娛樂服務的飛行器中的高速無線連接(High-Speed Wireless Connection in Aerial Vehicle for Entertainment Service)：本案例的應用場景旨在確保通訊穩定性，以增強終端用戶在空中、高海拔或高機動性應用情境在惡劣環境中的使用體驗，同時提供高質量的飛行器上娛樂服務。高品質的無線網路連接可以讓用使用者在飛行期間持續地享受很多服務，如視訊會議或多人連線遊戲，孩子可以在飛行期間使用教育資源。如果發生飛行中的醫療緊急情況，高品質的無線連接可以讓地面醫生進行遠端診斷、提出適當的治療方法。此案例使用到的技術對應到 Next G 的6G 目標為數位世界體驗。

(3) 6G 分散式感知和通訊：分散式感知和通訊此一分類是描述了世界的未來狀態，地面蜂窩行動通訊網路(Terrestrial Networks, TN)和非地面網路(Non-Terrestrial Networks, NTN)連接服務組成了無處不在的連接，非地面網路為氣球、無人機和衛星等非地面的飛行物體上設有基地台的所有網路的總稱，這樣的無線網路環境將會創造大量服務及感知器資料收集機會。

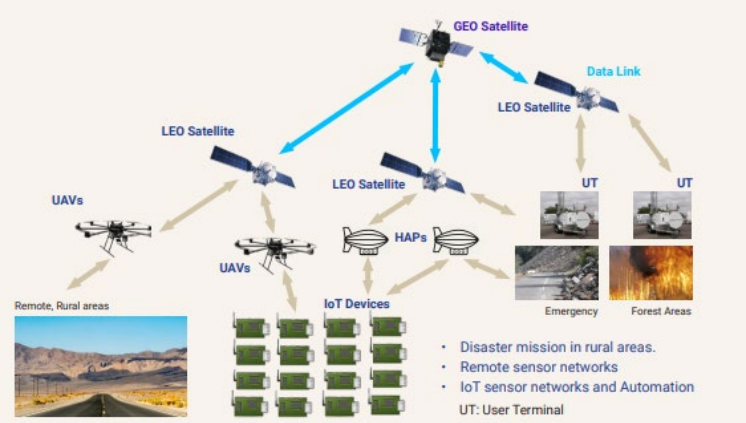


圖33、針對偏遠地區網路覆蓋多系統協同服務示意圖
資料來源：Next G Alliance Report: 6G Applications and Use Cases

A. 案例一，遠程數據收集(Remote Data Collection)：衛星網路未來可望為當前行動通訊網路無法充分支援物聯網服務的地方(如農村)提供快速連接、區域覆蓋和其他服務。為了支持農村地區的物聯網覆蓋，NTN 由不同的無線網路所組成，結合6G 網路為各種設備提供全球無處不在的移動網際網路覆蓋，可以用互連的衛星等設施補足

行動通訊網路基礎設施於農村覆蓋率不足的問題。為了更順暢地與地面6G 網路互連，衛星部分需要解決和支持6G 系統支持的相同功能(如介面、QoS、安全性)。此案例使用到的技術對應到 Next G 所規劃的6G 目標為具成本效益的解決方案(Cost Efficient Solutions)、分散式雲與通訊系統(Distributed Cloud and Communications Systems)及可持續性(Sustainabilit)。

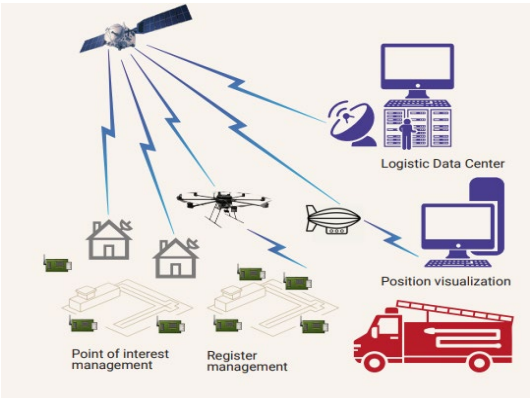


圖34、架構非地面網路下運用感知器的物流追踪示意圖
資料來源：Next G Alliance Report: 6G Applications and Use Cases

B. 案例二，消除北美數位落差(Eliminating the North American Digital Divide)：北美明顯的數位落差以多種方式存在，包括生活在城市地區的社區和生活在農村住區的社區、不同的社會經濟群體、不同的經濟發展國家以及不同的教育水準等。由於目前低性能計算機、有限的頻寬、網路速度的現況，能夠連接上的個人在數位應用

上有差異，而6G 的出現可望可緩解這些現象。此案例使用到的技術對應到 Next G 所規劃的6G 目標為信任、安全和彈性、數位世界體驗、分散式雲與通訊系統及可持續性。

C. 案例三，同步數據通道(Synchronous Data Channels)：未來隨著大量物聯網感知器的引入，資料收集將持續呈現指級增長。準確的數據對於支援6G 應用和服務需要準確計時和同步至關重要。預計由越來越多的感知器、人工智慧和元宇宙生成的大量數據將需要快速的傳輸，以便在完全同步的情況下按時提供這些資料。網路提供者需要確保邊緣設備的雲傳播指令的同步性，使數據發布與 GPS/網路時間協議(Network Time Protocol, NTP)時間同步保持一致，以提供對時間具有極端敏感性的服務和系統。此案例使用到的技術對應到 Next G 所規劃的6G 目標為信任、安全和彈性、具成本效益的解決方案、數位世界體驗、人工智慧原生及分散式雲與通訊系統。

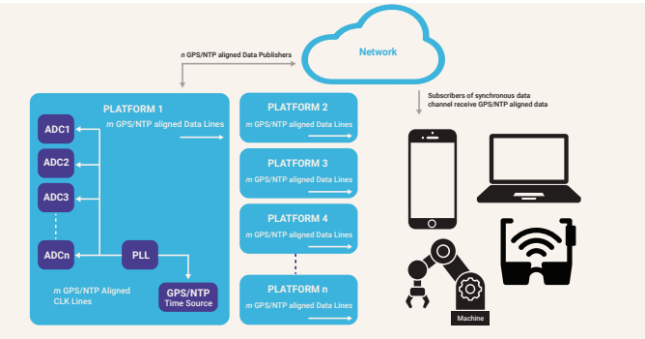


圖35、同步數據通道運作示意圖

資料來源：Next G Alliance Report: 6G Applications and Use Cases

D. 案例四，醫療保健–體內網路(Health Care – In-Body Networks)：目前可穿戴設備推陳出新的開發和持續改進，使醫療保健不斷發生變革。在某些狀況下需要對健康人和病人生理參數進行7×24全天候監測，這種監測是通過許多可穿戴設備進行的。此外，即時健康監測可能包括貼在皮膚表面(如可穿戴皮膚貼片、溫度和血壓感知器)或植入物(如心臟起搏器、胰島素泵和肌肉控制器)連接至通信的設備無線存取點(Access Point, AP)，它將數據(如健康參數)傳輸到網際網路，以便可以迅速採取行動。因此，透過蒐集、分析體內感知資訊，以及透過6G 廣域連接方式，來實現遠端醫療行為。此外，體內網路可以幫助解決當今醫療保健系統在封閉交互式遠端監控和預測治療方面的不足，提供個人基本的健康監測和報告(如溫度、脈搏、血糖指數和血壓)。預計到2030年代，這些

感知器將可以精確可靠地用於診斷目的，此類感知器作為體內子網路提供更新，並與分散式雲存儲庫互動。此案例使用到的技術對應到 Next G 所規劃的6G 目標為信任、安全和彈性、數位世界體驗。

(4) 個人化用戶體驗：個人化用戶體驗是基於使用者的個人剖析和上下文訊息(如用戶的偏好、趨勢和生物特徵)，發展設備、網路、產品和服務等元件，提供使用者的即時、全自動化和安全的個人化服務。

A. 案例一，個人化的旅館體驗(Personalized Hotel Experience)：在旅客在途中，可以追蹤客人的位置和預計到達旅館的時間，以便準備旅客的房間，而其他酒店服務(如晚餐預訂、客房服務)可以在抵達時準備就緒，並符合旅客們的喜好。當旅客進入酒店大堂時，旅館布署的感知器會在幾秒鐘內執行自動且安全的旅客入住流程。智慧感知器會對旅客進行臉部識別，並檢測旅客的個人設備(如智慧型手機、手錶和眼鏡)。旅館系統會向旅客的個人設備推送一條通知訊息，確認旅客已自動登記入住，並附上房間號碼和基於擴增實境的地圖，引導旅客前往

電梯前往。進入電梯後，電梯會檢測旅客抵達並自動選擇旅客的房間樓層。一旦進入旅客的樓層，基於擴增實境的樓層地圖就會顯示在旅客的個人設備上，指引其前往指定的房間，此時，門上的感知器執行自動和安全的解鎖程序。進入房間後，房間內各種智慧設備的個人化服務自動執行，如恆溫器、燈、百葉窗、電視和串流媒體服務、個人化數位圖片和禮賓服務等。這些訊息是從旅客或其家庭成員的個人設備和/或網路資源(如託管於雲中的服務)安全收集和彙整後，並用於配置房間內的設備，以為旅客提供更加個人化和滿意的旅館客房住宿體驗。另外，在報告中對於個人化旅館禮賓和自動化客房服務、自動退房和隱私保證亦有所描述。另一重點是，必須確保在這些服務資源提供用戶服務時，使用安全方法以建立信任，在用戶互動期間要確保個人訊息不會被洩露和濫用，此案例使用到的技術對應到 Next G 所規劃的6G 目標為信任、安全和彈性、數位世界體驗、人工智慧原生、分散式雲及通訊系統。

B. 案例二，個人化購物體驗(Personalized Shopping Experience)：虛擬購物中心以沈浸式虛擬環境方式呈現，提供即時購物體驗，使客戶能夠沉浸並出現在虛擬商店中，且能在實際購買行為發生前與產品互動。此外，客戶可以在這個虛擬世界中與朋友見面並即時一起購物。商店根據客戶的不同，可以為客戶提供不同程度的沉浸感和真實感。如當顧客進入虛擬服裝店時，預測分析客戶喜好，透過個人化聲音和氣味來自動化提供商店氣氛。此外，客戶還可以看到根據個人的喜好和可能正在瀏覽的衣服穿著風格的數位人體模型。零售商將通過多個資料深入了解每一位顧客，包括了解用於個人化零售空間的情感暗示，甚至由面部表情了解消費者是否喜歡產品。另外，當顧客進入虛擬商店時，會看到遊戲的選項，並根據個人化購物偏好和品牌遊戲中的成績獲得促銷和折扣，透過讓這些體驗，鼓勵用戶在虛擬商店中投入更多時間。此案例使用到的技術對應到 Next G 所規劃的6G目標為信任、安全和彈性、數位世界體驗、人工智慧原生、分散式雲及通訊系統。

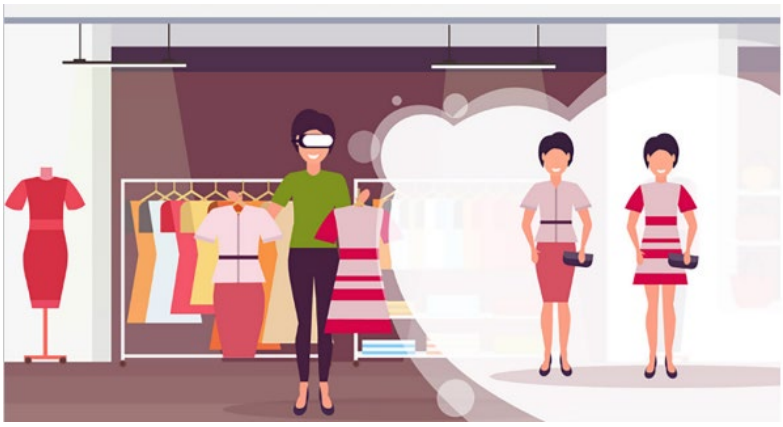


圖36、個人化客戶服務意圖
資料來源：Next G Alliance Report: 6G Applications and Use Cases

2. 歐盟 Hexa-X 計畫

歐盟於2021年啟動 Hexa-X 計畫協同產學研界探索6G 的新境界，Hexa-X 計畫共有20多家企業和科學研究機構參與，由諾基亞主導本計畫，愛立信則是負責技術經理，具體內容包括研發6G 智慧型網路架構、6G 技術、6G 使用案例等。

在前期 Hexa-X 創新成果的支持下，Hexa-X-II 計畫將需努力克服以下社會挑戰：

A. 可持續性(Sustainability)：Hexa-X-II 將研究有助於實現零碳足跡、限制能源和材料消耗的技術。

B. 包容性(Inclusion)：Hexa-X-II 旨在為發展中國家的人民以及發達社會的弱勢群體提供網路連通性。

C. 可信度(Trustworthiness)：Hexa-X-II 將確保數據透明性、安全性和隱私性以及網路穩健性。

3. 德國-諾基亞貝爾實驗室

貝爾實驗室就消費者觀點思考跨領域應，認為可以期待以下的情境在2030年可能發生：

A. 自駕車的服務應用將更被一般民眾接受，同時車輛感知器資料將即時上傳到網路，可以下載高分辨率的地圖，汽車之間可直接相互連接。

B. 環境中將部署大量的無線攝影機，各種資料可提供人工智慧和機器視覺技術的應用，攝影機將成為一種通用感知器，可以在任何地方使用。同時隱私保護的問題也需要被思考如何解決，必須對資料的存取進行限制以及資料匿名化。

C. 實際世界和數位世界中的交易都將透過大量終端設備進行，數位現金的使用和密碼技術的使用將可能成為常態，所以未來的網路環境必須針對這種轉變提供必要的安全和隱私防護。

D. 機器人的應用將會更普及，而這些應用可能會是由一群小型機器人共同協作的形式完成任務。這些機器人將配備攝影機，將資料以串流方式傳輸到計算伺服器進行即時處理，將看到家庭網路中設備數量的增加和更高的傳輸量、容量的需求。

E. 醫療保健將發生重大轉變，未來透過大量穿戴式設備、經由無線網路全天候蒐集監測健康重要健康參數，提供各種健康加值服務。

F. 自產業界的觀點，由於工業4.0的演進，需要超可靠低延遲通信的網路支援雲端的即時資料處理，將更需要6G 無線通訊的環境支持。

G. 全息呈現將成未來工作和社交互動的常態。它可以讓人看起來好像在某個地方，而實際上卻在不同的地點。

H. 在酒店、醫院、倉庫及包裹遞送等各個領域會更大量使用移動機器人和無人機，將替代傳統人力處理的方式。

I. 數位分身與實際世界的同步會更新越來越準確，將成為增強人類智能的重要平台。

4. 芬蘭-Oulu 大學

(1) 6G 應用的發展趨勢與未來使用情境

Oulu 大學預測未來可能的使用情境及6G 應用的發展趨勢如下：

A. XR 體驗取代智慧型手機：智慧型手機可能會被具高分辨率、影格率和動態的 XR 體驗所取代，具備 XR 體驗的輕

型眼鏡圖像投射到眼睛上，反饋將通過耳機和觸覺界面提供給其他感官。必要的配套技術包括：

a. 光場、全景、深度感知、高速相機等成像設備。

b. 用於監測心率、血壓和神經活動等健康狀況的生物感知器。

c. 用於計算機圖形、計算機視覺、機器學習和人工智慧的專用處理器。

d. 無線技術，包括定位和感知。感知器和成像設備可以蒐集整個生活歷程以及詳細的實際環境，而虛擬世界的保真度也不斷提高。這些前瞻性功能與分散式計算的要求相結合突出了對無線網路性能的需求。

B. 遠端呈現更為可行：高分辨率成像和感知技術、可穿戴式顯示器、移動機器人和無人機、專用處理器和下一代無線網路將使遙現(Telepresence)等應用變得更為可行。可透過實時蒐集、傳輸和渲染聚會中每個參與者的3D 全息表示來實現存在感，或者通過形表示和感知器蒐集的運動數據的組合來實現。

這些感知是由 XR 設備創建的，而使地理上分散各地的一群人，認知他們處於同一位置、空間。具備自主系統和機器人後，人們可以通過自己熟悉的機制(如語音和肢體語言)或使用類似於個人電腦(Personal Computer, PC)滑鼠的專用設備與遠端進行交流，可以控制遠端世界的變化。相關應用包括遠端教學、協作設計、遠端醫療、遠端辦公、高階的3D 仿真與訓練。

C. 自動駕駛汽車成為可能：隨著人口和全球化的增加，人員和貨物的流動是一個嚴峻的挑戰，2030年後的世界設想存在數以百萬計的聯網自動駕駛汽車協調運行，已使得運輸和物流盡可能高效率運作。線上消費者購物將導致需要將數百萬個包裹從倉庫運送到個人家中。比效率更需要關注的是安全，隨著自動駕駛汽車使用的增加，對人類的傷害基於人工智慧技術的加持不應該增加，甚至是應該會降低運輸和物流的傷亡率。

感知器、感知器融合和控制系統的進步提高安全性，但這必須架構在更強的網路效能要求下為基礎。未來網路中的每輛車都將配備許多感知器，包括攝影機、雷射掃描

儀等，可能還有使用到3D 成像、里程計等。人工智慧演算法必須快速融合來自多個來源的數據，快速決定如何控制車輛，同時考慮當地車輛所在環境、車輛在該環境中的位置、其他車輛、人、動物、結構體或可能導致危險的訊息碰撞或受傷，並且提醒車上乘客或駕駛應該注意的各種潛在風險，以便採取適當措施避免事故發生。為了使車輛網路高效安全地運行，無線網路除了低延遲和高頻寬外，還必須有超高可靠性。

(2)6G 網路應具備特性

除了上述預測未來可能的使用情境及6G 應用的發展趨勢外，Oulu 團隊針對6G 網路提出下列應具備特性：

A. 6G 應該有一內含信任的網路：未來數位世界和實際世界將深度交織，網路運行的可靠性深深影響人的生活。在數位世界中，攻擊可能會造成無形資產的損失，而在網路實際世界中，有形資產可能會因數位攻擊而被盜、喪失能力或受到損害。惡意網路活動可能導致財產和生命損失，為了應對，應該在網路中嵌入廣泛的信任模型，讓用戶信任網絡上的通信。

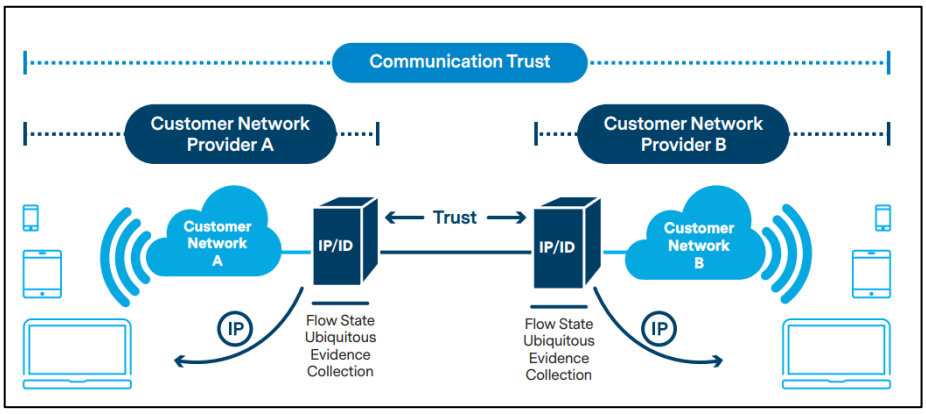


圖37、6G 通信通過的信任鏈示意圖

資料來源：Key drivers and research challenges for 6G ubiquitous wireless intelligence

B. 6G 將創造資料市場-隱私保護將成為關鍵推動因素：網路運作將會產生大量關於個人訊息包括大量商業敏感數據和個人資料數據。從實際世界收集到的隱私訊息非常敏感，若不妥善管理很可能會損害個人的利益。所以要讓6G 為所有民眾所接受，保護隱私訊息將是實現其全部6G 潛力的關鍵推動因素，市場將會要求保護敏感的業務資料。而使用者最終應該能夠透過簡單直觀的用戶界面來控制和管理他們自己的私人資料。個人資料的所有權和控制權應該歸於相關個人或實體。

C. 人工智慧和區塊鏈在6G 網路中有重要作用：機器學習必須在巨量資料中挖掘，以獲取有用的訊息和知識，這種方法可以應用於檢測遠端惡意行為的攻擊者。而網路運作中還有其他眾多需要「智能」的需求，如自我調適或複雜的頻

寬管理等作業。除了巨量資料，人工智慧還需要於大量的計算能量。6G 將使用不斷增加的計算能量來提供更高的計算效率。另一個目前常被關注的新技術是區塊鏈，又可稱作為分散式記帳本，此技術可以在不需要中央管理架構的情況下，以分散式方式允許儲存和共享不常修改的訊息，還可以保存了任何更動的完整記錄，這可能會產生建構資料市場或幫助維持網路用戶信任的新方法。

D. 6G 將成為一個包含通訊服務的服務框架：早期蜂巢系統開發的重點一直放在通訊方面，主要在優化傳輸效率，而其他服務的優先等級較低。未來6G 提供的服務，如 XR，因為需要定位、3D 映射、數位內容與物理模型等技術的融合，以及低延遲的極高速通訊眾多元件的統合支持，因此必須合作設計，如密集的無線網路、高頻天線陣列和邊緣的大量計算能量。

E. 在6G 中，所有使用者所需特定的計算和人工智慧都可能轉移到邊緣：在深度學習(Deep Learning, DL)的最新突破、可用資料的增加和智能裝置興起的推波助瀾下，激勵無線社群的激增。人工智慧運用到創建能夠自主管理網路資源

和控制網路功能的自我學習網路和系統。此外，隨著新型自主設備在其本地環境中進行感知、通訊和操作的激增。將極大量本地資料傳輸到集中式雲端，進行訓練和建模是不切實際的作法。Oulu 建議需要新的類神經網路架構及其相關的無線通信高效訓練算法，同時在網路邊緣進行即時和可靠的推理，其中所謂的聯合學習(Federated Learning, FL)這一類分散式機器學習的架構是可以思考的技術選項。

F. 感知、成像和高精度定位功能與移動性的組合開啟了6G 的無數新應用：與目前的行動網路不同，未來的通訊系統將普及到多個垂直行業，從而實現需要大量定位的服務，如資產追蹤、環境感知、運輸和物流系統、醫療保健等。事實上，在城市和室內依賴 GPS 衛星和有限量的部署傳統定位方法是很不切實際且不得不的方式。6G 的高載波頻率、大頻寬、大規模天線陣列、緻密化和設備到設備，都是規劃中將會出現的新興技術，這些技術除了有本身在通訊上的優勢，其固有的定位能力卻經通常被忽視。另外，基於射頻(Radio frequency, RF)使用高載波頻率的感知技術也為未來網路的帶來的另一個定位可能性。該報告提到

另一點特殊的應用，就是可以使用太赫茲頻率的光譜進行環境感知，能夠用以檢測和識別環境中的有害或有毒氣體。

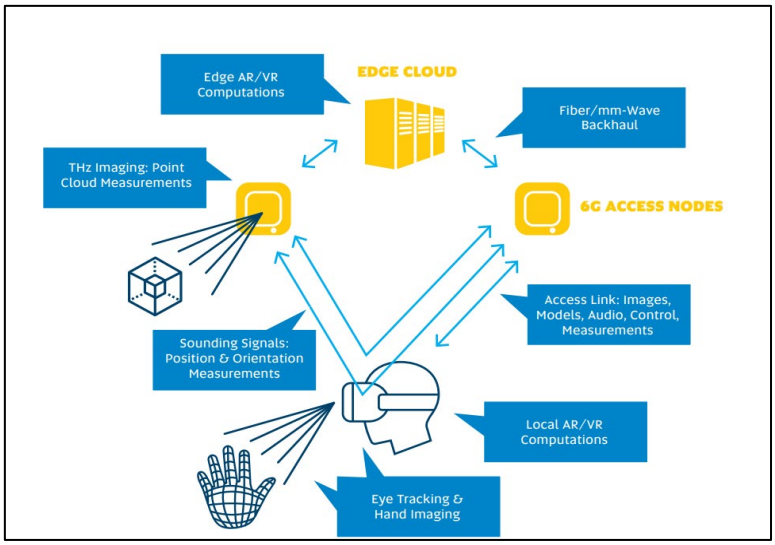


圖38、6G 網路可在邊緣處理定位、3D 和數據融合

資料來源：Key drivers and research challenges for 6G ubiquitous wireless intelligence

G. 信任和隱私是6G 服務平台成功關鍵的先決條件：未來6G 服務需要處理和儲存眾多有關網路使用者的個人資訊，甚至是敏感、機密的資料。例如，銀行或身分驗證應用程序在網路邊緣發生，而不是個人的行動設備上運行，更是需要最大限度地關注有關信任、隱私和資訊安全的議題。所有服務支持者、使用者對於應用系統在隱私和安全的上要求將會越來越高。

5. 南韓-科學技術情報通信部

有關南韓6G 行動通訊推動策略及推動階段分述如下：

(1)南韓6G 行動通訊推動策略主要三個面向如下：

A. 於下世代技術領域領先：開發產業較少投資之高風險技術。

B. 同步打造研究、產業基礎：育成高階人力促進國產化。

C. 確保高附加價值專利：主導6G 國際標準及確保相關專利。

(2)南韓6G 推動策略研發與應用階段：南韓6G 推動策略分為核心技術研發與應用兩階段，分別規劃為兩階段導入。

A. 第一階段(2021年～2025年)6G 核心技術研發：針對聚焦十大6G 技術策略課題分別為：

a. Tbps 行動通訊。

b. Tbps 光通訊。

c. 太赫茲(Terahertz/Tera-HZ, THz RF)零組件。

d. THz 頻段。

e. 空間行動通訊。

f. 空間衛星通訊。

g. 終端間超精密網路。

h. 智慧型無線存取。

i. 智慧型網路。

j. 6G 品質全天候保障安全技術。

B. 第二階段(2026年～2028年)6G 技術應用研發：在引用數位醫療、體感應用、自駕車、智慧城市及智慧工廠等多項 6G-Upgrade 示範事業範例，分別針對以量子密碼加密生理資訊、超遠距手術、遠距即時全息影像會議、以6G 衛星實現飛行車、無人機之超低延遲通訊。數位分身則針對物流、交通之移動物完整數位化重現及管理、以企業現場大數據為基礎，安全地提供最佳化之自動精密控制。

6. 南韓-三星

(1)三星所認知未來6G 的應用服務案例：

A. 真正的沈浸式延展實境:延展實境 XR 結合虛擬實境 VR、擴增實境 AR 和混合實境 MR 等技術的新興應用。目前延展實境要成功發展，除了要解決硬體上的需求及更大的無線容量，三星認為可將計算分載至強大的設備或伺服器來改善硬體的效能，另一挑戰是需要有足夠的無線通訊容量，未來延展實境容量更需超越擴增實境，至少一秒 0.44GB(Gbps)來達到更好的效能。

圖39、真正的沈浸式延展實境示意圖
資料來源：The Vision of 6G

B. 高度逼真的行動顯示：全息顯示將是能夠展現手勢、表情的新技術，藉由即時捕捉、傳輸和3D 渲染技術來獲得要顯示的內容。為了提供全息圖像顯示作為即時服務的一部分，需要極高的數據傳輸速率，而為了降低全息顯示所需的資料通訊數量，可以利用人工智慧實現全息數據的高效壓縮、提取和渲染。如果要即時傳輸全息影像，需要比當前 5G 系統高數百倍的數據傳輸速度，如在6.7吋行動裝置上約111億像素的全息影像即時顯示，就需要至少0.58 Tbps 速度，而5G 的峰值數據速率僅為20 Gbps。

圖40、行動裝置上3D 全息顯示示意圖
資料來源：The Vision of 6G

C. 數位複製：在6G 環境中，借助先進的感知器、人工智慧和通訊技術，使用數位分身的技術，讓用戶將可以不受時間、空間的限制，能夠在虛擬世界中探索並且監控現實環境。透過數位分身的技術，使用者將能夠觀察遠端環境的變化或檢測問題。所以，未來人類能夠透過自己的數位複製人，在虛擬世界中檢視各種狀況，甚至和其他數位複製人互動。在人工智慧技術的協助下，數位複製、現實世界的管理以及問題檢測和解決，都可以在無人在場監督的情況下高效地完成。例如用戶能夠透過數位分身技術掌握遠端動態，並即時控制現實環境下中的機器人，在人工智慧幫助下執行精細的作業。然此技術挑戰在於若是要複製1平方公尺虛擬空間，需要千億像素來描述，傳輸速度至少需0.8Tbps，且要延遲速度要在100ms 以內。

圖41、6G 環境數位複製應用示意圖
資料來源：The Vision of 6G

(2) 三星認為要成功實現6G 服務，須同時滿足三大需求，分別為效能、架構與可靠性。

A. 效能需求：

a. 峰值數據速率應達到每秒1,000 Gb。

b. 空中傳輸延遲應低於100微秒。

c. 峰值數據速率是5G 的50倍。

d. 延遲時間則是5G 的十分之一。

B. 架構需求：

a. 解決因行動裝置運算能力不足所引起的問題。

b. 在技術開發的最初階段及早導入人工智慧技術，實現新網路實體的靈活整。

C. 信賴需求：解決因廣泛使用用戶數據和人工智慧技術而衍生的安全及隱私問題。

a. 基於硬體、能提供程式碼安全運作且保護憑證的環境。

b. 應採用於「設計即安全」(Secure By Design)的原則，確保軟硬體均為可信任。

c. 透明化：確保系統能夠辨認人工智慧系統何時、如何獲取與個資相關的程式碼或數據。

d. 可安全使用空前大量資訊且嚴格保證資料隱私的機制。

7. 中國大陸-IMT-2030(6G)推進組

IMT-203所提出的「6G 總體願景與潛在關鍵技術白皮書」，認為未來6G 網路下的潛在應用場景將協助實現真實世界與虛擬數位世界的更深度融合。該白皮書中總共構思了8項應用場景，可以在民眾生活、社會生產、公共服務等各項領域的廣泛深入應用，支撐提升經濟發展高質量化的需求。以下將針對「6G 總體願景與潛在關鍵技術白皮書」的8項應用場景、10項潛在的關鍵技術方向以及新型網路技術進行說明：

(1)「6G 總體願景與潛在關鍵技術白皮書」之8項應用場景：

A. 沉浸式雲 XR：虛擬空間的廣闊天地

雲端化的 XR 技術中的將內容、渲染、空間計算等上雲，將顯著降低 XR 終端設備的計算負荷和耗能，降低線纜的束縛，XR 終端設備將變得更輕便、更沉浸、更智慧化，相對的也更利於商業化應用。

雲端化的 XR 系統將與新一代網路、雲計算、巨量資料、人工智慧等技術相結合，將能量運用於商貿創意、工業生產、

文化娛樂、教育訓練、醫療健康等領域，協助各行業的進行數位化轉型。

圖42、沉浸式雲 XR 示意圖
資料來源：6G 總體願景與潛在關鍵技術白皮書

B. 全息通訊：身臨其境的極致體驗

隨著無線網路傳輸能力、高解析度渲染及終端顯示裝置的不斷發展，未來的全息訊息傳遞將通過自然逼真的視覺還原，實現人、物及其周邊環境的三維動態交互，更加滿足人類對於人與人、人與物、人與環境之間的溝通需求。

未來全息通訊將廣泛應用於文化娛樂、醫療健康、教育、社會生產等眾多領域，人們不受時間、空間的限制，打通虛擬場景與真實場景的界限，使用戶享受身臨其境般的極致沉浸感體驗。

全息通訊將對資訊通信系統提出更高要求，在實現尺寸、高解析度的全息顯示方面，即時的互動式全息顯示需要足夠快的全息圖像傳輸能力和強大的空間三維顯示能力。另外應用於如遠端顯微手術等特殊場景，若是訊息封包有丟失狀況，即降低了系統的可靠性，所以此應用場景將會要求資料傳輸具有超高安全性和可靠性。

圖43、全息通訊示意圖
資料來源：6G 總體願景與潛在關鍵技術白皮書

C. 感官互聯：多維感官的交融回應

視覺、聽覺、視覺、觸覺、嗅覺和味覺等其它感官一直是人與人之間傳遞資訊的基本手段，6G 應用於2030年及未來世界，更多感官的資訊有效率的傳輸將成為通訊手段的一部分，感官互聯可能會成為未來主流的通訊方式，此部分可廣泛應用於醫療健康、技能學習、娛樂生活、道路交通、辦公生產和情感交互等領域。在此應用下，遠隔重洋的家庭成員可通過感官

互聯設備，將可感受到遠端家人的溫度、觸感，甚至在家中便可享受漫步風景區的的感覺。

為了支撐感官互聯的實現，需要保證觸覺、聽覺、視覺等不同感官資訊傳輸的一致性與協調性。在多維感官資訊協同傳輸的要求下，網路傳送的最大吞吐量預計將大量的增加，這正是6G 在效能上最基本的提升。此外，在安全方面的考量，由於感官互聯是多種感官相互合作的通信形式，為保護用戶的隱私，通訊的安全性必須得到更有力的保障，以防止用戶權益受損的事件發生。感官數位化表現方面，各種感覺都具有獨特的描述維度和描述方式，需要研究並統一其單獨和聯合的編解碼方式，使得各種感覺都能夠被有效地表示。

D. 智能互動：情感思維的互通互動

架構於未來6G 行動通訊網路，可望在情感互動和腦機互動(腦機介面)等全新研究方向上取得突破性進展。具有感知能力、認知能力、甚至會思考的智慧個體將取代傳統智慧交互設備，人與智慧體之間的支配和被支配關係將開始向著有情感、有溫度、更加平等的類人交互轉化。

具有情感交互能力的智能系統可以經由語音對話或面部表情識別等監測到使用者的心理、情感狀態，即時調節使用者情緒以避免影響個體的健康，降低隱患發生，通過心念或大腦來操縱機器，讓機器替代人類身體的某一些機能，彌補殘障人士的生理缺陷、短時間內學習大量知識和技能、實現「無損」的大腦資訊傳輸等。

在智能互動的場景中，智慧體將產生主動的智能的行為，同時可以實現情感判斷與回饋智慧，因此，資料處理量將會大幅增加。

E. 通訊感知：融合通信的功能拓展

未來6G 網路將可以利用通訊信號實現對目標的檢測、定位、識別、成像等感知功能，無線通訊系統將可以利用感知功能獲取周邊環境資訊，更智慧化且精確地分配通訊資源，挖掘潛在通訊能力。

毫米波或更高頻段的使用將可以加強對環境和周圍資訊的獲取，進一步提升未來無線系統相關的性能，催生更多的應用服務場景。

6G 將利用無線通訊信號提供即時感知功能，獲取環境的實際資訊，並且藉由先進的演算法、邊緣計算 EC 和人工智慧來產生超高解析度的圖像，在完成環境重構的同時，可實現釐米級的精確定位精度，從而實現構築虛擬城市、智慧城市的願景。

通過感知技術可以分辨出如行人、自行車、汽車、卡車等周圍環境物體。基於無線訊號所構建的感知網路相較現在以雷射雷達和攝影機為基礎感知環境，具備有更不受光和雲層等自然的外在因素影響的優勢，可以獲得全天候的高感知解析度和檢測機率。

此外，環境污染源、空氣含量監測和顆粒物(如 PM2.5)成分分析等可以透過更高頻段的感知來實現。

圖44、通訊感知示意圖
資料來源：6G 總體願景與潛在關鍵技術白皮書

F. 普惠智能：無處不在的智慧內核

預計2030年，會有越來越多的個人和家用設備、城市感知器、自駕車、智慧機器人等都將成為新型智慧終端機。不同於傳統的智慧手機，這些新型態終端設備不但可支援高速的資料傳輸，還可以實現不同智能設備間的協作與學習。可以想像，未來整個社會通過6G 網路連接起來的設備數量將到達上兆等級，智慧體終端可以不斷的學習、交流、合作和競爭，能夠現驅動對實際世界運作及發展的高效率模擬和預測，並給出建議相關決策。以下提出幾個面向的運作說明：

a. 在網路運維方面，智慧體將把網路的資料轉化為資訊並持續不斷學習和累積經驗，提供網路運作的分析和決策建議，支撐網路智能化控制，並且根據偵測到的環境變化對網路負載調整和協調。

b. 在智能工廠中，擁有大量用於生產的協作機器人，可以通過智慧體實現資訊的交互與學習，不斷更新自身行為模式，持續優化作業流程。

c. 未來6G 應用環境下還可以為無人機群、智能型機器人等無人系統提供即時動作處理策略，讓無人終端能夠高效率、精準地利用資源，實現高效控制與高精度定位。

d. 圖像、語音、溫度等資料也可以用於學習與協作上，人工智慧技術先將資料彙整起來，針對每個特定的環境下，實現不同智能終端機之間可靠、低延遲的通訊和協作，並且使用運作過程中所產生的巨量資料不斷學習，持續維持、提升工作效率和準確性。

e. 人工智慧應用的本質就是通過不斷增強的算力，對巨量資料中蘊含的價值進行充分挖掘與持續學習的過程。6G 網路將通過不斷的自主學習和設備間協作，持續為整個社會增加智慧，把人工智慧的服務和應用推到每個終端使用者，實現真正的普惠智能。

G. 數位分身：實際世界的數位鏡像

隨著感知、通信和人工智慧技術的不斷發展，實際世界中的實體或過程將可以鏡像複製數位世界，人與人、人與物、物與物之間可以在數位世界進行智慧的互動。在數位世界獲得豐富的資料，借助先進的人工智慧演算法建立模型，數位世界能

夠對實際實體或者過程實現類比、驗證、預測、控制，從而獲得實際世界的最佳狀態。未來6G 時代將進入虛擬化的數位分身世界，本白皮書列舉幾個可發生的應用：

a. 在醫療領域，醫療系統可以利用數位分身人體的資訊，做出診斷並預判最佳治療方案。

b. 在工業領域，透過數位技術優化產品設計，可降低成本並提高效率。

c. 在農業領域，利用數位分身技術對農業生產過程、必要因素等狀況進行模擬和推論，系統能夠事先預知已知生長不利的因素，通知農民預先即時處理，並可以提醒農民應於必要時機，執行適當的作物處理，提高農業生產力與土地利用效率。

d. 在網路運維的領域，可通過數位領域和實際環境閉環互動、自動化維運等操作，網路可快速適應複雜多變的動態環境。

e. 數位分身對6G 網路的架構和能力是很大挑戰，6G 網路需要擁有兆級的設備連接能力並滿足毫秒級的延遲要求，能夠精確、即時地獲得實際世界的細微變化。

f. 考慮到資料隱私和安全需求，需要6G 網路能夠在集中式和分散式架構下均可進行資料蒐集、儲存、處理、訓練和建模。通過快速的反覆運算優化和決策，按需採取集中式或分散式的建模，其中機器學習的聯合學習是一種可考慮的架構。

H. 全域覆蓋：無縫立體的超級連接

目前全球仍有超過30億人沒有基本聯網的能力，這些人大多數人分佈在農村和偏遠的地區，電信電信事業基於營運成本的考量不願意在這些地方建立通訊網路。此外，無人區、遠洋海域的通訊需求，基於營運及維運的考量，也無法通過部署地面網路來滿足。除了地球表面，無人機、飛機等空中設備也存在聯接網路的需求。

隨著應用場景的不斷擴展，地面蜂巢式網路與包括軌道衛星網路、高海拔平台站 HAPS、無人機等空中載具在內的空間網路相互融合，將構建起全球廣域覆蓋的空天地一體化三維立體網路，提供無死角的寬頻行動通訊服務。

全域覆蓋為全球沒有地面網路覆蓋的地區提供物聯網接入，保障緊急通訊、農作物監控、海上浮標資訊收集等服務；

提供精度為厘米級的高精度定位，實現高精度導航、精準農業等服務。此外，通過高精度地球表面成像，可提供緊急救援、交通調度等服務。

(2) 「6G 總體願景與潛在關鍵技術白皮書」之10項潛在的關鍵技術方向以及新型網路技術：

為滿足未來6G 更加豐富的業務應用以及性能的需求，需要在新型網路架構的基礎上創新，在關鍵核心技術領域實現突破。因此，「6G 總體願景與潛在關鍵技術白皮書」提出了10項潛在的關鍵技術方向以及新型網路技術，分述如下：

A. 內生智慧的新型網路

人工智慧技術在6G 網路中是原生的，從6G 網路設計之初就考慮引入人工智慧技術的支援，而不只是將人工智慧作為優化工具。總體上，可以從兩個不同角度來看待無線人工智慧在6G 時代的發展方向，即內生智慧的新型空中介面(Air interface)和內生智慧的新型網路架構。

所謂內生智慧的新型空中介面，即深度結合人工智慧、機器學習等技術，將打破現有無線介面模組化的設計框架，實現無線環境、資源、業務和用戶等多維特性的深度挖掘和利用，

以提升無線網路的高效性、可靠性、即時性和安全性，並實現網路的自主運 行和自我演進。

另外所謂內生智慧的新型網路架構，即利用網路節點的通訊、計算和感知能力，通過分散式學習、群智式協同以及雲、邊一體化算法部署，使得6G 網路原生可支援各類人工智慧應用，構建新的商機和以用戶為中心的業務體驗。

B. 增強型無線空中介面技術

6G 應用場景更加多樣化，性能指標更為多元，為滿足相應場景對輸送量/延遲/性能的需求，需要對實體層基礎技術進行特別的設計。在調製編碼技術方面，需要形成統一的編解碼架構，並兼顧多元化通信場景需求。

C. 新物理維度無線傳輸技術

除傳統的增強無線空中介面技術外，業界也在積極探索新的物理維度，以實現資訊傳輸方式的革命性突破，如智慧超表面技術、軌道角動量技術和智能全息無線電技術等。

D. 太赫茲與可見光通信技術

太赫茲(Terahertz/Tera-HZ)頻段(0.1~10THz)位於微波與光波之間，具有傳輸速率高、抗干擾能力強等特點，重點滿足

Tbps 量級大容量、超高傳輸速率的系統需求。太赫茲通信可作為現有空中介面傳輸方式的補充，將主要應用在全息通訊、微小尺寸通信、超大容量資料回傳、短距超高速傳輸等潛在應用場景。

可見光通信指利用從400THz 到800THz 的超寬頻譜的高速通信方式，具有無需授權、高保密、綠色和無電磁輻射的特點。可見光通信比較適合於室內的應用場景，可作為室內網路覆蓋的有效補充，此外，也可使用於水下通信、空間通信等特殊場景。

E. 通訊感知一體化

通訊與感知一體化是6G 潛在關鍵技術的研究熱點之一，其設計理念是要讓無線通訊和無線感知兩個獨立的功能在同一系統中實現且互惠互利。

一方面，通信系統可以利用相同的頻譜甚至共用硬體或訊號處理模組完成不同類型的感知服務。另一方面，感知結果可用於輔助通訊接取或管理，提高服務品質和通訊效率。

F. 分散式自治網路架構

6G 網路的規模較先前網路更為巨大、可提供網路體驗和支援導入更多樣化場景，需開展包括接入網和核心網在內的 6G 網路體系架構研究。對於接入網，應設計旨在減少處理延遲的架構和按需能力的架構，研究需求驅動的智能化控制機制及無線資源管理，引入軟體化、服務化的設計理念。對於核心網，需要瞭解分散式、去中心化、自治化的網路機制來實現靈活網路架構。

G. 確定性網路

新一代資訊技術與工業現場操作技術的融合促使行動通訊網路向「確定性網路」演進。工業製造、車聯網、智慧電網等對延遲敏感的業務發展，希望網路性能夠具備確定性的特性，包括：端點到端點訊息的及時交付，確定的最小和最大延遲等狀況、各種網路運行狀態下的丟包率、資料交付時有上限的亂序等。

H. 算力感知網路

為了滿足未來網路新型業務以及計算輕量化、動態化的需求，網路和計算的融合已經成為新的發展趨勢，業界提出了算

力感知網路的理念：將邊緣計算多樣的算力通過網路化的方式連接與協同，實現計算與網路的深度融合及協同感知，達到算力服務的按需調度和高效共用。

I. 星地一體融合組網

6G 將實現地面蜂巢網路、不同軌道高度上的衛星(高、中、低軌衛星)以及不同空域飛行器、高空平臺等融合而成全新的行動網路系統，通過地面網路實現城市熱點常態化覆蓋，利用天基、空基網路實現偏遠地區、海上和空中按需的覆蓋，具有組網靈活、韌性、抗毀等優點。而且空基、天基、地基網路的深度融合，構建包含統一終端、統一網路協定的服務化網路架構，可以在任何地點、任何時間、以任何方式支援各種資訊服務。

J. 支援多模信任的網路內生安全

資訊通訊技術與資料技術、工業操作技術融合、邊緣化和設施的虛擬化這些趨勢將會讓6G 網路安全邊界更加的模糊，傳統的安全信任模型已經無法滿足6G 網路的安全的需求，應該有能力支援如中心化的、公正第三者背書的以及去中心化的等多種信任模式共存的狀況。

而人工智慧、巨量資料與6G 網路的深度融合，也使得資料的隱私保護面臨著前所未有的新挑戰。新型態的網路傳輸技術和計算技術的發展，將帶動通訊密碼應用技術、智能韌性防禦體系，以及安全管理架構向具有自主防禦能力的內生安全架構演進。

8. 中國大陸-中國移動

中國移動提出了所謂「三體四層五面」6G 總體架構設計，為業內首次系統化的6G 網路架構設計。其中圖45為中國移動建議之「三體四層五面」6G 總體架構示意圖，相關內容如下：

(1)「三體」是架構的空間視角，描述6G 網路實體的客觀存在形式，分為網路本體、管理編排體和數位分身體。

(2)「四層」是架構的邏輯視角，展現6G 網路設計的結構與組織，是由資源與運算層、路由與連接層、服務化功能層、開放使能層所組成。

(3)「五面」是架構的功能視角，展示6G 網路功能的劃分和組成，包括控制面、使用者面(用戶面)、資料面、智慧面(智能面)與安全面，五個基本功能面。

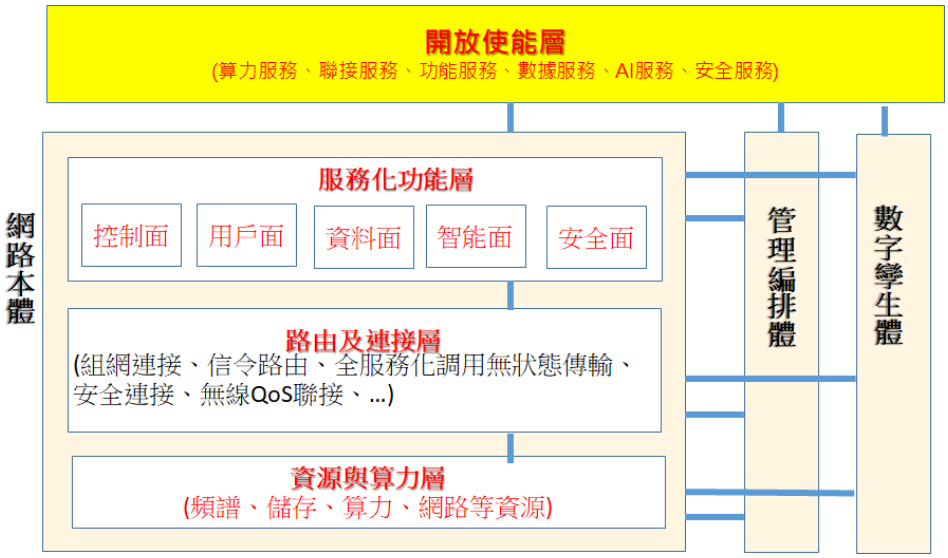


圖45、中國移動定義之三體四層五面之6G 總體架構圖
資料來源：中國移動 6G 網絡架構技術白皮書

在總體架構設計的基礎上，白皮書進一步提出了架構實現的分身設計、系統設計和組網設計。通過數位元化方式創建虛擬分身體，實現具備網路閉環控制和全生命週期管理的數位分身網路架構。

通過服務定義端到端的系統，實現全服務化系統架。在組網上，實現具有分散式、自治、自包含特徵，支援按需定制、隨插即用、靈活部署的分散式自治網路。

在有關跨領域應用，中國移動提出三個可能應用：

(1) 沉浸式多媒體應用：網路必須能支援大規模使用者通訊和計算的基礎環境，並對網路指標提出更極致的要求。如元宇宙業務，須提供交互協同網路服務，要求網路從以「能力」為導向轉變為以「服務」為導向，建立多種協同模式，

更好地支撐強交互的需求。在使能技術方面，需要交互技術、AI 技術、數位分身技術、區塊鏈技術和非同質化代幣(Non-Fungible Token, NFT)實現從網路到服務的轉化。

(2) 通感互聯：6G 網路架構將支援通訊能力與感知能力融合，拓展傳統通訊能力的維度，感知能力將是6G 行動通信系統基本通訊能力之外的一大重要能力。6G 基地台需要對覆蓋區域具備監控能力，同時還可對天氣、自然環境狀態、城市立體構造等具備即時測量感知能力，將感知結果進行即時處理分析。

(3) 泛在覆蓋：6G 網路將支援統一的一體化架構，打破地理限制，擴展網路覆蓋維度。架構於其覆蓋範圍廣、靈活部署、超低功耗、超高精度的特徵，支援智慧交通、精細化社會治理等。6G 網路需要支援衛星通訊、空間通信與地面通訊的一體化發展，從不同層次進行融合，構建空天地海一體化通訊系統，實現全球無縫立體覆蓋，用戶隨時隨地接入。

9. 中國大陸-賽迪智庫無線電管理研究所

以下就賽迪智庫的6G 基礎環境願景，探索未來應用服務下新的運作場景、新的業務形態和新的商業模式：

(1) 人體數位分身

目前數位科技對人體健康的監測在即時性和精準性尚未有很深的著墨，而隨著6G 技術的到來，以及生物科學、材料科學、生物電子醫學等的進一步成熟，未來可望實現完整的「人體數位分身」。在人體使用大量智慧感知器(>100個/人)，針對重要器官、神經系統、呼吸系統、情緒狀態等進行精確即時的「鏡像映射」，建構一個完整人體在虛擬世界的複製品，實現對於人體個人化健康資料的即時監測。

此外，結合核磁共振、彩色超音波、電腦斷層掃描、生化等醫療專業的影像和檢驗結果，利用人工智慧技術可對個體的健康狀況提供精準評估和即時處理，結果可提供給專業醫療機構精準診斷和個人化手術方案的重要建議。

(2) 空中高速上網

目前在飛機上進行「空中上網」服務主要有兩種模式—地面基地台模式和衛星模式。如採用地面基地台模式，由於

飛機具備移動速度快、跨界幅度大等特點，空中上網服務將面臨高機動性、頻繁切換以及基地台覆蓋範圍不夠等挑戰。如採用衛星通信模式，在空中上網服務品質可以相對得到保障，相對需要成本也較高。為了解決這一難題，6G 將採用全新的通訊技術以及超越「蜂巢」的新穎網路架構，在降低網路使用成本下，同時確保可在飛機上為使用者提供空中高速上網服務。

(3) 基於全息通訊的 XR

虛擬實境與擴增實境(VR/AR)被業界認為是5G 最重要的需求之一。隨著技術的快速發展，預期2030年以後，資訊互動的形式將由虛擬實境與擴增實境逐漸演變至延展實境(XR)為主，最終將全面實現無線全息通訊。使用者可隨時隨地享受全息通信和全息顯示帶來的體驗升級，視覺、聽覺、觸覺、嗅覺、味覺乃至情感將通過高傳真延展實境充分被引發，用戶將不再受到時間和地點的限制，以「自我」為中心，享受虛擬教育、虛擬旅遊、虛擬運動、虛擬繪畫、虛擬演唱會等完全沉浸式的全息體驗。

(4) 新型智慧城市群

目前，城市中不同的基礎設是由不同的部門分別建設和管理，絕大部分城市公共基礎設施的資訊感知、傳輸、分析、控制仍處於各自為政的狀況，缺乏統一的管理平臺。6G 將採用統一網路架構，引入新業務場景，構建高效、完備的網路。

未來6G 網路仍由多家電信事業投資共建，採用網路虛擬化技術、軟體定義網路(Software-Defined Networking)和網路切片(Network Slicing)等技術將實際網路和邏輯網路分離。人工智慧深度融入6G 系統之中，實際應用至高效傳輸、無縫介接、內生安全、大規模部署、自動維護等多個層面。

(5) 全域緊急通訊搶險

6G 將由地基、海基、空基和天基網路構建，成為分散式跨地域、空域、海域的一體化網路。到 2030年以後，完成6G 在沙漠、深海、高山等現有網路盲區的部署，實現全域無縫覆蓋。基於其覆蓋範圍廣、靈活部署、超低功耗、超高精度和不易受地面災害影響等特點，6G 網路在緊急通訊搶險、「無人區」即時監測等領域應用前景無限，能夠發揮強大的效益。例如，在發生地震等自然災害造成地面通訊網路毀壞

時，可以整合天基網路(衛星)和空基網路(無人機)等通訊資源，實現廣域、無縫覆蓋、隨時連接、資源整合支援急難現場遠距離訊息溝通和扁平化的緊急指揮。此外，利用6G 網路，還可以對於海洋、河流等容易發生自然災害的區域進行即時動態監控，提供颱風、洪水等災害預警服務，將災害損失降到最低。

(6) 智能工廠

利用6G 網路的超高頻寬、超低延遲和超可靠等特性，可以對工廠內車床、機台、零件等運行資料進行即時採集，利用邊緣計算和人工智慧等技術，在終端直接監測資料，並且即時下達執行命令或是提供建議。另外在6G 中已可引入區塊鏈技術，讓智能工廠所有終端之間溝通不再需要經過雲端中心，可以直接進行資料交換，實現去中心化操作，提升生產效率。

基於先進的6G 網路，工廠內任何需要聯網的智能設備/終端均可靈活組建網路，智能裝備的組合同樣可根據生產線的需求進行靈活調整和快速部署，從而能夠主動適應製造業

個人化、定制化消費者對商家模式(consumer to business, C2B)的大趨勢。

(7) 連接機器人與自主系統

6G 的發展對於連接機器人和自主系統的部署有很大的助益，如無人機快遞系統就是很顯著的一個應用案例。此外，基於6G 無線通訊的自動車輛可以極大地改變人們的日常生活方式，6G 系統將促進自動駕駛汽車或無人駕駛汽車的規模部署和應用，自動駕駛汽車通過各種感知器來感知周圍環境，6G 系統將支援可靠的車聯網以及車與伺服器之間的連接。

而對於無人機，6G 將支持無人機與地面控制器之間的通訊。無人機在軍事、商業、科學、農業、娛樂、城市治理、物流、監控、救災等許多領域都有很大可以想像的應用空間。當蜂巢式基地台不存在或遭到損壞無法工作時，無人機可以作為高海拔平台站 HAPS 為該區域的使用者提供廣播和上網服務。

10. 日本-NTT DoCoMo

NTT DoCoMo 該份白皮書提到其總體目標是持續提升5G的傳輸容量、高速傳輸、低延遲與多連接特性，同時發展更高頻的傳輸技術。以下就 DoCoMo 提出有關6G 的特性需求、8類6G 技術領域進行說明：

(1) NTT DoCoMo 所提出6G 特性需求：

A. 超高速大通訊容量：峰值速率>100Gbps

B. 超廣泛覆蓋：Gbps 全覆蓋、新覆蓋區域(如天空、海洋 與太空等)

C. 超低功耗與成本降低：支援 mmW/THZ 網路與終端 、終端無需電池充電

D. 超低延遲：E2E 超低延遲(<1ms)

E. 超可靠通訊：適用於各種應用案例的受保證的 QoS，如安全隱私。

F. 超大規模連結與感知：大規模終端連結(10M/平方公里)、感知功能與公分級的高精度定位。NTT DoCoMo 認為，未來運作模式需要迅速接收實際網路世界的各種資訊，並透過人工智慧技術分析後將結果輸出給用

戶以提供回饋，所以提高人工智慧性能是實現超低延遲的關鍵。另外，在其他各種應用程式中，NTT DoCoMo 期待人工智慧能夠實現人與物之間的通訊，如可直接與患者交談的全息虛擬醫生，進行問診。期待將網路延遲從5G 的5毫秒以內，降低至6G 的1毫秒以下，讓民眾在到處隨時都可以使用優質的無線服務。

(2) NTT DoCoMo 所提出8類6G 技術領域

A. 新網路拓樸：部署高密度分佈式天線的干擾控制技術、低成本的分佈式天線部署方法、前傳和回傳技術。

B. 包含非地面網路的覆蓋範圍擴展：擴展與 NTN 兼容的無線接、如何在高效的地面網路中使用頻率、如何實現配備 HAPS 的電台與地面網路之間的合作、擴大覆蓋範圍。

C. 頻率擴展和改進頻譜利用率：闡明太赫茲帶電波的傳播特性、建立傳播模型、太赫茲頻帶的設備技術問題(小型化，低功耗，高散熱等)、建立適合太赫茲訊號波形和無線技術等、優化包括現有頻段在內的多個頻段的使用。

D. mMIMO 技術與無線傳輸技術的進一步發展：檢驗多元素/多層 mMIMO 技術、分佈式 MIMO 中的傳播路徑控制技術、針對現有頻段的新無線電技術的開發。

E. 增強超可靠低延遲通信(Enhanced Ultra-Reliable and Low Latency Communication, eURLLC)和工業物聯網：支持包括極其嚴格的要求和「混合流量」在內的各種要求、實現更高的可靠性和更高的安全通信、公共網路與單個網路和網路結構之間的合作。

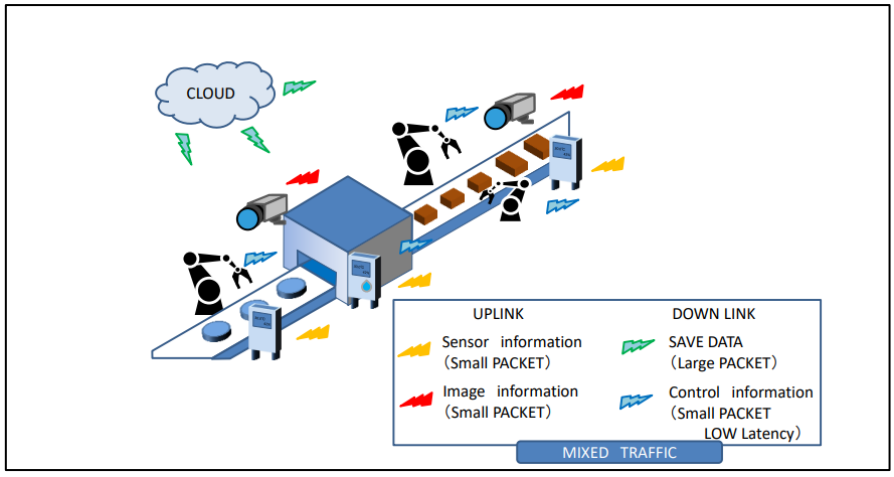


圖46、支援工業網路中的各種類型的資料流
資料來源：White Paper 5G Evolution and 6G

F. 除了行動通訊技術外的多種無線技術擴展集成:與其他網路技術的合作或集成方法及控制技術，使用者不需知道他們正在使用那種無線技術傳輸資料。

G. 行動網路的多功能化和人工智慧：同時實現無線通信和感知技術，無線電源技術等、審查適合引入人工智慧技術的無線標準。

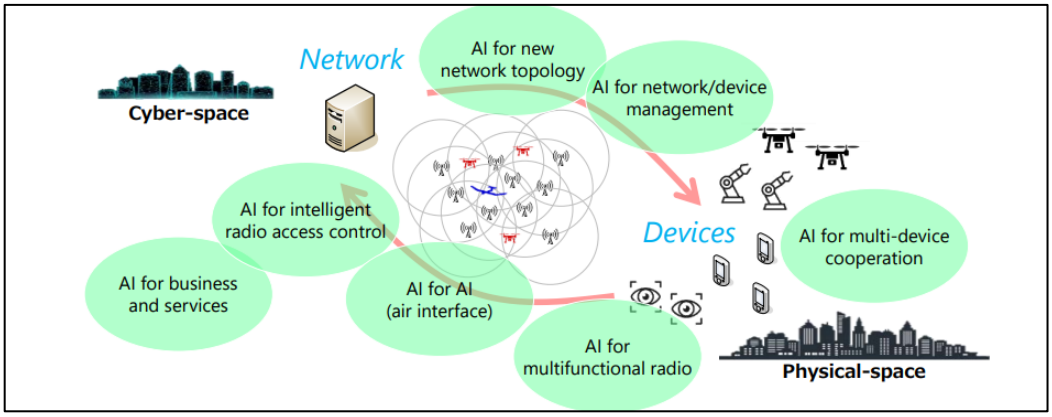


圖47、人工智慧在行動通信各個領域應用
資料來源：White Paper 5G Evolution and 6G

H. 網路架構：網路拓撲結構、靈活的網路功能配置、 網路的簡化、支持多種接入技術。

在 NTT DoCoMo 白皮書描述了以「人體增強」(Human aug mentation)、「大腦技術」(Brain Technologies)、「感知共享」(Perception Sharing)和「多層感知資訊」(Multilayered sensory information)等感知應用技術與6G 網路相結合，將有可能通過這些技術的雙向互動提供更多種使用案例，拉近人、空間、時間的認知距離，進一步豐富使用者的生活。

近年來因為疫情的關係，目前人與人之間使用數位通訊技術的溝通方式變得越來越重要。如在商業中採用視訊方式舉行會議，可望在未來的商業環境中會更有進一步利用。由於該領域的通訊技術主要集中在視覺和聽覺訊息，所傳達的虛擬現實在臨場感或氛圍展現上效果比較不逼真，如果存在更新類型的感官訊息可用於傳輸，則將有可能實現數位通訊，同時傳達更真實的存在感或氛圍。從實現福祉的角度來看，必須開發技術來實現這種具有逼真的存在感和氛圍的複雜通訊。

另外，使人體增強技術的使用案例，可以考量旨在消除現實世界和虛擬世界之間邊界的使用案例。在這種使用情境下，將可以從不同的環境中獲得每種身體的知覺，或者透過網路傳輸個人的感覺。也就是說，在不移動的情況下，將能夠從遙遠的地方為個人肢體收集不同的訊息，可以觸摸事物或感受事物。此外，不僅可以坐在一個地方進行多項任務活動，還可以從遠程位置參加會議，通過網路同時在多個地方進行工作。

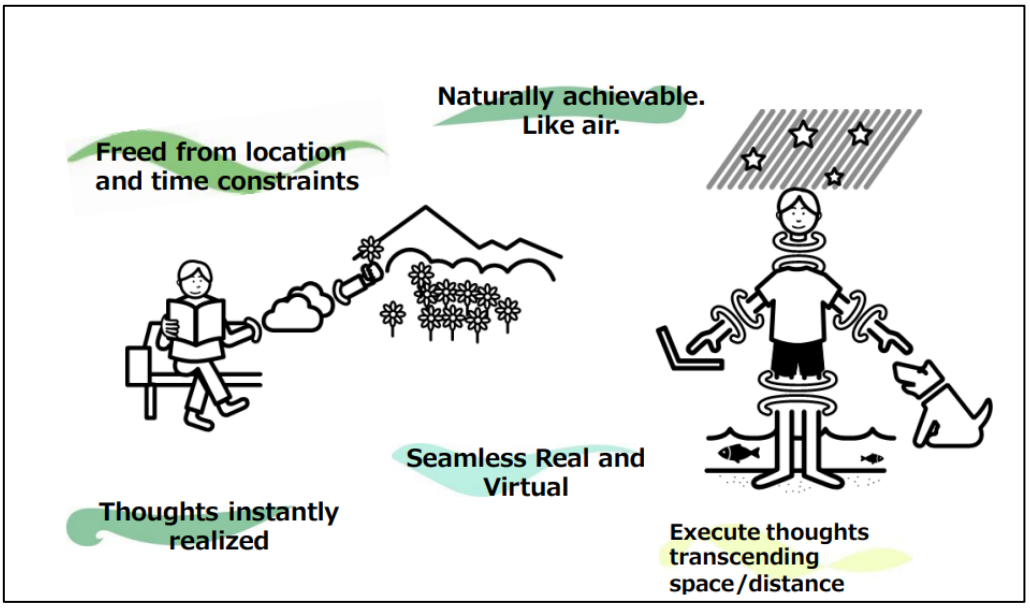


圖48、整合人體增強、大腦技術及感知共享應用範例示意
資料來源：White Paper 5G Evolution and 6G

(三)研析成果

綜觀前述所提到的世界各主要國家、組織、廠商對於6G 的想像、期望、規劃及布局，可以瞭解各界對於未來6G 發展都具備有相當期待，然而對於其所期待的願景都存在有若干異同。

本計畫綜整前述研析，彙整6G 行動網路關鍵性技術指標、6G 行動網路的跨領域應用情境兩個面向進行分析與比較，提供相關政策規劃者的參考，相關彙整資訊詳如表6、表7。

1. 6G 行動網路關鍵性技術指標

在6G 基礎建設技術需求發展下，全球致力於6G 發展的廠商對此議題均有明確期待及說明，如日本 NTT DoCoMo 針對峰值容量通訊、覆蓋模式、延遲等面向的功能，都有明確

的數字指標，相關指標描述都可以在廠商所推出白皮書中有詳細的描述。德國諾基亞貝爾實驗室也針對6G 所應有的效能需求，在流量大小、可接受延遲、連結大小、定位精度、組態適應時間以及裝置特性等面向提出對應的期待。

彙整各單位對於6G 相關關鍵性技術指標如表6所示：

表6、各單位對於6G 關鍵性技術指標表

關鍵性 技術指標	相關單位預期
通訊容量	• 美國 ATIS-Next G 計畫：1Tbps • 芬蘭-Oulu 大學：100Gbps~1Tbps • 南韓-科學技術情報通信部：1Tbps • 南韓-三星：1,000 Gb • 中國大陸-IMT-2030 (6G) 推進組：100GBps~1Tbps • 日本-NTT DoCoMo：至少 100Gbps
傳輸延遲	• 美國 ATIS-Next G 計畫：0.1ms • 芬蘭-Oulu 大學：0.1ms • 南韓-三星：小於 0.1ms • 中國大陸-IMT-2030 (6G)推進組：0.1ms • 日本-NTT DoCoMo：小於 1 ms
定位能力	• 芬蘭-Oulu 大學：室內 10 cm　室外:1m • 中國大陸-IMT-2030 (6G)推進組：室內 10 cm 室外:1m • 日本-NTT DoCoMo：最小公分等級
網路覆蓋	• 美國 ATIS-Next G 計畫：整合地面與非地面網路 • 中國大陸-IMT-2030 (6G)推進組：星地一體 • 中國大陸-賽迪智庫無線電管理研究：包含蜂巢網路、衛星通訊、無人機通訊、高空平台等 • 日本-NTT DoCoMo：包含與非地面網路的聯結

關鍵性 技術指標	相關單位預期
終端連結數密度	• 美國 ATIS-Next G 計畫：1 億/平方公里 • 芬蘭-Oulu 大學：1 億/平方公里 • 中國大陸-賽迪智庫無線電管理研究：1 億/平方公里 • 中國大陸-中國移動：1 千萬～1 億/平方公里 • 日本-NTT DoCoMo：1 千萬/平方公里

資料來源：本計畫整理

2. 6G 行動網路的跨領域應用情境

世界各大廠商及機構所推出的白皮書,除了針對6G 行動通訊的基礎建設各面向的需求有所描述外，另有一部分的重點是架構於各廠商所提出的基礎建設之下，能發展出更多的新興應用服務,以及實現相應的應用服務所需要的必要技術。這些相對應的必要技術可提供資源不是很充足的廠商參考，以因應在未來6G 行動的發展下,尋求適合發展的應用服務技術，提前布局6G 行動環境。

如德國諾基亞貝爾實驗室所提出有關6G 的關鍵應用場景，分別有產業 AR、遙現(Telepresence)、安全監視/瑕疵檢測、分散式運算/自動化動、態數位雙生/虛擬世界、資料中心無線化、零耗能裝置以及生體感知與人工智慧。而對應的關鍵應用技術有機器學習、利用新頻譜、定位精度、逼近網路極限、新型網路架構以及資安,隱私與信任。南韓三星則認為

6G 將提供下一個「超級互連體驗」，提出三項關鍵服務分別為真正的沉浸式 XR、高度逼真的行動全息顯示(High-Fidelity Mobile Hologram)以及數位複製(Digital Replica)。而實現這些關鍵服務的技術主要為用使用大量用戶資料和人工智慧技術，另外對於後續衍生個資及安全議題也需要有考量。

本計畫整理各單位植基於6G 網路環境的應用服務及可能的使用情境，期可提供未來規劃相關技術之參考，相關應用情境及技術對照詳如表7。

表7、6G 網路下應用情境及技術對照表

應用	提出情境單位	6G 關鍵特性	應用相關技術
XR 相關應用	✓ 美國 ATIS-Next G 計畫：多感官延展實境 ✓ 歐盟 Hexa-X 計畫：XR 技術及全息呈現 ✓ 德國-諾基亞貝爾實驗室 ✓ 芬蘭-Oulu 大學 ✓ 南韓-三星：真正的沈浸式延展實境 ✓ 中國大陸 IMT-2030：沉浸式雲 XR、全息通訊 ✓ 中國大陸-中國移動：沉浸式多	✓ 網路傳輸數據速率和延遲會限制影音刷新率	✓ 延展實境相關技術 ✓ 感知應用技術 ✓ 人工智慧 ✓ 定位

應用	提出情境單位	6G 關鍵特性	應用相關技術
	媒體應用 ✓ 日本-NTT DoCoMo：人體增強		
機器人應用	✓ 美國 ATIS-Next G 計畫：聯網機器人和自主系統 ✓ 歐盟 Hexa-X 計畫：聯網機器人 ✓ 芬蘭-Oulu 大學 ✓ 德國-諾基亞貝爾實驗：集群機器人/無人機 ✓ 中國大陸-賽迪智庫無線電管理研究所：連接機器人與自主系統	✓ 可信任、安全、彈性、數位世界體驗以及人工智慧原生	✓ 人工智慧 ✓ 感知應用技術
感知相關應用	✓ 美國 ATIS-Next G 計畫：6G 分散式感知和通訊 ✓ 德國-諾基亞貝爾實驗 ✓ 南韓-科學技術情報通信部 體感、自駕車、智慧城市、智慧工廠 ✓ 南韓-三星：高度逼真行動顯示 ✓ 中國大陸 IMT-2030：感官互	✓ 全球覆蓋 ✓ 大規模同時覆蓋	✓ 資訊安全 ✓ 異質網路結合 ✓ 分散式人工智建模技術 ✓ 感知應用技術

應用	提出情境單位	6G 關鍵特性	應用相關技術
	聯、通訊感知、普惠智能中國大陸-賽迪智庫無線電管理研究所：基於全息通訊的 XR、新型智慧城市群、全域緊急通訊搶險、智慧工廠 ✓ 中國大陸-中國移動：通感互聯、泛在覆蓋 ✓ 日本-NTT DoCoMo：感知共享、腦機互動		
個性化用戶體驗	✓ 美國 ATIS-Next G 計畫：個人化用戶體驗	✓ 全球覆蓋 ✓ 大規模同時覆蓋	✓ 人工智慧 ✓ 感知技術 ✓ 分散式雲與通訊系統 ✓ 資安技術(隱私保護) ✓ 感知應用技術
數位分身	✓ 歐盟 Hexa-X 計畫：數位分身 ✓ 德國-諾基亞貝爾實驗室 ✓ 南韓-三星：數位複製 ✓ 中國大陸 IMT-2030：數位分身 ✓ 中國大陸-賽迪智庫無線電管理研究所：人體數位分身	✓ 兆級的設備連接能力並滿足毫秒級的延遲	✓ 人工智慧(聯合學習) ✓ 資安技術(隱私保護 ✓ 感知應用技術

應用	提出情境單位	6G 關鍵特性	應用相關技術
感官互聯	✓ 美國 ATIS-Next G 計畫：多感官延展實境 ✓ 中國大陸 IMT-2030：感官互聯、智能互動	✓ 大規模同時覆蓋、頻寬和擁塞控制、QoE	✓ 人工智慧(聯合學習) ✓ 感知應用技術 ✓ 延展實境 ✓ 資安技術
遠端醫療、教育、保健	✓ 歐盟 Hexa-X 計畫 ✓ 南韓-科學技術情報通信部		✓ 資安技術(隱私保護) ✓ 感知應用技術
資料市集	✓ 芬蘭-Oulu 大學		✓ 資安技術

資料來源：本計畫整理

四. 計畫執行情形-6G 資安偵測與防護研析

臺灣現有工業電腦與伺服器廠商以及小型基地臺製造商，積極投入開放式無線接取網路（Open Radio Access Network, O-RAN）架構以及邊緣運算（Edge Computing, EC）平台網通設備的市場，電信三雄為了節流規劃 5G 企業專網採購國產第三方設備供應商的開放式無線接取網路(O-RAN)以及邊緣運算(EC)平台設備，網通設備「白牌化」商機應運而生。

隨著量子電腦運算(Quantum Computing)技術進入蓬勃發展的階段，使得現有的公鑰密碼系統受到挑戰，因為近期傳出中國駭客打算收集已加密的高價值資料，等到量子電腦發展突破，就能立即解開他們取得的加密內容，量子電腦運算破密技術如今已成真實威脅。

美國國家電信暨資訊管理局(National Telecommunications and Information Administration, NTIA) 透過 2020 年 11 月通過的「美國電信法(USA Telecommunications Act)」，加速全美 5G O-RAN 架構網路的布署和使用為了倡導推動建立「開放並可互操作」5G 網路架構，美國聯合全球數十家科技和電信企業成立「開放無線接入網政策聯盟(Open RAN Policy Coalition)」。美利堅合眾國眾議院(U.S. House)於 2021 年 10 月通過「開放式無線接取網路推廣法(Open RAN Outreach Act)」，支援全美加速 O-RAN 架構網路的布署和使用。

電信設備業者 Ericsson 認為相較於軟硬體高度整合的專有無線基礎設施，O-RAN 架構帶來了全新、額外的接觸點，以及軟體和硬體的脫鉤，導致技術天生就不安全。歐洲執行委員會 European Commission 在開放式無線接取網路依安研析報告(Report on the cybersecurity of Open RAN)亦點出 O-RAN 架構開放介面的安全議題，並將 O-RAN 的歐盟協調風險評估納入歐盟 5G 工具箱(EU 5G Toolbox)之中。開放式無線接取網路聯盟(Open Radio Access Network Alliance, O-RAN Alliance)的安全工作小組(Security Working Group, SWG)針對 Open RAN 開放式架構的安全確保機制，將採用全球行動通訊系統協會(Groupe Speciale Mobile Association,

GSMA)制定的網路設備安全保證方案(Network Equipment Security Assurance Scheme, NESAS)搭配 3GPP 制定的產品資安確保標準(Security Assurance Specification, SCAS)。

此外，由於假基地台(False Base Station, FBS)是從 GSM 系統就存在的安全性議題，故本計畫實作偽冒第六代行動通訊先期網路技術核心網路(Pre 6th Generation Mobile Network Core Network, Pre-6GC)誘騙終端用戶的實驗。

故本計畫針對以下偵測與防護應用的應用情境進行研析，研提 6G 通訊層和服務層威脅研析，包含相關威脅攻擊與其應對偵防技術，內容包括(一)Pre-6G 專網系統的多元應用情境資安威脅、(二)非地面網路的系統架構與安全威脅、(三)開放式無線接取網路安全確保機制、(四)開放式無線接取網路假基地台的資安威脅、(五)採用人工智慧的資安威脅以及與(六)量子安全(Quantum Safety)先期研析。6G 產業業者可透過此報告事先針對待解決的資安議題與挑戰進行跨產業合作與技術研發，亦可透過本報告建議尋求/發展解決方案，提高安全強度，提升國產產品資安防護能力與國際競爭力。

(一) Pre-6G 專網系統的多元應用情境與資安威脅

Pre-6G 專網行動邊緣計算(Multi-access Edge Computing, MEC)技術在靠近(proximity)用戶設備(User Equipment, UE)的網路位置，提供雲端運算的服務及儲存能力，藉以達成提供超低延遲 (Ultra-Low Latency, ULL)及超高頻寬(Ultra-High Bandwidth, UHB)的服務。3GPP 的第二工作組-架構工作組(SA2 Working Group – Architecture, SA2 WG)完成 Pre-6G 專網多接取邊緣運算架構的標準技術規格，使電信事業未來可以實現視訊分析、健康醫療或企業服務等不同類型的低延遲 Pre-6G 應用服務。

1. Pre-6G 專網系統的多元應用情境

依據 3GPP 的技術標準(Technical Specifications, TS)文件 23.501 所定義之 Pre-6G 獨立網組(SA)之多接取邊緣運算架構由用戶設備(UE)、Pre-6G 擷取網路(Pre-6GAccess Network, Pre-6G AN)、邊緣運算(EC)及 Pre-6GC 所組成，其中 Pre-6GC 由多個「網路功能(Network Function, NF)」的模組構成，並透過「以服務為基礎之介面」來實現網路功能，而網路資料庫功能(Network Function Repository Function, NRF)支持網路功能(NF) 服務註冊與狀態監測等機制，以實現 NF 服務自動化管理。

並透過控制平面(Control Plane, CP)與使用者平面(User Plane, UP)分離，可以為網路功能虛擬化 NFV 及多接取邊緣運算 MEC 提供較為完善的網路架構，如圖 49 所示。

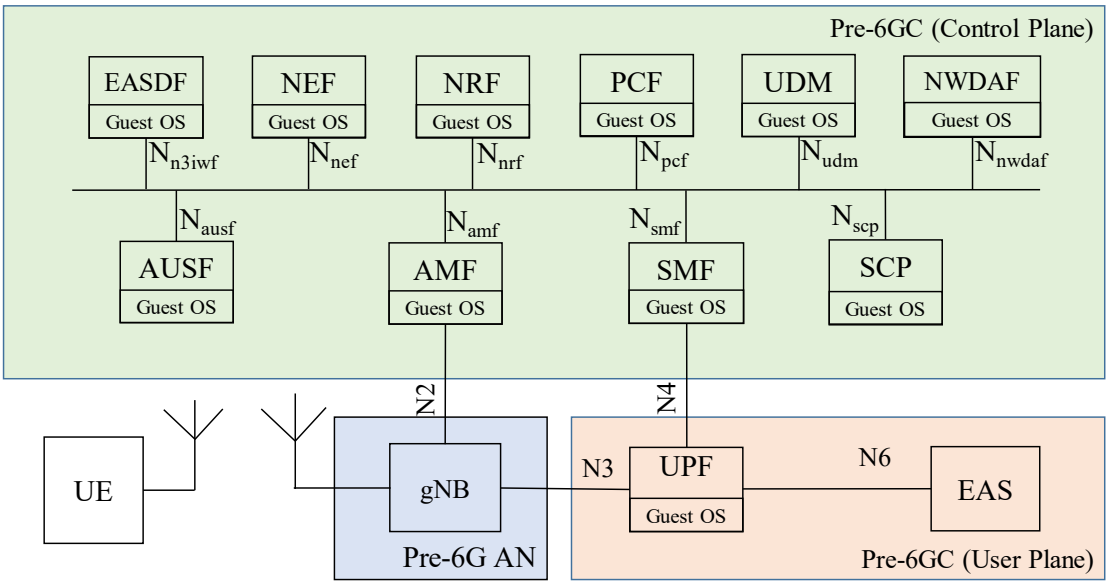


圖49、以服務基礎架構為導向的系統架構圖
資料來源：本計畫整理

其中 Pre-6GC 網路功能(NF)包含用戶平面功能 (User Plane Function, UPF)、存取與行動管理功能 (Access and Mobility Management Function, AMF)、認證伺服器功能 (Authentication Server Function, AUSF)、連結管理功能 (Session Management Function, SMF)、政策控制功能 (Policy Control Function, PCF)、統一資料管理功能 (Unified Data Management, UDM)、網路資料庫功能 (Network Repository

Function, NRF)、網路揭露功能 (Network Exposure Function, NEF)、服務通訊代理 (Service Communication Proxy, SCP)、網路數據分析功能 (Network Data Analytics Function, NWDAF)與邊緣應用伺服器探索裝置(Edge Application Server Discovery Function, EASDF)，而 Pre-6G 擷取網路(Pre-6G AN)則為基地台(gNodeB, gNB)。

Pre-6G 專網多接取邊緣運算的布建型態依據 3GPP 的 TS 文件 23.501 的規範分為由企業建構的「獨立布建專網(Stand-alone Non-Public Network, SNPN)」以及由電信營運商主導的「與公網整合專網(Public network integrated Non-Public Network, PNiNPN)」兩大類。當企業欲建立起 Pre-6G 專網環境時，可透過租用電信營運商的 Pre-6G 網路達成 PNiNPN 的布建型態，如圖 50 所示。其中 Pre-6GC 網路功能的 UPF 分為公網路由的用戶平面功能 UPF 使用之 C-PSA (Central PDU Session Anchor)與邊緣應用伺服器 (Edge Application Server, EAS)的用戶平面功能 UPF 使用之 L-PSA PSA (Local PDU Session Anchor)兩條資料路徑。

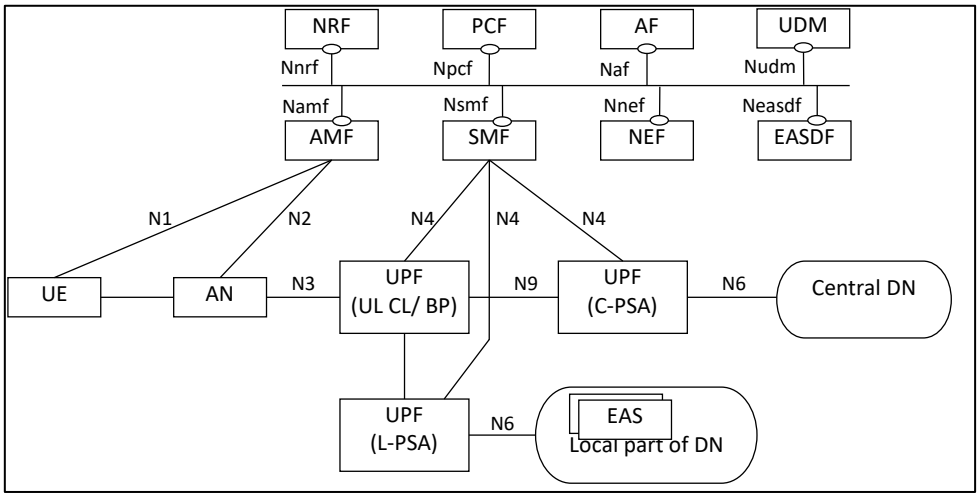


圖50、與公網整合專網(PNiNPN)的系統架構圖
資料來源：3GPP TS 23.548 V18.0.0 (2022-12)

針對與公網整合專網可以進一步分為三種布建型態模式：(1)在公有電信網路透過網路切片方式切一塊專屬企業用專網、(2)建置企業專用基地台與邊緣應用伺服器 EAS、(3)建置企業專用基地台與企客共用邊緣應用伺服器 EAS 提供跨廠區服務。當企業需要超可靠度低延遲通訊 URLLC 的專網環境時，則需要採用獨立的核心網路加上獨立基地台的 Pre-6G 獨立布建專網 SNPN，如圖 51 所示。

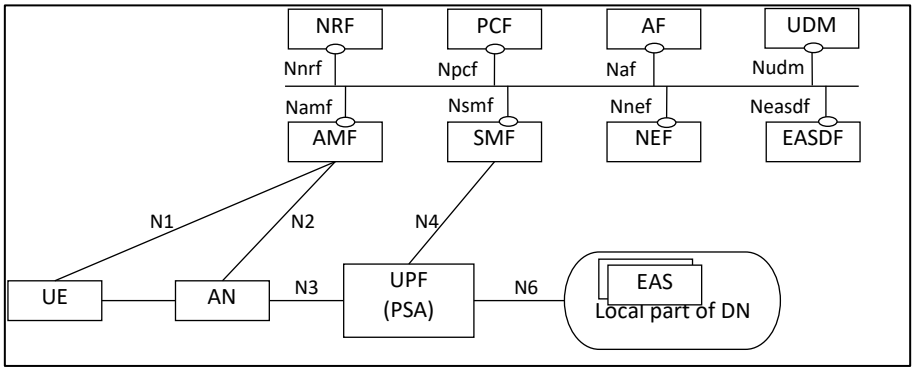


圖51、獨立布建專網(SNPN)的系統架構圖
資料來源：3GPP TS 23.548 V18.0.0 (2022-12)

3GPP 的第六工作組-關鍵任務應用工作組(SA6 Working Group - Mission-critical applications, SA6 WG)在將關鍵任務應用服務的技術規格移植到各垂直領域的應用服務，透過應用層功能元件和應用程式介面(Application Programming Interface, API)的標準技術規格，來滿足鏈結到各垂直行業的 Pre-6G 專網生態系統需求，進一步為 Pre-6G 提供垂直應用程序的通用服務平台做準備。為了達成低延遲和高頻寬通訊的垂直領域應用服務， Pre-6G 專網布建時需要垂直領域的邊緣應用伺服器 EAS 與電信業者間進行緊密整合，如圖 52 所示。透過啟用邊緣應用程序(Application Architecture for enabling Edge Applications, EDGEAPP)相關標準規範的制定，可以將用戶設備的資料導流至邊緣應用伺服器，以實現視訊分析、無人車、智慧製造、健康醫療或企業服務等不同類型的低延遲 Pre-6G 應用服務。

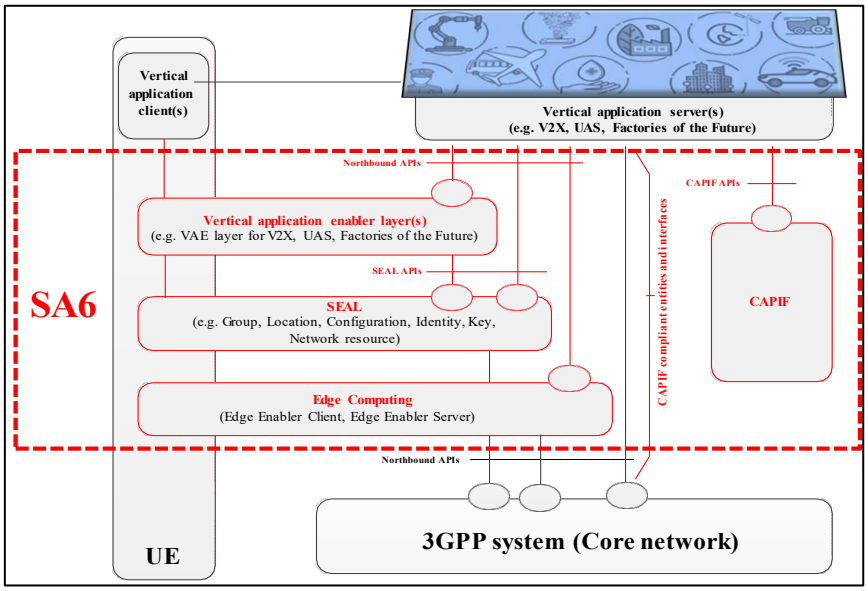


圖52、緊密整合垂直應用服務與多接取邊緣運算示意圖

資料來源：3GPP

啟用邊緣應用程序架構(EDGEAPP)支援在 Pre-6G 專網多接取邊緣運算平台上開發和託管應用程序的架構體，其包括如用戶設備移動性，邊緣應用程序可移植性，服務差異化和靈活部署，並提供邊緣應用程序對應之北向應用程式介面(Northbound Application Programming Interface, Northbound API)使及 Pre-6G 專用網路功能與邊緣運算服務(Edge Computing Service, ECS)之間緊密整合。

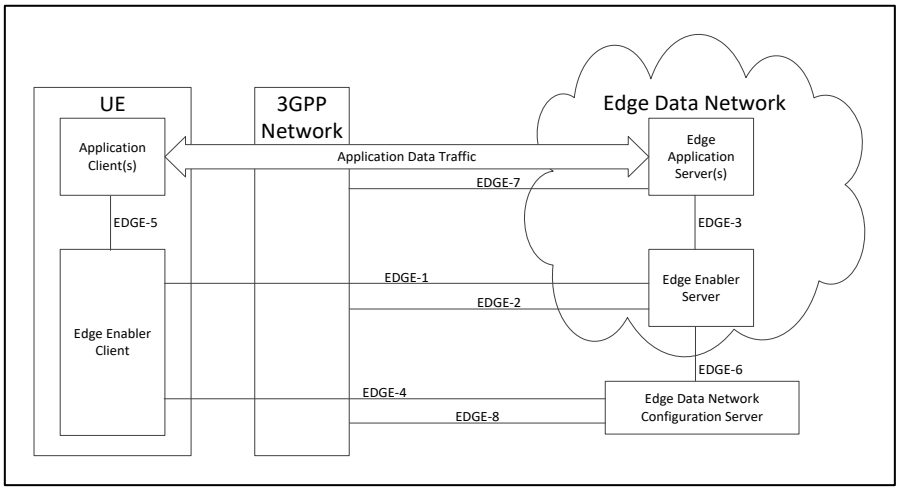


圖53、啟用邊緣應用程序架構(EDGEAPP)圖
資料來源：3GPP

共用應用程式介面框架(Common Application Programming Interface Framework, CAPIF)主要是參考開放行動通訊聯盟 (Open Mobile Alliance, OMA)以及歐洲電信標準協會 ETSI 的 5G 專網多接取邊緣運算之應用程式介面框架制定 3GPP 的技術標準文件 23.222 的技術標準規格。該標準規格結合第二工作組-架構工作組所制定之服務能力揭露框架(Service Capability Exposure Framework, SCEF)與網路曝光功能 NEF 之 Northbound APIs 以及第四工作組-編碼工作組制定之多媒體廣播多點服務 (Multimedia Broadcast/Multicast Service, MBMS)的 xMB 之北向應用程式介面，建立一個承載電信 Pre-6G 專網垂直領域應用服務框架的統一北向應用程式介面框架標準。

其允許第三方垂直領域業者藉由該共用應用程式介面構架來提供用戶設備相關垂直應用服務，同時導入兩個第三方垂直領域業者間透過共用應用程式介面構架相互連接以及以聯盟形式部署垂直應用服務的關鍵功能。並由共用應用程式介面構架核心功能(CAPIF Core Function, CCF)、應用程式介面揭露功能(API Exposure Function, AEF)與應用程式介面調用者(API Invoker)等三個主要實體組成，以支援第三方業者透過共用應用程式介面構架進行垂直領域應用服務分散式部署。

(1) 應用程式介面構架核心功能提供所有應用程式介面的核心功能與存儲資料庫，包含各垂直領域應用服務註冊(registration)、註銷(de-registration)、服務發現(service discovery)、身分驗證(authentication)和授權(authorization)、收費(charging)和日誌記錄所需使用的介面與相關功能。

(2) 應用程式介面揭露功能提供第三方垂直領域業公開的API。

(3) 應用程式介面調用者可以透過如 NEF 的應用程式介面揭露功能 AEF，訪問應用程式介面構架核心功能 CCF，以

執行如服務註冊(registration)以及身分驗證(authentication)和授權(authorization)的服務。

2. Pre-6G 專網系統的資安威脅

Pre-6G 專網多接取邊緣運算多元應用情境包含支援車聯網(Vehicle-to-Everything services, V2X)、未來工廠(Factories of the Future, FoF)、無人飛行系統系統(Unmanned Aerial Systems, UAS)、遠距醫療(Telemedicine)、虛擬實境 VR 以及擴增實境 AR 等垂直應用服務。Pre-6G 專網多接取邊緣運算除了要考量資訊安全外，還需要滿足使用穿戴式物聯網(Wearable Internet-of-Things, WIoT)技術實現遠距醫療的病患以及透過車聯網實現自動駕駛的乘客之隱私權保障。Pre-6G 專網多接取邊緣運算仰賴標準化的先進技術實現萬物相連的多元應用情境，用戶設備由於經常處於聯網狀態，會在不知情的情況下將使用數據傳送到網路上，因此增加個人資料外洩的隱私問題和資安威脅詳如表 8。

表8、隱私(Privacy)的安全威脅

威脅議題	安全威脅
用戶隱私資料竊聽	行動用戶永久識別碼(Subscriber Permanent Identifier, SUPI)擷取器(Catcher)導致用戶隱私被攔截與竊聽的威脅。

威脅議題	安全威脅
竊取用戶身分	Pre-6G 中提供輔助身分驗證功能，當此身分驗證機制遭受攻擊，可竊取行動用戶的個人資料與位置等隱私資訊。

資料來源：本計畫整理

此外，依據 3GPP 的技術研究報告文件 33.861 與 33.836，行動通訊物聯網(Cellular Internet-of-Things IoT, CIoT)與車聯網需要面對下列的隱私安全威脅，如表 9 所示。

表9、行動通訊物聯網與車聯網的隱私安全威脅

領域	威脅議題	安全威脅
行動通訊物聯網(CIoT)	非擷取層(Non-Access Stratum, NAS)資訊包含的行動通訊物聯網(CIoT)新參數的隱私保護	要防範透過交換參數以及和用戶設備行為關聯達成重新標識用戶設備的威脅
車聯網(V2X)	透過 PC5 介面的單播資訊隱私保護	能夠將 L2 識別碼與應用層識別碼(Identity, ID)真實或長期的識別碼做鏈結，進一步在時空上追蹤特定終端。這種可追蹤性(trackability)和可鏈結性(linkability)將對端點的隱私造成威脅
	透過 PC5 介面的群播資訊隱私保護	
	透過 PC5 介面的廣播資訊隱私保護	

資料來源：本計畫整理

由於 Pre-6G 應用情境多，部分的安全威脅仍然在討論中，其中車聯網 V2X、無人飛行系統系統 UAS、未來工廠 FoF 以及遠距機器人手術(Remote Robotic Surgery, RRS)等應用情境需要依賴 URLLC 技術。由於超可靠度和低延遲通訊極度嚴格的延遲與可靠度需求將對現有網路通訊系統與安全性帶來巨大的挑戰。依據 3GPP 的技術研究報告文件 33.825，其應解決的安全威脅詳如表 10。

表10、超可靠度和低延遲通訊(URLLC)的安全威脅

威脅議題	安全威脅
冗餘(redundant)傳輸的安全性	攻擊者可以監視資料流(data streams)並識別兩個資料流是否被用於冗餘資料流傳輸。如果相應的無線電承載(Radio Bearer, RB)或 N3 介面隧道缺乏完整性、機密性和重播保護，則攻擊者可以利用此類資訊針對 URLLC 服務發動攻擊。
支援用戶平面(UP) 冗餘資料高可靠性傳輸的安全性	兩個或多個用戶平面路徑必須採用同等的安全性保護，才能實現用戶平面冗餘資料通信的高度可靠性。破壞其中一個用戶平面路徑將使 URLLC 服務喪失高度可靠性。
處理建立多個協定資料單元(PDU)會話的	當攻擊者知道在第一條路徑上啟用了完整性保護而第二條路徑上未啟用完整性保護時，攻擊者可透過干擾第一條路徑並竄改第二條路徑從基

威脅議題	安全威脅
冗餘資料傳輸之用戶平面(UP)安全策略	地臺(gNB)轉發到用戶平面功能的用戶平面資料。
超可靠度和低延遲通訊服務 URLLC 的安全策略	如果 URLLC 服務的用戶平面沒有完整性保護，則可能在傳輸期間遭受竄改。如果 URLLC 服務的用戶平面使用完整性保護，則可能導致無法接受的時間延遲。如果 URLLC 服務沒有採用特定服務的安全策略，則可能導致服務沒有採用足夠保護的風險。
低延遲換手的安全性	當介面(如 N2 介面)沒有安全保護時，攻擊者可以竊聽、注入或竄改介面上傳輸的金鑰和安全參數。 如果 AMF 遭到入侵，且用戶設備的金鑰不具有後向安全性(backward security)，那麼攻擊者將能夠解密用戶設備先前與網路間的傳輸資料。且用戶設備的金鑰不具有前向安全性(forward security)，那麼攻擊者將能夠解密用戶設備未來與網路間的傳輸資料。 如果 AMF 遭到入侵，或裝置遭受到中間人(Men in the Middle, MiTM)攻擊，則攻擊者可以將演算法降階為容易破解的演算法設定。

威脅議題	安全威脅
服務品質(QoS)監控保護	當端對端 QoS 的監視過程缺乏安全保護時，攻擊者可能會修改資料封包或訊息導致系統獲得錯誤的延遲報告(latency report)。

資料來源：3GPP TR 33.825

而未來工廠在建置 Pre-6G 專網多接取邊緣運算平台時，需要新增如時間敏感網路(Time Sensitive Networking, TSN)以及區域網路型態服務(LAN-type service)等特定技術功能於 Pre-6G 專網多接取邊緣運算平台上，這些技術的資安風險議題都需要被納入考量。

Pre-6G 與 TSN 的整合是 Pre-6G 做為工業通訊系統中非常重要的組成，像是 Pre-6G 需要支援時間敏感網路的控制器協作、時間同步(Time Synchronization)、時間敏感網路限制延遲(Bounded Latency)與時間敏感網路可靠性要求等面向。依據 3GPP 的技術研究報告文件，時間敏感通訊(Time Synchronization, TSC)應解決的安全威脅如表 11 所示。

表11、時間敏感通訊(TSC)的安全威脅

威脅議題	安全威脅
保護 Pre-6G 系統與時間敏感網路間的交互作用介面	如果與時間敏感網路通訊的介面缺乏機密性保護、完整性保護以及重播保護，則攻擊者可能會竊聽資料、修改資料以及發動重播攻擊。
時間敏感通訊的時間同步	Pre-6G 與時間敏感網路的橋接器可能以下弱點：阻斷使用嚴格延遲邊(strict latencies boundaries)的確定性傳輸(deterministic transmission)。變造主/從網路單元間的時鐘同步和全域時間基準的主時鐘(Grand Master, GM)。變造時間感知排程(Time-aware Scheduling)和流量整形(traffic shaping)。變造通信路徑的選擇以及預留的頻寬和時間間隔。

資料來源：3GPP TS 23.502

固網與行動融合(Fixed and Mobile Convergence, FMC)技術讓 Pre-6G 與現有區域網路(Local Area Network, LAN)及無線區域網路(Wireless Local Area Network, WLAN)共同使用核心網路組成第六代行動通訊先期技術區域網路(Pre-6G LAN)架構。依據 3GPP 的技術研究報告文件，其應解決的安全威脅如表 12 所示。

表12、第六代行動通訊先期技術區域網路(Pre-6G LAN)的安全威脅

威脅議題	安全威脅
Pre-6G LAN 的用戶設備認證和授權	Pre-6G LAN 系統應提供一種相互身分驗證和授權機制，以確保僅提供授權的用戶設備使用 Pre-6G LAN group 服務。如果不進行身分驗證和授權，則任何未經授權的用戶設備都可獲得 Pre-6G LAN group 服務，導致 Pre-6G LAN group 通信遭到盜用服務和阻斷服務的風險。
Pre-6G LAN group 的使用者平面安全政策	如果屬於同一 Pre-6G LAN group 的用戶設備和基地台間的用戶平面流量中最弱的安全等級將成為整個 Pre-6G LAN group 的通信路徑安全等級。如果其中一個用戶設備關閉機密功能，縱使 Pre-6G LAN group 的其他用戶設備的通信路徑均被加密，但其交換的資訊仍然會被竊聽。

資料來源：本計畫整理

(二) 非地面網路的系統架構與安全威脅

隨著行動資料量不斷地增加並支援各類新業務與應用場景，Pre-6G 系統預期將具有龐大的移動數據和設備連接，而無線接取網路 RAN 除了需考慮關鍵性能指標要求、網路商業營運能力以及具備持續演進能力這三方面的因素外，全球電信事業也希望與第三方設備供應商合作推動介面開放並標準化，以完全開放互通的介面並結合無線接取網路智能控制(Radio Access network Intelligent Controller, RIC)，來降低行動通訊網路設備建置的成本，因此 Pre-6G 無線接取網路的基礎架構有走向開放、虛擬化、高靈活性與節能的趨勢。依據 3GPP 的第十八版本(Release-18, R18)

標準，也就是進階升級版 5G 系統架構，結合陸海空的開放式 Pre-6G 系統架構將會作為 6G 系統的基礎。

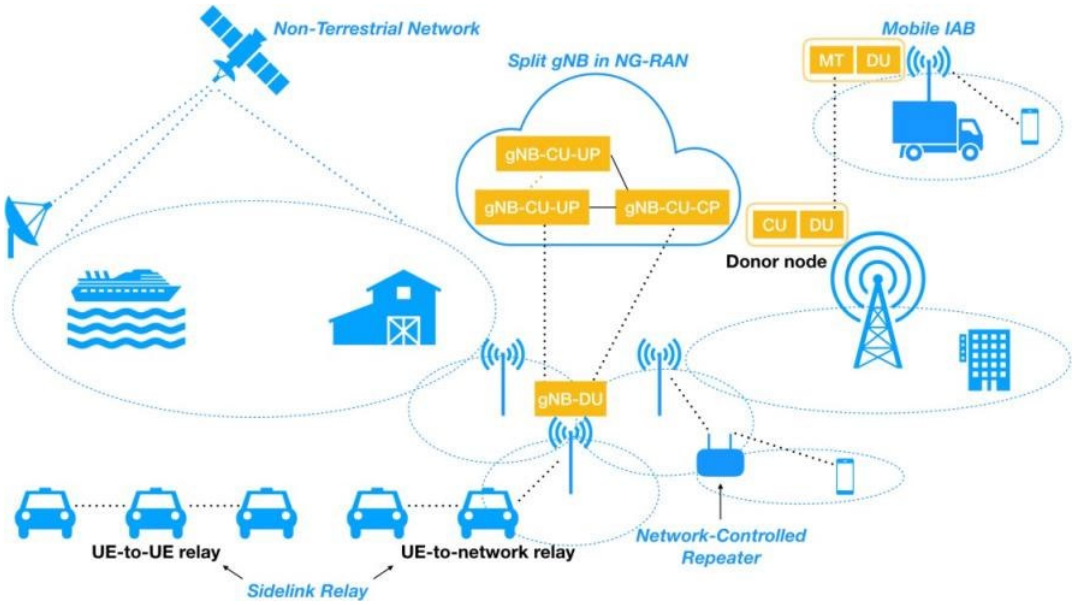


圖54、開放式 Pre-6G 網路系統架構圖
資料來源：An Overview of 5G Advanced Evolution in 3GPP Release 18

1. 非地面網路系統架構

非地面網路 NTN 指透過太空載體(Space-Borne)或高空載體(Air-Borne)配置通訊傳輸設備的方式實現大範圍的通訊網路覆蓋。其中，太空載體分為同步軌道衛星(Geostationary Orbit, GEO)、中軌道衛星(Medium-Earth Orbit, MEO)與低軌道衛星(Low-Earth Orbit, LEO)等三大類。同步軌道衛星所處位置約位在距離地表高度三萬六千公里處；中軌道衛星所處位置約位在八千公里至一萬八千公里處；低軌道衛星約位在五百公里至一

千五百公里處。而 HAPS (High Altitude Platform Station）為架設於高空的新一代通訊平台，又稱為高空偽衛星（High Altitude Pseudo Satellite），其系統位置與性質介於地面網路和衛星通訊之間，所處位置約位在二十公里至五十公里處。

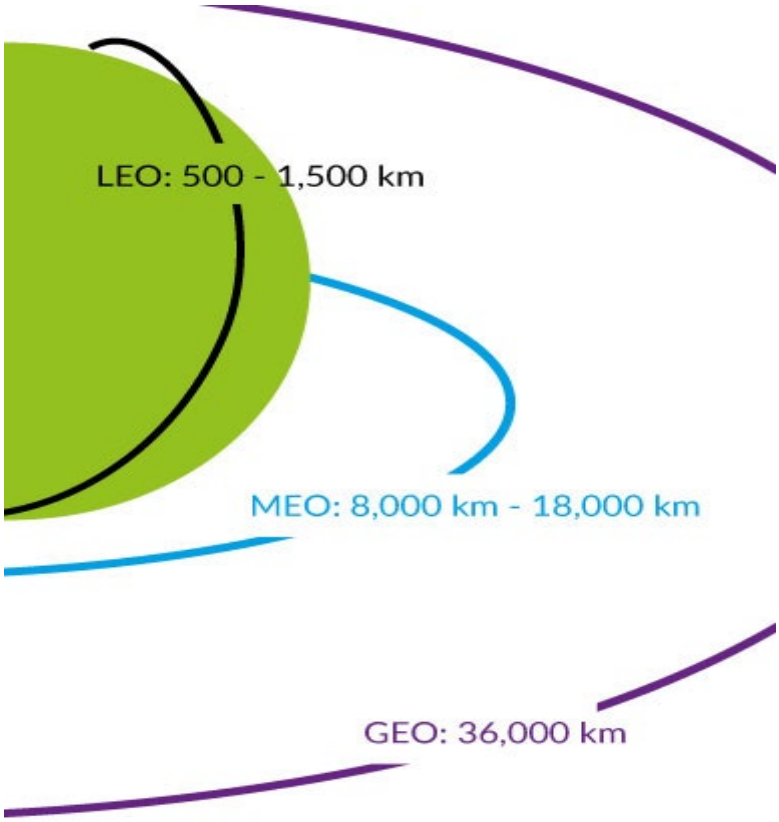


圖55、非地面網路示意圖
資料來源：3GPP，NTN & Satellite in Rel-17 & 18

國際通信聯盟 ITU 與 3GPP 等國際組織也開始重視以 HAPS 作為空中行動通訊基地台。國際通信聯盟無線通信部門 ITU-R 於 2000 年及 2006 年分別提出 ITU-R M.1456 及 ITU-R M.1641 兩篇報告，便開始對使用 HAPS 作為行動通訊系統提供服務的技術要求與作業條件進行研究。

於 2019 年世界無線電通訊大會(World Radio communication Conference, WRC-19)的第 247 號決議文(Resolution 247)中，研擬將 HAPS 視為行動通訊基地台(High-altitude platform stations as IMT base stations, HIBS) 作為地面行動通訊網路的一部分，並研議與地面行動通訊基地台(Mobile Base Stations, MBS)使用相同的通訊頻段。

而在 2015 年， 3GPP 的第十四版本(Release-14, R14)標準已經開始展高海拔平台站相關研究，並於 R15 標準、R16 標準以及 R17 標準，持續強化高海拔平台站與地面網路間的網路互通性技術標準化工作。

行動通訊與衛星通訊係為兩個獨立發展產業，隨著低軌道衛星通訊技術突破，應用需求增強與衛星寬頻成本下降，非地面網路將會納入 3GPP 的 R17 標準，預期將加速推動與衛星通訊接軌的腳步。故兩者產業鏈不僅有更多互動合作機會，且有望打造全新產業格局，而未來的 Pre-6G 將會是各種技術並存。NTN 在布建時可能採用 Pre-6G O-RAN 的系統架構，導入基地臺(gNB)集中單元與分散單元分割(CU-DU split)網路架構，如圖 56 所示。

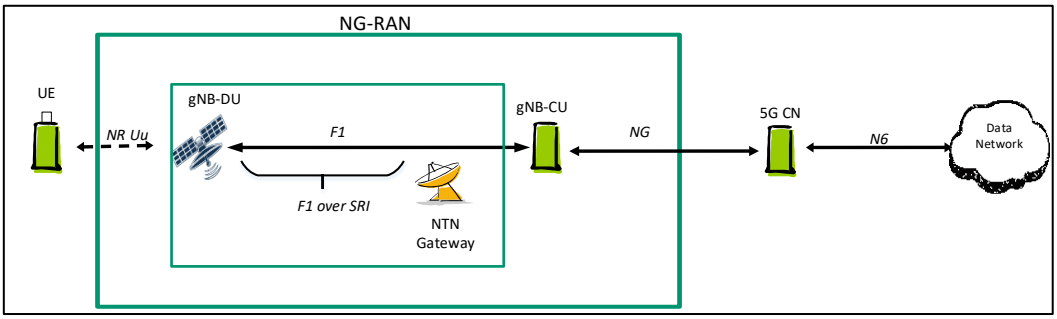
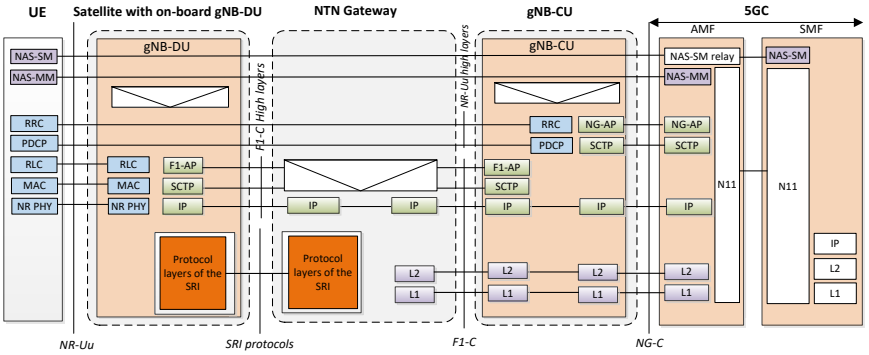
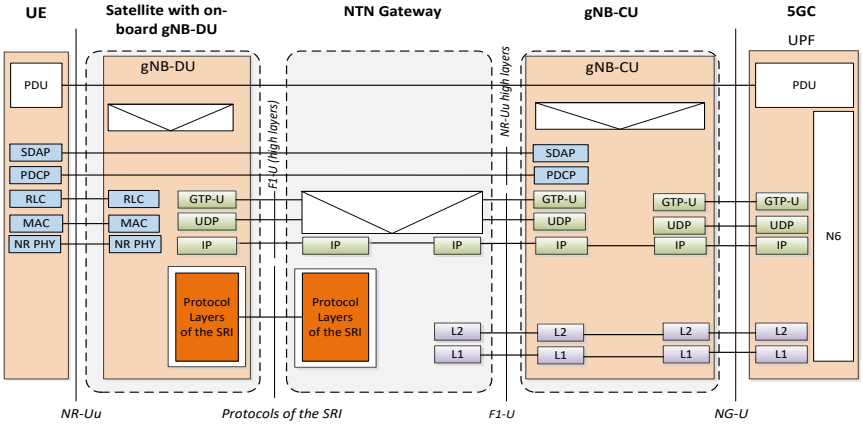


圖56、第六代行動通訊先期技術非地面網路示意圖
資料來源：3GPP TR38.821



(a) 控制平面



(b) 用戶平面

圖57、第六代行動通訊先期技術非地面網路通訊協定示意圖
資料來源：3GPP TR 38.821

2. 非地面網路的安全威脅

當非地面網路 NTN 導入基地臺(gNB)集中單元與分散單元分割(CU-DU split)網路架構後，電信事業可跳過傳統電信設備商，直接向硬體設備業者採購電信設備，有利於創建高靈活性的 Pre-6G。3GPP 在分散式基地臺標準制定過程中，於 3GPP 的技術研究報告文件 38.801 中，提到集中單元(Central Unit, CU)與分散單元(Distributed Unit, DU)分割的好處在於能夠靈活搭配硬體以節省布署成本。

報告中總共提出 8 種集中單元與分散單元分割架構的方案，如圖 58 所示，分別為於無線資源控制(Radio Resource Control, RRC)和封包數據匯聚協定(Packet Data Convergence Protocol, PDCP)間進行分割的第 1 方案、於 PDCP 和無線鏈路控制(Radio Link Control, RLC)間進行分割的第 2 方案、於上層無線鏈路控制(Upper-RLC)和下層無線鏈路控制(Lower-RLC)間進行分割的第 3 方案、於 RLC 和媒體存取控制(Media Access Control, MAC)間進行分割的第 4 方案、於上層媒體存取控制(Upper-MAC)和下層媒體存取控制(Lower-MAC)間進行分割的第 5 方案、於 MAC 和實體層(Physical layer, PHY)間進行分割

的第 6 方案、於上層實體層(Upper-PHY)和下層實體層(Lower-PHY)間進行分割的第 7 方案以及於 PHY 和射頻 RF 信號處理間進行分割的第 8 方案。

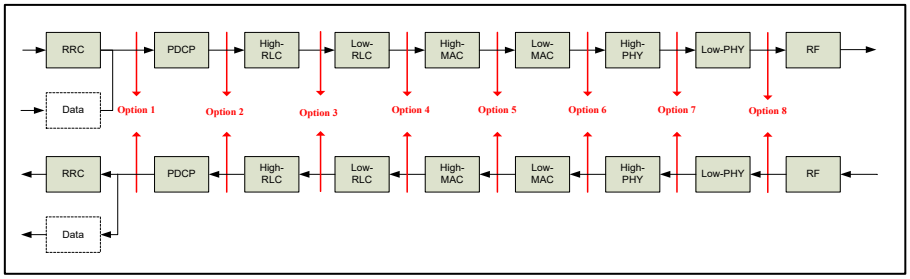


圖58、集中單元與分散單元分割架構方案
資料來源：3GPP TR 38.801

在考量 CU 與 DU 分割架構下，為了實現性能和負載管理的協調以及落實網路功能虛擬化(Network Function Virtualization, NFV)的架構。最後 gNB-CU 與 gNB-DU 分割架構採用了第 2 方案，兩者間透過 F1 介面連接。其中 gNB-CU 負責無基地臺中 RRC 與服務數據適配協定(Service Data Adaptation Protocol, SDAP)以及 PDCP 等網路功能，而 gNB-DU 則負責 RLC 與 MAC 以及 PHY 等網路功能。

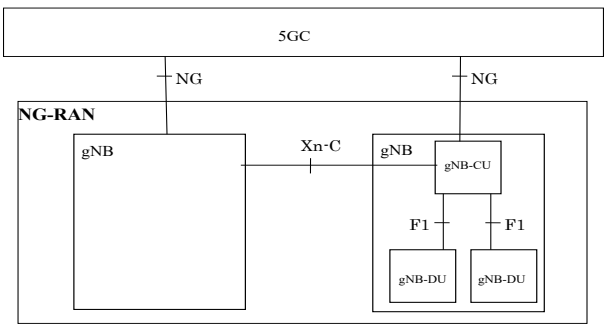


圖59、基地臺集中單元與分散單元分割架構
資料來源：3GPP TS 38.401

3GPP 也基於第 2 方案之集中單元與分散單元分割標準架構，如圖 60 所示，探討並制定了支援集中單元控制平面與用戶平面分離(CP-UP Separation)的架構及相關介面，將 gNB-CU 進一步拆分為基地臺集中單元-控制平面(gNB-CU Control Plane, gNB-CU-CP)與基地臺集中單元-用戶平面(gNB-CU User Plane, gNB-CU-UP)。優點包括增加網路運作管理的彈性與最佳化無線接取網路功能的效率，及增加不同廠商間設備的互通性，然而相對也會增加網路的複雜度、維運工作及信號傳輸的延遲。

gNB-CU-CP 主要負責基地臺中，RRC 與 PDCP 控制平面功能，gNB-CU-UP 者則負責基地臺中，SDAP 以及封包數據匯聚協定用戶平面功能，兩者間透過 E1 介面連接。

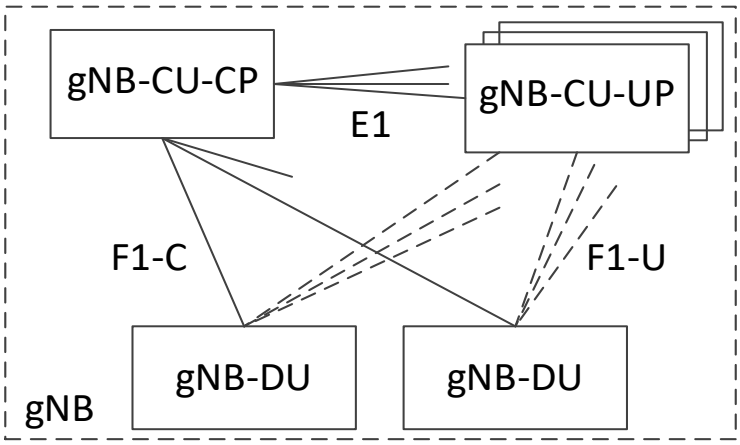


圖60、基地臺集中單元之控制平面與用戶平面分離架構圖
資料來源：3GPP TS 38.401

在依據 3GPP 的技術研究報告文件 38.806 技術研究報告所描述的分離架構中，一個基地臺(gNB)可由一個 5G gNB-CU-CP、多個 gNB-CU-UPs 以及多個 gNB-DUs 所組成。而一般電信事業在布署時，只會將一個 gNB-CU-UP 連接至一個 gNB-CU-CP，並將一個 gNB-DU 連接至一個 gNB-CU-CP，不過在高可用性的應用情境下，是可以連接至多個 gNB-CU-CP。

基地臺功能分割(functional split)的方式需要滿足不同應用場景的需求，如傳輸時延的多變性。在 3GPP 的技術研究報告文件 33.801 中，提到如何對基地臺進行功能分割取決於網路布署的場域、限制及服務等，如需要根據不同的應用服務設定低延遲與高傳輸率等不同的 QoS。因為基於第 2 方案之集中單元與分散單元分割標準架構不適用於低延遲的布署場域，為了滿足超可靠度低延遲通訊場域的需求， 3GPP 在分散式針對於上層實體層(Upper-PHY)和下層實體層(Lower-PHY)間進行分割的第 7 方案進一步進行分析討論。

O-RAN Alliance 主要是制定 3GPP 沒有標準化的低層分割(low layer split)架構(如圖 61 所示)，並提供協定外的裝置管理為主，發展重點也著重於開放硬體架構，故開放式無線接取網

路的架構不會重複定義 gNB-CU-CP 與 gNB-CU-UP 及 gNB-DU。其所制定的開放式無線接取網路分散單元(O-RAN Distributed Unit, O-DU)又稱為低層分割的集中單元(Lower Layer Split Central Unit)，與開放式無線接取網路無線電單元(O-RAN Radio Unit, O-RU)透過通用公共無線電介面(Common Public Radio Interface, CPRI)或演進版通用公共無線電介面(evolved Common Public Radio Interface, eCPRI)介面相連，O-RAN Alliance 所制定開放式無線接取網路低層分割的架構如圖 61 所示。

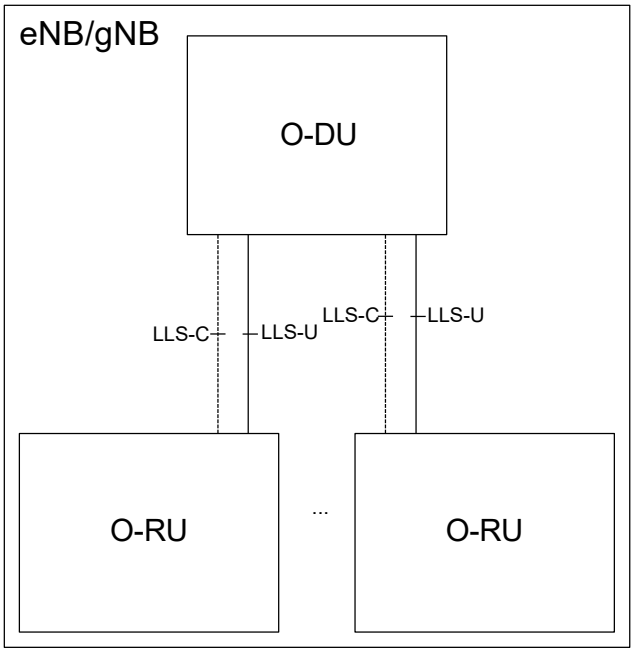


圖61、開放式無線接取網路基地臺低層分割(low layer split)
資料來源：3GPP TS 33.801

Pre-6G O-RAN 的集中單元負責 RRC、SDAP 以及 PDCP 等用戶平面的網路功能，涉及到用戶設備之控制平面與用戶平面封包的完整性和機密性。而分散單元DU與無線電單元(Radio Unit, RU)則負責無線鏈路控制 RLC 與媒體存取控制 MAC 以及實體層 PHY 等網路功能，不會涉及到 Pre-6G 用戶設備的完整性和機密性，但當其遭受攻擊時仍然會影響用戶設備的可用性。

依據 3GPP 的網路產品類別之威脅和關鍵資產的安全保證規範研究報告文件 33.926，以及開放式無線接取網路資安威脅建模和補救分析(O-RAN Security Threat Modeling and Remediation Analysis)研究報告，Pre-6G 的資安風險分析可以歸納出八種威脅層面的主要威脅，分別為 3GPP 定義的網路介面威脅 (Threats relating to 3GPP-defined interfaces)、O-RAN 定義的網路介面威脅(Threats relating to O-RAN-defined interfaces)、識別碼欺騙 (Spoofing identity)、竄改(Tampering)、否認性(Repudiation)、資訊揭露(Information disclosure)、阻斷服務(Denial of Service) 以及提高特權(Elevation of privilege)，其中針對 Pre-6G 基地臺風險分析如表 13 所示。

表13、第六代行動通訊先期技術基地臺風險評估

威脅種類	威脅細節
3GPP 定義的網路介面威脅	N2 介面威脅
	N3 介面威脅
	Xn-C 介面威脅
	F1-C 介面威脅
	NR-Uu 介面威脅
O-RAN 定義的網路介面威脅	O1 介面威脅
	O2 介面威脅
	A1 介面威脅
	E2 介面威脅
	開放前傳介面(O-FH)管理平面 M-Plane)威脅
	開放前傳介面(O-FH)控制平面 C-Plane)威脅
	開放前傳介面(O-FH)同步平面 S-Plane)威脅
識別碼欺騙 (Spoofing identity)	預設帳戶(Default Accounts)
	弱密碼政策(Weak Password Policies)
	窺視密碼(Password peek)
	直接根存取(Direct Root Access)
	網際通訊協定欺騙(IP Spoofing)
	惡意程式(Malware)
	竊聽(Eavesdropping)
竄改(Tampering)	軟體竄改(Software Tampering)
	所有權檔案誤用(Ownership File Misuse)
	開機竄改(Boot tampering)
	日誌竄改(Log Tampering)
	營運管理與維護流量竄改(OAM traffic Tampering)
	檔案寫入權限濫用(File Write Permissions Abuse)
	用戶通信期竄改(User Session Tampering)
否認性 (Repudiation)	缺乏用戶活動記錄(Lack of User Activity Trace)

威脅種類	威脅細節
資訊揭露 (Information disclosure)	不良金鑰產生(Poor key generation)
	不良金鑰管理(Poor key management)
	弱密碼演算法(Weak cryptographic algorithms)
	不安全資料儲存(Insecure Data Storage)
	系統指紋(System Fingerprinting)
	惡意程式(Malware)
	個人識別資訊違規(Personal Identification Information Violation)
	不安全預設組態(Insecure Default Configuration)
	檔案/目錄讀出權限濫用(File/Directory Read Permissions Misuse)
	資訊揭露-不安全網路服務(Insecure Network Services)
	非必要服務(Unnecessary Services)
	日誌揭露(Log Disclosure)
	非必要應用(Unnecessary Applications)
	竊聽(Eavesdropping)
	缺乏通用網路產品流量隔離導致安全威脅(Security threat caused by lack of GNP traffic isolation)
阻斷服務(DoS)	被破解/行為異常用戶設備(Compromised/Misbehaving User Equipment)
	實作缺陷(Implementation Flaw)
	阻斷服務-不安全網路服務(Insecure Network Services)
	人為錯誤(Human Error)
提高特權 (Elevation of privilege)	授權使用者誤用(Misuse by authorized users)
	超過特權的程序/服務(Over-Privileged Processes/Services)
	資料夾寫入權限濫用(Folder Write Permission Abuse)
	根所屬檔案寫入權限濫用(Root-Owned

威脅種類	威脅細節
	File Write Permission Abuse)
	高特權檔案(High-Privileged Files)
	提高特權-不安全網路服務(Insecure Network Services)
	透過非必要網路服務提高特權(Elevation of Privilege via Unnecessary Network Services)

資料來源：3GPP TR 33.926

(三) 開放式無線接取網路安全確保機制

Pre-6G 網路將會帶動整個上下游供應鏈的發展，會以大量不同的設備供應商加入 Pre-6G 產業中，因此對於供應鏈、產品設備風險的議題當中，GSMA 與 3GPP 合作共同提出針對網路元件之網路設備安全保證方案 NESAS，適用於電信設備生命週期的安全保障，定義功能網路產品的供應商構建安全認證框架。設備製造商可依循 3GPP 所制定之 SCAS，設計其產品符合基本安全要求，以提升行動產業的安全層級。

針對基地臺資安風險議題，未來在生產製造的過程中將會依據 SCAS 進行合規檢測，並由資安實驗室針對設備的弱點進行規範檢測及防駭漏洞檢測等兩階段測試。

O-RAN Alliance 為了加速 O-RAN O-CU 與 O-RAN O-DU 及 O-RAN O-RU 間的整合與測試，在 2019 年 6 月成立測試與整合焦點小組(Test and Integration Focus Group, TIFG)，訂定各介面

之測試項目規格書、制定 O-RAN 測試實驗室的標準與指南，並推廣 O-RAN 測試規範，以利各項設備的垂直整合，並於 2019 年 9 月成立開放測試與整合中心(Open Testing and Integration Centre, OTIC)。

關於 Open RAN 架構的資安問題部分，O-RAN Alliance 於 2021 年成立安全焦點小組(Security Focus Group, SFG)，並於 2022 年正式成為第十一工作小組之安全工作小組，專注於制定 Open RAN 網路產品的安全架構和安全保證規範，開放式無線接取網路安全架構與框架，同時也致力於開放測試與整合中心 OTIC 推動產品資安保證評估驗證程序。並將 SCAS 測試系統的技術延伸並融合在 Open RAN 架構中，確保 Open RAN 架構不論在控制平面或用戶平面可以擁有網路設備安全保證方案(NESAS)同等級之安全防護能力。

(四) 開放式無線接取網路假基地台的資安威脅

假基地台 FBS 是一種由軟體無線電與電腦等組成非法無線電通訊裝置，該裝置利用 GSM 系統單向認證的缺陷，讓用戶手機訊號被強制連接到該裝置上，讓用戶手機無法連接到合法的電信網路，進一步影響到手機用戶的正常使用與安全性。

假基地台啟動後，就會干擾和封鎖一定範圍內的電信業者訊號，監測全球行動通訊系統行動通訊過程中的各種訊號，並獲取該裝置覆蓋範圍內的手機號碼，以及手機用戶目前的位置資訊。功率大的假基地台輻射的範圍很廣，這些基地台可攔截並發送資料到市面中各式各樣不同系統的手機，除了可竊聽外，更可以進一步操控、綁架手機，並在背景執行各種功能。其實目前的手機系統中都存在著許多隱藏的次系統，由於架構的關係，有心人很容易透過中繼的手機基地台來攔截訊號，達成入侵系統、監聽或是竊取資料的目的。

全球行動通訊系統協會 GSMA 已經將惡意中繼站對行動通訊系統的中間人威脅 GSMA Doc CVD-2019-0024 列於協調性弱點揭露機制(Coordinated Vulnerability Disclosure, CVD)資料庫中，並行文 3GPP，請求在標準層面進行改善。

3GPP 的第三工作群組-安全性的國際標準會議中，針對 5G 基地台的安全威脅也正式通過由蘋果公司主導的對抗第五代行動通訊技術假基地台之安全增強型研究項目(Study on 5G Security Enhancement against False Base Stations)。

該工作提案除了包含蘋果 Apple、聯想 Lenovo、摩托羅拉行動 Motorola Mobility、維沃移動通信 vivo、廣東歐珀移動通信 OPPO、三星 Samsung、華為 Huawei、中興 ZTE 等手機製造機商的支持以外，還獲得包含沃達豐 Vodafone、T-mobile、AT&T、中國移動、英國電信 British Telecom、德國電信 Deutsche Telekom、Orange 等眾多電信營運的支持，並催生了 3GPP 研究報告文件 33.809 技術報告草案。

隨著無線通訊技術的快速成長，無線通訊的各種應用已充斥於人們的生活中，且人們對於無線通訊的需求亦日益增加。隨著無線通訊裝置的普及，開始有惡意人士透過偽基地台監測無線通訊系統中的各種訊號傳輸，以對無線通訊系統中的使用者裝置、基地台或核心網路進行攻擊，或自使用者裝置竊取私密資料而進行盜用或詐騙。有鑑於此，急需一種威脅偵測機制來偵測假基地台的存在，藉此保護行動通訊系統合法 Pre-6G 終端用戶的隱私安全性。

基於假基地台 FBS 的議題，本計畫實作誘騙終端用戶的實驗，偽冒第六代行動通訊先期技術的實驗架構如下所示。其中本計畫團隊實作的 Pre-6GC 資安模擬器，包含用戶平面功能 UPF、存取

與行動管理功能 AMF、認證伺服器功能 AUSF、連結管理功能 SMF、統一資料管理功能 UDM 與網路資料庫功能 NRF，而基地台(gNodeB, gNB)則採用 Amarisoft 的軟體基地台。用戶設備 UE 則分別採用 Amarisoft 的軟體用戶設備 UE 與三星手機。

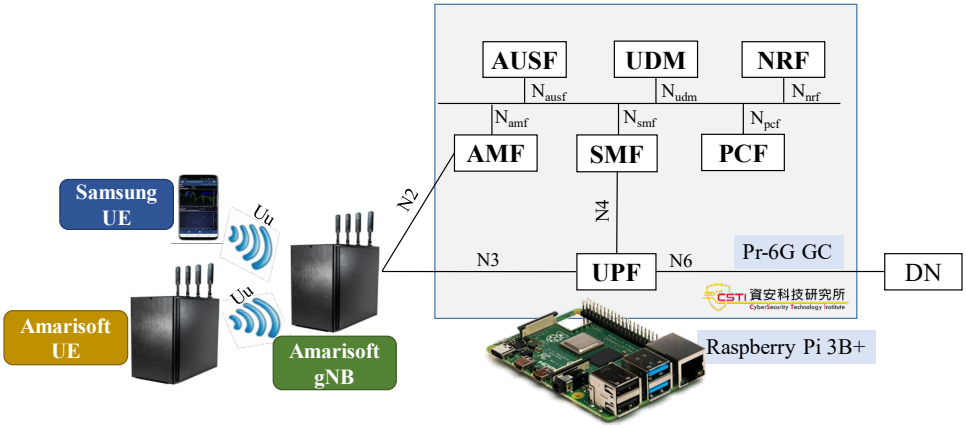
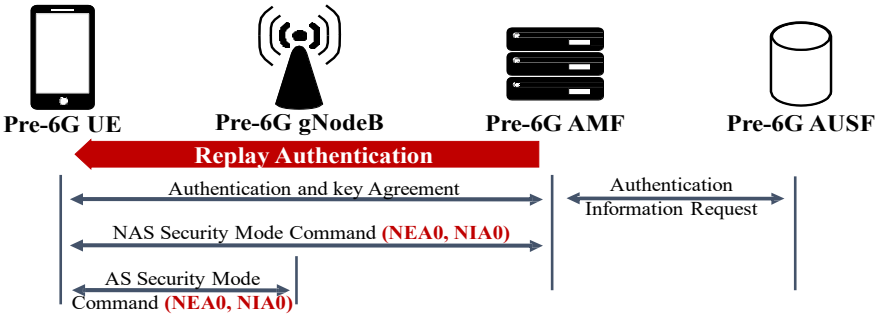


圖62、偽冒第六代行動通訊先期技術的實驗架構
資料來源：本計畫整理

由於 Pre-6G 入網認證用的認證向量(Authentication Vector)並未加密，故可以透過網路分析器(Sniffer)獲得認證向量(Authentication Vector, AV)。並透過偽冒 Pre-6GC 搭配 gNB 發送 Replay AV，誘騙 Amarisoft 的軟體用戶設備聯網通過認證程序，如圖 63 所示。接著搭配在 Security Mode Command 中發送 Null Security 的方式規避加密與完整性檢查，達成後續的入網程序，如下所示。三星手機將用戶設備(UE)安全設定設為不支援 5G-IA0，以防止 Security Mode Command 中發送 Null Security 的方式避免遭受誘騙。



Encoding	Integrity	Ciphering	Algorithm
X000X000	NIA0	NEA0	NULL

圖63、偽冒第六代行動通訊先期技術的安全威脅

資料來源：本計畫整理

圖64、偽冒第六代行動通訊先期技術重播認證向量的實測驗證

資料來源：本計畫整理

圖65、偽冒第六代行動通訊先期技術重播認證向量的實測驗證

資料來源：本計畫整理

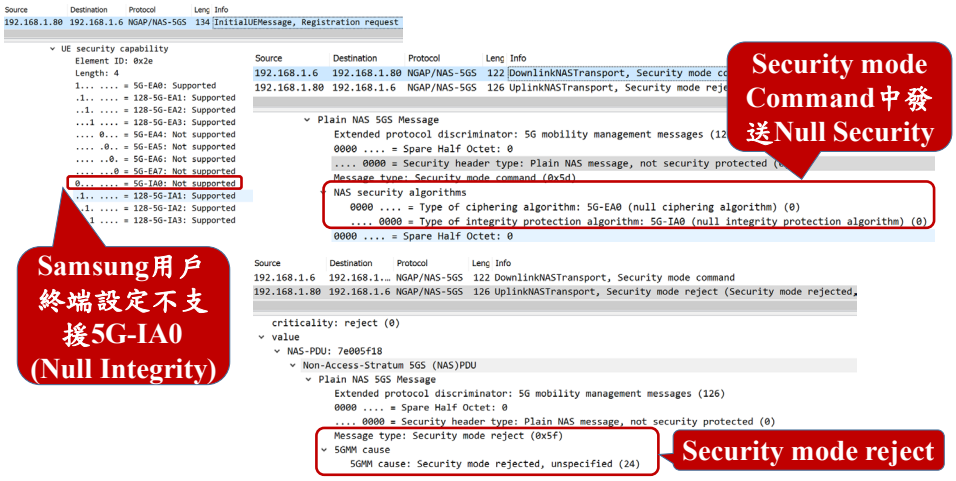


圖66、偽冒第六代行動通訊先期技術重播認證向量的解決方案
資料來源：本計畫整理

(五) 採用人工智慧的資安威脅

網路數據分析功能 NWDAF 與非即時無線接取網路智能控制 (Non-Real Time Radio Access Network Intelligent Controller, Non-RT RIC)為 Pre-6G 系統中具備人工智慧和機器學習的網路元件，具備最佳化網路性能與用戶體驗，在網域內實現網路巢狀層次的自動化服務。網路數據分析功能透過營運管理與維護 (Operations Administration and Maintenance, OAM)收集 Pre-6GC 的網路功能資訊，並透過 Pre-6G 應用功能全面收集與連接 Pre-6GC 之外部網路元件資訊。Pre-6GC 的政策控制功能(Policy Control Function, PCF)可以根據網路數據分析功能的分析結果執行網路切片等級的決策；而網路切片選擇功能(Network Slice Selection Function, NSSF)可根據網路負載分析結果選擇適合的網路切片。

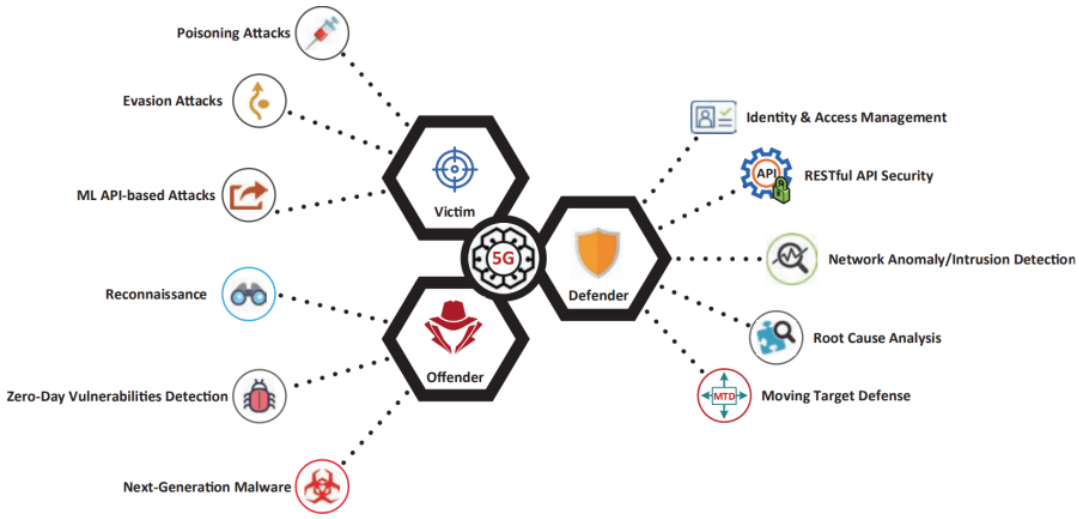
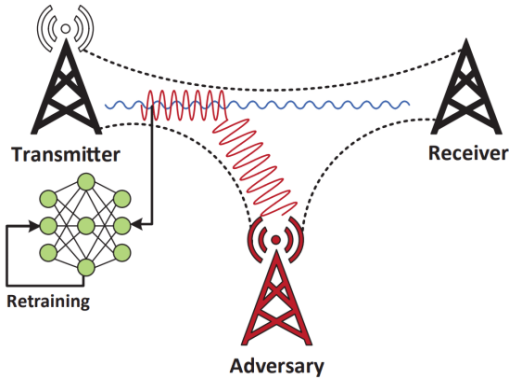


圖67、導入人工智慧之 Pre-6G 系統的安全威脅
資料來源：AI for Beyond 5G Networks： A Cyber-Security Defense or Offense Enabler?

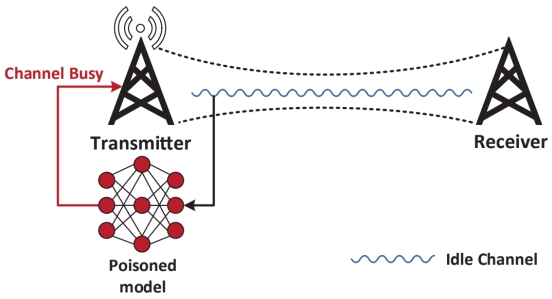
以人工智慧為基礎的無線訊號智能化(Intelligence Radio)透過邊緣智能負責多源數據收集，並運用機器學習演算法解決無線通訊領域中的精準頻道建模、敏捷式物理層設計、動態頻譜擷取、前瞻網路部署、最佳化和自主協作管理等問題，其結果高度依賴數據的正確性，同時在安全無線通信過程中預測惡意節點的可疑活動。Pre-6G 專用網路依靠各種決策引擎實現網路巢狀層次的自動化。

Pre-6G 智能網路管理需考量端到端自動化的網路服務管理與安全防護，如阻斷服務、攻擊欺騙、中間人攻擊等。使用基於運用意圖自動化調適的網管介面(Intent-Based Interfaces)可能容易受到訊息洩露、不良配置和異常行為攻擊。這種分層自動化在

很大程度上依賴於調整模型，從而提高大規模部署的效率和成本節省。然而，Pre-6G 電信產業也意識到 O-RAN 安全性是整個行動網路基礎架構中重要的元素。透過注入錯誤量測資料就能會損害機器學習的決策模型，改變決策的依據以實現毒化(Poisoning)人工智慧分層自動化的決策引擎。



(a) 收集資料學習階段



(b) 收發訊息決策階段

圖68、毒化人工智慧和機器學習示意圖

資料來源：AI for Beyond 5G Networks： A Cyber-Security Defense or Offense Enabler?

當惡意用戶終端(Malicious UE)對 Pre-6G 的無線訊號智能化與邊緣智能回報錯誤的訊號量測資訊，亦或透過指向天線針對不通方向的無線網路系統發送不同的訊號，將導致 Pre-6G 的服務管理與編排透過機器學習訓練識別的預測模型無法反映用戶終端的真實狀態，進而毒化人工智慧和機器學習的演算法，導致決策引擎發出錯誤決定。

Pre-6G 智能網路管理透過人工智慧和機器學習技術，在安全無線通信過程中預測已知與未知的惡意節點的可疑活動。但是當惡意用戶終端進一步偽冒合法用戶終端的用戶識別碼(如 SUPI)對 O-RAN 系統發動攻擊，智能化的資安防護模型雖然阻擋下攻擊，卻可能進一步阻擋合法用戶終端的正常入網流程，導致對 Pre-6G 的阻斷服務攻擊。

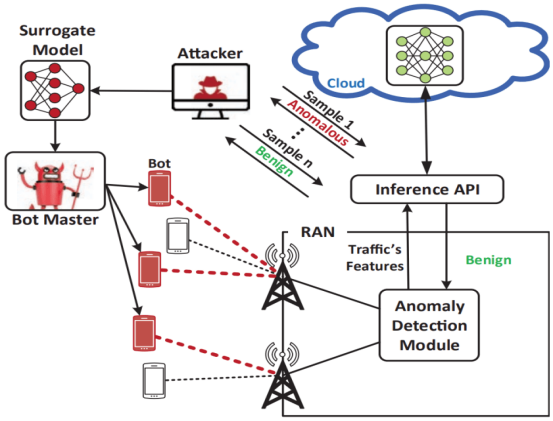


圖69、惡意用戶終端毒化智能網路管理示意圖
資料來源：AI for Beyond 5G Networks： A Cyber-Security Defense or Offense Enabler?

(六) 量子安全(Quantum Safety)先期研析

隨著量子電腦運算(Quantum Computing)技術出現，透過彼得·威利斯頓·秀爾(Peter Williston Sho)提出之秀爾演算法(Shor's algorithm)與洛夫·格羅弗(Lov Grover)提出之格羅弗演算法(Grover's algorithm)，將有機會實現對現有的對稱密鑰加密(Symmetric Key Encryption)與非對稱式加密(Asymmetric Encryption)系統進行量子破密。

依據美國國家標準和技術研究院(National Institute of Standards and Technology, NIST)發布的後量子時代密碼學研究報告(Report on Post-Quantum Cryptography)，量子電腦運算技術對於現有的對稱密鑰加密(Symmetric Key Encryption)與非對稱式加密(Asymmetric Encryption)系統的影響詳如表 14。

表14、量子運算對現有密碼學演算法的衝擊

密碼學演算法	類型	用途	量子運算的衝擊
進階加密標準(AES)	對稱密鑰加密	加密	需要較長的金鑰
SHA-2、SHA-3	N/A	雜湊函數	需要較長的輸出
RSA 加密演算法	非對稱式加密	簽章、建立金鑰	不安全
橢圓曲線密碼學(ECC)	非對稱式加密	簽章、金鑰交換	不安全
數位簽章演算法(Digital Signature Algorithm, DSA)	非對稱式加密	簽章、金鑰交換	不安全

資料來源：本計畫整理

依據 2020 臺灣資安大會，匯智安全科技股份有限公司暨臺大數學系陳君明兼任助理教授，提出之「量子計算對資安的威脅與應對之道」的建議進行先期研析如下。

傳統電子計算與網際網路領域廣泛使用的公鑰加密算法均基於三個計算難題：整數分解問題、離散對數問題或橢圓曲線離散對數問題，如迪菲-赫爾曼密鑰交換(Diffie-Hellman Key Exchange, DHKE)、迪菲－赫爾曼橢圓曲線 (Elliptic Curve Diffie–Hellman, ECDH)、R-S-A 三氏不對稱加密演算技術標準(Rivest-Shamir-Adleman, RSA)、橢圓曲線數位簽章算法(Elliptic Curve Digital Signature Algorithm, ECDSA)。然而，這些難題均可使用量子計算機並應用秀爾算法破解。

後量子密碼學 PQC 亦稱為抗量子計算密碼學，是密碼學的一個研究領域，專門研究能夠抵抗量子電腦的加密算法，特別是非對稱加密之公鑰加密演算法。不同於量子密碼學，後量子密碼學不依靠量子電腦，而是使用傳統電子計算機搭配無法被量子計算機有效解決的計算難題來抵抗量子破密。於 2006 年開辦第一屆後量子密碼學大會(Post-Quantum Cryptography, PQCrypto)後，美國 NIST、歐洲 ETSI、微軟、Google、滑鐵盧大學的量子計算

研究所等機構都在開展研究後量子密碼學。

在公開金鑰密碼學(Public-Key Cryptography)方面，後量子密碼學的研究方向包括了格密碼學、容錯學習問題(Learning with Errors, LWE)、多變量密碼學(Multivariate Public Key Cryptography, MPKC)、密碼雜湊函式(Cryptographic Hash Function, CHF)、編碼密碼學(Code-based Cryptography)與超奇異橢圓曲線同源密碼學(Super-singular Isogeny Cryptography)。基於這些計算難題，密碼學家認為可以構建出不受量子計算機的威脅的公開金鑰基礎建設(Public Key Infrastructure, PKI)。

美國國家標準技術研究所在 2017 年收到了各學者提交的共 69 個後量子密碼學演算法。美國國家標準技術研究所經過四次的演算法提案，在 2022 年選出 CRYSTALS-KYBER 作為公開金鑰加密(Public-Key Encryption)的後量子密碼學演算法，並選出 CRYSTALS-DILITHIUM、FALCON、SPHINCS+作為數位簽章演算法(Digital Signature Algorithm, DSA) 的後量子密碼學演算法。

(七) 研析成果

1. 彙整 Pre-6G 系統架構的安全議題

本研究報告探討 Pre-6G 系統架構的安全議題，參考國際開放式無線接取網路的安全政策以及 O-RAN Alliance 及 3GPP 之標準規範與技術研究報告。

針對 6G 系統架構的安全議題，FCC 根據 2021 年 12 月批准通過的「未來網路法(Future Uses of Technology Upholding Reliable and Enhanced Networks Act, FUTURE Networks Act)」與「理解行動通信網路資安法(Understanding Cybersecurity of Mobile Networks Act)」及「美國資安識辨能力法(American Cybersecurity Literacy Act)」，將針對業界主導的標準制定機構所提出的 6G 使用案例以及使用技術，分析其系統架構的缺點包含任何供應鏈或任何資安議題。

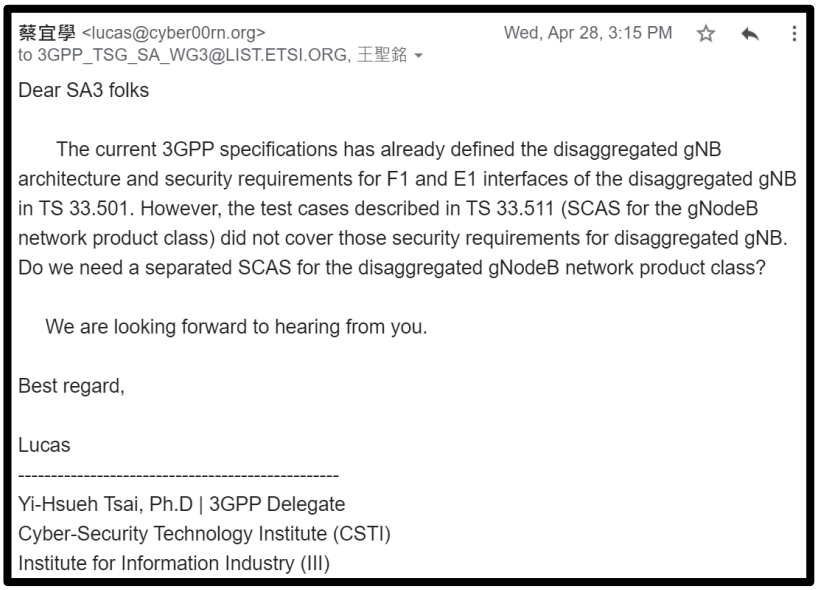
美國與歐盟成立貿易與科技理事會(EU-US Trade and Technology Council, EU-US TTC)的第四工作組-資通技術安全與競爭力(Working Group 4: ICTS security & competitiveness)亦將 6G 資安納入其主要的議題之一。不論是美國與歐盟都以 GSMA 制定的網路設備安全保證方案 NESAS 作為驗證 Pre-6G 系統架構安全的基礎。

2. 協助國內廠商與檢測實驗室建立 O-RAN 的資安檢測能量

隨著 O-RAN Alliance 的網通設備「白牌化」後，Pre-6G 電信事業也擔心開放架構會不會造成更多的資安漏洞。依據歐盟與北約組織「布拉格倡議(Prague Proposals)」，可信任的 Pre-6G 網路軟硬體設備供應鏈管理將是 Pre-6G 資安管理最重要的關鍵議題。因此，Pre-6G 電信事業不僅需要可信任的網路軟硬體設備供應鏈業者，更必須有能力驗證 Pre-6G 相關網路軟硬體設備的安全性才行。

臺灣已有工業電腦與伺服器廠商以及小型基地臺製造商積極投入O-RAN架構以及邊緣運算EC平台的網通設備市場，建議 O-RAN 基地臺以及邊緣運算 EC 的製造商及軟硬體開發商可依據 O-RAN Alliance 的方案，先依據 GSMA 制定的網路設備安全保證方案 NESAS，搭配 3GPP 制定的產品資安確保標準 SCAS 來驗證產品的安全性，以降低產品於商用時的資安修補成本。除了可以滿足潛在客戶的資安需求外，同時亦可提升產品的國際市場競爭力。

本計畫團隊透過電子郵件討論向 3GPP 的第三工作群組-安全性(SA3 Working Group - Security, SA3 WG)建議增訂 3GPP 分散式基地臺產品資安確保標準 SCAS，初期遭到華為極力反對新增相關測試案例。於第 3 工作組第 103 次線上會議時，由國際通訊晶片大廠高通提出測試案例，期間國際大型電信事業商 NTT DoCoMo 也支持相關測試案例。最後於制定 R18 標準時，才將相關測試案例納入 3GPP 的技術標準文件 33.742 中，團隊也會依據本研究報告的研究結果，向國際標準組織提出修訂產品資安確保標準 SCAS。臺灣資通產業標準協會 TAICS 預計於 2023 年完成第二次 5G Open RAN 資安測試規範產業專家會議後，訂定 TAICS TS-0053 v0.3-5G Open RAN 資安測試規範的測試項目，並於 TAICS 官網上公告。


蔡宜學 <lucas@cyber00rn.org> Wed, Apr 28, 3:15 PM
to 3GPP_TSG_SA_WG3@LIST.ETSI.ORG, 王聖銘

Dear SA3 folks

The current 3GPP specifications has already defined the disaggregated gNB architecture and security requirements for F1 and E1 interfaces of the disaggregated gNB in TS 33.501. However, the test cases described in TS 33.511 (SCAS for the gNodeB network product class) did not cover those security requirements for disaggregated gNB. Do we need a separated SCAS for the disaggregated gNodeB network product class?

We are looking forward to hearing from you.

Best regard,

Lucas

Yi-Hsueh Tsai, Ph.D | 3GPP Delegate
Cyber-Security Technology Institute (CSTI)
Institute for Information Industry (III)

圖70、第3工作組(SA3)電子郵件討論
資料來源：本計畫整理

為了驗證採用人工智慧之 Pre-6G 專網系統 O-RAN 基地臺產品與非地面網路之開放式無線接取網路的安全，在開發階段的強健性與安全性，臺灣廠商可以依據潛在客戶的需求導入產品資安確保標準、滲透測試以及機器學習資料毒害等相關資安測試，以提升產品競爭力。

為順應順應時代與資訊技術的更新，也為了因應新型態的駭客攻擊樣態，針對相關 6G 技術衍生的相關議題，對應至 ISO/ SO/IEC 27002：2022 的控制項目，目前國際標準化組織 (International Organization for Standardization, ISO) 已於 2022 年 2 月 15 日公布最新版本的 ISO/IEC 27002：2022 資訊安全、網路安全與隱私保護-資訊安全控制措施(Information

security, cybersecurity and privacy protection - Information security controls)，做為資訊安全管理系統(Information Security Management System, ISMS)的實作指引。其將 2013 年版本的 ISO 27002 重新綜整為 4 個控制主題分別為組織面、人員面、實體環境面與技術面等共計 93 項控制措施，除了資訊安全管理的範疇，亦著墨於網路安全與隱私保護的管理。對於每一個控制措施也都會再界定該控制措施的控制屬性(Control Attributes)：

(1) 控制型態(Control type)： 控制措施何時/如何介入因應資安事故之風險結果。

(2) 資訊安全特性(Information Security Properties)： 控制措施有助於保持哪些資訊特性(Characteristic)。

(3) 網路安全框架(Cybersecurity Concepts)：控制措施與 ISO/IEC TS 27101 中描述的網路安全框架中定義的網路安全概念的關聯。

(4) 運作能力(Operational Capabilities)：控制措施對應實作者的資訊安全能力。

(5) 安全領域(Security Domains)：控制措施對應所需要的資訊安全領域(fields)、專業能力(expertise)、服務或產品。

由於 Pre-6G 的系統線接沿用 5G 的系統架構 ISO/IEC 27002：2022 對應 Pre-6G 的資安控管與現有 5G 的資安控管措施類似，詳列如表 15。

表15、本計畫資安產出對應 ISO 27002控制項目或指引對照表

安全議題	威脅議題	對應 ISO 27002 控制項目/指引
隱私(Privacy)	用戶隱私資料竊聽	5.14 資訊傳送 (Information Transfer)
	竊取用戶身分	5.15 存取控制 (Access Control)
行動通訊物聯網 (CIoT)	非擷取層 NAS 資訊包含的 CIoT 新參數的隱私保護	5.15 存取控制 (Access Control)
車聯網(V2X)	透過 PC5 介面的單播資訊隱私保護	5.17 認證資訊 (Authentication information)
	透過 PC5 介面的群播資訊隱私保護	
	透過 PC5 介面的廣播資訊隱私保護	
超可靠度和低延遲通訊(URLLC)	冗餘(redundant)傳輸的安全性	5.14 資訊傳送 (Information Transfer)
	支援 UP 冗餘資料高可靠性傳輸的安全性	5.14 資訊傳送 (Information Transfer)
	處理建立 PDU 會話的冗餘資料傳輸之 UP 安全策略	5.1 資訊安全政策 (Policies for information security)
	超可靠度和低延遲通訊服務的安全策略	5.1 資訊安全政策 (Policies for information security)
	低延遲換手的安全性	5.14 資訊傳送 (Information Transfer)
	QoS 監控保護	5.14 資訊傳送 (Information Transfer)

安全議題	威脅議題	對應 ISO 27002 控制項目/指引
時間敏感通訊 (TSC)	保護 Pre-6G 系統與時間敏感網路間的交互作用介面	5.14 資訊傳送 (Information Transfer)
	時間敏感通訊的時間同步	5.14 資訊傳送 (Information Transfer)
Pre-6G LAN	Pre-6G LAN 的用戶設備認證和授權	5.17 認證資訊 (Authentication information)
	Pre-6G LAN group 的使用者平面安全政策	5.1 資訊安全政策 (Policies for information security)
基地臺風險	3GPP 定義的網路介面威脅	5.15 存取控制 (Access Control)
	O-RAN 定義的網路介面威脅	5.15 存取控制 (Access Control)
	識別碼欺騙 (Spoofing identity)	5.17 認證資訊 (Authentication information)
	竄改(Tampering)	5.15 存取控制 (Access Control)
	否認性 (Repudiation)	5.17 認證資訊 (Authentication information)
	資訊揭露 (Information disclosure)	5.18 存取權限 (Access)
	阻斷服務 (DoS)	5.18 存取權限 (Access)
	提高特權 (Elevation of privilege)	5.15 存取控制 (Access Control)

資料來源：本計畫整理

本計畫規劃每年度隨投入規劃，就資安驗測項目進行滾動式檢視與修訂，待 3GPP 的第二十一版本標準文件正式定案後，才能針對 6G 系統建立 ISO/IEC 27002：2022 的資安控管措施。

五. 計畫執行情形-6G 網元及通訊資安檢測研析

為因應未來 6G 世界的來臨，無遠弗屆的萬物連網以及萬物皆服務(Everything as a Service)的結果，將引來各種針對製造、物流、運輸、醫療、教育、零售及家用環境的破壞和勒索攻擊，使得駭客攻擊變得更加精密且精，因此必須要有極高的安全等級，以滿足工業和高端用戶的極高要求，提前因應 6G 產業發展與產品應用需求進行規劃與布署也更顯迫切，對應本計畫各國國際安全標準化的相關組織進行盤點，解析與評估相關規範下可能衍生之新型態資安威脅、攻擊/防護實證技術、風險評估、可能漏洞及對應攻擊手法，進行網通資安生態系解析，6G 系統與新興應用服務之推動規劃，提供我國未來 6G 資安應用服務研發布署與產業推動之指引參考。為使計畫有效達成預期目標，擬以 B5G/Pre-6G/6G 通訊技術為核心，規劃 6G 產品資安防護機制與發展兼顧效能與安全之 6G 資安偵防系統所需之技術與環境規格/規範，並

針對無人機、低軌道衛星、智慧醫療等產品進行規劃，透過 6G 新興技術所衍生之新型攻擊手法研提，由外而內建置完善 6G 資安偵防系統發展建議。

(一) 6G 潛在技術、可能存在威脅與對應防護方案分析

6G 網路會使用的技術有毫米波、太赫茲、可見光等通訊技術、分散式帳本技術、AI/ML、虛擬化無線電接入網路、6G 開發式架構、Open API 3.0，以下將針對 6G 潛在新技術作介紹。

1. 6G 毫米波(mmWave)通信的安全性

(1) 介紹

無線通訊技術提升頻段至 24GHz 以上，傳輸速率快、低延遲、頻寬更大，被稱為是進階的 5G 技術，為待突破開發，降低限制條件的下一階段目標技術。目前已知美國同步進行 Sub-6 和 mmWave 毫米波的開發。

(2) 威脅

A. 竊聽(Eavesdrop)：竊聽者可以在天線波束範圍內、或在波束範圍內使用反射器讓竊聽者在波束範圍外，監聽傳輸信號訊息。

B. 干擾攻擊(Active jamming)：使用干擾器注入無線電信號(與使用者頻率相同)，從而佔用共享的無線信道，使合法用戶無法使用無線信道進行通信，這是一種 DoS。

C. 汙染攻擊(Pilot contamination attack, PCA)：(發射器)A 發送信號給(用戶)B，竊聽者發送跟用戶 B 相同的導頻信號(欺騙的上行信號)給發射器 A，用以汙染發射器 A 的用戶檢測和信道，然後發射器 A 部分的下行信號通訊天線波束會指向竊聽者，導致用戶 B 的傳輸信號洩漏出去。

(3) 防護

A. 使用跳頻展頻(Frequency-hopping spread spectrum, FHSS)技術，在接收端與發射端之間偽隨機的在不同頻率中切換，以逃避竊聽。

B. 透過隱蔽通信(Covert Communication)技術，隱藏通信雙方的訊息傳輸，防止通信信號被惡意竊聽者發現。

C. 使用物理密鑰生成，發送端與用戶間的物理密鑰交換，來達到身分驗證傳輸。

2. 太赫茲通信的安全性

(1) 介紹

太赫茲通信可以通過增加頻寬貸來提高頻譜效率，他可以通過擴大頻寬帶和應用先進的 MINO 技術來實現，雖然 5G 引入了毫米波頻率以實現更高的數據速率並支持新的應用，然而對 6G 更大的需求就需要使用太赫茲通訊技術，以滿足更高的需求。

太赫茲是物理單位，也就是每秒 10 的 12 次方次的意思，太赫茲波段的頻率範圍是 0.1THz~10THz，介於微波與可見光之間，太赫茲易受環境造成傳播損耗跟繞射性差，所以太赫茲的通訊覆蓋範圍比較小，在幾十米以內，太赫茲可以為許多 6G 應用實現超高數據速率(高達每秒 TB)。

(2) 威脅：竊聽(Eavesdrop)，在太赫茲範圍內(1 GHz 至 10 THz)，以提高未來無線網路的頻譜效率和容量，並提供無處不在的高速互聯網接入。在這些頻率下，傳輸的信號具有很強的方向性，傳播環境惡劣，因此信號的攔截大多侷限於與合法用戶位於同一窄波束內的非法用戶，即使使用極窄的波束，非法接收器也可以攔截視距傳輸中的信號。

因此，太赫茲通信容易受到數據傳輸暴露、竊聽和訪問控制攻擊。

(3) 防護：使用 FHSS 技術，在接收端與發射端之間偽隨機的在不同頻率中切換，以逃避竊聽。

3. VLC 可見光通信的安全性

(1) 介紹

可見光通信 (Visible Light Communications , VLC) 是一種利用 400 至 800 THz 之間的可見光傳輸數據的高速通信技術。與太赫茲一樣，VLC/燈光上網技術(Light Fidelity, LiFi)比之前的無線通信技術(如 WiFi)更安全，由於與射頻系統相比具有數據速率高、可用頻譜大、抗干擾能力強、成本低等優點，因此受到了廣泛部署運用，VLC 也有很大的潛力來補充 RF 系統，以利用這兩個網路的好處。

VLC/LiFi 的覆蓋範圍很小，無法穿透牆壁等不透明物體。與太赫茲技術類似，竊聽者必須進入發射機-發射機 VLC/LiFi 鏈路的 LOS 區域才能攔截信號。

(2) 威脅：竊聽(Eavesdrop)，當節點部署在公共區域和/或覆蓋區域存在大窗戶以及存在合作的竊聽者時，與 RF 一樣容易受到攻擊。

(3) 防護：VLC 可使用光學透鏡可以通過聚焦訊息傳輸，來顯著提高保密率，降低傳輸訊息被竊聽風險。通過使用線性預編碼證明了 MIMO VLC 系統在可實現的保密率方面的保密性能的增強。

4. 分散式帳本技術 DLT

(1) 介紹

所謂 DLT，是將數據庫分拆為小塊，再以不能更改的加密鏈連接，讓使用者能以高效和高可靠度的方式創建、傳遞和儲存訊息。同時，由於 DLT 系統中的交易能在沒有中間人的情況下如常運作，大大增加了交易的透明度，並降低交易成本。

以用於加密貨幣和金融交易而聞名的區塊鏈和分散式帳本技術是在 6G 中構建信任網路的可能解決方案，從理論上講，區塊鏈和 DLT 的同行評審能力將保證關鍵的安全和隱私特性，例如不變性、透明性、可驗證性、匿名性和假名性、數據完整性、可追溯性、身分驗證和監控。使用分散式帳本技術

能提供 AI/ML 信任且不可變的資料來源，避免 AI/ML 遭受資料中毒攻擊(poisoning attack)。

(2) 威脅

A. 日食攻擊的可能性：當區塊鏈節點通信中斷或傳播時，它最終可能會接受虛假訊息，從而可能導致虛假交易的確認。

B. 51%攻擊：51%攻擊是對區塊鏈網路的潛在攻擊，單一實體或組織能夠控制大多數雜湊率，可能會導致網路中斷。

C. 重放攻擊 (Replay Attacks)：重放攻擊又稱回放攻擊，在該種網路攻擊的情況下，惡意實體將會攔截有效數據，並將其在網路中重覆傳輸。由於原始數據(通常自已授權使用者)的有效性，所以網路的安全協議通常會將此種攻擊視為正常的數據傳輸。

D. 分散式阻斷服務(Distributed Denial of Service, DDoS)：分佈式拒絕服務攻擊旨在減緩並最終阻礙網站的運行。這種攻擊式通過向它們發送大量請求來發起的，直到它們崩潰。

(3) 防護

A. 防止這種情況發生的最直接方法是讓阻止節點的非法接入，並僅建立到特定節點(如已被對等網路中的其他節點列入白名單的 IP)的出站連接。

B. 由於網路的規模，不太可能會發生 51%攻擊。一旦區塊鏈增長到足夠大，一個人或群體獲得足夠計算能力來壓倒所有其他參與者的可能性，迅速下降到非常低的水平，可以對參與者進行身分驗證，以確保使用者是可信任，不會被惡意攻擊者操控整個區塊鏈。

C. 「加隨機數」方法優點是認證雙方不需要時間同步，雙方記住使用過的隨機數，如發現報文中有以前使用過的隨機數，就認為是重放功擊。此外，「加時間戳」方法優點是不用額外保存其他訊息。缺點是認證雙方需要準確的時間同步，同步越好，受攻擊的可能性就越小。但當系統很龐大，跨越的區域越廣時，要做到精確的時間同步並不是很容易。

D. 盡可能保持服務、迅速恢復服務。由於分佈式攻擊入侵網路上的大量機器和網路設備，所以要對付這種攻擊歸根到底還是要解決網路的整體安全問題。

5. 虛擬化無線電接入網路 vRAN 的安全性

(1) 介紹

vRAN 和開放式 RAN 是提高 6G 安全性的前瞻性技術。vRAN 支持與傳統 RAN 相同的功能，但在商用服務器上進行了虛擬化(例如，虛擬化基帶單元)，而不是在供應商特定硬體上的物理部件。

vRAN 和開放式 RAN 模型在安全方面的另外兩個重要優勢是提高了模塊化，並減少了相互依賴性。

(2) 威脅

軟體供應鏈攻擊：虛擬化後服務變成系統上軟體來提供，使用 Open Source 的目的是讓開發者從社區中簡化開發複雜度跟加速開發。但是，假設源代碼沒有經過適當的設計和安全的深入檢查。在這種情況下，它可能會變得脆弱，攻擊者也可以輕鬆地尋找潛在的漏洞來利用。其次，如果重複使用易受攻

擊的源代碼(例如，作為 library 庫)來開發其他代碼，則漏洞會經常傳播。

(3) 防護

確保只使用可信任的開發工具開發軟體，且為確保系統和敏感數據的安全，定期或在重大系統變更後進行安全滲透測試，並對套裝軟體和相關組件實施程式碼簽署，以確保其真實性和完整性。所有全新及經修改的硬體、韌體、軟體和配置變更在推出作生產用途前，須於測試設施內進行徹底的檢查及測試。

6. 6G 開發式架構 / Open Source 的安全性

(1) 介紹

6G 開發式架構是指在 6G 技術的研發過程中，採用一種開放、靈活、可擴展的架構，讓各種技術能夠互相結合，以實現更高效、更可靠、更安全、更智慧的通訊。6G 開發式架構的主要特點包括：

A. 開放式架構：6G 開發式架構採用開放的技術平台，可以讓各種不同的技術和應用快速接入，實現開放、協同、操作。

B. 靈活性：6G 開發式架構具有靈活性，可以針對不同的應用場景進行靈活配置，實現定制化的網路應用。

C. 可擴展性：6G 開發式架構可以不斷擴展，根據新興的應用需求，不斷添加新的技術和功能。

D. 智慧化：6G 開發式架構具有智慧化的特點，可以實現自主學習、自動優化和自我修復等功能，提升網路的智慧化水平。

(2) 威脅

供應鏈攻擊(supply chain attack): 在硬體供應鏈攻擊，透過使用不信任的上游設備商生產的零件或委託不信任的廠商代工，造成硬體跟韌體被植入惡意程式。軟體供應鏈攻擊，系統軟體開發使用開源軟體套件，而套件有已知漏洞造成系統跟著有資安風險。

(3) 防護

採用信任的供應商提供的設備跟零件，掃描系統使用的開源軟體套件原始碼，定期使用弱點掃描工具，軟體套件有重大更新立即更新。

7. Open API 3.0 的安全性

(1) 介紹

Open API，通常稱為公共 API，是一種公開可用的應用程式介面，它是 Server Side Web API 的應用方式，提供開發者可以透過程式去存取應用軟體或網路服務。

(2) 威脅

A. 參數攻擊：未正確驗證的參數可能導致對跨域數據服務的注射攻擊。

B. 身分攻擊：利用身分驗證和授權中的缺陷，提取 API 密鑰並將其用作憑證。

C. 中間人攻擊：從 API 消費者和提供商之間的 API 消息的未加密訊息中獲取訊息。

D. DoS 攻擊/ DDoS 攻擊：通過大量請求壟斷服務。

(3) 防護

A. 輸入驗證和用戶身分驗證。

B. 授權基於角色的訪問控制，基於屬性的訪問控制，訪問控制列表。

C. 使用安全的加密通信使用。

D. 基於 AI 的 API 安全性用於主動監視。

8. 分佈式和可擴展的 AI/ML 的安全性

(1) 介紹

人工智慧是 6G 自治網路的基本特徵，因此 6G 最關鍵則是引入 AI 技術，但是人工智慧將完全支持 6G 以實現自動化，機器學習的進步為 6G 中的實時通信創造了更加智能的網路，在通信中引入人工智慧將簡化和改善實時數據的傳輸。

使用大量分析，人工智慧可以確定執行複雜目標工作的方式，提高了效率並減少了通訊步驟的處理延遲。AI 可用於快速切換服務、網路選擇等耗時任務，人工智慧還將在機器對機器、機器對人和人對機器通訊中發揮重要作用。它還會應用於腦機介面 BCI 中的通信。因此，人工智慧技術將有助於實現 6G 通訊中 uMUB、uHSLLC、mMTC 和 uHDD 服務的目標。最近的進展使得將機器學習應用於射頻訊號處理、頻譜挖掘和頻譜映射。

機器學習是人工智慧的一個分支，機器學習通常可以這樣定義：「透過從過往的資料和經驗中學習並找到其運行規則，最後達到人工智慧的方法。」可分以下幾種：

A. 監督式學習(Supervised learning)是電腦從標籤化(labeled) 的資訊中分析模式後做出預測的學習方式。標記過的資料就好比標準答案，電腦在學習的過程透過對比誤差，一邊修正去達到更精準的預測，這樣的方式讓監督式學習有準確率高的優點。監督式學習方式需要倚靠大量的事前人工作業，將所有可能的特質標記起來，這過程相當繁複。當範圍擴大、資訊量增加，會更難去對資料標記出所有特徵，所以在面對未知領域時，幾乎是完全無法運作。

B. 非監督式學習(Unsupervised Learning) 的訓練資料不需要事先以人力處理標籤，機器面對資料時，做的處理是依照關聯性去歸類 (Co-occurance Grouping)、找出潛在規則與套路 (Association Rule Discovery)、形成集群 (Clustering)，不對資訊有正確或不正確的判別。非監督式學習的特性讓它在資料探勘初期是好用的工具。對比監督式學習，非監督式學習可以大大減低繁瑣的人力工作，找出潛在的規則。但這樣的方式，也會造

成較多功耗，甚至，也可能造成不具重要性的特徵被過度放大，導致結果偏誤、無意義的分群結果。

C. 強化式學習(Reinforcement Learning)的特徵是不需給機器任何的資料，讓機器直接從互動中去學習，這是最接近大自然與人類原本的學習方式。機器透過環境的正向/負向回饋(positive / negative reward)，從中自我學習，並逐步形成對回饋刺激的預期，做出越來越有效率達成目標的行動，這個訓練過程的目標是獲取最大利益。

(2) 威脅

A. 中毒攻擊/模型中毒：竄改機器學習的訓練資料，從而損害模型的完整性，會影響模型輸出正確預測的能力，一旦模型中毒，從中毒中恢復模型式非常困難。

B. 逃避攻擊(Evasion Attacks) ：是指攻擊者在不改變目標機器學習系統的情況下，通過構造特定輸入樣本，以完成欺騙目標系統的攻擊。一般發生在模型已經完成訓練、在預測時。

C. 基礎設施物理攻擊和通信篡改：通信和計算基礎設施的故意中斷和損害，會導致決策/數據處理受損，甚至可能使整個人工智慧系統離線。

D. 人工智慧框架的漏洞：大多數 AI 解決方案都利用現有的 AI/ML 框架。這些人工製品或傳統攻擊向量中的漏洞，針對其軟體、韌體和硬體環境(尤其是以雲為中心的操作)的目標是 AI/ML 功能完整性。

(3) 防護

A. 未來可使用分散式帳本 DLT 技術，透過 DLT 的不變性、透明性、可驗證性、匿名性和假名性、數據完整性、可追溯性、身分驗證和監控，由 DLT 技術提供的資料來源就是可信任來源，避免掉攻擊者竄改資料攻擊 AI/ML。

B. 執行對抗訓練，訓練集除了真實資料集外，還有加了干擾的資料集，讓模型能判別干擾資料。而透過隨機化，向原始模型引入隨機變數，使模型具有一定的隨機性，全面提高模型的路棒性，使其對抗干擾容忍度變大。

C. 使用信任的上游供應商零組件，並在使用前執行沙箱測試。

D. 所有全新及經修改的軟體和配置變更，在推出作生產用途前須於測試設施內進行徹底的檢查及測試。

綜整上述 6G 主要關鍵技術風險，匯集其相對應降低威脅方法如表 16 所示。

表16、6G 主要關鍵技術風險

關鍵技術	安全威脅	降低威脅方法
6G 毫米波 (mmWave)	竊聽	使用 FHSS 技術，在接收端與發射端之間偽隨機的在不同頻率中切換，以逃避竊聽。
	干擾攻擊	透過隱蔽通信 (Covert Communication)技術，隱藏通信雙方的訊息傳輸，防止通信信號被惡意竊聽者發現。
	污染攻擊 PCA	使用物理密鑰生成，發送端與用戶間的物理密鑰交換，來達到身分驗證傳輸。
太赫茲 (THz)	竊聽	使用 FHSS 技術，在接收端與發射端之間偽隨機的在不同頻率中切換，以逃避竊聽。
可見光 (VLC)	竊聽	VLC 可使用光學透鏡可以通過聚焦訊息傳輸來顯著提高保密率，降低傳輸訊息被竊聽風險。通過使用線性預編碼證明了 MIMO VLC 系統在可實現的保密率方面的保密性能的增強。
分散式帳本技術(DLT)	日蝕攻擊的可能性	防止這種情況發生的最直接方法是讓阻止節點的非法接入，並僅建立到特定節點(例如已被對等網路中的其他節點列入白名單的 IP)的出站連接。
	礦工中心化 (51% 攻擊)	要避免使用算力較小的區塊鏈，因為一個礦工必須要有超過全網一半的算力才能完成攻擊，考慮到比特幣區塊鏈上有數百萬的礦工，即使是地球上

關鍵技術	安全威脅	降低威脅方法
		最強大的計算機也不能與該網路上的總計算能力直接競爭。
	重放攻擊(Replay Attacks)	加隨機數，該方法優點是認證雙方不需要時間同步，雙方記住使用過的隨機數，如發現報文中有以前使用過的隨機數，就認為是重放功擊。 加時間戳，該方法優點是不用額外保存其他訊息。缺點是認證雙方需要準確的時間同步，同步越好，受攻擊的可能性就越小。但當系統很龐大，跨越的區域越廣時，要做到精確的時間同步並不是很容易。
	分散式阻斷服務(DDoS)	盡可能保持服務、迅速恢復服務。由於分佈式攻擊入侵網路上的大量機器和網路設備，所以要對付這種攻擊還是要解決網路的整體安全問題。
虛擬化無線電接入網路(vRAN)	軟體供應鏈攻擊	確保只使用可信任的開發工具開發軟體，且為確保系統和敏感數據的安全，定期或在重大系統變更後進行安全滲透測試，並對套裝軟體和相關組件實施程式碼簽署，以確保其真實性和完整性。 所有全新及經修改的硬體、韌體、軟體和配置變更在推出作生產用途前，須於測試設施內進行徹底的檢查及測試。
6G 開發式架構 / Open Source	供應鏈攻擊	採用信任的供應商提供的設備跟零件，掃描系統使用的開源軟體套件原始碼，定期使用弱點掃描工具，軟體套件有重大更新立即更新。
Open API 3.0	參數攻擊	輸入驗證和用戶身分驗證，防止未正確驗證的參數可能導致對跨域數據服務的注射攻擊。
	身分攻擊	授權基於角色的訪問控制，基於屬性的訪問控制，訪問控制列表。

關鍵技術	安全威脅	降低威脅方法
	中間人攻擊	使用安全的加密通信使用。
	拒絕服務(DoS)/分散式阻斷服務(DDoS)	使用 DDoS 黑洞(black hole)路由/過濾技術建立特定的 IP 路由表堵截網路攻擊，並將 DDoS 攻擊流量導向至「黑洞」棄置。
人工智慧/機器學習(AI/ML)	中毒攻擊	未來可使用分散式帳本技術 DLT 技術，透過 DLT 的不變性、透明性、可驗證性、匿名性和假名性、數據完整性、可追溯性、身分驗證和監控。由 DLT 技術提供的資料來源就是可信任來源，避免掉攻擊者竄改資料攻擊 AI/ML。
	逃避攻擊	執行對抗訓練，訓練集除了真實資料集外，還有加了干擾的資料集，讓模型能判別干擾資料。 隨機化，向原始模型引入隨機變數。使模型具有一定的隨機性，全面提高模型的路棒性，使其對抗干擾容忍度變大。
	基礎設施物理攻擊和通信篡改	使用信任的上游供應商零組件，並在使用前執行沙箱測試。
	人工智慧框架的漏洞	所有全新及經修改的軟體和配置變更在推出作生產用途前，須於測試設施內進行徹底的檢查及測試。

資料來源：本計畫整理

(二)6G 網路架構潛在的威脅風險

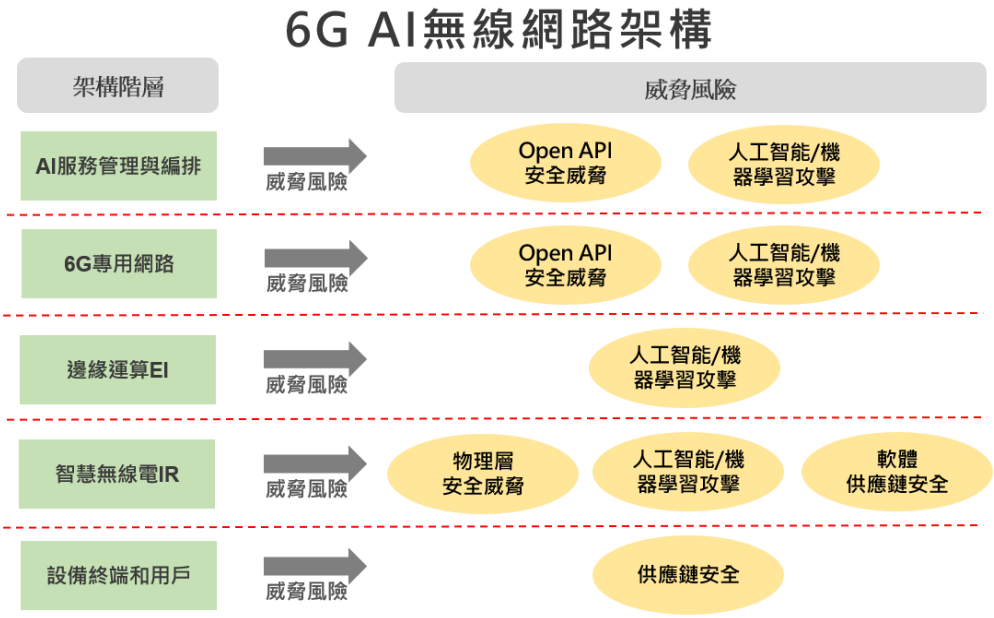


圖71、6G 網路潛在架構對應風險圖
資料來源：本計畫整理

由於人工智慧與機器學習的發展，在 5G 到 6G 的過程中，AI 於無線網路上的應用跟佔比會越來越高，未來 6G 網路將會結合 AI 的智慧無線網路，從現有的網路架構去推估 6G 的 AI 網路架構，並從物理層安全、網路訊息安全、應用安全和深度學習安全等面向討論 6G 安全，再從 6G 網路架構對應上面探討的 6G 關鍵技術，彙整如表 17 所示：

表17、網路架構主要關鍵技術風險

關鍵技術	說明	威脅風險	威脅種類
AI 服務管理與編排	在人工智慧的支持下，新的 6G 架構有望提供智慧端到端的網路和服務管理自動化。智能網路管理部署中的關鍵安全挑戰，開放 API 的安全威脅	Open API 安全威脅	• Open API 3.0 的安全性
		人工智慧/機器學習攻擊	• 分散式帳本技術 DLT • 分佈式和可擴展的 AI/ML 的安全性
6G 專用網路	專用 6G 網路有望作為獨立的小型化網路運行，用於多個垂直應用。當這些子網所有者或基礎設施使用應用程序服務的無線接口，這些外部通訊接口可能會帶來安全漏洞	Open API 安全威脅	• Open API 3.0 的安全性
		人工智慧/機器學習攻擊	• 分散式帳本技術 DLT • 分佈式和可擴展的 AI/ML 的安全性
邊緣運算 EI	無論是使用人工智慧/機器學習算法在網路邊緣獲取、存儲	人工智慧/機器學習攻擊	• 分散式帳本技術 DLT • 分佈式和可擴展的 AI/ML 的安全性

關鍵技術	說明	威脅風險	威脅種類
	或處理數據，都被稱為邊緣智慧		
智慧無線電 IR	智能無線電是融合天線、人工智慧技術與機器學習、數據挖掘和數據分析的智能天線	物理層安全威脅	• 毫米波通訊安全性 • 太赫茲通信的安全性 • 可見光的通訊安全性
		人工智慧/機器學習攻擊	• 分散式帳本技術 DLT • 分佈式和可擴展的 AI/ML 的安全性
		軟體供應鏈攻擊	• 虛擬化無線電接入網路的安全性
設備終端和用戶	延續 5G 無線接入網的開放式架構，設備終端來自多個供應商的硬體和軟體系統組成	供應鏈攻擊	• 6G 開發式架構 / Open Source 的安全性

資料來源：本計畫整理

(三)應用場景與降低威脅方案

本計畫從臺灣產業發展與觀察相關的應用去選擇此三類產品原因，主因為：

1. 無人機目前已有許多國家發展，仍然存在待突破的挑戰，適合臺灣 6G 無人機投入的產業是 HAPS 載體，為衛星通訊中繼站、空中行動通訊基地台與空中持續性監測，對臺灣的無人機上游零組件廠商打入國際市場和電信業者商轉都有巨大幫助。
2. 低軌衛星通訊的大面積覆蓋特性，在俄烏戰爭扮演重要角色，協助烏軍抵抗俄軍，將是 6G 必不可缺的基礎建設，世界各國目前也積極在投入發展，臺灣在通訊相關設備供應鏈中佔有重要角色，隨著地軌衛星發展，許多臺灣相關廠商可以打入國際供應鏈市場。
3. 選擇遠距醫療，是因為 COVID-19 在全球蔓延開來，造成各國醫療資源緊急不足，急需遠距醫療來應付高傳染率疾病，臺灣在疫情嚴重期間個醫院提供視訊看病的服務，但只靠鏡頭下的觀察遠遠不構，病患身邊並無醫療設備協助採集病人生理數據，在未來 6G 結合人工智慧與邊緣智慧設備、未來發展遠距智慧醫療，協助醫生診斷來提供人口老化跟偏遠地區的醫療需求。

以下將列舉無人航空載具、低軌道衛星、智慧醫療物聯網三種 6G 應用情境，並進一步介紹 6G 新應用服務與使用到的 6G 新技術下所遭遇到的資安威脅以及提供相對應之降低資安威脅的方法。

1. 6G 應用一：無人航空載具 UAV

無人航空載具俗稱無人機，無人機的應用在 6G 和 AI 的服務支持下，無人機上的邊緣智能設備 EI，計算無人機間的防撞、飛行路徑跟路線規劃、優化群體控制，讓群體無人機飛行控制獲得安全保障。

無人機也是 6G 無線通信的基本要素，在許多情況下，使用無人機技術提供高數據速率無線連接，無人機具有固定基礎設施所沒有的某些特性，例如易於部署、強大的視距鏈路以及具有受控移動性的自由度。

在自然災害等緊急情況下，實施地面通信基礎設施在經濟上是不可行的，有時在動蕩的環境中無法提供任何服務，而無人機可以輕鬆應對這些情況，無人機將成為無線通信領域的新典範，該技術可以促進無線網路的基本要求，即 uMUB、uHSLLC、mMTC 和 uHDD。

無人機基本架構如下：

A. 機架：該機架為安裝馬達和電子裝置提供了一個簡易環境。

B. 無刷馬達跟螺旋槳：馬達帶動螺旋槳旋轉產生推力，以抬升四軸飛行器。

C. 電子調速器(Electronic Speed Control, ESC)：電子調速器為無刷馬達供電，並提供脈衝寬度調變(Pulse-width modulation, PWM)介面，以允許飛行控制器控制每一個馬達的速度和推力。

D. 飛行控制器：飛行控制器其實是一台小型電腦，配備了慣性測量裝置(Inertial measurement unit, IMU)，包含陀螺儀和加速度計)，目的是保持四軸飛行器穩定。

E. 穩壓器：穩壓器旨在為飛行控制器提供 5V 恆壓。

F. 電池：鋰聚合物(LiPo)電池具有較高的能量重量比以及較大的最大放電電流，因此是為四軸飛行器提供動能的首選方式。

G. 射極器+接收器:射極器透過多個操縱杆和切換接收操作人員指令,然後透過 Wifi 發送到四軸飛行器的接收器上。

H. WiFi 無線網卡

I. Raspberry Pi：使用樹莓派電腦寫入 AI 程式，讓無人機有 AI 應用。

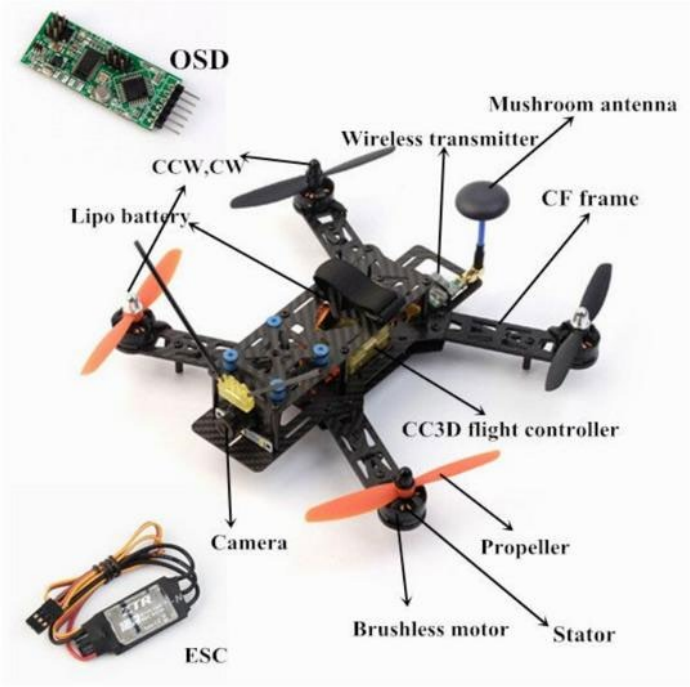


圖72、無人機架構
資料來源：https：//micro.rohm.com/

無人機還可用於多種用途，例如加強網路連接、火災探測、發生災難時的緊急服務、安全和監視、污染監測、停車監測、事故監測等，因此無人機技術被公認為 6G 通信的必備技術之一。常見的無人機產業應用詳如表 18 所示：

表18、UAV 產業應用與效益

產業 UAV 應用	產業效益
公共安全：以空拍獨特視角助力科學決策，高效回應現場所需	● 極速回應：快速部署，掌握先機，獲取任務行動主動權。 ● 掌握全局：空拍獨特視角幫助你全面掌握現場情勢，為科學決策提供重要依據。 ● 安全可靠：無懼各類危險環境，深入前線執行各類關鍵任務。
電力：針對危險、緊急、重複性任務提供一系列解決方案，高效保障電力系統建設、運維等工作	● 效率提升：讓工作人員告別重複性的低價值勞動，提高作業效率。 ● 降低成本：借助無人機技術實現電力作業自動化，有效降低維運成本。 ● 安全可靠：使用無人機代替人員前往高空、高危環境作業，執行任務更安全。
農業：無人機技術的智慧農業解決方案，推動農業生產轉型升級	● 效率提升：讓農夫告別重複性勞動。 ● 成本降低：借助無人機灑藥，操作簡單且自動化程度高，降低人力投入。
測繪：無人機解決方案極大提升了測繪工作的自動化和數位化水平，為測繪作業帶來成本和效率的優化	● 效率提升：無人機外業資料採集之效率約為傳統人力作業方式的 5 至 10 倍。 ● 成本降低：裝置成本低，操作簡單且自動化程度高，讓測繪機構降低人力投入。 ● 測繪成果標準化：提供 DOM、DSM、實景三維模型等標準化測繪成果，滿足多種測量需求。

資料來源：本計畫整理

無人機應用服務使用到的新技術有 AI/ML、可能有 6G 毫米波通訊、太赫茲通訊、可見光通訊、開放式架構、Open API，對應到新技術上會遇到的威脅跟風險和解決方案詳如表 19：

表19、UAV 技術上的威脅風險與解決方案

資安議題	議題描述	降低威脅
AI/ML - 中毒攻擊	通過故意準備的惡意樣本篡改訓練數據(例如，操作標記數據或弱標籤)，從而影響學習結果並導致錯誤分類和錯誤回歸結果。	保護 AI 訓練資料的完整性資料來源可以使用分散式帳本 DLT 技術來達到訓練數據不被竄改保護 AI 資料的完整性。
AI/ML - 逃避攻擊	通過嘗試通過向測試數據注入障礙來規避學習模型來定位測試階段。	用監督學習方式確保模型訓練完整，並建立檢測機制防範惡意攻擊躲過模型判斷機制。
AI/ML - 基於 ML API 的攻擊	在提取攻擊中，對手會獲得您的 AI 系統的副本。有時你可以通過觀察你給模型的輸入和它提供的輸出來提取模型，Rubtsov 說。你戳模型，你會看到反應。如果允許你戳模型足夠多次，你可以教你自己的模型以同樣的方式表現	為機構資訊系統建立、維持和實施事故應變程序、備份操作和運作復原計劃，以確保在緊急情況下關鍵資訊系統維持運作不受影響。 只允許來自獲授權 API 端點的訪問，並藉檢測和防止漏洞以保護 API。
AI/ML - 人工智慧框架的漏洞	大多數 AI 解決方案都利用現有的 AI/ML 框架。這些人工製品或傳統攻擊向量中的漏洞針對其軟體、韌體和硬體環境(尤其是以雲為中心的操作)的目標是 AI/ML 功能的完整性。	對使用的軟體做資安驗測，防範軟體開發的資安危害與降低使用者採用風險。
基礎設施物理攻擊和通信篡改	通信和計算基礎設施的故意中斷和損害會導致決策/數據處理受損，甚至可能使整個人工智慧系統。	使用信任的上游供應商零組件，並在使用前執行沙箱測試。

資料來源：本計畫整理

2. 6G 應用二：低軌道衛星

低軌衛星可整合地面及衛星通訊上的優勢，地面通訊雖頻寬大，但傳輸距離短的弱點，基站布建數量要多，成本高，較適合市區；衛星通訊則涵蓋範圍廣，頻寬較小，適合用於郊區，兩者可互補進而形成全區域覆蓋。

(1) 現行衛星軌道類型：現有衛星軌道共分為低軌道衛星、中軌道衛星、同步軌道衛星、高橢圓形軌道衛星四種。

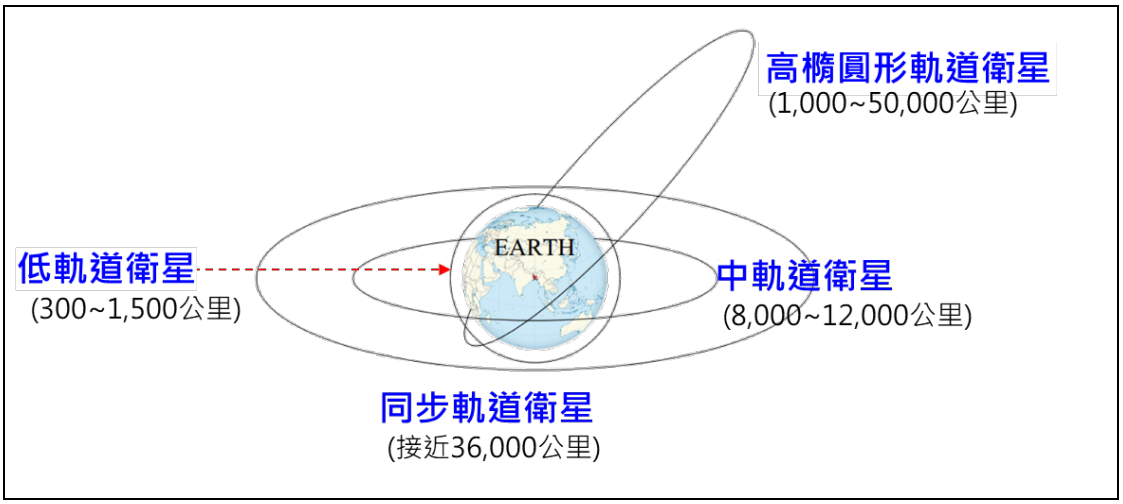


圖73、衛星軌道與種類

資料來源：本計畫整理

A. 低軌道衛星：運行軌道約離地球 300~1,500 公里，離地面近，資料傳輸延遲性低(30~5 毫秒)，主要應用為通訊與地球觀測，如環境監測與氣象觀測等。

B. 中軌道衛星：運行軌道約離地球 8,000~12,000 公里，資料傳輸延遲性中(125~250 毫秒)，主要應用以定位與導航為主。

C. 同步軌道衛星：運行軌道約離地球 36,000 公里，資料傳輸延遲性高(600~800 毫秒)，觀測範圍較大，會固定在相對於地面之同一個位置，可持續對地球上的同個範圍連續觀測，主要應用為訊號不能中斷之電視轉播與需連續觀測之氣象雲圖等。

D. 高橢圓形軌道衛星：運行軌道約離地球 1,000 ~ 50,000 公里，具有較低近地點和極高遠地點之橢圓軌道，可覆蓋高緯與極地地區，主要應用為針對高超聲速目標之飛航段進行探測預警。

(2) 衛星系統架構

衛星系統環境架構大致可分為太空區段(Space segment)與地面區段(Ground Segment)，他們通過無線電頻率 RF 訊號相互通訊。典型的人造衛星系統的結構如圖 74 所示，主要包含三個區段：

A. 太空區段(Space segment)：由眾多衛星組成，負責訊息之接收及轉發。

B. 地面區段(Ground Segment)：為各類通訊站與控制中心，包含地面通訊站、遙傳追蹤指令站、操作控制中心及網路控制中心。

C. 用戶區段(User segment)：為各類終端設備，包含手持裝置、IoT 裝置及小型衛星地面終端設備等。

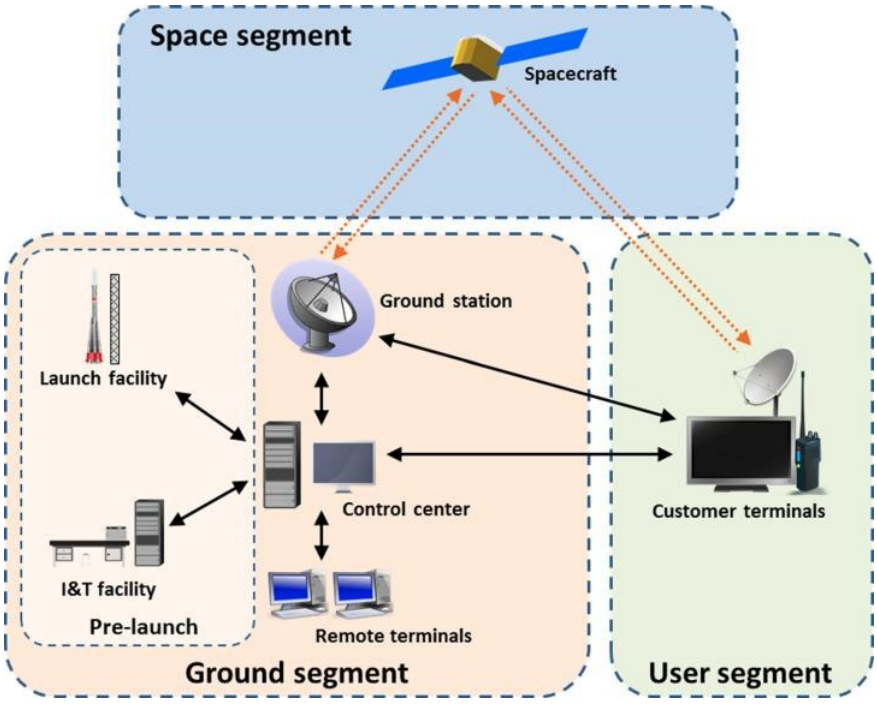


圖74、典型的衛星架構

資料來源：Cyber security in new space

(3) 低軌衛星為 B5G/6G 發展之關鍵技術

由於低軌道衛星具備低延遲性與廣泛覆蓋率之優點，為下一代通訊服務(如 B5G/6G)發展之關鍵技術。從 1980 年初開始，陸續開始興起了衛星的發射熱潮，截至 2021 年底，已有超過 4700 顆的低軌衛星成功上線，佔各類衛星總發射量的 86%。隨著全球網路覆蓋與高速通訊的需求增加、成本降低、技術的進步，許多國家與企業紛紛發射低軌衛星群，來提供覆蓋率更高的通訊服務。其中，低軌道衛星以 Tesla 創辦人馬斯克(Elon Musk)成立之 SpaceX 公司所屬之星鏈(Starlink)計畫為最具代表性，並已於 110 年底提出 Starlink 2.0 計畫，相較於 Starlink 1.0 計畫，提供了更多的頻寬與處理能力。截至 111 年 5 月，SpaceX 已發射約 2400 顆 Starlink 衛星，預計將部署共 1.2 萬顆低軌衛星。

低軌衛星的吞吐量（system throughput）指的是系統在單位時間內傳輸的數據量，而低軌衛星系統的吞吐量通常取決於以下因素：

A. 衛星數量：低軌衛星系統需要足夠的衛星來實現全球覆蓋，衛星數量越多，系統吞吐量越大。

B. 頻譜資源：低軌衛星系統使用的頻段資源有限，因此系統吞吐量也會受到頻譜資源的限制。

C. 地面設施：地面站點的數量和分佈對系統吞吐量也有影響，地面站越多、分佈越廣，系統吞吐量也會越大。

D. 衛星軌道：低軌衛星系統的軌道高度和形態也會影響系統吞吐量。通常而言，軌道高度越低，系統吞吐量越高；而軌道形態則會影響系統的連接性和遍歷能力。

低軌衛星系統的吞吐量詳見表 20：

表20、低軌衛星系統吞吐量表

低軌衛星系統名稱	吞吐量（Mbps）
Starlink	50 - 1500
OneWeb	375
Kuiper	5000
LeoSat	1.6 Tbps
Telesat LEO	300 Mbps

資料來源：本計畫整理

低軌衛星系統的吞吐量覆蓋面積通常用平方每公里（Mbps/km^2）來表示，這是系統在特定區域內提供的網路容量的度量單位。

系統的吞吐量覆蓋面積受到多種因素的影響，包括衛星數量、地面設施、頻譜資源等等。因此，不同的低軌衛星系統的吞吐量覆蓋面積也會有所不同，表 21 為低軌衛星系統的吞吐量覆蓋面積表。

表21、低軌衛星系統吞吐量覆蓋面積表

低軌衛星系統名稱	吞吐量覆蓋面積（Mbps/km^2）
Starlink	0.15 - 3
OneWeb	0.01 - 1.5
Kuiper	2
LeoSat	45
Telesat LEO	0.5 - 1.5

資料來源：本計畫整理

低軌衛星系統可以用於多種用途，例如提供高速互聯網、衛星通訊、地球觀測等。因此，設計低軌衛星系統的目的不是針對特定的用途，而是為了提供更好的衛星通訊和數據傳輸的能力。在過去，低軌衛星的應用主要集中在科學和軍事領域。但現在，由於技術的發展和市場需求的增加，越來越多的公司開始投資和開發低軌衛星系統，以提供各種應用，例如寬頻網際網路連接、物聯網、智慧城市、跟 6G 垂直應用服務的通訊等。

總的來說，低軌衛星系統的設計並不是針對特定的用途而是為了提供更好的衛星通訊和數據傳輸能力，是由於過往對低軌衛星的發展跟應用還不成熟，導致低軌衛星較多在軍事或特定領域內應用，在未來隨著低軌衛星應用的普及會有更多領域使用低軌衛星帶來的通訊便利性，因此，低軌衛星系統不僅針對特定少數使用者而設計，而是面向廣泛的市場和用戶。

低軌衛星作為衛星應用的新型發展方式，近年來在國際上也得到了越來越多的關注和發展，而目前各國都在積極部署各自的低軌衛星，針對低軌衛星未來的應用，除了傳統的衛星大國之外各國都還在部屬階段，而台灣已有相當多的衛星設備製造公司，具有高精度和高品質的生產能力，可以提供低軌衛星所需的各種儀器、設備和元件，例如太陽能電池板、光學器件、通信設備等，且台灣的軟體業發展十分成熟，擁有豐富的資訊技術和數據處理能力，台灣的數據相關產業可提供技術與服務來處理與分析低軌衛星產生的大量數據。

(4) 低軌衛星可能遭遇的威脅風險與應對方法

綜上所述，台灣在低軌衛星產業中可以發揮多種供應鏈角色，從設備製造到數據處理都可以提供相應的技術和服務來支援低軌衛星的發展，這也有助於台灣在未來低軌衛星市場中佔有一席之地。以下將整理低軌衛星可能遇到的威脅風險如下：

A. 威脅：

a. 服務阻斷攻擊(DDoS)：是一種網路攻擊手法，其目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其正常使用者無法存取。

b. 中間人攻擊(MitM)：是一種從中「竊聽」兩端通訊內容的攻擊手法，指攻擊者與通訊的兩端分別建立獨立的聯絡，並交換其所收到的資料，使通訊的兩端認為他們正在通過一個私密的連接與對方直接對話，但事實上整個對談都被攻擊者完全控制。

c. 供應鏈攻擊：是一種傳播間諜軟體的方式，一般通過產品軟體官網或軟體包存儲庫進行傳播。通常來說，黑客會瞄準部署知名軟體官網的服務器，篡改服務器上供普通用戶下載的軟體源代碼，將間諜軟體傳播給前往官網下載軟體的用戶。

d. 社交工程攻擊：在資訊安全方面，社交工程是指對人進行心理操縱術，使其採取行動或洩漏機密資訊。如：網路釣魚、身分盜竊。

e. 未授權訪問攻擊：非授權訪問指未經授權使用網路資源或以未授權的方式使用網路資源，主要包括非法用户進入網路或系統進行違法操作，以及未經合法用户授權的方式進行操作。

B. 降低威脅方法：相關對應的解決方案詳如表 22。

表22、低軌衛星的威脅風險與解決方案

資安議題	議題描述	降低威脅
服務阻斷攻擊(DDoS)	是一種網路攻擊手法，其目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致其正常使用者無法存取。	● 網路流量和使用者行為分析：來自單個 IP 地址或 IP 範圍的可疑流量，或奇怪的流量模式，如在非正常時段激增，或不自然的模式。 ● 中斷受影響的網路設備與機構網路之間的連接。 ● 使用 DDoS 黑洞(black hole)路由 / 過濾技術建立特定的 IP 路由表堵截網路攻擊，並將 DDoS 攻擊流量導向至「黑洞」棄置。 ● 應評估DDoS攻擊造成的損害並制定合適的復原措施，以恢復受影響的服務並防範再遭遇相同攻擊。
中間人攻擊(MITM)	是一種從中「竊聽」兩端通訊內容的攻擊手法，指攻擊者與通訊的兩端分別建立獨立的聯絡，並交換其所收到的資料，使通訊的兩端認為他們正在通過一個私密的連接與對方直接對話，但事實上整個對談都被攻擊者完全控制。	● 使用者行為分析：網域和本機的帳號監控，使用者地理位置登入模式分析，透過分析與監控來發現傳送可疑流量的使用者或執行程序就將它終止。
供應鏈攻擊	是一種傳播間諜軟體的方式，一般通過產品軟體官網或	● 部署強式程式碼完整性原則，只允許授權的應用程式執行。

資安議題	議題描述	降低威脅
	軟體包存儲庫進行傳播。通常來說，黑客會瞄準部署知名軟體官網的服務器，篡改服務器上供普通用戶下載的軟體源代碼，將間諜軟體傳播給前往官網下載軟體的用戶。	● 對平台監控：使用可自動偵測和補救可疑活動的端點偵測。 ● 執行程式隔離：對可疑或已感染之程式與系統隔離或中止程式。 ● 對軟體廠商和開發人員：確保只使用可信任的開發工具開發軟件、為確保系統和敏感數據的安全，定期或在重大系統變更後進行保安滲透測試、通知供應鏈攻擊事故，並提供最新最準的資訊。
社交工程攻擊	在資訊安全方面，社交工程是指對人進行心理操縱術，使其採取行動或泄露機密資訊。例如:網路釣魚、身分盜竊。	● 訊息分析：寄件者信譽是反垃圾郵件功能的一部分，會根據寄件者的許多特性來封鎖郵件。 寄件者信譽依賴寄件者相關保存的資料來判斷對輸入訊息採取的動作。 ● 檔案分析：使用動態分析工具分析惡意程式。
未授權訪問攻擊	非授權訪問指未經授權使用網路資源或以未授權的方式使用網路資源，主要包括非法用户進入網路或系統進行違法操作和合法用户以未授權的方式進行操作。	● 可執行白名單，或使用黑名單過濾使用者訪問。 ● 採用多因素身分驗證，並限制用戶對敏感系統的訪問。 ● 監控登入活動：系統在部屬了檢控系統之後，就可以即時發現企業系統或設備中存在的可疑帳戶登入或異常登入活動，並採取相應的補救策略，如撤銷帳戶訪問權限以避免攻擊。

資料來源：本計畫整理

3. 6G 應用三：遠距醫療傳輸

(1) 遠端醫療介紹

由於人口平均年齡的增長和慢性病患者數量急速增加，對未來的醫療保健系統形成挑戰，新冠狀病毒出現後改變了人類社會的生活行為，且必須跟新冠狀病毒共存，智慧醫療可用於檢測冠狀病毒，降低醫療人力負擔，健康醫療為未來關鍵的垂直應用之一。

遠端醫療物聯網用到的關鍵技術，有多路訪問邊緣計算和 D2D 通訊，MEC 是一種分散式雲提供儲存、計算、網路資源，為內存受限的醫療物聯網設備提供額外儲存空間，通過低延遲更貼近消費者以滿足患者遠程監護等應用的需求，讓資源受限設備(如穿戴裝置)上要處理的複雜計算透過MEC處理降低工作負載，透過 D2D 通訊提供患者相關訊息，無需透過基站允許相互靠近的設備直接通訊減少延遲，遠端醫療的電子健康系統分層架構如下：

A. 傳感層：包括部屬用於健康資料(如血壓、血氧、飽和度跟心跳)檢測的 IoMT 設備和組織集群。測量資料通過 D2D 通訊從設備發送到節點，這得益於 IoMT 設備和節點之間的接近性(資料傳輸)。

B. 處理層：每個集群由一個節點管理，部屬的目的是減少低端 IoMT 設備的工作量，同時減輕 MEC 服務器執行的任務。

C. 儲存層：MEC 節點代表所提出架構的最高級別，位置於 RAN，其主要功能涉及儲存儲存從控制器獲得的訊息(訊息儲存)。因為儲存在邊緣的資料可以低延遲訪問，此外 MEC 可以由節點委託執行計算特別複雜的資料處理(Complex Data Elaboration)。

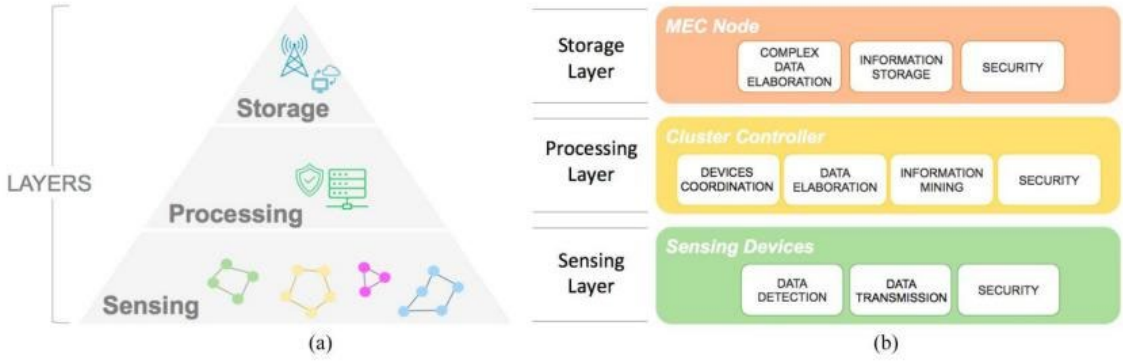


圖75、電子健康系統分層架構

資料來源：MEC and D2D as Enabling Technologies for a Secure and Lightweight 6G eHealth System ,IEEE

(2) 遠端醫療保健使用的技術：

A. 遠程監測和援助：它允許遠程患者監控和遠程提供醫療服務。

B. 環境輔助生活：它在技術上使護理人員能夠在偏遠地區獨立生活。

C. 電子病歷系統(electronic health record, EHR)：這些系統維護所有與健康相關的數據，並能夠使用最新的 ICT 共享這些數據。

D. 數據管理和分析：現代醫療保健中產生了大量數據，因此有效的數據管理和分析有助於在正確的時間做出正確的決定。

E. 分佈式服務架構：它代表了新的服務架構，可以在用戶附近處理和存儲醫療保健訊息，以提供及時的醫療保健。

F. 人工智慧和機器學習：由人工智慧和機器學習領域的最新技術和工具，完成對 MIot 等大量設備生成的大量數據的分析。

G. 6G：6G 為遠程醫療技術和服務提供底層連接基礎設施。

H. 醫療物聯網：它使物聯網和醫學學科的結合為醫療保健帶來深遠的好處，從開發專門的醫療保健特定物聯網設備和連接基礎設施，到啟用新的服務和實踐。

I. 定位技術：它允許準確定位患者、遠程護理單元、車輛和人員，以實現醫療保健服務，例如準確監測和協助。

J. 分散式帳本技術：安全地共享和交換數據並追蹤其使用情況。

K. 增強現實和虛擬現實：為護理人員提供視覺遠程協助，並為護理人員提供監控模式。

L. 機器人：機器人技術在醫療保健中有大量應用，從遠程協助和幫助到遠程手術。

M. 安全和隱私：用戶訊息的敏感性需要強大的安全和隱私技術。

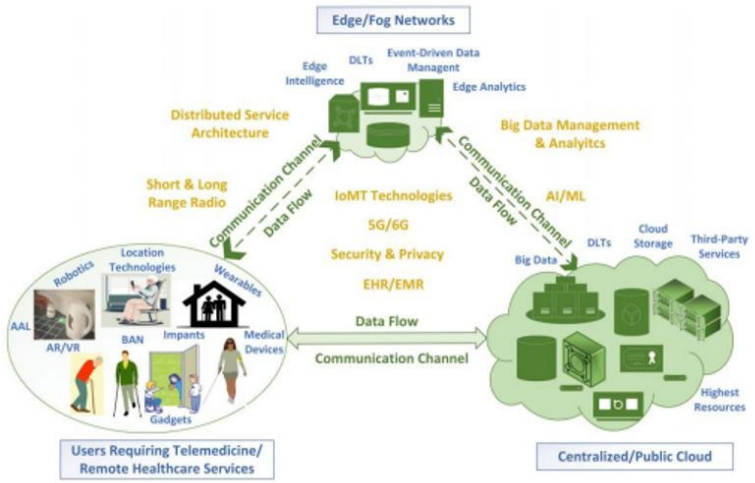


圖76、遠端醫療保健使用的技術

資料來源： Emerging Technologies for Next Generation Remote Health Care and Assisted Living,IEEE

表23、遠距醫療傳輸的威脅風險與解決方案

資安議題	議題描述	降低威脅
供應鏈攻擊 (Supply Chain Attacks)	攻擊者通過獲信賴的第三方供應商可以接達多個機構的系統。機構即使已經安裝最穩健可靠的	基站、邊緣設備：確保第三方供應商已採取足夠的保安措施保護供應鏈渠道，並根據機構的資訊保

資安議題	議題描述	降低威脅
	數據保安系統，但由於商業或開放源碼軟體/系統組件的保安漏洞而被攻擊者植入惡意程式碼，仍然有可能受到網路攻擊或發生保安事故。	安政策定期進行資訊保安評估和審計。 確保廠商或開發人員使用可信任來源的開發軟體。 對全新或修改過的硬體、固體、軟體和配置變更在上線使用前，須於沙箱環境檢查測試。
服務阻斷攻擊(DDoS)	DDoS 攻擊是，攻擊者通過遠端控制多台受到感染的邊緣設備向特定目標(可能是基站)同時發動攻擊消耗其資源，使其不能提供正常服務。	偵測 DDoS 攻擊：在基站的系統放置監測 IP 網路流量、和系統資源的使用情況，在發生 DDoS 攻擊時能迅速中斷感染設備的連線以減低損害。 復原：評估 DDoS 造成的損害並制定復原計畫，分析系統潛在漏洞並修復，防範日後再被同攻擊損害。
中間人攻擊(MITM)	中間人攻擊技術將自己定位在兩個或多個網路設備間，以支持後續攻擊行為，如封包竊聽或傳輸數據操作。通過濫用網路協議的功能(如 ARP、DNS、LLMNR 等)，攻擊者可能會強制設備通過攻擊者控制的系統進行通訊，以便他們可以收集訊息或執行其他操作。	中間人攻擊是一個缺乏相互認證的攻擊。大多數的加密協定都專門加入了一些特殊的認證方法以阻止中間人攻擊，如 SSL 協定可以驗證參與通訊的一方或雙方使用的憑證是否是由權威的受信任的數位憑證認證機構頒發，並且能執行雙向身分認證。 監控基站系統網路流量，連線設備的使用者行為分析，發現異常流量跟行為模式則對其網路隔離或中止。

資料來源：本計畫整理

(四)研析成果

本章節以 6G 無線網路潛在相關技術與資安議題為主，針對國際相關應用情境進行研析，盤點 6G 相關的資安威脅攻擊，並進一步延伸至無人機、低軌衛星、遠距醫療此三類產品，進行資安威脅與降低資安威脅方法進一步整理與說明。

臺灣是全球通訊設備供應鏈的主要供應國，更需要知道在 6G 產業出現的新形態基礎設施，像是低軌衛星、HAPS，UAV 等設備，這幾年國際間相當注重供應鏈安全，在 2020 年美國公佈一份 5G 乾淨網路名單，目的確保其電信網路、雲端、數據分析、行動應用、物聯網、5G 技術不使用不受信任的設備供應商，大多數是指來自中國的供應商，此趨勢大致會延續到 6G，這對臺灣的設備供應商是一個擴大全球市占率的機會，但前提是需要證明我國設備供應商的設備能符合國際資安標準。

透過本章節可以初步了解 6G 可能架構，與使用新興技術當前會遇到的資安威脅，讓各家廠商可以有資安實作參考方向，並於未來計畫中持續規劃與建置 UAV 端的資安檢測平台，以期提供給 UAV 廠商，對 6G 場域進行資安健檢，提升未來我國 6G 產業的資安防護能力。

六. 計畫執行情形-6G 跨產業資安聯防生態探索研究

本計畫以 B5G/Pre-6G/6G 通訊技術為核心，進行 6G 跨領域生態應用的特性與業者營運進行研析，期望推動 6G 資安產業與生態體系發展，並促進未來 6G 應用場域實驗建立落實政府、法人研發與產業合作，結合國內資安業者、系統整合商、網通設備廠商與專網業者合作，辦理 4 場座談會議，進行 6G 產業變遷預測、服務發想規劃、在地專網資安解決方案與服務框架研析，進而協助國內資安檢測服務業者，預先了解 6G 可能面臨與 5G 不同資安風險與威脅，超前部署 6G 資安檢測能量，提升國際競爭力。

(一) 6G 跨領域生態應用特性探索

由於 B5G、Pre-6G、6G 等預計將運用上高空平台、衛星傳輸等技術，其覆蓋面積將更勝今日全數用地面基地台架設的 5G 系統。在覆蓋面積更廣泛下，其應用與產業生態也將更廣泛。

單以今日 4G 而言，由於 4G 強化行動頻寬傳輸率與即時性，今日許多線上遊戲已從個人電腦轉向手機，遊戲開發商與遊戲營運業者紛紛推出行動裝置原生的遊戲；又如過往多數國內用戶是透過有線電視系統業者所牽佈的同軸電纜收看電視，而今已轉成過頂服務(Over-The-Top, OTT)型態的網路電視，或直接以手機觀

看相關視訊。

4G 改變了遊戲與收視等內容服務傳遞通路，甚至早已音樂、閱讀等領域，以及改變電信業自身，過往電信營運商可在春節前後收取可觀的 SMS 營收，但在即時傳訊(Instant Message, IM)的行動應用程式普及後，此一營收也明顯下滑，特別是從年輕族群開始侵蝕，甚至已大幅涵蓋長輩年齡層。

進一步的，4G 的 LTE-MTC、5G 的 mMTC 雖然有多種物聯網應用可能，但多數認為其殺手應用(killer application)將為智慧抄錶，因此電力業者必然成為下一個行動通訊服務的含括對象，從而進入應用生態圈，後續更可能進一步擴展至水力、瓦斯等相近似的公用事業。

再加上 5G URLLC 的加入，以及正在摸索發展中的 6G 等，必然使行動通訊的生態更為複雜，故有必要先行推探與討論 6G 應用生態，進而對應推敲出其對應的資安防護生態。

1. 現行5G 生態

我國現階段 5G 行動通訊已有數個 5G 專網的實際應用案例，例如中華電信的 5G 專網讓新北市自駕車使用 C-V2X 通訊來提供路側資訊予自駕車，以此強化自駕車的行駛安全。

或有臺灣大哥大提供 5G 專網服務供智慧工廠應用(具體企業匿名)，由於 Wi-Fi 有覆蓋、干擾、跨廠區傳輸等問題，故改以 5G 專網替代其通訊，包含用 5G 通訊連線產線設備、生產管理系統等以利即時檢驗作業，以及自動搬運車的控制等，並獲得具體營運提升效益，如貨料搬運速度增快 15%。

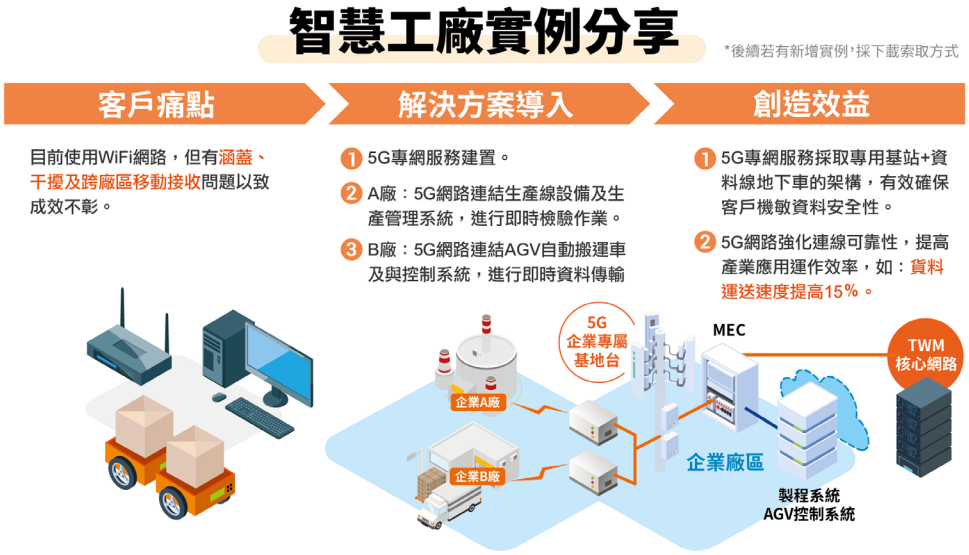


圖77、我國製造業者運用5G 專網實現智慧工廠
資料來源：臺灣大哥大

類同於此，臺灣大哥大也有 5G 專網的智慧醫療案例，運用於急診室與護理站間的資訊傳遞，以及支援 AR 應用，協助急診室醫護人員即時掌握病患資訊，另也有智慧零售、智慧校園等實例。

遠傳電信也運用 5G 專網實現全台第一個 5G 糖尿病連續式醫療照顧服務，或在台東導入第一個 5G 遠距醫療區域，也用於

蘭嶼、綠島等心臟專科遠距診療，甚至運用 4G NB-IoT 通訊傳遞患者的血糖數據。或者也用於桃園市的智慧路燈、用於桃園水務局的下水道監測、用於台北自來水事業處建置智慧水錶、台北市 5G 自駕巴士等。

歸結而言，4G、5G 除了由三大電信商持續提供個人、家戶的行動通訊服務外，也已經以專網型態用於公部門、醫療業、製造業、教育業、運輸業，也確實解決諸多痛點，例如離島間通訊、跨廠區通訊能力的不足等。

除此之外，三大電信商也已提出多種專網應用情境，例如中華電信提出用專網無線無人機操控，使無人機可執行空中巡檢任務，或提供企業各類型展售的增強實境需求傳輸，或遠傳電信提出可用於跌倒偵測的看護服務等，很明顯 5G 乃至未來 6G 服務可望深入各類型產業。

圖78、中華電信官網提出5G 專網的無人機巡檢支援服務
資料來源：中華電信

2. 6G 營運生態描繪

6G 估計仍會延續與 5G 相同，以各國特許的電信營運商為主要業者，原因包含 5G、6G 所用及的新波段頻譜多需要授權，而非免授權的全球通行波段，僅少數例外，例如 60GHz。在需要頻譜授權下，仍需要主要營運商統籌管理與運用頻譜。

另一原因是許多國家已出租、競標出頻譜多年時限，例如我國為 15 年使用權，很明顯 15 年的頻譜使用時間必然跨通訊世代，每一世代約 6 至 8 年時間，故 5G 的主要營運商，在未來 6G 時代仍大程度會是主要營運商。

不過，由於 5G 已開始探索物聯網相關應用，不再是人們手持式的通話、上網、看影視的應用，故必然需要產業垂直應用來支撐，故 5G 電信營運商已於近幾年陸續開通 5G 專網服務，基礎建設仍然由主要電信商建置與完成覆蓋，但可提供不同組態配置供企業租用。

舉例而言，遠傳電信即提供四種型態的專網供企業選擇，分別為共享型、專用型、獨立型、切片型。遠傳電信也同樣提供四型，稱法則為：網路切片、企業專用基地台、企業專用基地台及資料面核心網，以及獨立網組，詳如圖 79 所示：

圖79、遠傳電信提供四種5G 專網組態
資料來源：遠傳電信

不同的組態也分別適合不同的應用，例如車聯網適合網路切片，一般物聯網服務或各種綜合性應用也適合用網路切片，但新創應用開發程式則適合用企業專用基地台，或者綜合性應用也可以採行獨立組網等。

至於臺灣大哥大則提供六種組態，分別為：「專頻專網」、「共頻專網」、「共頻專網＋共基站(即基地台)」、「企業 MEC＋共基站」、「網路切片＋共基站」以及「網路切片」。六種組態具有特性差異，簡要對應如下：

方案	企業資訊路由	企業維運難度	擴充彈性	資料處理延遲性	企業建置成本	3GPP標準	資安維護*
專頻專網	自有	高	低	低**	高	是	高(企業)
共頻專網	自有	高	低	低**	高	是	高(企業)
共頻專網+共基站	自有	高	低	低**	高	是	高(企業)
企業MEC+共基站	自有	一般	一般	低**	中	是	高(企業)
網路切片+共基站	台灣大	低	高	低	中	是	高(台灣大)
網路切片	台灣大	低	高	低	低	是	高(台灣大)

圖80、臺灣大哥大提供六種5G 專網組態

資料來源：臺灣大哥大

除了基礎建設外，主要電信營運商也跨入商務、內容及其他服務領域發展，例如臺灣大哥大即有同一集團的 momo 購物台，遠傳電信亦因此購併時間軸科技的 Friday 購物網，並改名為遠時科技，宣布同樣進入電子商務領域。

另一個應用案例，是臺灣大哥大與美國迪士尼合作，於電信方案中搭配 Disney+訂閱，或試圖與有線電視系統業者合作，推動有線電視同軸電纜的數據服務應用。整體而言，未來的訊號傳輸、內容與服務傳遞，都將朝更聚合、統合的趨向發展。

3. 對應防護生態描繪

6G 移動網路是透過衛星網路打造的陸海空三度空間全都隔為一體的網路環境，除了繼承前幾代的漏洞外，將帶來未知的資訊安全威脅與挑戰，同時，跨洲之間 9 成以上語音和數據流量傳遞仍大量倚賴海底電纜，興起中的衛星通訊也難在短時間取代，這其中牽涉到更多機密敏感數據在海纜間傳遞，隨著地緣政治的變動因素、駭客無差別攻擊升溫，也會增加資料竊取、竄改等風險。

由於 5G、6G 有諸多應用屬物聯網應用，物聯網裝置的運算效能、硬體資源不若個人電腦與智慧手機，因此其資安防護方式也必須對應改變。以下歸納幾種對應的防護情境做為發想參考：

(1) 加強裝置內的硬體防護技術，例如使用有加解密加速電路的晶片，取代以單純軟體搭配通用型處理器、控制器的加解密運算工作，或者使用硬體隨機數字產生器(Random Number Generator, RNG)，或其他硬體方式實現的資安防護，例如硬體隔離運算、硬體隔離的金鑰儲存等。

(2) 裝置上使用嵌入式的資安防護軟體，有可能是以原生方式開發的嵌入式防護軟體，也可能是以個人電腦、智慧手機為基

礎，進行瘦身(thin)化、輕量(lightweight)化工程而成的嵌入式防護軟體。

(3) 盡可能將吃重的防護運算工作轉移(off-load)至裝置外，或改以其他輕量的方式達到相近的防護水準。以轉移而言，可以將防護運算工作轉移到後端的資料中心，資料中心有充沛的運算力可大幅分擔裝置端的安全防護工作，例如應用程式安全性查核、資料完整性檢查等。若為了追求防護的時效性、反應速度，也可以將工作轉移至邊緣運算，亦即鄰近基地台處。

上述輕量化防護移轉是另類的改變安全防護的演算法，舉例而言，美國資安業者 Cylance 強調以人工智慧模型的推論來實現資安防護，其模型僅有 25MB 容量，且人工智慧能將相近的行為均判定為威脅，目前的 AI 形成 Model 是透過威脅出現的時間差，在模型的創建和第一個受害者和安全人員之間，看到威脅的時間，來保護這些受害者的公司。另外將 Model 使模型面臨一系列威脅。這些包括九個不同的「威脅家族」，每個家族集合包含五個在外在發現的變體。圖 81 顯示了平均有利條件(Predictive Advantage, PA) 值，每個威脅家族。 數字越大，與模型的時間距離越大，創

立日期到第一次已知的檢測特定的資料集。更高的 PA 值更多展示了模型預測未來的威脅的能力。

Predictive Advantage by Threat Family	
Threat Family	Predictive Advantage (months)
Bad Rabbit	29
Cerber	30
GhostAdmin	24
GoldenEye	23
Locky	20
NotPetya	25
Petya	26
Reyptson	27
WannaCry	24

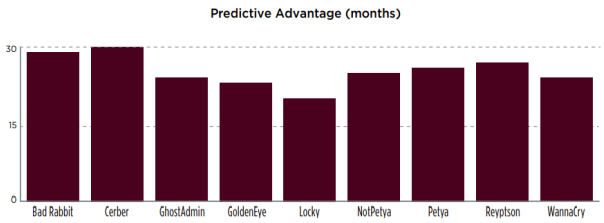


圖81、透過九大威脅家族建立模型
資料來源：Cylance，本計畫整理

另外模型建立也透過個別「威脅家族」來建立，將程式運行持續一段時間，透過添加部分功能變量及不同的入侵方式與控制單元一起改變，每個"家族"使用了不同的變體，透過每一個"威脅家族"組內新攻擊為變體，可能會在不同時間出現在現實世界中。例如以黃金眼為例，樣本範圍從 2016 年 12 月到 2017 年 5 月至 2017 年 7 月如圖 82 所示。

CAMPAIGN: GoldenEye	
Threat Variant	Predictive Advantage (months)
GoldenEye1	20
GoldenEye2	26
GoldenEye3	26
GoldenEye4	19
GoldenEye5	24

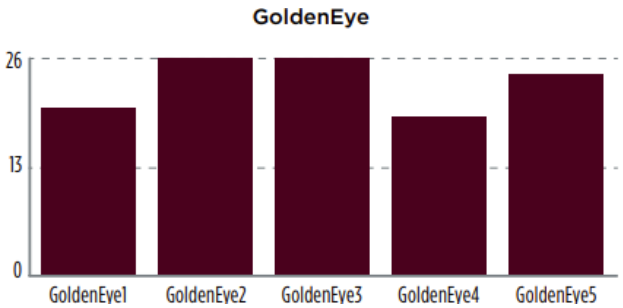


圖82、透過個別威脅家族變化建立模型
資料來源：Cylance，本計畫整理

故對惡意程式的特徵資訊更新的倚賴度較低，允許每半年進行一次更新。相對的，傳統倚賴大量惡意程式特徵碼比對的防護方式，則過去耗佔運算資源，且必須每日、每週進行特徵碼更新，不適合 6G 物聯網應用。

另一例子是 Google 為平價訴求的 Android One 手機所提出的加密演算法鐵線蕨(Adiantum)，傳統手機內資料的加密多採行高級加密標準(Advanced Encryption Standard, AES)演算法，設備製造商考量成本，有時會運用低階的處理器，例如 ARM Cortex-A7，它並沒有支援 AES 的硬體。在這些設備上，AES 運算速度太慢，會導致不好的使用者體驗； 應用程式將需要更長的時間才能啟動，並且設備通常會讓人感覺慢得多。因此，雖然 Android 6.0 以來，大多數設備都需要存儲加密，但 AES 性能較差(50 MiB/s 及以下)的設備除外。Google 公司一直在努力改變，因為 Google 相信應用新的加密法更適合所有人。特別在 HTTPS 加密中， 當硬體加速不可用時，ChaCha20 流密碼比 AES 快，同時也非常安全。演算法由於它速度很快，完全可依賴於所有 CPU 支持的操作：加法、旋轉和互斥運算(eXclusive OR, XOR)。 出於這個原因，Google 運用 ChaCha20 軟體速度也很快的 Poly1305 身分

驗證器作為新的傳送層安全協定(Transport Layer Security protocol, TLS)密碼套件來保護 HTTPS 網際網路連接。ChaCha20-Poly1305 已成為標準 RFC7539，它極大地提高了缺少 AES 指令的設備上的 HTTPS 性能。AES 演算法恐過於吃重，故改用鐵線蕨演算法，該算法減少加密演算的循環次數，加上其他的權宜設計等，但最終仍能達到足夠的防護強度，且只需 AES(以 256 位元而言)加密 20%運算力，詳如圖 83：

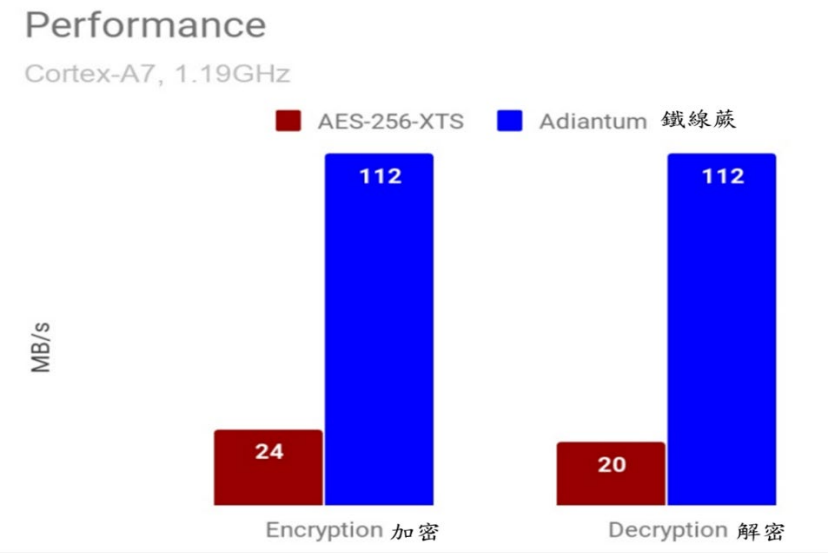


圖83、加解密演算法明顯比 AES 輕量快速
資料來源：Google，本計畫整理

磁碟和檔案加密在存儲設備上的資料數據組織通常為 4096 位元的「區間(sector)」。當檔案系統向設備提出讀取或寫入區間要求時，加密層會截錄該要求，並在明文和密文之間來進行轉換。這意味著必須在 4096 位元的明文和 4096 位元的密文之間進行

轉換。 但是要運用 RFC7539，密文必須比明文稍大； 密碼隨機數和資料完整性資訊需更多一點空間。 有一些軟體技術可找到存儲這些額外資訊的地方，但它們會降低效率並且會給文件系統設計帶來很大的複雜性。

在使用 AES 運算，磁碟加密的傳統解決方案是使用分組加密演算法 XTS 或磁碟扇區加密演算法 CBC-ESSIV。目前 Google 已經強制設備製造商在 Android 6.0 或更高版本採用 AES-128-CBC-ESSIV 進行全磁碟加密，和 AES-256-XTS 進行檔案系統加密，但是這並無法廣泛運作在低階 ARM 處理器上，導致目前市場上的許多低階接設備都沒有使用加密。

Google 使用前述鐵線蕨加密演算法 Adiantum，基於 AES 的長度維持加密方案(如 HCTR 和 HCH)，這項技術實作在 ARM Cortex-A7 上，對 4096 位元區間的加密和解密約為每字節 10.6 個週期，不但可以在低階設備上使用，而且可以比 AES-256-XTS 快約 5 倍。

歸結上述，硬體電路、硬體晶片手法的資安防護，我國有力旺科技、鴻璟科技能提供矽智財授權，或有新唐電子(Nuvoton，前身為華邦電子 Winbond 的邏輯晶片事業單位)的可信任模組平

台(Trusted Platform Module, TPM)晶片，或有匯智安全科技的硬體安全模組，以及伊諾瓦科技 eNova 的安全晶片與硬體模組，國外亦有多家知名業者提供安全晶片與硬體安全模組，如歐洲意法半導體 STMicro、德國英非凌 Infineon 等。

至於嵌入式防護軟體也有鴻璟、趨勢科技，國外知名業者也包含前述的 Cylance 以及邁克菲 McAfee 等。而轉移至後端資料中心，則牽涉較多在物聯網裝置內的代助程式(agent)，資料中心多半能因應處理。

某種程度上，5G、6G 物聯網所用的防護技術會與產業自動化、工業控制領域所用的防護技術高度雷同，此類型的設備具有多樣性，運算力同樣有限、硬體資源同樣有限。至於雲端與資料中心的資安防護，已與一般傳統資訊技術(Information Technology, IT)的資安防護無異，大體多會用上防火牆、網頁型應用程式防火牆(Web Application Firewall, WAF)、負載平衡(Load Balance, LBS)、入侵偵測系統(Intrusion Detect System, IDS)等。

此外，也會用及防護營運中心(Security Operation Center, SOC)、防護資訊與事件管理(Security Information and Event Management, SIEM)、資安協調、自動化與回應(Security

Orchestration Automation and Response, SOAR)、資安威脅資訊分享與分析中心(Information Sharing and Analysis Center, ISAC)等，此方面多以外商為主導主佔，例如 Splunk、Fortinet。

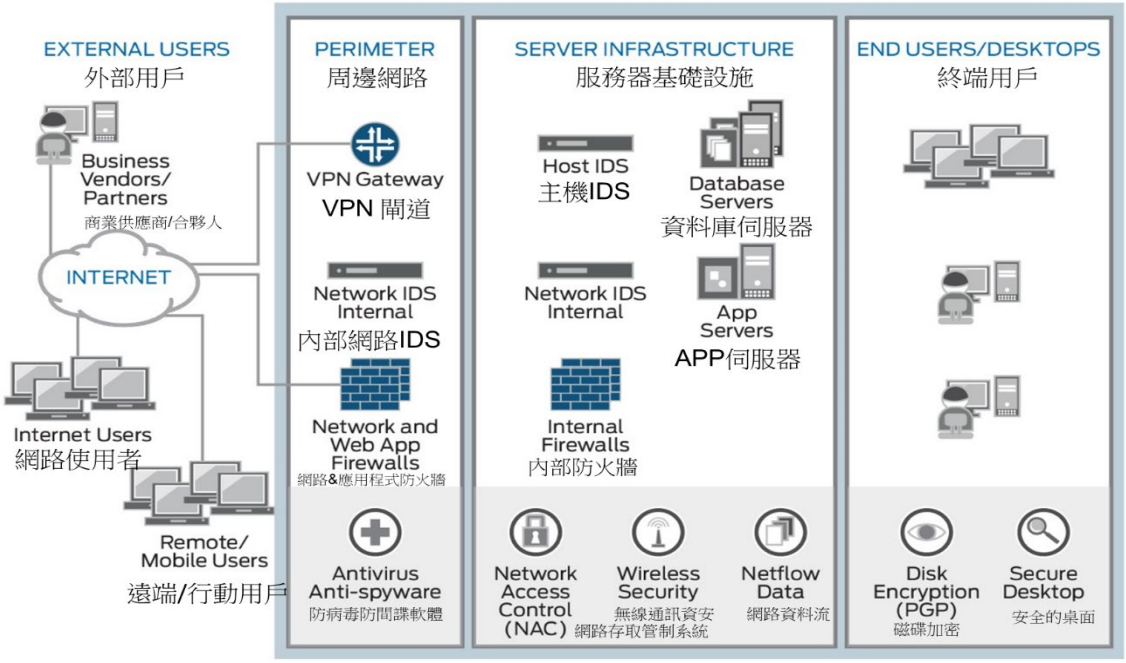


圖84、典型 SIEM 功能示意圖
資料來源：Juniper，本計畫整理

(二) 6G 跨領域生態業者營運解析

3G、4G 的出現，已使過往的數位娛樂通路開始改變，2003 年 Apple iTune Store 的出現，逐步顛覆傳統以光碟片印製與上架的銷售通路，2007 年 Apple TV 也逐步帶動今日 OTT 視訊的發展，而逐步瓦解傳統地面無線電視、衛星無線電視，乃至於同軸電纜的有線電視，2010 年 iPad 的出現也開始改變閱讀市場，更之後遊戲產業也同樣變化，如 Steam。故電信營運商也開始建立

自己的數位娛樂通路，不再單純提供通訊連線服務(產業俗稱笨水管 dump pipe)，如中華電信推出 Hami 系列的服務，如 Hami Video、Hami 書城、Hami 市集，臺灣大哥大也有 My 系列服務，如 MyVideo、MyMusic 等。

不僅前端改變，4G、5G 的後端也開始改變，4G 全面 IP 化，廢除切換式傳輸，但 4G 設備仍以專屬系統方式提供，而 5G 則允許以一般用途伺服器搭配軟體方式來實現專屬設備，毫無疑問的，行動通訊產業比過往更擁抱開放、更擁抱產業現行大宗技術，以及更傾向以商業現貨(Commercial-off-the-shelf, COTS)來實現。另外 6G 將引入 HAPS 及衛星通訊，此必然會衝擊影響現行衛星產業，特別是以轉播或通訊任務為主的衛星，包含現行的 SNG 車與轉播衛星、衛星電話，現行船舶與飛行器所用的衛星通訊等，是否要從業者專屬轉向相對開放標準的 6G，也同樣需要評估。

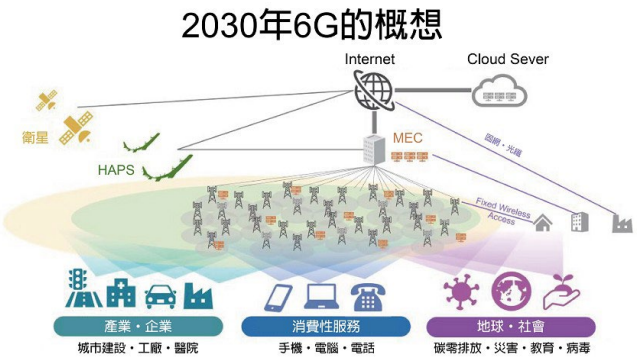


圖85、2030年6G 構想用及衛星與 HAPS

資料來源：Softbank

應用情境以「下世代遠程醫療保健服務」為例，因世界人口老齡化、全球慢性病的流行率迅速增加等因素，將對全球醫療保健系統的功效與人力服務成本效益造成巨大的影響，未來將透過新型智慧的遠程醫療保健服務，以提高治療結果之水平、成本效益與醫療保健的可持續性，所會用到的技術包括：精準定位技術、機器人技術、AR/VR、與醫療物聯網設備，用 6G 網路及人工智慧/機器學習技術串連起來，所衍生的資安議題就有 AI/ML(AI/ML 攻擊問題)、Location 定位(隱私洩漏問題)、IoMT(供應鏈安全)，尤其在 PLS 物理層傳輸的資安，6G 是智慧醫療的底層通訊基礎設施，例如網路切片技術，為醫療服務網路提供專用切片，因使用了網路切片，可能會遭遇網路切片攻擊，僅幾秒的延遲，就可能危及病患生命安全，資安防護的等級應列為最高，網路系統必須做到嚴密的監控管理。展望 6G，必然前端、後端會有更多的融合，不僅是傳統通路服務的改變，更可能出現跨領域、跨產業的合作與新應用，因此有必要先行推探以利未來產業布局。

資安議題在電信網絡的發展一直是很重要的考慮重點，與 3G 相比，4G 的安全性顯著的有所增強。在認證安全機制採用 EPS-AKA(Evolved Packet System – Authentication and Key

Agreement)方式完成 4G 認證，包含 3 個主要單元完成身分認證程序，包括用戶設備、服務網路和本地網路，但 4G/LTE 安全架構仍存在一些弱點，包含 4G 可以透過身分認證請求發動 DDoS 攻擊、駭客也可以偽造正常的網路服務來跟蹤訂閱者。而 5G 行動通訊也持續強化改善認證安全機制，主要包含 EAP-AKA(Extensible Authentication Protocol – Authentication and Key Agreement)、5G-AKA 與 EAP-TLS(Extensible Authentication Protocol – Transport Layer Security)3 種身分認證機制，EAP-TLS 在 5G 定義為在有限使用情況下(例如專用網路和 IOT 環境)，包含筆電或物聯網設備，都可以使用 EAP-TLS 訂閱和訪問 5G 核網；但由於其複雜性更高，因此 5G 也衍生了更多安全漏洞待解決。例如，由於它方服務網絡和基礎網絡之間的仍缺乏信任機制，此漏洞可能允許攻擊者追蹤，而 5G-AKA 可以防止偽基站攻擊(IMSI-catcher)，但網路駭客透過時間觀察同步失敗消息，在 5G 中仍然可以進行用戶跟蹤，以及透過欺騙性的預身分驗證，在 5G 中也還尚未得到解決。6G 網絡設計基於雲及開放可程式編輯網絡平台的變化，將促使認證架構的改革，需要新的身分驗證模型和密碼方案來確保通信安全， 6G-AKA、量子安全密碼方案和物

理層安全都是發展的重點，此外，6G 可能會繼承 5G 的一些安全模型，但是，需要添加許多新功能來補充這些功能，如跨網路漫遊的身分驗證機制、滿足電信事業需求的新業務模型或電信事業之間的相互信任協議、跨切片通信中的認證等。

1. 電信營運商角度

電信營運商過往均直接銷售通訊服務給個人、家戶及企業，均為服務的終端使用者，然之後開始有允許分銷的作法，例如行動虛擬網路營運商(Mobile Virtual Network Operator，MVNO)，由其運用現行基礎設施提供特色化、加值化的通訊服務。

而至 5G 時代，因網路切片等技術的出現，5G 專網服務開始出現，允許企業大程度使用電信營運商的基礎建設，支援其現行營運，或進一步實現新應用。

不過，5G 因其技術特性，也使營運商承受比過更高的建置成本、營運成本。舉例而言，5G 由於使用更高頻段，相同功耗下的服務覆蓋面積較過往小，需要建置更多的基地台方能達到與過往相同的覆蓋，建置成本高。同樣的，相同覆蓋面積內的服務運作，也會耗用比過往更多的電力，達現行的數倍。

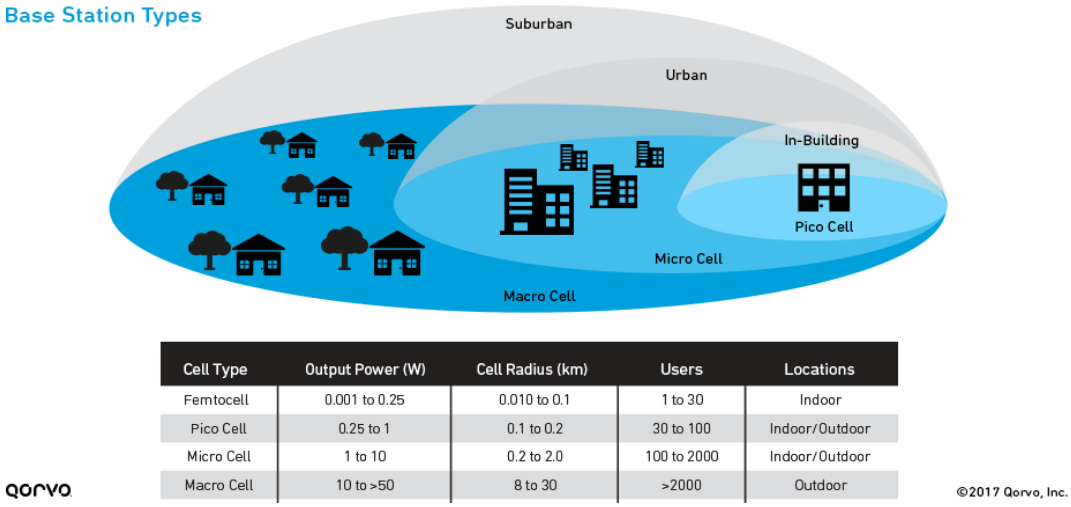
另外，更高頻段的信號其指向性也高，比過往更容易遭受建物阻隔，為了避免覆蓋死角問題，也必須增設基地台，同樣會增加布建成本。為了降低建置與營運成本，故 5G 允許用一般伺服器搭配軟體方式實現，允許用切片方式以便更加善用頻譜資源，同時也支援新應用，另外也提出中繼器(relay)降低成本，以及後續考慮高空平台、衛星化等，均是為了降低成本，以及後續考慮高空平台、衛星化等，均是為了降低成本。除了技術外，業者營運策略也開始改變，例如 2019 年臺灣大哥大拋出共網、共頻、共建主張，而行動通訊設備大廠瑞典 Ericsson 也表示 5G 網路可以共享，技術上沒有問題，但癥結將在於商業模式。

從 5G 的推動上，可以觀察到電信營運商在資安所面臨的問題，國家通訊傳播委員會(National Communications Commission, NCC)指出干擾將是設置專網很重要的資安疑慮，專網的網路架構除了可連接雲端，因此就有許多網路營運管理的問題，值得注意可能帶來的資安威脅及風險，如果有心人特意干擾電信營運商的專網，對於正常運作就會造成不小的損失。使用無線頻譜資源建置網路，依法電信商需提出資通安全計畫，在企業專網管理辦法中，企業也不例外。因此 NCC 要求設置自用網路者如為上市、上

櫃公司，需提出資通安全維護計畫經主管機關審核，維護計畫需包括資通安全的目標及維護範圍、專責組織、風險評估、防護及控制措施、安全事件通報機制等，如果非上市櫃公司，亦要檢具資通安全維護計畫供主管機關備查。而到了 6G 環境，營運商需要注意兩大類資安議題，其一是網路的安全訪問，確保 UE 端能夠安全的認證和接入網路（包含 3GPP 接入和非 3GPP 接入），並防止對頻段接口的攻擊；其二是確保網絡節點能夠安全交換，特別是保護「控制訊令資料(signalling data)」、「用戶資料(user plane data)」，確保負責 Packet 的路由以及轉發，讓 UE 能夠通到外部網路。

2. 設備商角度

與 4G 相比 5G 設備已更為開放，包含天線、基頻模組(Baseband Unit, BBU)、遠程無線電頭(Remote Radio Unit, RRU)、核網等各環節均傾向更彈性拆解、更開放選擇，估計 6G 也將維持開放態度，同時因為基地台的小型化，亦即 Small Cell 趨勢，過往 macro 型基地台適合大面積覆蓋，而今更重視彌補死角或室內使用的基地台，如 micro 型、pico 型、femto 型的基地台，詳如圖 86：



Cell Type	Output Power (W)	Cell Radius (km)	Users	Locations
Femtocell	0.001 to 0.25	0.010 to 0.1	1 to 30	Indoor
Pico Cell	0.25 to 1	0.1 to 0.2	30 to 100	Indoor/Outdoor
Micro Cell	1 to 10	0.2 to 2.0	100 to 2000	Indoor/Outdoor
Macro Cell	10 to >50	8 to 30	>2000	Outdoor

qorvo ©2017 Qorvo, Inc.

圖86、不同覆蓋範疇的基地台

資料來源：Qorvo

開放化、小型化對我國網通產業而言為機會，過往我國網通產業已在 Wi-Fi、WiMAX 領域累積技術能力與經驗，此可大程度沿用至 5G 乃至未來 6G 領域。

設備商要注意的是如何在 6G 環境中取得設備的認證，在設備身分管理部分，專網在使用者端是利用 SIM 或 eSIM 認證終端設備 5G 接取的使用權，一旦 SIM 卡被抽出，使用在陌生的設備就可能造成安全問題，因此除了 SIM 卡認證，也要對終端設備進行認證，避免非授權設備透過 SIM 卡連至 5G 專網。進一步則要強化專網的接取安全，因此要對終端設備上的應用、邊緣運算上的應用進行認證，同時要一對一綁定，達到終端設備上的某項應用，只能接收邊緣運算伺服器某項應用的指令，才能確保未通過認證的終端設備連到不該連的邊緣運算伺服器及應用。

3. 應用服務商角度

目前應用服務商多與電信營運商保持「既競且合」的態度，例如臺灣大哥大既有自己的 MyVideo 同時也合作推廣 Disney+，多數應用服務商傾向不帶有通訊通路的綁限性，而是允許用戶自由使用各種通訊網路、各種裝置，既可以有線上網觀看影片也可以無線上網觀看影片，既可以用電腦觀看影片，也可以用平板、手機觀看影片。

應用服務商須關注的是應用服務安全(Application domain security)，確保用戶應用軟體和供應商應用服務能夠安全地交換資料，另一個需注意的是服務架構的安全性(Service-based architecture security)，確保服務的網路功能能夠在服務網域和其他域內安全的通訊，例如網絡功能註冊、查詢等。

4. 生態利益相關組成者

除了應用生態外，與 6G 系統對應的防護系統也有其生態性，包含公部門、國際規範組織，進一步的則有設備製造商、應用開發商，甚至包含 6G 晶片、硬體與電子元件、手機製造商和網路設備供應商、網路營運商，以及提供邊緣無線設備、雲端計算服務、資料中心服務等成員。另外，資安業者與鑑識檢測服務商也

在整體生態中具有角色與份量，詳見圖 87：

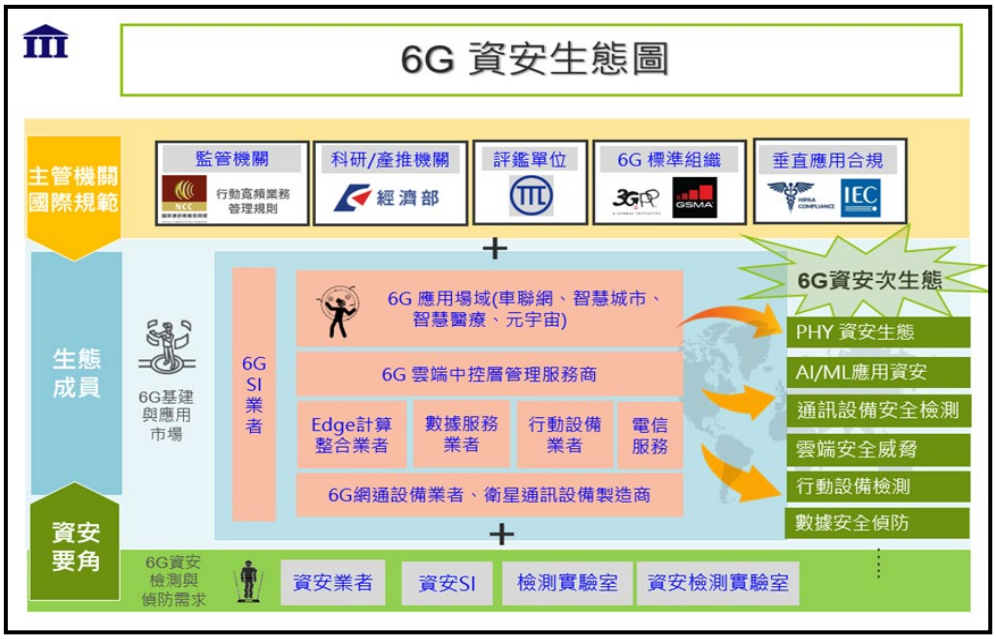


圖87、6G 資安生態圖

資料來源：本計畫整理

生態可進一步分成兩種情境，一是機構或企業使用的專網，另一則是直接服務消費大眾的公網，公網的生態成員如電信服務商(或稱電信營運商)、系統整合商、軟硬體設備商，或者是核網業者、資安服務業者等。與此配套的還有相關的資安服務，例如資安檢測服務、顧問服務，例如建置上的顧問、資安方面的顧問，而檢測則有基地台(或稱基站)的檢測、相關晶片的檢測。

另外，流量的監控也不可或缺，包含偵測出惡意流量而加以監視、阻斷，或者有分散式阻斷服務攻擊時能夠加以緩解等，詳如圖 88：

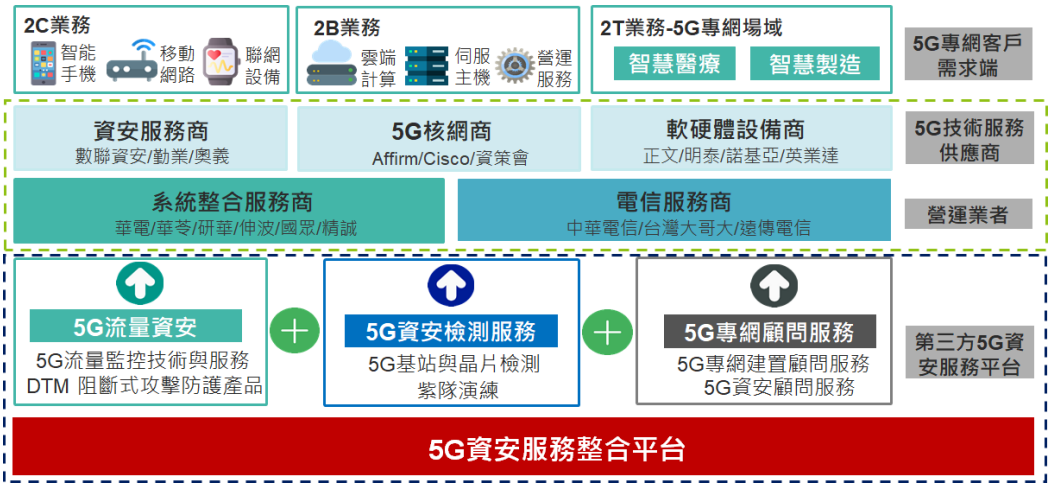


圖88、5G/6G 專網資安生態圖

資料來源：本計畫整理

至於公網的 5G、6G 的資安防護生態也包含諸多成員在內，以上游而言有威脅情資業者、晶片資安業者、新創團隊、外商等，而透過第三方服務平台進行聚合後，則連續下游相關產業，例如檢測顧問、系統整合、營運商、雲端業者、通訊設備商等。另外相關法規標準也在生態範疇內，例如：數位發展部資通安全署、電信監管單位國家通訊傳播委員會、資通訊標準訂立的 TAICS，以及各種公協會。同時資安卓越中心(Cyber Security Center of Excellence, CCoE)、技術服務中心、電信技術中心，或科技法律中心等政策幕僚智庫也同樣在列，如圖 89：

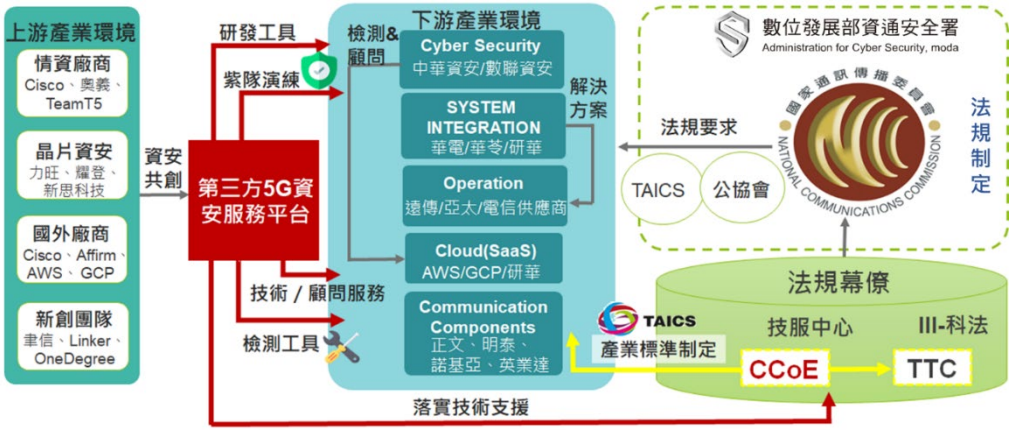


圖89、5G/6G 公網資安生態圖

資料來源：本計畫整理

5. 生態業者營運應用情境探索

藉由 6G 跨領域生態業者合作，可創造出更多應用情境，列舉如下：

(1) Everyday Living：6G 應用將有助於提高日常生活品質

A. 隨著無處不在的感測器和智慧網路結構的能力增強，人類作為 6G 服務的最終用戶，有望通過環境智能在居住環境中或旅行時從提高普通生活品質中獲益。

B. 服務機器人可以提供醫療保健、護理、室內/本地送貨服務和智能出行輔助。

C. 隨著全球人口老齡化趨勢，支持社會日常生活所需的勞動力將變得更加突出。

D. 聯合國《世界人口老齡化》：歐洲/北美老年撫養比最高，每 100 名工作人口(20-64 歲)/30 名老年人(>65 歲)。預計到

2050 年將提升至 49 名，智慧護理需求日益增長，巨大市場潛力和商機。

(2) Experience：動態和擴展的 6G 應用將改善客戶體驗和技術介面。

A. 預計增強功能將擴展人類與設備的互動，從語音助手到服務機器人，以及提供豐富的沉浸式虛擬/增強/混合現實 (VR/AR/MR) 體驗的系統。

B. 針對 MR 娛樂、人機交互、醫療保健輔助、具有物理交互的即時互動遊戲、由 MR 內容驅動的教室及機器人技術和增強 XR 的定位領域的服務為基礎的應用。

(3) Critical roles：醫療保健、製造、農業、交通和公共安全等關鍵領域

A. 運用機器人技術提高醫療保健、製造、農業和公共安全領域及其周圍技術品質。

B. 由 6G 技術、網路和應用程序驅動的自主機器人被設想為與人類互動，以提高生產力並維持基本操作。這些應用程序可能使用數位分身，其中人類與數位空間中的機器人自然交互以在現實世界執行動作或任務，例如遠程手術、治

療和監控等。

(4) Societal goals：實現高層次的社會目標並提高公共安全

A. 聯合國永續發展議程列出 2030 年希望實現的 17 個目標 - 社會、環境和經濟。

圖90、聯合國提供為社會價值之永續發展框架

資料來源：歐盟 5G-PPP，本計畫整理

B. 6G 可為社會和經濟提供應用程式和服務關鍵價值。例如數位公平(成本效率、可負擔性、存取和社會可持續性)，預計 6G 應用將提高意識和協作，同時將服務擴展到偏遠地區或數位隔離的人群。

C. 預計 6G 將建立符合保護地球生態之創新應用，減少二氧化碳排放並提高能源效率。超長壽命電池、零數據零能源設備和自供電感測器等。

(三) 閉門座談會

因應未來整體 6G 資安產業生態推動，希冀從政策面、技術面、應用服務面以及產業生態面等構面進行進一步縝密以及深度產官學研各方的深度回饋，更有效地與相關專家學者進行意見交流以及共識探討，以期將活動所蒐集之回饋意見進行整理解析，做為未來計畫執行推動以及策略藍圖規劃之參考依據。因此修訂原有 2 場座談活動，改為舉辦 4 場座談活動，從政策面、技術面、應用服務面以及產業生態面進行活動規劃，以下即為本計畫執行迄今之活動相關紀錄以及回饋意見彙整：

1. 第一場專家座談會

(1) 活動名稱：6G 座談會 I

(2) 活動時間：民國111年09月14日(三)，下午1：30-5：00

(3) 活動地點：台北市松山區民生科服大樓_14樓第一會議室

(4) 活動方式：實體會議

(5) 活動議程：如下表所示

表24、6G 座談會 I 議程表

時間	主題	主講人/專家學者
13:30~14:00	報到/簽到	-
14:00~14:20	主席開場致詞 議題：6G 產業發展概況	張 O 村總監
14:20~15:20	6G 主題討論與意見交流	專家學者
15:20~15:30	中場休息	-

時間	主題	主講人/專家學者
15:30~16:30	6G 主題討論與意見交流	專家學者
16:30~16:40	會議總結	張 O 村總監

資料來源：計畫整理(111/09)

(6) 討論議題：

A. 議題一：目前5G 通訊設備的技術應用是否有待解決議題，以及對6G 技術的展望？

B. 議題二：目前國內外物聯網在5G 的應用下之發展現況與6G 期望突破的點

C. 議題三：在未來6G 應用情境下，通訊設備與物聯網期望如何結合運用，產業進入市場的利基點

(7) 與會專家：如下表所示

表25、6G 座談會 I 與會專家名單

編號	姓名	服務單位	職稱
1	張 O 昌	中華民國資訊經理人協會	理事長
2	鄧 O 來	SGS 無線通訊實驗室	協理
3	黃 O 男	臺灣電信產業發展協會	監事
4	詹 O 宗	中央研究院	主任
5	陳 O 宏	臺灣醫學資訊學會	會員代表
6	賴 O 宏	MIH 聯盟	SIG 會員代表

資料來源：計畫整理(111/09)

(8) 會議結論

A. 議題一：

a. 因 6G 技術無可避免會依 3GPP 所制定的核心規範來運作，若要爭取先機，必須先加入相關工作小組，進而提出貢獻，以期能領導規格制定。

b. 在萬物聯網的 6G 時代，建議應以民眾有感的民生應用及產品層面切入資安議題，而非 5G 以前從技術方向來入手，過去 5G 是以產業需要推動資安，未來 6G 應是以社會應用服務需求來做推動。

c. 6G 是延續 5G 具高速穩定低延遲，再加上廣域通訊含 NTN，牽涉更廣更複雜，資安的影響面更大，事前的防範及驗證將是關鍵。

d. 在 6G 的應用情境上分成三層，第一層網路層應注重晶片的資安，AI Edge intelligence、Open RAN、Open source 資安的檢測；第二層是網管，Intelligent Network management，必須防駭客入侵；第三層是應用，特別注意定位系統、國安相關的系統、自駕車系統、無人機系統、機器人等應用，而此類的應用，資料都須作為後續

AI 處理的基礎，因此資料收集、轉換、儲存及使用都應處理好資安議題。

e. 先應國內產業發展、服務內容開始首先推動：電動車、自駕車、智慧製造、智慧醫療，並發展零信任，保護隱私，量子運算和網路基本理論或可先了解，但不宜先投入實體資源。

B. 議題二：

a. 期望像資策會等法人單位能整合國內產業力量，將學界研究落實到製造及機器人、醫療、自駕車等領域。

b. 資安牽涉範圍廣且需公信力，資策會是公設法人，除帶引領防範外，可進行準公權力的檢測或驗證。

c. 民生公共互連網的基礎建設，應該是 6G 資安優先考慮研發的目標。

d. 未來 6G 的發展，針對公眾網路的資安防護方面，相關業者應會尋求供應商提供相應的解決方案，而在專網部分的資安防護，相關業者皆不是通訊專長，此部分可作為法人未來推動重點。

C. 議題三：

a. 宜有上位階的機構協調各部會的資安生態之縱向及橫向聯繫，可由醫療、工業機械先下手。

b. 先遵從國際 ITU 上位政策來訂定 6G 資安的政策依據。社會目標：滿足聯合國永續發展目標(Sustainable Development Goals, SDGs)，並可以 SDGs 來梳理計畫框架。市場期許：支援新型態服務應用類型。 運作的必要性：如何實現新技術的複雜性。

c. 盤點出 6G 資安必須規劃之項目，擬定相關的政策建議，並放入今年計畫之結案報告中。

d. 建議未來可以往 Nature AI 的方向建置未來 4 年的方向。

圖91、專家學者進行6G 座談會 I 相關議題討論

資料來源：本計畫整理

2. 第二場專家座談會

(1) 活動名稱：6G 座談會 II

(2) 活動時間：民國111年10月14日(四)，下午1：30~5：00

(3) 活動地點：台北市松山區民生科服大樓_14樓第一會議室

(4) 活動方式：實體會議

(5) 活動議程：如下表所示

表26、6G 座談會 II 會議程表

時間	主題	主講人/專家學者
13:30~14:00	報到/簽到	-
14:00~14:20	主席開場致詞 議題：6G 產業發展概況	張 O 村總監
14:20~15:20	6G 資安標準	蔡 O 學講師
15:20~15:30	中場休息	-
15:30~16:30	6G 主題討論與意見交流	專家學者
16:30~16:40	會議總結	張 O 村總監

資料來源：計畫整理(111/10)

(6) 討論議題：

A. 議題一：目前5G 通訊設備的技術應用是否有待解決議題，以及對6G 技術的展望？

B. 議題二：目前5G 通訊設備的技術應用是否有待解決議題，以及對6G 技術的展望？

C. 議題三：在未來6G 應用情境下，通訊設備與物聯網期望如何結合運用，產業進入市場的利基點。

(7) 與會專家：如下表所示

表27、6G 座談會 II 與會專家名單

編號	姓名	服務單位	職稱
1	李 O 益	中國無線電協進會	理事長
2	溫 O 瑜	國家通訊傳播委員會	處長
3	杜 O 國	工業技術研究院 資訊與通訊研究所	前組長
4	郭 O 敏	軟鑄國際股份有限公司	執行長
5	葉 O 勝	中華電信數據通分公司	前處長
6	張 O 安	臺灣資料科學股份有限公司	研發副總
7	賴 O 輝	邊信聯科技股份有限公司	總經理
8	徐 O 東	乒乓話網股份有限公司	董事長
9	王 O 煥	宇通物聯股份有限公司	顧問
10	龔 O 雲	昱鑫智慧科技有限公司	執行長
11	簡 O 康	鴻齡科技股份有限公司	總監
12	杜 O 賢	仁寶電腦	經理

資料來源：計畫整理(111/10)

(8) 會議結論

A. 議題一：

a. 我國應提早進行使用頻段之規劃。

b. 可搭配標檢局「5G 智慧桿系統技術規範」針對微型基地台建置進行推動。

c. 因應未來大量 AI 之應用，需提升電池的持久與動力。

d. 6G 因走向開放架構，導入 O-RAN 技術後多部設備的管理與認證需妥善規劃設計規範。

e. 目前5G 發展尚存在覆蓋侷限的問題，網路基礎建設布建困難與整體部署成本高。

B. 議題二：

a. 終端設備多為複合性的設備器材，且含有藍芽與 Wi-Fi 模組，此類設備測試及驗證時間冗長、費用較高，應該朝解除或降低管制。

b. 終端設備於設計時須考慮設置資安介面，以達到最基礎之資安控管。

c. 車聯網往往建置成本與效益不符，須思考如何下降成本並達到效益。

d. 物聯網將會與 AI/ML 進行高度整合，需加強 AI 模型對於資安的防護能力。

C. 議題三：

a. 通信業者須考量後續費率，提高個人使用意願，最大商機可能用於商業界的應用與軟硬體製造業者。

b. 透過國際合作打造低軌衛星產業鏈，像是半導體 IC 設計系統整合等。

c. 6G 目前在國內被定位為衛星固定，並建構在5G 的基礎上，未來可應用在垂直場域應用中，作為企業專網、跨領域或跨境物聯網的應用，感測器、網通設備等應該是產業的立基點。

圖92、專家學者進行6G 座談會 II 相關議題討論
資料來源：本計畫整理

3. 第三場專家座談會

(1) 活動名稱：6G 座談會 III

(2) 活動時間：民國111年11月10日(四)，下午1：30~5：00

(3) 活動地點：台北市松山區民生科服大樓_14樓第一會議室

(4) 活動方式：實體會議

(5) 活動議程：如下表所示

表28、6G 座談會 III 會議程表

時間	主題	主講人/專家學者
13:30~14:00	報到/簽到	-
14:00~14:20	主席開場致詞	張 O 村總監
14:20~15:20	6G 資安簡介	張 O 村總監
15:20~15:30	中場休息	-
15:30~16:30	6G 主題討論與意見交流	與會專家學者
16:30~16:40	會議總結	張 O 村總監

資料來源：計畫整理(111/11)

(6) 討論議題：

A. 議題一：探討目前國內外5G 應用情境下所面臨的資安議題與解決方案，並衍生到6G 應用時會發生的資安議題有哪些？

B. 議題二：未來6G 資安產業需要突破之資安困境有哪些，以及建議解決做法？

C. 議題三：資安業者對於6G 資安市場之商機，如何針對6G 資安產業進行相關規劃作法與需要投入資源有哪些？

D. 議題四：就現有4G/5G 發展所觀察與實務經驗，目前6G 資安產業發展與推動對於法人扮演的角色有無想法與建議？

(7) 與會專家：如下表所示

表29、6G 座談會 III 與會專家名單

編號	姓名	服務單位	職稱
1	梁 O 先	華苓科技	董事長
2	賴 O 州	椰棗科技(TMRTEK)	副總
3	張 O 綾	FORESCOUT	總經理
4	傅 O 方	喬立成資安股份有限公司	資安長
5	黃 O 寧	創泓科技	董事長
6	藍 O 彥	美商帕洛爾托網路有限公司	資安顧問
7	廖 O 強	士欣資訊管理股份有限公司	總經理
8	張 O 智	台中市電腦公會總幹事	總幹事
9	張 O 峰	台中市電腦公會副總幹事	副總幹事
10	褚 O 敏	邁達特產品經理	經理
11	蔡 O 俊	國眾電腦	經理
12	宋 O 文	木弈勝網路國際	總經理

資料來源：計畫整理(111/11)

(8) 會議結論

A. 議題一：

a. 5G 是特定場域應用，6G 會比較偏向全域應用，建議注意終端、服務端的弱點改善。

b. 以前居多電信與網路詐騙，未來將重視虛擬、元宇宙詐騙問題等策略。

B. 議題二：

a. 扮演媒合角色，互補與融合產業資安供需。

b. 整合資安應用情境，提供資安發展示範，建立業者後續資安發展標竿。

c. 促進資安人培的教育養成。

C. 議題三：

a. 辨別 AI 虛擬人的真假、身分綁定、金流跟資產等資安議題。

b. 建立 AI 應用審核與法規指引。

c. 物聯網加密與隱私權的議題，應評估中間人對資訊攔截、攻擊、外洩，確保資料傳輸安全。

d. 設備隨著趨勢變小，如何組裝資安防禦模組，調整適當的網路防禦的架構與應用。

e. 6G 未來發展會安裝大量的感測器，及收集 AI 大量的學習分析資料，導致網路資安問題將可能轉變成實體上的傷害，建議開發前就應評估因應對策。

D. 議題四：

a. 6G 元宇宙沉浸式產業應用商機發展。

b. 6G 將會與衛星結合，超高頻寬、低延遲、突破地理限制，建議可往萬物聯網產業發展，如：智慧醫療、製造、交通、金融投入商機。

c. 建議6G 資安可往醫療業落實，同時協助醫療院所資安意識教育發展、平台與工具發展，讓經驗跟實務結合。

d. 未來網路部屬將去中心化，區塊鏈將使用 Web 3.0等技術發展，建議可從此著手投入資源。

圖93、專家學者進行6G 座談會 III 相關議題討論
資料來源：本計畫整理

4. 第四場專家座談會

(1) 活動名稱：6G 座談會 IV- 5G 到6G 關鍵技術資安布局

(2) 活動時間：民國111年12月2日(五)，下午1：30~5：00

(3) 活動地點:10364台北市大同區承德路二段239號6樓大會議室

(4) 活動方式：實體會議

(5) 活動議程：如下表所示

表30、6G 座談會 IV 會議程表

時間	主題	主講人/專家學者
13:30~14:00	報到 / 簽到	-
14:00~14:10	主席開場致詞	資策會 何 O 玲所長 中華軟協沈 O 延理事長
14:10-14:30	演講：全球資訊安全發展趨勢與關鍵議題	國立臺灣大學 孫 O 麗教授
14:30~14:50	6G 應用場景與資安關鍵技術探索(議題引言)	資策會資安所 徐 O 真
14:50~16:20	專家議題討論與經驗交流	與會專家學者
16:20~16:30	總結	資策會 張 O 村總監
16:30	賦歸	

資料來源：計畫整理(111/11)

(6) 討論議題：

A. 議題一：目前5G 通訊設備的技術應用是否有待解決議題，以及對6G 技術的展望？

B. 議題二：目前5G 通訊設備的技術應用是否有待解決議題，以及對6G 技術的展望？

C. 議題三：在未來6G 應用情境下，通訊設備與物聯網期望如何結合運用，產業進入市場的利基點。

(7) 與會專家：如下表所示

表31、6G 座談會 IV 與會專家名單

編號	姓名	服務單位	職稱
1	洪 O 峰	台達電子工業股份有限公司	副理
2	王 O 富	中華電信股份有限公司	科長
3	劉 O 立	臺灣經濟研究院	所長
4	劉 O 寧	臺灣經濟研究院	資安組組長
5	吳 O 明	和平整合公司	顧問

編號	姓名	服務單位	職稱
6	胡 O 武	東元電機股份有限公司	特別助理
7	李 O 彬	東豐科技股份有限公司	技術長
8	呂 O 錦	國立陽明交通大學	榮譽教授
9	張 O 玲	神盾股份有限公司	副總經理
10	汪 O 珍	越世實業股份有限公司	董事長
11	林 O 堂	財團法人電信技術中心	執行長
12	李 O 財	中央研究院	院士
13	陳 O 宏	臺灣大哥大	處長
14	沈 O 延	中華民國資訊軟體協會	理事長
15	喻 O 貞	中華民國資訊軟體協會	副秘書長
16	孫 O 麗	臺灣大學	教授

資料來源：計畫整理(111/12)

(8) 會議結論

A. 議題一：

a. 5G 垂直場域的應用為發展重點，6G 則應具備全覆蓋、自主智慧化、節能環保發展，建議藉此投入相應資源。

b. 5G 重要功能如 TSN 和 Network Slicing 的可行性應該早日實現，並建設企業專網成功案例，未來將具有成長性發展的專網建設費用降低，其中 O-RAN 的成熟度為關鍵。

c. 6G 將兼具演進和變革，預期將往降低成本和重視新興應用，為投入與發展重點。

B. 議題二：

a. 可朝向 AI、IoT、大數據、無人機、機器人、自駕車、3D 通訊(衛星、地面、海底)等應用發展。

b. 著重於低軌衛星供應鏈檢核與安控措施、資安防護方向著手，包含網路監控、端點系統監控。

c. 結合政府、公協會、企業、使用者共同發建立產業應用 Eco-system。

d. 以特定領域金融等專網建立應用為優先實施方向。

e. 網路高頻發展，需建立共通語言，軟體重於硬體，制度重於技術。

C. 議題三：

a. 秉持零信任原則，除了技術資安開發與檢驗發展，產學人培也要同步推廣，而政府可扮演政策引導之角色。

b. 設備逐漸軟體化發展，軟體開發應遵循 SSDLC 概建立，包含檢驗驗證、獨立驗證及確認(Independent Verification & Validation, IV&V)機制及資安稽核制度標準。

c. 根據國際趨勢，評估 6G 標準與需求，規劃因應產業指引、法規，進而訂定國際通用標準。

d. 威脅在不斷演變，例如：量子時代(Years to Quantum, Y2Q)，量子計算可能帶來威嚇，煽客攻擊者攻擊手段，該注意因應與防護議題。

圖94、專家學者進行6G 座談會 IV 相關議題討論
資料來源：本計畫整理

5. 6G 問卷調查結果

(1) 問卷回收份數：21份。

(2) 問卷填答對象：通訊設備商、通訊相關法人單位、硬體製造商、軟體業、電子電纜業、SI 廠商、資安業者、電信相關產業等。

(3) 對6G 的了解程度：14%的廠商了解程度為中高；38%的廠商了解程度為中；14%的廠商了解程度為中低；34%的廠商了解程度為低。

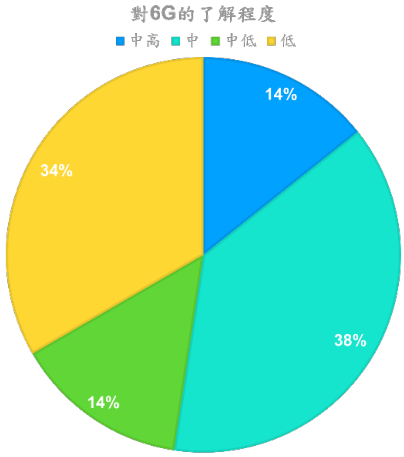


圖95、廠商對6G 的了解程度

資料來源：本計畫整理

(4) 廠商認知的6G 整理如下：

A. 為提供更快捷、跟智慧化且親民的網路，並可利用低軌衛星提供通訊。

B. 補足5G 問題，提高速率、效能，應用層面更加廣泛，並降低成本能讓科技世代產生巨大改變。

C. 實現完整物聯網與 AI 的基礎建設，透過布建緊密的高速網路能讓各端點搭配雲端運算的效能提高，高頻寬的特性也更適合應用於網路與實體世界的連結。

(5) 廠商目前對6G 最感興趣之應用項目如下：廠商有興趣之項目比例25%為極致的行動寬頻；24%為智慧城市與極致低能源網路；18%為全像通訊；9%為無人機為基礎的系統，詳如圖96：

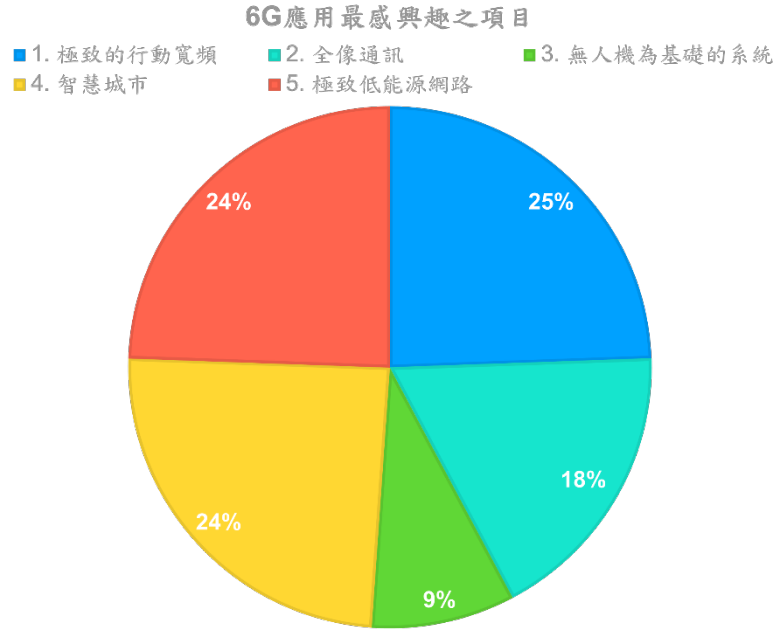


圖96、廠商對6G 最感興趣之項目

資料來源：本計畫整理

(6) 廠商認為目前對6G 領域影響最大之項目如下：廠商有興趣之項目比例25%為物聯網發展與智慧軌道系統;23%為AI；16%為工業4.0網路；11%為智慧醫療，詳如圖97：

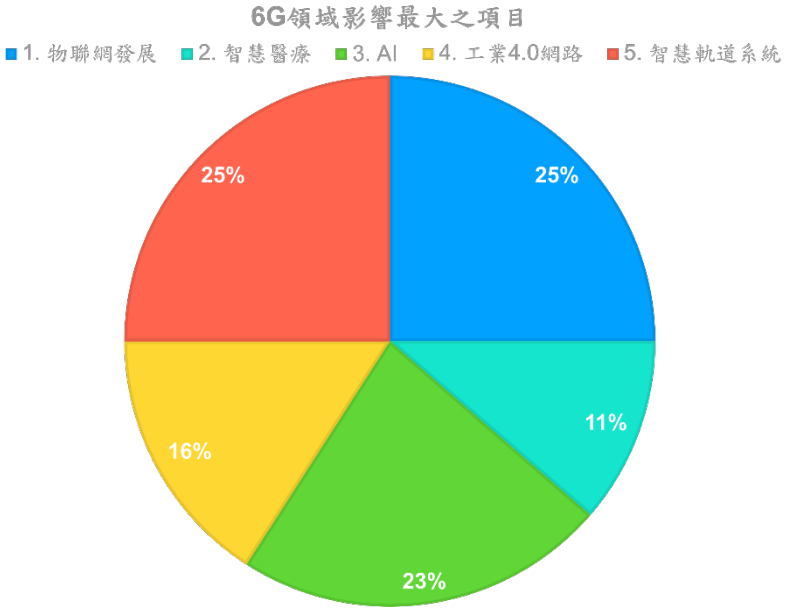


圖97、廠商認為6G 領域影響最大之項目

資料來源：本計畫整理

(7) 廠商目前投入6G 相關領域研究如圖98所示：25%的廠商目前有規劃投入，如 HEP 公司與 ARUBA 公司投入的網路產品相關整合因應；35%的廠商目前未規劃，將來考慮投入；40%的廠商無規劃投入。

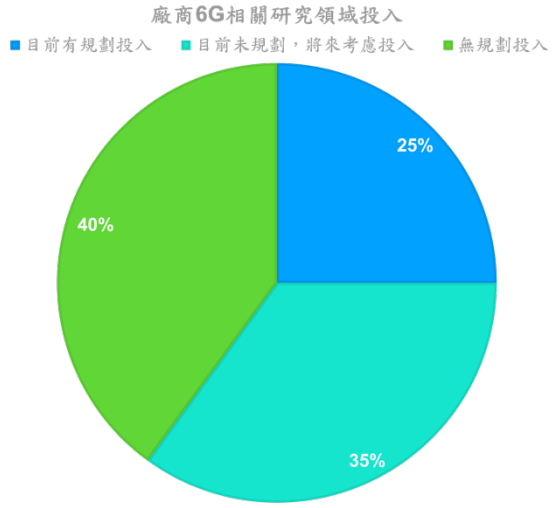


圖98、廠商對於6G 相關研究領域之投入
資料來源：本計畫整理

(8) 廠商認為我國6G 最大的限制為何統計如圖99所示：36%為國內基礎設施水平；25%為國家政策；21%為相關資費問題；18%為相關技術不夠成熟。

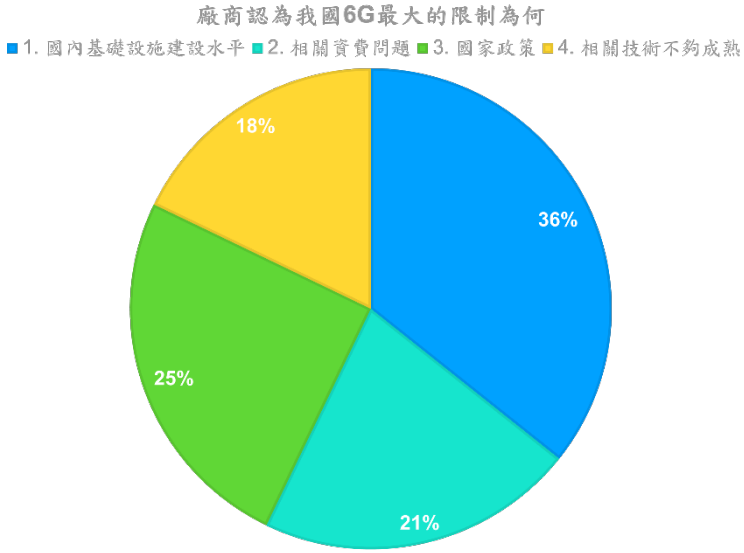


圖99、廠商認為我國6G 最大限制之項目
資料來源：本計畫整理

(9) 廠商認為我國從5G 應用延伸到6G 應用所面臨的困難點為何？是否有建議作法？

A. 目前法規尚不成熟，需要政府帶領制定政策，並提供補助。

B. 電信業者尚未回收投入的頻譜與建設投資、應用尚未有明確方向，民間基礎設施與國內的建設水平皆無明確方向。

C. 困難點可能會是6G 基地台的布建，由於6G 的頻寬較高，傳輸範圍會小於5G，因此相較於5G 來說6G 則需要布建密度更高的基地台，如此一來在基地台架設地點與架設成本將是未來要面臨的棘手問題。

D. 5G 尚未成熟，市場規模、商業模式，應該還沒讓現在投入的廠商獲得相對收益。

E. 雖然已有5G 技術，但應用上尚未普及。從5G 延伸到6G，需考慮到基地台建置成本及民眾升及到6G 的意願是否夠高。

F. 5G 的關鍵技術有多都是中國的華為所掌握，所以美國倍感威脅大力阻止，並投入6G 的開發。

(10) 6G 市場屬萌芽階段，臺灣極需先期投入不能缺席，因此若要與國際接軌，廠商認為首要解決的問題如下：

A. 需要政府帶領制定政策，並提供應用方向與規範的制定，需要政府政策投入與資金的投入。

B. 首要解決的應該是6G 相關人才培養，新技術發展的前期最為重要，若臺灣能在前期就展現相關技術能力，必能成為國際間發展6G 不可或缺的一份子。

C. 除了參加國際標準組織，投入先期研究外，先將5G 產業生態完備。

(11) 廠商對我國6G 生態應用發展之期待如下：

A. 希望可搶佔重要的關鍵專利。

B. 普及化物聯網的應用，讓各端點間的資料傳遞不再受限制，打造更便利的生活。

C. 投入研發，加速布建，而不是被動地等別人的成果。

(四) 研析成果

1. 研究規劃遵從國際3GPP 規劃

依據 3GPP 的規劃，2017 年通過的 R14 標準，2018 年通過的 R15 標準方為正式的 5G 行動通訊標準，而 2020 年通過的 R16 為標準的持續增修。3GPP 後續在 2020 年至 2025 年間進行 4 次版本的增修， R17～R20 稱為 B5G 標準，或有業界稱為 Pre-6G 標準，並以 2026 年的 R21 標準為正式 6G 標準，相關標準制訂時間規劃詳見圖 100：

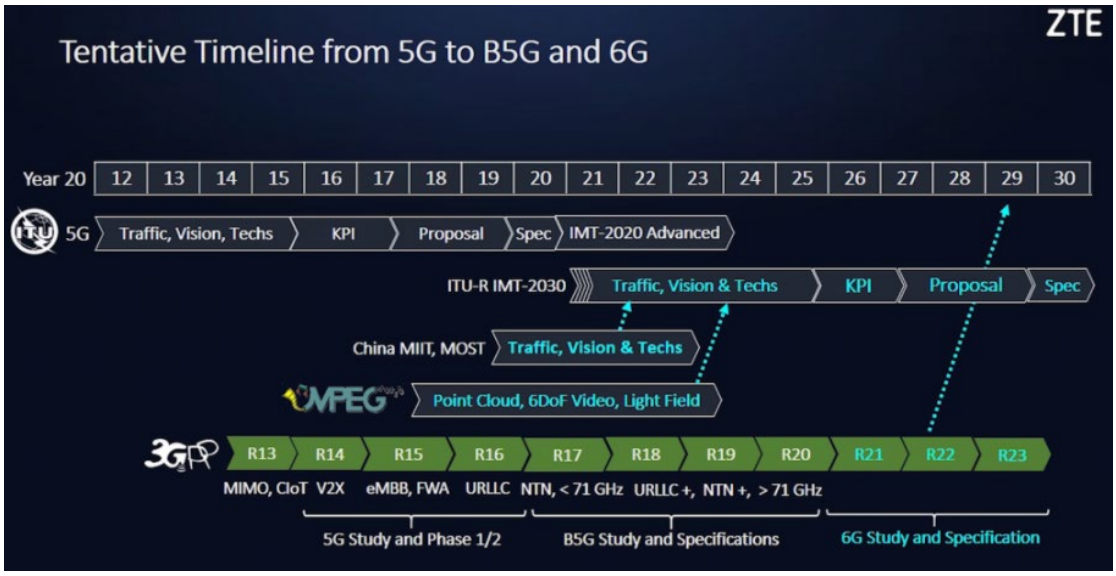


圖100、5G、B5G、6G 標準制訂規劃時間表
資料來源：6G Wireless Summit 2020 的 ZTE 主講內容

或業界對第一、第二階段另有設定，將 R15～R17 視為第一階段，而 R18～R20 為第二階段，第一階段為 5G，第二階段稱為 5.5G 或 5G-Advanced。無論認定為何，業界共識上均將 2026 年將通過的 R21 標準視為正式的 6G 通訊準則，而後進行約 1、2 年的試行，預計於 2028 年能正式商業化營運，部分專案機構(如 Hexa-X、6G Flagship)則預估至 2030 年方可能商業營運。

2. 6G 應用可能發展創新技術

依據前述，以 3GPP 的規劃時程為設定可展開 4 年的探索研究，即 112 年為 R18 標準，113 年為 R19 標準，114 年為 R20 標準，115 年為 R21 標準。

而在探索上，以標準內的重點技術為依據進行展開，例如 R18 將在不同層次的網路中引入機器學習技術，或持續精進邊緣運算設計，或在移動載具上建立通訊中繼站點。

另也包含低功耗、高精度的工業物聯網應用，或進一步強化在 5G 標準時確立的網路切片技術，以及讓 5G 網路能以衛星通訊做為其回程(backhaul)通訊等。

而 R19、R20 標準預計將強化 URLLC 標準、強化非地面通訊 NTN 技術，實現同頻全雙工(In-Band Full Duplex)，以及在控制平面與用戶平面的上層使用人工智慧技術加以融合。

R21 將有機會引入 500GHz～1THz 波段的運用，感測器節點方面將能夠支援能源收割、無電池運作、無線供電，此與公用事業的智慧抄錶高度關連。

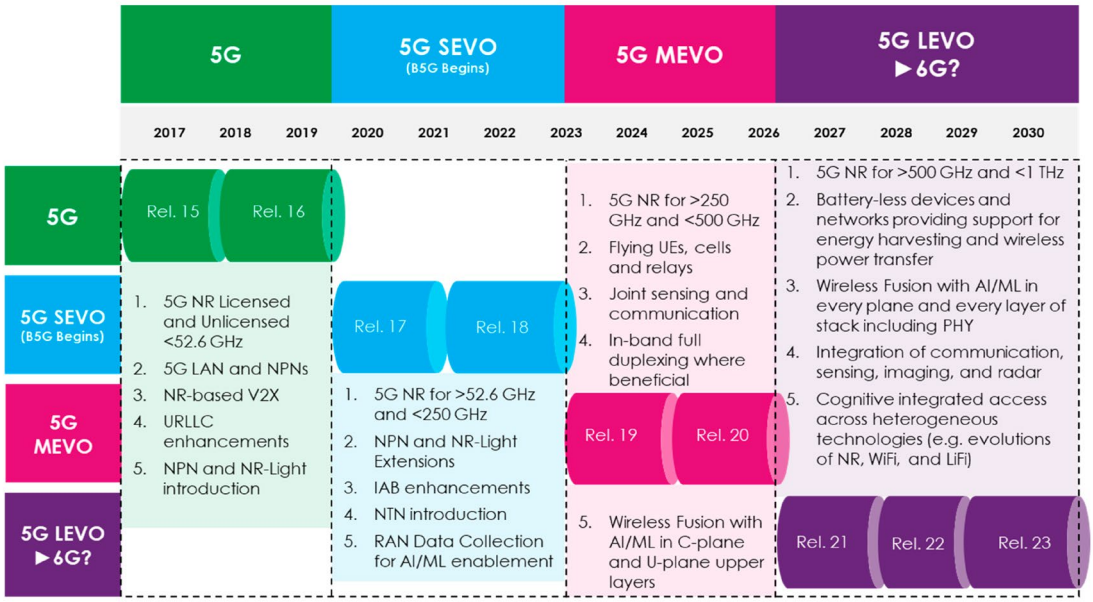


圖101、5G 演進至6G 的技術展望規劃圖
資料來源：Electronics 2020

3. 6G 發展衍生典範轉移

以上述技術提案可探索其相關生態，例如衛星通訊可能取代現行衛星新聞轉播(Satellite News Gathering, SNG)車輛通訊，未來新聞電視台將成為 6G 整體生態中的一環，而不再是自成一套、與行動通訊無關的通訊體制。

其他潛在引入的技術也包含 DLT 技術，如此也將會與區塊鏈、數位加密貨幣、金融科技等生態關連，而與此相關的資安防護也將具有生態特性。

4. 專家座談相關建議綜整：透過本計畫辦理的產官學專家會議，相關建議綜整如下

(1) 臺灣 6G 應用情境未來發展方向分成三層

A. 晶片資安：AI Edge intelligence、Open RAN、Open source 資安的檢測。

B. 網路資安：Intelligent Network management，必須防駭客入侵。

C. 應用情境：特別注意朝向 AI、IoT、大數據、無人機、機器人、自駕車、3D 通訊(衛星、地面、海底)等應用。

(2) 與國內外產、學、研上層相關組織對接推動面：

A. 先遵從國際 ITU 3GPP 上位政策來訂定 6G 資安的政策。同時宜有上位階的機構協調各部會的資安生態之縱向及橫向聯繫，可由醫療、工業機械先下手。

B. 5G & Beyond 行動數位網路，以及企業數位轉型(變革整合至企業)，讓虛實整合支援更多商業活動，並串聯

所有人、事、物，讓資安議題具有更多更複雜面向，政府應加快著手建立相關防護措施。

C. 網路高頻度發展，需建立共通語言，軟體重於硬體，制度重於技術，並如何透過各方協力的機制下推動。從生態推動的角度下應協助產業界提供 easy-to-use 解決方案(如 119-call center)，有效協助託管安全服務提供商(Managed Security Service Provider, MSSP)業者在資安議題強化 供應鏈/關係企業/跨國公司 等合作協同關係。

D. 產業生態體系的建立與國際組織參與是非常重要，例如在線快速身分識別(Fast IDentity Online, FIDO)聯盟，PKI，Web3 security 等國際聯盟參與，以及國內對應組織(如臺灣資通標準協會 TC5 產業委員會)的投入，都是未來投入的重點。

E. 政府未來提供第三方 IV&V 認證，政府機構應有零信任機制，對公務員及民眾提供教育宣導、認知素養，以建立國家數位韌性及數位自主的信任產業。

(3) 6G 通訊/物聯網設備資安未來推動方向

A. 民生公共所需基礎建設的安全營運，應是 6G 資安優先考慮研發的目標。邊緣資安的防禦能力需與雲端核網資安整合作業，並有效考量 IT、運作技術(Operational Technology, OT)與 CT 間資安作法、思維以及切入定點的差異，需有客製化/權宜化作法，並具一定程度的資安防護能力。

B. 導入 O-RAN 技術後，多部設備的管理與認證需妥善規劃設計規範，以達成零信任的的基礎。同時終端設備於設計時須考慮設置資安介面，以達到最基礎之資安控管，需有安全系統發展生命週期(Secure Software Development Life Cycle, SSDLC)導入，提供產業具公信力檢驗測技術、工具以及機制，並提昇可信度/可靠度，開發商需有資安議題考量。

C. 因我國 ICT 產品為重點國際市場供應大宗，其中供應鏈產品安全最為重要，而在系統整合上大量運用開源軟硬體的風險與威脅亦需注重，因此諸如導入軟體物料清單(software bill of materials, SBOM)表及 Zero Trust 以

及所屬相關查驗，須優先導入設計規劃以及推動。

D. 6G 通訊推動與 ESG 與 SDGS 社會公益之合作推動：未各類應用需滿足聯合國永續發展目標，而 6G 環境下可透過專網及 AIoT 感測技術，有效監控管理政府企業等相關設施協助政府達到 ESG 零碳政策目標，支援新型態服務應用，於節能減碳及資安治理提供協助措施。

5. 盤點不同產業之應用生態與對應防護

在 6G 網路環境與應用情境下，其整體生態相關組成者，包括政府角色、國際規範組織、從設備製造商到應用開發商，包含 6G 晶片、硬體與電子元件、手機製造商和網路設備供應商、網路電信事業，以及提供邊緣無線設備、雲計算服務、數據中心服務等成員及資安業者與鑑識檢測角色，大致上可以在圖 102 中的 6G 產業鏈中進行解析與規劃各自互動的角色：

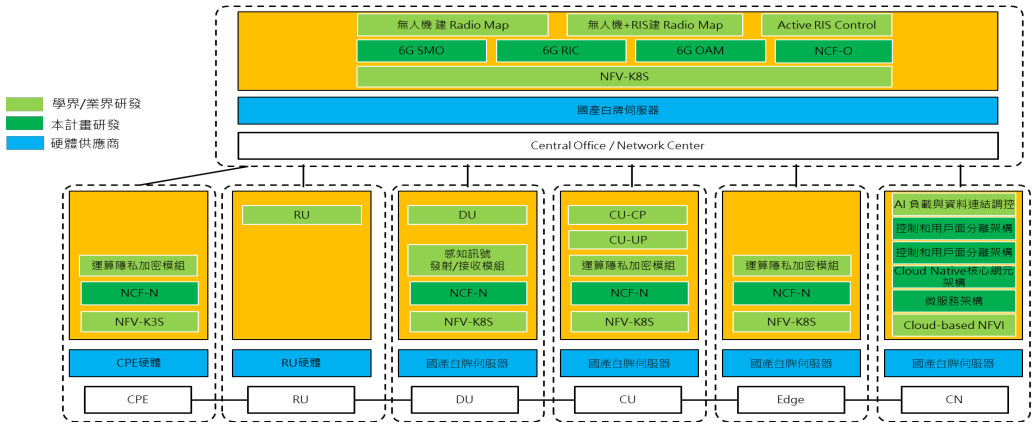


圖102、6G 網路區塊相關產業鏈

資料來源：TAICS，本計畫整理

從以上的 6G 網路區塊相關產業鏈，我國相關廠商可在白牌的伺服器及終端設備具備較多優勢，故先以以下幾項產品重點，來提出相關之資安議題，如表 32 所示：

表32、6G 網路區塊相關國內產業資安議題導入建議

國內相關產業	資安議題導入建議
6G 組網國產白牌伺服器	a. **需預先進行資安測試**：於 6G 網路伺服器設計時須考慮設置資安介面，以達到最基礎之資安控管，並於產品出廠以及布建之前需預先進行相關資安測試。 b. **需加強 AI 模型對於資安的防護能力**：由於 6G 網路與應用將會與 AI/ML 進行高度整合，網通設備營運管理相關系統，需加強 AI 模型對於資安的防護能力，以及對於 AI/ML 模型訓練間資料，並避免受到汙染與干擾。
6G 組網的終端設備	a. **應加強邊緣資安防禦能力**：需與雲端核網資安整合作業，應考量 IT 與 OT 終端設備資安作法之不同，應有客製化/權宜化作法，並具一定程度的資安防護能力。 b. **設置資安介面**：端設備於設計時須考慮設置資安介面，以達到最基礎之資安控管，需有 SSDLC 導入，提供產業具公信力檢驗測技術，工具以及機制。 c. **導入相關查驗機制**：ICT 終端設備產品中，供應鏈產品之安全最為重要，而開源軟硬體的風險與威脅需注重，應導入 SBOM 表，及 Zero Trust 以及所屬相關查驗。
6G 組網的應用場景技術落地推動工作	a. **國際組織合作**：透過與國際組織(如歐盟)合作、學界合作鏈結國際/國內電信業與基地台廠商，並透過廠商合作展示具資安防護功能之6G E2E 雛型系統打入國內外市場。 b. **系統整合商加值導入資安機制**：未來國內廠商可預期陸續完成6G 環境所需之智慧表面技術(Reconfigurable Intelligent Surface, RIS)產品的

國內相關產業	資安議題導入建議
	設計研發，對應資安機制可協助系統整合商進行加值導入，進合發展對應具資安防護功能之6G智能組網與管理技術，以提供兼具低能耗、高效能以及高韌性的 RIS 架構網路解決方案。 c. **國際產學研合作**：因應未來相關國際網通組織將對應6G 技術列入技術白皮書，透過國際產學研合作，結合國內學界與業界合作展示6G 智慧化之分散式核心網路系統，尋求合作機會與實地 PoC 並打入市場，可及早與學界合作團隊一同爭取歐盟國際合作計畫，以產學研合作，進行具資安功能之6G 系統 PoC 展示，提早打國際市場。

資料來源：本計畫整理

七. 計畫執行情形-通訊整合增強型人工智慧協作設計與驗證

5G 無線通訊網路從2020年開始在全球範圍內部署，其用戶數量已經達到非常大的規模，許多功能正在標準化過程中，例如大規模連接 mMTC、高傳輸頻寬 eMBB 和超可靠低延遲 uRLLC。由於不同類型的智慧裝置(如智慧手機/手錶/感測器等)數量快速增長，基於萬物互聯的智能服務預計將在未來獲得巨大的普及，像是工業 5.0、智慧城市、全息通訊、數位分身、遠距醫療、區塊鏈技術、虛擬實境以及無處不在的人工智慧等。這些新興應用已經突顯了現有5G 無線通訊網路的局限性，包含傳輸速率、延遲、可靠性、可用性、處理、連接密度和網路覆蓋等面向都將無法滿足2030年及以後的所有需求。在此背景下，促使繼續推動現有無

線通訊網路向下一代發展，即6G。目前，學術界和工業界正在努力建立基礎，以滿足未來網路布署的迫切需要。

近年來，移動設備配備了越來越先進的傳輸和計算能力，再加上深度學習的進步以及未來6G 的蓬勃發展，這為上述許多有意義的應用開闢了無數可能性。人們普遍認為，6G 將建立在無處不在的人工智慧的新願景之上，實現以異構和大規模網路中由資料驅動機器學習的解決方案。然而傳統以雲端為中心的機器學習服務是透過集中收集資料和訓練模型來實現，這種傳統的訓練技術包含兩個挑戰：(i)由於資料通訊量增加導致的高通訊和能源成本，(ii)資料集中會有隱私/機密洩漏的疑慮，帶給使用者隱私問題的困擾，而成為日常生活中大規模實施的瓶頸。

有鑑於這些限制，出現了一種新興技術，即聯合學習Federated Learning，將機器學習帶到無線網路的邊緣。聯合學習以分佈式方式訓練，並藉由伺服器協調全局來提取不同參與者資料的特點進而優化模型。由於聯合學習利用分散的資料集和參與者的計算資源來開發通用機器學習模型，將不會損害資料隱私。然而，在6G 大規模且複雜的移動網路中，涉及到具有不同條件的異構設備(heterogeneous devices)，這對大規模實施聯合學習的

通訊成本、資源分配以及隱私和安全提出了挑戰。目前已有很多研究提出在6G 通訊背景下進行聯合學習未解決的問題，並探討關鍵技術挑戰以及對應的聯合學習方法。

(一) 研析方法與過程

本報告先整理對6G 的技術需求指標 KPI 及相對應有潛力的技術，並總結代表性機構的6G 研究現況；其次介紹6G 中的關鍵技術-聯合學習，以及6G 通訊背景下可能的應用，並分析聯合學習在6G 通訊的需求下所遭遇的挑戰及解決方法，最後設計與規劃一實驗，說明如何改進聯合學習技術，解決 edge 端計算效能不足問題滿足6G 通訊的需求。

1. 國際標準與技術趨勢

為了支持 2030 年及以後的顛覆性應用，6G 系統將提供更高的頻寬、可靠性、效率等，原先用於評估5G 的 KPI 對 6G 仍然有效，而一些新的 KPI 將被引入用於評估新技術特性。表33整理關鍵需求的 KPI，並與5G 比較：

表33、6G 關鍵需求 KPI

KPI	Description	Requirements (v.s. 5G)
Peak data rate	每個用戶或設備在理想條件下可達到的最大數據速率，以 Gbit/s 表示	1 Tbit/s (20 Gbit/s)
User−experienced data rate	使用者有至少 95%的機率可以在任何時間或地點獲得此數據速率，以 Mbit/s 或 Gbit/s 表示	1 Gbit/s (100 Mbit/s)
Latency	從來源端發送一個數據封包至目的端接收所需的時間，以 ms 表示	0.1 ms (1 ms)
Mobility	在屬於不同的傳輸層和無線接取技術 (Multi-layer/Radio Access Technology, RAT)的無線節點間在被限定傳送 QoS 與無縫轉移下，可以實現的最快速度(以 km/h 表示)	1000 km/h (500 km/h)
Connection density	每單位面積的設備連接數和進行通道存取的總數，以 km^2 表示	$10^7/km^2$ ($10^6/km^2$)

資料來源：請參閱附錄-參考資料 1.4, 1.5, 1.7, 1.13, 1.14, 1.17, 1.18

✓ 1.4 J. R. Bhat and S. A. Alqahtani, "6G Ecosystem: Current Status and Future Perspective," IEEE Access, vol. 9, pp. 43134-43167, 2021.
✓ 1.5 A. L. Imoize, O. Adedeji, N. Tandiya and S. Shetty, "6G Enabled Smart Infrastructure for Sustainable Society: Opportunities, Challenges, and Research Roadmap," Sensors, vol. 21, 2021.
✓ 1.7 W. Jiang, B. Han, M. A. Habibi and H. D. Schotten, "The Road Towards 6G: A Comprehensive Survey," IEEE Open Journal of the Communications Society, vol. 2, pp. 334-366, 2021.
✓ 1.13 D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, D. Niyato, O. Dobre and H. V. Poor, "6G Internet of Things: A Comprehensive Survey," IEEE Internet of Things Journal, vol. 9, pp. 359-383, 2022.
✓ 1.14 S. K. Pattnaik, S. R. Samal, S. Bandopadhaya, K. Swain, S. Choudhury, J. K. Das, A. Mihovska and V. Poulkov, "Future Wireless Communication Technology towards 6G IoT: An Application-Based Analysis of IoT in Real-Time Location Monitoring of Employees Inside Underground Mines by Using BLE," Sensors, vol. 22, 2022.
✓ 1.17 Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis and P. Fan, "6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies," IEEE Vehicular Technology Magazine, vol. 14, pp. 28-41, 2019.
✓ 1.18X. You, C. X. Wang, J. Huang, X. Gao, Z. Zhang, M. Wang, Y. Huang, C. Zhang, Y. Jiang, J. Wang, M. Zhu, B. Sheng, D. Wang, Z. Pan, P. Zhu, Y. Yang, Z. Liu, P. Zhang, X. Tao, S. Li, Z. Chen, X. Ma, I. Chih-Lin, S. Han, K. Li, C. Pan, Z. Zheng, L. Hanzo, X. S. Shen, Y. J. Guo, Z. Ding, H. Haas, W. Tong, P. Zhu, G. Yang, J. Wang, E. G. Larsson, H. Q. Ngo, W. Hong, H. Wang, D. Hou, J. Chen, Z. Chen, Z. Hao, G. Y. Li, R. Tafazolli, Y. Gao, H. V. Poor, G. P. Fettweis and Y. C. Liang, "Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts," Science in China, Series F: Information Sciences, vol. 64, January 2021.

上述 KPI 需關鍵技術支持，如傳輸、網路溝通、AI 等將被開發並應用於 6G 系統。表34對關鍵技術進行分類，由表34可以發現6G 新的應用都將會跟 AI 有關，原因是將有大量資料來自個人且異質的網路，像是智慧手機、穿戴式裝置(如智慧手錶)、各式各樣的感測器(如監控攝影機、溫度/重量/壓力/震動感測器)等，透過這些做為人類與環境媒介的裝置所取得的資料(或訊號)，開發以人為中心理念的 AI，將會帶來更便利的生活；例如智慧照護可避免老人或小孩發生跌倒的危險；智慧醫療可更早檢測出病症提前治療；智慧交通可以規劃最佳路徑，減少塞車的問題；智慧工業可做出最佳排程減少人力的浪費。傳統中心化的機器學習方法不再適合，例如將資料集中在雲端訓練模型，會有隱私洩漏的疑慮，以及傳輸/訓練大量資料所需的成本。聯合學習將會是新的解決方案，下一章節將會有更詳細的介紹。

表34、6G 關鍵技術分類

Category	Technology
Spectrum	mmWave
	THz
	OWC(VLC)
	DSM
Networking	NFV & SDN
	RAN Slicing
	O-RAN

	Post-Quantum Security	
Air interface	Massive MIMO	
	IRS(RIS/SRE)	
	CoMP	
	New modulation	Intelligent OFDMA
		NOMA
Architecture	Large-scale LEO satellite constellation	
	HAP	
	UAV	
Paradigm	AI	Deep learning
		Federated learning
		Transfer learning
		AI as a service
	Block-chain	
	Digital twin	
	Edge intelligence	
	CoCoCo convergence	

資料來源：請參閱附錄-參考資料 1.2,1.3,1.5,1.6,1.7

✓ 1.2 M. Alsabah, M. A. Naser, B. M. Mahmmod, S. H. Abdulhussain, M. R. Eissa, A. Al-Baidhani, N. K. Noordin, S. M. Sait, K. A. Al-Utaibi and F. Hashim, "6G Wireless Communications Networks: A Comprehensive Survey," IEEE Access, vol. 9, pp. 148191-148243, 2021.
✓ 1.3 C. D. Alwis, A. Kalla, Q.-V. Pham, P. Kumar, K. Dev, W.-J. Hwang and M. Liyanage, "Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research," IEEE Open Journal of the Communications Society, vol. 2, pp. 836-886, 2021.
✓ 1.5 A. L. Imoize, O. Adedeji, N. Tandiya and S. Shetty, "6G Enabled Smart Infrastructure for Sustainable Society: Opportunities, Challenges, and Research Roadmap," Sensors, vol. 21, 2021.
✓ 1.6 W. Jiang and H. D. Schotten, "The KICK-OFF of 6G Research Worldwide: An Overview," in 2021 7th International Conference on Computer and Communications (ICCC), 2021.
✓ 1.7 W. Jiang, B. Han, M. A. Habibi and H. D. Schotten, "The Road Towards 6G: A Comprehensive Survey," IEEE Open Journal of the Communications Society, vol. 2, pp. 334-366, 2021.

2. 關鍵技術-聯合學習

在過去的十年中，機器學習及其應用得到了快速發展，特別是在深度神經網路 (Deep Neural Network)領域，然而通常需要大量的資料來訓練複雜任務的準確模型，例如影像分類和計算機視覺。由於資料隱私法規和傳輸頻寬的限制，將所有訓練資料集中傳輸至一個中心位置儲存和訓練通常是不可行的。Google 於2016年提出了聯合學習，是一種協作分散的隱私保護技術，用於克服數據孤島和數據敏感性(data silos and data sensibility)的挑戰。藉由讓所有參與者「合作式」訓練一個強大的模型，同時資料可以只存在參與者端，維持了資料的隱私性。近年來隨著隱私意識與法規的提升，聯合學習也受到了各大公司、研究機構的重視。另外，由於智能物聯網設備迅速普及，進而帶動相關應用，需要使用更有效率的機器學習來訓練模型。聯合學習能克服隱私洩漏的疑慮，並降低傳輸/訓練大量資料所需的成本，成為 IoT 應用的最佳方案。

聯合學習系統架構和訓練過程如圖103所示，分為以下4個步驟：

(1) Edge 端以 local data 訓練模型：參與者不用上傳資料到雲端，只要把資料存在自己裝置中並訓練模型(m)，且需儘可能降低訓練所需資源及時間(local computation energy and latency)

(2) Edge 端上傳訓練模型：訓練完後把跟資料無關的參數(如 model weight)上傳至雲端，且需儘可能降低上傳所需資源及時間(uplink transmission energy and latency)

(3) Cloud 端結合眾人的訓練結果產生新的訓練模型：伺服器(cloud server)統整各個參與者上傳的參數後，訓練一新的模型(M)其正確率能接近把所有參與者資料統整起來一起訓練的結果，且需儘可能降低訓練所需資源及時間(global computation energy and latency)

(4) Edge 端下載新的訓練模型:參與者從伺服器下載新的模型(M)，其正確率應高於原模型(m)，且需儘可能降低下載所需資源及時間(downlink transmission energy and latency)

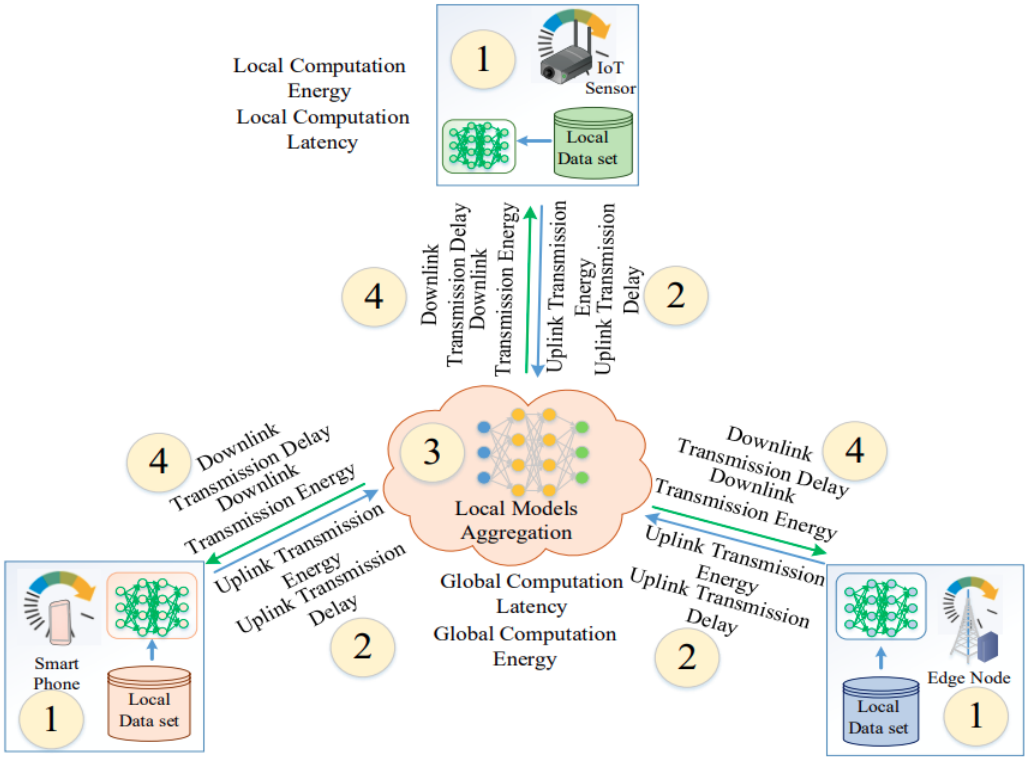


圖103、聯合學習系統架構和訓練過程

資料來源：請參閱附錄-參考資料 1.9, 1.26

根據資料的分佈特徵可將聯合學習分類如下：

(1) Horizontal Federated Learning：如圖104，每個參與者的資料有相同的特徵，而彼此之間比較少樣本重疊，可以讓每個參與者只上傳部分特徵的資料到雲端上依舊能訓練出一個好的模型。

✓ 1.9 L. U. Khan, S. R. Pandey, N. H. Tran, W. Saad, Z. Han, M. N. H. Nguyen and C. S. Hong, "Federated Learning for Edge Networks: Resource Optimization and Incentive Mechanism," IEEE Communications Magazine, vol. 58, pp. 88-93, 2020.
✓ 1.26 Q. Yang, Y. Liu, T. Chen and Y. Tong, "Federated Machine Learning: Concept and Applications," ACM Transactions on Intelligent Systems and Technology, vol. 10, pp. 1-19, January 2019.

(2) Vertical Federated Learning：如圖105，每個參與者的資料重複的特徵較少，但是重疊的樣本將含有該樣本接近全部的特徵，需要使用特徵加密的方法來保護參與者的隱私。

(3) Federated Transfer Learning：如圖106，參與者的資料彼此的特徵跟樣本都重疊較少，此類型將會提高訓練的難度，但若能達成則能同時保障隱私且提升模型準確率。

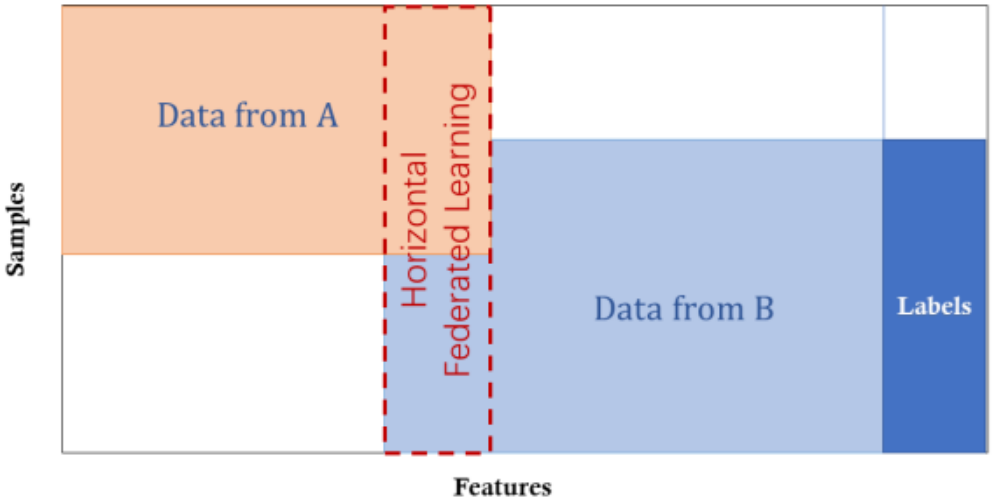


圖104、Horizontal Federated Learning

資料來源：請參閱附錄-參考資料 1.26

✓ 1.26 Q. Yang, Y. Liu, T. Chen and Y. Tong, "Federated Machine Learning: Concept and Applications," ACM Transactions on Intelligent Systems and Technology, vol. 10, pp. 1-19, January 2019.

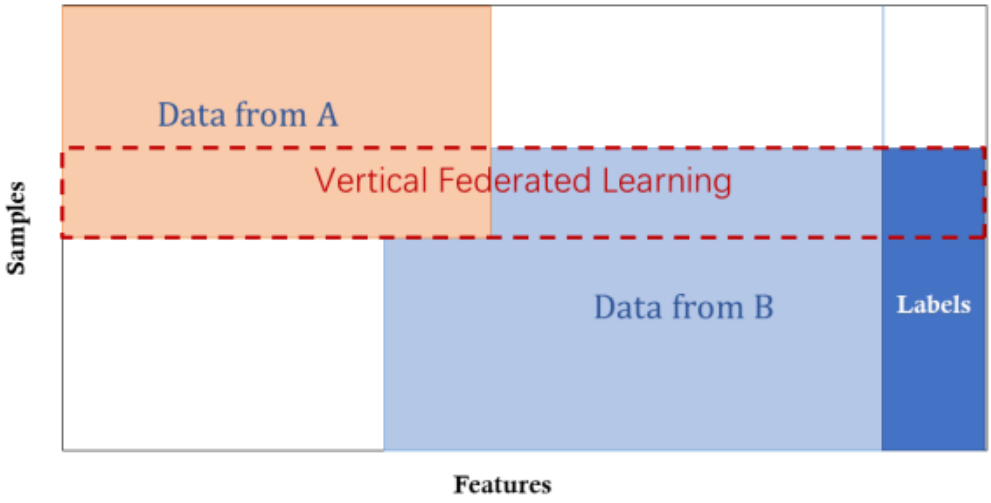


圖105、Vertical Federated Learning
資料來源：請參閱附錄-參考資料 1.26

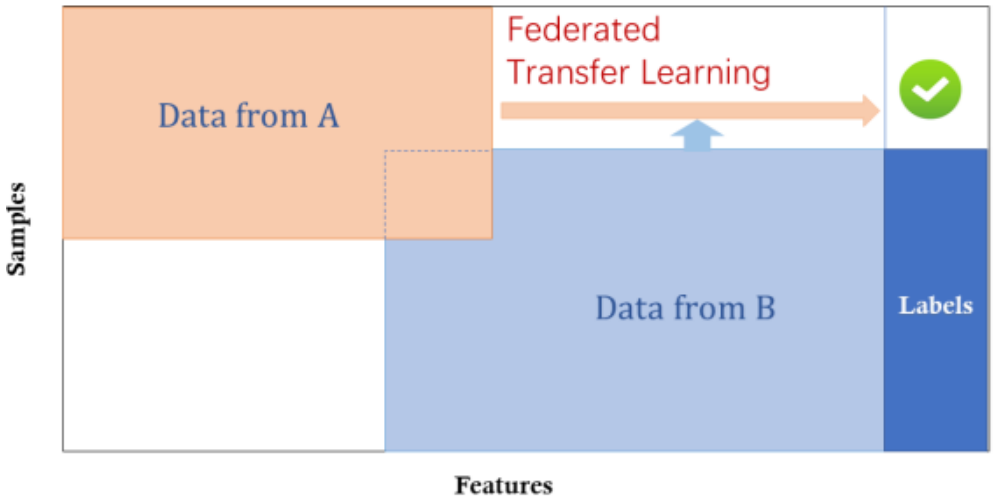


圖106、Federated Transfer Learning
資料來源：請參閱附錄-參考資料 1.26

✓ 1.26 Q. Yang, Y. Liu, T. Chen and Y. Tong, "Federated Machine Learning: Concept and Applications," ACM Transactions on Intelligent Systems and Technology, vol. 10, pp. 1-19, January 2019.

3. 新服務類型

6G 無論在頻寬、連接數量及延遲等指標都遠勝5G，加上在工業5.0和深度學習技術的推動下，6G 將提供如圖107新的服務類型，相關說明如下：

(1) 新媒體：隨著無線網路通訊技術的飛速發展，訊息的溝通互動將從擴增實境 AR/虛擬實境 VR 逐步演進到高擬真擴展現實 XR，甚至實現無線全息通訊(wireless holographic communication)。使用者可以隨時隨地享受全息通訊和顯示帶來的新服務，如虛擬教育、虛擬旅遊、虛擬體育、虛擬音樂會等身臨其境的全新體驗。

(2) 新服務：藉由新的傳輸技術(如量子通訊 quantum communication, 可見光通信 visible light communication)，6G 將實現高精度且低延遲的傳輸品質，這將會為用戶提供更好的服務模式。例如，遠程手術、智慧交通系統等。

(3) 新基礎設施：隨著深度學習技術的發展，6G 通訊系統催生了許多新興的基礎設施，例如地面和空間集成、聯合學習網路、去中心化基礎設施和可信賴的基礎設施，特別是聯合學習網受益於6G 網路的高頻寬和低延遲，將為城市、工廠和人們帶來

了許多新興的智能應用。

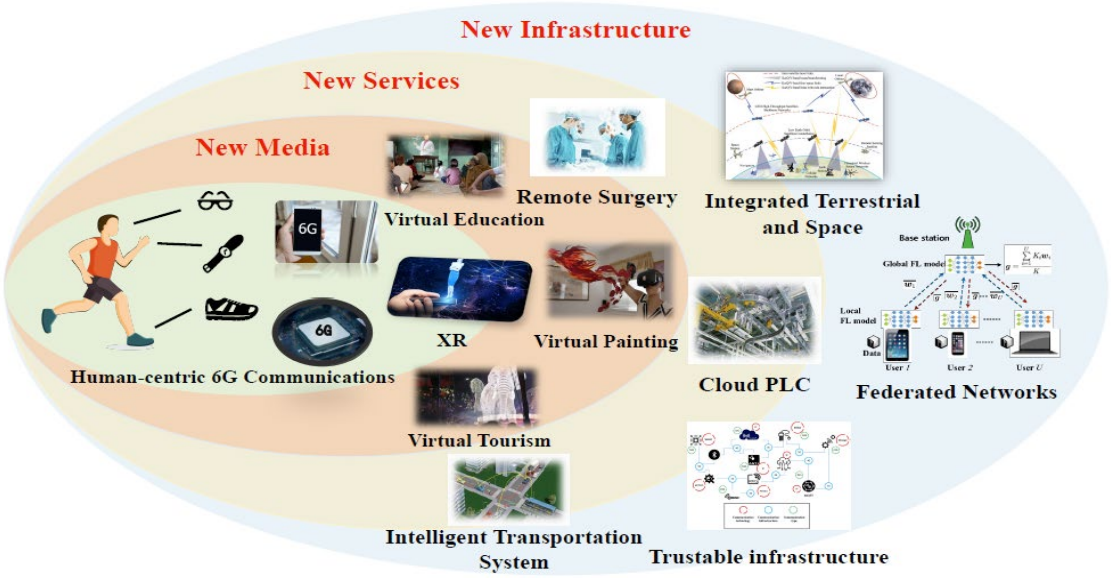


圖107、6G 新服務類型
資料來源：請參閱附錄-參考資料1.12

4. 需求分析

在需求分析中，將說明聯合學習的核心挑戰，這是聯合學習在6G 應用中大規模布署之前的主要瓶頸問題：

(1) 即時/省電(effective issues)

將聯合學習模型布署到裝置通常涉及模型訓練和推論，如果模型訓練和推論的速度比較慢，使用者將無法感受到沉浸式的智能服務體驗。因此，當聯合學習系統在6G 網路廣泛部署時，將面臨以下挑戰：

✓ 1.12 Y. Liu, X. Yuan, Z. Xiong, J. Kang, X. Wang and D. Niyato, "Federated learning for 6G communications: Challenges, methods, and future directions," China Communications, vol. 17, pp. 105-118, 2020.

A. 聯合學習模型的尺寸太大，無法放到單個裝置(記憶體不足)，且模型正確率維持一定水準。

B. 聯合學習模型訓練速度太慢，無法滿足6G 網路低延遲的要求，需降低模型訓練時間(包含 edge 端及 cloud 端)，減少延遲。

C. 聯合學習模型推論速度太慢，無法滿足使用者的即時及省電需求，因此，高效的訓練和推論對於聯合學習和6G 網路的完美融合是必要的。然而，對於聯合學習系統來說，在大規模的異構網路中實現高效的模型訓練和推論是一項挑戰。

(2) 大量的裝置及資料傳輸(Expensive communication)

由於聯合學習在模型訓練過程中涉及數千個裝置，因此資料傳輸是聯合學習在6G 中廣泛使用的關鍵瓶頸。此外，實現聯合學習網路中的資料傳輸與裝置的本地計算同步也是一項挑戰。為了使聯合學習模型適用於具有大量異構裝置(手機、手錶、感測器等)及網路架構的6G 網路，有必要開發一種資料傳輸效率高的方法，可以大大減少裝置和雲端之間交換梯度(gradient)的次數及梯度訊息大小。因此需要考慮

兩個關鍵方面來減少上述的資料傳輸：

A. 需降低訓練時所需的傳輸次數。

B. 需降低訓練時每次傳輸所需的梯度參數數量。

(3) 提供可信賴的服務(Reliable Security)

由於 6G 網路可以在更廣泛的地理區域內提供無處不在的服務，因此網路中每個裝置的計算和資料傳輸能力可能會因硬體(中央處理器 Central Processing Unit, CPU、圖形處理器 Graphics Processing Unit, GPU)、網路連接(4G、5G、6G、WiFi)和能量(電池電量)而有不同的效率，顯然地裝置之間的系統異質性會給聯合學習模型和6G 網路帶來一些混亂和故障。此外，聯合學習中可能存在不可靠的裝置，這可能導致系統故障。同樣攻擊者可能會對異構裝置發起基於學習的主動攻擊而導致聯合學習系統出錯。這些聯合學習系統的安全漏洞極大地加劇了惡意挑戰。因此開發一個安全且健壯的聯合學習必須滿足：

A. 防禦惡意攻擊(如 Byzantine failure、 poisoning/backdoor attacks)。

B. 異質裝置或網路皆可使用(如不同的 CPU/GPU、UAV/IOV)。

C. 有效結合眾人的訓練結果。

(4) 隱私保護(Privacy concerns)

儘管聯合學習通過共享模型更新(例如梯度)而不是原始資料來保護每個裝置的隱私，但在裝置與雲端之間的傳輸過程中仍會公開私有資料。例如，攻擊者可從裝置中竊取本地訓練資料(成員推斷 membership inference/梯度洩漏攻擊 gradient leakage attacks)。傳統用來增強聯合學習隱私性的方法，例如：安全多方計算(Secure Multi-Party Computation, SMPC)、同態加密(Homomorphic Encryption, HE)只能防止資料洩露問題，無法解決上述惡意攻擊。因此，聯合學習系統迫切需要開發新的隱私增強技術來抵抗或減輕上述惡意攻擊。

5. 現有技術與需求差異

為了應對上述挑戰，本節整理不同的新興技術或方法用以改良聯合學習系統：

(1) 6G 運算高效的聯合學習(Effective FL for 6G)

為了達到即時及省電的需求，有必要從訓練和推論中實現高效的聯合學習。

A. Efficient Training：高效的訓練可以大量減少裝置端的訓練時間

a. Federated Parallelization：可藉由資料/模型並行化(data/model parallelization)來加速模型訓練。如圖108資料並行化為訓練時不同裝置使用不同的資料(batches)，但整個模型的參數都有更新；模型並行化則是將模型拆分到多個裝置，訓練時跑相同資料(batch)，但是各自更新模型不同部分。

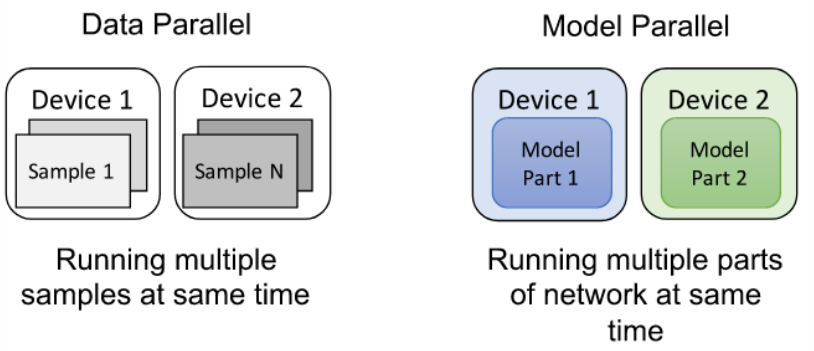


圖108、資料/模型並行訓練比較
資料來源：請參閱附錄-參考資料1.2

✓ 1.2 M. Alsabah, M. A. Naser, B. M. Mahmmod, S. H. Abdulhussain, M. R. Eissa, A. Al-Baidhani, N. K. Noordin, S. M. Sait, K. A. Al-Utaibi and F. Hashim, "6G Wireless Communications Networks: A Comprehensive Survey," IEEE Access, vol. 9, pp. 148191-148243, 2021.

b. Federated Distillation：如圖109採用遷移學習(transfer learning)，利用預訓練的複雜模型(teacher model)的輸出作為監督結果來訓練另一個簡單的模型(student model)。這種方式可以訓練學生模型，提高模型訓練的效率。

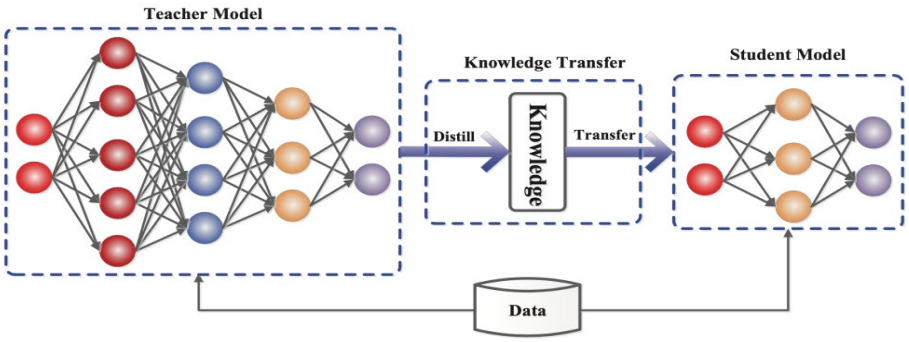


圖109、Teacher/Student model
資料來源：請參閱附錄-參考資料 1.3

B. Efficient Inference：現有模型過大，在運算資源較低的裝置無法實現即時的推論。可藉由以下方式實現高效推論。

✓ 1.3 C. D. Alwis, A. Kalla, Q.-V. Pham, P. Kumar, K. Dev, W.-J. Hwang and M. Liyanage, "Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research," IEEE Open Journal of the Communications Society, vol. 2, pp. 836-886, 2021.

a. Pruning：一種模型優化技術，藉由去除模型中較不重要的節點/權重(圖110)，不僅使得神經網路運行速度更快，而且降低了訓練模型的計算成本，這是將模型布署到手機或其他邊緣裝置(edge device)的關鍵步驟。

b. Weight Sharing：權重共享通過共享權重來減少模型參數的數量，從而實現高效的推論。如圖111，參數 W0,0= W0,1，W1,0= W1,1，W2,0= W2,1，參數量為原始模型的1/2。

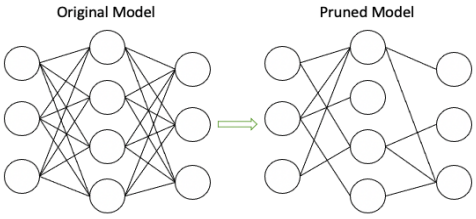


圖110、Model Pruning
資料來源：請參閱附錄-參考資料 1.4

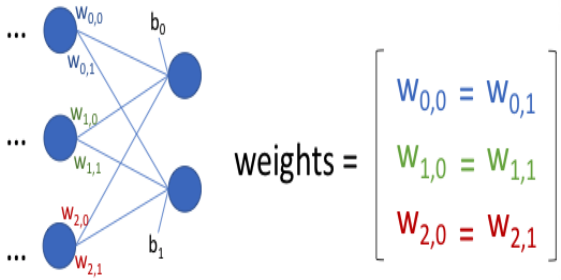


圖111、Weight Sharing
資料來源：請參閱附錄-參考資料 1.4

✓ 1.4 J. R. Bhat and S. A. Alqahtani, "6G Ecosystem: Current Status and Future Perspective," IEEE Access, vol. 9, pp. 43134-43167, 2021.

(2) 6G 傳輸高效的聯合學習(Communication-efficient FL for 6G)

分別從系統及演算法的角度解釋傳輸高效的聯合學習，從而促進6G 傳輸中更廣泛的聯合學習部署和應用。

A. System Level：從系統的角度來看，資料的分佈(如彼此獨立)、裝置分佈(如跨區域、跨網路連接的異構裝置)、機器學習方法(如去中心化和集中式)、通訊機制(如同步和非同步)等，在不同應用場景下對傳輸效率皆有不同的影響；如圖112，非同步的聯合學習系統(Asynchronous FL System)將會比同步的聯合學習系統(Synchronous FL System)傳輸效率高，原因是模型更新的機制不需等到所有的裝置都訓練完成才進行傳輸，降低裝置彼此等待時間。

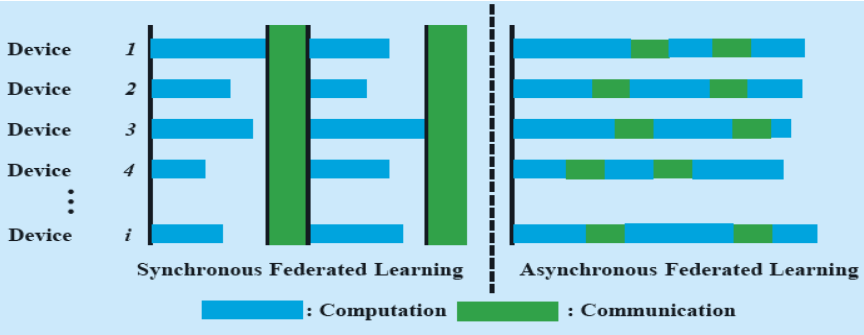


圖112、非同步聯合學習系統

資料來源：請參閱附錄-參考資料 1.12

✓ 1.12 Y. Liu, X. Yuan, Z. Xiong, J. Kang, X. Wang and D. Niyato, "Federated learning for 6G communications: Challenges, methods, and future directions," China Communications, vol. 17, pp. 105-118, 2020.

B. Algorithm Level：在演算法層面可藉由以下方式提高傳輸效率

a. Accelerating Model Convergence：使用基於 zero-order、first-order, second-order 隨機梯度下降法(stochastic gradient descent, SGD)演算法來減少模型訓練的回合數。如圖113，由於 SGD 更新梯度會加入隨機的概念，將有助於跳出 local minimum 而加速收斂。

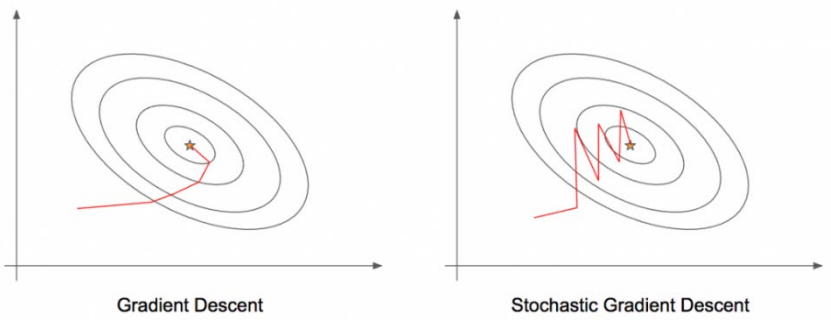


圖113、GD 與 SGD 比較
資料來源：請參閱附錄-參考資料 1.5

b. Reducing Communication Overhead：可藉由梯度稀疏化(sparsification)的方式將梯度壓縮，如此可以大大減少裝置和雲端之間大量的梯度交換，實現傳輸高效的聯合學習。已經不少研究證明將梯度壓縮以減少梯度的數量而不影響模型準確性。

✓ 1.5 A. L. Imoize, O. Adedeji, N. Tandiya and S. Shetty, "6G Enabled Smart Infrastructure for Sustainable Society: Opportunities, Challenges, and Research Roadmap," Sensors, vol. 21, 2021.

(3) 6G 可信賴的聯合學習(Secure FL for 6G)

由於6G 網路連接範圍廣泛，聯合學習在訓練過程中會遭受來自異構網路/設備和惡意參與者的攻擊，可由以下方式改善：

A. Robust Aggregation Algorithm：因結合眾人的訓練結果，若參與者提供偏差資訊，整個模型訓練將遭受很大的影響，可利用類似 filter 或 regularization 的方法來減少異構設備/網絡的干擾。

B. Robust Detection Mechanism：另一個直觀的想法是檢測惡意裝置以阻止它們參與聯合學習訓練。這種機制一般利用裝置生成的子模型的準確性作為檢測惡意裝置的評估指標。

C. Reliable Reputation Management：裝置的歷史行為可以作為一個關鍵指標-信譽值(reputation)，藉由它來評估該裝置的可靠性和可信度。較高的信譽值代表裝置更可靠。

(4) 6G 隱私保障的聯合學習(Privacy-preserving FL for 6G)

聯合學習需要開發新的隱私增強技術來抵抗或減輕惡意攻擊(membership inference/gradient leakage attacks)，可由以下方式改善：

A. Differentially Privacy：直觀想法是如果隨機修改資料庫中的一個記錄造成的影響足夠小，而使求得的統計特徵不能被用來反推出單一記錄的內容；這一特性可以被用來保護隱私，但可能的代價為犧牲模型性能，因此，目前有一些先進的方法可以平衡隱私和性能。

B. Deep Net Pruning：可藉用上述模型優化技術-pruning 的概念，在資料去除某些特徵的情況下也能維持模型準確率，為平衡實用性和隱私性提供了新的機會。

C. Gradient Compression：由於梯度包含豐富的語義訊息(semantic information)，攻擊者可藉此推斷裝置的本地資料。因此很直覺產生破壞梯度訊息分佈從而保護梯度隱私的方法，例如梯度壓縮可以在不影響模型準確率的情況下防禦梯度洩漏攻擊。

6. 目標與技術探索

聯合學習允許從邊緣/移動裝置收集的本地資料中進行模型訓練，同時保護資料隱私，這對視覺和語音應用具有廣泛的適用性。然而與雲端中心的伺服器相比，參與者裝置的計算和傳輸資源是有限的，例如智慧手機是以攜帶方便為主，通常不會搭載高階的 GPU。

在這種資源有限的邊緣裝置上訓練可以包含數百萬個參數/權重(weights)的深層神經網路(Deep Neural Network, DNN)模型可能需要非常長的時間並消耗大量的能量。因此，一個自然的問題是：如何有效地執行聯合學習，以便在合理的時間及運算資源下訓練模型。為了克服這一挑戰，模型壓縮(model compression)或模型剪枝(model pruning)是目前熱門的研究方向，藉由調整模型大小以減少傳輸和計算開銷並最小化整體訓練時間，同時能保持與原始模型相似的準確性。例如 Google 提出在線模型壓縮(Online Model Compression, OMC)的框架，以壓縮格式儲存模型參數並僅在需要時對其進行解壓縮。在兩個用於語音辨識的神經網路和兩個不同資料集的實驗中，與不壓縮的訓練模型相比，OMC 可以將模型參數的內存

使用和傳輸成本降低高達59%，同時獲得相當的準確度和訓練速度。PruneFL 則是運用模型剪枝技術，具有分佈式和自適應修剪(Distributed and Adaptive Pruning)的新型聯合學習方法。分佈式修剪包括在選定參與者的初始修剪以及在聯合學習訓練過程中選取一部分模型進一步修剪；自適應修剪則是持續監控一個模型，若該模型足夠小(內存佔用少)可以高效傳輸和計算，則保持有用的連接及其參數，使模型收斂到與原始模型相似的準確度。

本計畫選用模型剪枝的技術進行實驗，實現 AIoT 運算裝置間，模型資料降低以達成傳輸效率提升的目標。原因是根據大樂透假說(Lottery Ticket Hypothesis)，2個同樣大小的模型 m1,m2，m1初始由原本一個大的模型 M 隨機刪除一些參數產生，m2初始則是隨機生成，經過訓練後 m1的準確度會比 m2好，甚至與 M 相當。

6G 關鍵性能指標之一為超大規模同時連網，加上深度學習的蓬勃發展，無處不在的人工智慧將被實現。例如智慧商店商品影像辨識應用，使用者可透過手機辨識商品，得知更多產品訊息，如買一送一，或是店員可使用平板識別架上商品，進

行理貨及盤點，如庫存不足需補貨，如圖114所示。

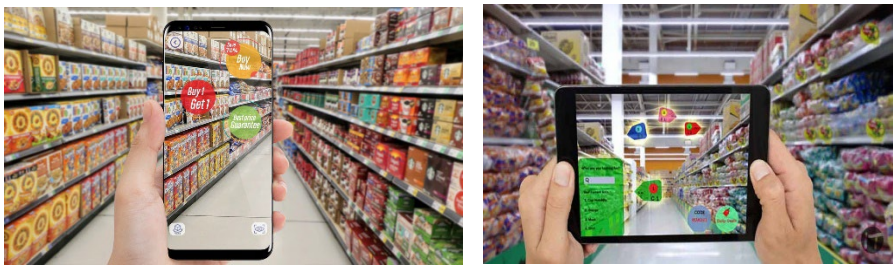


圖114、智慧商店商品影像辨識應用
資料來源：Augray、Peru-Retail

然而因辨識模型過於複雜，需龐大的記憶體及運算資源才能執行，導致無法在一般 Edge Device(如手機)執行。本計畫模擬6G 運算高效的聯合學習(Effective FL for 6G)；藉由降低模型的複雜度(Model Pruning)，使其能在一般手機執行，並維持與複雜模型相當的正確率，達成6G 關鍵性能指標「超大規模同時連網」。

本計畫目標情境為智慧商店的商品影像辨識應用，需要訓練品項繁多且高辨識率的商品辨識模型，這將會遭遇以下挑戰：

(1) 耗費大量資源蒐集及訓練：若由總公司統一訓練模型，則會因各分店光源、背景、貨架、商品配置的不同，而必須集中大量分店的訓練資料，然後耗費龐大的運算資源訓練一複雜的模型。

✓ Augray：https://www.augray.com/blog/augmented-reality-solutions-to-engage-in-store-shopping/supermarket_price_01-1/
✓ Peru-Retail ： https://www.peru-retail.com/de-ikea-a-walmart-la-realidad-aumentada-revoluciona-el-retail/

(2) 若使用傳統的聯合學習，雖可將蒐集大量資料及訓練資源由各分店分擔訓練，但參數量多需要龐大的記憶體及運算單元，最終複雜的模型也很難在計算資源普通的 Edge Device 運作。(參數量多需要龐大的記憶體及運算單元)

如圖115，在傳統聯合學習的基礎上，有效利用各節點的資料及資源，並藉由模型剪枝的技術降低模型複雜度並維持正確率，不僅縮小模型至可以部署到邊緣裝置(如手機)，同時也能確保正確率。

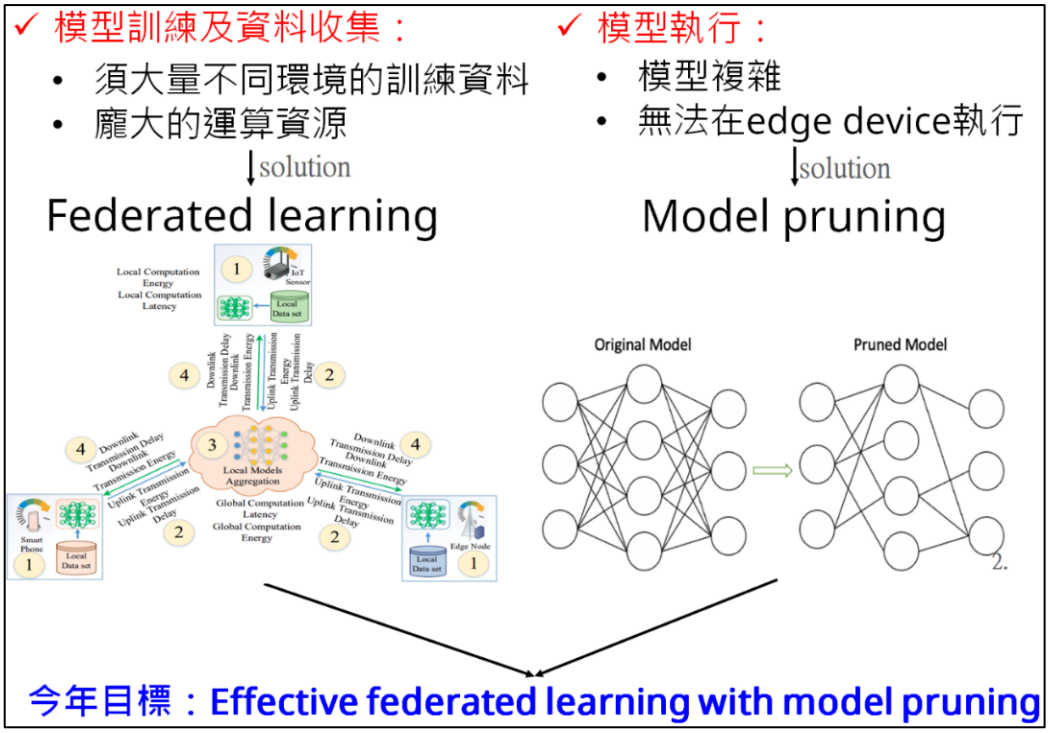


圖115、Effective federated learning with mode pruning
資料來源：本計畫整理

(二) 研析成果

實驗規劃參考附錄資料1.8 (Effective FL for 6G 中的 Model Pruning) 進行影像辨識。在傳統聯合學習的基礎上，有效利用不同來源的影像及資源，藉由模型剪枝的技術降低模型複雜度並維持正確率。細節說明如下：

1. 實驗規劃

(1) 任務：影像分類。

(2) 資料集：分別在2種資料集上進行實驗。

A. CIFAR-10[1.28]：是一組常用於訓練機器學習和計算機視覺算法的影像資料庫。它是機器學習研究中使用最廣泛的資料集之一。包含10個不同類別的彩色影像，分別是飛機、汽車、鳥類、貓、鹿、狗、青蛙、馬、輪船和卡車。

B. 商品資料集：由本計畫蒐集之商品影像，如圖116，分別在三種不同環境下使用行動裝置拍攝收集，模擬真實情況下使用者可能的使用情境，包含餅乾、泡麵、飲品等40類商品。

✓ 1.8 Y. Jiang, S. Wang, V. Valls, B. J. Ko, W.-H. Lee, K. K. Leung and L. Tassiulas, "Model Pruning Enables Efficient Federated Learning on Edge Devices," IEEE Transactions on Neural Networks and Learning Systems, pp. 1-13, 2022.
✓ 1.28CIFAR-10 and CIFAR-100 Datasets. www.cs.toronto.edu/%7Ekriz/cifar.html.

圖116、三種不同的智慧商店

資料來源：本計畫整理

(3) 演算法開發：運用模型剪枝技術的聯合學習，演算法架構如圖117，其中聯合學習分為兩個部分：Server 及 Client，分別以虛擬機器(virtual machine, VM)方式模擬。Client 根據本地端的資料進行模型訓練後上傳梯度(gradient)；Server 負責統整來自 Client 端的梯度後進行模型更新。然後 Server 在預設的修剪比例下(如10%、20%)，進行模型剪枝，最終將剪枝後的模型傳給參與的 Client；重複上述步驟直到模型收斂。細節說明如下：

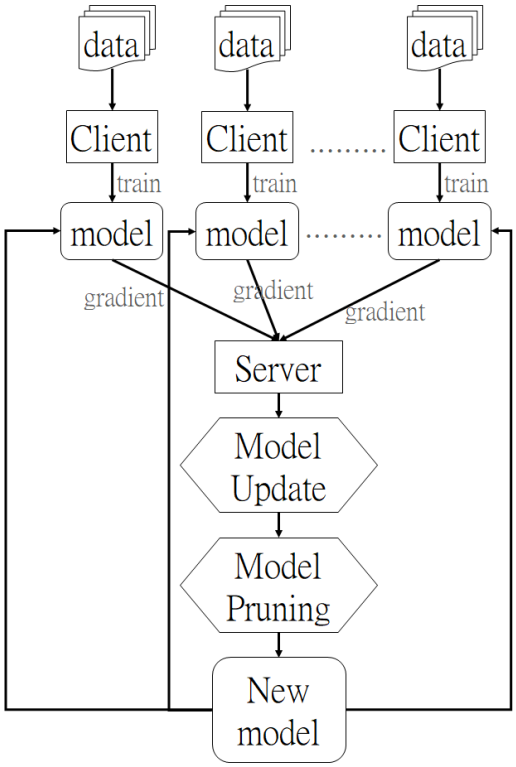


圖117、運用模型剪枝技術的聯合學習演算法架構

資料來源：本計畫整理

A. 聯合學習：Server 端可設定有幾個 Client 參與；Client 端則可設定每回合(Run)要訓練幾個 Epoch 後才上傳梯度。相關配置如下：

a. 作業系統:Win 10

b. 硬體:I5-10400、NVIDIA GeForce GXT 1660、32GB ram

c. 軟體：Python 3.6、Pytorch1.7.1、Flower 1.2.0

B. 模型剪枝：將訓練後的模型參數經過計算後，可得出對模型貢獻度並依照貢獻度排序，根據預設的修剪比例將

低貢獻度參數移除；移除方式為在權重檔中加入一個 mask，使之後模型運算時不會對被 mask 的參數進行計算，以此減少計算量。相關配置如下：

a. 作業系統:Win 10

b. 硬體:I5-10400、NVIDIA GeForce GXT 1660、32GB ram

c. 軟體：Python 3.6、Pytorch1.7.1 (torch.nn.utils.prune)

2. 實驗結果

(1) CIFAR-10：50,000張訓練照片分割為五份，並分別在5個 Client 使用各自獨立的訓練資料訓練，由於類別數只有10類，網路架構即使用 EfficientNet-B0，EfficientNet 是 Google Research 發表在 ICML 2019 的工作。EfficientNet 根據網路尺寸從小到大，分爲了 B0到 B7共8個網路，其中 EfficientNet-B0模型尺寸最小，速度最快，準確率相對最低；EfficientNet-B7模型尺寸最大，準確率最高，速度也相對最慢。由於不適合在 GPU 類硬體上運行，因此設備需求很高且模型訓練時間長。EfficientNet-V2(網路尺寸從小到大，分成了 S、M、L、

XL 4個網路)改善了在 GPU 的運行效率，不只準度更好、模型尺寸更小、訓練速度也更快。訓練後將梯度上傳至 Server；Server 在預設的修剪比例下進行模型剪枝。重複上述步驟直到模型收斂。如表35，分別修減0~50%的參數量(計算量)，正確率分別為74%、74%、74%、73%、71%、63%。在修剪低於40%的參數量下，正確率幾乎與不修剪相同，符合預期成效。而參數量的減少比例則可視模型結構及情境需求來調整，例如若要兼顧使用者滿意度(正確率僅低3%)且同時能降低網路傳輸及 edge 端效能需求(模型大小及運算次數僅約原本的一半)，可選擇減少40%的參數量。相關程式可由此下載：https://github.com/justin61013/FL/tree/main

表35、CIFAR-10實驗結果

參數量減少% (影響 edge 端效能需求)	模型大小 (影響網路傳輸及 edge 端效能需求)	正確率 (影響使用者滿意度)
0% (1562.79M 個 FLOPS、3.61M 個參數)	100 MB	74%
10% (1406.51M 個 FLOPS、3.25M 個參數)	80 MB	74%
20% (1250.23M 個 FLOPS、2.89M 個參數)	60 MB	74%

30% (1093.95M 個 FLOPS、2.53M 個參數)	55 MB	73%
40% (937.67M 個 FLOPS、2.17M 個參數)	53 MB	71%
50% (781.39M 個 FLOPS、1.81M 個參數)	50 MB	63%

資料來源：本計畫整理

(2) 商品資料集：三種環境分別收集每種商品25張影像，其中20張拿來訓練，5張做為測試，總共3,000張影像。分別在3個 Client 使用各自獨立的訓練資料訓練，由於類別數較多，本計畫使用較大的網路架構 EfficientNet-V2-s，訓練後將梯度上傳至 Server；Server 在預設的修剪比例下進行模型剪枝。重複上述步驟直到模型收斂。實驗結果如表36，在修剪低於40%的參數量下，正確率幾乎與不修剪相同，符合預期成效。

表36、商品資料集實驗結果

參數量減少% (影響 edge 端效能需求)	模型大小 (影響網路傳輸及 edge 端效能需求)	正確率 (影響使用者滿意度)
0% (2924.13M 個 FLOPS、20.38M 個參數)	160.84 MB	93.5%
10% (2631.6M 個 FLOPS、18.342M 個參數)	147.98 MB	93.4%

參數量減少% (影響 edge 端效能需求)	模型大小 (影響網路傳輸及 edge 端效能需求)	正確率 (影響使用者滿意度)
20% (2339.12.M 個 FLOPS、16.34M 個參數)	132.6 MB	93.4%
30% (2047.09M 個 FLOPS、14.27M 個參數)	114.64 MB	92.7%
40% (1754.48M 個 FLOPS、12.23M 個參數)	88.42 MB	92.4%
50% (1462.1M 個 FLOPS、10.5M 個參數)	85.1 MB	87%

資料來源：本計畫整理

3. 未來規劃

(1) 手機是未來6G 主要的平台，但由於目前深度學習模型過大，使得手機因效能不足或過於耗電無法部署，因而限制了6G 高傳輸及大連結的功能。現階段的開發先以改善演算法為主，藉由使用 model pruning 的方法，不僅縮小模型至可以部署到邊緣裝置(如手機)，同時也能確保正確率。整合 Android/iOS 的平台及網路環境的測試則是下階段的目標，然系統及環境設定、網路溝通傳輸等，是另一待克服的難題。

(2) 解決異質節點共同參與訓練問題(heterogeneous device)

A. 運算效能不同：目前假設各節點都會同時上傳/更新參數，需開發更彈性的架構解決非同步問題，使得6G關鍵性能：超高速傳輸更能發揮其效用，不需因單節點延遲而影響整體訓練速度。

B. 取得資料不同：目前假設各節點取得的資料品質相同，需設計一篩選機制進一步提升模型準確率，使得6G關鍵性能：超低延遲、高可靠度更能發揮其效用，如自動駕駛需快速且精準識別周遭環境，不因裝置提供不可靠的資訊而造成安全問題。

(3) 解決現有聯合學習的問題，包含以下兩點，而這些問題將可由 Federated Continue Learning/ Federated Class Incremental Learning 獲得改善。如圖118，藉由同時從 global 和 local 兩個角度出發，使模型能選擇性地接收知識，防止不相關知識的干擾，使得新舊類別都能辨識：

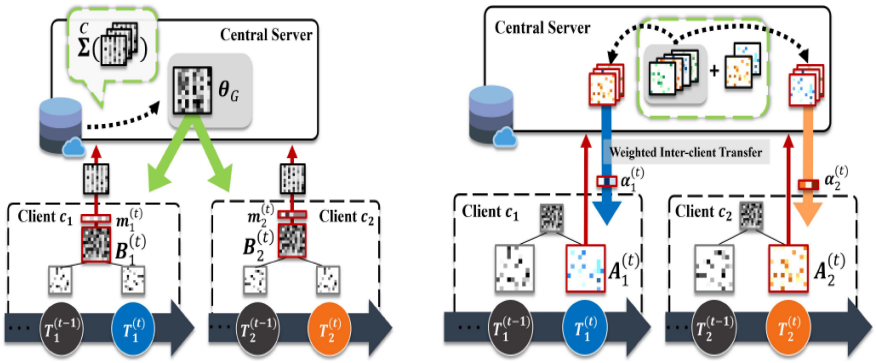


圖118、(左) Global：集合各個 client 的資料提升模型準確率
(右)Local：Client 選擇性下載所需參數，避免不相關干擾
資料來源：請參閱附錄-參考資料1.2、1.32

A. 假設類別固定且已知，新類別(unseen class)將無法識別，如圖119，每個醫院有一個不斷學習的疾病診斷模型，此模型會想要利用來自其他醫院的相關任務參數。當某醫院發現新疾病時，需能新增疾病類別並更新聯合學習模型，使得其他醫院受益。

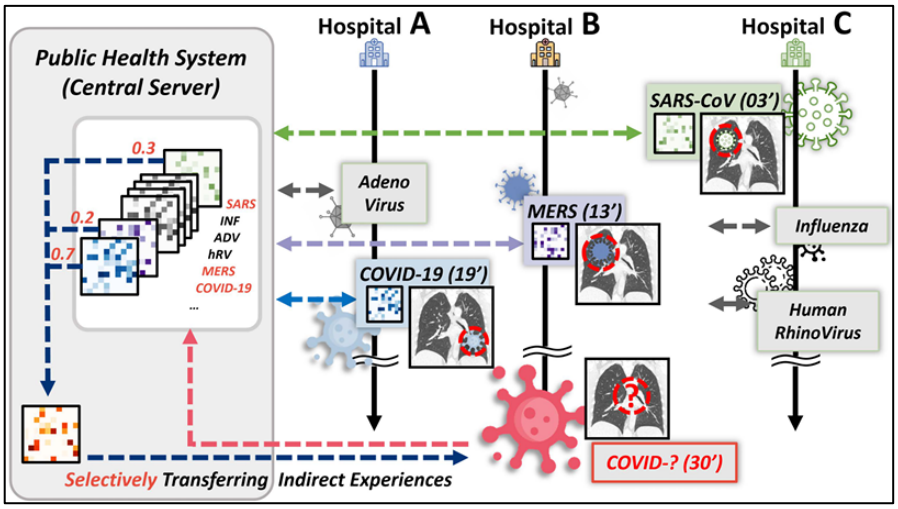


圖119、聯合學習問題1：無法識別新疾病(新類別)
資料來源：請參閱附錄-參考資料1.2

✓ 1.2 M. Alsabah, M. A. Naser, B. M. Mahmmod, S. H. Abdulhussain, M. R. Eissa, A. Al-Baidhani, N. K. Noordin, S. M. Sait, K. A. Al-Utaibi and F. Hashim, "6G Wireless Communications Networks: A Comprehensive Survey," IEEE Access, vol. 9, pp. 148191-148243, 2021.
✓ 1.32 Dong, Jiahua, et al. "Federated class-incremental learning." Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2022.

B. 新類別可能會對舊類別的辨識率造成傷害(catastrophic forgetting)，如圖120，要辨識的目標類別(藍色)應該使用既有相關的類別資訊(綠色)來訓練模型，但因新類別(紅色)的加入而干擾了模型的學習，導致正確率下降(灰色折線)。

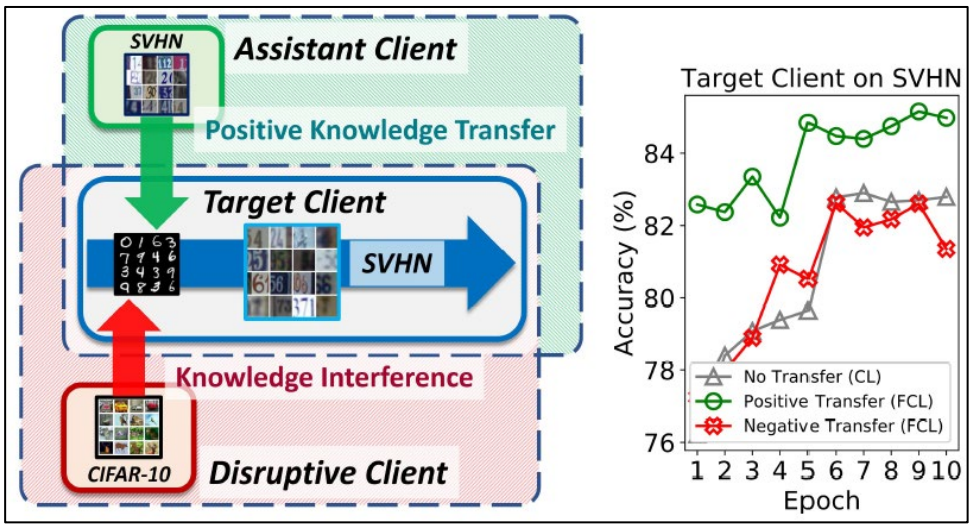


圖120、聯合學習問題2：新類別影響舊類別的辨識準確率
資料來源：請參閱附錄-參考資料1.2

✓ 1.2 M. Alsabah, M. A. Naser, B. M. Mahmmod, S. H. Abdulhussain, M. R. Eissa, A. Al-Baidhani, N. K. Noordin, S. M. Sait, K. A. Al-Utaibi and F. Hashim, "6G Wireless Communications Networks: A Comprehensive Survey," IEEE Access, vol. 9, pp. 148191-148243, 2021.

八. 計畫執行情形-安全可靠與受信賴的分散式運算設計與驗證

市場預測推估電信業在區塊鏈的投資增長率為48.5%[2.1]，此報告以2020年為基準，提供2021-2026的市場預估值，如圖121所示。

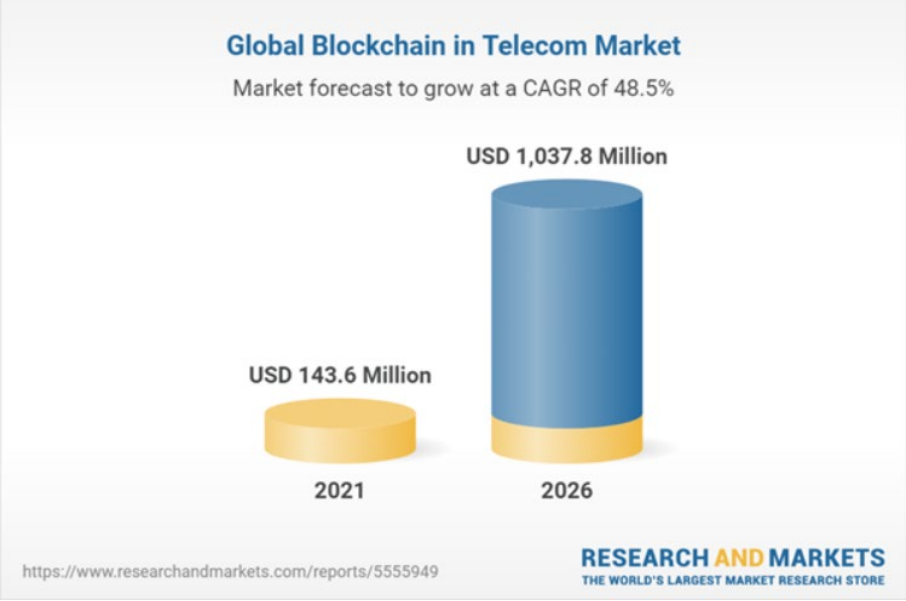


圖121、電信業投資區塊鏈之複合成長率
資料來源：請參閱附錄-參考資料2.1

就如報告預估的趨勢，許多電信業者已經開始多方面應用區塊鏈以解決計費糾紛，用戶身分管理等問題，並思考這樣的趨勢是否會改變現有營運方式。

✓ 2.1https://www.researchandmarkets.com/reports/5555949/blockchain-in-telecom-global-markets?utm_source=GNOM&utm_medium=PressRelease&utm_code=mhrq3r&utm_campaign=1671646+-+Blockchain+in+Telecoms%3a+2022+Industry+Analysis+-+Global+Market+to+Grow+from+%24143.6+Million+in+2021+to+%241.03+Billion+by+2026%2c+Witnessing+a+CAGR+of+48.5%25&utm_exec=joca220prd

區塊鏈系統是分散式帳本 DLT 的一種，DLT 可以移除中央管理系統，可提供每個用戶每筆交易的分類帳，而非被迫信任業者提供的交易紀錄。區塊鏈本身就是網路，每筆交易皆使用雜湊(hash)函數加上時間戳形成區塊(Block)，Block 需要達成共識才能進入鏈中，這即是共識協議(Consensus Protocols)。

共識協議有一個最長鏈規則(The Longest Chain Rule)，只有在最長鏈(主鏈)的交易才會被認可，其他短鏈的交易不會被認可，這些交易資訊將會回到網路重新包裝。因此，最長的鏈不僅證明了事件的先後順序，而且證明大多數處理交易的節點達成了共識。只要攻擊者不擁有網路的節點大部分計算能力，共識協議就會產生最長的主鏈並跑得比攻擊者快，使得區塊鏈系統可以提供無信任基礎的服務。

電信業者使用區塊鏈解決的現有問題有計費糾紛，用戶身分管理問題等。計費糾紛大都源自於呼叫詳細記錄(Call Detail Records, CDR)，因為 通訊服務商(Communication Service Providers, CSP)必須依賴合作夥伴的網絡和數據來收集、處理和傳輸呼叫和數據記錄，造成效率低下且容易欺詐，Telefónica 與 IBM 合作開發了基於 BC 的 CDR 解決計費問題。

美國電信公司 AT&T 正在開發一個安全的多因素身分驗證平台，將數據記錄在 IBM 和微軟提供的區塊鏈解決方案上，可減少對中介機構的需求、削減費用。對於漫遊，使用區塊鏈技術可以實現更高效、即時和無縫的電信事業間流程。

由於6G 行動網路高規格需求，電信業者需要共享資料、設備，以滿足使用者對於新科技的需求。最基本的共享項目有頻譜共享，目前的頻譜管理政策為各頻段由各家電信業者擁有，面臨頻譜擁有者在某些地區、某些時段找不到頻譜需求者，或是頻譜需求者過多造成頻譜不夠用，為了解決供需不匹配的問題，需要頻譜共享的解決方案。電信業者共享資料用戶使用紀錄，制定最佳頻譜分配方式，這需在沒有預先建立信任關係的各方之間即時進行頻譜分配交易，即是無信任服務的基礎建設，而區塊鏈系統正好滿足此需求。除此之外，頻譜分配交易還需要 AI 技術才可做精密的動態分配，以達成更好的頻譜使用率，而 AI 演算法都需要大量資料訓練才能做出準確的預測，若資料來自不同用戶，則須考慮隱私保護機制，在現有技術中，以聯合學習的架構最符合此應用場景，因為用戶不用送出資料就可與其他用戶共同完成模型訓練，可增加用戶貢獻的意願。這意味著區塊鏈和聯合學習兩種架構的

結合，用戶可以提供大量資料可由區塊鏈得到安全保障及獎勵，而 AI 演算法可以得到大量資料訓練模型，使得電信業者可以建構更好的服務網路，這樣的趨勢有機會改變現有營運方式。

6G 網路提供大頻寬、低延遲的無線網路環境，連結密集且多樣的無線裝置。6G 標準更允許數量逐漸增長的應用程式在前述的無線網路環境執行，如物聯網系統。物聯網裝置會產生非常多的資料，若將這些都上傳雲端中心將不可行，原因有：

- ✓ 通訊/計算/儲存成本會提高，應用程式接收/處理資料，以提取資料中所涵蓋的資訊，作為後續決策使用。這過程可能需要多種機器學習方法，需消耗大量計算資源且會產生額外的資料占用更多儲存空間，若引進平行計算方法，會有額外的傳輸成本。
- ✓ 延遲時間會增加，許多應用程式，如自動駕駛，需要即時處理，而大量資料向雲端中心可能會造成通訊瓶頸，增加延遲時間。
- ✓ 隱私保護需求，歐盟的法規如一般資料保護規則(General Data Protection Regulation,GDPR)，規定包含個資的資料需要管制，一旦違反法規將影響營運。

因此，發展一個安全可靠與受信賴的分散式機器學習環境，以持續管理及利用不斷大量增加的資料與通訊成本(尤其是裝置對裝置)，對6G 行動網路是重要的。安全可靠與受信賴的分散式運算環境，需允許分散式機器學習相關應用程式不用傳輸大量資料給雲端中心以產生模型。取而代之為裝置在網路邊緣處理自己的資料，再透過行動邊緣伺服器傳遞參數給雲端中心，以進行分散式機器學習，這樣的解決方案可以明顯地降低網路傳輸負載並降低違反隱私保護法規風險。

除此之外，6G 行動網路已經不再只是電信網路，3D 立體通訊網路將包括低軌衛星、無人機以及高空平台都已被涵蓋，如圖122所示，這些網路的營運商有可能不同，現有的認證機制會非常沒有效率，無法達到6G 行動網路的需求。

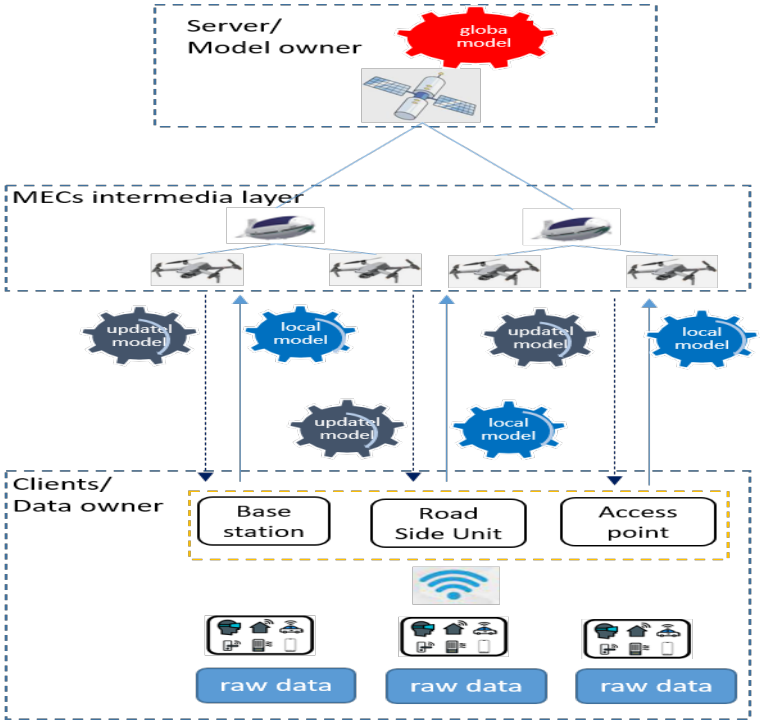


圖122、聯合學習在3D 空間網路 FL 處理流程

資料來源：請參閱附錄-參考資料2.23

(一) 研析方法與過程

結合區塊鏈和聯合學習 FL 兩種架構建構的分散式運算環境需考慮安全機制如何布署以及如何減少延遲，才可滿足各種異質網路之需求。

為此，本計畫將借助邊緣計算的概念，將計算的位置拉近資料，取消中央式運算/儲存環境，並應用區塊鏈為分散式儲存空間，保證數據不可篡改、可追溯，以區塊鏈信任關係取代用戶與網路營運商認證機制，建構分散式運算環境。預期可以為6G 行動網建構安全且開放的資料共享的運算環境。

✓ 2.23 Harayama ,Y.(2016), 600 Trillion Yen GDP TargetSTI Policies for Moving Toward Society 5.0!. Retrieved Jul.20, 2017

本工作項目分別就 Hyperledger Fabric 架構，基於區塊鏈之聯合學習(BlockChain based Federated Learning, BCFL)，及 Model update Poisoning 攻擊進行研析，相關研析結果說明如下：

1. 區塊鏈系統建置

區塊鏈本質上就是一種分散式帳本，經由密碼學的雜湊函式、點對點通信、共識機制、分散式儲存及置智慧型合約等技術組合，可以在沒有第三方公正機構的情形下，解決互不信任的雙方或多方交易過程的信任問題。

基本上，區塊鏈具有去中心化、可追蹤、匿名及不變性等特性，其中匿名的特性需由加密個人訊息達成。區塊鏈系統可劃分成6層，分別為：

(1) 資料層，包含 block header 及 block body。block header 包含了前一筆交易的 block header、Nonce、Time Stamp。區塊鏈資料結構具有分散式、不可竄改等性質，由區塊鏈所有節點，即是礦工(miner)，共同維護。

(2) 網路層，提供點對點網路、廣播機制及驗證機制(verification mechanism)，其中驗證機制檢查交易格式、數位簽章等，避免浪費計算資源。

(3) 共識層，產生隨機數以滿足交易的 hash(前一筆交易的 block header，當前交易資料、Nonce)符合特定格式的摘要值，其中特定格式的摘要值通常是多個前導零組成的數字字串所組成，如0000000ABC...12F，也就是 Difficulty Value，而此過程即為挖礦。

(4) 激勵層，獎勵發行/發放，用以激勵個節點挖礦行為。

(5) 合約層，區塊鏈的代碼，無須第三方公正單位。

(6) 應用層，區塊鏈系統對外溝通的解決方案。

Hyperledger Fabric 除了擁有上述的基本功能，還設定節點需要公司或組織許可，因此可以依節點狀況，設定部分節點即可達成共識，同時也增加一些額外設定，讓 Hyperledger Fabric 可以用不同通道區分不同應用，使得 Hyperledger Fabric 適合用於企業應用。

Hyperledger Fabric 中有以下各種基本元件：

(1) 工作應用程式：終端程式，交易請求的發起者，在本次實驗中，是一個 python 程式呼叫 peer 的 Web API 以進行操作。

(2) Peer：Peer 即是區塊鏈網路上節點，用於組成區塊鏈。負責保存區塊鏈帳本(Ledger)以及智能合約(Chaincode)。Peer 可以存放多個 Ledger 及 Chaincode。

(3) Channel：一個以公開金鑰密碼系統建立的私密通訊及交易的機制。加入 Channel 的 Peer 都需要維護一份相同的 Ledger，Peer 需加入 Channel 才可以存取這份 ledger，以此達到保護隱私的作用。

(4) Orderer：Hyperledger Fabric 設計的特殊節點用來確保 Peers 的 Ledger 一致性，並負責排序交易及打包成區塊回傳給 Peer 以加入區塊鏈。

(5) Chaincode: 區塊鏈節點背書程式，程式內容為一些商業邏輯，即是此次實驗的 Plugin，也是圖123的 Endorser。

Hyperledger Fabric 架構如圖123所示，Fabric 包含兩種節點，即 Peer，Orderer，其中 Peer 可以布署 Chaincode，讀寫區塊鏈(Blokchain, BC)帳本，Orderer 則為排序節點，可以排序交易，以及將交易批次組合成區塊，發給 Peer 節點。所有節點會以通道(Channel)連結。

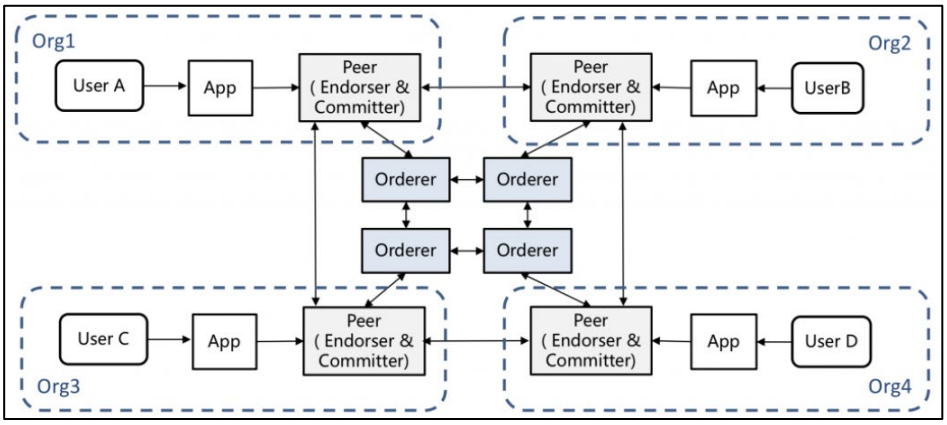


圖123、Hyperledger Fabric 架構圖

資料來源：請參閱附錄-參考資料2.5

交易流程如圖124所示，相關說明如下：

(1) 用戶(如 User A)向 Peer 提出交易提案(Proposal)，Peer 對 Proposal 驗證/簽章，再回傳 Proposal

(2) 用戶透過 Peer 將交易廣播到 Orderer，Orderer 驗證 Peer 簽章，比較各背書節點傳回的交易結果是否一致，將傳回的交易結果組成資料集，發送給 Peer

(3) Peer 將訊息廣播發送給 Orderers

(4) Orderers 交易排序讓其他 Peer 進行共識驗證，若驗證完成則產生區塊，寫入區塊鏈。

✓ 2.5https://github.com/hyperledger/fabric

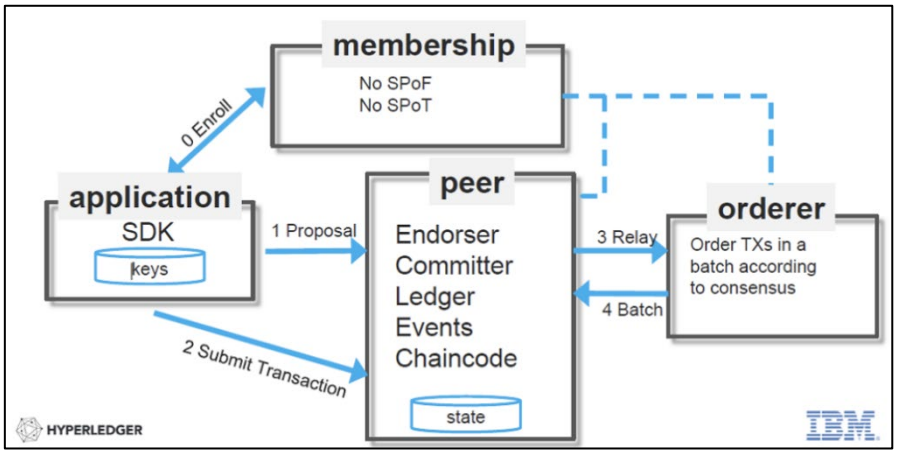


圖124、Hyperledger Fabric 交易流程圖

資料來源：請參閱附錄-參考資料2.5

Hyperledger Fabric 屬於私鏈，用戶及節點需要公司或組織許可，由於是許可制，參與者作惡的機率較小，可以用少量節點進行共識，因此比公鏈(如比特幣)較有效率，且 Hyperledger Fabric 可以用不同通道區分不同應用，由於前述兩個原因，使得 Hyperledger Fabric 適合用於企業組織。

2. 基於區塊鏈之聯合學習 BCFL 建置

傳統的聯合學習是屬於中央式機器學習系統，可允許多個資料擁有者共同訓練取得共同的機器模型，中央設置的伺服器通常需要較大的資源及特別設定的網路排程，否則無法服務太多客戶端工作。傳統中央式 FL 運作流程如下：

✓ 2.5https://github.com/hyperledger/fabric

(1) Clients Selection：依據事先定義好的協議，選擇參與的計算節點，即是 client，計算節點下載最新的 Global Model 當成初始值。

(2) Local Model Training：計算節點使用 raw data 訓練 local model。

(3) Update Local Model：計算節點上傳最新的 local model。

(4) Global Model Aggregation/update：FL server 收集 local model，進行 global model 訓練，並對計算節點 global model。

具有行動邊緣計算 MEC 層，使得 FL 兩層計算架構轉變為三層，這是5G 行動網路為了拉近客戶端與運算資源的距離以最小化延遲，但中央的伺服器並未移到 MEC，如圖125所示。

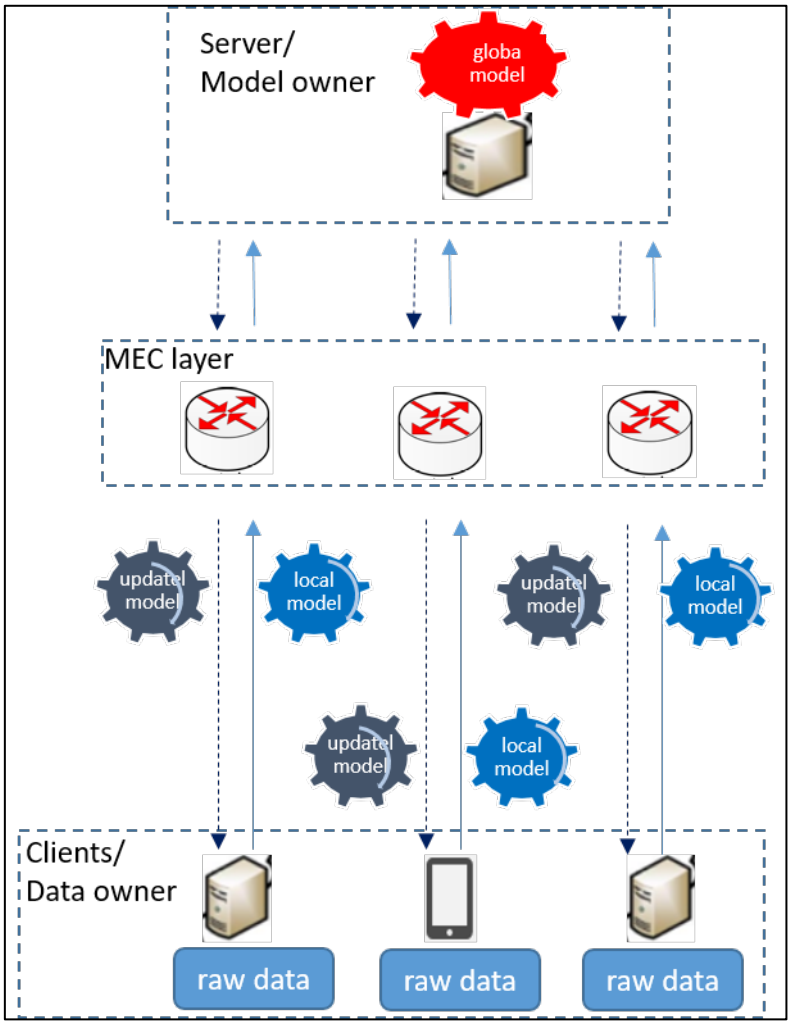


圖125、三層式的 FL 架構圖
資料來源：請參閱附錄-參考資料 2.14

BCFL 工作流程，如圖126所示，除了 BC 的工作程序外，FL 的工作程序也都放在 BC 的節點上，這將降低布署 FL 的彈性。

✓ 2.14 M. Satyanarayanan, V. Bahl, R. Caceres, and N. Davies, “The case for vm-based cloudlets in mobile computing,” IEEE pervasive Computing, 2009

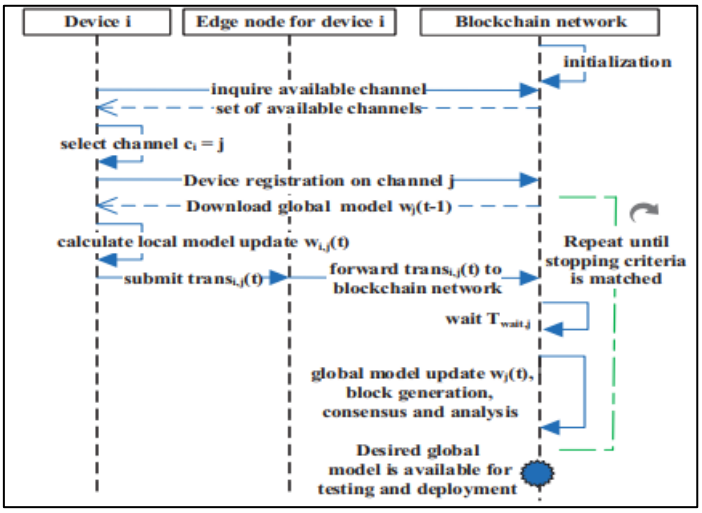


圖126、BCFL 工作流程圖

資料來源：請參閱附錄-參考資料2.6

基於區塊鏈之聯邦學習主要目的為最小化延遲，避免單點故障。現有的解決方案都將區塊鏈當成是分散式儲存空間，所提架構類似圖126所示的架構，不同的地方為 FL 伺服器要如何被取代，以避免遠距通訊來收集/更新模型，作法有：

(1) 所有 FL 計算節點，更新 Local Model 到區塊鏈，當更新完畢，FL 計算節點計算 Global Model，然後重複此步驟到模型收斂。

(2) 並非所有 FL 計算節點都有足夠的資源更新 Global Model，因此有些方案建議將區塊鏈建置在 MEC 層，由 MEC 裝置扮演區塊鏈節點。

✓ 2.6 Majeed, Umer & Hong, Choong. (2019). FLchain: Federated Learning via MEC-enabled Blockchain Network. 10.23919/APNOMS.2019.8892848.

(3) 在6G 行動網路中，MEC 裝置也有可能是資源受限的無線裝置，因此一些方案建議將 FL 伺服器放在大基地台(Macro Base Station)，降低通訊成本。

現有 BCFL 解決方案，如[2.7][2.8]，分別以有向無環圖(Direct Acyclic graph, DAG)及 Ring 方式建構 BC，加快 BC 的存取速度。

DAG 架構的區塊鏈以流言協議(gossip protocol) 演算法，讓區塊鏈可以使用非同步通訊以提升交易速度，但非同步通訊會造成一致性不可控，在[2.7]中，作者克服此問題達成非同步的聯合學習系統，然而基於DAG 的區塊鏈的交易時不可控，有可能導致本實驗無法由區塊時間確認模型順序而無法聚合，且尚未經過大規模測試，無法保證未來可以持續存在，因此並未採用。

✓ 2.7 Shuo Yuan, Bin Cao, Yao Sun, and Mugen Peng. Secure and efficient federated learning through layering and sharding blockchain. arXiv preprint arXiv:2104.13130, 2021.
✓ 2.8https://www.researchgate.net/publication/344802472_GFL_A_Decentralized_Federated_Learning_Framework_Based_On_BlockchainMajeed

而[2.8]的作者則以一致雜湊 (consistent hashing)演算法將 BC 節點的存取順序以 Ring 的方式排序，但在6G 行動網路複雜的無線網路環境，無法滿足作者的假設，或需增加額外的處理，因此在此次實驗中也未採用，而提出如圖127所示之架構。

在圖127中發起工作，可以在第三方主機或是聯合學習的節點，訓練完成的模型要上鏈，都需大部分節點同意，也就是達成共識。

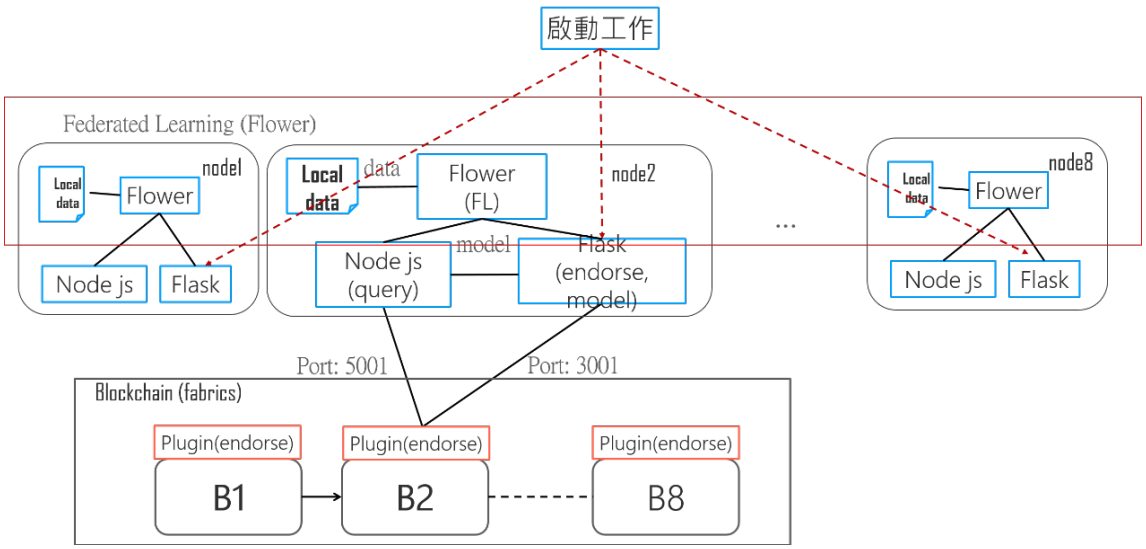


圖127、BCFL 實驗架構圖

資料來源：本計畫整理

✓ 2.8https://www.researchgate.net/publication/344802472_GFL_A_Decentralized_Federated_Learning_Framework_Based_On_BlockchainMajeed

在此次實驗，結合區塊鏈及聯合學習兩種架構，除上述區塊鏈系統外，還以 Flower 套件[2.10, 2.11]組成聯合學習系統，與前述區塊鏈相同，此次實驗也建置八個節點，並包成 WEB API 形式，方便第三方主機發起聯合學習流程，目前發起的主機依然是桌上主機，不過所使用的 Flower 套件已經找到如何移植 Android 的方法[2.26]，但還有一些技術問題未解，計畫未來會將啟動工作測試平台移植到手機平台。

3. 模型更新中毒(Model Update Poisoning)減緩機制

聯合學習應用中，依據攻擊目標的不同，可以將對抗性攻擊大致分為兩類，即 Untargeted Attacks 和 Targeted Attacks[2.9]。

Untargeted Attacks 的目的是破壞模型，使模型無法達到最佳效能。Targeted Attacks(又稱為 Backdoor Attacks)的目的是讓模型只在某些特定的子任務中表現出較差的效能。

✓ 2.9 Abdulrahman, Sawsan & Tout, Hanine & Ould-Slimane, Hakima & Mourad, Azzam & Talhi, Chamseddine & Guizani, Mohsen. (2020). A Survey on Federated Learning: The Journey From Centralized to Distributed On-Site Learning and Beyond. IEEE Internet of Things Journal. PP. 10.1109/JIOT.2020.3030072.
✓ 2.10 https://flower.dev/blog/2021-12-15-federated-learning-on-android-devices-with-flower/
✓ 2.11 https://flower.dev/
✓ 2.26 https://federated-learning.org/fl-aaai-2022/Papers/FL-AAAI-22_paper_29.pdf

由於 Untargeted Attacks 會降低主要任務的整體效能，因此更容易被發現。而攻擊者的目標往往是事先不知道的，Targeted Attacks 則較難檢測。

(二) 研析結果

1. 實驗規劃

(1) 結合 BC 與 FL 技術，建立 FL 流程

就目前收集的資料所知，目前全球電信業者相關於區塊鏈的實作計畫主要是為了解決現存問題，如呼叫詳細記錄 CDR 系統引起的計費糾紛，以及實現更高效、即時和無縫的電信事業間漫遊流程，而與分散式運算無關。但這背後的技術內涵為零信任架構，即是人或機器不需事先在電信業者或網際網路服務提供商註冊，就可取得服務或查詢自己的資料，而這種不需預先建立信任關係的概念若用於各方共享資料，可將6G 環境中大量的移動裝置所產出之具有隱私敏感且多維的數據釋出，進而滿足 AI 技術需要大量訓練資料的需求，因此已有許多學術研究探討 BC 與 FL 的結合，但就目前所知，多數學術研究則集中於提升 BC 存取速度，直到近期才有論文探討 BCFL 以智慧合約自動化 FL 工作，用於建立公開的資料

市集。讓開發人員、數據科學家和 AI 工程師可以在市集中發布他們的模型並協助其他用戶使用市集的資料集建立模型，但此資料市集直接分享資料也缺少資料安全/隱私保護方面的說明，若要應用於6G 行動網路資料共享的情境還需補強。因此，在本計畫結合 BC 與 FL 兩種技術，建立 FL 之流程，分述如下：

A. 用戶使用本地資料訓練本地模型，並上傳模型到 BC，上傳前 BC 會利用共識機制讓每個節點檢查模型參數，以避免模型更新中毒，若達成共識則此模型參數就可進入區塊鏈。

B. 用戶使用 BC 所提供的資訊，查詢適當的模型參數，進行更新/聚合全域模型。

在此次實驗的交易內容是儲存節點產出的模型，因此共識層不同於上述的方式，而是以估算節點產出模型與本地資料產出模型的相似度，當相似度小於某臨界值則達成共識。達成共識所需程式在實驗中稱為 Plugin(節點插入程式)，也稱為背書(Endorse)程式，程式內容除了為達共識的計算流程，還可加入一些商業邏輯，如回饋貢獻模型的使用者一些獎勵，如

圖128所示。

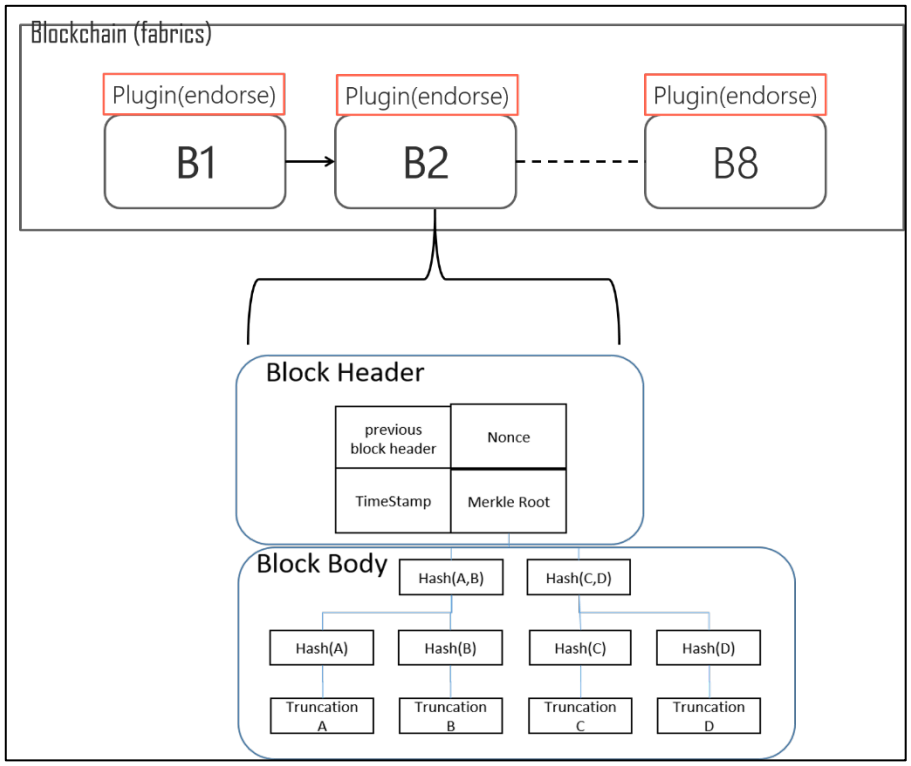


圖128、區塊鏈示意圖

資料來源：本計畫整理

本工作項目即是以 Hyperledger Fabric 建置計畫所需的區塊鏈系統。區塊鏈實驗系統具有八個節點的網路，如圖129所示。圖129下方是實驗區塊鏈以 Hyperledger Explorer 所呈現的現況，目前有8個節點組成，已經紀錄1,169筆紀錄，紀錄內容如表37所示，而 Chaincode 則是進行共識流程所需程式，這就是圖129上方的 Plugin(節點插入程式)，目的是讓所有節點評估上傳模型是否可以記錄到區塊鏈，而實驗的節點插入程式讓節點以本地的資料輸入到上傳模型，及自行訓練的模

型得到兩個正確率輸出值，當兩值的差小於事先設定好的臨界值則認可，當多數人都認可就是達成共識，上傳模型就可以進入區塊鏈。

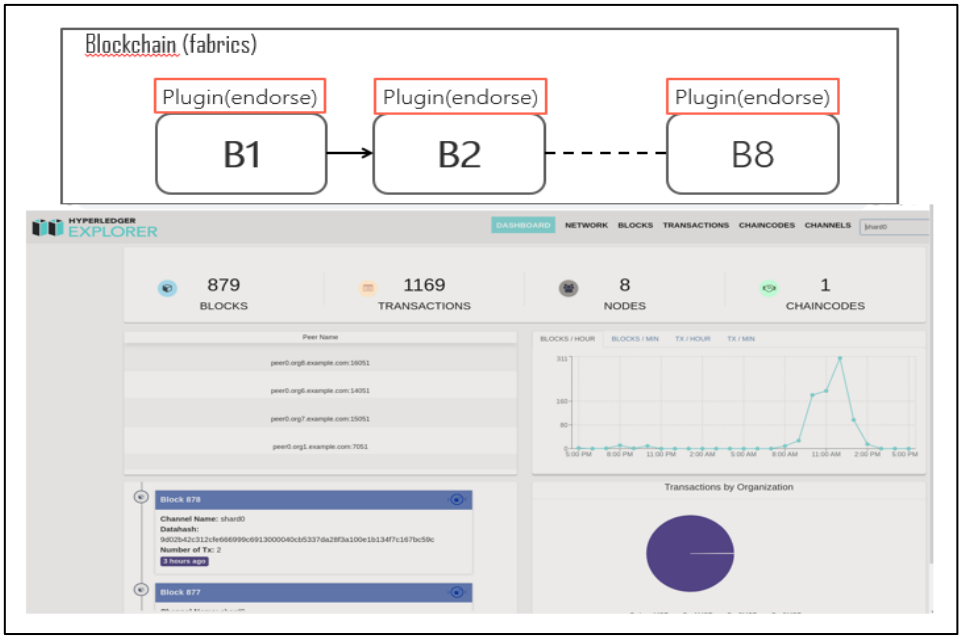


圖129、區塊鏈系統圖

資料來源：本計畫整理

在此實驗，主要紀錄的內容有模型參數，模型參數摘要值及正確率等，可用於事後的訓練流程，在本實驗設計中，區塊鏈可視為輔助的角色。表37則是紀錄項目相關註解。

表37、區塊鏈紀錄項目表

項目	型態	註解
模型摘要值	文字串(String)	模型參數摘要值，長度為64位元，用於確認模型參數是否被更動
模型參數	文字串(String)	模型參數以文字串形式存放，本實驗產出得模型約2M位元
測試正確率	正數(int)	
模型參數數量	正數(int)	
差分隱私預算	浮點數(float)	差分隱私的參數，參數大小會影響正確率

資料來源：本計畫整理

此次實驗假設所有 Local data 都類似，因此在區塊鏈的節點插入程式放入這樣的檢查邏輯，只要放入區塊鏈的模型，日後取出只要檢查模型摘要值，就可以有某種程度安全的保障，也可減少日後的存取延遲。未來，可以考慮將更新的檢查機制放入區塊鏈的節點插入程式，提高系統安全。

無論 Untargeted Attacks 或 Targeted Attacks，在6G 行動網路應用 FL 的情節中都有可能發生，因為用戶不只使用模型，也會參與模型訓練，用戶可能是蓄意更新惡意參數，也可能不小心設定錯誤，這需要系統有模型過濾政策。而此次實驗即是將檢查機制放入區塊鏈的節點插入程式，保護整體系統安全。而實驗的節點插入程式，是讓節點以本地的資料輸入到上傳模型及自行訓練的模型，得到兩個正確率輸出值，當兩值的差小於事先設定好的臨界值則認可，當多數人都認可就是達成共識，上傳模型就可以進入區塊鏈。

由上述可知，BCFL 實驗架構圖可以用模型參數取代資料分享，但是在6G 行動網路包括多種異質的網路，時間延遲有可能會影響 FL 效能，因此就這兩個保護機制產生的延遲進行探討，希望可做為未來 BCFL 架構移植到6G 環境的參考。

(2) 測試環境

為了探討如 BCFL 實驗架構圖中產生的延遲時間，以下面的配置環境設計此次實驗：

A. 作業系統: Ubuntu 20.04

B. 硬體：AMD Ryzen 9 5900X 12-Core Processor、64GB RAM、NVIDIA GeForce RTX 3090

C. 軟體：PYTHON 3.9、PYTORCH1.13.0、opacus 1.2.0、Flask 2.0.2

D. 區塊鏈網路: Hyperledger Fabric 2.3.3

E. 聯合學習系統: flwr 0.17.0

(3) 實驗系統架構

此次實驗使用主機模擬行動邊緣計算 MEC 裝置。在真實的環境下，MEC 裝置的計算和傳輸資源有大有小，而本次實驗的假設是，有8個資源不受限的 MEC，每個 MEC 分別安裝 Flask 伺服器及 Hyperledger Fabric 節點，構成 BCFL，即是以 MEC 群集同時架構聯合學習系統及區塊鏈群集，其中 FL 系統以 Flask 包裝成簡易的 WEB 伺服器，提供三個 WEB API：

A. FL_start_train：以 local data 開始 FL 訓練程序，訓練會呼叫 BC 寫入模型參數函數，此時寫入模型參數函數呼

叫其他其他 BC 節點會以背書程序(Endorsement Plugin)檢驗模型，若達成共識則將模型寫入區塊鏈。

B. FL_evaulate_model：此 API 接收到模型，會以 local data 評估模型是否接受，這是假設其他節點的資料與 local data 會互相類似，應該不會相差太多。

C. FL_query_model：以 model 的摘要值透過 Hyperledger Fabric API 查詢模型(model)。

透過任一 MEC 裝置，客戶端可使用 WEB API 發起 FL 工作程序，FL 工作流程中，MEC 寫入模型至 BC 前，需要呼叫其他 MEC 的 FL_evaulate_model，只有達成共識的模型才可寫入模型到 BC，當所有的 MEC 的模型都可以寫入模型到 BC，FL 的聚合動作會在發起的 MEC 裝置啟動將所有 Local Model 聚合成 Global Model，如圖130所示。在實際的運作中，區塊鏈紀錄項目可加入模型的相關描述，如日期、地點及模型組態，客戶端可以查詢模型再聚合出 Global Model，來得到最符合現狀的服務，如自動駕駛，而這服務可以用去中心化應用程式(Decentralized Applications, DApps)呈現。

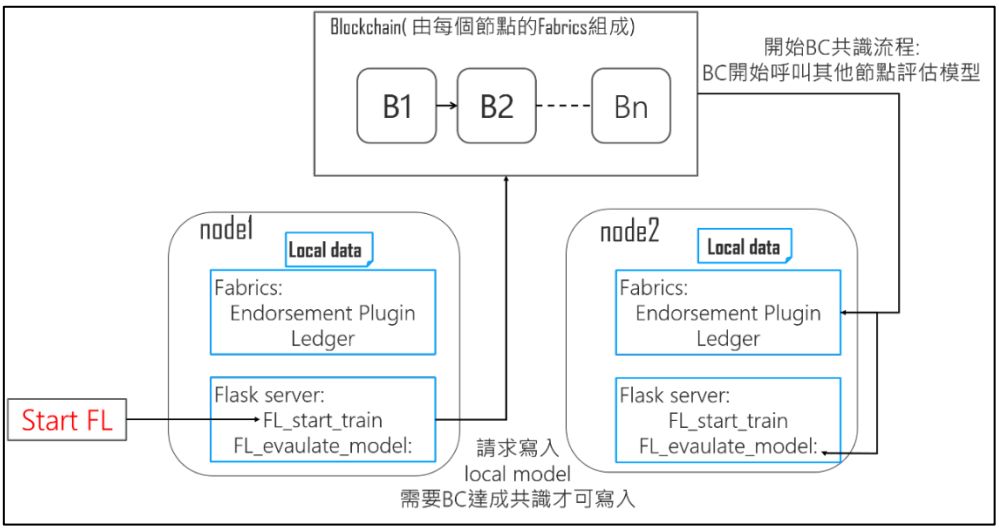


圖130、系統流程圖

資料來源：本計畫整理

BC 的節點會事先安裝背書程序，此程序會依照模型過濾政策決定模型參數是否可寫入區塊鏈，而本計畫的背書程序會呼叫 FL_evaulate_model 進行模型評估。整體的系統架構圖131。以 MNIST 手寫數字辨識資料集 (Modified National Institute of Standards and Technology, MNIST)為資料集，所提的 BCFL 方法與傳統 FL 做比較。延遲時間是以三台主機發送訓練工作，計算每個工作的平均執行時間，實驗顯示分散工作可以減少執行時間。實驗方式如圖132所呈現，使用裝有聚合(Aggregation)程式的三台主機(host1~host3)，發送主機(如host1)同時對所有聯合學習節點發送工作，最後的聚合工作就在原發送主機，其中單一主機發送工作到6個後就無法執行，因此只顯示部分結果如圖133所示。

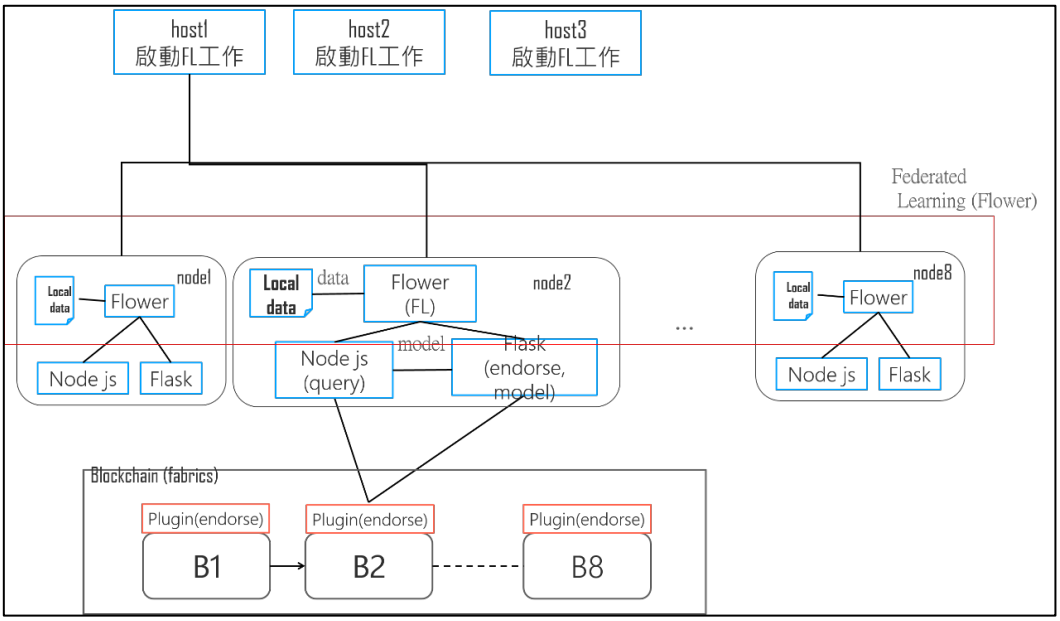


圖131、實驗架構圖

資料來源：本計畫整理

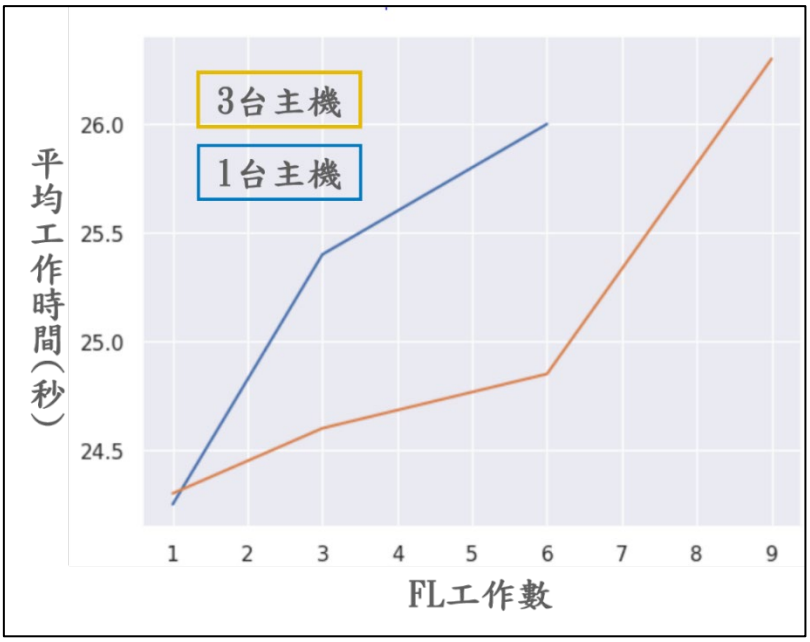


圖132、平均執行時間圖

資料來源：本計畫整理

(4) 測試目標

此次實驗探討的延遲時間為區塊鏈完成共識產生的延遲，及依照差分隱私方法在模型參數加入雜訊後增加的訓練時間，兩個測試目標說明如下：

A. 區塊鏈完成共識產生的延遲：實驗所使用共識機制，是以估算節點產出模型與本地資料產出模型的相似度，即是以本地的資料輸入到上傳模型及自行訓練的模型得到兩個正確率輸出值，當兩值的差小於事先設定好的臨界值則認可，當多數節點都認可就是達成共識。為了達成共識，BCFL 節點需要額外時間進行模型推論(Model Inference)計算。而需要幾個節點認可，則可以設定在區塊鏈的智慧合約。若未來採用許可式區塊鏈，可以減少達成共識的節點數以減少延遲時間，因此，先就節點數對延遲時間的關係作探討。

B. 模型參數加入雜訊後增加的訓練時間：為了避免攻擊者由模型推論出原資料，此次實驗設定每個 FL 節點會以 opacus 套件加入雜訊，在實驗中發現加入雜訊後，需要更多回合的訓練模型才會收斂。因為實驗設定每個 FL 節

點都會加入雜訊，隨著節點增加，訓練時間也會增加，由於在某些環境下，可以只在聚合階段加入雜訊，因此探討此延遲時間做為未來設計的參考。

2. 實驗結果

此次實驗使用 FL_evaulate_model 所描述的方法減緩 MEC 的模型更新中毒，還在訓練階段依照差分隱私方法在模型參數加入雜訊，防止攻擊者由產出模型推論出原始資料，由圖133可以看出加入雜訊會引響模型收斂的速度，增加訓練回合數。

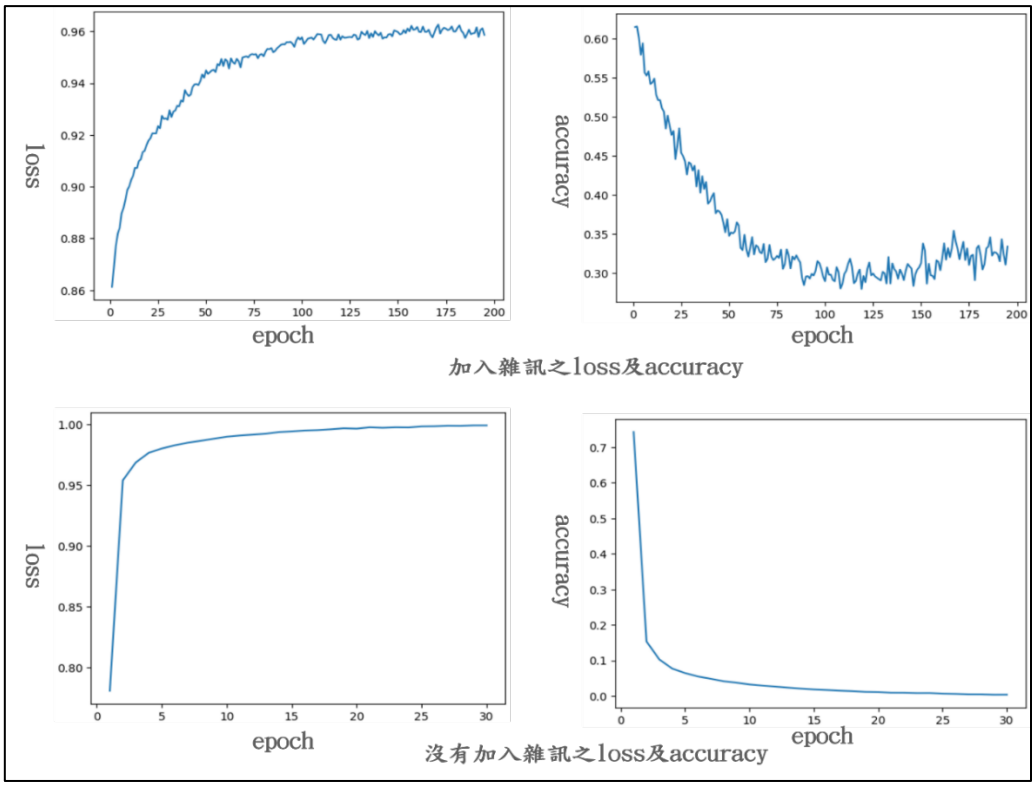


圖133、損失及正確率比較圖

資料來源：本計畫整理

圖134呈現 BCFL 加入雜訊的情況下，延遲時間將增加，此數據是在三台主機同時發出 FL 工作的平均延遲時間。

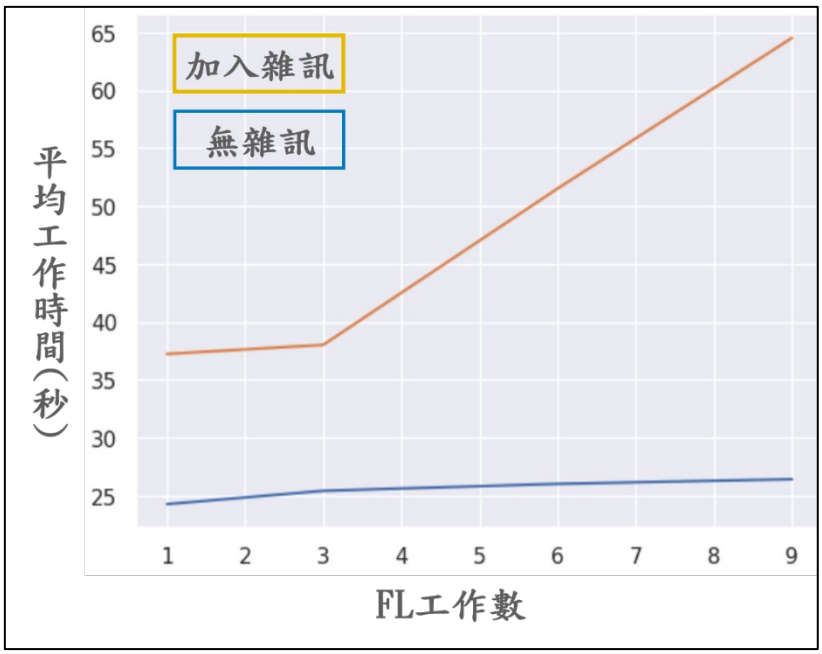


圖134、BCFL 有/無雜訊之平均執行時間圖
資料來源：本計畫整理

圖135是將 BC 節點數進行變更，再於同一主機發送 FL 工作所紀錄的工作時間。由圖135可觀察到，BC 節點數減少可以降低延遲時間。

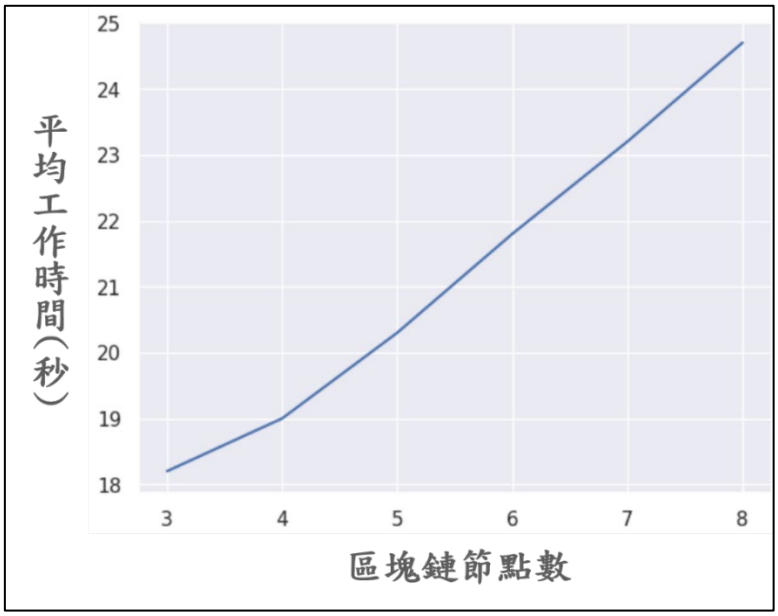


圖135、不同區塊鏈節點數之 FL 工作執行時間
資料來源：本計畫整理

表38整理 FL 與 BCFL 正確率的比較，其中 Epochs 是訓練 Local Model 所設定的 local epoch 與 FL 所設定之回合數(round number)的乘積，即是 Epochs=local epoch x round number。

表38、正確率比較表

Batch size	Epochs	FL正確率	BCFL正確率
10	1	0.8781	0.984
10	5	0.9512	0.9897
10	15	0.9654	0.9895
20	1	0.725	0.9759
20	5	0.9251	0.9882
20	15	0.9545	0.989

資料來源：本計畫整理