出國報告（出國類別：開會）

參加 2024 年新加坡國際資安週
Singapore International Cyber Week
（SICW 2024）出國報告

服務機關：數位發展部資通安全署

姓名職稱：林春吟副署長

戴瑞娥代理科長

林儀郡資安系統分析師

派赴國家：新加坡

出國期間：113 年 10 月 14 日至 113 年 10 月 18 日

報告日期：113 年 12 月 12 日

目　錄

摘　要

由新加坡網路安全局（Cyber Security Agency of Singapore，CSA）主辦的新加坡國際資安週（Singapore International Cyber Week，SICW），自 2016 年開始舉辦至今，為亞洲大型資安活動，每年吸引來自各國的產、官、學界代表參加，分享網路安全政策、實務經驗及技術手法等。

新加坡國際資安週（SICW）會議期間搭配 GovWare 國際資安大會及展覽（GovWare Conference and Exhibition）、物聯網黑客松(IoT Hackathon:SPIRITCYBER)活動共同辦理，爰活動期間聚集了來自多國的公私部門專家，擴大交流面向及視野。SICW 不僅是資安領域的重要活動，除促進網路安全技術與解決方案之討論，也是各國交流資安政策與實務經驗的平台，增進國際間的數位信任，共同應對日益嚴峻的網路安全挑戰。

參訪團提出相關建議包括：推廣國際資安活動並加強國際資安合作與交流、鼓勵運用新興科技強化資安防禦措施、系統化管理與深化培育資安人才等，期促進我國資安領域相關作業與國際接軌交流，共同加強資安防護能量。

壹、目的

新加坡國際資安週（Singapore International Cyber Week, SICW）係由新加坡網路安全局（Cyber Security Agency of Singapore, CSA）主辦，自 2016 年舉辦迄今，SICW 已成為亞太地區知名的資安活動之一。新加坡政府每年邀請各國產、官、學界代表，就網路安全政策、實務營運經驗、資安技術手法與國際安全外交等不同層面進行分享與交流。

2024 年第九屆新加坡國際資安週於 10 月 14 日至 17 日在新加坡金沙會展中心舉行，活動期間不僅匯集來自世界各國的資通安全或網路安全政策之制定者、執行官、產業領袖與專家學者等共同參與，同時也搭配 GovWare 國際資安大會及展覽(GovWare Conference and Exhibition）、物聯網黑客松（IoT Hackathon： SPIRITCYBER）等資安活動，進行網路安全技術與解決方案之探討。

本年主軸為「數位時代的信任與安全」（Trust and Security in the Digital Era），主要針對地緣政治和經濟競爭、供應鏈脆弱性以及民主轉型等影響國際安全與穩定等相關議題，探討影響國際安全與穩定的資安問題與因應策略，分享數位挑戰、網路空間和資通安全政策演變、規範執行、物聯網（IoT）安全及關鍵基礎設施工業控制（Operation Technology, OT）領域安全等最佳實踐方案，期透過推動關鍵對話交流，建立國際夥伴關係，培養跨國數位信任（Digital Trust），強化跨域網路安全。

參與新加坡國際資安週（SICW）各項數位與網路安全議題相關的研討，並與新加坡網路安全局、荷蘭參訪團與德國參訪團等進行資安架構、政策以及執行策略等議題交流與分享，期能有助於我國資安主管單位進一步地瞭解國際資安發展的趨勢與現況、數位網路安全的挑戰與威脅、各國資安政策的實施與規劃、新興資安產業的熱絡發展等，並且透過資安政策、實務技術與執行面之討論，促進未來國際交流與合作之機會。

貳、過程

一、議程內容

2024 年第九屆新加坡國際資安週（SICW）於 2024 年 10 月 14 日晚間正式登場，由「SICW Summit 高峰會」拉開序幕，致詞貴賓為新加坡數位發展與資訊部長、內政部第二部長兼智慧國家與網路安全部部長 Josephine Teo 女士。SICW Summit 高峰會歡迎晚宴的照片如圖 1 和圖 2。

圖 1：SICW Summit 高峰會

圖 2：SICW Summit 高峰會-貴賓致詞

新加坡國際資安週（SICW）會議議程相當豐富與多元，包括：開幕式（Opening Ceremony）、高階全體會議及各項高階主題式會議（High-Level Panels）、GovWare 國際資安大會及展覽（GovWare Conference and Exhibition)，以及物聯網黑客松（IoT Hackathon：SPIRITCYBER）等。SICW 2024 大會場內照片如圖 3 至圖 6，議程內容詳如表 1。

圖 3：SICW 2024 大會-報到處

圖 4：SICW 2024 大會-入口處

圖 5：SICW 2024 大會-開幕致詞

圖 6：SICW 2024 大會-會場平配圖

表 1：SICW 2024 議程內容

日期	時間	活動名稱	性質
10/14	19：00－21：30	SICW Summit 高峰會	邀請制
10/15	09：00－09：20	SICW Opening Ceremony 開幕式	公開場次
	09：00－17：30	GovWare Conference and Exhibition 2024 國際資安大會及展覽	
		IoT Hackathon： SPIRITCYBER 2024 2024 物聯網黑客松	

日期	時間	活動名稱	性質
	09：20－12：30	High-Level Panels： Opening Plenary 〔高階座談〕開幕全體會議	
	10：00－16：00	ASEAN CERT Incident Drill （ACID） 東協 CERT 資安事件演練	閉門會談
	14：00－15：00	High-Level Panel： Insights into 2024’s Cyber Threats 〔高階座談〕 2024 資安威脅之洞察	公開場次
	14：00－15：30	SICW Women in Cyber 新加坡資安週女性網路從業人員會議	
	14：00－16：00	National Positions on International Law in Cyberspace： Challenges, Opportunities, and Best Practices 國家對網路空間國際法的立場：挑戰、機遇和最佳實踐	
		SG Cyber Safe for Enterprises 新加坡企業資訊安全會議	閉門會談
	14：00－16：15	Empowering RIE （Research, Innovation and Enterprise） Forum 賦能（研究、創新和企業）論壇	公開場次
	14：00－18：00	World Economic Forum Systems of Cyber Resilience：Electricity Initiative Global Community Meeting 世界經濟論壇（WEF）網路韌性體系： 電力倡議全球社群會議	閉門會談
	16：00－17：30	Solidarity in Cyberspace： How To Assist Countries in Need 網路空間的團結：如何協助有需要的國家	公開場次
10/16	08：30－12：30	ASEAN Ministerial Conference on Cybersecurity 東協網路安全部長級會議	閉門會談
	08：30－17：30	ASEAN Cybercrime Prosecutors’ Roundtable Meeting 東協網路犯罪檢察官圓桌會議	
	09：00－17：30	GovWare Conference and Exhibition 2024 GovWare 國際資安大會及展覽	公開場次
		IoT Hackathon： SPIRITCYBER 2024 2024 物聯網黑客松	
	09：30－11：00	High-Level Panel： Can AI be Secure？ 〔高階座談〕人工智慧的安全性？	

日期	時間	活動名稱	性質
	10：00－12：00	ASEAN CERT Incident Drill（ACID） 東協 CERT 資安事件演練	閉門會談
		The Geneva Manual： How Do Cyber Norms Guide Us In Protecting Critical Infrastructure？ 日內瓦指南：資安規範如何指引我們保護關鍵基礎設施？	公開場次
	10：30－12：00	International IoT Security Roundtable（IIoTSRT） 國際物聯網安全圓桌會議	
	11：00－11：25	2024 Global Challenge for Safe and Secure LLMs（Track 1）Prize Giving Ceremony 2024 全球安全可靠的 LLM 挑戰賽頒獎典禮	
	13：00－15：30	High-Level Panel： Trust and Security in the Quantum Era 〔高階座談〕量子時代的信任與安全	
	14：00－18：00	Global Forum on Cyber Expertise Southeast Asia Regional Meeting 2024 全球網路專業論壇：東南亞區域會議	閉門會談
	14：30－17：30	Mobile Security x Scams 行動裝置安全及詐騙	公開場次
10/17	09：00－10：35	High-Level Panel： Has the Era of Tech Broken Multilateralism？ 〔高階座談〕科技時代打破了多邊主義嗎？	
	09：00－16：00	10th Senior Officials Roundtable on Cybercrime 第 10 屆資深官員網路犯罪圓桌會議	閉門會談
	09：00－11：00	Whose Responsibility？ Indo－Pacific Perspectives on Responsible State Behavior in Cyberspace 誰的責任？印太地區對於網路空間負責任國家行為的觀點	公開場次
	09：00－17：30	GovWare Conference and Exhibition 2024 GovWare 國際資安大會及展覽	
	10：00－12：00	IoT Hackathon： SPIRITCYBER 2024 2024 物聯網黑客松－閉幕和頒獎典禮	
	11：00－13：00	SG Cyber Safe for Enterprises 新加坡網路安全計畫－企業版	閉門會談
	11：15－12：15	High-Level Panel： When the Next Disruption Strikes, Who is Responsible for Digital Resilience？ 〔高階座談〕當中斷發生時，誰該負責數位韌性？	公開場次

日期	時間	活動名稱	性質
	13：00－ 14：00	High-Level Panel： Augmentation of Cybersecurity Operations Using Artificial Intelligence 〔高階座談〕透過使用人工智慧以擴增資安運作	
	13：30－ 15：00	Securing Smart Cities 保障智慧城市之安全	
	14：00－ 16：00	Cyber Frontiers－ The Implications of AI for Security 網路邊境－AI 對安全的影響	

二、會議紀要

(一)活動主軸

現代日常生活已高度依賴數位系統，因此數位信任對於各國相互合作、資訊聯繫和數據交換等至關重要，對於政府、公民和行業互動和組織我們的社會、政治和經濟生活方式等相關的社會與經濟效益也影響甚巨，然而，當今數位世界複雜且多變，地緣政治衝突、經濟強烈競爭及供應鏈漏洞風險攀升等相關網路威脅也日益嚴峻，不僅是個資外洩、人工智慧誤用，抑或是新興科技如：生成式 AI、元宇宙和量子計算等所帶來的各種數位風險，都有可能嚴重地侵蝕與破壞對國際穩定和社會繁榮至關重要的數位信任，因此確保數位信任與安全是必要的，它不僅是技術問題，更是社會問題。

(二)會議摘要

1. 網路安全的威脅與挑戰

1-1. 假訊息氾濫衝擊民主選舉

為建立民眾對於數位選舉制度的信賴感，須有強大的資通訊安全措施和足夠的透明度機制，各國因地制宜地採取了不同做法，例如：巴西全面

採取電子投票，而荷蘭則保留紙本投票，然而關鍵性的重點應在於效率和安全性的權衡。

民主選舉等政治面制度的數位化應用欠缺信任感與安全性，已對 2024 全球選舉年的民主進程造成強力衝擊，政府必須採取打擊錯誤資訊或假訊息的相關措施，例如：波蘭建立選舉資訊平台，而馬來西亞不僅通過網路安全法案、修訂個人資料保護法及成立國家 AI 辦公室，也正在建立數位信任與安全委員會等來進行管理，惟同時仍須避免過度審查，以保護言論自由。

公眾教育也著實顯得重要，須讓民眾了解數位系統如何運作，更須從小培養人民批判性的思維，提高他們辨識假新聞的能力。

圖 7：SICW 2024 大會-場次照片 A

1-2. 人工智慧誤用凸顯監管必要

隨著人工智慧的廣泛使用，信任、控制和安全等資訊議題日益受到關注，特別是金融領域和醫療領域方面。人工智慧若遭到惡意地使用或誤用，極可能會造成人們的錯覺、偏見，或引用到不準確或虛假資訊等潛在風險。

1-2-1.各國應權衡資通訊安全、創新與監管策略

1-2-1-1.為加強國家的網路安全措施，同時兼顧公共利益及數位創新；政府和產業界必須透過強而有力的夥伴關係，建立明確的監管邊界，制訂靈活敏捷的監管架構，因此，科技產業監管機制的成功關鍵是協作。

1-2-1-2.當技術問題出現才進行監管，恐導致重大漏洞和巨大損害；因此，必須及早採取主動且彈性的監管措施，方能有效降低風險。

1-2-1-3.全面實施監管措施前，可透過監理沙盒（regulatory sandboxes）環境來測試、完善相關法規。

1-2-1-4.監管框架的設計必須隨著技術進步而發展，確保能快速地順應新興科技創新，並因應不斷變化的資安威脅。

為確保網路空間的穩定和安全，各國開始制定全面性的人工智慧治理指導方針，用以監督人工智慧技術的設計、開發和部署，例如：英國為促進人工智慧於創新、安全與道德因素之平衡發展，發佈了「人工智慧監管白皮書」（A pro-innovation approach to AI regulation），期透過實施靈活且具彈性的 AI 監管策略，支持企業發展新興科技並創造就業機會，同時確保 AI 使用的安全性與公平性。而新加坡網路安全局（CSA）於 2024 年 10 月 15 日發布「人工智慧系統安全指南」（Guidelines and Companion Guide on Securing AI Systems），期能確保 AI 系統運作的安全與穩定、降低供應鏈攻擊的潛在風險。

1-2-2.人工智慧的挑戰

人工智慧的管理，須優先解決安全風險的關鍵性議題，包括：可解釋性、排除偏見、合規性要求及透明度等，有賴政府、企業和學術界共同努力應對各種挑戰，包括：

1-2-2-1.規範面的挑戰，政府與企業須共同研議並制定人工智慧相關監管法規。

1-2-2-2.道德面挑戰:須提高各界對人工智慧應用的風險意識,如:網路威脅、數位身份等。

1-2-2-3.教育面挑戰：應鼓勵多元、創新的各種解決方案，包括：打擊人工智慧詐欺等。

1-2-2-4.國際面挑戰：須針對人工智慧應用系統進行安全性評估，並倡議全球專業學者進行協作討論。

圖 8：SICW 2024 大會-場次照片 B

1-3. 量子計算威脅下的數位安全需求

現代通訊與儲存的保密，高度仰賴加解密、數位簽章等密碼演算法，然而量子計算（Quantum Computing）的研發持續進展，未來大規模地通用量子電腦後，恐將破解當今的所有公鑰密碼系統（public-key cryptosystems），形成網路安全的重大威脅，使得機密資訊容易受到未經授權的惡意利用；因此，量子時代的當務之急，便是要保護數位信任並提供量子安全解決方案，同時更須開展各國政府與企業合作，以確保數位韌性，並保護數位資產免於量子威脅。

因應量子計算的威脅風險，美國、英國、法國、德國、中國、澳大利亞和日本等國，及 IBM、Google、Intel 等科技巨擘，皆已投入軍備等級的龐大資源，進行量子計算領域的研發工作。

以美國國家標準暨技術研究院（National Institute of Standards and Technology, NIST）為例，NIST 組織於 2024 年 8 月發布後量子密碼（Post Quantum Cryptography）標準，作為各國政府與企業據以保護數據、設備、連接和組件密碼的指導原則。

而新加坡則在 2024 年 5 月推出國家量子戰略（National Quantum Strategy），由科技研究局（A*STAR）、新加坡國立大學、南洋理工大學及新加坡科技設計大學等研究團隊整合推動量子研究及人才培育，將量子科技廣泛運用在各領域，並與海內外業者合作探討量子運算方案，期能創造新的經濟價值。面對後量子時代的挑戰，各領域皆須致力於保護系統、資料和基礎設施，確保數位韌性。

NIST 組織發布後量子密碼（PQC）標準，即代表後量子密碼保護時代正式來臨，全球密碼學和網路安全進入了全新的階段。

為維護數位時代之資安和隱私保護，量子安全系統必須經過適當的測試、評估與認證，但仍有可能存在未知的漏洞風險，故需國際合作夥伴，包括：政府、企業和研究機構等的緊密合作，共同進行開發、測試和更新加密技術。

圖 9：SICW 2024 大會-場次照片 C

2. 網路犯罪活動需各方合作抵制

勒索軟體氾濫、資料不當竊取與行動裝置詐騙等網路犯罪活動，隨著科技時代的進步已愈加顯得增長；烏克蘭戰爭和中東衝突所引發的駭客行動主義相關活動，甚至讓網路攻擊工具變得更加容易取得。各國、各界急需透過合作，共同努力打擊網路詐騙等犯罪活動，可行的做法包括：

2-1. 適當權衡便利性的要求與安全性的必要

不應為了追求便利而犧牲安全性相關檢驗，例如：金融機構為防堵詐騙，針對民眾的巨額交易行為，當下會採取延遲交易的機制來確保交易安全，但卻因此引發使用者不滿。而新加坡網路安全局與金融管理局則和規模較大的金融機構合作，強化其銀行的應用程式，當客戶使用該應用程式，程式便會自動啟動掃描手機的程序，一旦發現有疑似惡意軟件運作情形，該應用程式便自動無法開啟。

2-2. 加強使用者的公共教育

全面提升民眾對於防詐措施的認知、即時支付的警覺性等。

2-3. 深化服務提供者的責任歸屬

包括：電信商、數位皮夾等電子支付服務供應商、社交媒體網站或平台業者等，均應負起交易管道的責任問題。

2-4. 技術創新

2-4-1. 社交媒體平台可透過導入人工智慧技術，過濾詐騙資訊，並鼓勵使用者勇於舉報或標記。

2-4-2. 網路防禦者可運用人工智慧增強安全操作，例如：惡意軟體 AI 偵測、垃圾郵件 AI 過濾、日誌 AI 分析和事件 AI 調查等。

2-4-3. 強化資訊流安全，例如：隱私增強技術、加密傳輸技術等，防止機密資訊外流或遭未經授權的不當利用。

2-5. 應變能力

2-5-1. 透過即時資訊的共享和協作，讓受害者和相關權責單位均能夠在網路詐騙事件發生時，迅速採取行動，例如：MECA（Mount Druitt Ethnic Communities Agency）與金融機構合作分享情報，促進跨行業的資訊分享。

2-5-2. 德國已將關鍵基礎設施的網路與資訊系統安全性要求納入法規，且刻正建置一個統一的通報平台，一旦網路攻擊事件，關鍵基礎設施提供者須在指定時間內進行通報。

圖 10：SICW 2024 大會-場次照片 D

3. 全球數位治理的共通框架

加強國際合作，建立全球共通的數位治理框架與規範，是因應網路犯罪和不當威脅的必要作為，對於創新與監管的平衡，須採取基於原則的治理方式。聯合國等國際組織在推動全球數位治理中已發揮關鍵性作用，並確保規則得以遵行。公、私部門和民間社會都需要共同參與保護關鍵基礎設施和應對假訊息等具體挑戰，俾利在數位空間中建立安全、信任與必要的復原能力。

3-1. 全球 ICT 安全條約

數位技術促進全球經貿發展，同時帶來潛在濫用的負面影響。面對地緣政治競爭、軍事衝突和經貿競賽等議題，網路威脅和數位平台無國界，需要國際性的 ICT 安全條約或法規，來解決網路安全和資訊安全問題、促進網路空間的團結。

3-1-1. 2023 年歐盟與 28 個國家共同簽署的布萊切利宣言（Bletchley Declaration），率先促進人工智慧安全之全球性合作宣言。

3-1-2. 東協（ASEAN）會員國亦於 2024 年發布人工智慧治理和道德指南（ASEAN Guide on AI Governance and Ethics）。

圖 11：SICW 2024 大會-場次照片 E

3-2. 適應數位時代的多邊主義

3-2-1. 在科技時代下，網路安全議題持續提升跨國合作需求，促進多邊

主義（multilateralism）的發展，各國政府在網路空間應為其行為負責，強調採取集體協作和承擔責任的重要性。

3-2-2. 各國應致力於縮小數位落差（digital divide），促進所有利害關係者如：民間社會、企業、政府等，在決策過程中皆有平等的發言權，確保多邊主義的開放和包容，讓不同立場的聲音都得到傾聽，尋求各方共同利益以及解決方案，讓所有國家參與全球數位治理。

3-2-3. 網路外交須結合傳統外交技能與技術專長，外交官須提升技術知識，技術專家也須培養談判能力。

圖 12：SICW 2024 大會-場次照片 F

4. 跨國、跨域、跨業的公私協力合作及共享責任（Shared Responsibility）

4-1. 面對網路安全威脅的多樣性，「公私協作」是激勵技術創新和因應社會挑戰的最佳方式，未來需促進政府機關、產業界、學術界之間更多的合作機會，共同提出創新解決方案。

4-1-1. 新加坡網路安全局（CSA）與甲骨文（Oracle）公司共同研發建構一套網路安全生態系統，因應當前和未來的網路安全問題和挑戰。另外，新加坡網路安全局（CSA）也與 Google 合作推出「Safe App Standard 安全手機應用標準」，讓設計手機應用的開發者參考該

標準，實現安全設計。

4-1-2. 荷蘭政府與私部門合作收集更廣泛且及時的情資，不僅提高情資收集效率，還促進整個社會對網路安全的重視。同時，荷蘭除了是歐盟成員國外，也參與一些較小規模的區域安全聯盟，藉由多層次的合作，使國家能夠在不同場合分享和獲取關鍵資訊。

4-2. 區域組織在全球數位治理的作用，是將各國聚集在一起，分享想法，執行聯合國相關規範；透過跨國合作計畫，縮小數位落差，促進發展中國家取得技術和數位資源的管道、減少不公平。

4-2-1. 聯合國於 2024 年 9 月在紐約舉辦「未來峰會」及「未來峰會行動日」，聚焦多個關鍵領域包括：永續發展、國際和平與安全、科技創新、數位合作、青年賦權和全球治理等，會議中通過 3 項重大決議：《未來契約》、《全球數位契約》和《未來世代宣言》，旨在為國際社會提供一個共同的行動框架，以應對全球性挑戰並創造更美好的未來。 其中《全球數位契約》聚焦於科技創新和數位合作，期建立一個更加包容、安全和公平的數位世界。同時探討了全球治理體系的轉變，須建立更有效的國際合作機制，俾利更好地應對未來的複雜挑戰。另外「未來峰會行動日」，特別關注多方利益關係者的夥伴關係和具體行動，希望推動更具包容性和網路化的多邊主義，強調全球治理正在向更加開放、靈活和參與性的模式轉變。

4-2-2. Google 近年持續投資太平洋地區海底電纜系統之鋪設與營運，強化網路效能和數位韌性，期能滿足各方需求，凸顯大型科技巨擘積極為包容性和繁榮投入貢獻。

4-3. 鑒於大型科技公司的重大影響力，如何讓這些科技巨擘承擔保護公民的責任，係各國政府面臨的挑戰。以 Google 為例，Google 近年持續投資太平洋地區海底電纜系統之鋪設與營運，強化網路效能和數位韌

性，期能滿足各方需求，凸顯大型科技巨擘積極為包容性和繁榮投入貢獻。

圖 13：SICW 2024 大會-場次照片 G

5. 數位韌性

5-1. 關鍵基礎設施是民生社會重要支柱，但數位系統的脆弱性將受網路攻擊等問題而產生跨領域性的連鎖反應。

5-2. 數位韌性，對維持民眾信心和促進數位化發展起著關鍵性作用，且數位復原力不僅是技術問題，尚涉及政策、責任分配和跨部門合作等更廣泛的議題。

5-3. 相關利益關係者應共同參與數位韌性，政府、產業、學界等均須協作提出解決方案，包括：公私部門資訊共享機制、完善法規並鼓勵協作、採用國際規範標準及供應鏈網路安全認證等。

5-4. 荷蘭國家網路安全中心（National Cyber Security Centre, NCSC）透過鼓勵政府與企業之間的合作，提升荷蘭社會的數位恢復能力。NCSC 目前專注於評估荷蘭面臨的整體網路威脅、了解關鍵基礎設施的 IT 和 OT 系統運作，以及分析軟、硬體和供應鏈漏洞，為政府和關鍵基礎設施提供者提供資安建議、風險評估和事件應變支援。未來 NCSC 依據即將公布的歐盟指令，將成為國家網路安全權責機構，因此 NCSC

正在 IT 系統和運作流程等方面進行大規模投資並推動數位轉型，朝向以數據為導向的決策模式發展。

圖 14：SICW 2024 大會-場次照片 H

三、GovWare Conference and Exhibition 國際資安大會及展覽

GovWare 國際資安大會及展覽以「保護動態數位路線圖：重新審視身份識別、數位信任與韌性（Securing Dynamic Digital Roadmaps: Relooking Signposts in Identity, Trust, and Resilience）」為主題，提供變革性見解，解決現代安全問題，重建數位信任，並規劃一個安全、包容的數位未來。

展覽活動中，新加坡網路安全局（CSA）分享其正在為建立一個值得信賴、有韌性且更安全的網路空間做努力，包括：強化基礎設施數位韌性、加強國際網路安全合作、開發網路安全生態系統，與發展強大網路人才管道等。

對於培育網路人才方面，新加坡網路安全局（CSA）提出網路安全發展計畫（Cybersecurity Development Programme），此計畫是一項為期 12 個月的發展計畫，旨在將應屆畢業生培養成全面發展的初級網路安全專業人員，透過在公共部門建立網路安全能力，為新加坡的數位經濟和數位政府做出貢獻。

圖 15：GovWare 國際資安大會及展覽 A

圖 16：GovWare 國際資安大會及展覽 B

參、心得及建議

新加坡國際資安週（SICW 2024）聚集來自美國、加拿大、巴西、澳洲、紐西蘭、波蘭、荷蘭、烏克蘭、瑞士、英國、汶萊、菲律賓、印尼、馬來西亞、日本、俄羅斯與中國等公私部門之產、官、學界專家代表，就政策、實務、技術與外交等進行不同層面的分享與交流。

隨著變化不斷的跨境威脅增加，臺灣應加強與國際機構合作，建立符合全球規範的技術監管標準，促進網路安全和數位治理領域跨國合作的雙邊和多邊協議（bilateral and multilateral agreement）。

借鑒於荷蘭政府的國際合作模式，採納多方位、多層次的方式與私部門和國際組織進行廣泛合作，不僅可提升自身的安全能力，也有助於使我國在全球的網路安全格局中佔有重要地位。

資安是產業的基石，臺灣未來應持續集結政府、產業界和學術界的能量，促進各利害關係者的對話交流，強化產業資安和資安產業相關工作，包括後量子遷移技術的推進。面對後量子時代的挑戰，各領域皆須致力於保護系統、資料和基礎設施，確保數位韌性。我國數位發展部的施政三箭「積極推動打詐、強化數位韌性、驅動數位經濟發展」，其中數位韌性有賴於導入「後量子加密」（post-quantum cryptography, PQC）技術遷移及創新應用，提升整體產業資安韌性，推動後量子資安相關產業發展、強化後量子資安技術能力。

為提升物聯網設備的安全性，新加坡推動「網路安全標章計畫（Cybersecurity Labelling Scheme, CLS），透過 CLS 標章的品質保證，協助消費者了解智能設備的網路安全。新加坡網路安全局（CSA）於本次會議中宣布與韓國、德國簽署「網路安全標章相互認證協議」，以降低合規成本、促進市場准入，希望未來也能跟更多國家或跨國公司合作。我國未來可加強輔導軟體及資訊服務業之國際發展，積極加入新加坡 CLS 計畫，促進臺灣資安產業鏈接國際市場數位商機；亦可透過數位經濟相關產業創新研發補助，引導業者開發具市場競爭力之數位產品或服務，進而提升民眾對於我國資安廠商技術及服務能量之信任。

全面提升國民資安意識，包括：網路詐騙、身分驗證等，有助提升民眾辨識假訊息並避免落入社交工程釣魚陷阱之知能。持續舉辦資安女捷思活動，從教育女學生應有正確資安概念著手，鼓勵女性投入資安科技領域。推動在學資安知能培育與在職資安技能訓練等，全面性發展資安人才生態，建立我國資安人才源本。

參考上述資安管理思維與作法，提出相關持續精進之三項建議如下：

一、推廣國際資安活動並加強國際資安合作與交流

隨著變化不斷的跨境威脅增加，資安是全球共同面臨之議題，建議善用國際資安活動與交流機會，推廣我國資安政策及執行策略，同時介紹及邀集各國產、官、學界代表參與我國定期辦理之「前瞻資安探索會議」（Advanced Cybersecurity Exploration Conference, ACE）以及跨國網路攻防演練活動（Cyber Offensive and Defensive Exercise, CODE），進一步地促進國際資安交流與技術經驗分享。

二、鼓勵運用新興科技強化資安防禦措施

在國家級跨部門合作平台，建議運用新興技術如：AI、大數據分析等，提升情資收集、處理和分析的能力，協助篩選重要資訊、識別潛在風險，並自動化分享，縮短反應時間，以加強關鍵基礎設施領域情資分享，提升國家和企業應對各種威脅（如：自然災害、網絡攻擊或其他安全事件）防範能力。同時也建議推廣運用零信任架構，透過身份驗證、設備鑑別與信任推斷機制，增強各機關資安防護能量。

三、系統化管理與深化培育資安人才

持續地加強培育工控領域攻防實戰人才或關鍵基礎設施相關人員的安全意識和技術培訓，強化相關領域資安防護水準。同時也建議透過系統化地管理政府機關資安人才資料，藉此精進資安人才培育與任用。