財團法人電信技術中心出國報告

出席 2019 全球行動通信系統協會行動通訊大會（2019 GSMA Mobile World Congress）

單位名稱：檢測暨網通技術組、資通安全組

姓名職稱：李贛麟工程師、李兆文工程師、吳東興高級工程師

派赴國家：美國

出國期間：2019/10/20-2019/10/27

報告日期：2020/1/27

摘要

2019 年 10 月 22 日至 24 日於美國洛杉磯舉辦之「2019 年世界行動通訊大會（MWC19 Los Angeles）」，本次大會主題為「智能連結（Intelligent Connectivity）」，本團隊參加 MWC 展覽會議，藉由會中電信業者、設備製造商、服務應用提供者、政府機關等組織單位分享經驗，汲取美國在 5G、IoT 物聯網、以及電信安全發展之最新技術及趨勢，並將此次參訪所獲得之最新資訊與成果紀錄於參訪報告中。

今年 MWC 展場最令人驚艷的為許多 5G 的具體實現，展覽會場上展出許多 5G 的設備從晶片、手機、基地臺、到核心網路及網路技術解決方案，並透過眾多 5G 場域的垂直應用體現，以及物聯網應用結合人工智慧(AI)，除展現今年大會智慧聯接(Intelligent Connectivity)的主題，讓各界參加者可藉由各種展出思考未來可能的商業模式與發展。在此引述 GSMA 執行長洪曜莊(John Hoffman)的談話，他表示「行動產業觸及全球數十億人的生活，隨著 5G 到來，它將再次改變全球消費行為和商業模式。MWC19 洛杉磯將展示橫跨整個產業的龐大生態系統和鄰近產業的一系列最新行動科技的變革用例，探索當今的新可能性。」

內容

壹、　目的

本次前往美國洛杉磯參與參加 MWC Los Angeles 論壇會議，主要是邀關注美國在 5G 上的發展趨勢，並鎖定相關技術發展之資安議題，調查美國最新政策作為或防護指引。本次 MWC 19 LA 的參與者主要來自歐美地區，亞洲廠商偏少，且中國品牌的 5G 設備供應商並無出席。近兩萬名與會者共同探討 5G 行動行業和更廣泛的生態系統的主要趨勢。本次出國行程主要目的包含：

參加 MWC19 Los Angeles 論壇會議，了解全球各國際組織、官方單位、國際電信設備製造商、大型跨國電信業者等專題演講、就 5G 技術、垂直應用專網、物聯網應用服務、以及資安議題，包含邊緣運算 MEC、網路虛擬化、網路切片、開源端對端設備、智慧城市應用、領域知識及商業模式進行資料收集與了解。

參觀 MWC19 Los Angeles 各電信設備廠商或垂直應用服務業者之展示攤位，蒐集全球最新主流之通訊技術、應用服務及商業模式等相關資訊。

貳、 行程

一、 出國時間：108 年 10 月 21 日至 10 月 27 日

二、 地點：美國洛杉磯

三、 本中心出席人員：李贛麟工程師、李兆文工程師、吳東興高級工程師

四、 時間安排：

日期	行程
10 月 20 日(日)	差旅時間：臺北－洛杉磯 桃園機場 10 月 20 日 19:20 出發 洛杉磯國際機場 10 月 20 日 16:20 抵達 （臺灣時間 10 月 21 日上午 7：20）
10 月 21 日(一)	調整時差、會議準備
10 月 22 日(二)	2019 洛杉磯世界行動通訊大會 MWC 三日議程
10 月 23 日(三)	
10 月 24 日(四)	
10 月 25 日(五)	整理會議資料
10 月 26-27 日(六-日)	差旅時間：洛杉磯－臺北 洛杉磯國際機場 10 月 26 日 00:50 出發 （臺灣時間 10 月 26 日下午 15：50） 桃園機場 10 月 27 日 05:45 抵達

五、會議資訊

(1) 會議名稱：2019 洛杉磯世界行動通訊大會（MWC）

(2) 2019 MWC Los Angeles 展覽會場資訊：

https://www.mwclosangeles.com/conference-programs/agenda/#day=1799

(3) 會議時間：108 年 10 月 22 日至 10 月 24 日

(4) 會議地點：洛杉磯會議中心（Los Angeles Convention Center）

(5) 會議議程：

除了主題演講活動之外，MWC19 洛杉磯大會還推出 27 場數位轉型相關的專題活動，以 5G、物聯網(IoT)、人工智慧(AI)和沉浸式內容為四大主題。主題具體內容包括：

圖 1 2019 洛杉磯世界行動通訊大會四大主題

- 5G：經濟學、邊緣運算、工業物聯網、頻譜和網路切片 。
- 物聯網：運輸、協作智慧和安全。
- 人工智慧：倫理觀、區塊鏈、顛覆性創新和資料分析。
- 沉浸式內容：擴增實境/虛擬實境(AR/VR)、現場表演、內容創作、發行、遊戲、運動和娛樂等主題領域。

參、 會議過程及內容

以下就主要展場參觀及交流、參與場次分別重點介紹：

一、主題演講（Keynote）

(1) 技術長們對 5G 之看法

AT&T 技術長 Andre Fuetsch 宣示，公司將全力以赴為企業組織提供 5G 服務。Fuetsch 表示，我們認為 5G 最大宗之用戶將會是公司企業，而且我們正在進行數十項測試來證明這一點。Fuetsch 敘述，5G 多接取邊緣運算（Multi-access Edge Computing, MEC）技術在智慧工廠上扮演重要角色，例如能完成生產線上所有產品之數據即時收集、分析、傳輸，這主要依賴於 5G 增強型行動寬頻通訊（Enhanced Mobile Broadband, eMBB）之實現。Sprint 技術長 John Saw 針對他們的競爭對手 AT＆T 和 Verizon 電信業者悠然自得的評論，AT＆T 以及 Verizon 都在毫米波（mmWave）上推出了 5G 的服務，但是他們忽略了覆蓋率這個關鍵問題。然而，Sprint 的優勢在於我們擁有全國最大的 5G 覆蓋範圍，我們的行動客戶在城市中任何地方都可以體驗 5G 網路的快速服務。T-Mobile USA 技術長 Neville Ray 強調 T-Mobile 計畫將在今年年底之前為 2 億人提供 600 MHz 頻段之使用覆蓋率，而且會找尋可以使用於該頻段並具相容性之行動網路設備，預計在 5G 網路開臺之前就會公布所使用之 600MHz 行動網路設備。行動網路設備運營商在今年初已經在 28 GHz 和 39 GHz 毫米波頻段中提供一些相關的 5G 應用服務。Verizon 資深副總裁兼首席網路官 Nicki Palmer 談論到，Verizon 的 5G 服務即將來臨，將會在 2020 年正式提出商用 5G 獨立（Standalone, SA）網路解決方案。5G SA 關鍵基礎設施架設就是 Verizon 未來發展方向，我們會儘快實現。Verizon 對 5G SA 的商用化非常重視，因為 5G SA 網路能夠實現才能真正展現 5G 網路服務的快速特性。

(2) 加速美國創新－國防部 5G 契機

美國國防部（United States Department of Defense, DoD）透露了目前正在評估 5G 實驗並尋求建議，同時計畫在許多軍事基地啟動 5G 測試平臺的計畫，DoD 將與民營公司夥伴合作進行大規模實驗。國防部副部長 Dr. Lisa Porter 在發表演講時說；「國防部認為，掌握無處不在的網路連結將使軍隊維持與對手的競爭優勢。」但她也補充說明選擇 5G 並非是最終的決定，而是保持「我們將永不辜負我們與持續創新的承諾」，與民營企業和整個政府的合作夥伴進行合作。

此外 Lisa 還強調了 5G 的安全性試驗：「我認為最大的挑戰是我們想確保我們真正了解 5G 的潛在弱點（Vulnerability），例如使用 5G 可能暴露用戶的位置，將用戶的服務降級到舊的行動數據網路，大量增加用戶的無線網路賬單，甚至追踪用戶打電話、發短訊、瀏覽網頁之記錄。國防部真的想與業界合作，以確保我們儘早了解 5G 技術及安全性的發展，並開始推動大眾對行動數位化時代的安全性重視。」國防部預計將在今年 2019 年末時候開始宣布測試地點和用例，並根據當年度可用預算，進行各季預算調配，與民間企業進行合作，確保 5G 對國防之可用性及安全性。

二、政策演講（Everything Policy）

(3) CISA 總監 Christopher Krebs 主題演講

美國國土安全部新成立的部門主管認為美國在 2016 年的大選中所遭到的網路安全事件，使得美國民眾開始把網路安全視為重要的事情，美國人民意識到網路安全的風險與攻擊，不僅僅是破壞銀行或商業公司，亦有可能動搖了美國人的生活方式並且造成政府動盪。所以主講人的單位開始與國會以及其他的聯邦機構合作與對談來應付目前的情況。除了政府機關煎的合作，也需要民間更廣泛的參與，達成風險識別和解決方案的整合，也就是說 CISA 將進行合作式風險管理和風險分析，共享資訊，並以公私協力聯繫以幫助管理風險。主講

人認為若要達成上述願景，需要有四個支柱，第一個支柱是確保和提高美國關鍵基礎設施的強韌性。第二個支柱是與聯邦機構合作，以增強防禦態勢。第三個支柱是創建可互通的緊急通信，而第四個是長期風險管理。最後主講人提到他們今年已經與其他聯邦機構展開工作，並對聯邦政府的 ICT 供應鏈安全作出指導建議。

(4) 保護新興的 5G 網路

主持人首先提到關於近期美國聯邦政府所組織的 ICT 供應鏈風險工作小組(Information and Communications Technology Supply Chain Risk Management Task Force)的完成工作與目前情況。由來自美國國土安全部(DHS)的 Robert Kolasky 回答，Kolasky 表示這是一個跨機關的工作小組，這個工作小組本身沒有特定的法定職權去決定任何事情，但 DHS 有建立公私合作的職權，它所做的事情是把利害關係人都聚集在一起，包含政府機關與私人公司，這個工作小組會指導各聯邦政府機關如何降低供應鍊風險，他認為這樣展開對公共政策的對話做法是相當合適與聰明的。

該工作小組第一年的成果是已經建立一些模組，這些模組有些可以展示供應鏈目前有哪些威脅與風險，也有的模組是進行情資分享，特別是從情報部門來的情資，另外有些模組是針對如何進行軟硬體設備的採購。透過這樣的模組框架，聯邦政府除了可以對各模組進行整合外，聯邦政府可以大量採用這些模組，這也有助於情資分享。小組的另一個工作成果是該工作小組列出好幾種關於供應鏈的風險情境，把威脅進行分類，也針對業務需要進行分類，同時也列出資安防護的最佳實務。

(5) 內部的無線政策：FCC 顧問的觀點

FCC 的 Rosenworcel 委員辦公室，無線與國際法律顧問 Umair Javed 描述，Gartner 於分析新興技術發展週期中提到，大家對 5G 的期望都太高，原因是許多電信業者還無法確認 5G 核心業務到底為何，5G 網路將如何推動並提供新形

態的產品和服務，以滿足消費者心中真正想要的價值與渴望。關於中頻帶頻譜，FCC 僅在致力於如何通過高頻段頻譜市場化，以支援 5G 無線網路之應用服務。然而，將高頻段頻譜商業化並不容易且價錢不會更便宜，瞭解企業和消費者真正需求將會比密集化網路部署更為重要。

FCC 的 Pai 委員辦公室無線與國際法律顧問 Aaron Goldberger 說明，新型態的 3.5 GHz 頻譜共享概念，反映了小型和大型的電信營運商、設備商、第三方應用服務供應商的高獲利營運模式，且能改變軟體開發商、晶片製造商、手機與設備製造商之商業經營方式。我迫不及待的期望能看到這種新形態企業組織之組成，且多元化聯盟的合作成果能夠成功。

FCC 的 Starks 委員辦公室幕僚長兼無線與國際資深法律顧問 William Davenport 陳述，今天我要傳達的資訊是在技術上的解決方案，是有機會幫助與解決世界上最重要的關鍵問題。5G 網路的啟用帶來新挑戰，並可讓我們用來克服相關難題。5G 網路將連結數十億個設備，讓能源使用更有效率，並降低對國家、地方及當地環境的影響。

圖 2 政策演講 Everything Policy 議程 - 內部的無線政策：FCC 顧問的觀點

三、5G 演講

(6) **5G 營銷：從速或從優進入市場？**

與會中專家們探討了行動網路技術中之先發優勢的歷史、其在 5G 無線通信中的運用、最佳市場的地位以及對消費者、用戶及企業的利益之真實意涵。專家們提出 5G 還處於初期階段，但電信業者已經看到了一些值得注意的地方以及商業網路之利益。5G 網路不僅會提供更快的速度且新技術將提供使用新的高頻寬和高容量結構。高頻頻段亦將有助於減輕頻段擁塞影響了整個行動網路之消費者體驗。而且 4G 升級不僅會體現在速度上，5G 也會大大改善了延遲，創造了一個全新的世界行動應用服務場景，但是要普及到 5G 需要很長時間。

圖 3 5G 演講議程 - 5G 營銷：從速或從優進入市場？

(7) **偏鄉地區之連接：商業模式是否存在？**

American Tower Corporation 垂直市場副總裁 Steve Baker 認為，對於行動網路之鄉村地區的連通性是非常大的挑戰，電信業者必須了解鄉村地區消費這對於 5G 網路之服務需求是什麼，是要將 5G 網路服務品質提升至城市地區的水準，還是能讓鄉村消費者有超越城市環境之使用體驗?不管鄉村地區或城市地

區，只要消費者有所需求就要部署 5G 基礎設施與其使用。在網路之有效利用上並符合電信業者經之營利條件，5G 新技術之軟體無線電（Software Defined Radio）與頻譜共享是可以考慮運用的。

圖 4 5G 演講議程 - 偏鄉地區之連接：商業模式是否存在？

(8) **5G：力量、全球、利潤**

Cisco 服務提供者業務資深副總裁兼總經理 Jonathan Davidson 描述，Cisco 的精神在於公司的責任就是社會的責任，以積極力影響人類、社會及地球，並加速解決全球問題。在傳輸能量消耗上的創新突破，Cisco 研發的技術在傳輸相同的資料量下，一直持續降低能量耗損，從 2009 年的 10Watts/ Gbps 變成 2019 年 0.2Watts/ Gbps，足足降低了 50 倍的耗損，進而達到保護環境的政要關鍵技術。服務提供商面臨的經濟挑戰上，包括 5G、數位影像、雲端等服務，其 CAPEX 的 Exabytes / month 從 2007 年的 12MBpm 一直持續增加到 2018 年的 230MBpm。Cisco 5G 提供了一種開放的、高度可編程的架構，可將企業、供應商、消費者之多域網路精簡為一個精簡、快速、統一的系統。Ericsson 持續發展與企業責任副總裁 Heather Johnson 描述，Ericsson 敢於領導並兼具設計力量，幫助服務提供商突破可能的極限，使 5G 栩栩如生。在專注力的設計概念上，透過提高

生產力、娛樂性、沈浸式遊戲的新水平來提升消費者的遊戲水平。將高速連接與低延遲相結合，超優質的解決方案使消費者能夠提供令人難忘的獨特用戶體驗。考量更有效率的設計，城市無線傳輸方案和室內解決方案可為消費者提供廣泛而密集的高訊號品質的覆蓋範圍。每一位消費者都能賞受到一致性的傳輸以及 5G 核心服務之效能，以提供更快、更智慧、更可靠的網路服務。在消費者實際運作上，透過為企業與消費者所配備的智慧、可擴展、靈活的物聯網解決方案，以超高速和高彈性之連接來增加公司之營收。Spirent Communications 5G 業務主管 Stephen Douglas 接下來描述，Spirent 一直致力於發掘電信運營商在 5G 中取得成功所需的測試和保證解決方案，我們一直在探討在智慧連接的概念上，如何讓 5G 實現並讓企業與消費者有著真實體驗。然而，5G 網路中的智慧連接會涉及到新的天線模組和晶片模組技術，進而完成新的架構、新的 KPI、新的供應商、雲分佈及新的頻率。因此，行動網路整個生命週期中的智慧測試和服務對於保證 5G 的成功實現至關重要。

圖 5 5G 演講議程 - 5G：力量、全球、利潤？

(9) **5G 網路：深入討論**

美國公司首席安全官 Andy Purdy 呼籲採用更全面的 5G 安全檢驗方法，以解決圍繞該技術的長期安全擔憂。同時希望 3GPP 應該著眼於針對不同應用服務的場景威脅建模研究，參考在歐盟和德國建立安全框架的類似工作，並加快對電信產品安全的通用測試標準和法規要求等協調制定工作。Purdy 指出，「到目前為止，在應對 3G 和 4G 時代的威脅方面，我們已經做出了一些安全性增強工作，這些作為讓人鼓舞，但是我們還有一段路要走。」他也建議國家管理機構需要對產業政策進行重新思考，因為舊的信任模型不再符合未來需要，我們正處在一個需要強化風險管理和增強抵禦能力的網路環境。「我們的想法是，透過與公私單位合作，以我們應該弄清楚作為一個設備供應商需要考慮什麼、做什麼、以及開展什麼研發，以符合國家的新監管模式。」

圖 6 5G 演講議程 - 5G 網路：深入討論

(10) 專用網路 vs 5G 網路切片

會議主持人 Besen Group 創辦人兼執行長 Alex Besen 指出，專用網路是針對消費者，企業和物聯網的獨立專用網路。專用網路需具備行動性、安全、高可靠度、足夠覆蓋、低延遲等主要特徵，至今已有超過 33%的工業製造廠商評估過 5G 專用網路，其中並有超過 46%開始進行研究專用網路的部署案例。

ASOCS 執行長 Gilad Garon 則以結合專用網路與網路切片技術的使用範例為題，強調以內網結合邊緣運算之專用行動雲將創造新的商機，舉出在包括手機/平板控制、影像追蹤、智慧機械手臂、無人機監控、智慧眼鏡等工業 4.0 上的多種應用，以及在運動賽事現場及企業分支機構的使用範例，並期待全球政府能對專網釋出免費或共享的頻譜。他說：「ASOCS 通過開放和虛擬化的軟體解決方案正在改變傳統的 RAN 市場，提供 4G 和 5G 的 LAN or WAN 的行動接取網路解決方案。我們的本地移動雲可通過現成商用的 IT 硬體，提供符合 ORAN 的解決方案，使電信業者及其客戶能夠享受更高水平的性能與可靠性，滿足關鍵任務和本地專用網路。」

座談會小組一致認為隨著大規模的 IoT、VR、AR、以及智慧工廠等多元化應用，將給目前行動通訊網路的效能與容量帶來巨大壓力。為了支援 5G 應用，電信業者需要提供具有網路切片，小型行動基地臺和覆蓋範圍等優勢的客製化 5G 服務網路，而這些量身定制，提供智慧連接時的私有網路興起也將會大幅改變電信業者的商業模式。

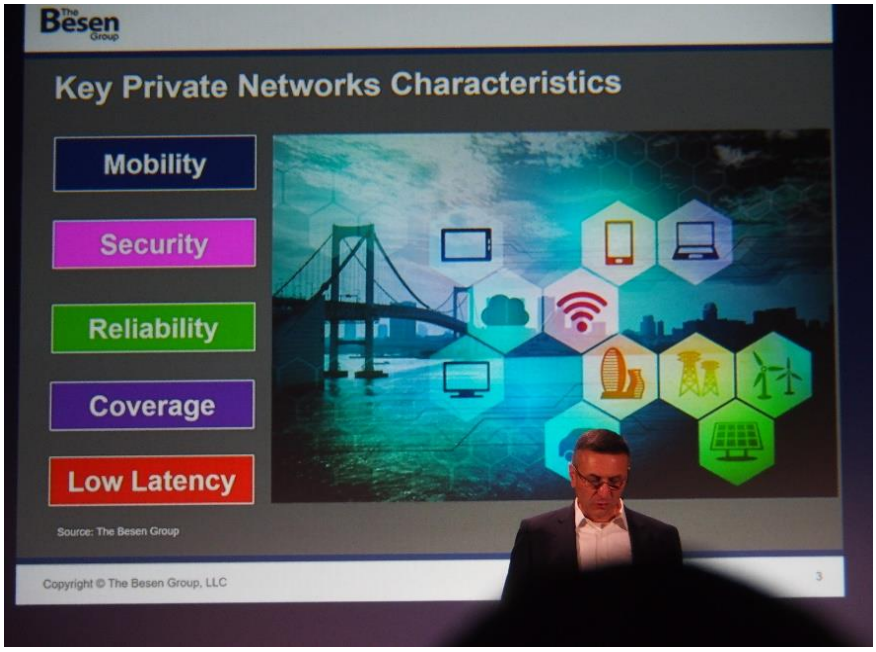

圖 7 Besen Group 提出之專用網路應具備之特性說明

(11) **5G 之網路邊緣**

主持人 GSMA 行動智庫主管 Peter Jarich 在座談會上提到，透過邊緣運算可以讓行動計算資源更接近數據來源，加上 AI 技術的利用可以降低延遲並減少傳輸量、提高容量和彈性；行動計算對邊緣設備的數據分析增加了系統的整體分析能力、獲得更好的安全性和隱私保護，同時處理數據越接近源頭可減少數據量及跨網路傳輸，降低了潛在攻擊面。

Akamai 物聯網及行動技術長 Lior Netzer 提及「Akamai 相信，我們正在提供具有可擴展性、操作簡便性和安全性的下一代資訊傳遞解決方案，以及一個可以讓客戶專注於核心業務的全包式解決方案，使得客戶無需集成和管理離散但必要的資訊傳遞元件。隨著 IoT 邊緣運算的推出，我們正在利用邊緣的力量並將其帶入由聯網設備和應用程序組成的下一個先進領域。」。

Altiostar Networks 策略及產品管理執行副總裁 Thierry Maupile 則表示，透過開放式虛擬 RAN 解決方案，客戶可以使用同類最佳的解決方案來部署其無線接入網路；這不僅可以實現硬體和軟體的分解，還可以使運營商實現一個平臺，從而可以部署微服務。這個新生態系統的關鍵基本方面之一是，它使服務提供商處於構建供應鏈，控制支出，安全性和自身移動網路集成的主導地位，而不是依靠一兩個供應商而已。

圖 8 5G 演講議程: 5G 之網路邊緣

(12) **保障 5G 策略不過時**

主持人 Price waterhouse Coopers（PwC）合夥人 Dan Hays 現場說明了 PwC 對 5G 迄今進展的分析，並預測了未來 6 個月的進展。隨著 5G 設備的問世以及更多市場上線，5G 部署可能是一個漫長的過程。他說「截至 2019 年 7 月 1 日的分析發現，我們才剛剛起步，不到 1%的美國人口在家中或公司可使用 5G 網路，而且使用的行動設備中只有不到 0.5%啟用了 5G。這兩個數據點的交集反映了美國 5G 市場。前面的路很長，而且在很多方面都比前幾代移動電話要復雜。展望到 2020 年 1 月 1 日的六個月，我們預測美國人口的 10%將獲得 5G 網路覆蓋，而 2%的設備將啟用 5G。」

VMware 執行副總裁兼電信與邊緣雲業務總經理 Shekar Ayyar 則樂觀表示:「5G 將是一種變革性技術，這使我想起了網際網路的早期，因為創新和提高成本效率的潛力是巨大的。」，隨後現場座談會成員並討論到由於既有技術的規範，建立 5G 網路不同於 4G；部署 5G 的成本非常高昂，它需要一個更高密度的網路，該網路面臨監管，成本和運營方面的挑戰，包括它需要非常大的頻譜網段，以及在全國範圍內安裝數十萬個小型蜂巢小區，而且目前消費者並不要求或願意為此付出更多的費用。

5G 保證高效能連接體驗，並改善我們享受多媒體娛樂，購買產品和服務甚至經營我們的家庭和企業的方式。但是理想用例遠非真實情況，行動營運業者需要努力使用戶願意使用 5G 消費，而且產業鏈參與者間的合作結盟仍未產生足夠的吸引力，並給創新帶來了新的障礙。

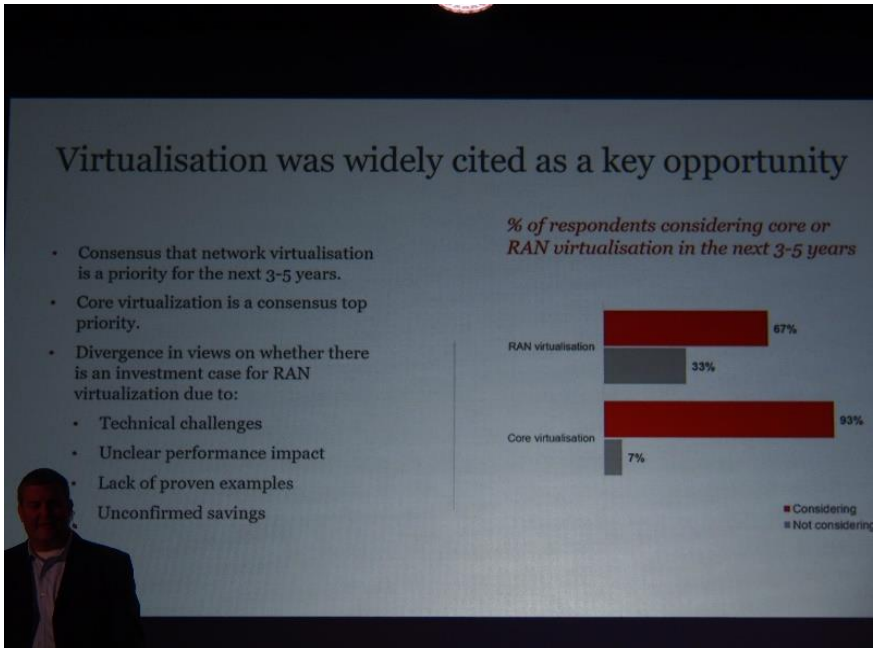

圖 9 PwC 提出之 5G 網路虛擬化預測趨勢

(13) 5G 對您的未來安全嗎？

主持人 GSMA 產業安全及技術主管 Jon France 提及，在 5G 時代，由於各項垂直應用將高度採用虛擬化與雲端化系統，加上全球資安威脅與攻擊手法與日俱增，強化行動通訊安全是愈發重要且需要被重視及落實，5G 標準在制定之初就帶來增強的安全性和隱私性的設計。

Nokia 安全副總裁 Mary O'Neill 則強調，5G 需要從架構的第一天開始就考量到安全性，而不是趕快大量部署才在後續對其進行修補；O'Neill 提醒電信業者需要趕快改變現狀，不再可以使用既有的解決方案來面對 5G 安全問題。她說：「我們需要更多的技術，當我為 Nokia 制定策略時，我們將投資於機器學習、演練腳本、工作流程，並且我們非常相信自動化可以改善此問題。」。

McAfee 首席消費者安全宣傳員 Gary Davis 也提及，5G 即將到來，隨之而來的是不斷變化的威脅格局，既有 Mirai 攻擊將透過大量 IoT 轉化成更具破壞力的 Reaper 殭屍網路；隨者 5G 將廣泛應用於生活各層面，越來越多的設備連上網路，提供更多更容易施展攻擊的管道，未來網路犯罪（Cybercrime）將隨著這波趨勢逐步成長且工業化。

Qualcomm 安全產品管理資深總監 Jesse Seed 則將焦點放在 IoT 的安全性議題；她說，2018 對 IoT 惡意攻擊就成長了三倍，因此在 5G 即將推出之時，隨之而來需要增強網路安全性；此外還需要強化終端安全性，在系統單晶片（System on a Chip）設計時就考慮進去，因為當前設備經常缺乏足夠的安全，同時也需要和為 IoT 終端推出國家法規及安全認證標準。

圖 10 Nokia 提出現今資安面臨新的挑戰

(14) 這是我們所熟知的行動終端嗎？

主持人 Mobile Ecosystem 常務董事 Mark Lowenstein 特別指稱：未來十年的行動通訊將與過去十年非常不同，包括 eMBB 外更具吸引力的服務與應用、執照與非執照的無線技術的混合、動態共享的頻譜、IoT 的爆發性、以及企業專網的契機，這也帶來很大的挑戰，包括能夠更快地部署的電信基礎系統、仍不

明確的商機與案例、企業的基礎架構將以多快的速度被替換？而又由誰付款？另外網路經濟學的透明度仍然很少、而且我們需要 1~2 個重大催化劑（就像我們使用 4G 一樣），以上這些仍有待探討及研究。

HarrisX 則著眼在探討智慧手機是否仍將在 5G 和物聯網世界中佔據統治地位。執行長 Dritan Nesho 說：「我們才剛剛開始掌握 5G 的力量和影響，這項技術有望比 4G 帶來更廣泛，更深入的發展。」,「我們正在推出 5G 情報平臺，以清晰並深入地了解無線和有線服務的業務主管，家庭主管以及訂戶對 5G 的期望，採用和經濟影響，並以此為基礎我們跟踪每種新一代電信技術反應的遺產。」。

HYLA Mobile 總裁兼執行長 Biju Nair 也總結如下：5G 首先將在發達經濟體中對我們的生活和工作產生積極影響，還將為其他設備創建用例；行動通訊設備將繼續在當前使用模式中扮演重要角色；其他設備（如 IoT）將繼續增長，並且可能許多設備將增強/替換傳統設備的特定功能；在新興經濟體（如印度）中，智慧手機的採用正在增長，在這些新興市場中，行動通訊將在數位化和經濟增長中扮演關鍵角色。最後他強調：智慧手機的未來還活著，並且在不久的將來仍會很好。

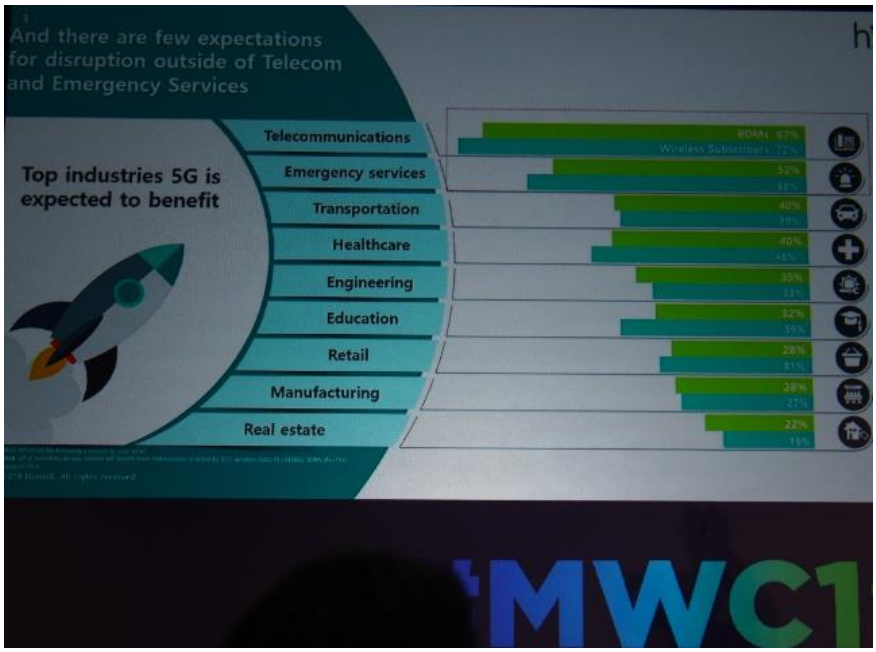

圖 11 HarrisX 預測未來 5G 的主要營收項目及比重

四、IoT 演講

(15) 擴展智慧物聯網

Deloitte 電信戰略與運營總經理 Phil Wilson 表示，IoT 發展已即將接近開始大規模部署的臨界點，但迄今為止，仍缺乏將傳統終端機器設備連結無線網路的殺手級應用仍尚未出現。

Ericsson 物聯網業務部技術主管 Kiva Allgood 強調進入 IoT 領域的業者應更多地關注應用服務成果本身。他說：「只關注技術驗證概念意味著您很少能夠擴展，當您這樣做時，您將到達臨界點。」

KORE 總裁兼首席執行官 Romil Bahl 表示贊同並指出他最初對與客戶的一些對話感到困惑。他說：「我對電信公司是陌生的，我來自於具有消費背景的應用服務產業。而這使我感到困惑，例如，當人們想談論天線的尺寸時，所需要的只是拿出可使用的終端連接體驗。我們可以說，任何技術的發展都越來越快，但我們同時也把它變得更複雜難懂了。」。

Cisco 網路副總裁兼首席技術官 Michael Beesley 則表示他並不認為 IoT 發展處於一個臨界點；但他指出目前連接機器和設備的應用價值需要有更多驅使加速動力，因為人們意識到了實際商業應用成果對所需技術配合的相對落差。

圖 12 IoT 演講議程：擴展智慧物聯網

(16) 邊緣計算：創造新的物聯網應用

主持人 GSMA Intelligence 主管 Peter Jarich 提及，5G 網路的演進路線讓實現萬物互聯成為可能；5G 網路切片（Network Slicing）技術將可依據終端應用需求，將網路「切開」給不同場景與族群使用，例如其低延遲特性可應用於要求零時差的工業控制需求，而高頻寬特性則可對應工廠內多媒體需求應用。

Corning 技術與市場開發經理 Karen I. Matthews 將物聯網應用的焦點放在工業 4.0，她指出工業 4.0 可以創造新的生產模式並大幅增加營收；達成工業 4.0 願景的背後是 IoT、Cyber-Physical、Systems、Fiber、以及 Deep backhaul 所組成的基礎架構，而 Fiber Deep 傳輸骨幹將能夠滿足巨量數據傳料流的傳輸承載。

IBM 全球業務服務總經理 Albert Opher 指出，新技術的發展將創造出新的商務架構，公司從傳統處理交易過程，演進到數位化企業，再進化為透過新技術轉變策略、產品、服務的認知型企業；這是一種學習型企業，由各種智慧平

臺的 ecosystem 所組成，其競爭力優劣取決於對及業務環境的轉變有多快的適應及反應力；其核心的工作流程和程序包括：導入專有數據資料，基於 AI、IoT 技術及區塊鏈技術，始終透過機器學習改進，轉變人機界面，整合 IT 和 CT 彈性處理服務數據。

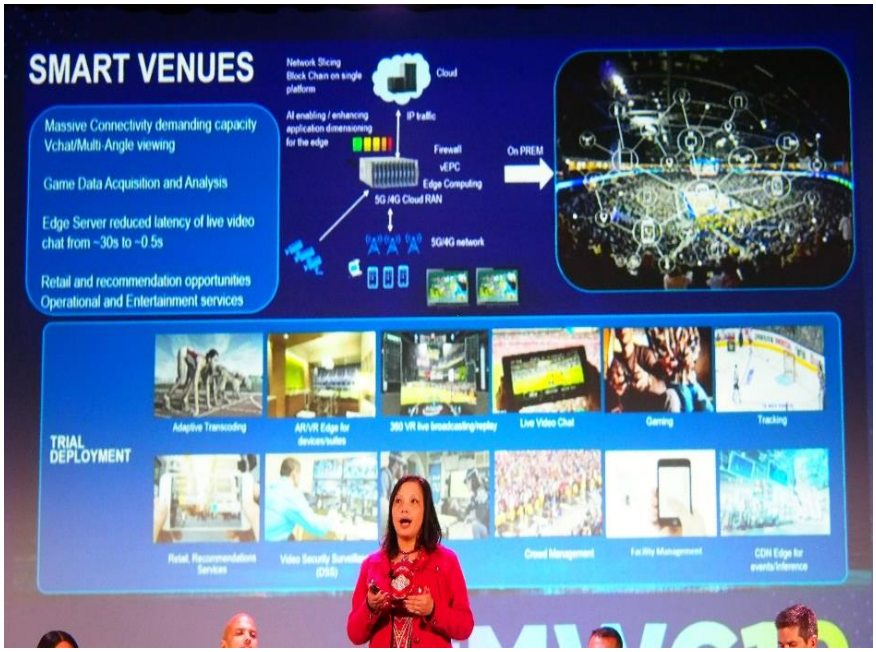

圖 13 Intel 提出之邊緣運算應用說明

(17) 物聯網連接的承諾

主持人 TM Forum 副總裁 Joann O’ Briend 開場表示 5G 生態系統的成功意味著改變既有核心運營和 IT 產業經營模式；也就是促使其他產業進行數位化，預估整個 5G 生態系統將具有 5,820 億美元的市場，但要抓住 5G 商機就需要徹底進行商務轉型，發展 IoT 物聯網絕對是這波趨勢中最重要的產業之一，物聯網的應用廣泛牽涉到包含了環境監控、工業製造、運輸與物流、以及醫療保健等領域；而這些數位化系統轉型計畫需要創建新的重要標準和工具，包括商業模式、商業架構、Ecosystem 平臺獲利方式、以及 IoT 物聯網管理。她在總結說到，「5G 進一步降低了進入這些領域的壁壘，超過一半的實施者正在考慮 5G。」。

Accenture 網路服務全球負責人 Amol Phadke 強調快速可靠的行動通訊網路對於許多行業的擴展至關重要。當 5G 網路無處不在時，蓬勃發展的 IoT 物聯

網產業將看到巨大成長的商機；這些很快將帶來變革的服務，如 3D 視頻，身臨其境的電視，自動駕駛汽車和智慧城市基礎設施等突破性發展，將釋放出當今難以想像的商機，電信公司將在促進這些前景方面發揮關鍵作用。

Semtech 無線 LoRa 與物聯網副總裁 Marc Pegulu 則強調，即便 5G 時代來臨，已發展多年的 LoRa 技術仍有存在價值，LoRa 具備低頻寬，適用於短距離和長距離的特性剛好可填補其他技術的空白部分；由全球超過 500 個成員的 LoRaAlliance 所發展的 LoRaWAN 可支援最多 10 億個終端設備的部署，LoRa 作為最受歡迎的 LPWAN 技術、蜂巢式物聯網的相容性、以及與行動通訊生態系統的無縫連結將使得 LoRaWAN 能與 5G IoT 長期共存。

Sprint 物聯網與產品開發資深副總裁 Ivo Rook 在座談會上分享了有關該公司 Curiosity 物聯網產品的最新消息，一種新的 NB-IoT 專用網路選項以及與亞利桑那州立大學合作的案例。同時也提到：如果電信公司將支援物聯網趨勢以實現數位化經濟的承諾，則應該規劃建設一個專用網路以實現此雄心壯志；他說：「如果電信公司仍在考慮智慧手機的情況下設計網路，那麼物聯網彩虹盡頭的金礦很可能會遭到競爭對手的突襲」。

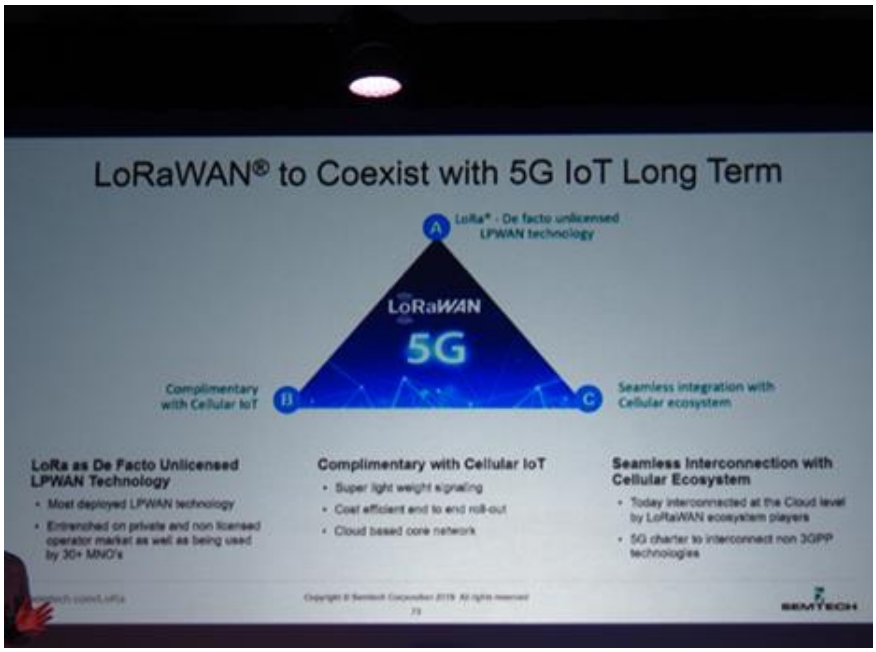

圖 14 Semtech 提出 LoRaWAN 與 5G IoT 共存

(18) **智慧城市及智慧世界**

來自 Bird 滑板車公司的 David Allison 闡述，該公司除了出租滑板車給市民使用外，也會提供騎乘的 MDS 資料給該城市的交通部門。但是隱私卻成為這些騎行資料的使用障礙，Allison 指出由於各地方的隱私法案之故，有些不具備隱私保護技術的城市政府單位是不願意接收這些可以用於城市規劃的資料。對於隱私保護，Allison 有兩點保護策略，第一個是改變資料的索取方式，將整批資料餵入資料庫的方式，改成提供 API 查詢，限定存取次數，並且透過數據概略化達成隱私保護。第二個是描述騎行資料時，資料的主體是設備序號，不要待入租用人的資料，根本上避免個資。

來自 Ouster 公司 Raffi Mardirosian 提到，Ouster 是一間 LiDAR 的製造廠商，LiDAR 乃用來量測自身與目標距離的裝置，常用於自駕車技術，了解車子周圍之環境情況。Ouster 的特色是強調提供服務提供商可負擔的 LiDAR 裝置。Mardirosian 也說明若 LiDAR 裝置設置在街口，亦可了解路口的情況，例如公車是否依照路線轉彎，有多少行人等。Mardirosian 也舉出一個實際案例，有顧客發生車禍，將車上的 LiDAR 紀錄作為行車紀錄，來證明自己是被撞的一方。

(19) 物聯網裝置：始終傾聽、觀察及學習

Greystar 建築公司的 Dave Denslow 談論到 IoT 與智慧建築的未來願景，未來的建築不僅是單純的住宿功能，還能理解人的需求。他們公司相信智慧建築的成功需要具有三要素，分別是有效率（Efficiency）、體驗（Experience）以及可行動的情資（Actionable Intelligence）。他們公司一直思考智慧建築的意義是甚麼，如何去擁抱科技的進步？他們認為手機是其中的關鍵，他們在建築物中廣佈熱點，使得手機能持續連線，透過手機去控制門鎖，監控溫度等功能。不只這樣，透過對建築物與生活空間的控制、監視與管理，用戶能更好的對生活需求做出決策，以便利他的生活。

Boingo Wireless 的 Derek Peterson 談論個人的物聯網，他認為隨著越來越多的裝置會連網，此時要討論的重點應該擺在這些 IoT 裝置要符合個人的使用，要使得 IoT 變成生活的一部分，使得用戶從中獲益，不是單純為技術而技術。他舉例子說明，現在智慧門鎖是用手機當作鑰匙，但技術越進步，裝置連網比對生物與行為資料庫，用戶用其手掌或臉，就可以當作鑰匙。這個轉變就是把科技與人相互關聯，實體世界與虛擬世界相互關聯，且以人為本。而這些科技都要網路來串連才有發生的可能，也就是單一技術是沒辦法獨立帶給用戶更便利的生活，是要整合跨科技與跨地域的各類技術來達成，而其中的整合關鍵就是連網技術。

Ericsson 的 Bodil Josefsson 則說 IoT 使得每個東西都連線，這種新潮流帶來好處，但是越多裝置也代表著許多資安的洩漏點。所以產業界需要物聯網是可靠且安全的。要達到這樣的狀態，資安要求在設備開發之初時就要納入設計，不能夠等到產品發布後再以事後補充的方式進行功能增補。所以 IoT 安全要先有安全的裝置，例如裝置密碼的設計，再來是安全的通訊連線，最後是平臺安全。IoT 系統的端到端安全是要整體考量的，不能夠只有裝置安全，當然 Ericsson 身為設備商，他們也樂於使得裝置取得認證，希望看到很多認證計畫推出。

Figleaf 的 Pankaj Srivastava 則說未來應該建立以隱私為優先的生態系，他舉例說道現在只要一上網就會有十多種追蹤器，試圖辨識用戶指紋，建立用戶的偏好以推送廣告，這種情況很像小說 1984 的老大哥看著你的預言。但是隱私議題在不同的國家地區有不同態度，這仰賴客戶的對隱私議題的洞見與看法，但他也認為未來客戶會逐步的認識到隱私的重要性，使得公司對隱私保護變成市場競爭力。

OMNIFLOW 的 Pedro Ruao 則是介紹 OMNIFLOW 是一間生產街頭上的監控設備的 IoT 系統設計製造公司，他們公司的產品特別強調使用再生能源如太陽能與風力來提供 IoT 裝置的穩定性與強韌性。他也預測未來 5G 的發展會對 IoT 有好處，例如車聯網就需要 5G uRLLC 的特性，但也需要注意額外的安全需求。

(20) 安全的物聯網

主持人請 Alex Rice 先介紹一下他所屬的駭客社群，Alex Rice 回答該公司社群約 500 人，成員的組成很多元，也有來自學術界，又或者最小的成員才 15 歲，但可以說是一群以創新方法繞過保護機制的技術人。主持人接著詢問 Alex Rice 獎勵平臺的獎金制度，Rice 回答促進網路安全的進步，造福人群本身就是這群人的心靈回饋，但他們公司也有提供實質回饋的獎金，依照影響程度的不同，獎金約為 3,000 到 10,000 美金。主持人接著請 Rice 預測 IoT 威脅的未來演變。Rice 回答，他已經看到未來 IoT 的攻擊將朝向有著更大影響層面的裝置，或者可以造成更大經濟上損害的系統，來進行經濟勒索。另一個可能性是朝著更私人的領域進攻，以往勒索軟體是加密檔案，但他認為未來勒索軟體可能會朝向刺探私人的隱私，譬如透過網路攝影機來窺看私人生活，並據以勒索。

來自 CUJO AI 公司的 Marcio Avillez 回答說不同的 IoT 裝置有不同的情況，若是家用的 IoT 裝置、智慧家庭等目前的解法不多，但是若談到商用的 IoT 裝置，隨著業務的不同，解決方案就有各式各樣的解法，這樣的資源很多。但總

歸的來說，採用 AI 可能是未來可行的解法。Avillez 另外也提到 API 安全也是相當重要的一環。

Cisco 公司的 Nancy Cam-Winget 則從設備商角度，講出工廠業界的看法，她認為工業界講求可用性，而解法採用獨立網段（air-gap）與限制存取（least access），就她的經驗看來，工廠環境基本上沒加密也沒認證，整個網路安全防禦都不存在，如同赤手空拳一般，這種情況非常普遍，甚至美國與歐洲都相同，相同的環境，也就代表威脅是相近的，目前工業界為了處理這種情況，推出 IEC62443 標準，不失為未來的解法。Ncncy 認為由於公司不能處理所有的威脅，故進行風險分析後，使得公司的資安態勢能足夠應付威脅是其中的關鍵。

NIST 的 Michael Fagan 則談論到美國聯邦政府採用 IoT 的經驗，他舉例說即使是政府單位，各單位的差異也相當大，如 NSA 就有集中辦公區域，也有相當技術人員可以好好的管理 IoT 的使用，但是反觀 IRS 可能就沒辦法有相同的條件。他另外也提到說公司若使用家用產品，因為商用與家用對於資安要求等級的不同，有可能造成新的資安缺口。

Blancco 公司的 Russ Ernst 則認為越來越多的 IoT 裝置，同時意味著越來越多的資料，未來的公司要會需要知道如何大量進行資料儲存，處理與管理。而據他的經驗表示，這些資料中 85%的資料是好幾年都用不到的，處於相對靜態的狀態中，若公司不知道如何管理這類資料，擁有這些資料就是本身就帶來風險。

A10 Networks 的 Ravi Raj Bhat 則是先提出來未來的物聯網數量與其產生之巨量資料的預測數字，他認為未來的挑戰是這些資料的安全與隱私。同時他也認為製造商有責任，負擔資安義務，例如裝置不能有預設密碼。

再來主持人提到如何透過法律處理 IoT 安全議題，他舉例說道：如同早年的汽車安全帶與安全氣囊，也都是以法規引導車廠去製造與裝設。來自 NIST 的 Michael Fagan 則說明監管單位當然有其效果，但他認為製造商也有其責任，資安人員不能只想著管制控制，造成用戶不便，這樣反而會有反效果，造成用

戶不使用這些資安功能，資安擾人就無效。作為一個資安的研發工程師要盡力使得資安功能是自動化開啟，同時簡單易於使用。他舉了一個例子說沒有人想要返家開冰箱時，還需要輸入密碼。來自 Blancco 公司的 Russ Ernst 則說道：有時合規不等於安全，但合規會驅動安全。

五、5G 資安高峰會

(21) 網路防護

演講者是來自 Ericsson 的安全解決方案總經理 Keijo Mononen，他在會中指出，5G 行動通訊網路雖是商用網路，但是考量 5G 將滲透到每個國家的各個層面，新的業務和服務交付模型，不斷發展的威脅格局，以及對隱私的日益關注，因此需要新的安全要求是 5G 網路時代一項非常重要的環節，政府應重視此問題，適當地介入並要求 5G 電信業者善盡 5G 資安防護責任。整體來說，所有電信業者對其所面臨的 5G 資安挑戰仍缺乏整體性（End to End）資安可視性，無法得知威脅或風險存在網路何處、資安或隱私合規性，雖然掌握很多資料，但如何保護才符合法令，在應用與違法之間也難拿捏、偵測跟回應威脅能力不足，以及仍以人工抵擋並處理資安攻擊。

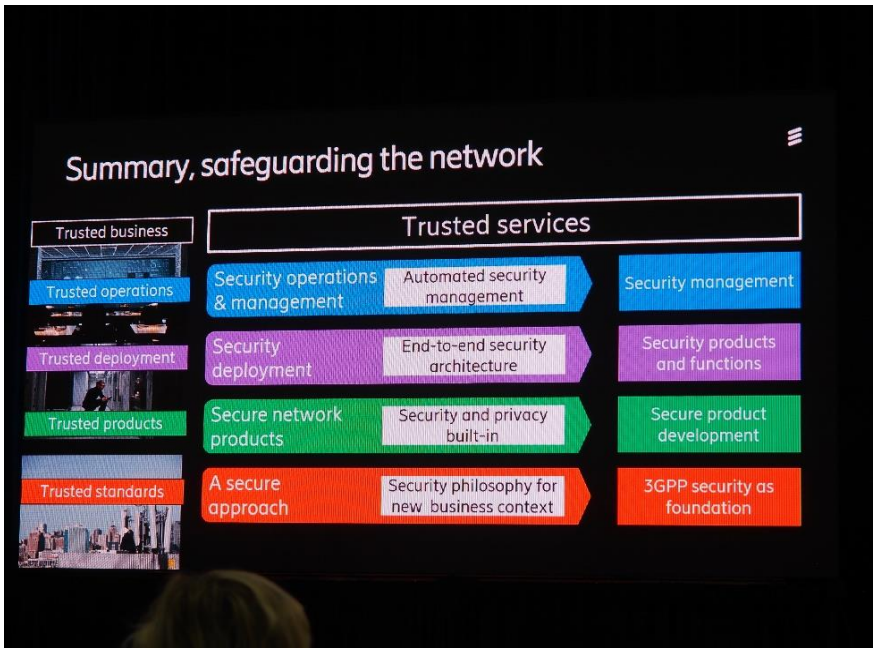

圖 15 Ericsson 提出確保 5G 網路安全之整體概念

(22) 5G 案例及新興資安需求

Nokia 軟體副總裁 Mary O'Neill 完全同意維護資安是 5G 網路時代一項非常重要的環節，5G 雖是商業網路，但是考量行動通訊網路將滲透到每個國家的各個層面，政府應重視此問題，適當地介入並要求 5G 電信業者善盡 5G 資安防護責任。Nokia 針對 5G 網路防護的解決方案強調管理網管人員存取網路系統的記錄並透過 AI 分析每個帳號使用行為，確保即使帳號被盜用仍可在第一時間得到示警。

O'Neill 進一步向行動通訊服務提供商發出了呼籲，要求他們加快 5G 安全的部署速度，並警告說，優先考慮速度而不是安全性可能會導致更大的問題。在會議上，O'Neill 承認，要「更快，更快，更快地」推出 5G 仍在進行中，但為了確保他們贏得部署競賽而損害安全性是一種落後的方法。她說：「從架構的第一天開始就可以構建安全性，而不必之後再對其進行修補而付出更多代價。」這位來自 Nokia 的資安專家強調 5G 安全相關要求已經改變，不可再用現有解決方案來解決所有問題。我們需要更多的技術。當我為 Nokia 制定策略

時，我們將投資於機器學習，演練腳本，工作流程，並且我們非常相信自動化可以幫助解決此問題。

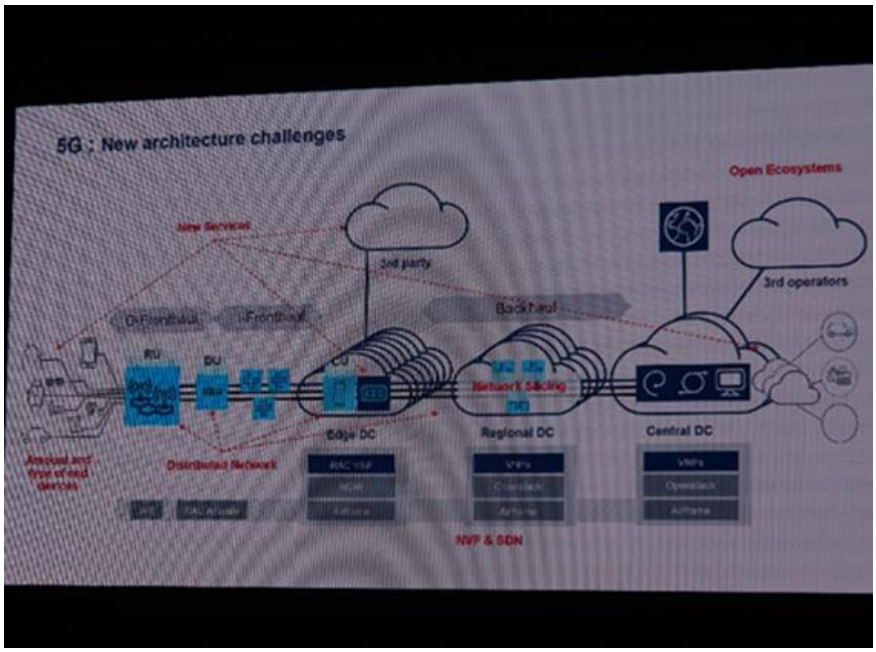

圖 16 Nokia 提出 5G 新網路架構所面臨之安全挑戰

(23) **物聯網安全**

來自 L-Spark 創新公司加速器的 Leo Lax 是本場的主持人，L-Spark 協助了幾間新創公司連結如黑莓（BlackBerry）的四家大公司，使新創公司可以在四家大公司的平臺上，對 IoT 的安全議題上進行技術開發與創新。這些新創公司的解決方案目前是選擇以 eSIM 為開發基礎，對電信產業提供了基於硬體的高度安全的 IoT 信任基礎，可確保設備及應用程式的安全，使得設備與其應用程式服務平臺之間建立相互信任關係，例如未來的 5G 進行遠距醫療時，整個診斷與治療的過程，這些醫療裝置是要透過身分驗證功能確認與確保其安全可靠，贏得醫師與病人的信任。

Telus 的 Alfred Baghouzian 認為隨著物聯網裝置的變多，連結更密集，AI 與雲端技術的興起，新的機會來到也伴隨著新的威脅，為了安全，兩個原則必須遵守：第一是安全設計原則（Security by Design），以及第二是把 IoT 是作一個整體來看待安全，GSMA 的推出的 IoT 安全指引是好的框架參考。電信產業使

用資安技術已經有二三十年之久，透過硬體來達到安全是電信業一直以來的做法，利用硬體金鑰與認證算法來對終端裝置進行生命周期的管理，這樣的產業供應鏈已經成熟，這樣的經驗 Telus 認為可以應用到目前 IoT 與網路的安全議題，所以 Telus 與新創公司合作在電信平臺上驗證概念測試。

BlackBerry 的 Sarah Tatsis 認為要 IoT 裝置間要進行溝通，IoT 裝置要給人使用，IoT 業務要推展，之中的關鍵是要有信任，以達成消費者所需之隱私、安全與連接可用。BlackBerry 現在是為一家軟體安全公司，以車聯網為例，已經有多個國家使用公司的 IoT 車聯網平臺。BlackBerry 認為要達成端到端的安全是一個挑戰，但大多數的公司都沒有資安背景，也顧不起資安專家，所以他們認為需要有一個中介軟體平臺，把安全功能納入作為軟體開發時基礎元件，對開發人員來說，可以更輕鬆的達到安全要求。另外，採用該平臺也可以達成合規與自動化（zero-touch）的信任。

Solace 的 Eugene Hallinan 則說 IoT 成功的關鍵在於數量，只有數量達到一定規模，至少幾百萬的裝置，才有應用效益，Solace 目標就是要能管理這樣的大量裝置，這挑戰是數百萬的訊息如何有效率的同時安全傳遞。他們的平臺現在在航空業與物流業使用，同使也串好了銀行的金流系統。

G&D 的與會者 Simon 則說在這些大量的 IoT 裝置的安全是仰賴於像 SIM 卡的硬體安全元件。G&D 的目標市場是高端與高價值的物聯網裝置，如車聯網、手機與平板、身分證晶片與金融卡，G&D 可以提供上述服務的身分驗證安全功能。他認為隨著消費者安全意識的提高，服務提供商需要滿足消費者的安全需求，像消費者展示擁有足夠安全的身分驗證功能相當重要。

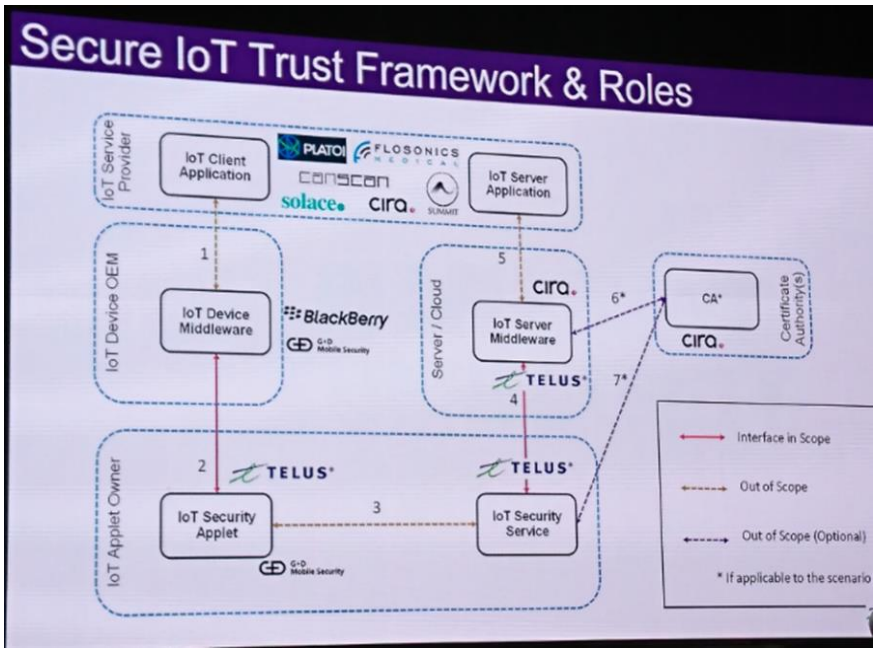

圖 17 Telus 提出之 IOT 網路信任框架與角色

(24) 如何在 5G 時代持續受到保護

來自 Ericsson 的 Bodil Josefsson 表示，在這個萬物聯網的時代，大家的確會從中獲得一些便利，IoT 服務商也勢必要提供安全的服務，所以服務商要去理解物聯網的資安威脅，理解自身系統的資安態勢（Security Posture），同時也要認清安全功能要在系統設計之初就納入，不能已逐次增加系統的安全功能的方法來去營運 IoT 服務。

接著主持人詢問來自 Verizon 的 Jack Gallagher，身為電信業者，對於資安風險，最擔心的事情是什麼？Jack Gallagher 回答作為業者最擔心的資安風險還是連線中斷的問題。當然端到端的安全也是他會考慮的，所謂端到端的安全指的是連線通道本身、到手機終端的安全、空中介面安全、後傳網路安全、核網安全，到客戶雲端運算平臺的安全，他都會關心。以上個點也會成為攻擊的進入口，當然要入侵手機終端可以比較困難，可能要實體接觸到手機，也比較沒有效益，但是若是攻擊 IoT 服務的平臺，這就非常吸引駭客去攻擊，因為從平臺可以連接到數以萬計的裝置，平臺也有可能連結到高價值的控制設備。所以

如何提供客戶安全的連線服務，甚至未來安全的 MEC 服務業是他會思考的議題。

主持人接著詢問威脅增長的議題，主持人認為隨著 5G 與 IoT 的發展，公司從中獲利的比例也會逐年增加，但隨著獲利的增加，這些為公司帶來利潤的系統也會變成駭客覬覦的目標，這對公司來說表示越發展就越危險，對公司變成一種兩難局面。Bodil Josefsson 表示這種發展兩難的議題需要發展技術來解決，特別是 5G 安全技術。Gallagher 則表示這些高價值的物聯網設備都會因 5G 而更興盛，例如車聯網，故 3GPP 也發展安全技術來試圖解決。

主持人反問是否因為 3GPP 有發展 5G 安全技術，所以我們就不需要再擔心資安議題。Bodil Josefsson 表示這是錯誤的陳述，這是由於 5G 會持續發展，也會有新的事物進來 5G，新的資安問題也需要關心。Dean Weber 則回答，當然還是要擔心 5G 安全議題，5G 會與 4G 共存，信令安全會是個議題。生動的說若 4G 是雙線道公路，那麼 5G 就是 200 線道的公路，所以當攻擊發生時，受損的速度與後續擴大的影響也是指數增長。

主持人問 Gallagher 關於身為早期進入 5G 的電信業者，Verizon 會採取何種特殊的措施保障來 5G 安全？Gallagher 回答就他自己所知，3GPP 已經做了一些安全的工作，3GPP 也減緩了一些從 4G LTE 時代就存在的弱點，但在 5G 時代，Verizon 還關心供應鏈安全、也關心軟硬體模組元件的安全，端到端的安全，也包含垂直應用領域的特殊需求。

主持人問從終端裝置到網路的端到端安全，其中的哪的環節是較為危險的或者較為有挑戰來確保安全，各位與談人的看法。Dean Weber 則回答供應鏈安全，元件來自各地，要分辨每個元件是否會被攻陷或是被埋入木馬是不可能的任務。但以軟體為例，NIST 發表了相關的指引。他認為軟體供應鏈是新興的重要議題，且因元件來自各地，這是一個信任與信用問題。Bodil Josefsson 表示端到端安全要先釐清端到端的範圍，只是指加密，還是雲端安全，還是指縱深

防禦，Josefsson 認為端到端的安全是很多面向與層次的，而中間的關鍵能力在於可視性，接著是建立資料關聯性，才能達到端到端安全。

肆、　心得與建議

本次前往美國洛杉磯參與 2019 MWC Los Angeles，在會議中聆聽北美地區相關電信監管機構、城市管理單位、電信運營商及設備大廠就 5G 產業的部署與應用，包含 IoT、垂直領域、供應鏈安全及商業模式的經驗分享，並於 MWC 展場蒐集全球主要 5G 服務提供商與設備業者邁入 5G 時代之推動策略，所得出之心得與建議如下三點。

- 美國 5G 政策以強化應用市場影響力邁進

美國很清楚目前在 5G 通訊技術上落後，故在政策上已經不在通訊技術層上搶奪領先地位，轉而要搶奪 5G 在應用與服務上的競爭優勢，試圖打造下一個 Google 與 Facebook。同時要豐富供應鏈的多樣性，避免單一國家壟斷示場，同時解決國家安全、經濟領導力與影響力議題。在與 5G 產業鏈逐漸成熟之際，尋求下一個殺手級的 5G 應用，是美國奪取 5G 領導力與影響力的目標。雖然在 5G 部署初期，eMBB 是大多數消費營客戶之需求，但垂直應用需求如車聯網、智慧工廠、醫療、災害監控等 5G 應用是另一個發展關鍵區域。

- 5G 應用驅動資安防護技術發展

由於 5G 系統以軟體化為其特色，各個網路功能元件基於 NFV 和 MEC 技術，構成網路切片此一 5G 服務。隨著各地 5G 建設的起跑，MWC 19 的眾多與會人士都呼籲建設 5G 時一定要將資安就納入建設藍圖中，若是等到事後才進行資安功能的增補會耗費更大成本。因此美國政府也針對通訊系統的如何提升強韌性與可靠性，收集基礎設施的攻擊與威脅手法，下足了準備功夫。也透過國土安全部的預算補助通訊系統各層間的防護技術研發與創新發展，因此若我國要外銷 5G 系統與應用服務，網路安全也是須優先考量的相關議題。

- 5G 與 AI 將促進智慧城市應用發展：

5G 將促進現有智慧城市發展，例如帶動智慧路燈上整合 5G 基地臺，不僅僅包含無線發射單體之無線發射單體，更會提供附掛多項感測器與攝影機，產生高密度的數據資料數據。這裡我們要指出這是一個多科技融合才能達到的智慧城市的理想境界，5G、IoT、AI、大數據與雲端技術缺一不可。沒有 5G，不能承載與傳輸大量即時數據。沒有 IoT，無法取得異質與多維度數據與控制實體設施，與真實世界產生連接。沒有 AI 技術，機器無法訓練與學習，使人類決策思維重複利用。沒有大數據與雲端技術，資訊基礎建設根本不合成本效益。如何融合這些科技，發展應用創新，將是未來的核心競爭能力，但這些技術相信不是單一企業可以擁有，缺乏熟練的人才與強有力的領導力，國內要發展 5G 創新應用，如智慧製造、智慧醫療與車聯網，合理的發展策略應該依照國際供應鏈分工下，緊緊跟著主流市場走。而我們在 MWC 19 觀察到的，供應鏈安全與隱私人權絕對是歐美主流市場所心心念念的重中之重，例如邊緣運算中有個需求是將街口的攝影機，利用邊緣運算就去除掉車輛與行人之外觀，回傳後端系統就只有簡單的計數數字與描述資料就是個好例子。而這卻是國人在設計系統時，很難想像的需求。

伍、附件：相關照片及資料

一、2019 全球行動通信系統協會行動通訊大會：

https://www.mwclosangeles.com/

二、會議議程：

「主題演講 Keynote」議程 (Keynote Auditorium)		
10/22	09:30~ 11:30	開幕專題演講 Keynote 1: Opening Keynote
10/23	09:00~ 10:30	專題演講 Keynote 2
	10:45~ 11:45	技術長們對 5G 之看法 CTOs Talk 5G
	11:45~ 12:00	加速美國創新－國防部 5G 契機 Accelerating American Innovation － DoD 5G opportunities
10/24	09:30~ 11:00	專題演講 Keynote 3

「政策演講 Everything Policy」議程 (Theater 411)		
10/22	13:00~ 13:45	立法政策倡議：國會議程 Legislative Policy Initiatives: Congressional Agenda
	13:45~	FCC 委員 Brendan Carr 主題演講

「政策演講 Everything Policy」議程 (Theater 411)		
	14:05	Keynote Remarks Featuring FCC Commissioner Brendan Carr
	14:05~ 14:50	5G 年：頻譜政策更新 The Year of 5G: A Spectrum Policy Update
	14:55~ 15:10	CISA 總監 Christopher Krebs 主題演講 Keynote Remarks Featuring CISA Director Christopher Krebs
	15:10~ 15:55	保護新興的 5G 網路 Securing the Emerging 5G Networks
	16:00~ 16:15	FCC 委員 Jessica Rosenworcel 主題演講 Keynote Remarks Featuring FCC Commissioner Jessica Rosenworcel
	16:15~ 17:00	5G 20/20：美國的市場驅動力 5G 20/20: Market Drivers across the U.S.
10/23	13:00~ 13:15	FCC 委員 Mike O’ Rielly 主題演講 Keynote Remarks Featuring FCC Commissioner Mike O’ Rielly
	13:15~ 14:00	無人空中服務 Up, Up and Away: Unmanned Aerial Services
	14:05~ 14:50	WRC-19 的國際頻譜優先事項 International Spectrum Priorities Heading into WRC-19
	14:55~ 15:10	NTIA 助理部長 Diane Rinaldo 主題演講 Keynote Remarks Featuring Diane Rinaldo
	15:10~	通過聯邦隱私立法保護消費者

「政策演講 Everything Policy」議程 (Theater 411)		
	15:55	Protecting Consumers with Federal Privacy Legislation
	16:00~ 16:15	FCC 委員 Geoffrey Starks 主題演講 Keynote Remarks Featuring FCC Commissioner Geoffrey Starks
	16:15~ 17:00	內部的無線政策：FCC 顧問的觀點 Wireless Policy from the Inside: FCC Advisors' Views
「5G 演講」議程 (Concourse 152)		
10/22	13:00~ 14:00	5G 營銷：從速或從優進入市場？ Marketing 5G: First or Best to Market?
	14:15~ 15:15	偏鄉地區之連接：商業模式是否存在？ Rural Connectivity: Is the Business Model There?
	15:45~ 17:00	5G：力量、全球、利潤 5G: Power, Planet, Profit
10/23	13:00~ 14:00	5G 網路：深入討論 5G Networks: Hard Talk
	14:15~ 15:15	專用網路 vs 5G 網路切片 Private Networks vs 5G Network Slicing
	15:45~ 17:00	5G 之網路邊緣 5G On The Edge
10/24	11:00~ 12:00	保障 5G 策略不過時 Future Proofing your 5G Strategy

「政策演講 Everything Policy」議程 (Theater 411)		
	12:15~ 13:15	5G 對您的未來安全嗎？ Is your Future Safe with 5G?
	14:00~ 15:00	這是我們所熟知的行動終端嗎？ Is this the End of Mobile as we Know it?
「IoT 演講」議程 (Concourse 151)		
10/22	13:00~ 14:00	擴展智能物聯網 Scaling the Internet of Intelligent Things
	14:15~ 15:15	邊緣計算：創造新的物聯網應用 Edge Computing: Creating New IoT Applications
	15:45~ 17:00	物聯網連接的承諾 The Promise of IoT Connectivity
10/23	13:00~ 14:00	零售物聯網：逛街及購物體驗 IoT in Retail: The Shopping and Purchase Experience
	14:15~ 15:15	醫療照護物聯網：改變治療及改變生命 IoT in Healthcare: Changing Treatments and Changing Lives
	15:45~ 17:00	製造業物聯網：自動化、改善與機器人 IoT in Manufacturing: Automation, Optimization and Robots
10/24	11:00~ 12:00	智慧城市及智慧世界 Smarter Cities, Smarter World
	12:15~	物聯網裝置：始終傾聽、觀察及學習

「政策演講 Everything Policy」議程 (Theater 411)		
	13:15	IoT Devices: Always Listening, Watching and Learning
	14:00~ 15:00	安全的物聯網 The Internet of Safe Things
「IoT 演講」議程 (NexTech Stage - West Hall)		
10/23	10:30~ 11:15	網路防護 Safeguarding the Network
	11:30~ 12:30	5G 案例及新興資安需求 5G Use Cases and New Security Needs
	14:00~ 14:45	物聯網安全 IoT Security
	15:00~ 15:45	如何在 5G 時代持續受到保護 How to Stay Protected in the 5G Era