參考資料

第一章 緒論

1.1 W. Lawrence Neuman 著朱柔若譯. 社會研究方法－質化與量化取向(2000)

第二章 建立 6G 跨領域應用情境之參考架構先導評估

2.1 林咨銘，包偉丞，葉庭語，蔡峻嘉，周威宏，“全球 5G 標準系統與技術效能評估”，工研院電腦通訊期刊，第 181 期 5G 技術專輯，2020 年 3 月 17 日。

2.2 本章節資料來源，主要整理 ITU-R WP5D 第 44 次會議之相關討論與決議文件。(來源參考 https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/Pages/default.aspx)

2.3 ITU-R R19-WP5D-221010-TD-0740,“Naming for International Mobile Telecommunications ”, WP5D #42, October 18th, 2022.

2.4 依據 ITU-T 建議書 Y.4600 之定義，數位雙生專指一個可在某一數位應用或情境中，代表特定之實體主客體，且可即時同步連動之數位物件。

2.5 依據 WHO 研究報告“Global strategy on digital health 2020-2025”，數位醫療包含各種透過電子與網路技術，可用來改善醫療照顧服務與環境之數位科技，包含物聯網，人工智慧，與機器人等。

2.6 ITU-R R19-WP5D-230612-TD-0905, “Framework and overall objectives of the future development of IMT for 2030 and beyond, ” WP5D #44, June 22th, 2023.

2.7 3GPP RAN Release-19 workshop, RWS-230012

2.8 3GPP RAN Release-19 workshop, RWS-230147

2.9 3GPP RAN Release-19 workshop, RWS-230264

2.10 3GPP RAN Release-19 workshop, RWS-230192

2.11 3GPP RAN Release-19 workshop, RWS-23090

2.12 6G-ANA (2022). 6G 网络原生 AI 技术需求白皮书. (2022). Retrieved from http://www.6g-ana.com/upload/file/20220523/637889301773049743470606 8.pdf

2.13 Dong, Jiahua, et al. "No One Left Behind: Real-World Federated Class-Incremental Learning." arXiv preprint arXiv:2302.00903(2023).

2.14 Da-Wei Zhou, Han-Jia Ye, De-Chuan Zhan (2021) Co-Transport for Class-Incremental Learning. Retrieved from https://arxiv.org/pdf/2107.12654.pdf

2.15 Medium. (2020) Retrieved from https://gino6178.medium.com/%E6%A8%A1%E5%9E%8B%E5%A3%93%E7%B8%AE%E5%8F%8A%E5%84%AA%E5%8C%96-learning-rate-c340a0b940e4

2.16 GitHub. yfjeffliu/itri_cil_goods. Retrieved from https://github.com/yfjeffliu/itri_cil_goods

第三章 規劃與建立安全與可靠的 6G 跨領域應用機制與技術先導評估

3.1 [ITU-2410] Minimum requirements related to technical performance for IMT-2020 radio interface(s), 2017 report, Retrieved from https://www.itu.int/pub/R-REP-M.2410

3.2 [RFC-1] Network virtualization research challenges, https://datatracker.ietf.org/doc/html/rfc8568

3.3 R. Glitho Cloudifying the 3GPP IP multimedia subsystem: why and how? 6th International Conference on New Technologies, Mobility and Security (NTMS) (2014), pp. 1-5 Google Scholar

3.4 [RFC-2] Multi-domain Network Virtualization. Retrieved from https://www.ietf.org/archive/id/draft-bernardos-nfvrg-multidomain-00.txt

3.5 Raghubir Singh, Sukhpal Singh Gill. (2023) Edge AI: A survey. Retrieved from https://www.sciencedirect.com/science/article/pii/S2667345223000196#bbib72

3.6 Gartner. (2018) Retrieved from https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders

3.7 GRISM-MEC. (2023) Retrieved from https://packetx.biz/zh/products-grism.php (Jul. 03, 2023)

3.8 K. Piotrowski, P. Langendoerfer, and S. Peter. (2009). “tinyDSM: A highlyreliable cooperative data storage for Wireless Sensor Networks,” in 2009 International Symposium on Collaborative Technologies and Systems, pp. 225–232, Ieee, 2009.

3.9 Richard Coppen, Andrew Banks, Ed Briggs, Ken Borgendale, Rahul Gupta (2019) MQTT Version 5.0. Retrieved from https://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.pdf.

3.10 S. Ratnasamy, B. Karp, L. Yin, F. Yu, D. Estrin, R. Govindan, and S. Shenker. (2002) “GHT: A Geographic Hash Table for Data-Centric Storage,” in Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications (WSNA ’02), vol. 5, pp. 78–87, ACM, 2002.

3.11 J. Neumann, N. Hoeller, C. Reinke, and V. Linnemann. (2010) “Redundancy Infrastructure for Service-Oriented Wireless Sensor Networks,” in 9th IEEE International Symposium on Network Computing and Applications (NCA 2010), pp. 269–274, IEEE Computer Society, July

3.12 Yun Chao Hu, Milan Patel, Dario Sabella, Nurit Sprecher and Valerie (2015). Mobile Edge Computing A key technology towards 5G Retrieved from https://www.etsi.org/images/files/etsiwhitepapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf

3.13 ETSI. (2015). Mobile-Edge Computing Retrieved from https://portal.etsi.org/portals/0/tbpages/mec/docs/mobile-edge_computing_-_introductory_technical_white_paper_v1%2018-09-14.pdf

3.14 Adopting Multi Access Edge Computing (MEC) into 5G Networks. Retrieved from https://www.hsc.com/resources/blog/adopting-multi-access-edge-computing-mec-into-5g-networks/ (Jul. 03, 2023)

3.15 Sami Kekki, Walter Featherstone, Yonggang Fang, Pekka Kuure, Alice Li, Anurag Ranjan, Debashish Purkayastha, Feng Jiangping, Danny Frydman, Gianluca Verin, Kuo-Wei Wen, Kwihoon Kim, Rohit Arora, Andy Odgers, Luis M. Contreras, Salvatore Scarpina. (2018) MEC in 5G networks. Retrieved from https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf

3.16 ETSI. (2015). Mobile-Edge Computing Retrieved from https://portal.etsi.org/portals/0/tbpages/mec/docs/mobile-edge_computing_-_introductory_technical_white_paper_v1%2018-09-14.pdf

3.17 ITU_Y.4486. (2023) Framework of cross edge decentralized service by using DLT and edge computing technologies for IoT devices. Retrieved from https://www.itu.int/rec/T-REC-Y.4486

3.18 ETSI GR PDL 009 V1.1.1 (2021-09) Permissioned Distributed Ledger (PDL); Federated Data Management.

https://www.etsi.org/deliver/etsi_gr/PDL/001_099/009/01.01.01_60/gr_PDL009v010101p.pdf

3.19 Chonggang Wang (Lead), Mischa Dohler, Diego R. López, Raymond Forbes, Shahar Steiff, Tooba Faisal, Sheeba Backia Mary B., Qianren Liu, Ismael Arribas. (2022). An Introduction of Permissioned Distributed Ledger (PDL) Retrieved from https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP48-PDL.pdf

3.20 ITU_Y.3530. (2020). Cloud computing - Functional requirements for blockchain as a service Retrieved from https://www.itu.int/rec/T-REC-Y.3530/en

3.21 Draft ETSI GS PDL 013 V0.0.1 (2021-12); Permissioned Distributed Ledger (PDL); PDL for Supporting Distributed Data Management (Draft)

3.22 IEEE (2020) Standard for Functional Requirements in Blockchain-based Internet of Things (IoT) Data Management. Retrieved from https://standards.ieee.org/standard/2144_1-2020.html.

3.23 ISO/TR 23455:2019. (2019). Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems

3.24 徐慶柏, (2023) 【新興領域/2023.05 焦點】2023 年 H1 物聯網領域早期投資觀測：如風嗎？也不如風！. Retrieved from https://findit.org.tw/researchPageV2.aspx?pageId=2247

3.25 Gowri Sankar Ramachandran, Kwame-Lante Wright, Bhaskar Krishnamachari. (2018). Trinity: A Distributed Publish/Subscribe Broker with Blockchain-based Immutability Retrieved from https://arxiv.org/pdf/1807.03110.pdf (Jul. 03, 2023)

3. 26 Edoardo Longo, Alessandro E.C. Redondi, Matteo Cesana, Andrés Arcia-Moret, Pietro Manzoni. (2020) MQTT-ST: a Spanning Tree Protocol for Distributed MQTT Brokers Retrieved from https://ieeexplore.ieee.org/document/9149046

3. 27 ITU-T Y.4464. (2020). Framework of blockchain of things as decentralized service platform. Retrieved from https://www.itu.int/rec/T-REC-Y.4464

3. 28 Dinh C. Nguyen, Pubudu N. Pathirana, Ming Ding, Aruna Seneviratne. (2020). Blockchain and Edge Computing for Decentralized EMRs Sharing in Federated Healthcare. Retrieved from https://ieeexplore.ieee.org/document/9347951

3. 29 Cloud RAN and MEC: A Perfect Pairing (2018) Retrieved from https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp23_MEC_and_CRAN_ed1_FINAL.pdf

3. 30 ETSI GR. (2020). Permissioned Distributed Ledger (PDL); Application Scenarios Retrieved from https://www.etsi.org/deliver/etsi_gr/PDL/001_099/003/01.01.01_60/gr_PDL003v010101p.pdf

3. 31 ETSI GR. (2021) Permissioned Distributed Ledgers (PDL) Smart Contracts System Architecture and Functional Specification. Retrieved from https://www.etsi.org/deliver/etsi_gr/PDL/001_099/004/01.01.01_60/gr_PDL004v010101p.pdf

3. 32 ITU_Y.2342. (2019). Scenarios and capability requirements of blockchain in next generation network evolution Retrieved from https://www.itu.int/rec/T-REC-Y.2342/en

3. 33 ITU-T. Series F. (2021) SERIES F: NON-TELEPHONE TELECOMMUNICATION SERVICES Overview of convergence of artificial intelligence and blockchain

4.1 Abdel Hakeem SA, Hussein HH, Kim H. Security Requirements and Challenges of 6G Technologies and Applications. Sensors (Basel). 2022 Mar 2;22(5):1969. doi: 10.3390/s22051969. PMID: 35271113; PMCID: PMC8914636.

4.2 V. -L. Nguyen, P. -C. Lin, B. -C. Cheng, R. -H. Hwang and Y. -D. Lin, "Security and Privacy for 6G：A Survey on Prospective Technologies and Challenges," in IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2384-2428, Fourthquarter 2021, doi: 10.1109/COMST.2021.3108618.

4.3 台灣資通產業標準協會－TC5 網路與資訊安全技術工作委員會 (2023) 物聯網場域資安防護評估指引 v2

4.4 Defining AI native: A key enabler for advanced intelligent telecom networks (BCSS-23:000056) Ericsson White Paper Retrieved from https://www.ericsson.com/49341a/assets/local/reports-papers/white-papers/ai-native.pdf

4.5 "What is 5G network slicing?" Retrieved from https://stlpartners.com/articles/private-cellular/what-is-5g-network-slicing/

4.6 Danish Sattar, Ashraf Matrawy. (2019). Trinity: Towards Secure Slicing: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices. Retrieved from https://arxiv.org/pdf/1901.01443.pdf (Jul. 03, 2023)

4.7 What is IP Spoofing? . Retrieved from https://www.zenarmor.com/docs/network-security-tutorials/what-is-ip-spoofing (Jul. 03, 2023)

4.8 Shyam Oza. Denial-of-Service (DoS) Attacks — Web-based Application Security, Part 7. Retrieved from https://spanning.com/blog/denial-of-service-attacks-web-based-application-security-part-7/ (Jul. 03, 2023)

4.9 DrDoS Attacks. Retrieved from https://www.arturai.com/en/support/faqs/drDOS-attacks (Jul. 03, 2023)

4.10 Amrita Mitra. (2020). What is TLS Downgrade attack? . Retrieved from https://www.thesecuritybuddy.com/data-breaches-prevention/what-is-tls-downgrade-attack (Jul. 03, 2023)/

4.11 "STIX (1)" (2018). Retrieved from https://ithelp.ithome.com.tw/articles/10206720 (Jul. 03, 2023)

4.12 國家資通安全研究院. https://www.nics.nat.gov.tw/.htm (Jul. 03, 2023)

4.13 zcom. https://www.zcom.com.tw/ (Jul. 03, 2023)

4.14 GitHub. openaicellular/oaic. Retrieved from https://github.com/openaicellular/oaic.git

4.15 OAIC.(2022). Retrieved from https://openaicellular.github.io/oaic/quickstart.html

4.16 GitHub. openaicellular/nonrtric. Retrieved from https://github.com/openaicellular/nonrtric.git

4.17 GitHub. openaicellular/main-file-repo. Retrieved from https://github.com/openaicellular/main-file-repo.git

4.18 O-RAN Non-Real Time RIC Installation Guide. Retrieved from https://openaicellular.github.io/oaic/nonrtric.html

4.19 GitHub. wineslab/colosseum-oran-commag-dataset. Retrieved from https://github.com/wineslab/colosseum-oran-commag-dataset

第五章 6G 資安產業研析與防護實證應用驗測先導評估

5.1 6G Flagship
5.2 GSMA. https://www.gsma.com/security/network-equipment-security-assurance-scheme/
5.3 3GPP TR 33.805
5.4 3GPP TS 33.511
5.5 3GPP SWS-230074, SA Release-19 workshop
5.6 3GPP RAN Chair's summary of Release-19 workshop
5.7 3GPP SA Release-19 workshop, SWS-230073
5.8 3GPP SA Release-19 workshop, RWS-230463
5.9 3GPP SA Release-19 workshop, SWS-230069
5.10 3GPP SA Release-19 workshop, SWS-2230027
5.11 AMARI UE Simbox E Series. Retrieved from https://www.amarisoft.com/app/uploads/2022/03/AMARI-UE-Simbox-E-Series.pdf (Mar. 03, 2022)
5.12 CISA. (2022). Retrieved from https://www.cisa.gov/news-events/alerts/2022/07/05/prepare-new-cryptographic-standard-protect-against-future-quantum-based-threats

第八章 結論與建議

8.1 ITU-R. (2023). Overview timeline for IMT towards the year 2030 and beyond. Retrieved from https://www.itu.int/oth/R0A060000C8/en
8.2 主要整理 ITU-R WP5D 第 44 次會議之相關討論與決議文件。(來源參考 https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/Pages/default.aspx)
8.3 NIST. (2022). PQC Standardization Process：Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates. Retrieved from https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4

中英文名詞對照

縮寫	原文	中文
3GPP	3rd Generation Partnership Project	第三代合作夥伴計劃
5G	5th Generation Mobile Networks	第五代行動通訊
6G	6th Generation Mobile Networks	第六代行動通訊
AI	Artificial Intelligence	人工智慧
AI RMF	Artificial Intelligence Risk Management Framework	人工智慧風險管理框架 1.0 版
AI-AI	AI-Native Air Interface	AI 原生無線介面
AIGC	Artificial Intelligence Generated Content	人工智慧生成內容
AIoE	Ambient Internet of Everything	環境萬物聯網
AIoT	Artificial Intelligence of Things	智慧物聯網
AKA	Authentication and Key Agreement	認證與金鑰協議
AMF	Access and Mobility Management Function	存取與行動管理功能
API	Application Programming Interface	應用程式介面
App	Application	應用程式
AR	Augmented Reality	擴增實境
ATSSS	Access Traffic Steering, Switching and Splitting	接取流量導向、切換和拆分技術
AUSF	Authentication Server Function	認證伺服器功能
AV	Authentication Vector	認證向量
AWS	Amazon Web Services	亞馬遜雲端運算服務
BaaS	Blockchain as a Service	區塊鏈即服務
BC	Blockchain	區塊鏈
CCNF	Common Control Network Functions	通用控制網路功能
CDN	Content Delivery Networks	內容遞送網路
CIL	Class-Incremental Learning	類別增量學習

縮寫	原文	中文
CLI	Command Line Interface	命令行介面
CNCF	Cloud Native Computing Foundation	雲端原生運算基金會
CNN	Convolutional Neural Networks	卷積神經網路
COIL	Co-Transport for Class-Incremental Learning	類別增量協作學習
CP	Control Plane	控制平面
CPU	Central Processing Unit	中央處理器
CRAN	Cloud Radio Access Network	雲端化無線存取網路
CSC	Cloud Service Customer	雲端服務客戶
CSN	Cloud Service Partner	雲端服務合作夥伴
CSP	Cloud Service Provider	雲端服務供應商
CT	Communications Technology	通訊技術
CU	Central Unit	集中單元
CVD	Coordinated Vulnerability Disclosure	協調性弱點揭露機制
dApp	Decentralized Application	去中心化應用程式
DDoS	Distributed Denial of Service	分散式阻斷服務攻擊
DID	Decentralized Identity	去中心化身分
DL	Deep Learning	深度學習
DLP	Data Leakage Prevention	資料遺失防護
DLT	Distributed Ledger Technology	分散式帳本技術
DNS	Domain Name System	網域名稱系統
DoS	Denial of Service	阻斷服務攻擊
DPI	Deep Packet Inspection	深度包檢測
DrDoS	Distributed Reflection Denial of Service Attack	分布式反射拒絕服務攻擊
DRL	Deep Reinforcement Learning	深度強化學習
DSL	Digital Subscriber Line	數位用戶線路
DU	Distributed Unit	分散單元
eMBB	Enhanced Mobile Broadband	增強行動寬頻

縮寫	原文	中文
eNB	Evolved Node B	4G 基地臺
ENISA	European Union Agency for Cybersecurity	歐盟網路安全局
ETSI	European Telecommunications Standards Institute	歐洲電信標準協會
EU-US TTC	EU-US Trade and Technology Council	貿易與科技理事會
eXRM	enhancements for Extended Reality and Media services	增強型擴展實境與媒體服務
FCC	Federal Communications Commission	美國聯邦通訊委員會
FGSM	Fast Gradient Sign Method	快速梯度標記法
FL	Federated Learning	聯合學習
FT	Fault Tolerance	容錯
FUDM	False Unified Data Management	偽冒統一資料管理功能
FUTURE Networks Act	Future Uses of Technology Upholding Reliable and Enhanced Networks Act	未來網路法
GDPR	General Data Protection Regulation	一般資料保護規則
GHG	Green House Gas	溫室氣體
gNB	Next generation NodeB	5G 基地臺
GNU GPL	GNU General Public License	GNU 通用公眾授權條款
GSMA	Groupe Speciale Mobile Association	全球行動通訊系統協會
H2H	Human-to-Human	人與人
H2M	Human-to-Machine	人與物
HA	High Availability	高可用性

縮寫	原文	中文
HetNet	Heterogeneous Network	異質網路
HPC	High Performance Computing	高效能運算
HRLLC	Hyper Reliable and Low-Latency Communication	超極可靠低延遲通訊
HTTPS	Hypertext Transfer Protocol Secure	保全超文字傳送協定
IBM	International Business Machines Corporation	國際商業機器公司
ICT	Information and Communications Technology	資訊與通訊科技
IDC	International Data Corporation	國際資料資訊有限公司
IDS	Intrusion-Detection System	入侵偵測系統
IEC	International Electrotechnical Commission	國際電工委員會
IEEE	Institute of Electrical and Electronics Engineers	電機電子工程師學會
IMSI	International Mobile Subscriber Identity	國際行動用戶識別碼
IoE	Internet of Everything	萬物聯網
IoT	Internet of Things	物聯網
IP	Internet Protocol	網路通訊協定
IPFS	InterPlanetary File System	星際文件系統
IPS	Intrusion-Prevention System	入侵防禦系統
IPsec	Internet Protocol Security	網際網路安全協定
IS	Infiltrate Situation	滲透情境
ISAC	Integrated Sensing and Communications	感測與通訊整合
ISO	International Organization for Standardization	國際標準化組織

縮寫	原文	中文
ISP	Internet Service Proveder	網際網路提供商
ITU	International Telecommunication Union	國際電信聯合會
ITU-R	International Telecommunication Union Radiocommunication Sector	國際電信聯盟無線電通訊部門
KAIST	Korea Advanced Institute of Science and Technology	韓國科學技術院
M2M	Machine-to-Machine	物與物
MASQUE	Multiplexed Application Substrate over QUIC Encryption	運用快速端到端數據協定加密技術之多工應用底層程式
Massive MIMO	Massive Multi-Input Multi-Output	大規模多傳入 / 多傳出天線系統
MDT	Minimization of Drive Test	路測工作最小化
MEC	Multi-access Edge Computing	多存取邊緣運算
MEO	Multi-access Edge Computing Orchestration	多存取邊緣運算編排器
MitM	Men in the Middle Attack	中間人攻擊
ML	Machine Learning	機器學習
mMTC	Massive Machine Type Communications	大規模機器型通訊
MQTT	Message Queuing Telemetry Transport	訊息佇列遙測傳輸
MR	Mixed Reality	混合式實境
MRSS	Multi-RAT Spectrum Sharing	多傳輸層和無線接取技術頻譜動態共享
MWC	Mobile World Congress	世界通訊大會
NAS	Non Access Stratum	非存取層
NAT	Network Address Translation	網路位址轉譯

縮寫	原文	中文
NDR	Network Detection and Response	網路檢測和響應
Near-RT RIC	Near-Real-Time Radio Access Network Intelligent Controller	近即時無線接取網路智慧控制器
NESAS	Network Equipment Security Assurance Scheme	網路設備安全保證方案
NFV	Network Function Virtualization	網路功能虛擬化
NFVI	Network Functions Virtualization Infrastructure	網路功能虛擬化基礎設施
NGN	Next Generation Networks	次世代網路
NICT	National Institute of Information and Communications Technology	國立研究開發法人情報通訊研究機構
NIDS	Network Intrusion Detection System	網路入侵偵測系統
N-ISAC	National Information Sharing and Analysis Center	國家資安資訊分享與分析中心
NIST	National Institute of Standards and Technology	美國國家標準暨技術研究院
NPN	Non-Public Networks	專網系統
NRF	Network Repository Function	網路資料庫功能
N-SOC	National Security Operation Center	國家資安聯防監控中心
NTN	Non-Terrestrial Network	非地面網路
NTP	Network Time Protocol	網路時間協議
NWDAF	Network Data Analytics Function	網路數據分析功能
OASIS	Organization for the Advancement of Structured Information Standards	結構化資訊標準促進組織
O-RAN	Open Radio Access Network	開放式無線接取網路
O-RAN Alliance	Open Radio Access Network Alliance	開放式無線接取網路聯盟

縮寫	原文	中文
OWASP	Open Web Application Security Project	開放網頁應用程式安全專案
P2P	peer-to-peer	點對點
PDL	Permissioned Distributed Ledger	許可制分散式帳本
PDLF	Permissioned Distributed Ledger Function	許可制分散式帳本功能
PIA	Policy Infiltrator Attack	策略滲透攻擊
PQC	Post-Quantum Cryptography	後量子密碼
PT	Penetration Testing	滲透測試
QoS	Quality of Service	服務品質
RADIUS	Remote Authentication Dial In User Service	遠端認證撥接使用者服務
RAM	Random Access Memory	記憶體
RAN	Radio Access Network	無線接取網路
RAN message	Radio Access Network message	無線電存取網路訊息
RAT	Multi-layer/Radio Access Technology	傳輸層和無線接取技術
RIC	Radio Access Network Intelligent Controller	無線接取網路智慧控制器
RIS	Reconfigurable Intelligent Surface	智慧表面技術
RU	Radio Unit	無線電單元
SA	Services and Systems Aspects	服務與系統
SA1 WG	SA1 Working Group - Service	第 1 工作組-服務工作組
SA2 WG	SA2 Working Group - Architecture	第 2 工作組-架構工作組
SA3 WG	SA3 Working Group - Security	第 3 工作群組-安全性

縮寫	原文	中文
SAGIN	Space-air-ground integrated network	空陸海一體化運算網路
SAN	Storage Area Network	儲存區域網路
SC	Security Controls	安全控制項目
SCAS	Security Assurance Specification	資安評估準則
SDGs	Sustainable Development Goals	永續發展目標
SDN	Software Defined Networking	軟體定義網路
SEAF	Security Anchor Function	安全錨定功能
SECAM	Security Assurance Methodology	資安評估標準方法論
SGD	Stochastic Gradient Descent	隨機梯度下降法
SIEM	Security information and event management	安全性資訊與事件管理
SLA	Service Level Agreement	服務水準協議
SMC	Security Mode Command	安全模式設定
SMF	Session Management Function	連結管理功能
SMO	Service Management and Orchestration	服務管理與編排
SNG	Satellite News Gathering	衛星新聞轉播
SON	Self-Organizing Network	自我組織網路
SQL	Structured Query Language	結構化查詢語言
SSL	Secure Socket Layer	安全資料傳輸層
STIX	Structured Threat Information eXpression	網路威脅情資結構化資料交換格式
SUPI	Subscriber Permanent Identifier	用戶永久識別碼
SWG	Security Working Group	安全工作小組
TAF	Taiwan Accreditation Foundatio	財團法人全國認證基金會
TAICS	Taiwan Association of Information and Communication Standards	台灣資通產業標準協會

縮寫	原文	中文
TAXII	Trusted Automated eXchange of Indicator Information	指標資訊的可信自動交換
TLS	Transport Layer Security protocol	傳送層安全協定
TN	Terrestrial Network	地面網路
U.S. House	United States House of Representatives	美利堅合眾國眾議院
UDM	Unified Data Management	統一資料管理功能
UE	User Equipment	用戶設備
UEBA	User and Entity Behavior Analytic	使用者行為分析
UP	User Plane	使用者平面
UPA	Universal Perturbation Attack	訊號擾動攻擊
UPF	User Plane Function	使用者平面功能
uRLLC	Ultra-reliable and Low Latency Communications	超可靠低延遲通訊
uRPF	Unicast Reverse Path Forwarding	單播反向路徑轉發
VLAN	Virtual LAN	虛擬區域網路
VM	Virtual Machine	虛擬機器
VNF	Virtualized Network Function	虛擬化網路功能
VPN	Virtual Private Network	虛擬專用網路
VR	Virtual Reality	虛擬實境
Web	World Wide Web	全球資訊網
WFH	Working From Home	居家上班
XR	Extended Reality	延展實境
XSS	Cross-Site Scripting	跨站腳本攻擊
ZT	Zero Trust	零信任

附件資料

附件一、常駐履約人員工作項目

一、常駐履約人員出勤管理

本計畫之常駐履約人員出勤應每月向數位發展部提交常駐履約人員出勤紀錄。常駐履約人員應依行政院人事行政總處公告之政府行政機關辦公日曆表配合數位發展部辦公時間出勤，並派駐於數位發展部資源管理司辦公室。

經於 112 年 3 月 13 日完成常駐履約人員派駐，並依契約約定管理、定期提交常駐履約人員出勤紀錄。112 年 3 月 13 日至 11 月 30 日期間，常駐履約人員按契約約定出勤，並每月製作簽到表，逐日記載出勤情形。

二、公部門連結小組電子報

依據本計畫需求，本團隊每月發報公部門連結小組電子報，並放置於數位部官網，協助公部門連結小組於活動參與前可橫向連結，以掌握 6G 通訊標準發展方向。本團隊於履約迄今，協助各期電子報所收集相關內容如表 56。

表 56、每月電子報發報列表

2 月份電子報	
填報類別	**內容標題**
國內會議	MWC 行前交流會
國際活動	Mobile World Congress 2023
資訊分享	TWNIC-IETF 相關報告
3 月份電子報	
填報類別	**內容標題**
國內會議	5G-Advanced & 6G Technology Workshop - Apple
	MWC 2023 行動通訊大展重點趨勢研討會
國際活動	FNC 2023-未來聯網汽車研討會
	WSIS forum 2023

	2023 全球 6G 技術大會
	IEEE WCNC
資訊分享	高通白皮書:通往 6G 之路的願景、市場驅動因素和研究方向
	5G Stand-Alone 相關報告
4 月份電子報	
填報類別	**內容標題**
國內會議	ChatGPT 崛起：產業的應變及創新
	Touch Taiwan
國際活動	ICNWC 2023
	SVIAZ 2023
	MPLS SD & AI Net World 23
	6G Symposium
	Critical Communications World
	IEEE ICC
資訊分享	MWC 主題亮點
	經濟部工業局領軍重磅回歸 MWC 大秀臺灣 5G 產業戰力
	GSMA 提供後量子電信網路影響評估白皮書
5 月份電子報	
填報類別	**內容標題**
國內會議	CYBERSEC 2023 臺灣資安大會
	2023 TAICS 標準論壇 B5G/6G NTN 技術發展與應用
	COMPUTEX 2023
國際活動	Global Symposium for Regulators 2023（GSR23）
	2023 EuCNC & 6G Summit
資訊分享	The Rolling Plan for ICT Standardisation 2023
	The Evolution of Open RAN
	Industrial 5G Edge Computing – Use Cases, Architecture and Deployment
	6G 架構無線通訊網路惡意活動的預測和檢測元模型

重點成果摘要	111 年跨領域應用規劃計畫-結案報告
6 月份電子報	
填報類別	**內容標題**
國內會議	5G-Advanced & 6G Technology Workshop
	EU 資安研討會
國際活動	3GPP TSGs#100 Taipei
	2023 COMNEXT
	IETF 117
資訊分享	ETSI GS Quantum Key Distribution（QKD）016
	IOWN Global Forum Releases Its Vision 2030 White Paper Version 2.0
	Ministerial Declaration The G7 Digital and Tech Ministers' Meeting 30 April 2023
	Bharat 6G Vision
	6G Roadmap for Vertical Industries
7 月份電子報	
填報類別	**內容標題**
國際活動	WTIS-23
	AI for Good Summit
	INISCOM 2023
資訊分享	MediaTek 6G Technology White Paper-Satellite and Terrestrial Network Convergence
	Reconfigurable Intelligent Surfaces（RIS）; Use Cases, Deployment Scenarios and Requirements
	Spectrum sharing frameworks for temporary, dynamic, and flexible spectrum access for local private networks
	首台可涵蓋 4G 到 Beyond 5G/6G 頻率的氮化鎵增幅器試驗實證

	世界首次 300GHz 帶的波束成形與高速資料傳送成功
8 月份電子報	
填報類別	**內容標題**
國內會議	SEMICON TAIWAN
國際活動	Cloud Native Telcom Summit
	IoT Tech Expo
資訊分享	MEC Support for Edge Native Design
	6G Technologies for Wide Area Cloud Evolution
	2023 年 6 月愛立信行動趨勢報告
	Toward a Quantum Internet
	6G Requirement and Design Considerations
	Ofcom：Enabling mmWave spectrum for new uses
9 月份電子報	
填報類別	**內容標題**
國內會議	台歐 EU ENISA 雙向合作交流會
國際活動	ETSI Security Conference 2023
	CSNet 2023
資訊分享	ETSI launches First Software Development Group
	Beyond Speed：Promoting Social and Economic Opportunities through 6G and Beyond
	6G の整備状況(令和 4 年度末)の公表
	デジタル変革時代の電波政策懇談会 ５Ｇビジネスデザインワーキンググループ報告書
	「革新的情報通信技術(Beyond5G（6G）)基金事業」令和 5 年度社会実装･海外展開志向型戦略的プログラムの公募(第 1 回)を開始
10 月份電子報	
填報類別	**內容標題**
國內會議	2023 臺灣網路治理論壇
	EU 資安研討會

	眺望~2024 產業發展趨勢研討會
國際活動	Future Net Asia 2023
	NetworkX 2023
資訊分享	Cloud Native Manifesto: An Operator View
	6G Waves Magazine 6/2023
	ATIS' Next G Alliance and India's Bharat 6G Alliance Announce Memorandum of Understanding
	6G Spectrum Considerations
11 月份電子報	
填報類別	**內容標題**
國內會議	5G+產業新星揚帆啟航計畫-5G 產學研交流會
	5G 開放架構發展動態與應用趨勢分享會
	Meet Taipei 創新創業嘉年華
國際活動	IEEE Future Networks World Forum
	5G-ACIA 會員大會暨 Industrial 5G Day
	IEEE GLOBECOM 2023
資訊分享	6G POSITION STATEMENT
	FCC Permits Very Low Power Device Operations in 6 GHz Band
12 月份電子報	
填報類別	**內容標題**
國內會議	第八屆臺灣區塊鏈愛好者年會
國際活動	The Indo-European Conference on Standards & Emerging Technologies
資訊分享	經濟部引領臺灣網通產業躍上國際舞台 共創全球 5G 革新時代
	6G 專網服務管理系統資安評估指引
	Shaping Tomorrow:The Evolution of Personalized Digital Experiences Through 6G Technologies

資料來源：本計畫整理

三、專案工作會議

依據本計畫書需求指示，應配合數位發展部指定之時間召開工作會議說明全案規劃及進度，以利進度管考。本團隊於履約期間迄今，配合數位部辦理之工作會議及討論重點彙整如表 57。

表 57、每月工作會議討論重點

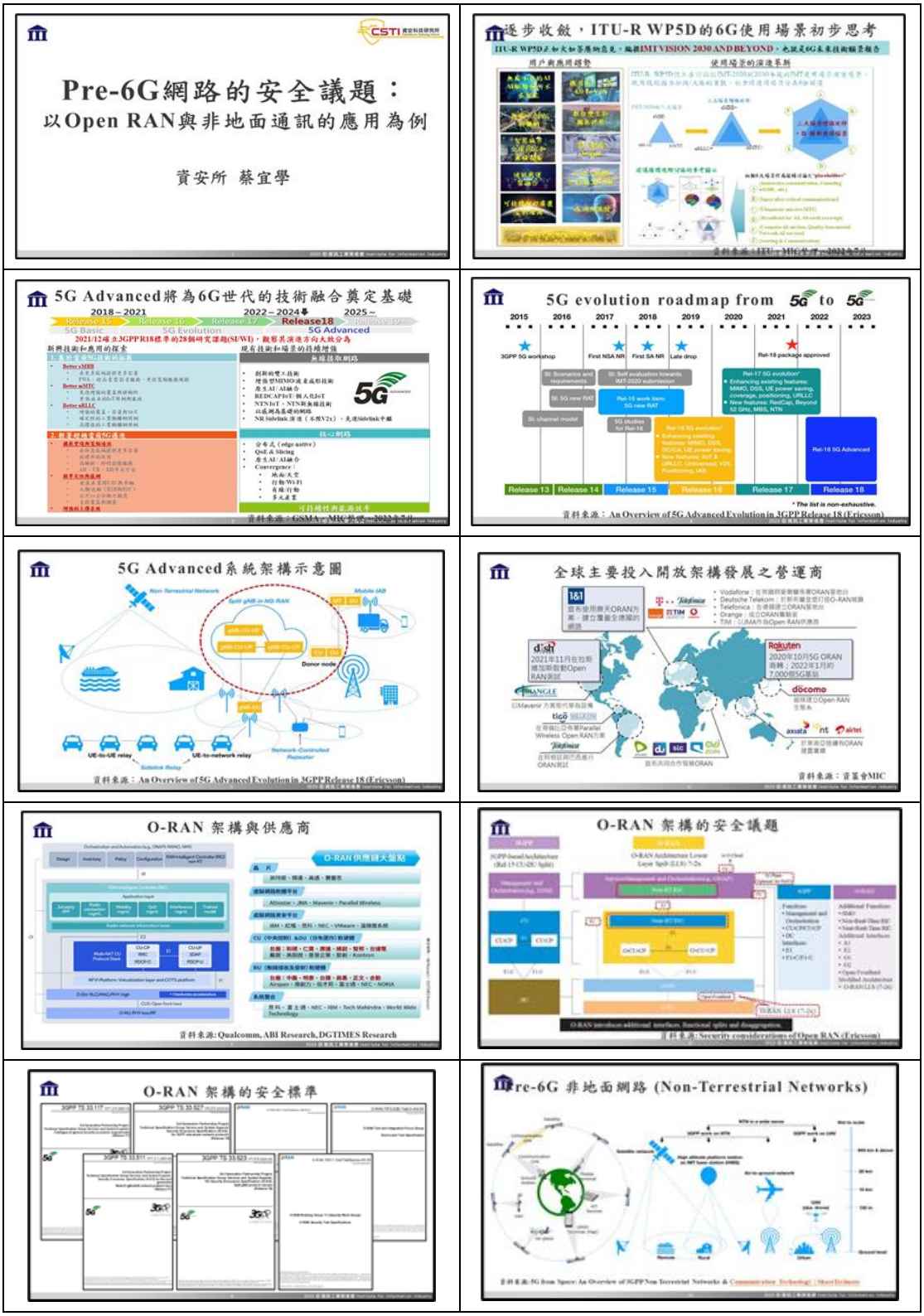
會議日期	會議內容	
3/27	報告事項	1. 執行規劃期程之甘特圖：調整甘特圖進度及各工作項查核點。 2. 期中報告預計於 7 月 12 日提出，請於 6 月底先提供期中報告草稿。 3. 公部門連結小組會議： (1) 邀請民間諮詢委員參與，請聯繫委員參與方式之建議、方法或推薦人選。 (2) 後續各場會議，皆新增報告歷次電子報各工作組填報比例。
4/20	報告事項	1. 各工作項進度報告：報告 4 月工作進度項目。 2. 公部門連結小組：邀請民間諮詢委員會參加公部門連結小組。
	臨時動議	請協助針對 GSMA Open-API 議題進行研析。
6/1	報告事項	1. 各工作項進度報告：報告 5 月工作進度項目。 2. 座談會議：因應座談會議時程調整，同步更新執行規劃時程表。 3. 因應期中報告時程，故 7 月份工作會議將暫停乙次。
9/13	報告事項	1. 各工作項進度報告：報告 8 月及 9 月工作進度項目。 2. 本案各項目之實證，應補充使用的軟硬體、使用情境及模擬原因。

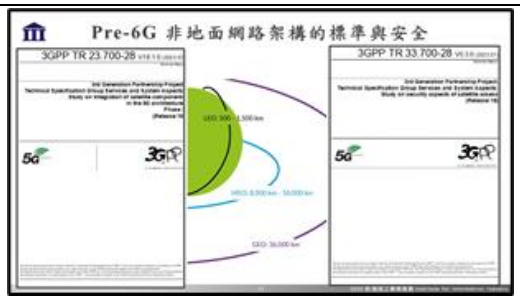
會議日期	會議內容	
		3. 112 年 7 月 31 日期中報告審查會議結論之 10 月份工作會議增列本案進度成果先期討論議題，預計於 10 月 11 日召開工作會議。
10/11	報告事項	各工作項進度報告：針對各工作項之測試實證進行報告。

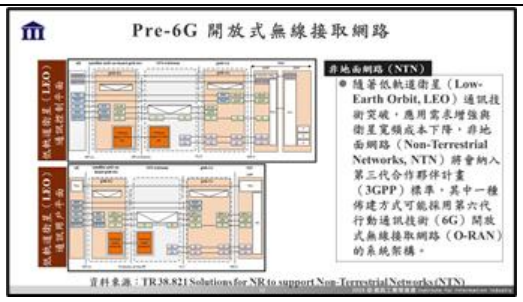
資料來源：本計畫整理

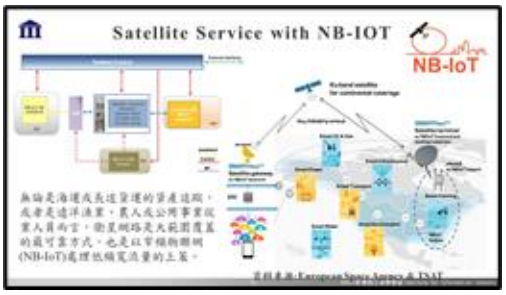
附件二、6G 資安產業研析座談會

一、支援零信任(ZT)架構的定期評估會議簡報

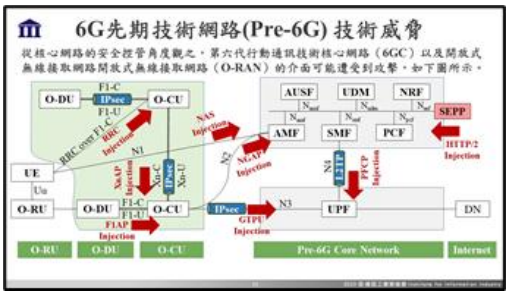



Pre-6G 非地面網路架構的標準與安全
3GPP TR 23.700-28
3GPP TR 33.700-28


Pre-6G 開放式無線接取網路
非地面網路（NTN）
隨著低軌道衛星（Low-Earth Orbit, LEO）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（Non-Terrestrial Networks, NTN）將會納入第三代合作夥伴計畫（3GPP）標準，其中一種佈建方式可能採用第六代行動通訊技術（6G）開放式無線接取網路（O-RAN）的系統架構。
資料來源：TR38.821 Solutions for NR to support Non-Terrestrial Networks (NTN)


Satellite Service with NB-IOT
NB-IoT

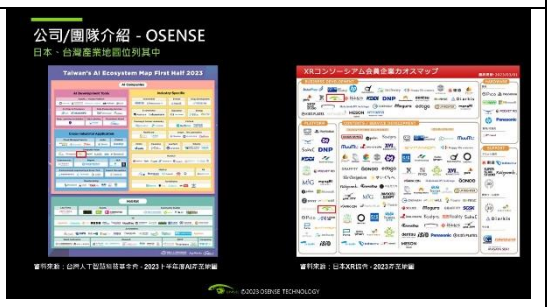

6G資安威脅攻擊與偵測防護技術演進
1G
2G
3G
4G
5G
6G

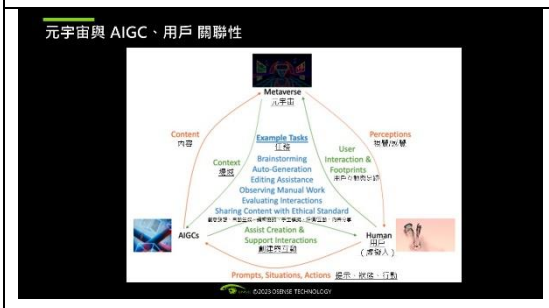

6G先期技術網路(Pre-6G) 技術威脅
O-DU
O-CU
O-RU
UE
AUSF
UDM
NRF
AMF
SMF
PCF
SEPP
UPF
DN
Pre-6G Core Network
Internet

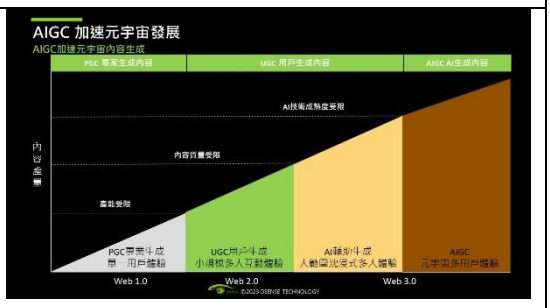

RAN-Release 19 Workshop
RAN-Release 19 workshop - Meeting information
You Are Cordially Invited

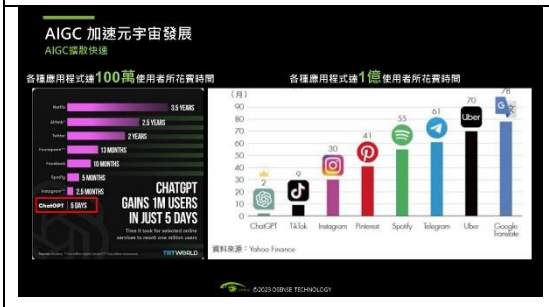

Q&A

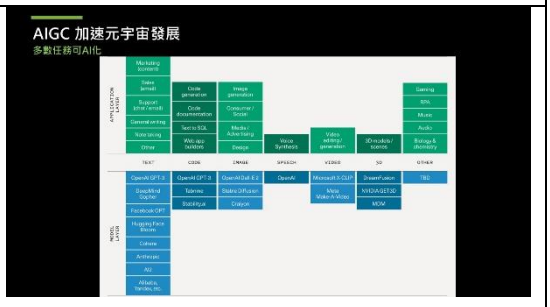
二、用 AI 感知世界 以資安防護未來會議簡報












元宇宙中 AIGC 與 虛擬人 的應用
AIGC + 虛擬人 -> 元宇宙
AI × XR


元宇宙中 AIGC 與 虛擬人 的應用
GPT-4
AI主播報氣象

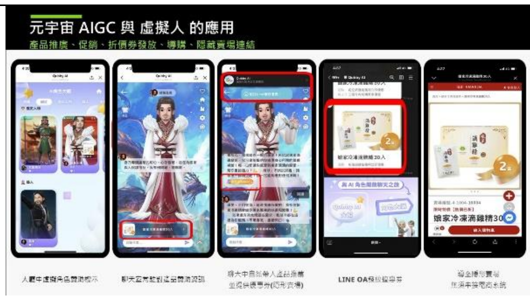

元宇宙中 AIGC 與 虛擬人 的應用


元宇宙 AIGC 與 虛擬人 的應用
AI助理
O2O AI reception
AI NPC

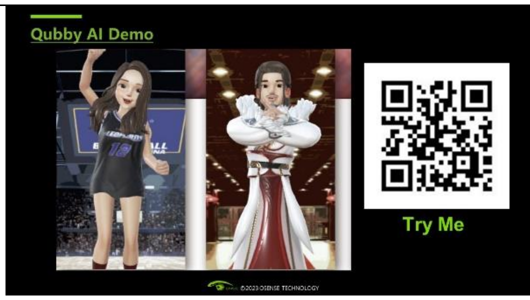

元宇宙 AIGC 與 虛擬人 的應用
AI數位分身

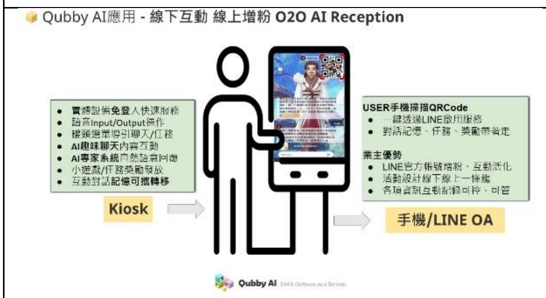

元宇宙 AIGC 與 虛擬人 的應用
AI數位分身
深度交流：AI 數位分身創造新情境


元宇宙 AIGC 與 虛擬人 的應用


元宇宙 AIGC 與 虛擬人 的應用


OSENSE AI數位分身特點
最低摩擦
使用者樂趣
沉浸感強化
行銷推廣
高流量轉換
綁定LLM
精準行銷


Qubby AI Demo
Try Me


Qubby AI應用 - 線下互動 線上增粉 O2O AI Reception
Kiosk
手機/LINE OA


元宇宙、AIGC快速發展的同時，
加強民眾對新科技認知與防範意識
不可忽視

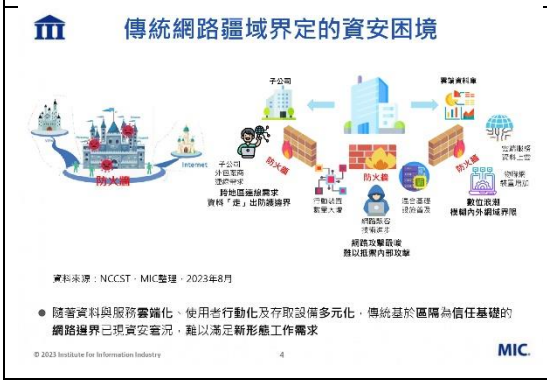

OSENSE與你一同
開啟元宇宙、AIGC、虛擬人
新展望


MIC
AIoT浪潮下資安產業發展趨勢
童啟晟
資深產業分析師兼產品經理
產業情報研究所
財團法人資訊工業策進會
2023.08.29


資訊安全產業範疇與分類


簡報大綱
●資安產業生態體系的動態觀測
●浪潮下資安產業發展方向剖析
●AI/ML應用在資安防護的案例
●企業資安轉型策略思維與布局

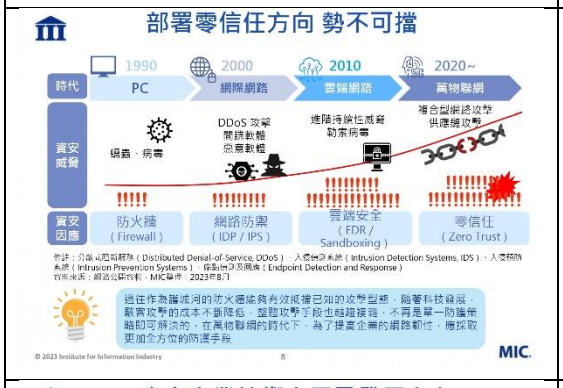

資安產業生態體系的動態觀測

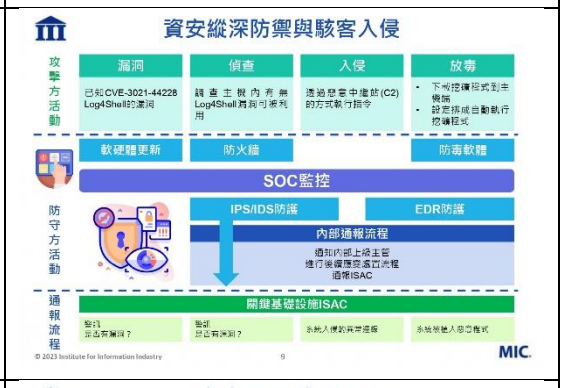

傳統網路疆域界定的資安困境
防火牆
跨地區組織需求
資料「走」出防護邊界
數位服務
模糊內外網域界限
資料來源：NCCST，MIC整理，2023年8月
隨著資料與服務雲端化、使用者行動化及存取設備多元化，傳統基於區隔為信任基礎的網路邊界已視資安常況，難以滿足新形態工作需求
MIC


近年全球知名攻擊一覽表
Colonial Pipeline
JBS
Kaseya
Olympus EMEA
Volvo
JVC Kenwood
HK Fimmick
EMIT
Acer
Asteroflash
Quanta
Kia
Oldsmar
Brenntag
Olympus
Irwenergy
ERG
MIC


近年台灣企業遭駭名單概覽
2020
2021
2022
2023
看不見的異常登入行為
VPN, AD, PrH, PrT
看不見的網路流量
Google Drive, Dropbox, Blog
看不見的惡意程式
Asset Mgr, Task schedule, Wmi, Powershell, LNK
MIC


浪潮下資安產業發展方向剖析


部署零信任方向 勢不可擋
時代
PC
網際網路
雲端網路
萬物聯網
資安威脅
資安因應
防火牆 (Firewall)
網路防禦 (IDP / IPS)
雲端安全 (FDR / Sandboxing)
零信任 (Zero Trust)
MIC

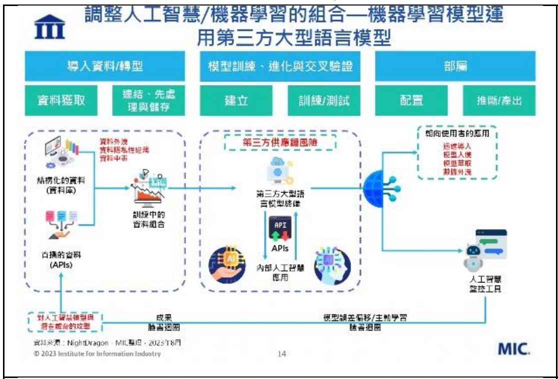

資安縱深防禦與駭客入侵
攻擊方活動
漏洞
偵查
入侵
放毒
防守方活動
軟硬體更新
防火牆
防毒軟體
SOC監控
IPS/IDS防護
EDR防護
內部通報流程
通報流程
關鍵基礎設施ISAC
MIC

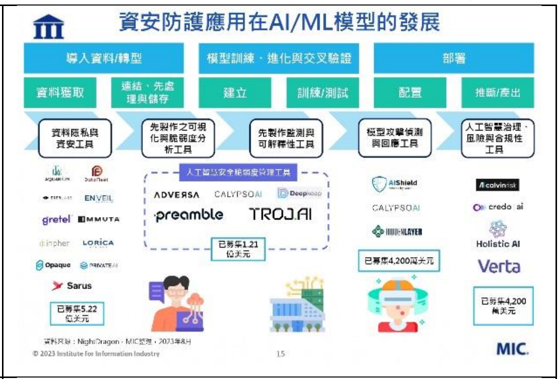

資安產業技術布局及發展方向
1. Cloud Security
2. Network Security
3. Device Security
4. Data Security
5. Enterprise IAM
6. Application Security
7. Advanced Detection & Response
8. Cyber Incident Response

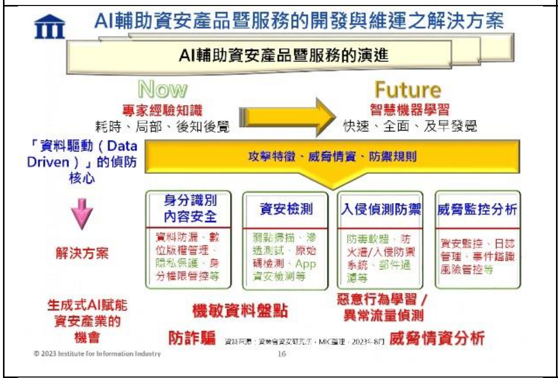

資安產業發展方向
方向1 駭客攻擊無所不在，資安防禦力成要務
方向2 賦能科技企業轉型，資安長的核心職能
方向3 遠距辦公成新常態，雲端資安持續發燒
方向4 營運科技應用場域，物聯網安全迎商機
方向5 安全存取服務邊緣，重新定義網路架構
方向6 晶片資安關鍵議題，成熟度模型成顯學
方向7 軟硬系統委外服務，供應鏈安全展韌性
方向8 零信任的網路安全，數位身分識別正夯
人
場域
產品服務
供應鏈
基礎建設
MIC


AI/ML應用在資安防護的案例

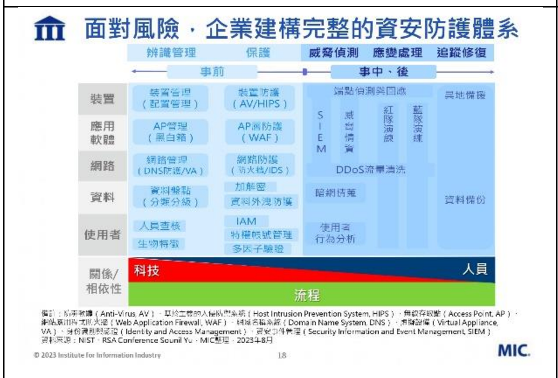

資訊安全：生成式 AI 應用服務的攻擊威脅
攻擊手法
造成威脅
超過十萬筆 ChatGPT
登錄憑據被洩露到暗網
5 月被竊憑據近 2.7 萬筆
研究進行 400 多個提問查詢
回應引用 100 個程式碼的
Python, Node.js package
虛構 150 個不存在來源
MIC


調整人工智慧/機器學習的組合—機器學習模型運用第三方大型語言模型
導入資料/轉型
模型訓練、進化與交叉驗證
部屬
資料獵取
連結、先處理與儲存
建立
訓練/測試
配置
推斷/產出
第三方供應鏈風險
第三方大型語言模型服務
APIs
內部人工智慧應用
人工智慧監控工具
MIC.

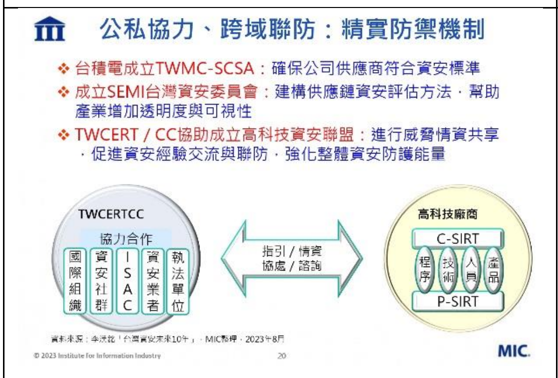

資安防護應用在AI/ML模型的發展
導入資料/轉型
模型訓練、進化與交叉驗證
部署
資料獵取
連結、先處理與儲存
建立
訓練/測試
配置
推斷/產出
資料隱私與資安工具
先製作之可視化與脆弱度分析工具
先製作監測與可解釋性工具
模型攻擊偵測與回應工具
人工智慧治理、風險與合規性工具
ADVERSA
CALYPSOAI
preamble
TROJAI
已募集1.21億美元
已募集4,200萬美元
Verta
已募集4,200萬美元
已募集5.22億美元
MIC.

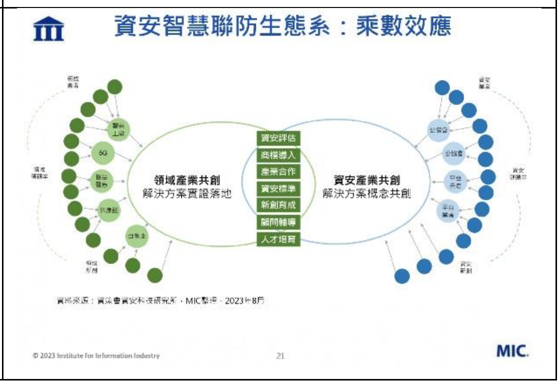

AI輔助資安產品暨服務的開發與維運之解決方案
AI輔助資安產品暨服務的演進
Now
Future
專家經驗知識
耗時、局部、後知後覺
智慧機器學習
快速、全面、及早發覺
「資料驅動（Data Driven）」的偵防核心
攻擊特徵、威脅情資、防禦規則
解決方案
身分識別內容安全
資安檢測
入侵偵測防禦
威脅監控分析
生成式AI賦能資安產業的機會
機敏資料盤點
惡意行為學習/異常流量偵測
防詐騙
威脅情資分析


企業資安轉型策略思維與布局


面對風險，企業建構完整的資安防護體系
辨識管理
保護
威脅偵測
應變處理
追蹤修復
事前
事中、後
裝置
應用軟體
網路
資料
使用者
關係/相依性
科技
人員
流程
MIC.

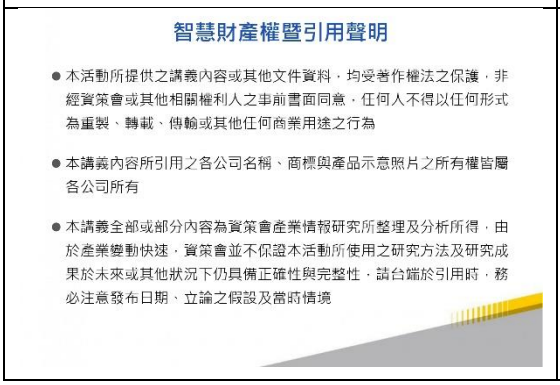

資安轉型乃企業營運當務之急
準備資安轉型
資安轉型：地位等同防禦的復原力
資安轉型：量身訂作、風險校準程式與投資
考量網路風險管理時，可以分成三個要素
1. 威脅管理
2. 弱點管理
3. 災害後果管理
資安轉型：架構議題
資安轉型：無邊界安全性
演練
在數位化的工作環境中，建立對於資安的基本認知（意識），也是確保企業數位邊界防禦的關鍵，畢竟人往往是資安最脆弱一環
The "unknown" is the biggest cyber threat businesses will face.
MIC.


公私協力、跨域聯防：精實防禦機制
台積電成立TWMC-SCSA：確保公司供應商符合資安標準
成立SEMI台灣資安委員會：建構供應鏈資安評估方法，幫助產業增加透明度與可視性
TWCERT / CC協助成立高科技資安聯盟：進行威脅情資共享，促進資安經驗交流與聯防，強化整體資安防護能量
TWCERTCC
協力合作
國際組織
資安社群
ISAC
資安業者
執法單位
指引/情資
協處/諮詢
高科技廠商
C-SIRT
程序
技術
人員
產品
P-SIRT
MIC.

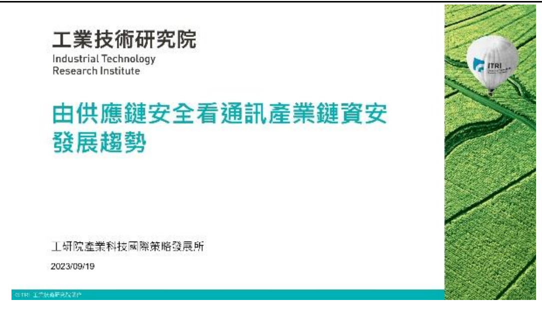

資安智慧聯防生態系：乘數效應
領域產業共創
解決方案實證落地
資安評估
商模導入
產業合作
資安標準
新創育成
顧問輔導
人才培育
資安產業共創
解決方案概念共創
MIC.


企業信任架構的調適與變革：數位轉型下的資安解藥
人
場域
產品服務
供應鏈
基礎建設
1.駭客攻擊無所不在，資安防禦力成要務
2.賦能科技企業轉型，資安長的核心職能
3.遠距辦公成新常態，雲端資安持續發燒
4.營運科技應用場域，物聯網安全迎商機
5.安全存取服務邊緣，重新定義網路架構
6.晶片資安關鍵議題，成熟度模型成顯學
7.軟硬系統委外服務，供應鏈安全展韌性
8.零信任的網路安全，數位身分識別正夯
數位賦能
資安轉型
Talent
Resilience
Unity
Security
Technology
信任對防守方才具有意義，對攻擊者而言，信任關係是攻擊利用的方式之一
© 2023 Institute for Information Industry
22

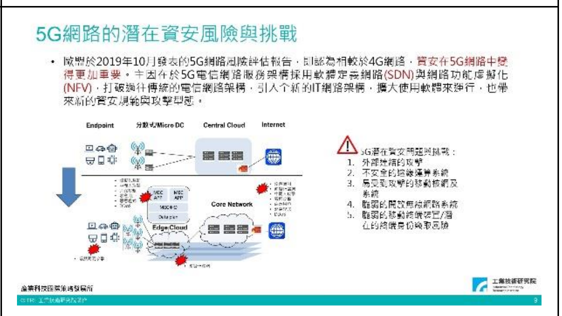

MIC
產業提昇的關鍵力量
Thank You
童啟晟 資深產業分析師兼產品經理
leotung@iii.org.tw
產業情報研究所


智慧財產權暨引用聲明
● 本活動所提供之講義內容或其他文件資料，均受著作權法之保護，非經資策會或其他相關權利人之事前書面同意，任何人不得以任何形式為重製、轉載、傳輸或其他任何商業用途之行為
● 本講義內容所引用之各公司名稱、商標與產品示意照片之所有權皆屬各公司所有
● 本講義全部或部分內容為資策會產業情報研究所整理及分析所得，由於產業變動快速，資策會並不保證本活動所使用之研究方法及研究成果於未來或其他狀況下仍具備正確性與完整性，請台端於引用時，務必注意發布日期、立論之假設及當時情境

三、從 5G 到 6G 邊緣運算資安的變革與商機會議簡報

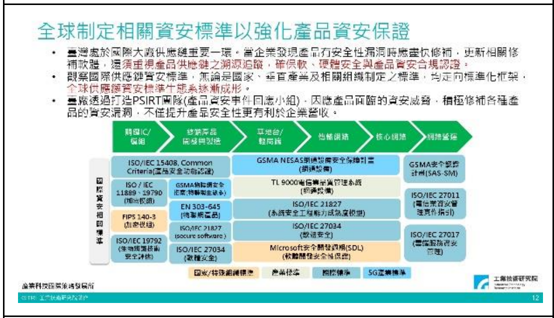


階段	原則
了解風險	1. 了解需要保護的內容以及原因 2. 了解您的供應商是誰並了解他們的安全狀況 3. 了解您的供應鏈帶來的安全風險
建立控制	4. 向供應商傳達您對安全需求的看法 5. 為您的供應商設定和傳達最低安全要求 6. 將安全考慮納入您的合約流程，並要求您的供應商也這樣做 7. 履行您作為供應商和消費者的安全責任 8. 提高供應鏈內的安全意識 9. 為安全事件提供支持
檢查供應商	10. 將確保安全活動納入您的供應鏈管理
持續性改善	11. 鼓勵持續改進供應鏈內的安全性 12. 與供應商建立信任




製造業供應鏈急需落實資安管理

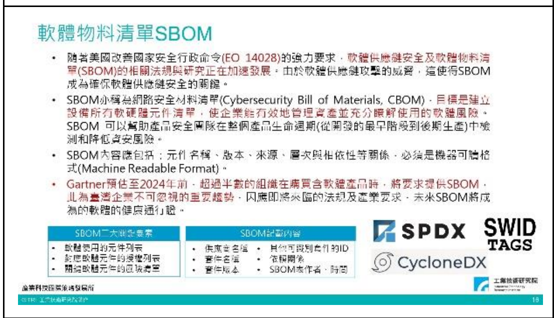

軟體供應鏈攻擊持續發生

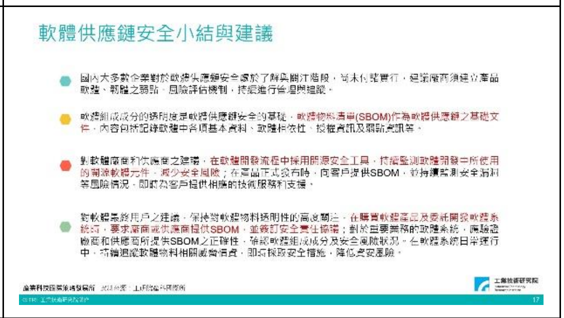

全球制定相關資安標準以強化產品資安保證


簡報大綱
一、供應鏈安全趨勢
二、通訊產業鏈資安威脅
1. 軟體供應鏈安全
2. 產品資安
三、ICT供應鏈資安的機會與挑戰
四、結論與建議

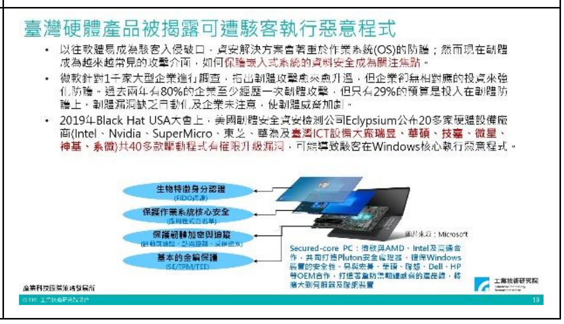

軟體供應鏈開源化趨勢 導致資安風險加劇


軟體供應鏈的安全挑戰

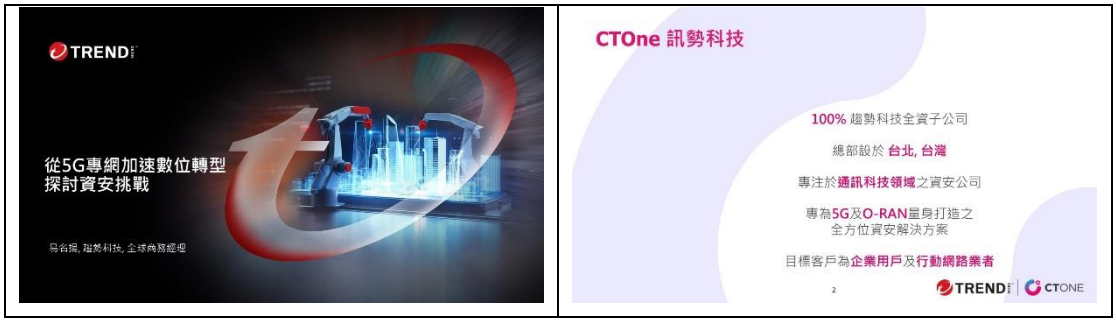

軟體物料清單SBOM
SPDX
SWID TAGS
CycloneDX

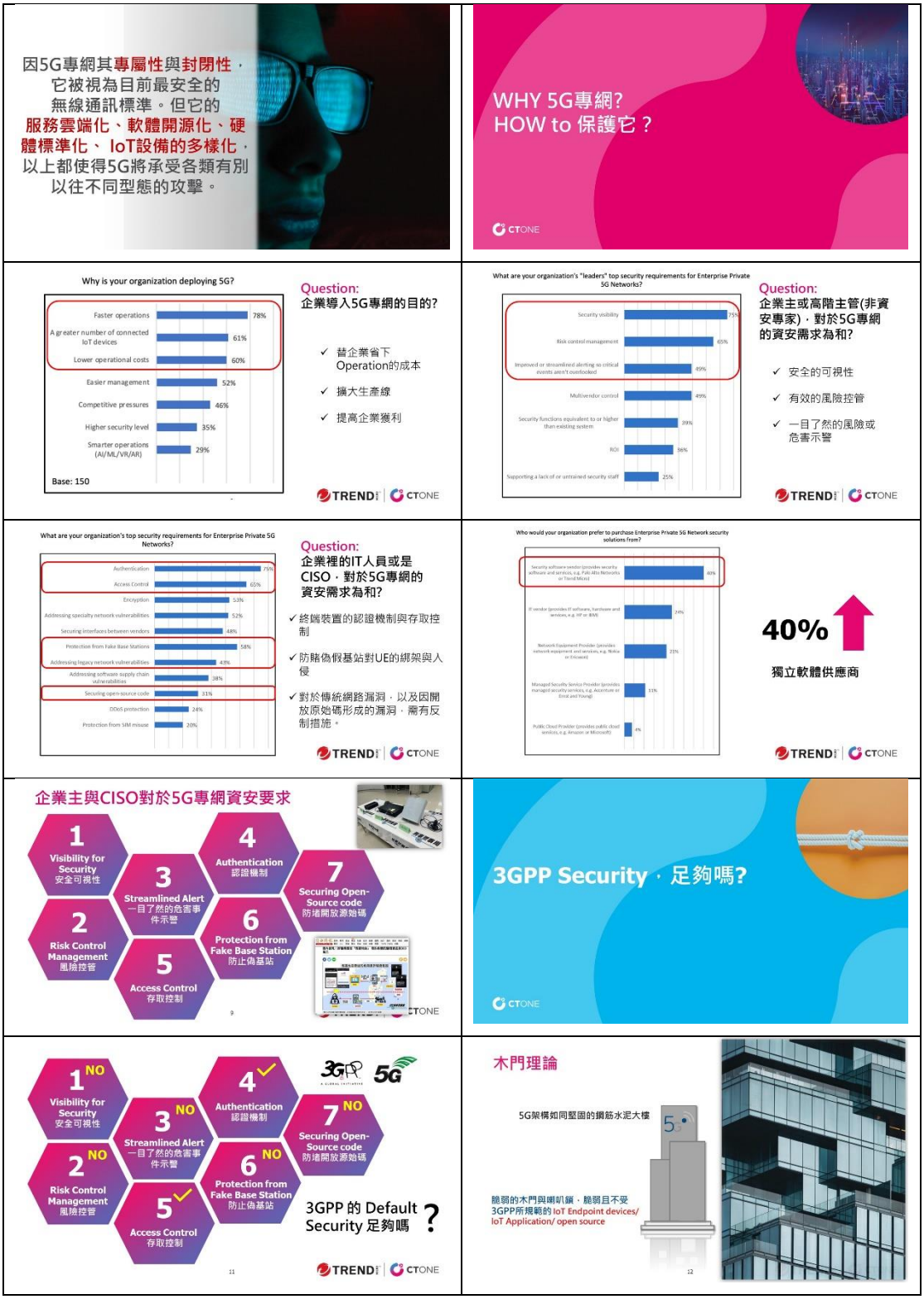

軟體供應鏈安全小結與建議


簡報大綱
一、供應鏈安全趨勢
二、通訊產業鏈資安威脅
1. 軟體供應鏈安全
2. 產品資安
三、ICT供應鏈資安的機會與挑戰
四、結論與建議

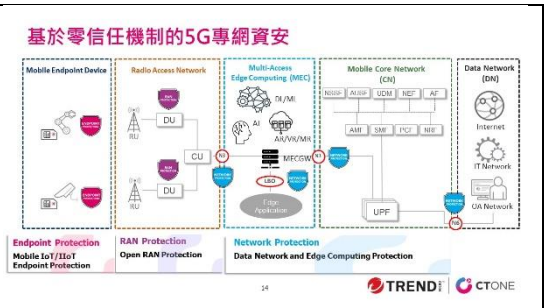

臺灣硬體產品被揭露可遭駭客執行惡意程式

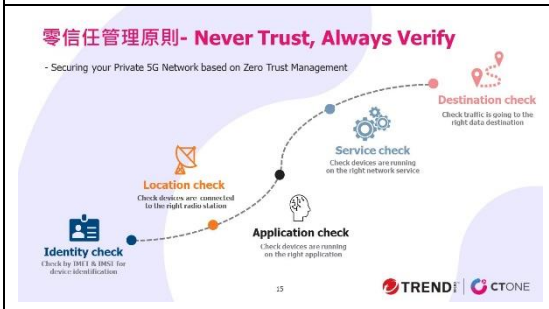

產品資安是供應鏈安全重要環節
Secure by Design
Privacy by design
事件處理
外部溝通
教育訓練
歐美政府制定相關政策強化產品資安
強化產品資安漏洞處理流程 為消費者負責
簡報大綱
一. 供應鏈安全趨勢
二. 通訊產業鏈資安威脅
1. 軟體供應鏈安全
2. 產品資安
三. ICT供應鏈資安的機會與挑戰
四. 結論與建議
供應鏈資安與產品資安為重要資安議題
供應鏈安全被視為企業採購規範一部份
物聯網產品要求安全生命週期資安防護
軟體供應鏈溯源追蹤與透明化
簡報大綱
一. 供應鏈安全趨勢
二. 通訊產業鏈資安威脅
1. 軟體供應鏈安全
2. 產品資安
三. ICT供應鏈資安的機會與挑戰
四. 結論與建議
結論與建議
樂淨零 綠色生活 你我同行
徐嘉柱 經理
+886-3-5919207
Akuoi.Hsu@itri.org.tw
古通詩 產業分析師
HanShihKu@itri.org.tw
IEK Consulting


TREND
從5G專網加速數位轉型
探討資安挑戰
CTOne 訊勢科技
100% 趨勢科技全資子公司
總部設於 台北, 台灣
專注於通訊科技領域之資安公司
專為5G及O-RAN量身打造之
全方位資安解決方案
目標客戶為企業用戶及行動網路業者
TREND | CTONE


因5G專網其專屬性與封閉性，
它被視為目前最安全的
無線通訊標準。但它的
服務雲端化、軟體開源化、硬體標準化、 IoT設備的多樣化，
以上都使得5G將承受各類有別
以往不同型態的攻擊。
WHY 5G專網?
HOW to 保護它？
CTONE
Why is your organization deploying 5G?
Faster operations 78%
A greater number of connected IoT devices 61%
Lower operational costs 60%
Easier management 52%
Competitive pressures 46%
Higher security level 35%
Smarter operations (AI/ML/VR/AR) 29%
Base: 150
Question:
企業導入5G專網的目的?
✓ 替企業省下 Operation的成本
✓ 擴大生產線
✓ 提高企業獲利
TREND | CTONE
What are your organization's "leaders" top security requirements for Enterprise Private 5G Networks?
Security visibility 75%
Risk control management 65%
Improved or streamlined alerting so critical events aren't overlooked 49%
Multivendor control 49%
Security functions equivalent to or higher than existing system 39%
ROI 36%
Supporting a lack of or untrained security staff 25%
Question:
企業主或高階主管(非資安專家)，對於5G專網的資安需求為和?
✓ 安全的可視性
✓ 有效的風險控管
✓ 一目了然的風險或危害示警
TREND | CTONE
What are your organization's top security requirements for Enterprise Private 5G Networks?
Authentication 75%
Access Control 65%
Encryption 53%
Addressing specialty network vulnerabilities 52%
Securing interfaces between vendors 48%
Protection from Fake Base Stations 58%
Addressing legacy network vulnerabilities 43%
Addressing software supply chain vulnerabilities 38%
Securing open-source code 31%
DDoS protection 24%
Protection from SIM misuse 20%
Question:
企業裡的IT人員或是CISO，對於5G專網的資安需求為和?
✓ 終端裝置的認證機制與存取控制
✓ 防賭偽假基站對UE的綁架與人侵
✓ 對於傳統網路漏洞，以及因開放原始碼形成的漏洞，需有反制措施。
TREND | CTONE
Who would your organization prefer to purchase Enterprise Private 5G Network security solutions from?
40%
獨立軟體供應商
TREND | CTONE
企業主與CISO對於5G專網資安要求
1 Visibility for Security 安全可視性
2 Risk Control Management 風險控管
3 Streamlined Alert 一目了然的危害事件示警
4 Authentication 認證機制
5 Access Control 存取控制
6 Protection from Fake Base Station 防止偽基站
7 Securing Open-Source code 防堵開放源始碼
CTONE
3GPP Security，足夠嗎?
CTONE
1 NO Visibility for Security 安全可視性
2 NO Risk Control Management 風險控管
3 NO Streamlined Alert 一目了然的危害事件示警
4 Authentication 認證機制
5 Access Control 存取控制
6 NO Protection from Fake Base Station 防止偽基站
7 NO Securing Open-Source code 防堵開放源始碼
3GPP 5G
3GPP 的 Default Security 足夠嗎 ?
TREND | CTONE
木門理論
5G架構如同堅固的鋼筋水泥大樓
脆弱的木門與嘶吼鎮，脆弱且不受3GPP所規範的 IoT Endpoint devices/ IoT Application/ open source


基於零信任機制的5G專網資安
CTONE


基於零信任機制的5G專網資安
Mobile Endpoint Device
Radio Access Network
Multi-Access Edge Computing (MEC)
Mobile Core Network (CN)
Data Network (DN)
DU
CU
DU
AI
DL/ML
AR/VR/MR
MECSW
Edge Application
UPF
Internet
IT Network
OA Network
Endpoint Protection
Mobile IoT/IIoT Endpoint Protection
RAN Protection
Open RAN Protection
Network Protection
Data Network and Edge Computing Protection
14
TREND
CTONE


零信任管理原則- Never Trust, Always Verify
- Securing your Private 5G Network based on Zero Trust Management
Destination check
Check traffic is going to the right data destination
Service check
Check devices are running on the right network service
Location check
Check devices are connected to the right radio station
Application check
Check devices are running on the right application
Identity check
Check by IMEI & IMSI for device identification
15
TREND
CTONE


聯合防禦策略
Network Protection 加上 Endpoint Protection 的聯合防禦策略，
幫助企業加速 IT & CT 領域的資安維運。
TREND
CTONE
Endpoint Protection
Mobile IoT/IIoT Endpoint Protection
Network Protection
Data Network and Edge Computing Protection
趨勢科技與 CTOne 整合 IT & CT 領域的資安情資，搭配絕佳的端點至端點防護，
協助企業應對可能的資安威脅。
16
TREND
CTONE


TREND
Global Leader in Cybersecurity

四、B5G 邁向 6G 發展，萬物聯網探索資安應用新契機會議簡報

B5G/6G萬物聯網探索資安新契機

黃彥男
主任
Research Center for Information Technology Innovation
Academia Sinica
IEEE Fellow

Disruptive Innovation -》 Lifestyle Changes

- Electric Line
- Telephone Line
- Network Line
- Intelligent Data Line: AI + IoT + B5G/6G (AIoT)
  - B5G Killer apps (low latency, big data): GPT, Internet of Vehicles, Self Driving Vehicles, Drones, etc.

2

AIoT Opportunities

- Data, Data, Data
  - IoT generates Data
  - 5G/6G transmits Data
  - AI analyzes Data
- In addition
  - WWW Data
  - Open/Public Data
  - Government Data
  - Multidiscipline domain combined Data
- Big Data -> breakthrough innovation and efficiency

AIoT Challenges

- Share and analyze data to avoid the following issues
  - legal
  - security
  - safety
  - ethics
  - efficiency
  - Privacy
- New IoT applications using B5G or 6G must solve the above problems.

AIOT TECHNOLOGY CHALLENGES

5

IoT Characteristics

- Lack of standards/too many standards
- Vertical integration, difficult to move applications from one domain to another domain
- No clear leader in each domain
- Technologies still evolving
- No clear business model

6

IoT Security Issues

- Large scale
  - Too many sensor objects and too many connections
  - Too much private data transmitted
  - Too many communication protocols
  - Difficult to monitor and manage
- Long term operation
  - Lack of on-line update capability
  - Resource constraint, lack of computing power, battery
- No human operation and lack of supervision
  - Hard to detect errors
  - In non-secure environment, devices can be damaged, stolen or substituted.
  - Wireless communication in open environment, susceptible to attacks and interference
  - Sensors in non-secure network, no firewall protection.

7

IoT Threats

- Drones
  - In 2016, someone in Northern Ireland using Drone to take video and steal ATM passwords
  - On 4 August 2018, at least two drones armed with explosives detonated in the area where Maduro, President of Venezuela, was delivering an address to military officers in Venezuela.
  - In 2018, near Lyon France, members of Greenpeace used a drone to hit nuclear spent-fuel facility。
  - In November 2018, Check Point reported that a security hole in DJI authentication process such that a hacker can take over the control of a DJI drone.
  - On Sept 14, 2019, Two Major Saudi Oil Installations Hit by Drone Strike
- Self-Driving Vehicles

8

IOT is a Perfect Platform to Launch DDoS

- **Billions of devices**
- 24x7 on-line
- **Good computing power**： Raspberry Pi 2 having ARM Cortex-A7 and 1GB memory
- **No sufficient security protection**：for computing and power efficiency
- **Mostly using** Linux or Windows embedded systems

Example: Mirai

9

Memory Corruption Bugs

- Buffer Overflow :
- Dangling Pointers: a program attempts to access memory that has already been freed or deallocated.
- Uninitialized Pointer Dereferencing: Dereferencing a null or uninitialized pointer can result in memory access violations, leading to crashes or undefined behavior.
- Data Races: happen when multiple threads access shared memory concurrently without proper synchronization, leading to unpredictable behavior.
- Type Safety: preventing type-related errors that can lead to memory corruption or security vulnerabilities.

Memory Corruption Bugs and Computer Security

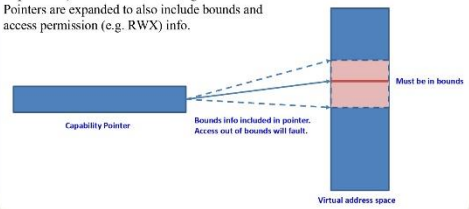
- Most critical computer security exploits these days are caused by memory corruption bugs.
- All major operating systems (e.g.: Windows, Linux, Android, MacOS) as well as many applications are all written in unsafe languages like C or C++.
- Innocent "Use after free", "Type confusion", "Integer Overflow/Underflow" bugs in these unsafe languages can result in an exploitable memory corruption bug.
- Once an exploitable memory safety bugs exists, the entire memory space of the affected process can be modified by attackers to become malicious to attack rest of system.
- There are simply too many such bugs, and we adding more bugs every day.

Capability Hardware Enhanced RISC Instructions (CHERI)

- Enhance computer security by providing hardware support for fine-grained memory protection and security capabilities.
  - RISC-V or ARM
- Fine-Grained Memory Protection:
  - dealing with memory-unsafe programming language such as C/C++.
  - each memory object (e.g., data structure or code segment) to be associated with a set of capabilities.
- Security Capabilities:
  - used to control access to memory objects, and the hardware enforces the rules associated with capabilities.
- Software Ecosystem: recompiling and adapting existing codebases.

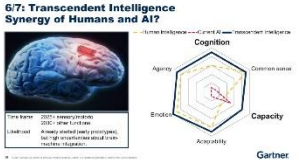
CHERI

Pointers becomes a first-class data type (called Capabilities) that the hardware recognizes
Pointers are expanded to also include bounds and access permission (e.g. RWX) info.



AI Security and Privacy Issues

AI vs Human Brain



What can Generative AI do? (BingChat)

I can do a lot of things! I can help you with writing, rewriting, improving, or optimizing your content. I can also generate imaginative and innovative content such as poems, stories, code, essays, songs, celebrity parodies, and more using my own words and knowledge.

What can Generative AI do? (ChatGPT)

Text Generation:
Content Summarization:
Code Generation:
Data Augmentation:
Art and Creativity:
Content Personalization:
Language Understanding:
Content Moderation:
Education:
Game Development:
.....

Language Translation:
Chatbots and Virtual Assistants:
Content Creation:
Image Generation:
Conversational Agents:
Storytelling:
Scientific Research:
Healthcare:
Language Generation for Accessibility:
Market Research:

Gen AI 個人助理

- Microsoft Windows 11 Copilot
- Microsoft Office 365 Copilot
- Microsoft GitHub Copilot
- Microsoft Azure Copilot
- Google Bard：整合 Google Docs、Gmail、Google 地圖、Youtube 等
- Meta "Gen AI Personas"
- Amazon CodeWhisperer, QuickSight, Bedrock,.....

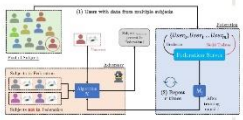
Powerful, Personalized, But Privacy?

Attacks on AI Models

- Reconstruction Attacks
- Model Inversion Attacks
- Membership-Inference Attacks
- Attribute-Inference Attacks
- Model Poisoning Attacks
- …

Membership-Inference Attacks

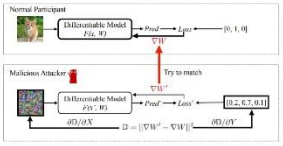
- 透過分析機器學習模型的輸出，從而推斷某個數據樣本是否被用於訓練模型。
- 攻擊步驟：
  - 攻擊者獲取黑盒機器學習模型
  - 攻擊者建構訓練集和測試集
  - 進行多次訓練得到二元分類器
  - 用來區分某個樣本是否出現
  - 樣本被判斷是否為屬於訓練集
  - 不斷優化二元分類器提高成功率



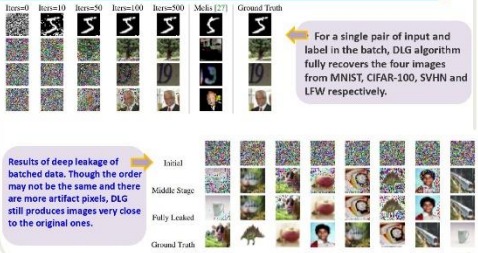
Comprehensive Privacy Analysis of Deep Learning: Passive and Active White-box Inference Attacks against Centralized and Federated Learning, Milad Nasr; Reza Shokri; Amir Houmansadr, Published in: 2019 IEEE Symposium on Security and Privacy (SP)

Methods of DLG

- The malicious attacker updates its dummy inputs and labels to minimize the gradients distance



DLG



AI Trust, Risk and Security Management (AI TRiSM)

- Gartner has found that almost 50% of AI models do not make it into production due to security, ethics or privacy issues, and 41% of organizations had experienced an AI privacy breach or security incident.
- AI TRiSM combining methods for
  - explaining AI results,
  - rapidly deploying new models,
  - actively managing AI security and controls for privacy and ethics issues.

AI Privacy Concerns

- 沒有被去識別化、匿名化、或是假名化， 從 AI 的 model 來反推個資是有可能的。
  - 所以training data 應該要先做個資保護的處理

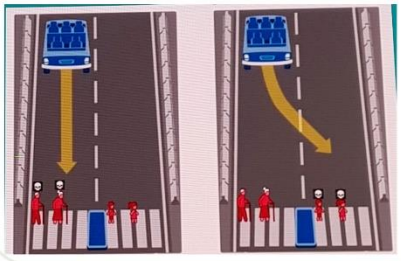
Privacy Concern for Collecting Data

- Before releasing data to third party or even open the data to the public, the data owner must first protect sensitive data attributes well to eliminate the possible of privacy leak.
- Data transmission: could be intercepted and decoded
- Both needs to be addressed…….

25

AI Ethics，Moral and Regulation

AI Ethics



AI for Weapons

The Pentagon is getting serious about AI weapons

'We must see to it that we cannot be surprised,' says the Pentagon's top scientist

AI Ethics

- Transparency
- Bias in Algorithms
- Bias in Data
- AI Security
- AI Privacy
- Accountability
- Human Dignity
- ….

Concluding Remarks

- AI + IoT +6G will change how we live and how we produce.
  - Many innovative applications and services
  - Big data, Big business
- AIoT has a lot of challenges in Security and Privacy.
- AIoT Security and Privacy R&D is very important - Whoever provides the best security and privacy solutions will win most business.

國立成功大學 National Cheng Kung University

National Cheng Kung University

後量子密碼(PQC)前瞻技術應用於 6G網路安全研析

成功大學
李南逸 教授
112/10/05

- 李南逸 教授
- 現　職：
  - 成功大學計算機與網路中心 教授
  - 計算機與網路中心網路與資安組組長
  - 成功大學電機系 合聘教授
  - 中華民國資訊安全學會理事
  - 行政院資通安全稽核委員
  - 全國認證基金會審查委員
  - 國家文官學院講座
- 主要學歷：成功大學資訊工程系博士
- 專長領域：資訊安全、密碼學、工控安全、區塊鏈、後量子密碼學
- EMAIL: nylee@gs.ncku.edu.tw

National Cheng Kung University

大綱

01 後量子密碼技術發展

02 6G網路安全威脅

03 後量子密碼於6G網路之安全防護

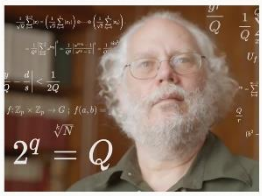
量子電腦的發展

- Google : 72 qubits (2019)
- IBM Q53 : 53 qubits (2019)
- USTC : 76 qubits (2020)
  （中國科學技術大學）
- ERR ≈10^{-3}, 1ms/1cycle
- Quantum processors are difficult to compare due to the different architectures and approaches.

IBM Quantum Computer

1994 Shor Algorithm

- Shor algorithm 是一個量子演算法，可用來計算因數分解或離散對數難題
- Using Shor quantum algorithm to crack all RSA/ECC
- 利用量子電腦，透過 Shor quantum algorithm分解整數N，只需要多項式時間



量子電腦對傳統密碼學的危機

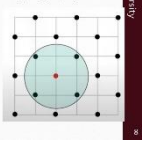
- 4099 perfectly stable qubits QC could break the RSA-2048 in 10 seconds
- 20M "imperfect" qubits QC (error rate of 0.6%) could break the RSA2048 in 8hr (2021)
- 成功大學NCKU Public Key 256 byte (RSA2048)

量子電腦對傳統密碼學的轉機

- 預計未來十年內還不會有具有此算力的量子電腦
- So …
  1. Long RSA/ECC key
  2. Quantum cryptography
  3. Post Quantum cryptography (後量子密碼學)
     - 新演算法可以保護資料免於量子電腦攻擊，並取代RSA/ECC等傳統密碼演算法

後量子密碼演算法的類型

- 分類：
  1. Lattice based encryption and signatures
     - Lattice cryptography gives another way to construct hash functions, signature schemes, public-key encryption, and more.
     - Lattices are competitive with classical cryptography, and have a strong presence in the NIST's latest post-quantum cryptography round. (Moody et al., 2020)
  2. Hash based signatures
  3. Code based encryption and signatures
  4. Multivariate based encryption and signatures



NIST PQC 標準化進程

- 2016: PQCrypto 2016
  - Call for Proposals
- 2017: Initial Posting of Round 1 Algorithms
  - 69 algorithms
- 2019: Second Round Candidates Announced
  - 26 algorithms
- 2020: Third Round Candidates Announced
  - 7 Finalists / 8 Alternates
- 2022: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates

NIST PQC 演算法標準（候選優勝）

- 金鑰封裝演算法
  - CRYSTALS-Kyber (Lattice-based)
- 數位簽章演算法
  - CRYSTALS-Dilithium (Lattice-based)
  - FALCON (Lattice-based)
  - SPHINCS+ (Hash-based)

NIST PQC Standardization – Fourth Round Candidates

- 金鑰封裝演算法
  - BIKE (Code-based)
  - HQC (Code-based)
  - Classic McEliece (Code-based)
  - SIKE (not secure)
- 徵求基於其他數學難題的數位簽章演算法…

Kyber, Dilithium, and Falcon are all lattice-based algorithms where the security is based on well-known mathematical problems in 512-1024 dimensions. The lattice-based algorithms NIST will standardize are as fast or faster than the fastest elliptic curve algorithms but have much larger public key, encapsulation, and signature sizes

Public key, encapsulation, and signature sizes in bytes

(AES-128, SHA-256, AES-192, SHA-384, AES-256)

Algorithm	Security level	I	II	III	IV	V
Kyber	Public key	800		1184		1568
	Encapsulation	768		1088		1568
Dilithium	Public key		1312	1952		2592
	Signature		2420	3293		4595

the sizes are at least twice as large as RSA and at least ten times larger than elliptic curve algorithms with the same security level

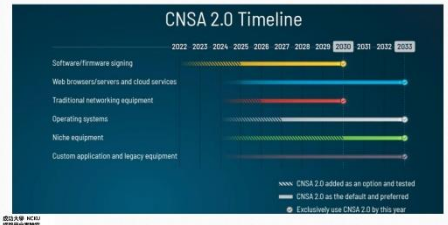
Performance in microseconds (μs)

Algorithm	Security level	I	II	III	IV	V
Kyber	Key pair generation	6.4		11.1		15.7
	Encapsulation	9.3		14.2		20.4
	Decapsulation	7.5		11.6		16.9
Dilithium	Key pair generation		28.9	38.1		59.8
	Sign		41.8	87.8		103.1
	Verify		23.2	38.4		61.0

NIST plan to recommend Level III as the default option for Kyber

National Cheng Kung University 13

美國國家安全局公布商業國家安全系統CNSA 2.0時間表



National Cheng Kung University 14

大綱

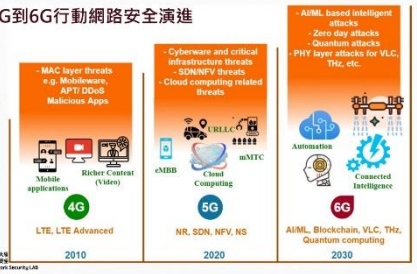
01 後量子密碼技術發展

02 6G網路安全威脅

03 後量子密碼於6G網路之安全防護

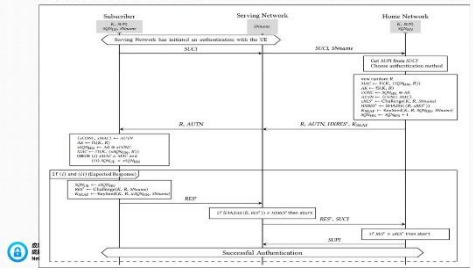
National Cheng Kung University 15

從4G到6G行動網路安全演進



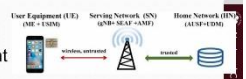
National Cheng Kung University 16

5G 身份認證與金鑰協議



National Cheng Kung University 17

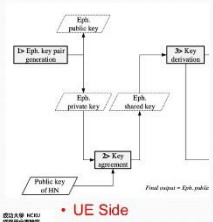
5G 身份認證與金鑰協議
Authentication and Key Agreement

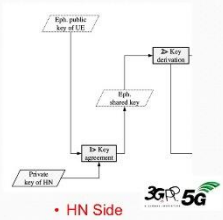


- 以身分認證與金鑰管理為基礎
- 在用戶端和網路之間進行雙向身分認證
- 並產生加密金鑰以保護控制面(Control Plane)和用戶面(User Plane)資料
- 包含三種身分認證機制
  1. EAP-AKA(Extensible Authentication Protocol–AKA)
  2. 5G-AKA
  3. EAP-TLS(Extensible Authentication Protocol–Transport Layer Security)
- 5G認證安全機制中，識別用戶身分的用戶永久訂閱辨識符(SUPI，用於唯一識別用戶)會經過加密保護後，以用戶隱藏辨識符(SUCI)進行身分認證，避免IMSI被竊聽，造成身分冒用或隨私洩漏等風險
- 5G認證安全機制中，用戶身分認證必須經由本地網路AUSF完成最終身分認證，解決服務網路遭受內部人攻擊(Insider Attack)

National Cheng Kung University 18

5G 身份認證與金鑰協議





• UE Side • HN Side

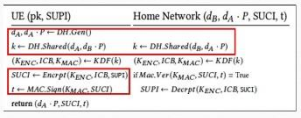
• 3Gpp ETSI TS 133 501 V15.1.0 Security architecture and procedures for 5G System (2018-07)

National Cheng Kung University 19

5G身份認證與金鑰協議之資安問題

- 遭受Linkability attack, Replay attack
- 遭受De-synchronization attacks (SQN number)
- 缺乏Forward、Backward secrecy
- 缺乏Quantum Safe

	UE	HN
pk	$H_A = d_A \cdot P$	$H_B = d_B \cdot P$
sk	d_A	d_B



Attack
Known: H_B, P
Quantum -> d_B
Capture: H_A, SUCI
De-anonymize

- Encryption
  - SUPI to SUCI (Subscription Concealed Identifier)
  - ECIES (Elliptic Curve Integrated Encryption Scheme)

National Cheng Kung University 20

6G 應用、需求與資安

• IEEE 2021 Pavani Porambage, etc.

National Cheng Kung University 21

6G 資安威脅

- Quantum computing
- More targets
  - Global network coverage
  - More IoT devices
  - Increased data traffic, low latency
- Possible attack vectors
  - Authentication attacks
  - Communication attack
  - Endpoint security

• IEEE 2021 Pavani Porambage, etc.

National Cheng Kung University 22

大綱

01 後量子密碼技術發展

02 6G網路安全威脅

03 後量子密碼於6G網路之安全防護

6G 行動網路安全設計1

- 5G標準目前定義兩種將SUPI加密為SUCI的保護方案，這兩種方案都依賴橢圓曲線整合加密方案(Elliptic Curve Integrated Encryption Scheme, ECIES)來加密SUPI
- 2022 Ulitzsch, Park, Marzougui, Seifert針對未來6G環境提出KEMSUCI
  - 解決量子電腦的威脅
  - 解決身份認證問題
  - 解決共享金鑰問題

KEMSUCI – 概念

- KEMSUCI採用後量子金鑰封裝技術(eg, Kyber)來保護SUPI

UE (pk, SUPI)	Home Network (sk, c, SUCI, t)
$(k, c) \leftarrow Kem.Enc(pk)$	$k \leftarrow Kem.Dec(sk, c)$
$(K_{ENC}, ICB, K_{MAC}) \leftarrow KDF(k)$	$(K_{ENC}, ICB, K_{MAC}) \leftarrow KDF(k)$
$SUCI \leftarrow Encrpt(K_{ENC}, ICB, \text{SUPI})$	if $Mac.Ver(K_{MAC}, SUCI, t) = \text{True}$
$t \leftarrow MAC.Sign(K_{MAC}, SUCI)$	$SUPI \leftarrow Decrpt(K_{ENC}, ICB, \text{SUCI})$
return $(c, SUCI, t)$	

KEMSUCI – 概念

- KEMSUCI採用Kyber的分析
- 優勢
  - 較快的加密速度
  - 可接受的密文長度
  - 抗量子電腦攻擊
- 劣勢
  - 較高的耗能
  - 較多記憶體需求
  - 較高的頻寬需求

Protection Schemes	Scheme Output Size (Bytes)	Public Key Size (Bytes)	Cycle Count Until Secret Establishment
KEMSUCI-LightSaber [33]	815	672	481,006
KEMSUCI-Kyber-512 [33]	847	800	551,681 ✓
ECIES-Curve25519 [21]	111 ✓	32 ✓	894391
ECIES-secp256r1 [53]	112	33	11,630,000

KEMSUCI – 其他安全問題

- KEMSUCI只注重於AKA協議中身份識別階段，未顧及其他安全性，例如
  - 阻斷服務攻擊 (Denial of Service attack)
  - 共享金鑰機密性
  - 鏈接攻擊 (Linkability attack)
  - 前、後向保密性 (Forward/Backward secrecy)

6G 行動網路安全設計2

- 2022 Damir, Meskanen, Ramezanian, Niemi針對整體協議進行優化，並提出新型後量子AKA協議
  - 解決量子電腦的威脅
  - 解決身份認證問題
  - 解決共享金鑰問題
  - 解決鏈接攻擊、重送攻擊、去同步攻擊
  - 解決前、後向保密性

6G 行動網路安全設計2：設計架構

- 3 個階段
  - 階段 A: UE發起識別請求
  - 階段 B: HN識別UE身份
  - 階段 C: 身份驗證階段
- KEM
  - Kyber, Classic McEliece, BIKE, HQC, SIKE

6G 行動網路安全設計2：量子威脅

UE

$\text{Identification\_Request}(K', \text{SUPI}, \text{ID}_{SN}, \text{ID}_{HN})$:
1) $(\text{pk}_U, \text{sk}_U) \leftarrow \textbf{KeyGen}()$.
2) $(c_1, K_{s_1}) \leftarrow \textbf{Encaps}(\text{pk}_{HN})$.
3) $\text{SUCI}_{conc} \leftarrow \text{Enc}_{K_{s_1}}(\text{SUPI} || \text{pk}_U, \text{ID}_{SN})$.
4) $\text{MAC}_U = f_1(\text{SUCI}_{conc}, K_{s_1}, K')$.
5) **Send** $(c_1, \text{SUCI}_{conc}, \text{MAC}_U, \text{ID}_{HN})$ to SN.

HN

$\text{Identification\_at\_HN}(sk_{HN}, \text{ID}_{SN}, c_1, \text{SUCI}_{conc}, \text{MAC}_U)$:
1) $K_{s_1} \leftarrow \textbf{Decaps}(c_1, \text{sk}_{HN})$.
2) $(\text{SUPI}, \text{pk}_U) \leftarrow \text{Dec}_{K_{s_1}}(\text{SUCI}_{conc})$.
3) Use SUPI to retrieve $K_{\cdot}$.
4) Compute $K' = f(\text{pk}_U, K)$.
5) $\text{MAC}'_U = f_1(\text{SUCI}_{conc}, K_{s_1}, K')$.
6) **If** $\text{MAC}_U \neq \text{MAC}'_U$ abort.
7) **Else** $(c_2, K_{s_2}) \leftarrow \textbf{Encaps}(\text{pk}_U)$.

6G 行動網路安全設計2：DoS攻擊

UE

$\text{Identification\_Request}(K', \text{SUPI}, \text{ID}_{SN}, \text{ID}_{HN})$:
1) $(\text{pk}_U, \text{sk}_U) \leftarrow \textbf{KeyGen}()$.
2) $(c_1, K_{s_1}) \leftarrow \textbf{Encaps}(\text{pk}_{HN})$.
3) $\text{SUCI}_{conc} \leftarrow \text{Enc}_{K_{s_1}}(\text{SUPI} || \text{pk}_U, \text{ID}_{SN})$.
4) $\text{MAC}_U = f_1(\text{SUCI}_{conc}, K_{s_1}, K')$.
5) **Send** $(c_1, \text{SUCI}_{conc}, \text{MAC}_U, \text{ID}_{HN})$ to SN.

$K' = f_1(pk_U, K)$ (K'主要用於身份識別)

HN

$\text{Identification\_at\_HN}(sk_{HN}, \text{ID}_{SN}, c_1, \text{SUCI}_{conc}, \text{MAC}_U)$:
1) $K_{s_1} \leftarrow \textbf{Decaps}(c_1, \text{sk}_{HN})$.
2) $(\text{SUPI}, \text{pk}_U) \leftarrow \text{Dec}_{K_{s_1}}(\text{SUCI}_{conc})$.
3) Use SUPI to retrieve $K_{\cdot}$.
4) Compute $K' = f(\text{pk}_U, K)$.
5) $\text{MAC}'_U = f_1(\text{SUCI}_{conc}, K_{s_1}, K')$.
6) **If** $\text{MAC}_U \neq \text{MAC}'_U$ abort.
7) **Else** $(c_2, K_{s_2}) \leftarrow \textbf{Encaps}(\text{pk}_U)$.

- 未知K, 攻擊者無法自行計算K'
- 無法直接傳送合法請求

6G 行動網路安全設計2：鏈接攻擊

- K_{S2}取代了RAND (明文)
- KEM封裝的K_{S2}同時抵抗量子威脅

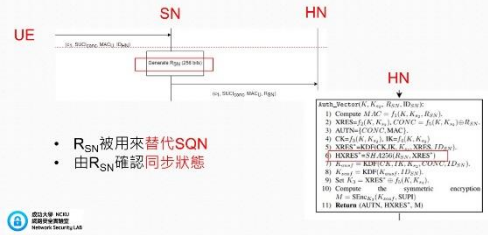
HN

$\text{Identification\_at\_HN}(sk_{HN}, \text{ID}_{SN}, c_1, \text{SUCI}_{conc}, \text{MAC}_U)$:
1) $K_{s_1} \leftarrow \textbf{Decaps}(c_1, \text{sk}_{HN})$.
2) $(\text{SUPI}, \text{pk}_U) \leftarrow \text{Dec}_{K_{s_1}}(\text{SUCI}_{conc})$.
3) Use SUPI to retrieve $K_{\cdot}$.
4) Compute $K' = f(\text{pk}_U, K)$.
5) $\text{MAC}'_U = f_1(\text{SUCI}_{conc}, K_{s_1}, K')$.
6) **If** $\text{MAC}_U \neq \text{MAC}'_U$ abort.
7) **Else** $(c_2, K_{s_2}) \leftarrow \textbf{Encaps}(\text{pk}_U)$.

UE

$K_{s_2} \leftarrow \textbf{Decaps}(c_2, \text{sk}_U)$.

6G 行動網路安全設計2：去同步攻擊



- R_{SN}被用來替代SQN
- 由R_{SN}確認同步狀態

National Cheng Kung University

結語

1. “Harvest Now – Decrypt Later” 威脅問題
2. PQC標準需要持續關注與佈局
3. 6G行動通訊網路安全的趨勢與研究尚須努力

National Cheng Kung University

國立成功大學
National Cheng Kung University

- The End -

National Cheng Kung University

Auray 耀睿科技

邁向6G O-RAN資安技術發展介紹

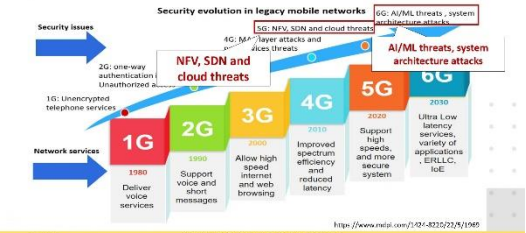
耀睿科技蔡志明
2023/10/7

www.auray.com.tw

目錄

- 行動網路演進與6G標準概況
- 6G O-RAN技術發展
- 6G O-RAN資安要求

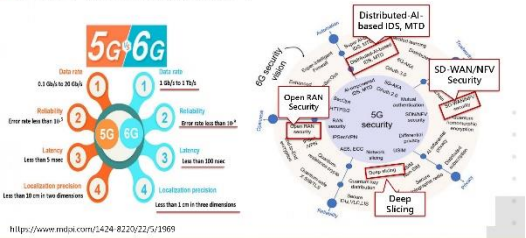
行動網路演進的關鍵技術



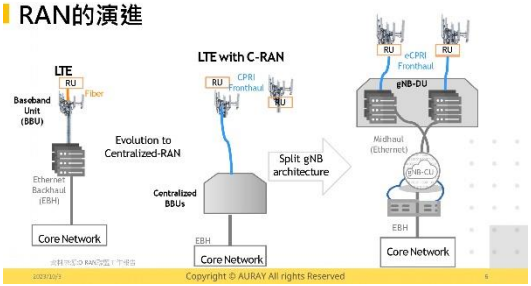
6G國際標準最新進展

- 3GPP預期於2026年開始針對6G技術及標準進行討論，樂觀判斷最早3GPP將在Release 20進行6G標準化
- 國際大多以2030年作為6G正式進入商用階段的關鍵時間點

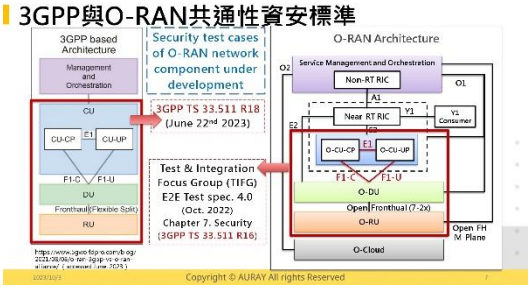
5G邁向6G的關鍵議題



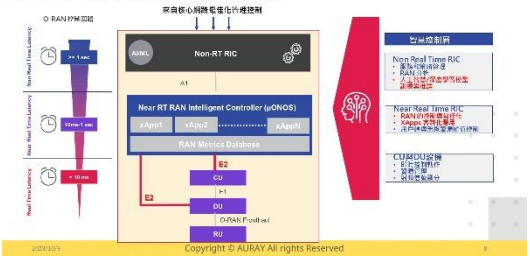
RAN的演進



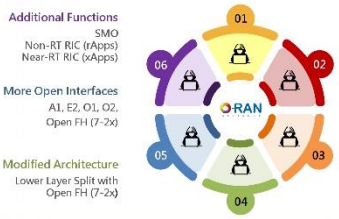
3GPP與O-RAN共通性資安標準



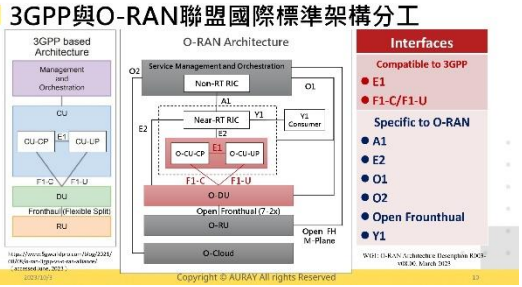
6G O-RAN關鍵技術發展



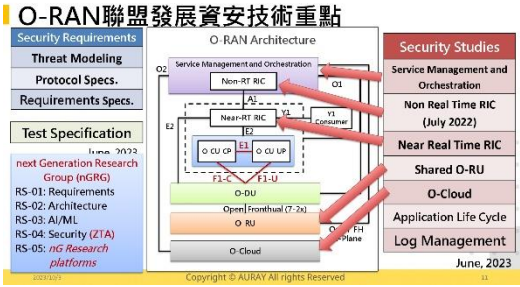
O-RAN技術的資安威脅



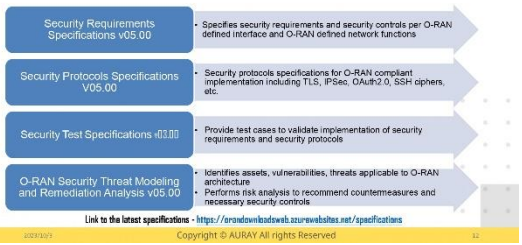
3GPP與O-RAN聯盟國際標準架構分工



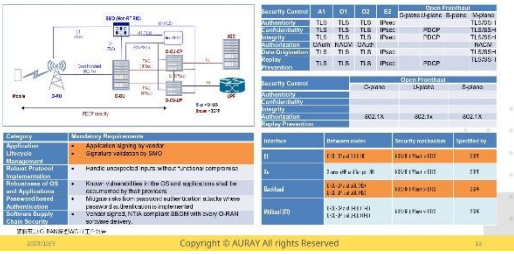
O-RAN聯盟發展資安技術重點



O-RAN聯盟發展中的資安規範



O-RAN架構的資安控制要求



O-RAN聯盟發展中的資安要求

Category	Security Focus
SMO	• Internal SMO functions/communications, external data sources and external interfaces
Non-RT RIC	• Secure on boarding and use of rApps
Near-RT RIC and xApps	• E2 authorization controls, external interfaces for RAN analytics, secure onboarding of xApps
Fronthaul C/U/S/M Planes	• IEEE 802.1X requirements, collaboration with IEEE and ITU-T on IEEE 1588 PTP Integrated security for S-plane, investigation of MACSec for security improvements
O-Cloud	• Risk assessment and development of O-Cloud platform security requirements
Automated Certificate Management for O-RAN	• O-RAN X.509v3 certificate management, using CMPv2 and ACME.
Security Log Management	• Comprehensive framework for security log management across the O-RAN
AI/ML Security	• Threat analysis and potential security controls
Application Life Cycle Management Security	• Security requirements for development, testing, onboarding, operations, and maintenance of O-RAN software
O-RU Controlled User Management	• Centralized user management for O-RU's

For details see https://www.o-ran.org/specifications

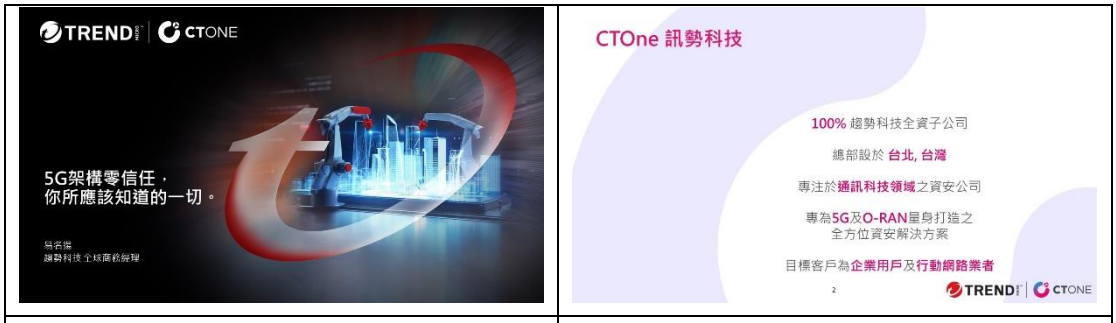
O-RAN發展中資安測試項目

O-RAN Network Functions and Apps	O-RAN Network Interfaces	O-Cloud platform	Security Infrastructure
• Near-RT RIC security including authentication and authorization for xAPPs • Non-RT RIC security • Security for SMO • AI/ML Security	• Open Fronthaul security for CUS Plane • Open Fronthaul M-plane security • A1 Interface security • E2 Interface • O1 Interface security • R1 Interface security	• Container (CNF) security including image signing • Container orchestration security • O-Cloud Notification API security • O2 Interface security (including IMS and DMS services) • Host OS hardening	• Certificate Management Framework • Security Log Management • Application Lifecycle Management (App LCM) including software signing, onboarding and deployment of application • O-RU Centralized User management • SBOM for Open-source s/w traceability

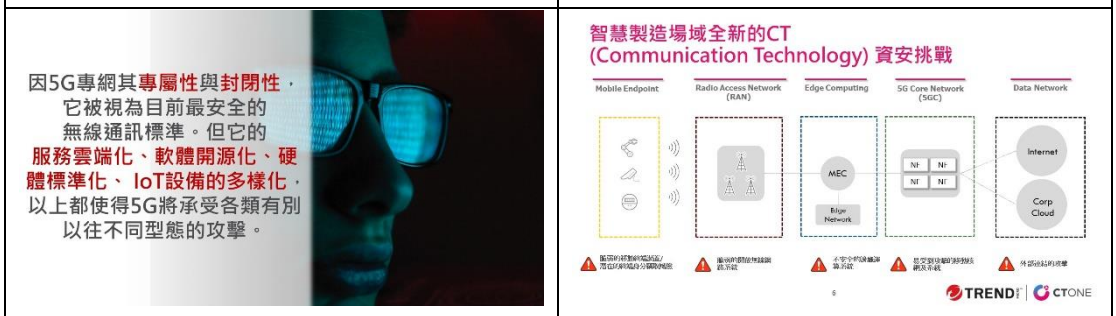
WG11 also develops security test specifications for audit and verification of security compliance

國內O-RAN資安測試標準概況


耀睿OTIC& Security Lab
O-RAN
* 5 Certificates & 2 Badges; coming more in the following months
Copyright © AURAY All rights Reserved
Auray
耀 睿 科 技
簡報完畢
敬請指教
www.auray.com.tw
service@auray.com.tw
Copyright © AURAY All rights Reserved


TREND | CTONE
5G架構零信任，
你所應該知道的一切。
CTOne 訊勢科技
100% 趨勢科技全資子公司
總部設於 台北, 台灣
專注於通訊科技領域之資安公司
專為5G及O-RAN量身打造之
全方位資安解決方案
目標客戶為企業用戶及行動網路業者


連結 IT & OT, 5G專網加速的企業數位轉型
Cloud
Server Fram/Data Center
IT/OA Networks
IT Network
CT Network
OT Network
Smart Factory
Smart Airport
Smart Port
Smart Mining
Smart Healthcare
5G無線網路所帶來的優勢
eMBB
Enhanced mobile broadband
mMTC
Massive machine-type communication
URLLC
Ultra-reliable and low latency communication
更可靠、穩定、安全的無線網路
- OPEX
- 生產力
- 企業獲利


因5G專網其專屬性與封閉性，
它被視為目前最安全的
無線通訊標準。但它的
服務雲端化、軟體開源化、硬
體標準化、 IoT設備的多樣化，
以上都使得5G將承受各類有別
以往不同型態的攻擊。
智慧製造場域全新的CT
(Communication Technology) 資安挑戰
Mobile Endpoint
Radio Access Network (RAN)
Edge Computing
5G Core Network (5GC)
Data Network
MEC
Edge Network
Internet
Corp Cloud


CT 資安責任可共同分擔, 但企業卻需承擔完全風險
3GPP
5GC Vendor
5GNR Vendor
End user (IT/InfoSEC)
IoT Endpoint Vendor
Application Vendor
5G SI/Operator
Don't just rely on your 5G service providers and existing IT tools.
Combining the communication technology mindset to build an end-to-end zero trust security strategy is the key to ensuring your critical applications run reliably and securly on the enterprise 5G networks.
3GPP Security規範
在專網內，足夠嗎？
Beyond Secure by Default
What you need to know about enterprise private 5G network security
OMDIA


企業主與CISO對於5G專網資安要求
1 Visibility for Security 安全可視性
2 Risk Control Management 風險控管
3 Streamlined Alert 一目了然的危害事件示警
4 Authentication 認證機制
5 Access Control 存取控制
6 Protection from Fake Base Station 防止偽基站
7 Securing Open-Source code 防堵開放源始碼
TREND | CTONE
1 NO Visibility for Security 安全可視性
2 NO Risk Control Management 風險控管
3 NO Streamlined Alert 一目了然的危害事件示警
4 Authentication 認證機制
5 Access Control 存取控制
6 NO Protection from Fake Base Station 防止偽基站
7 NO Securing Open-Source code 防堵開放源始碼
3GPP 5G
3GPP 的 Default Security 足夠嗎 ?
台灣專網法對於資安的要求，入網前 vs 入網後
網路之資通安全偵測及防護規劃
台灣專網法對於資安的要求，入網前? 入網後?
第 11 條
申請者應檢具下列文件，向主管機關提出申請：
一、設置申請書。
二、網路設置計畫。
(後略)
第 12 條
前條第二款之網路設置計畫應載明下列事項：
(前略)
九、使用符合有關機關國家安全考量之電信設備。
台灣專網法對於資安的要求，入網前? 入網後?
六、網路之資通安全偵測及防護規劃。
台灣專網法對於專網存取雲端服務的資安規範
連接雲端服務之應用情境規劃與資通安全維護計畫
台灣專網法對於資安的要求，連接雲端服務的資安維護計畫？
七、連接雲端服務者，應檢附應用情境規劃說明與資通安全維護計畫；其資通安全維護計畫內容應至少包含資通安全目標與維護範圍、風險評估、防護與控制措施及事件通報機制。
台灣專網法對於資安的要求，連接雲端服務者？
雲端 IoT服務
Cloud Native 5GC
連連Cloud的 On-Prem. 5GC
5GC
零信任管理原則- Never Trust, Always Verify
- 有效的網路之資通安全偵測及防護規劃
- 資通安全目標與維護範圍、風險評估、防護與控制措施及事件通報機制。
Destination check
Check traffic is going to the right data destination
Behavior check
Ensure your mobile assets operates within expected behaviors
Location check
Check devices are connected to the right radio station
Identity check
Check by IMEI & IMSI for device identification
TREND Global Leader in Cybersecurity
Ming-Yang Yi 易名揚
0905 702 716
mingyang_yi@trendmicro.com

附件三、公部門連結小組電子報

一、公部門連結小組 112 年 2 月份電子報


Vol.1 2023.02

6G
標準應用及觀測
The 6th Generation Wireless Systems

第六代行動通訊系統（The 6th Generation Wireless Systems, 6G）預估在2030年將可商規應用化。

活動訊息

■ 國內活動

MWC行前說明會	2023/2/8	相關網址：https://s.moda.gov.tw/P3cQPUTYoel4	工業技術研究院	02-2380-0716
	2023/2月下旬	相關網址：https://s.moda.gov.tw/qrNX6lE18KrA		02-6607-3882

■ 國際活動

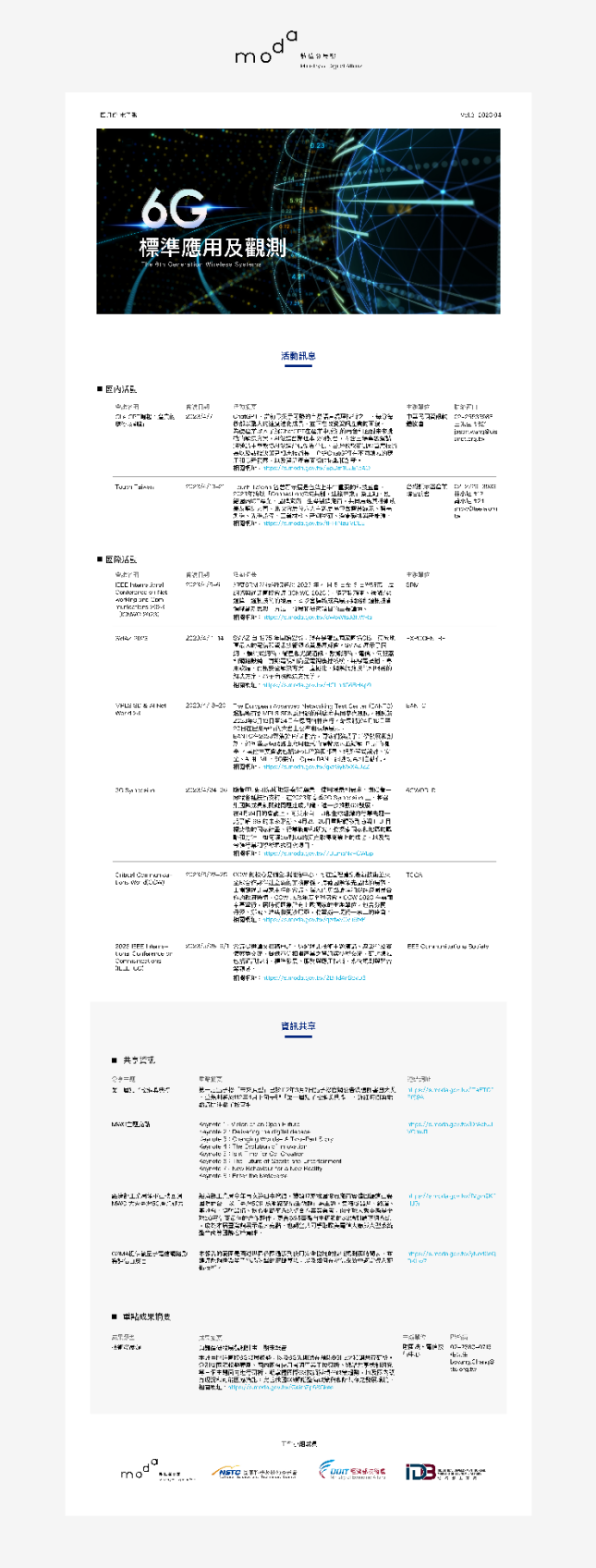
2023 Open RAN Workshop - From Research to Industry	2023/2/15-17	相關網址：https://s.moda.gov.tw/u6psZ382kGXo	EURECOM
Mobile World Congress 2023 (MWC 2023)	2023/2/27-3/2	相關網址：https://s.moda.gov.tw/VDdWM5hwN6NT	GSMA

資訊分享

TWNIC IETF	網際網路工程任務組（Internet Engineering Task Force，IETF）於西元1986年成立。Request for Comment，RFC	https://s.moda.gov.tw/c7QfedGGatUW
TAICS TC1	台灣資通產業標準協會（Taiwan Association of Information and Communication Standards, TAICS） 1. TAICS https://www.taics.org.tw/MbrJoin.aspx 2. TC1 https://www.taics.org.tw/TCMeetInfo.aspx?tcCat_id=1	https://s.moda.gov.tw/qAcd6qio5KCr
	2月17日 (https://wewideathon.tw/tw)	https://s.moda.gov.tw/XAJdkUH7eEbd
	112年2月 6G	https://s.moda.gov.tw/HEUAWGzrrzkb

二、公部門連結小組 112 年 3 月份電子報

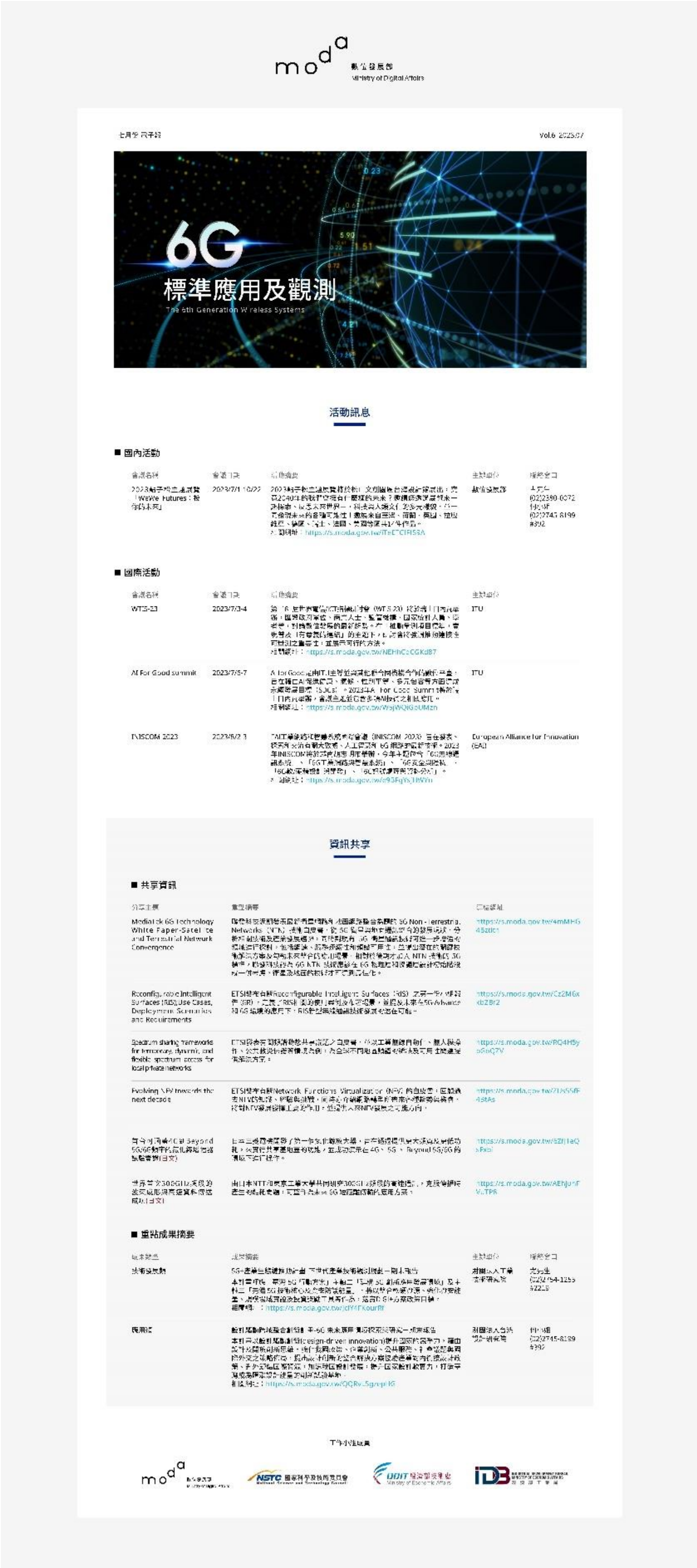
三、公部門連結小組 112 年 4 月份電子報



四、公部門連結小組 112 年 5 月份電子報

五、公部門連結小組 112 年 6 月份電子報

六、公部門連結小組 112 年 7 月份電子報



七、公部門連結小組 112 年 8 月份電子報

moda 數位發展部 Ministry of Digital Affairs

八月份 電子報 Vol.7 2023.08

活動訊息

■ 國內活動

會議名稱	會議日期	活動摘要	主辦單位	聯絡窗口
SEMICON TAIWAN	2023/9/6-8	以贏得未來為目標透過鏈結創新與永續「Inspire Innovation, Empower Sustainability」為主軸，聚焦半導體熱門議題包含先進製程、異質整合、化合物半導體、車用晶片、智慧製造、永續製造、半導體資安、人才等。 相關網址：https://s.moda.gov.tw/oZUGKMZsekn1	SEMI	李小姐 (03)560-1777 #108

■ 國際活動

會議名稱	會議日期	活動摘要	主辦單位
2023 IEEE International Symposium on Personal, Indoor and Mobile Radio Communications	2023/9/5-8	2023 IEEE pimrc將於加拿大多倫多舉辦，會議內容包括技術會議、主題演講、產業與學術論壇、展覽以及著名專家學者的研討會，並提供論文發表事宜。 相關網址：https://s.moda.gov.tw/4AdRdMHQDrpd	IEEE Communications Society
Cloud Native Telecom Summit	2023/9/12-14	雲端原生電信峰會已連續第五年舉辦，探討電信服務商如何運用新的方法和工具來支持其日益面向雲端的戰略。今年峰會強調「雲端」和「雲端原生」之間的區別，不僅是將工作負載移轉至雲端架構，更多的是思維方式和文化的轉變。 相關網址：https://s.moda.gov.tw/QQcJSqyuoP9L	TelecomTV
IoT Tech Expo EUROPE	2023/9/26-27	2023 歐洲 IoT Tech Expo將於荷蘭阿姆斯特丹舉辦，展覽聚焦於「物聯網」、「數位孿生」、「企業轉型」、「資訊安全」、「5G領域」及「邊緣運算」等議題。 相關網址：https://s.moda.gov.tw/wYPGHXA55NeX	TechEx Media

資訊共享

■ 共享資訊

分享主題	重點摘要	連結網址
MEC Support for Edge Native Design	ETSI發布了一份有關多接取邊緣運算架構(Multi access Edge Computing, MEC)支援邊緣原生(Edge Native)設計的白皮書，詳細解釋邊緣原生的概念及其對開發者在應用結構方面的重要性，並介紹了ETSI ISG MEC工作組和其他組織如何支援邊緣原生設計的示範。其中特別重要的是，白皮書指導開發者瞭解邊緣運算的原則和實際要求，以及如何將其與現代架構中的雲端原生相結合。	https://s.moda.gov.tw/qhpXqLT7dxXi
6G Technologies for Wide Area Cloud Evolution	Next G Alliance 探討有關6G廣域雲端(Wide Area Cloud, WAC)的概念，對雲端和邊緣之間的協調機制進行深入分析。	https://s.moda.gov.tw/mg3NmurJTQFH
2023年6月愛立信行動趨勢報告	愛立信基於對不同地區的行動網路數據流量成長和模式分析，分享有關未來網路演進的關鍵因素見解。同時正在著手解決下一波5G應用帶來的挑戰，強調建立新型態模型來評估行動用戶體驗(QoE)的重要性，以便設計出滿足未來服務性能需求的網路。另外，在行動設備使用「擴增實境服務」之數量不斷成長下，行動網路需要為更高的性能需求做好準備，主要方法是在現有基礎上添加新的頻譜或功能。	https://s.moda.gov.tw/akUakJCTqwjK
Toward a Quantum Internet	NTT發布有關量子網路的報告，有望實現量子感測、量子電腦網路以及量子通信，將會是長期且重要的科學和技術里程碑。本文將探討量子網路定義、實現條件以及該領域最新進展。	https://s.moda.gov.tw/oQDPzhoc2JVJ
6G Requirement and Design Considerations	NGMN聯盟對6G的若干重要需求進行定義，以過去網路演進發展，考量未來機會、挑戰及設計目標。將於技術設計的各階段與民眾、產業、城市及社區代表持續討論，確保成果同時滿足社會需求、市場導向及高效率技術開發和後續布建。	https://s.moda.gov.tw/wKUnQn6RCtcs
Enabling mmWave spectrum for new uses	英國Ofcom於2023年3月公布新增26GHz及40GHz毫米波頻譜供未來行動服務使用。	https://s.moda.gov.tw/NzJcraCYruYf

工作小組成員

moda 數位發展部 Ministry of Digital Affairs　NSTC 國家科學及技術委員會 National Science and Technology Council　DOIT 經濟部技術處 Ministry of Economic Affairs　IDB Industrial Development Bureau, Ministry of Economic Affairs 經濟部工業局

八、公部門連結小組 112 年 9 月份電子報

moda 數位發展部 Ministry of Digital Affairs

九月份 電子報 Vol.8 2023.09

活動訊息

■ 國內活動

會議名稱	會議日期	活動摘要	主辦單位	聯絡窗口
歐盟6G SNS計畫媒合會議	2023/9/6	台灣資通產業標準協會(TAICS)與歐盟6G智慧網路和服務產業協會(6G-IA)將邀集歐盟產學研機構，與台灣產學研單位直接對談交流合辦線上媒合說明會「6G Vision and Competences –Taiwan」，臺灣廠商若要參與2024年歐盟Horizon Europe 6G SNS 計畫提案，將可與國際大廠6G研發同步，展現科研實力。 相關網址：https://s.moda.gov.tw/Z3R3ws5bPGKr	經濟部技術處 TAICS ITRI	工研院廖小姐 (02)2394-6000 #2507
台歐EU ENISA雙向合作交流會 (EU Cybersecurity Workshop)	2023/9/14	數位發展部數位產業署將邀請ENISA、ETSI、JTSEC、TÜV等國內外專家及高階共同探討未來EU資安規範對於我國產業的影響，以及因應對策與建議。 相關網址：https://s.moda.gov.tw/LQQwfMa6yDAi	數位發展部 數位產業署	(02)2356-7598 #607黃小姐 #605朱小姐
點子松論壇	2023/9/21	數位發展部與台灣設計研究院合辦2023年點子松論壇，將邀請在科技設計整合上、極具前瞻視野的台灣學者與國際機構主理人，探討AI技術如何整合社會數據、應用於設計創新，入選共創的新價值及應該怎麼思三。 相關網址：https://s.moda.gov.tw/cxm9BoAiAGwM	數位發展部 台灣設計研究院	古先生 (02)2380-0072 何小姐 (02)2745-8199 #392

■ 國際活動

會議名稱	會議日期	活動摘要	主辦單位
2023 IEEE 98th Vehicular Technology Conference	2023/10/10-13	IEEE運輸技術協會(IEEE VTS)主辦之第98屆會議將於香港舉辦，匯集來自學術界、政府和工業界的人士，交流討論行動通訊及相關技術領域的想法。 相關網址：https://s.moda.gov.tw/MrfrDNyYhEqW	IEEE
ETSI Security Conference 2023	2023/10/16-19	ETSI主辦之2023年安全會議將於法國蘇菲亞舉辦，本年度將關注「安全研究」和「全球安全標準」的進行，邀集相關專家分享觀點，並亦將考慮如何吸引下一代網路安全標準化的專業人員及中小企業參與。 相關網址：https://s.moda.gov.tw/DixMbujqUwoV	ETSI
CSNet 2023	2023/10/16-18	IEEE通訊協會(IEEE ComSoc)主辦之第7屆網路安全會議(CSNet 2023)將於加拿大蒙特婁舉辦，本年度主題為「the resilient networked systems」，將邀集學界和業界人員分享未來科技前景，同時提出5G資安的威脅與挑戰。 相關網址：https://s.moda.gov.tw/P36MTvozoX2h	IEEE Communications Society

資訊共享

■ 共享資訊

分享主題	重點摘要	連結網址
Beyond Speed：Promoting Social and Economic Opportunities through 6G and Beyond	Next G聯盟發表最新的白皮書，討論未來6G行動通訊對社會和經濟的具體貢獻、數位公平等成果，以及接下來如何有效影響評估成長。	https://s.moda.gov.tw/FGiZwdiztQts
5Gの整備状況(令和4年度末)の公表	日本總務省根據行動業者報告，至2022年財務年度末，全國5G人口覆蓋率已達96.6%，較原先《日本數位城市國家基礎建設整備計畫》的目標，提前一年達成。	https://s.moda.gov.tw/srCS354o7FpC
デジタル変革時代の電波政策懇談会 5Gビジネスデザインワーキンググループ報告書	日本總務省成立的5G業務設計工作組提出報告書，透過設計有條件的拍賣制度等方式，以促進5G業務拓展。	https://s.moda.gov.tw/bF2oRJZ2h9rL
「革新的情報通信技術(Beyond 5G (6G))基金事業」令和5年度社会実装・海外展開志向型戦略的プログラムの公募(第1回)を開始	日本國家研究開發法人情報通訊機構(NICT)之「革新的情報通信技術(Beyond 5G (6G))基金事業」於2023年首次啟動，將針對全光網路(All Optical Network, AON)、非地面網路(Non Terrestrial Networks, NTN)及安全系統整合等相關議題進行首次提案公開募集。	https://s.moda.gov.tw/rwnePTBRGILC

工作小組成員

moda 數位發展部　NSTC 國家科學及技術委員會　DOIT 經濟部技術處　IDB 經濟部工業局

九、公部門連結小組 112 年 10 月份電子報

moda 數位發展部 Ministry of Digital Affairs

十月份電子報 Vol.9 2023.10

活動訊息

■ 國內活動

會議名稱	會議日期	活動摘要	主辦單位	聯絡窗口
2023臺灣網路治理論壇	2023/10/3-4	臺灣網路治理論壇是一個將網路多方利害關係群體，包括政府、學術、技術、公民等，聚集在一起共同討論網路公共政策的一個溝通互動平臺。今年度論壇將聚焦於人工智慧法規趨勢、隱私權保護、網路韌性等網路治理議題。相關網址：https://s.moda.gov.tw/6d6JvkA9Toxs	中華民國國家資訊基本建設產業發展協進會	(02)8729-1099 #213 吳先生 #287 潘小姐
EU資安研討會	2023/10/13	歐盟網路與資訊安全局已於2021年5月完成ICT產品與服務的歐盟網路安全認證(European Cybersecurity Certification, EUCC)方案，本研討會將詳細介紹EUCC所採用的資訊技術安全評估共同準則(Common Criteria, CC)與評估驗證流程，以協助ICT廠商設計研發符合歐盟規範之產品，提升未來我國進入歐盟市場的競爭力。相關網址：https://s.moda.gov.tw/RX2vQYo8Eq8W	數位發展部數位產業署	(02)2356-7698 #601 黃小姐 #605 朱小姐
眺望2024產業發展趨勢研討會	2023/10/24-27、10/30-11/3	工研院產科國際所以「跨域趨勢 x AI 崛起」為主軸，邀請超過60名資深講者，今年首度以雙周雙主軸方式進行，第一周由年度專刊《奔未來：深耕50 領融世界》於開幕論壇發表，為眺望系列研討會揭開序幕，第二周則由《生成式AI產業高峰論壇》接續探討近期熱門議題。相關網址：https://s.moda.gov.tw/yQ9z7UR55bTS	工業技術研究院產業科技國際策略發展所	(02)2737-7340 柯小姐

■ 國際活動

會議名稱	會議日期	活動摘要	主辦單位
FutureNet Asia 2023	2023/10/18-19	FUTURENET WORLD主辦之FutureNet Asia 2023將於新加坡舉辦，匯聚鄰近區域的電信業者討論對數位產業戰略及未來網路的考量，並聚焦於網路自動化及人工智慧應用。相關網址：https://s.moda.gov.tw/Nos4tFyEbknM	FUTURENET WORLD
NETWORK X 2023	2023/10/24-26	NETWORK X 年度會議將於法國巴黎舉辦，作為大型B2B電信產業盛會，將匯聚固定網路、行動網路及網路軟體領域的意見領袖，共同探索構建光纖、5G和雲端網路的獲利策略，以及電信業者如何藉由雲端連結固定網路和行動網路功能，來提升基礎設施的效率。相關網址：https://s.moda.gov.tw/VZ4pvTwhKYTG	NETWORK X

資訊共享

■ 共享資訊

分享主題	重點摘要	連結網址
Cloud Native Manifesto: An Operator View	NGMN聯盟發布關於雲端原生的重要出版品，提供從營運商觀點的關鍵原則和要求，並闡述業界需要關注的重點，以加速在行動通訊中使用雲端原生解決方案。	https://s.moda.gov.tw/SMGsy2ajFmpM
6G WAVES MAGAZINE 6/2023	6G WAVES雜誌為芬蘭6G旗艦計畫不定期出版的刊物，包含該計畫各項願景及成果，最新一期雜誌於2023年6月出刊。	https://s.moda.gov.tw/cqcNa1Wr5sXv
ATIS' Next G Alliance and India's Bharat 6G Alliance Announce Memorandum of Understanding	北美Next G聯盟與印度Bharat 6G聯盟宣布簽署合作備忘錄，深索6G技術合作機會，建立安全、可靠、具韌性的電信網路及供應鏈。	https://s.moda.gov.tw/85gh7aqRsPUE
6G Spectrum Considerations	Next G聯盟發布白皮書評估潛在適合用於6G的頻段，旨在從北美的觀點建立6G頻譜需求的全球共識。本文總結加拿大、美國及墨西哥3G至5G頻段分配概況，並對適合6G的頻段進行研究。	https://s.moda.gov.tw/N6zV2RrcZ54v

工作小組成員

moda 數位發展部 Ministry of Digital Affairs　NSTC 國家科學及技術委員會 National Science and Technology Council　DOIT 經濟部技術處 Ministry of Economic Affairs　IDB Industrial Development Bureau, Ministry of Economic Affairs 經濟部工業局

各期電子報回顧
https://s.moda.gov.tw/NPGQ6ZPZ3gNq

十、公部門連結小組 112 年 11 月份電子報

moda 數位發展部 Ministry of Digital Affairs

十一月份電子報 Vol.10 2023.11

活動訊息

■ 國內活動

會議名稱	會議日期	活動摘要	主辦單位	聯絡窗口
5G+產業新星揚帆啟航計畫-5G產學研交流會	2023/11/3	經濟部產業發展署主辦之5G產學研交流會，將於高雄市國立高雄科技大學舉辦，邀集各大專院校、5G相關實驗室教授及領航企業，分享歷年5G技術發展之產學合作經驗與成果，並透過雙向交流促進5G產業人才供需媒合。 相關網址：https://s.moda.gov.tw/pSgC7TascUBh	經濟部產業發展署	(07)601-1000 #31471 蘇小姐
5G開放架構發展動態與應用趨勢分享會	2023/11/6	資策會主辦之5G開放架構發展動態與應用趨勢分享會，將於臺北市集思交通部會議中心舉辦，邀請亞洲唯一的OTIC第三方公正實驗室及網通標竿大廠，分享全球5G產業之開放架構的發展動態、開放網路標準檢測與產業推動趨勢。 相關網址：https://s.moda.gov.tw/GvRHmZVTYq1c	財團法人資訊工業策進會	(02)6631-1407 黃小姐
Meet Taipei 創新創業嘉年華	2023/11/30 12/2	三創文化主辦之第10屆Meet Taipei 創新創業嘉年華，將於臺北市南港展覽館2館舉辦，以新創為中心，聚集創投、企業、創業育成、新創服務提供者、媒體、政府單位等臺灣創業生態圈Key Players，其中也包含資通訊新創及應用服務，一同打造最完整創業生態架構，成為創業者獲取創業所需資金、資源、與國際鏈結的機會平台。 相關網址：https://s.moda.gov.tw/RVYashaxhaDw	巨思文化股份有限公司	(02)8773-9808 #210 歷先生 #370 許小姐

■ 國際活動

會議名稱	會議日期	活動摘要	主辦單位
IEEE Future Networks World Forum	2023/11/13-15	2023 年 IEEE 未來網路世界論壇，將於美國馬里蘭州巴爾的摩舉辦，延續 IEEE 5G 世界論壇在2018年制定的路線，匯聚來自工業界、學術界和研究界的專家，進行願景交流及分享網路技術發展，包括5G、6G等跨領域的創新突破。 相關網址：https://s.moda.gov.tw/9Pdc4wuiADcE	IEEE
5G-ACIA會員大會暨Industrial 5G Day	2023/12/4-7	5G智慧工廠聯盟主辦之第5屆會員大會暨第28屆全體會議，將於臺灣臺北市舉辦，藉此吸引全球智慧製造領導廠商來臺，推動國內商機。為期一週的系列活動包含會員大會、全體會議、MOU簽署儀式、與臺灣合辦Industrial 5G Day等。 相關網址：https://s.moda.gov.tw/TeMUzr64UH9p https://s.moda.gov.tw/6MqRsfefkYAM https://s.moda.gov.tw/daR8eqqaxR9n	5G-ACIA 台灣資通產業標準協會 財團法人工業技術研究院
IEEE GLOBECOM 2023	2023/12/4-8	IEEE ComSoc 主辦之旗艦會議，將於馬來西亞吉隆坡舉行，以「促進智慧通訊共享繁榮」為主題，包含專題討論及各種主題教學研討會，預計將匯聚來自研究機構、產業界和政府代表參與。 相關網址：https://s.moda.gov.tw/soyBSBJTwq87	IEEE ComSoc

資訊共享

■ 共享資訊

分享主題	重點摘要	連結網址
經濟部成功爭取歐盟主導規劃6G計畫之聯盟首度來臺簽訂產業合作意定 推動6G跨區研發	經濟部技術處112年5月30日於臺北國際會議中心與歐盟執委會資通訊總署共同於歐盟創新週期間舉辦「2023臺歐盟6G SNS 聯合研討會」，針對臺歐盟6G願景及6G前瞻研發進行交流；更於本次會議成功爭取到歐盟主導規劃6G計畫的歐盟6G智慧網路和服務產業協會主席來臺，與台灣資通產業標準協會正式簽約，達成合作協議，未來將強化臺歐盟6G的科技研發合作。	https://s.moda.gov.tw/aDyXuCwvuncR
搶攻6G先進技術商機！經濟部率團前進瑞典 深化臺歐盟6G交流	經濟部籌組史上最大6G產業研發團隊，112年6月6日前往歐盟瑞典歌德堡參與具指標性的前瞻科研展會「歐洲網路通訊大會」，包含中華電信、仁寶、譁登、円通科技、工研院、資策會等14個單位，展示6G數位孿生應用的MR智慧眼鏡、高效節能基地臺、中低軌衛星通訊設備等19項技術。	https://s.moda.gov.tw/DZQVxdeyjkKA
6G POSITION STATEMENT	NGMN聯盟發布營運商觀點的立場聲明，採取積極主動的立場，為未來網路演進的方向提供相關意見，並強調需要以一種新的型式實現網路的演化。	https://s.moda.gov.tw/8uus5ftM76ah
FCC Permits Very Low Power Device Operations in 6 GHz Band	美國FCC宣布允許極低功率(Very Low Power, VLP)設備使用6GHz之U-NII-5和U-NII-7，共計850MHz之頻段。VLP設備功率低於其他免執照的6GHz設備，可在室內或室外進行操作，而無需任何頻率協調系統。	https://s.moda.gov.tw/AoJYSBKAjyUr

工作小組成員

moda 數位發展部 Ministry of Digital Affairs　NSTC 國家科學及技術委員會 National Science and Technology Council　DOIT 經濟部產業技術司　經濟部產業發展署 Industrial Development Administration, Ministry of Economic Affairs

各期電子報回顧
https://s.moda.gov.tw/NPGO6ZPZ3gNq

十一、公部門連結小組 112 年 12 月份電子報

moda 數位發展部 Ministry of Digital Affairs

十二月份電子報 Vol.11 2023.12

活動訊息

■ 國內活動

會議名稱	會議日期	活動摘要	主辦單位	聯絡窗口
第八屆臺灣區塊鏈愛好者年會	2023/12/7-8	臺灣區塊鏈愛好者協會主辦之年會，將於臺北市松菸文創園區舉辦，以「隱私計算」為題，探討未來 Web3 世界資安領域的深度發展，聚焦「零知識證明」、「安全多方運算技術」、「帳戶抽象」及「Layer 2技術」等方面議題。相關網址：https://s.moda.gov.tw/ZHH9GWNMpz9n	臺灣區塊鏈愛好者協會	contact@chain.tw

■ 國際活動

會議名稱	會議日期	活動摘要	主辦單位
4th The Indo European Conference on Standards & Emerging Technologies	2023/12/7	SESEI 主辦之印度-歐洲標準和新興技術會議，將於印度新德里舉辦，會議上議題包含「循環經濟」、「智慧城市連結」及「資料隱私及網路安全」，來自歐盟與印度的專家學者分享其實踐、差距及挑戰，並就合作方式提出建議。相關網址：https://s.moda.gov.tw/phefTrVPWw8J	SESEI

資訊共享

■ 共享資訊

分享主題	重點摘要	連結網址
經濟部引領臺灣5G產業躍上國際舞台 共創全球5G新時代	經濟部產業發展署112年5G產業推動成果展以「玩學5G新視界」為主題，假華山文創園區舉辦，集結300多位國內產業、學界人士共襄盛舉，共同見證我國5G產業生態鏈的佳績。另外，以「產業出題，人才實戰，以戰代訓」的5G人才研發實戰，提供學生與企業一同投入挑戰解題，並發出可用的5G解決方案，推動迄今成功引導69家企業出題，吸引近百所大專院校響應。	https://s.moda.gov.tw/4FjZEp31fGJT
6G潛力技術白皮書	台灣資通產業標準協會發表6G潛力技術白皮書，針對國際6G應用情境與技術需求發展趨勢，基於臺灣產學研各界之研發能量，並依據 ITU 於2022年11月發布之 " Rep. ITU-R M.2516-0 -Future technology trends of terrestrial IMT systems toward 2030 and beyond" 的未來技術項目，所進行臺灣產學意見調查之結果為根據，進行本白皮書技術項目之提列與撰寫方向。以臺灣產業界、學界、法人研發單位所匯集的共識，聚焦勾勒出臺灣資通訊產業於6G世代的優勢，提出臺灣6G潛力技術發展方向，作為臺灣6G政策管理與產業研發之參考依據。	https://s.moda.gov.tw/xAzKQXLenrzH
5G專網服務管理系統資安評估指引	台灣資通產業標準協會發表5G專網服務管理系統資安評估指引，參考NIST的SP 800系列標準文件，歸納出包含10大類安全領域、46個安全控制項，以進行5G場域服務管理系統的資安評估。該指引之適用範圍為針對已建置完成之5G專網場域，其中包含結合他人核心網路或接取網路。	https://s.moda.gov.tw/QeaVij3WN6Wy
Shaping Tomorrow: The Evolution of Personalized Digital Experiences Through 6G Technologies	Next G聯盟發布6G技術下個人數位體驗報告，描繪2035年三代同堂家庭的一日生活，包含購物、醫療、旅遊及保健領域，展示為每個人量身訂製的環境，勾勒未來技術發展。	https://s.moda.gov.tw/yzWprwCogq9w

■ 重點成果摘要

成果類型	成果摘要	主辦單位	聯絡窗口
技術發展類	調控電磁環境之可重構智慧面雛型平台研發報告 可重構智慧面(RIS)已成為下世代通訊的關鍵技術，除了能夠重塑場域的電磁環境，更能協助進行通訊系統的優化。但RIS須具備大尺寸、寬頻段、快重構、低功耗、簡結構等5項特徵，才能有效且實用地融入到6G無線網路中。本計畫接續2022-2023年的先期規劃計畫，規劃4年時程將近年發展的「純被動」與「可重構」電磁面技術，持續與法人機構以及產業界合作，完成「調控電磁環境之可重構智慧面雛型平台」，並進行場域驗證。 相關網址：https://s.moda.gov.tw/k7HVSFV7MRh9	國立中正大學電信研究中心	簡先生 (02) 737-7276
技術發展類	支援3D智能通訊之6G網路報告 5G進化至6G勢必會產生眾多技術缺口，連接裝置數量大幅上升，需要更加強大的MIMO多天線新型態無線技術；網路功能增加，則要求比5G更有效能及彈性化之核心網路；人與萬物連接的安全性需求增加，使節能及安全性也成為6G的重要課題；效能大幅增加導致功耗上升；加入人工智慧，並進行聯邦式學習，可最佳化整個6G網路；而將運算資源放置在邊緣端，可降低傳輸瓶頸及延遲。本計畫針對上述所有技術缺口進行研發考量，並提出解決方案。 相關網址：https://s.moda.gov.tw/V3PKAteJHaY2	國立陽明交通大學資訊工程學系	簡先生 (02) 737-7276

工作小組成員

moda 數位發展部 Ministry of Digital Affairs　NSTC 國家科學及技術委員會 National Science and Technology Council　DOIT 經濟部產業技術司　IDA 經濟部產業發展署 Industrial Development Administration Ministry of Economic Affairs

本期電子報網頁
https://s.moda.gov.tw/NPGQ6ZPZ3gNq

附件四、公部門連結小組第 1 次會議會議紀錄

一、會議時間：112 年 3 月 13 日(一)上午 10：00-11：30

二、會議地點：數位發展部新光大樓 20A01 會議室

三、主持人：數位發展部資源管理司牛司長○仁

四、與會人員：

(一)數位部資源司：沈專門委員○雄、陳科長○呈、張科員○筠

(二)數位部策略司：林科長○宜、古視察○瑋

(三)經濟部技術處：張專門委員○凱、洪科長○陽、張研究員○翔

(四)經濟部工業局：曾科長○華、尤技正○

(五)資策會：蔡副主任○霖

(六)國科會工程處：陳副研究員○鈞、簡助理研究員○洪

(七)工業技術研究院：許主任○陽、王經理○傑、王○儀、王○宇、許○庭

(八)專家學者：中興大學楊教授○章、臺灣科技大學鄧教授○中

(九)電信技術中心：王副研究員○寧

(十)台灣設計研究院：常組長○潔、向專案經理○表

五、報告事項：

(一)第一案：歷次會議列管事項執行情形說明。

決定：洽悉，持續追蹤「電信業者對 6G 需求與規劃訪談議題討論-各產業設備使用頻段等基本資訊」、「研擬舉辦聯合大型研討會之可行性」。

(二)第二案：本年度小組會議規劃及現況報告。

決定：洽悉，各工作組針對點子松計畫所提出相關建議如下：

1. 得獎作品資訊已揭露於第一期電子報，考量相關通訊及情境類之創意思維可作為各工作組 6G 應用參考，且得獎團隊亦可藉由各工作組將點子進一步落實於技術層面，爰本

部將於會後另行電郵提供臺灣設計研究院聯絡窗口，俾供各工作組進一步交流合作。

2. 點子松計畫之相關活動(如：得獎作品頒獎典禮等)請放入電子報供各工作組參考。

六、討論事項：

(一)第一案：MWC 會後心得分享交流規劃。

決議：

1. 工研院產科國際所預計於 112 年 3 月 17 日舉辦「MWC2023 行動通訊大展重點趨勢研討會」，相關活動訊息已公開於公部門連結小組 3 月份電子報中，請各工作組踴躍參與，並將為各工作組保留 1 至 2 個參加名額。
2. 由本部於研討會後，續洽工研院產科國際所確認是否有相關可公開資料得揭露於公部門連結小組 4 月份電子報。

(二)第二案：112 年 6 月份 3GPP 來臺之國際交流事宜。

決議：

1. 3GPP 來臺會議由聯發科技及台灣資通產業標準協會爭取主辦，有關公部門資源投入部分，建議工業局可再洽詢國發會亞洲矽谷之意願。
2. 請工業局持續追蹤並分享 3GPP 來臺之可公開資訊於電子報，相關可公開成果亦請於國際交流後帶回公部門連結小組會議討論。

(三)第三案：公部門連結小組資訊共享平臺之電子報推動情況。

決議：

1. 維持現有電子報發行方式，發行頻率以每月發刊為原則，發刊內容為未來兩個月之相關國內外活動。另各工作組之填報內容不限於純 6G 議題，資通訊相關領域議題亦屬可共享內容。

2. 請各工作組將 111 年度相關計畫之結案報告或研究報告分享至電子報，並以可完全公開供各界使用之內容為限。

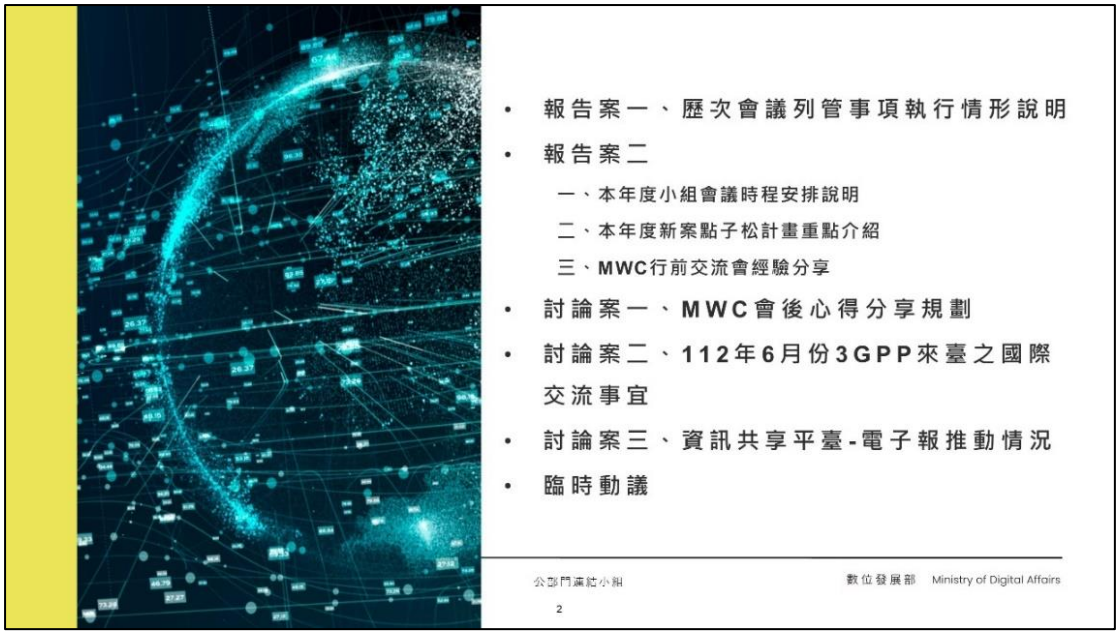
七、臨時動議：

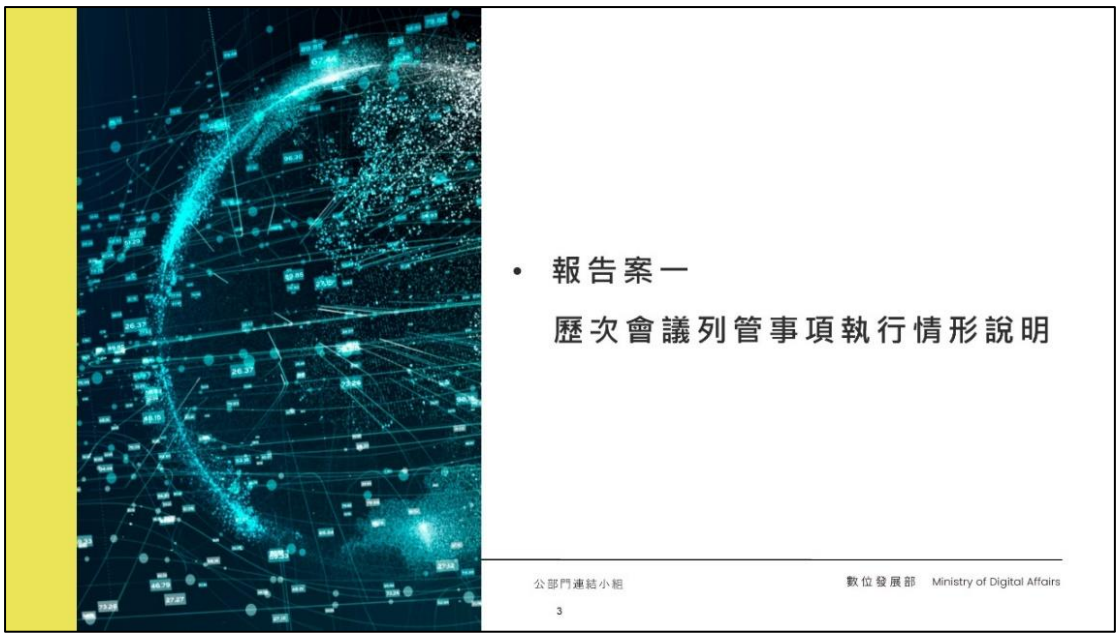
「頻譜整備暨跨域發展」工作組提出「頻段需求現況調查」議題：

1. 本案屬公部門連結小組內部之資訊協作平臺，不對外公開，供意見交換與討論之用，並非代表機關最終決定。
2. 「協作議題 1-頻段需求現況調查表」已放置於本部共筆平臺，請各工作組積極利用，並適時於該平臺給予相關回饋。
3. 各工作組亦可視需求提出協作議題，以利小組間資訊得以共享交流。

八、會議簡報


數位發展部
Ministry of Digital Affairs
moda
112年度
公部門連結小組第一次會議
資源管理司
112/3/13


報告案一、歷次會議列管事項執行情形說明
報告案二
一、本年度小組會議時程安排說明
二、本年度新案點子松計畫重點介紹
三、MWC行前交流會經驗分享
討論案一、MWC會後心得分享規劃
討論案二、112年6月份3GPP來臺之國際交流事宜
討論案三、資訊共享平臺-電子報推動情況
臨時動議
公部門連結小組
2
數位發展部 Ministry of Digital Affairs


• 報告案一
歷次會議列管事項執行情形說明
公部門連結小組
3
數位發展部 Ministry of Digital Affairs


歷次會議列管事項執行情形說明-重點追蹤事項
頻段需求
電子報
交流會議
點子松
• 各工作組如於FY112相關計畫有各產業設備使用頻段、受眾之基本資訊，請回饋到公部門連結小組，將於後續規劃之共享平台提供給各工作組參考
• 已完成資訊共享平臺-電子報發行，首發稿於2月17日公告於數位發展部官網，並由參與本公部門連結小組之各政府部會自行轉知相關產學研先進
• 業已於112年2月8日辦理MWC行前交流會，擬於MWC展後聯繫與會者獲取相關分享資訊，並分享至電子報供參
• 視各主責部會下半年度規劃，持續研擬舉辦聯合大型研討會之可行性
• 未來應用探索「點子松」於112年移撥數位部數位策略司，邀請點子松團隊於FY112第一次會議分享計畫執行規劃
公部門連結小組
數位發展部 Ministry of Digital Affairs
4

111年度第一次會議列管事項

會議場次	議題	決議	建議列管狀況	追蹤辦理情形-112.3.13
A.111年9月23日 第一次會議	A1-【第一案】 參與**國際合作**橫向支援與溝通機制之討論	為利會議資訊共享及建立產學界溝通管道，請各工作組於下次會議提供112年預計參與之相關會議清單（含時程、參加團隊名單、參與方式、議題等）及各議題項下之預期利害關係人清單。	■解除列管 □持續追蹤 □併案追蹤	• 已完成112年各工作組預計參與之國際6G相關會議清單彙整，相關資訊已在111年度第二次會議中進行議題討論（請參看111年度第一次會議簡報頁次10至12）。
	A2-【第二案】 **電信業者**對6G需求與規劃訪談議題之討論。	2.各工作組如會後有其他對電信業者訪談議題之補充，可再與本部資源管理司聯絡，俾利統整議題進行訪談。	■解除列管 □持續追蹤 □併案追蹤	• 已完成電信業者對6G需求與規劃訪談，相關資訊已於111年度第二次會議中進行議題討論（請參看111年度第二次會議簡報頁次7至9）。
		3.請各工作組協助於明年計畫履約過程中，留意目前各產業設備使用頻段受眾之基本資訊，俾利頻譜整備暨跨域發展工作組研議後續頻譜之開放方向。	□解除列管 ■持續追蹤 □併案追蹤	• 各工作組如於112年度相關計畫有**各產業設備使用頻段、受眾之基本資訊**，請回饋到公部門連結小組將於後續規劃之共享平台提供給各工作組參考。 • 112年度第一次會議之臨時動議將提請各工作組提供相關頻段需求，以利資訊交流。
	A3-【第三案】其他重要議題討論-產業諮詢小組提供議題如下： 3.各分項皆邀請專家群，技術面、標準面及頻譜面，如何**相互交流整合**	3.請各工作組研擬舉辦聯合大型研討會之可行性，俾利專家學者於會議交流整合意見，及讓業界了解政府將持續積極協助。	■解除列管 □持續追蹤 □併案追蹤	• 已於111年度第二次會議提請各工作組檢視業管計畫之大型會議，並將會議資訊放置於「資訊共享平臺」。

公部門連結小組 數位發展部 Ministry of Digital Affairs
5

111年度第二次會議列管事項1/3

會議場次	議題	決議	建議列管狀況	追蹤辦理情形-112.3.13
B.111年12月7日 第二次會議	B1-【第一案】 **電信事業訪談結果**討論案	一、針對電信業者訪談，因6G尚在發展初期，後續相關電信訪談宜採階段方式進行資訊蒐集，如：2023年MWC會議後，請電信業者及有參與的各工作組分享具潛力的應用情境與需求。	■解除列管 □持續追蹤 □併案追蹤	• 已完成電信業者對6G需求與規劃訪談，相關資訊已於111年度第二次會議中完成討論，並由訪談主責單位TTC將相關結論回覆電信業者。
		二、針對電信業者所提6G政策建議，請將回應內容放置於「資訊共享平臺」，具體內容如下： 1.國家整體推動6G政策建議 (1)政府平臺：政府來協助相關政策的制定與產業垂直與橫向串連，可邀集產、官、學、研單位，研議符合我國使用情境及需求。 (2)協助投入：可多方嘗試亦須審慎考量投入規模，更須對6G的應用面多加摸索。 (3)智慧財產布局：建議及早進行國家層面的專利佈局。	■解除列管 □持續追蹤 □併案追蹤	• 已完成資訊共享平臺-電子報建置，首發稿業已於2月17日發布，並公告於數位發展部官網，由參與本公部門連結小組之各政府部會自行轉知相關產學研先進。 • 有關「國家整體推動6G政策建議」參採意見，將於探索階段多方考量6G各應用面向之潛在議題。 • 有關智慧財產布局由雛型系統與國際布局工作組（經濟部技術處、國科會工程處）納入考量布局專利。

公部門連結小組 數位發展部 Ministry of Digital Affairs
6

111年度第二次會議列管事項2/3

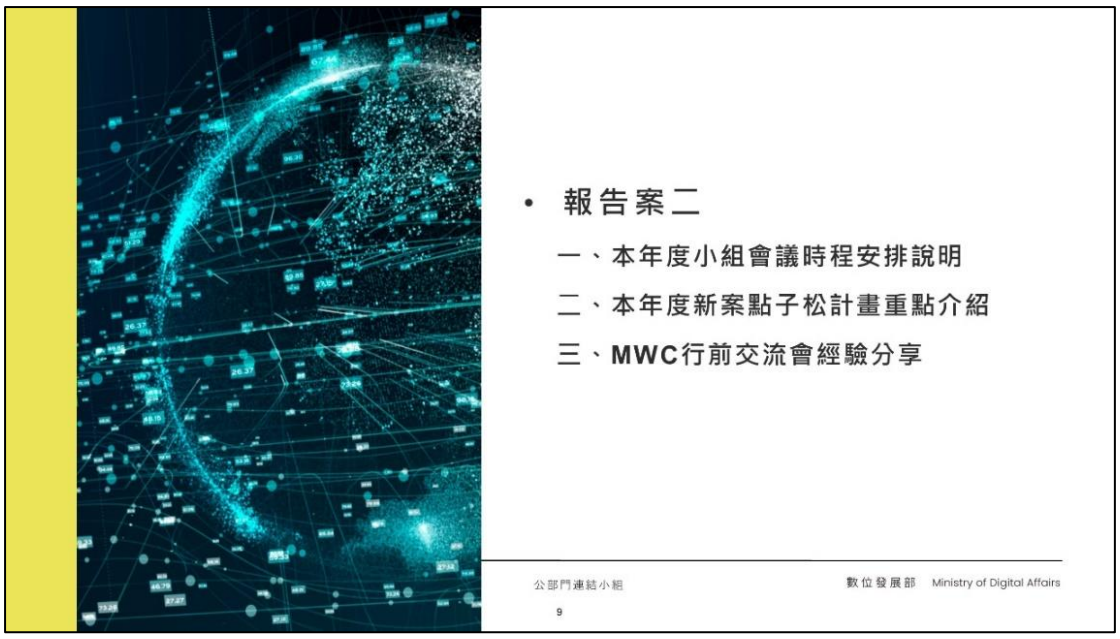
會議場次	議題	決議	建議列管狀況	追蹤辦理情形-112.3.13
B.111年12月7日第二次會議	B2-【第二案】112年各工作組參與國際會議資源術型」、「應用情境型」及「經貿交流型」），另小型國際會議揭露於「資訊共享平臺」即可。分享討論案	一、本次統計之各國際會議其屬性、規模皆不同，爰建議本項所填報國際會議可定義為大型國際會議（初步分類為「學術論文型」、「標準技	■解除列管 □持續追蹤 □併案追蹤	• 已調整相關調查表，並建置於資訊共享平臺-電子報後端填報系統 https://s.moda.gov.tw/NLx1H98ZXcwd
		二、有關大型會議部分，請各工作組重新員體盤點目前國際6G重要會議再提供參加資訊，據以瞭解國際發展現況，建議合適部會及其監管業者與產研機構出席會議，提升資訊的實用度。	■解除列管 □持續追蹤 □併案追蹤	• 已先行盤點目前國際6G重要會議(如IEEE、3GPP、MWC)，並將會議資訊放置於「資訊共享平臺」，提請各工作組一併員體盤點相關重要會議，於**每月電子報填報時追蹤各工作組填報情形**。
		三、本案盤點之重要大型國際會議包含3GPP、IEEE及MWC，有關建議各主責工作組召開行前橫向整合溝通活動，結論如下： **1.3GPP**：考量台灣資通產業標準協會（TAICS）業員相關行前討論機制供協會會員組隊參加，爰建議經濟部技術處於「資訊共享平臺」提供該協會之加入會員方式及TC1議程公開資訊。 **2.IEEE**：考量本會議皆屬於教授論文投稿性質，爰無須召開行前橫向整合溝通活動。 **3.MWC**：由數位部統籌行前橫向整合溝通活動，俾利出席該國際會議之各工作組及產學研界專家進行資訊交流。另考量MWC即將於112年2月底召開，相關行前活動之聯繫工作，請數位部積極辦理。	■解除列管 □持續追蹤 □併案追蹤	• 經濟部技術處已提供該協會之加入會員方式及TC1議程公開資訊，並公告於112年**2月版電子報**。 • 數位部業已責成工研院於112年2月8日完成辦理**MWC行前交流會**。

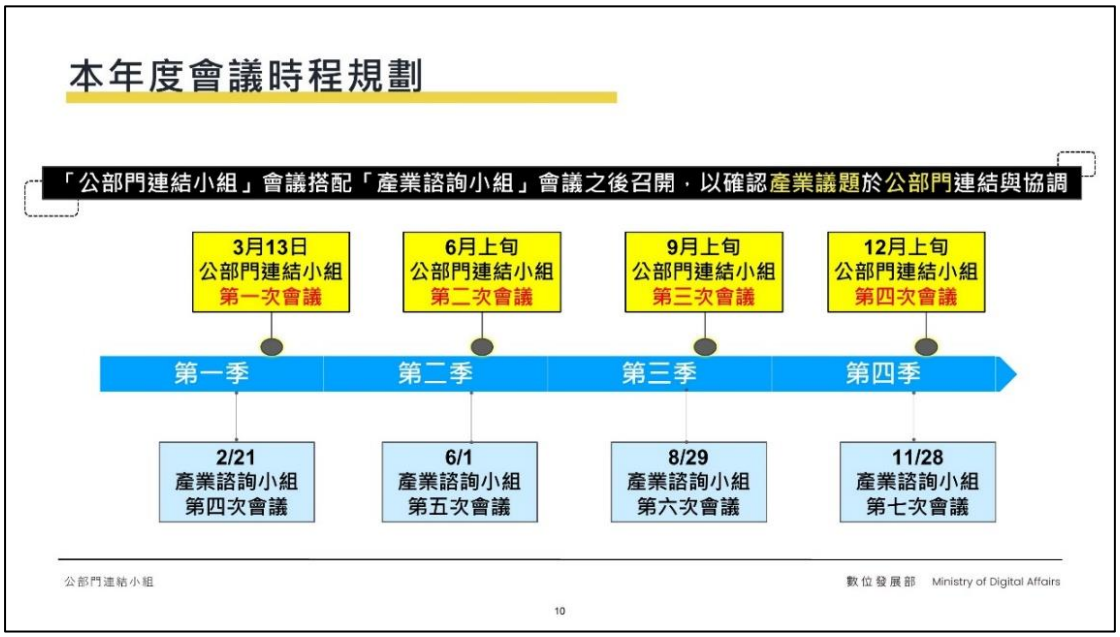
公部門連結小組 數位發展部 Ministry of Digital Affairs
7

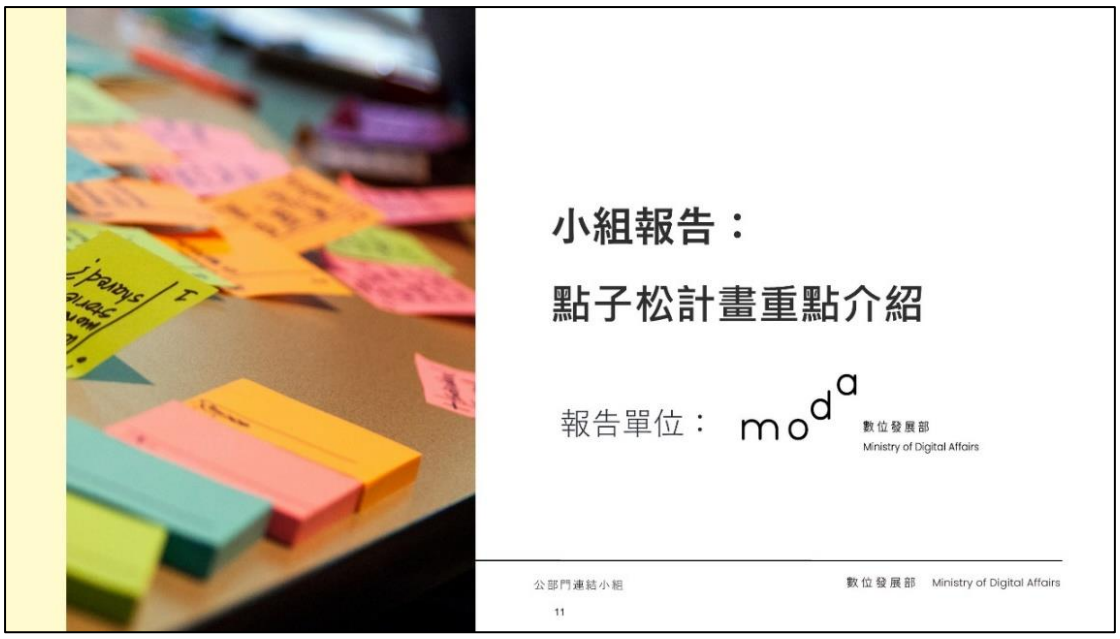
111年度第二次會議列管事項3/3

會議場次	議題	決議	建議列管狀況	追蹤辦理情形-112.3.13
B.111年12月7日第二次會議	B3-【第三案】其他重要議題討論	一、**資訊共享平臺運作方式**： **1.運作方式**：初步決議採電子報。 **2.發送週期**：考量電子報尚為初創階段，爰發送週期暫不決議，惟下次公部門連結小組會議前須至少完成一次電子報內容。 **3.填報方式**：預計採共筆方式供各工作組填寫，相關填報連結：https://s.moda.gov.tw/NLx1H98ZXcwd，請各工作組於112年2月20日前於連結自行完成。 **4.發送對象**：由數位部統整，並常態提供各工作組及本公部門連結小組專家學者（PDF檔），再由各工作組自行轉發相關團隊。 **5.填寫資料**：分為「活動訊息」及「資訊共享」兩大主軸，以可完全公開供各界使用為限，另考量6G行動通訊涉及多與5G/B5G有關聯，爰填報內容不侷限於純6G議題，填寫資料不限未來單個時段，只要為已知訊息即可於電子報呈現。 **6.版面**：以會議所呈現草案版本為主，標題建議先行以「6G標準應用觀測」取代「公部門連結小組」，並移除「新政策研擬」及「版權所有」相關文字，請各工作組視需求自行增加表格或欄位。 **7.資料存放位置**：考量電子報尚為初創階段，要有關歷次電子報存放位置暫不決議。	■解除列管 □持續追蹤 □併案追蹤	• 已完成資訊共享平臺建置，現採**電子報**方式辦理，並已於2月17日、3月2日發行該月電子報
		二、**召開聯合大型研討會可行性**：持續依各工作組提供電子報之活動資訊內容，檢視共同會議交流時間點，檢討由數位部召開MWC行前交流活動，邀集出席該國際會議之各工作組及產學研界專家進行資訊交流。	□解除列管 ■持續追蹤 □併案辦理	• 已於112年2月8日辦理MWC行前交流會，將於112年度第一次會議討論案3進行討論 • **112年6月份3GPP來台事宜**將於112年度第一次會議討論案2進行討論，研擬未來公部門合作事宜。 • 持續研擬舉辦聯合大型研討會之可行性。

公部門連結小組 數位發展部 Ministry of Digital Affairs
8


• 報告案二
一、本年度小組會議時程安排說明
二、本年度新案點子松計畫重點介紹
三、MWC行前交流會經驗分享
公部門連結小組
9
數位發展部 Ministry of Digital Affairs


本年度會議時程規劃
「公部門連結小組」會議搭配「產業諮詢小組」會議之後召開，以確認產業議題於公部門連結與協調
3月13日 公部門連結小組 第一次會議
6月上旬 公部門連結小組 第二次會議
9月上旬 公部門連結小組 第三次會議
12月上旬 公部門連結小組 第四次會議
第一季
第二季
第三季
第四季
2/21 產業諮詢小組 第四次會議
6/1 產業諮詢小組 第五次會議
8/29 產業諮詢小組 第六次會議
11/28 產業諮詢小組 第七次會議
公部門連結小組
數位發展部 Ministry of Digital Affairs
10


小組報告：
點子松計畫重點介紹
報告單位：
moda
數位發展部
Ministry of Digital Affairs
公部門連結小組
11
數位發展部 Ministry of Digital Affairs


moda 數位發展部
Ministry of Digital Affairs
IDEATHON
點子松111年計畫成果及未來規劃
公部門連結小組第一次會議
2023.3.13
主辦機關｜數位發展部
執行單位｜財團法人台灣設計研究院

大綱

一、111年計畫成果

二、未來規劃

13

111年計畫成果 第一屆點子松行銷推廣

- 以**多元管道**觸及不同年齡層民眾
- 透過**案例**、**設計工具**、**互動體驗**，啟發民眾對於未來想像

展覽/導覽	未來原型工作坊	未來新聞親子工作坊	啟動記者會	點子松論壇
				
辦理展覽啟發民眾未來想像，並在最後可即時上傳內容，參與未來想像	經由導師的分享與引領，透過畫布逐一完成搜資、發想、討論、創作等步驟	透過直觀的仿報紙的學習單製作及未來繪本引導小朋友畫/寫出未來	曝光第一屆徵件、強化民眾對於主題的感知。宣告第一屆點子松徵件開始與展覽同步開展	對談數位及公民參與的未來可能
計8145人參觀	計12場次，共368人參加			

14

111年計畫成果 第一屆點子松徵件結果

- 「未來新聞」個人徵件邀請民眾創作2040年可能發生的事件或消息報導，共募集到1,149件作品，經由各領域專家評選出10件「未來洞見獎」作品。
- 「未來原型」團體徵件鼓勵發展2040年的設計概念，包含有形空間商品、無形服務機制或生命體，共募集到201件作品，初選入圍作品經由共創設計後，由各領域專家及民眾選出5件「評審團大獎」作品。

未來新聞：1,149件作品

- 10件「未來洞見獎」作品內容主題包含未來的祭祖、觀光、選舉、長照、失眠、機器人權利等。由此可見，大家對於2040年的關心，不僅限於科技發展可能造成的挑戰，也有對於日常生活的反思。
- 作品不只表現出自由想像未來的創意，更代表大家對生活的期待，例如因貧富差距產生的共享機器人管家計畫、未來AI及機器人是否有能力發展自己的思考甚至主張人權等。

未來原型：201件作品

- 5件「評審團大獎」作品包含永續森林、記憶應用裝置、DNA技術、心理健康諮商等主題，例如運用虛擬分身進行24小時心靈諮詢、探討森林永續再開發的願景及大腦波與DNA序列對未來生活的影響。

數位部頒發點子松「未來洞見獎」

共創未來生活無限可能

111年計畫成果 第一屆點子松共創輔導

- 邀請未來情境類專家與元宇宙技術類專家作為入圍團隊輔導顧問，深化其未來原型提案，共創具有元宇宙沉浸式體驗之決選作品
- 舉辦交流會：讓入圍團隊了解顧問專長，並讓顧問了解入圍團隊作品，使共創設計更加順利。

未來情境類顧問

5位未來情境類顧問各提供每組入圍團隊 1 次線上諮詢，帶領團隊突破現實限制，探索更多未來可能性。

鄭陸霖 實踐工設系副教授 / 社會學家
林家齊 夢想動畫創辦人
林日璇 政大傳播學院特聘教授
宮保睿 《WeWe Futures：2040多元宇宙》策展人
曹筱玥 北科大元宇宙XR研發中心主任

元宇宙技術類顧問

2 位元宇宙技術類顧問(黑洞創造、宇萌數位科技)各提供5組入圍團隊元宇宙平台實體教學，輔導團隊使用元宇宙技術，讓評審及民眾更能體驗未來原型應用情境。

元宇宙作品成果

MARINE CITY.TW Let trees make things 智慧健康管家

未來規劃 112年度總體時程規劃

17

未來規劃 未來情境策展

展期｜2023年7月1日至10月29日，周一休館
地點｜台灣設計館01-02展間，共126坪
概念｜以「共融」跟「永續」為出發點，延伸探討以下議題
門票｜免費參觀

1. 人與非人生物共存（跨物種未來 interspecies futures）
2. 氣候科幻（氣候變遷的科幻原型inclusion & diversity of future gender）
3. 多元性別未來討論LGBTQ+的未來 （inclusion & diversity of future）
4. 未來醫學/未來身體
5. 展示第一屆成果及行銷第二屆徵件活動

策展人｜顧廣義

陽明交大應用藝術研究所兼任助理教授
具有牙醫師、生物藝術家以及**推測設計師**等多重身分，擅長跨領域的前瞻議題探討，結合藝術、設計與科學，思考科技、人類個體和環境之間的關係。

18

未來規劃 點子松論壇

主題及講者名單(洽邀中)

與民眾**溝通推測未來世界問題及構築未來共同願景，進而培養前瞻性創新思維。**

影響未來的關鍵因素?
#大趨勢 #議題
未來推測

未來科技的可能模樣?
#數位科技發展
前瞻科技

如何體驗未來?
情境建構
#虛實整合

Jane McGonigal
#未來學
IFTF未來研究所總監

童子賢
#科技創新
華碩共同創辦人

Simon Caspersen
#未來設計
IKEA space 10
共同創辦人

Fiona Raby(備)
#推測設計
Parsons
推測設計教授

石井裕(備)
#可觸媒體
MIT教授與可觸媒體小組創辦人

19

未來規劃 國際徵件推廣

媒體行銷

全球媒體推廣發佈**4則新聞稿，至少100則媒體報導，以建立點子松國際影響力。**

徵件說明會

以泰國，日本及英國長期合作機構作為本屆重點推廣國家。

國家	泰國	日本	英國
學術單位	CEA CREATIVE ECONOMY AGENCY	KNOWLEDGE CAPITAL	British Office
產業單位	จุฬาลงกรณ์มหาวิทยาลัย	千葉工業大学	

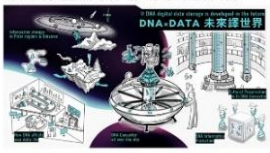
20

未來規劃 成果擴散

- 協助輔導第一屆未來原型獲獎5組團隊，並優化其作品呈現方式，以利參加國際競賽及展覽。
- 邀請第一屆未來新聞/原型獲獎團隊，參與說明會，分享作品及參賽經驗。

優化對象

未來原型評審團大獎5組作品



精進作品可視化

協助作品精進並進一步可視化

21

國際擴散連結

優化後作品參加國際相關競賽

INTERNATIONAL DESIGN EXCELLENCE AWARDS

reddot design award

NOVUM DESIGN AWARD

GOOD DESIGN

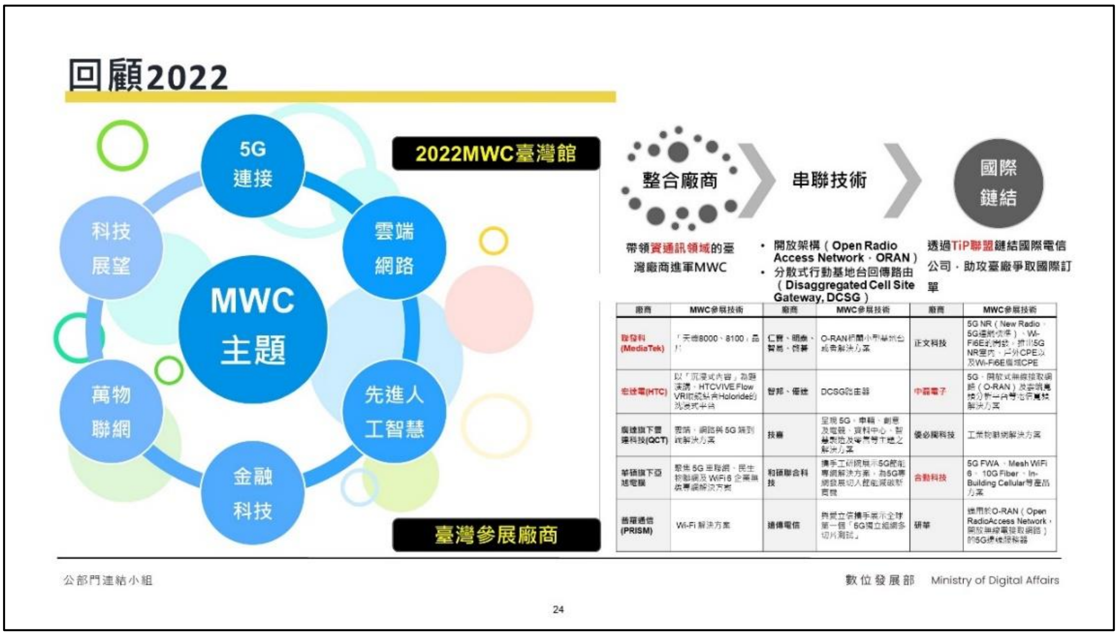
小組報告：
MWC行前交流會經驗分享

報告單位： moda 數位發展部 Ministry of Digital Affairs

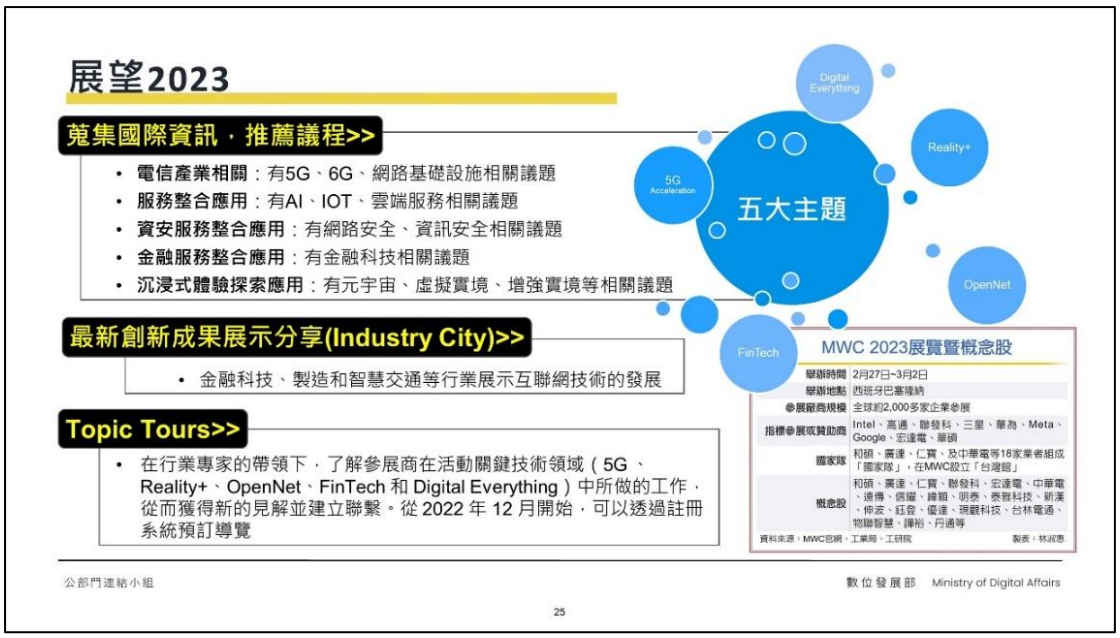
公部門連結小組

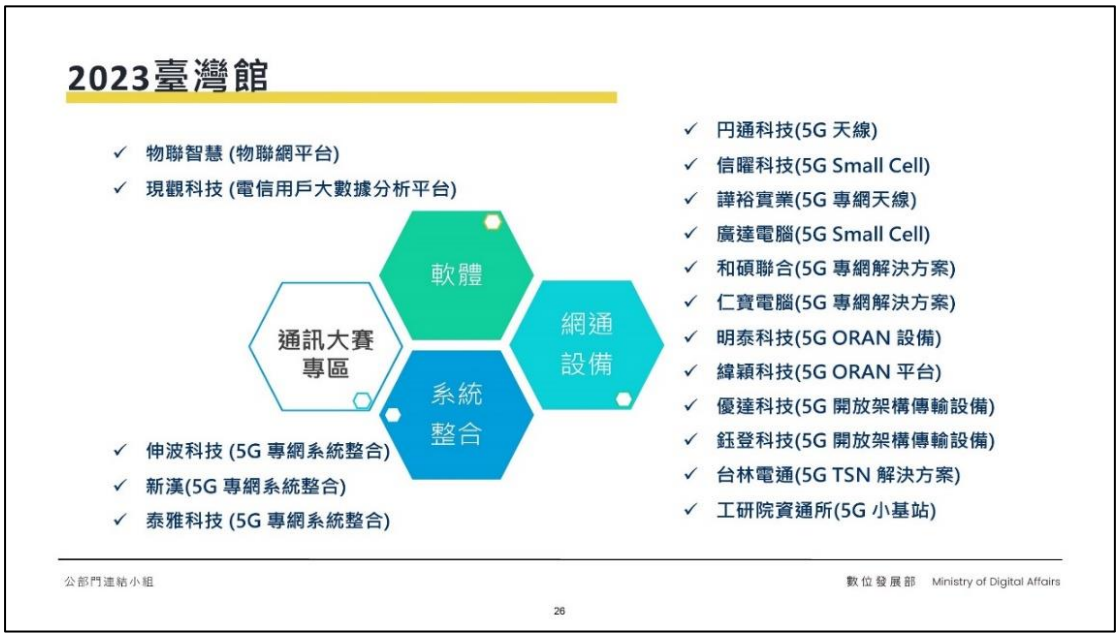
數位發展部 Ministry of Digital Affairs

22



廠商	MWC參展技術	廠商	MWC參展技術	廠商	MWC參展技術
聯發科(MediaTek)	「天璣8000、8100」晶片	仁寶、明泰、智易、啟碁	O-RAN相關小型基地台或套解決方案	正文科技	5G NR（New Radio，5G通訊標準）、Wi-Fi6E... 推出5G NR室內、戶外CPE以及Wi-Fi6E區域CPE
宏達電(HTC)	以「沉浸式內容」為題演講，HTC VIVE Flow VR眼鏡結合Holoride的沉浸式平台	智邦、優達	DCSG路由器	中磊電子	5G、開放式無線接取網路（O-RAN）及雲端儲存分析平台等電信業解決方案
廣達旗下雲達科技(QCT)	雲端、網路與5G端到端解決方案	技嘉	呈現5G、車輛、創意及電競、資料中心、智慧製造及零售等主題之解決方案	優必闊科技	工業物聯網解決方案
華碩旗下亞旭電腦	聚焦5G專網、民生物聯網及WiFi6企業無線專網解決方案	和碩聯合科技	攜手工研院展示5G智能專網解決方案，為5G專網發展切入智能減碳新商機	合勤科技	5G FWA、Mesh WiFi 6、10G Fiber、In-Building Cellular等產品方案
普羅通信(PRISM)	Wi-Fi解決方案	遠傳電信	與愛立信攜手展示全球第一個「5G獨立組網多切片測試」	研華	適用於O-RAN（Open RadioAccess Network，開放無線電接取網路）的5G邊緣伺服器


展望2023
蒐集國際資訊，推薦議程>>
電信產業相關：有5G、6G、網路基礎設施相關議題
服務整合應用：有AI、IOT、雲端服務相關議題
資安服務整合應用：有網路安全、資訊安全相關議題
金融服務整合應用：有金融科技相關議題
沉浸式體驗探索應用：有元宇宙、虛擬實境、增強實境等相關議題
最新創新成果展示分享(Industry City)>>
金融科技、製造和智慧交通等行業展示互聯網技術的發展
Topic Tours>>
在行業專家的帶領下，了解參展商在活動關鍵技術領域（5G、Reality+、OpenNet、FinTech 和 Digital Everything）中所做的工作，從而獲得新的見解並建立聯繫。從 2022 年 12 月開始，可以透過註冊系統預訂導覽
Digital Everything
Reality+
5G Acceleration
五大主題
OpenNet
FinTech
MWC 2023展覽暨概念股
舉辦時間 2月27日~3月2日
舉辦地點 西班牙巴塞隆納
參展廠商規模 全球約2,000多家企業參展
指標參展或贊助商 Intel、高通、聯發科、三星、華為、Meta、Google、宏達電、華碩
國家隊 和碩、廣達、仁寶、及中華電等18家業者組成「國家隊」，在MWC設立「台灣館」
概念股 和碩、廣達、仁寶、聯發科、宏達電、中華電、遠傳、信驊、緯穎、明泰、泰雅科技、新漢、伸波、鈺登、優達、視觀科技、台林電通、物聯智慧、譁裕、丹通等
資料來源：MWC官網、工業局、工研院 製表：林淑惠
公部門連結小組
數位發展部 Ministry of Digital Affairs
25


2023臺灣館
物聯智慧 (物聯網平台)
現觀科技 (電信用戶大數據分析平台)
軟體
通訊大賽專區
網通設備
系統整合
伸波科技 (5G 專網系統整合)
新漢(5G 專網系統整合)
泰雅科技 (5G 專網系統整合)
丹通科技(5G 天線)
信曜科技(5G Small Cell)
譁裕實業(5G 專網天線)
廣達電腦(5G Small Cell)
和碩聯合(5G 專網解決方案)
仁寶電腦(5G 專網解決方案)
明泰科技(5G ORAN 設備)
緯穎科技(5G ORAN 平台)
優達科技(5G 開放架構傳輸設備)
鈺登科技(5G 開放架構傳輸設備)
台林電通(5G TSN 解決方案)
工研院資通所(5G 小基站)
公部門連結小組
數位發展部 Ministry of Digital Affairs
26

西班牙旅遊注意事項

「西班牙超不安全的耶，你真的要去？」

- ✓ 避免一個人行動，尤其是夜晚的暗巷
- ✓ 身上不要帶太多現金，盡量使用信用卡
- ✓ 護照特別要收好，或是考慮放在住宿點
- ✓ 在人擠人的場合，譬如廣場、地鐵站，一定要有警覺心，顧好包包
- ✓ 不要在路上把自己搞得手忙腳亂，搭車、結帳、放東西，都慢慢來
- ✓ 不要讓陌生人靠近你，別人的好意可能是行搶的伎倆
- ✓ 如果不幸遭劫，一定要記得報案，把信用卡停卡；如果護照不見，則持報案證明至馬德里的駐西班牙代表處補辦護照，才能順利飛回台灣。至於不見的東西，或是歹徒本人，原則上不會再找到了。當然，在這邊還是希望大家都不會遇到這樣的事情

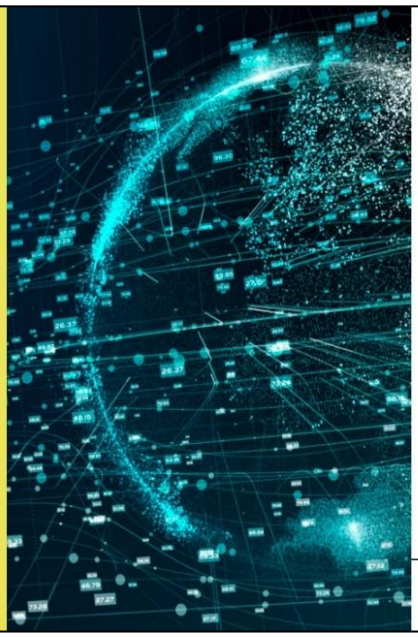
※資料來源：Klookhttps://www.klook.com/zh-TW/blog/attractions-spain/

台灣駐西班牙台北經濟文化辦事處
Oficina Economica y Cultural de Taipei, España

- ✓ 地址： C / Rosario Pino 14-16， Piso 18 Dcha， 28020 Madrid, España (Spain)
- ✓ 搭乘地下鐵(Metro)1路(淺藍)線Valdeacederas站或10路(深藍)線Cuzco站皆可抵達
- ✓ 電話：境外：(+34) 915714678、(+34)915718426、(+34)915714729 境內直撥： 915714678、915718426、915714729
- ✓ 電子郵件：esp@mofa.gov.tw
- ✓ 官網：https://www.roc-taiwan.org/es/index.html

急難救助全球24小時專線800-0885-0885

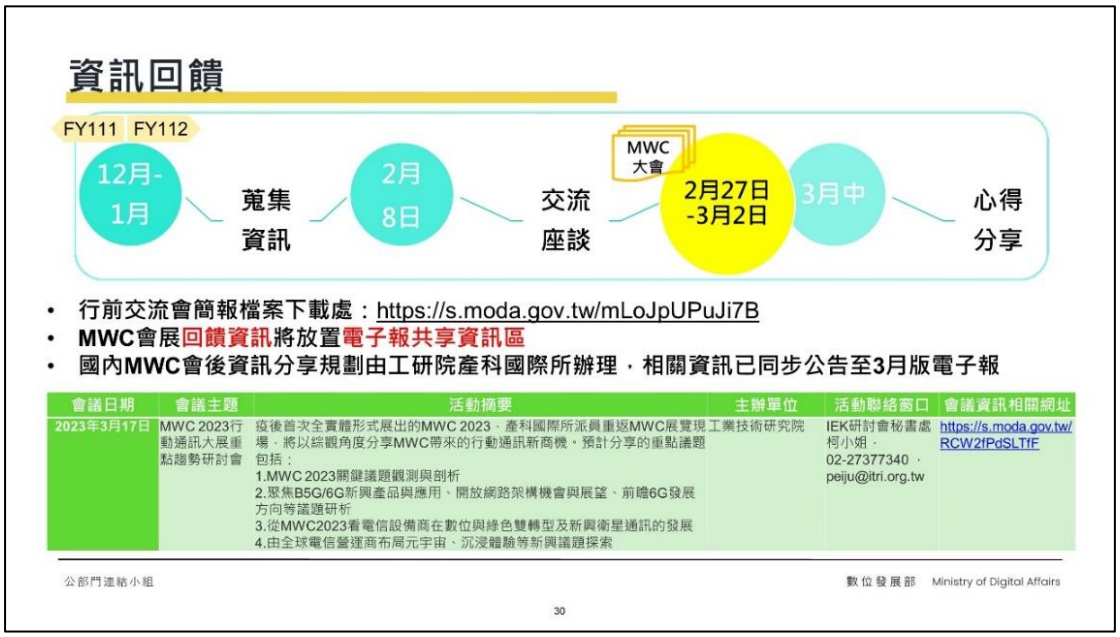
公部門連結小組 數位發展部 Ministry of Digital Affairs
27

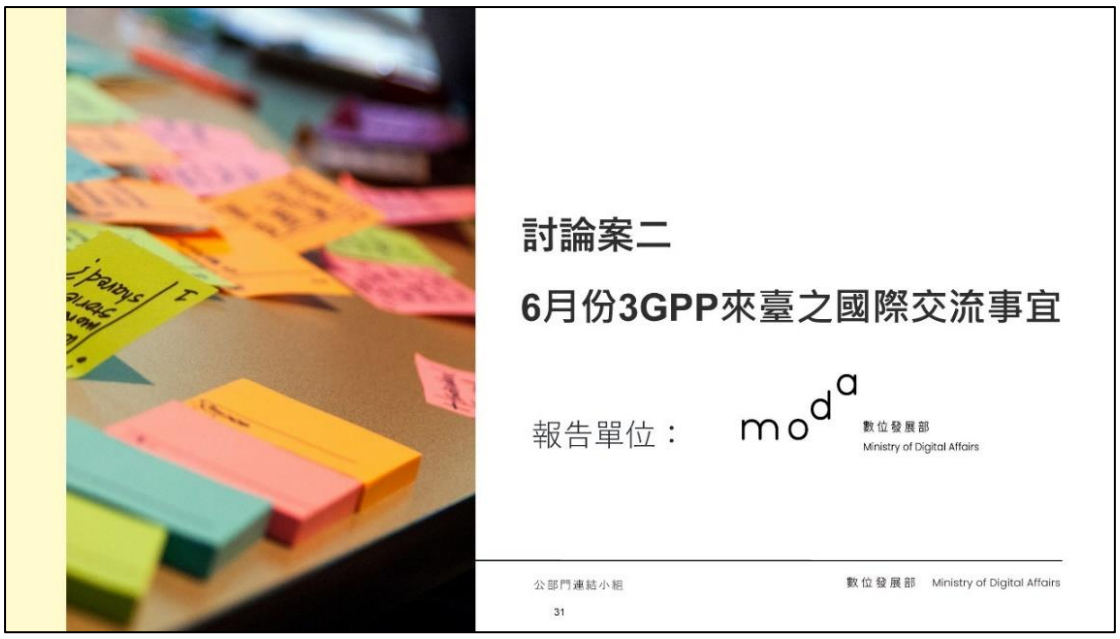


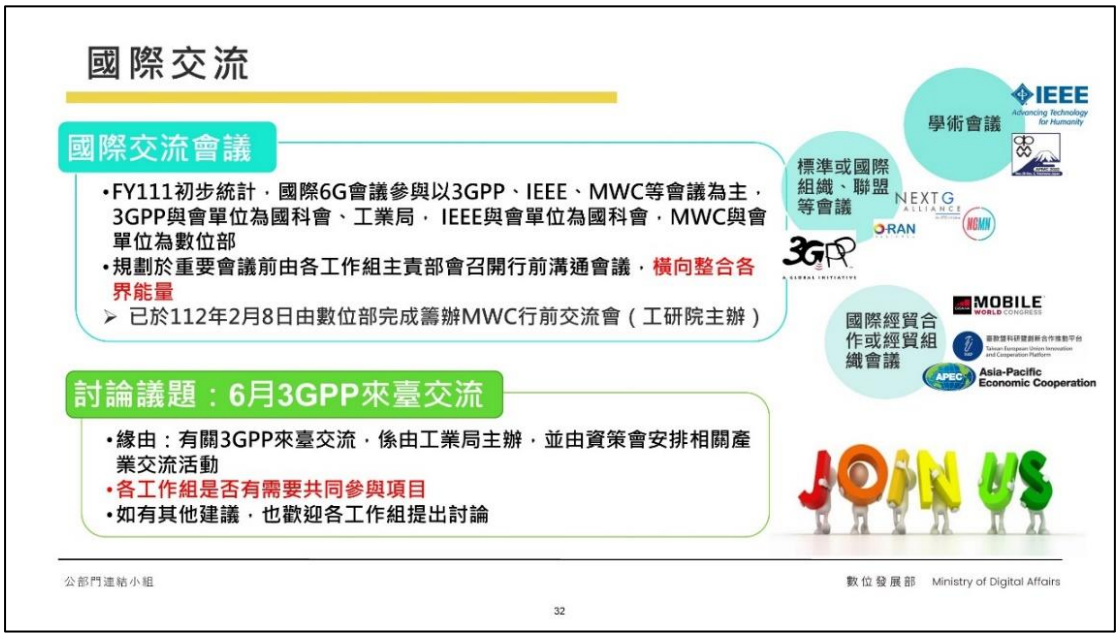
- 討論案一、MWC會後心得分享規劃
- 討論案二、112年6月份3GPP來臺之國際交流事宜
- 討論案三、資訊共享平臺-電子報推動情況

公部門連結小組 數位發展部 Ministry of Digital Affairs
28

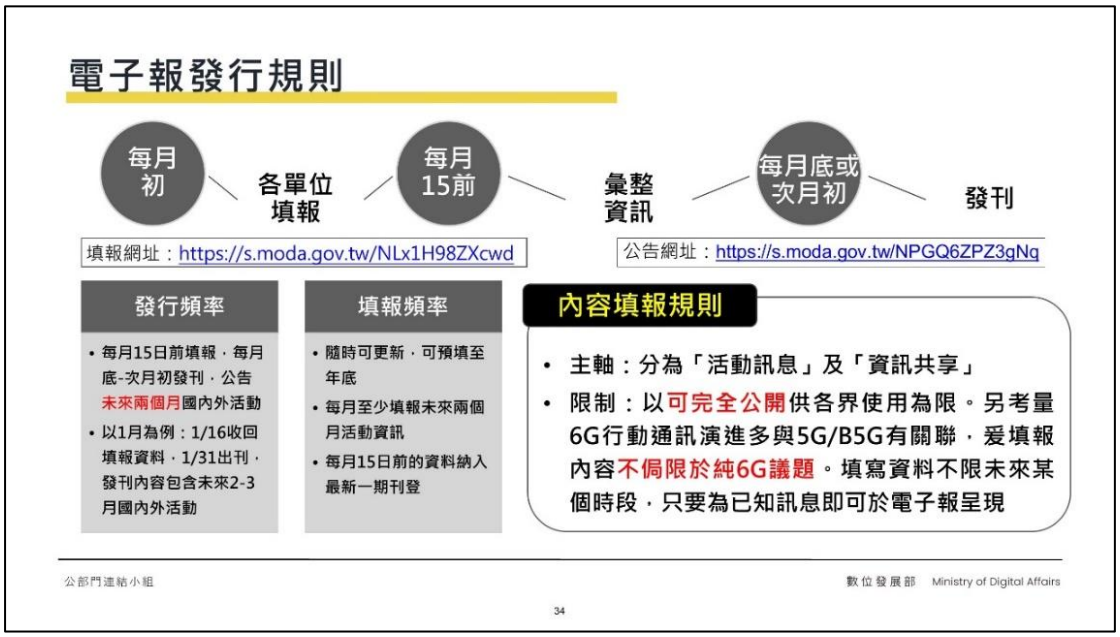

討論案一
MWC會後心得分享規劃
報告單位：
moda
數位發展部
Ministry of Digital Affairs
公部門連結小組
29
數位發展部 Ministry of Digital Affairs

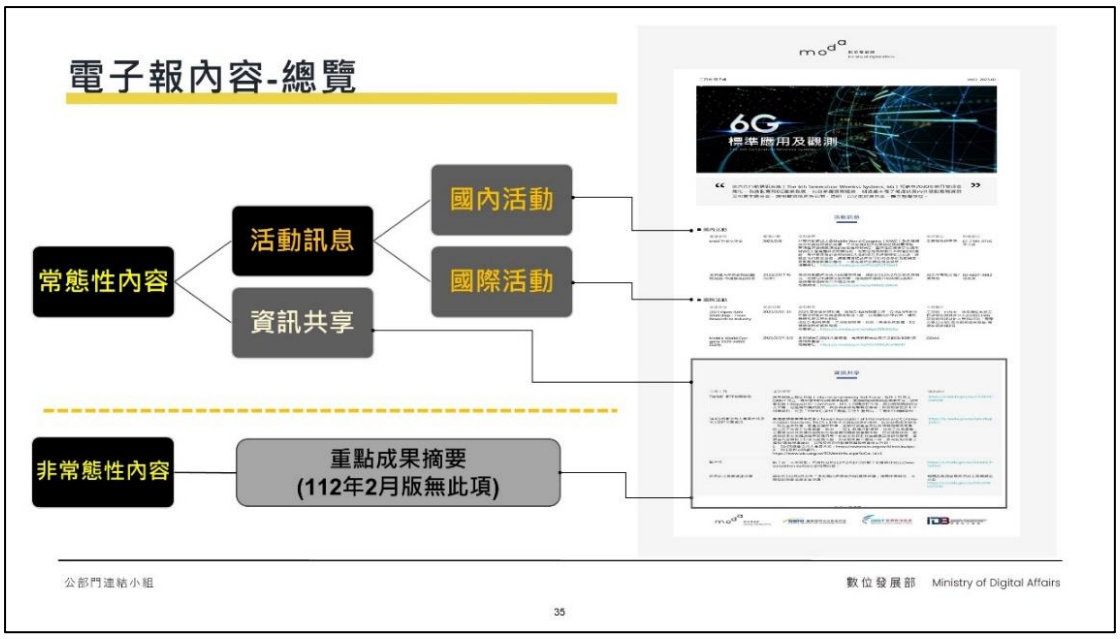

資訊回饋
FY111 FY112
12月-1月
蒐集資訊
2月8日
交流座談
MWC大會
2月27日-3月2日
3月中
心得分享
• 行前交流會簡報檔案下載處：https://s.moda.gov.tw/mLoJpUPuJi7B
• MWC會展回饋資訊將放置電子報共享資訊區
• 國內MWC會後資訊分享規劃由工研院產科國際所辦理，相關資訊已同步公告至3月版電子報
會議日期 會議主題 活動摘要 主辦單位 活動聯絡窗口 會議資訊相關網址
2023年3月17日 MWC 2023行動通訊大展重點趨勢研討會 疫後首次全實體形式展出的MWC 2023，產科國際所派員重返MWC展覽現場，將以綜觀角度分享MWC帶來的行動通訊新商機，預計分享的重點議題包括：
1.MWC 2023關鍵議題觀測與剖析
2.聚焦B5G/6G新興產品與應用、開放網路架構機會與展望、前瞻6G發展方向等議題研析
3.從MWC2023看電信設備商在數位與綠色雙轉型及新興衛星通訊的發展
4.由全球電信營運商布局元宇宙、沉浸體驗等新興議題探索
工業技術研究院
IEK研討會秘書處 柯小姐，02-27377340，peiju@itri.org.tw
https://s.moda.gov.tw/RCW2fPdSLTfF
公部門連結小組
數位發展部 Ministry of Digital Affairs
30


討論案二
6月份3GPP來臺之國際交流事宜
報告單位：
moda
數位發展部
Ministry of Digital Affairs
公部門連結小組
31
數位發展部 Ministry of Digital Affairs


國際交流
國際交流會議
•FY111初步統計，國際6G會議參與以3GPP、IEEE、MWC等會議為主，3GPP與會單位為國科會、工業局，IEEE與會單位為國科會，MWC與會單位為數位部
•規劃於重要會議前由各工作組主責部會召開行前溝通會議，橫向整合各界能量
➢ 已於112年2月8日由數位部完成籌辦MWC行前交流會（工研院主辦）
學術會議
IEEE
標準或國際組織、聯盟等會議
NEXT G ALLIANCE
O-RAN
3GPP
國際經貿合作或經貿組織會議
MOBILE WORLD CONGRESS
APEC
Asia-Pacific Economic Cooperation
討論議題：6月3GPP來臺交流
•緣由：有關3GPP來臺交流，係由工業局主辦，並由資策會安排相關產業交流活動
•各工作組是否有需要共同參與項目
•如有其他建議，也歡迎各工作組提出討論
JOIN US
公部門連結小組
32
數位發展部 Ministry of Digital Affairs


討論案三
電子報推動情況
報告單位：
moda
數位發展部
Ministry of Digital Affairs
公部門連結小組
33
數位發展部 Ministry of Digital Affairs


電子報發行規則
每月初
各單位填報
每月15前
彙整資訊
每月底或次月初
發刊
填報網址：https://s.moda.gov.tw/NLx1H98ZXcwd
公告網址：https://s.moda.gov.tw/NPGQ6ZPZ3gNq
發行頻率
• 每月15日前填報，每月底-次月初發刊，公告未來兩個月國內外活動
• 以1月為例：1/16收回填報資料，1/31出刊，發刊內容包含未來2-3月國內外活動
填報頻率
• 隨時可更新，可預填至年底
• 每月至少填報未來兩個月活動資訊
• 每月15日前的資料納入最新一期刊登
內容填報規則
• 主軸：分為「活動訊息」及「資訊共享」
• 限制：以可完全公開供各界使用為限。另考量6G行動通訊演進多與5G/B5G有關聯，爰填報內容不侷限於純6G議題。填寫資料不限未來某個時段，只要為已知訊息即可於電子報呈現
公部門連結小組
34
數位發展部 Ministry of Digital Affairs


電子報內容-總覽
常態性內容
活動訊息
國內活動
國際活動
資訊共享
非常態性內容
重點成果摘要
(112年2月版無此項)
6G
標準應用及觀測
公部門連結小組
數位發展部 Ministry of Digital Affairs
35


電子報內容欄位說明
國內活動
會議日期 | 會議主題 | 活動摘要 (請勿超過150字) | 主辦單位 | 活動聯絡窗口 | 會議資訊相關網址 | 填報單位/填報人/聯絡方式 (此欄不會出現在電子報中)
【填報範例】 111年2月27日-111年3月2日 | 5G創新應用服務研討會 | 面對5G帶來的加速競爭，強化5G創新應用服務、發展創新結盟，已成為全球發展5G產業鏈之關鍵價值。這場以5G驅動產業鏈結，引領數位轉型的「5G創新應用服務研討會」，將幫助產官學研各界掌握5G創新應用市場先機。 | 電信技術中心 | 02-77137852 吳小姐、陳小姐 | http://dreambig.com.tw/event/2020/5G_EmpoweringTaiwan/ | 數位發展部/王琇儀 /LinnaWang@itri.org.tw，02-2380-0716
國際活動
日期 | 會議主題 | 活動摘要 (請勿超過150字) | 主辦單位 | 會議資訊相關網址 | 填報單位/填報人/聯絡方式 (此欄至右以後欄位不會出現在電子報中) | 建議與會單位 | 國際會議類型
【填報範例】 111年2月27日-111年3月2日 | Mobile World Congress 2023 (MWC 2023) | 參與MWC 2023大會展區，蒐集國際廠商展示之B5G/6G新興應用與產品 | GSMA | http://www.gsma.com | 數位發展部/王琇儀 /LinnaWang@itri.org.tw，02-2380-0716 | 數位發展部 | 大型會議-經貿交流型
重點成果摘要
成果類型 | 主辦單位 | 重點成果摘要 | 聯絡窗口 | 填報單位/填報人/聯絡方式 (此欄不會出現在電子報中)
其他共享資訊
資訊提供單位 | 分享資訊重點摘要 | 填報人/聯絡方式
公部門連結小組
數位發展部 Ministry of Digital Affairs
36

112年2月版電子報內容-置頂

公部門連結小組 數位發展部 Ministry of Digital Affairs

37

112年2月版電子報內容-活動訊息區

建議填報方式

- 以各工作組提供資訊為主
- **不限**配合計畫執行之活動，與**6G或資通訊相關領域**議題皆歡迎提供分享
- 以1月為例，發刊內容包含**未來2-3月**國內外活動

活動訊息

■ 國內活動

會議名稱	會議日期	活動摘要	主辦單位	聯絡窗口
MWC行前交流會	2023/2/8	世界行動通訊大會Mobile World Congress（MWC）為全球通訊業界最具權威的展覽，工業局自2017年開始即籌組臺灣館，帶領臺灣資通訊領域的廠商推展MWC，臺灣電信業者在歷年MWC大會蔚聯各式創機技術，在數位發展部整合各部會的能量後，希望能集預計參與MWC大會的各方先進聯繫在地交流，透過此次行前交流會，讓臺灣資通訊產業可以有更多的互動機會，更期能透過能量的整合，一起在國際的舞台發光發熱。 相關網址：https://s.moda.gov.tw/P3cQPUTYbet4	工業技術研究院	02-2380-0716 王小姐
支持國內產業參與6G國際組織-申請辦法說明會	2023/2月下旬(待定)	為支持我國產業投入6G國際組織，預計於112年2月公告支持辦法，並辦理申請辦法說明會，透過國際組織介紹與辦法說明，邀請業者組隊或合作提出申請。 相關網址：https://s.moda.gov.tw/qhNX6tE18KrA	台北市電腦公會/資策會	02-6607-3882 徐先生

■ 國際活動

會議名稱	會議日期	活動摘要	主辦單位
2023 Open RAN Workshop：From Research to Industry	2023/2/13-14	2023 開放基地研討會，邀請O-RAN聯盟主席、O-RAN軟件社區需求與軟件架構委員會聯合主席，以及國內外學術界、研究機構和產業界的B5G/6G O-RAN專家，共同探討標準、技術、開源系統軟體、5G等網應用的最新發展。 相關網址：https://s.moda.gov.tw/u6psZB82kGXo	工研院、台科大、法國通信系統工程師學校與研究中心(EURECOM)、新加坡科技設計大學(SUTD)、電電公會以及5G 產業創新發展聯盟-開源系統軟體SIG
Mobile World Congress 2023 (MWC 2023)	2023/2/27-3/2	參與MWC 2023大會展區，蒐集國際廠商展示之B5G/6G新興應用與產品。 相關網址：https://s.moda.gov.tw/VDdWM3hwN6NT	GSMA

公部門連結小組 數位發展部 Ministry of Digital Affairs

38

112年2月版電子報內容-資訊共享區

建議填報方式

- 以各工作組提供資訊為主
- **不限**配合計畫執行之資訊，與**6G或資通訊相關領域**議題皆歡迎提供分享

資訊共享

分享主題	重點摘要	連結網址
TWNIC-IETF相關報告	網際網路工程任務組（Internet Engineering Task Force，IETF）於西元1986年成立，為非營利的國際標準組織，透過制定網際網路標準文件：徵求意見稿（Request for Comment，RFC）和開放程式碼，提出網際網路技術及架構，促進網際網路發展，其參與者皆為無償志願者，如欲瞭解更多IETF相關資訊，可至「TWNIC-資料下載區-研究計畫報告」下載IETF相關資料。	https://s.moda.gov.tw/c7QfedGGatUW
TAICS協會之加入會員方式及TC1議程公開資訊	臺灣資通產業標準協會（Taiwan Association of Information and Communication Standards, TAICS）針對未來資通技術的發展，鎖定台灣適合領域，制定產業標準，推進至國際標準，並按照資通產業技術領域和專業範圍，設立若干技術工作委員會。其中，「TC1 前傳行動通訊」技術工作委員會，主要關注的技術標的為新世代無線通訊關鍵與產業技術，包括接取技術、網路技術及未來情境與產業應用等，針對未來新世代無線通訊技術的發展，凝聚國內產學研之研發力量與共識，形成對外單一溝通平台，進而推動相關之國際/區域標準連結，以布局未來行動通訊國際標準核心智財。 1. TAICS協會之加入會員方式：https://www.taics.org.tw/MbrJoin.aspx 2. TC1議程公開資訊：https://www.taics.org.tw/TCMeetInfo.aspx?tcCat_id=1	https://s.moda.gov.tw/qAcd6qip5K1r
點子松	點子松「未來原型」得獎作品於112年2月17日於點子松官網 (https://www.ideathon.tw/tw)公告相關內容。	https://s.moda.gov.tw/XAJdkUH7eEbd
經濟部工業局資訊分享	預計於112月2月公告「支持國內產業參與6G國際組織」相關作業辦法，並辦理說明會協助廠商申請。	相關訊息請留意經濟部工業局網站公告 https://s.moda.gov.tw/HEUAWGzrzkb

公部門連結小組 數位發展部 Ministry of Digital Affairs

39

電子報討論事項

1. 發行**頻率**是否需要調整
2. 發行**內容**是否需要增刪
3. 各工作組在**填報上**是否有問題
4. 是否有**其他**建議事項

公部門連結小組 數位發展部 Ministry of Digital Affairs

40

臨時動議

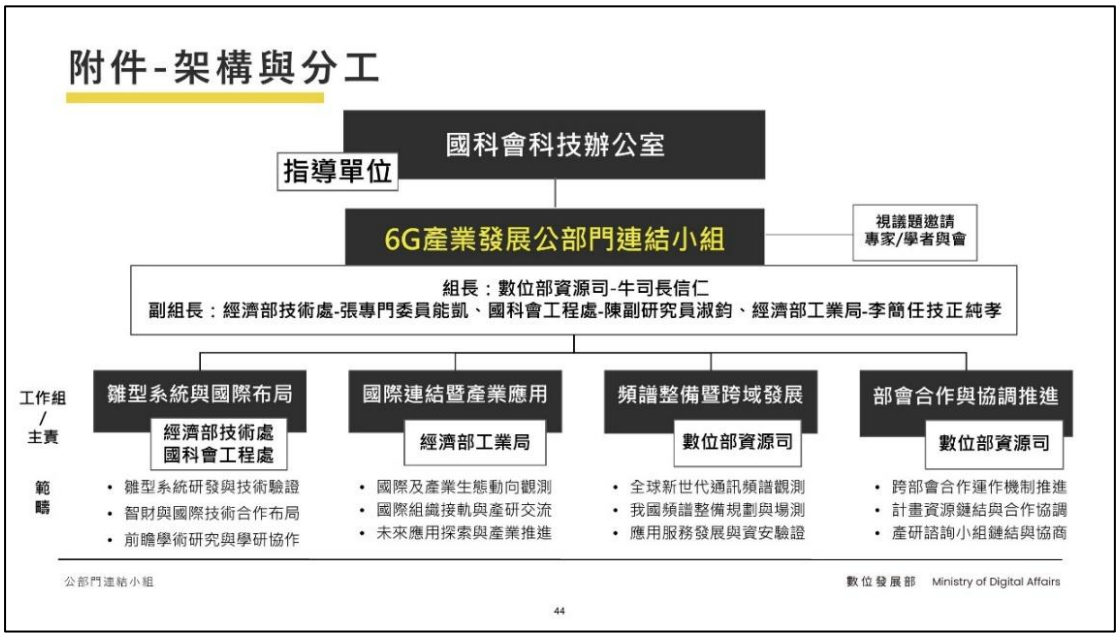
協作議題

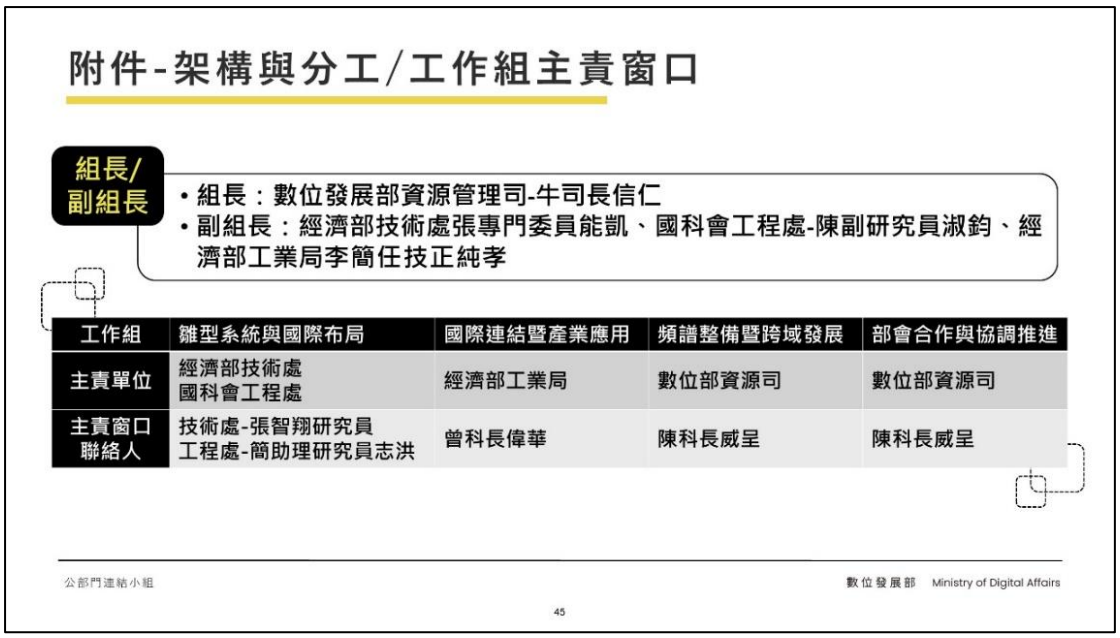
- **協作議題1-頻段需求現況調查**：各工作組如有頻段需求，歡迎填報需求表，以確保產學研界研擬方向之可行性
- **各工作組可視需求提出協作議題，以利資訊共享交流(非政策制定)**

頻段需求現況調查表

需求者	發射地點	電台類型	涵蓋範圍	發射頻率	使用頻寬	最大發射功率	使用目的或用途	主管機關相關建議回饋
(機關/單位)	(範例)新北市林口區新創園區	□固定臺 □行動臺	新創園區A棟周邊10公里	1775-1785MHz、1870-1880MHz	10x2MHz	37dBm	實驗研發-促進國內車聯網產業應用服務落地	技術處： 工程處： 工業局： 數位部：


感謝您的蒞臨與會
Thank You
moda
數位發展部
Ministry of Digital Affairs


附件-架構與分工
國科會科技辦公室
指導單位
6G產業發展公部門連結小組
視議題邀請
專家/學者與會
組長：數位部資源司-牛司長信仁
副組長：經濟部技術處-張專門委員能凱、國科會工程處-陳副研究員淑鈞、經濟部工業局-李簡任技正純孝
工作組/主責
範疇
雛型系統與國際布局
經濟部技術處
國科會工程處
• 雛型系統研發與技術驗證
• 智財與國際技術合作布局
• 前瞻學術研究與學研協作
國際連結暨產業應用
經濟部工業局
• 國際及產業生態動向觀測
• 國際組織接軌與產研交流
• 未來應用探索與產業推進
頻譜整備暨跨域發展
數位部資源司
• 全球新世代通訊頻譜觀測
• 我國頻譜整備規劃與場測
• 應用服務發展與實安驗證
部會合作與協調推進
數位部資源司
• 跨部會合作運作機制推進
• 計畫資源鏈結與合作協調
• 產研諮詢小組鏈結與協商
公部門連結小組
數位發展部 Ministry of Digital Affairs
44


附件-架構與分工/工作組主責窗口
組長/副組長
• 組長：數位發展部資源管理司-牛司長信仁
• 副組長：經濟部技術處張專門委員能凱、國科會工程處-陳副研究員淑鈞、經濟部工業局李簡任技正純孝
工作組 | 雛型系統與國際布局 | 國際連結暨產業應用 | 頻譜整備暨跨域發展 | 部會合作與協調推進
主責單位 | 經濟部技術處 國科會工程處 | 經濟部工業局 | 數位部資源司 | 數位部資源司
主責窗口 聯絡人 | 技術處-張智翔研究員 工程處-簡助理研究員志洪 | 曾科長偉華 | 陳科長威呈 | 陳科長威呈
公部門連結小組
數位發展部 Ministry of Digital Affairs
45


附件-成立目的與運作規劃
成立目的
•整合能量、凝聚共識：為推動臺灣6G產業發展，於行政院科技會報辦公室(2022.7.27更名為國科會科技辦公室)指導下，成立本「公部門連結小組」，作為跨部會合作協調平台，協調計畫內之部會合作議題並推進，及計畫外相關產業之公部門協作，統合相關議題提供政策建言予科技辦公室，促進產業6G先期發展
議題研討
• 計畫內合作議題研析
• 計畫外相關產業之公部門協作
整合能量
• 橫向連結小組內相關計畫
• 統合議題予科技辦公室提出建言
運作規劃
會議召開
• 原則上會議以每季之頻度召開
• 組長/副組長得視議題或調和時程召開臨時會議
分工
• 設立四個工作組-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
• 由（部會合作與協調推進）工作組負責會議之規劃、安排及統合相關協調工作，包含與「產研新創小組」鏈結工作與協尚等
合作
• 由（部會合作與協調推進）工作組於每次會議前，調查各工作組所遭遇執行合作之推進困難或外部會議應合作等議題，安排於會議中討論，並請科會辦派員指導
• 各工作組不受限每季頻度之會議時程，可即時提出遭遇困難，由組長/副組長擇定召開臨時會議
公部門連結小組
數位發展部 Ministry of Digital Affairs
46

附件-點子松 111年計畫成果 未來洞見獎作品

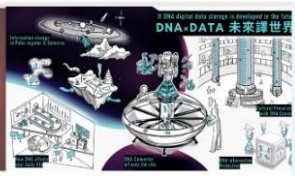
獲獎者	新聞標題	概述
陳彥蓉	台積電推出「人類休眠晶片」解決你的睡眠不足！	從現代容易失眠的問題出發，並提出透過植入性科技解決，相當諷刺但別具意義。
蘇靖雯	DeEpR：非傳統形式的毒品技術與器官盜賣	與器官盜賣和藥物藥物濫用結合，反映了當代社會議題，隨著虛擬技術越來越豐富，這樣的事件很可能未來將會發生。
曾彥翔	公廟推出鏈上祭祖活動，實體紙錢將走入歷史	勾勒宗祖先牌位上鍊、祭祖用品、香油錢等儀式細節，結合NFT技術雖看似誇張，但推測未來技術應用不難想像。
馮力文	首批區塊鏈簽證遊客入境，未來可期商務及觀光客再成長	將護照與身份在區塊鏈上鍊，提供快速入境申請的解決方案。
鄭伊翔	2040年總統大選DID區塊鏈線上投票系統首次應用！	結合總統大選場景和去中心化身份辨識的區塊鏈技術，發展未來可能的便捷投票與開票方式。
章騰允	長照8.0邁向數位高齡世代 共享機器人管家計畫正式啟航	呼應未來長照可能缺乏人力的議題，提出因貧富差距而可能產生的共享機器人管家計畫。
林家妤	「人生展覽設計」展示告別式會場，供來訪親友弔念交流	思考未來高齡化社會以及長者不避諱生死的價值觀改變，將每個人的思考與人生經歷透過元宇宙保存展示，延伸為人生一輩子的數位典藏。
張凱婷	娛樂圈驚爆！影帝去逝多年竟是複製人代演！	連結把演員的臉或表情保存下來的技術，提出虛擬演員發展的未來可能。
黎亮頡	機器人罷工事件延燒至125 個國家	令人反思AI跟機器人是否有能力發展自己的思考甚至主張人權，創作內容引發想像空間和討論。
楊行	立法院敲板，智慧分身稅明年上路！法案原委一次說清！	出機器人繳稅的議題，並完整分析社會各族群情況，內容反應正反面聲浪，點出未來稅制設計可能面臨的考驗。

47

附件-點子松 111年計畫成果 評審團大獎作品

團隊名稱	未來原型標題	概述
CoCoTree	Let trees make things	討論從疏伐、輪伐到碳匯，台灣森林永續再開發的願景其實不那麼脫離現實地科幻，而是勾勒出一個循序漸進築夢踏實的生態台灣路徑。
伴夜睡不著覺	牽伴 Hand in Hand	運用虛擬分身進行24小時心靈諮詢，藉由訓練AI來做對話，賦予心理諮商新的可能性，在「正確時機」給予「適當協助」，針對每個獨特的個體，用負擔得起的價格觸及諮商。
DNA魔法師	DNA×DATA 未來譯世界	從生物技術DNA序列編碼技術，突破對接到數位資訊儲存的瓶頸，定位一個起始點的圓心，往各種方向發散應用情境的各種想像。
無虛設計	記憶應用裝置｜M.A.D	記憶是儲存一個人過去的經驗，感受的能力。M.A.D 能夠通過腦電波儀偵測大腦的運動，讀取圖像記憶、知覺等各種數據，擁有能分享、學習記憶等各種使用，例如傳承先代記憶、分享個人生活、學習技能等各式應用。
SHM Lab	智慧健康管家-下個世代的醫療方針	在2040年的未來，每個人一出生就會有一個屬於自己的數位分身，利用各種數值構建出屬於個人的數位分身，醫生則可以透過數位分身追蹤病人的資訊讓診斷更準確，並透過各種病例讓數位分身背後的資料庫數據更加龐大。





48

九、會議實況

公部門連結小組第一次會議 簽到表

日期：2023年3月13日 星期一 10:00-11:30

地點：數位發展部新光大樓20A01會議室

編號	單位	姓名	職稱	簽到
1	數位部資源司	牛仁	司長	
2	數位部資源司	沈雄	專門委員	
3	數位部資源司	陳呈	科長	
4	數位部資源司	張筠	科員	
5	數位部策略司	林宜	科長	
6	數位部策略司	古瑋	視察	
7	經濟部技術處	張凱	專門委員	
8	經濟部技術處	洪陽	科長	
9	經濟部技術處	張翔	研究員	
10	經濟部工業局	李孝	簡正	
11	經濟部工業局	曾華	科長	
12	經濟部工業局	尤	技正	
13	經濟部工業局/資策會	蔡霖	副主任	
14	國科會工程處	陳鈞	副研究員	
15	國科會工程處	簡洪	助理研究員	

公部門連結小組第一次會議 簽到表

日期：2023年3月13日 星期一 10:00-11:30

地點：數位發展部新光大樓20A01會議室

編號	單位	姓名	職稱	簽到
16	工業技術研究院	許陽	主任	
17	工業技術研究院	王傑	經理	
18	工業技術研究院	王儀		
19	工業技術研究院	王宇		
20	工業技術研究院	許庭		
21	中興大學電機工程學系	楊章	教授	
22	台灣科技大學資訊工程系	鄧中	教授	
23	台灣大學電機工程學系	廖君	教授	
24	電信技術中心	王寧	副研究員	
25	電信技術中心			
26	台灣設計研究院		組長	
27			APM	
28				
29				
30				