出國報告（出國類別：開會）

2024年布拉格資安大會

出國報告書

服務機關：數位發展部資通安全署

姓名職稱：闕河鳴政務次長

鄭欣明副署長

鄒博全專員

派赴國家/地區：捷克/布拉格

出國期間：**113**年**3**月**16**日至**113**年**3**月**22**日

報告日期：**113**年**6**月

摘 要

捷克國家網路及資訊安全局（National Cyber and Information Security Agency ， NÚKIB）邀請數位發展部出席2024年布拉格資安大會（Prague Cyber Security Conference 2024），布拉格資安大會前身為「布拉格5G 安全會議」（Prague 5G Security Conference），是關於網路及電信安全防護的國際重要會議，成員遍布全球30多個國家的政府官員，以及來自歐盟、北大西洋公約組織和業界的代表，共同聚集捷克布拉格探討各國5G 網路架構及電信網路供應的安全性。

今年布拉格資安大會適逢《布拉格5G 安全法案》（Prague Proposals on 5G Security）通過五週年，鑑於該法案是全球尋求次世代網路安全與可信任供應商的重要里程碑，為各國建造及設計5G 網路基礎設施的重要參考來源，大會今年特別邀請各國資安專家共同針對網路威脅、資通訊政策和監管、公私合作夥伴關係、後量子密碼學、人工智慧等議題進行討論和交流，數位發展部應邀代表我國與會。

海纜對於國內外通訊、安全及經濟至關重要，近年來遭受越來越多破壞、干擾與網攻威脅。數位發展部闕河鳴次長應邀出席布拉格資安大會擔任與談人，該場座談主題為「關於水下：保護海底電纜免受資安威脅和外國干擾」（Under Water: Protecting Subsea Cables from Cyber Threats and Foreign Interference），分享2023年3月馬祖連接臺灣本島的海纜中斷之處理經驗，如即時切換成微波及衛星通訊，確保國內通訊韌性；並強調數位部持續盤點不同情境對通訊網路的風險，規劃和落實多元異質的通訊備援網路措施，從海、陸、空多維度強化通訊韌性與資安防護作為。

此外，各國資安人才短缺問題嚴重，無論公部門及私部門皆在積極尋找及培育優秀的資安人才，本次大會主題「資安人才：建立和保留資安人才是一項共同責任（Cyber Workforce: Building and Retaining Cyber Talent as a Shared Responsibility）」，邀請日本、愛沙尼亞、阿爾巴尼亞及 Google 公司的專家學者，就現行各領域資安人才應具備的溝通能力及技術能力進行討論，並分享各國培育資安人才的方法。

目 錄

壹、基本資料

一、活動名稱：2024年布拉格資安大會（Prague Cyber Security Conference 2024）

二、活動時間：2024年3月19日至3月20日，上午8時至下午4時30分（布拉格）

三、活動地點：捷克國家銀行會議中心（The Congress Centre of the Czech National Bank）

四、出席人員：數位發展部（以下稱本部）關河鳴政務次長、資通安全署鄭欣明副署長、鄒博全專員（以下簡稱參訪團）

五、參與場次表

日期	參與場次	參與人員
3月18日	拜會駐捷克台北經濟文化辦事處	關河鳴政務次長 鄭欣明副署長 鄒博全專員
3月19日	1. 拜會捷克國家網路及資訊安全局 2. 《布拉格5G 安全法案》通過5年後ICT 供應鏈資安防護及電信業的發展 3. 是否需要技術上的防護措施、法律來確保人工智慧的安全 4. 布拉格資安大會－關於水下：保護海底電纜免受資安威脅和外國干擾	關河鳴政務次長 鄭欣明副署長 鄒博全專員
3月20日	1. 網路無國界：實現全球夥伴合作關係 2. 布拉格資安大會－資安人才：建立和保留資安人才是一項共同責任	鄭欣明副署長 鄒博全專員

註：本報告書揭露範圍，係本次出國行程所參與之國際交流合作相關會議與活動未涉及機敏部分，另布拉格資安大會以下場次，因訪團參加與捷克國家網路及資訊安全局及其他國家之交流會議，故未能參加：

（一）對抗網路攻擊及建立數位韌性（Countering Cyber Aggression & Building Resilience）。

（二）相同目標，不同方法；關鍵基礎設施事件通報之協調（Same Goal, Different Approaches: Harmonizing Incident Reporting for Critical Infrastructure）。

（三）共同嚇阻勒索軟體生態系統（Disrupting Ransomware Ecosystem Together）。

貳、會前拜會活動

一、拜會駐捷克台北經濟文化辦事處

訪團於布拉格資安大會前1日拜會駐捷克台北經濟文化辦事處，由駐捷克台北經濟文化辦事處科技組洪廷甫組長，洪廷甫組長亦為國立屏東科技大學材料工程系教授，與本次訪團闕河鳴次長及鄭欣明副署長皆為大學教授，洪組長亦分享捷克之學術環境，並依其對學術上專業及對捷克國情與外交實務經驗，分享捷克近年來公共數位化、資安防護作為及科技發展及臺灣與捷克關係及過往合作的情形。

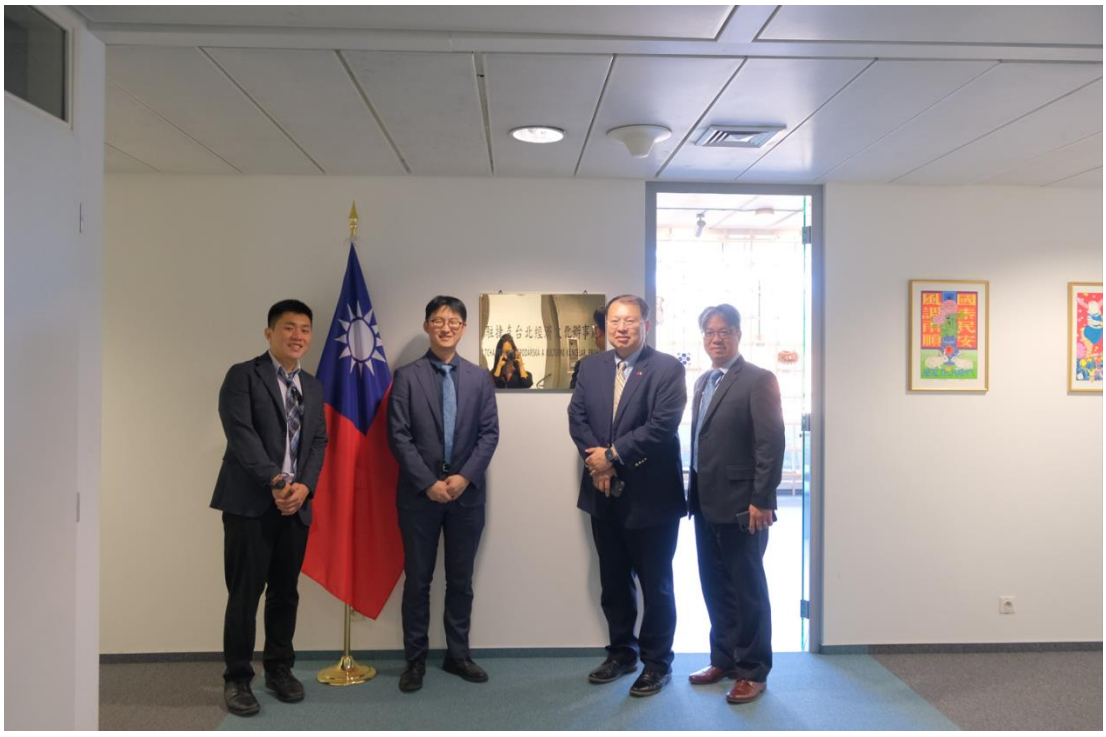

圖 1　訪團與駐捷克代表處合影

訪團亦分享數位發展部過往與捷克國家網路及資訊安全局（National Cyber and Information Security Agency, NÚKIB）交流情形，包含自2019年 NÚKIB 參與「2019年首屆跨國攻防演練（CODE）」，並獲得第1名佳績，2023年亦組隊參加資安署舉辦之「2023年跨國網路攻防演練（CODE）」等等，並與駐捷代表處說明本次訪團將與捷克國家網路及資訊安全局討論進一步參與國際間的跨國攻防演練之可行性，請駐捷代表處就深化雙方關係提出建議以及討論隔日與捷克未來可共同合作的項目，駐捷代表處亦建議本訪團未來可積極推動與捷克間之公共數位化及資安攻防演練等合作。

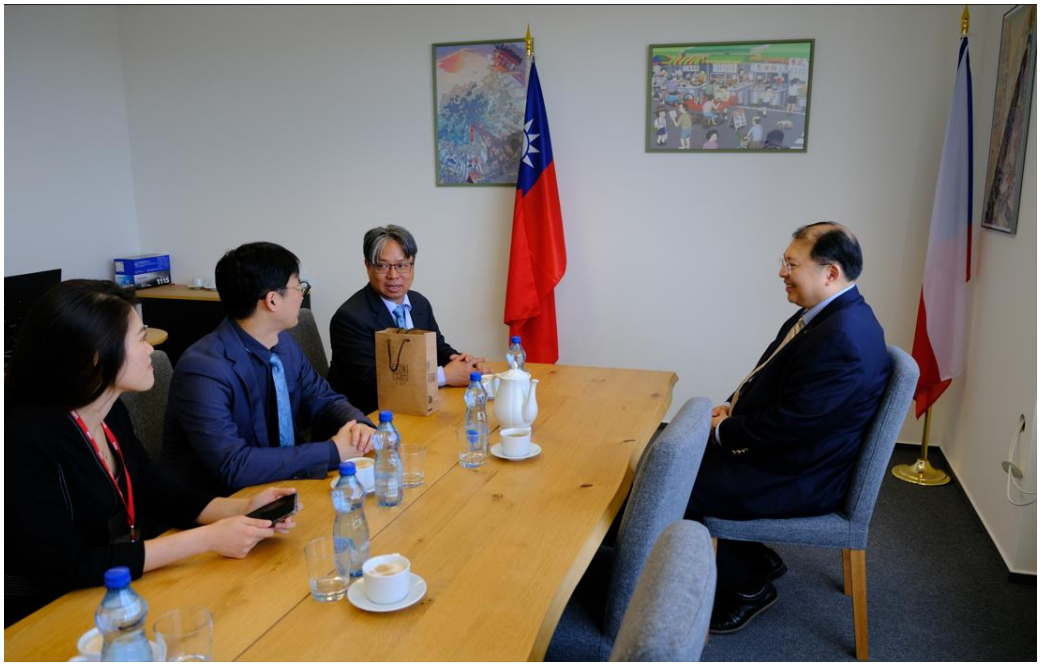

圖 2　資安大會會前會議討論過程

二、 拜會捷克國家網路及資訊安全局

訪團此行於布拉格資安大會第一天，與主辦方捷克國家網路及資訊安全局局長 Lukáš Kintr、國家通訊與資訊安全局局長內閣 Josef Kopecký 及捷克駐澳洲大使館的印太網安協調官 Veronika Kolek Netolicka 等人進行雙邊會談，共同研商臺灣與捷克未來在資安領域合作的方向，訪團分享我國的資安防護的近況，雙方就臺灣及捷克合作資安防護、資安人才培育、共同演練資安攻防等議題進行對話交流，

交流國際間資安攻防專業知識及經驗。

圖 3 代表團闕河鳴團長與捷克國家網路及資訊安全局局長 Lukáš Kintr 合影

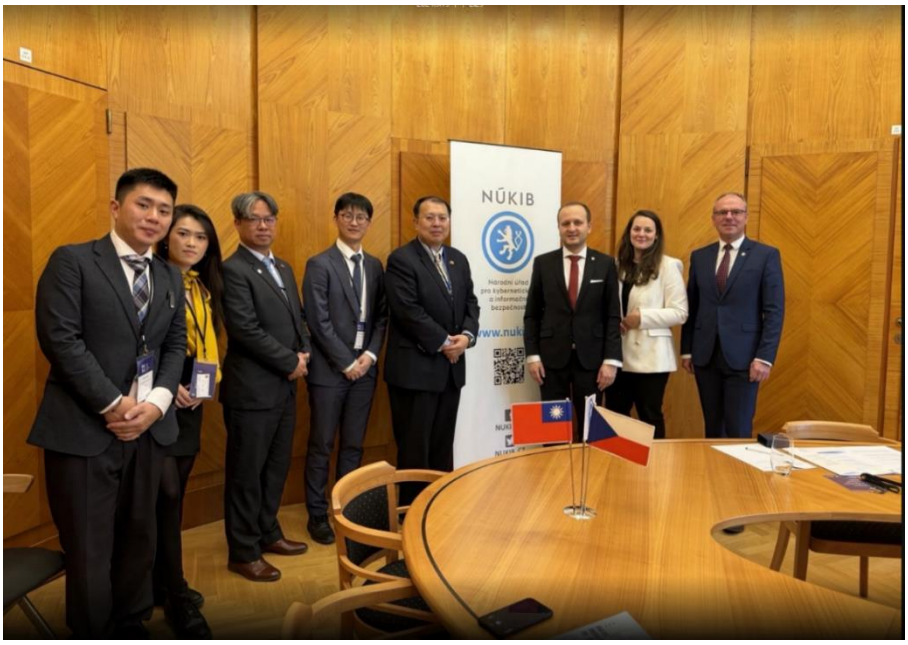

圖 4 訪團全體與捷克國家網路及資訊安全局代表合影

訪團亦邀請捷克方參加數位發展部舉辦之2024年「前瞻資安探索會議」（Advanced Cybersecurity Exploration Conference, ACE），亦邀請未來與我國合作參加跨國攻防演練，期盼藉由國際資安專業知識及實

戰演練交流，持續強化臺灣與捷克之網路資安防護，提升我國數位韌性。捷克方由衷感謝訪團應邀參加本次布拉格資安大會，並允諾未來會加強並延續臺灣與捷克之合作關係。

參、會議重點摘要

一、會議現場概況

布拉格資安大會舉辦於捷克國家銀行會議中心（The Congress Centre of the Czech National Bank）為布拉格的金融中心，大會的安全措施非常完善，警力部署充足，入場必須經過嚴格的保全系統，確認沒有攜帶任何危險物品。

通過安檢後，會議外部設立站立桌，提供各國資安專家彼此交流，會議開場典禮播放捷克共和國總統 Petr Pavel、歐盟委員會價值與透明副主席 Věra Jourová 及美國國家安全委員會網路與新興技術副國家安全顧問 Anne Neuberger 開場演講，強調各國資安合作的重要性，會場內部提供講台供各場次講者上台共同討論該場次主題，供觀眾隨時發問。

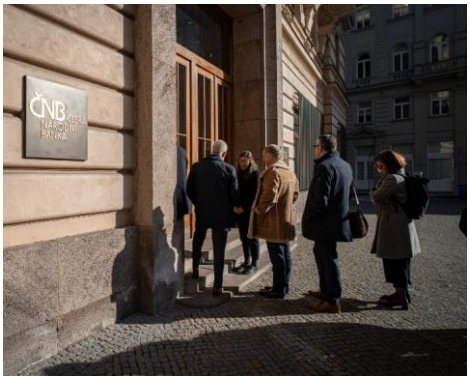

圖 5 大會進場隊伍

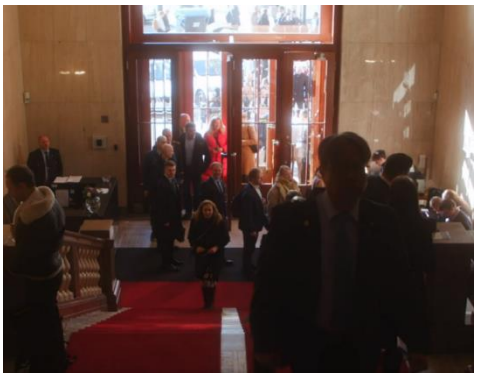

圖 6 大會安檢櫃台

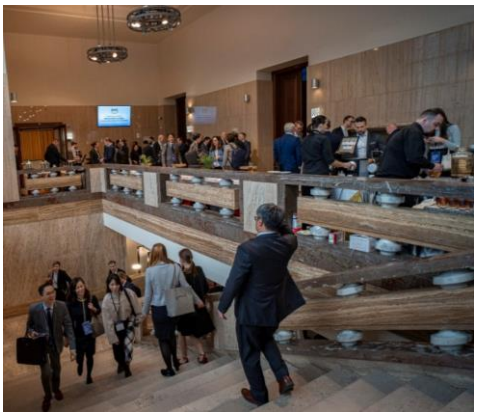

圖 7 大會外部交流現場

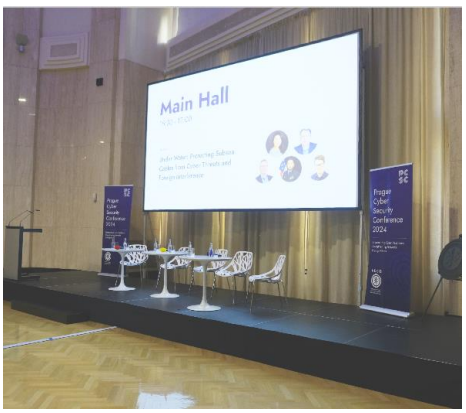

圖 8 大會內部設置

二、《布拉格5G 安全法案》通過5年後 ICT 供應鏈資安防護及電信業的發展（Five Years Since the Prague Proposals on 5G: ICT Supply Chain Security Beyond Telecommunications）

（一）主持人：Katie D'Hondt Brooks, Director, Global Cybersecurity Policy, ASPEN DIGITAL

（二）與談者：

1. Pavel Štěpáník, Deputy Director, Strategic Affairs and Engagement Division, NÚKIB
2. Brendan Dowling ,Ambassador for Cyber Affairs and Critical Technology （DFAT）, Australia
3. Isamu Yamaguchi, NISC, Japan
4. Dan Cimpean, Director of Romanian National Cyber Security Directorate
5. Jennifer Bachus, Deputy Ambassador for Cyberspace and Digital Policy, USA

（三）重點摘要：

1. 《布拉格5G 安全法案》及布拉格資安大會之時空背景及影響力

捷克國家網路及資訊安全局副局長Pavel Štěpáník 提到，五年前，我們在這裡召開會議，首次發布了《布拉格5G 安全法案》，法案中強調在推動供應鏈安全時，所有利害關係人的共同責任，在這場討論中更詳細地探討彼此的共同責任，特別是電信業的供應商，通常在建置5G 網路時，會需要依賴其他供應商的技術，然而，跨供應商間的技術複雜性淺藏著重大的資安風險，在現今5G 網路被廣泛採用，規範供應鏈安全及電信業者的責任，對國家安全、經濟安全和其他國家利益有著重要影響，有關《布拉格5G 安全法案》起源，可以追溯到2018年使用華為通訊設備的安全爭議，或是更早的2014年。

當時，捷克意識資安防護到不是只有技術層面的問題，也涉及到非技術層面的問題，捷克發現使用華為所提供的設備或技術存在潛在

風險，對華為發出警告，即便這個警告涉及到中國的法律，但從捷克的情報機構得知，當時捷克國家的關鍵數據可能會被竊取，因此不能袖手旁邊。

Pavel Štěpáník 提到資通安全法規的基礎涉及到很多層面，包含政府的採購以及國家安全與自由市場經濟之間的權衡問題，因此2018年召開布拉格安全會議，發布《布拉格5G 安全法案》，是為了分享捷克和其他類似國家的經驗，讓不同國家可以針對不同的資通安全議題進行討論。

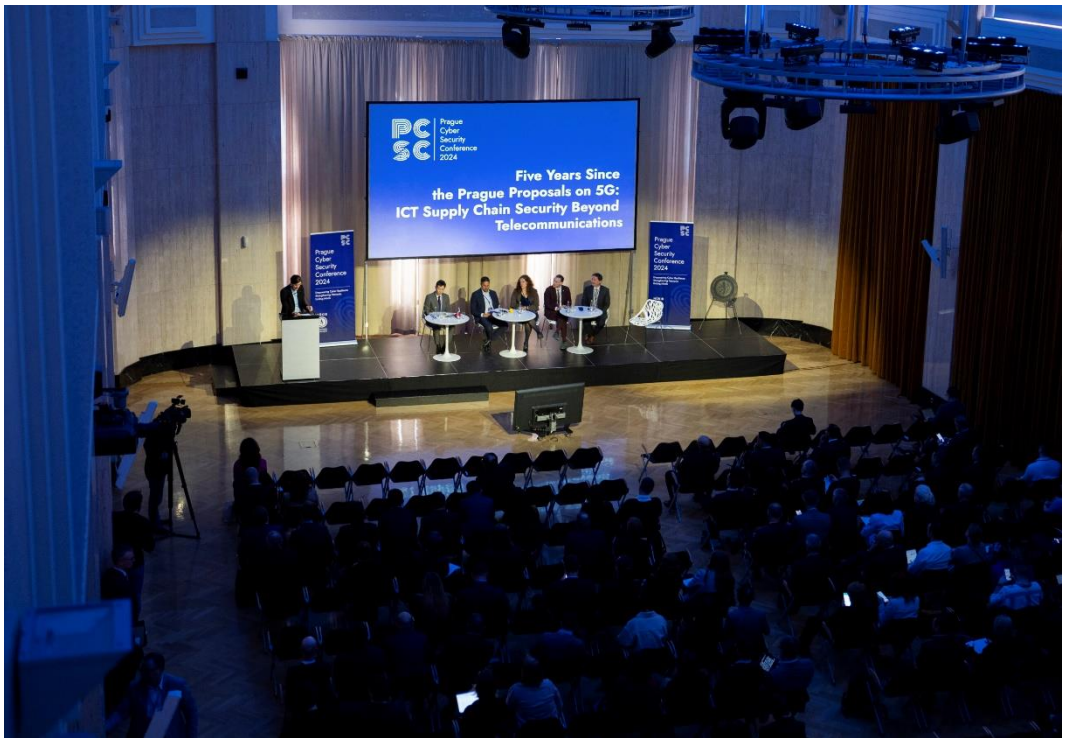

圖 9 5G 供應鏈資安防護討論過程

澳洲講者感謝《布拉格5G 安全法案》所帶來的影響力，也提到在《布拉格5G 安全法案》發布前一年，澳洲已經要求國內的通訊業5G廠商，在建設5G 網路時禁止使用高風險的技術或設備供應商，通常被稱之為「華為禁令」，當時澳洲是少數表態推行「華為禁令」的國家之一，在「華為禁令」公布之後，澳洲也付出了代價，隨即面臨了中國的經濟脅迫，但澳洲政府在市場經濟以及國家安全之間，選擇了國家安全。

捷克講者提到，因為5G 帶來了更多機會，但也帶來了更大的風險，

強調推行法案不是出於地緣政治的考量，不是針對特定國家，而是需要保護國家需要保護的主權，各個國家都有共鳴，覺得國家主權至關重要，捷克花很多時間在指導印太地區國家對於5G 網路投資的政策，但即便在《布拉格5G 安全法案》推行5年後，國際間供應鏈及電訊業5G 網路的資通安全問題尚未解決，許多國家仍然處於國家經濟因素和安全性之間做選擇的困境。《布拉格5G 安全法案》希望政府和民間業者對國家安全負責，在國家安全的情況下保有選擇的空間，並能夠優先考慮建置安全的5G 網路，而不是妥協於經濟因素，全球需要更多樣化的5G 網路技術供應商市場，需要更多創新技術加入無線網路的市場。

2. 《布拉格5G 安全法案》最成功的地方及可改進之處

日本講者提到，日本總務省在2019年制定了「5G 頻率分配指南」，要求日本政府和固定廠商在部署5G 網路時需要考慮安全性，該指南方向與布拉格提案一致，日本的電信業者在5G 核心網路不使用不受信任的技術供應商，日本非常感謝捷克政府主辦這次重要會議，《布拉格5G 安全法案》在2019年和2021年在供應鏈安全上提供多方面的指引。日本在2023年 G7廣島峰會會場上發布了 G7領導人關於經濟韌性和安全的聲明，該文件中也引用了《布拉格5G 安全法案》相關的指導原則，整體來說《布拉格5G 安全法案》指導文件對日本的5G 網路政策制定帶來重大的影響及幫助。

美國講者提到，《布拉格5G 安全法案》推行5年後，在許多國家仍有工作還沒有完成，他在世界各地旅行時看到，很多國家確實面臨著經濟因素與安全性之間的選擇問題，這些國家的建置網路決策最終是由私人企業做出的，而私人企業通常會基於經濟利益做決策，因此，政府需要在國家安全問題上發揮作用，就像在做對消費者保護一樣，然而安全性問題不僅僅局限於5G，還包括從海底電纜到雲數據中心和衛星的所有通訊相關基礎設施，這是一個廣泛的議題，需要共同面對經濟脅迫帶來的挑戰，並且支持那些受到影響的國家。

羅馬尼亞講者提到，當時在羅馬尼亞提出5G 安全指南草案時，我們參考了《布拉格5G 安全法案》中的許多原則，包括供應鏈管理，我們決定將這些原則提升到國家最高決策層級，由國家最高安全委員會來做決策，目的是確保5G 網路的部署和運行安全，並能識別及管理相關風險。這是一個非常複雜的過程，涉及到軟體和硬體等技術，在羅馬尼亞，這不僅僅是政府網路安全監管相關機構的責任，而是整個國家安全系統的責任，因此需要借鑒其他國家的經驗，內部協調一致來應對挑戰。

三、是否需要技術上的防護措施、法律來確保人工智慧的安全（**Ensuring Safe and Secure AI: Do We Need Principles, Guardrails or Regulation?**）

（一）主持人：Evi Fuelle, Director, Global Policy, Credo AI

（二）與談者：

1. Nicole Foster, Director of Global AI/ML & Canada Public Policy, Amazon Web Services
2. Priscilla Delgado Argeris, Chief Counsel, U.S. Federal Communications Commission
3. Daniel Všetečka, Director of Digital Economy Department, Ministry of Industry and Trade, Czech Republic
4. Krzysztof Socha, Team Leader of the Incident Handling Team, CERT-EU - Poland

（三）重點摘要：

隨著生成式人工智慧的興起，全球社會正在尋求應對人工智慧風險的方法，包括通過歐盟人工智慧法案或美國人工智慧行政命令，本場討論探討人工智慧對網路威脅格局的影響、人工智慧監管的未來，以及國際間相互協調及合作的機會。

1. 使用人工智慧服務的潛在風險

主持人提到，在過去的一兩年中人工智慧的領域發生了顯著變化，雖然預期的變化並沒有那麼深遠，有許多新的研究和各種想法以及技術正在湧現，特別是法律和資安防護方面，從實際技術面的角度來看，使用人工智慧仍存在著風險，現今應致力於如何保護使用者免受這些風險，然而，這些風險經常需要即時應對，當今可透過很多不同的技術來解決使用人工智慧所帶來的風險，然而使用技術本身也淺藏著風險，我們必須同時考慮使用技術及不使用技術背後所潛藏的風險。

捷克講者提到特別在使用人工智慧無法律規範的情況下，瞭解使用人工智慧的風險很重要，因為這些風險非常棘手，然而，在過去的大部分時間裡，政府並沒有真正理解人工智慧。

捷克講者過去投入人工智慧研究多年，研究領域涉及機器學習和其他人工智慧技術，後來被納入了各種學術研究中，捷克講者指出，當我們檢視人工智慧的技術發展，會發現它們已經使用機器學習技術很長一段時間，但起初機器學習的技術並沒有被廣泛接受，因為很少有人能夠接觸到這些技術，即使在2019年 GPT-2模型推出時，也只是引起了有限的公眾關注，並沒有迅速推廣，直到2022年才真正開始被廣泛討論。

當時機器學習的工具、知識和技能還未普及，經常使用機器學習的技術，是根據觀察來改進機器學習的結果。有時候它們很成功，有時候卻不太成功，因為當時缺乏明確的訊息，無法知道它們是如何工作的以及可以得到什麼效果，現在大眾更加注重人工智慧的發展，投入人工智慧的領域日趨增加，開始有更多關於人工智慧方面的討論，人工智慧技術提供者在使用時會更加謹慎。

捷克講者強調，雖然目前最新的模型可以得到我們想要的答案，但現在我們對人工智慧的風險和問題的理解還很有限，這些風險通常很難發現和檢測，需要進行大量測試和評估，才能確保它們的安全性，現今有許多公司僅僅假設它們是安全的，並在沒有進行充分測試的情況下，依賴人工智慧來執行工作，這是需要警惕的情形。

美國講者認為這涉及人工智慧在初期階段僅專注於某些方面，例如製造或是提供餐飲服務，當今，我們已經看到人工智慧被用來解決各種問題，比起被作為製造產品或提供某種服務的技術，現在人工智慧更像是一個具有多重用途的工具，在網路安全領域，人工智慧被用用來監控網路中的惡意攻擊，並透過機器學習技術收集攻擊數據，並透過人工智慧與惡意攻擊互相攻擊，美國國防部門和其他機構也在關注人工智慧發展，在美國有多個信息模型來應對個是惡意攻擊，並使用人工智慧來確保國家全，這是一個非常專業的領域，必須投入更多資源，以應對不斷變化的情況。

波蘭講者提到，人工智能的應用在快速擴展，但我們應該注意其人工智慧在不同領域的所帶來的影響和可能的威脅，比如透過人工智

慧研究如何更好地管理和共享頻譜使用，特別是在各種設備皆在使用頻譜的情況下，如何透過人工智慧技術改進頻譜管理和共享的過程，檢測和預測可能的干擾源，人工智慧的技術對改善頻譜使用及預測可能出現的問題非常重要。

圖 10 人工智慧使用風險討論過程

2. **對於人工智慧所需要的防護措施。**

Amazon 及主持人提到有很多人工智慧的服務在快速進行，需要確保使用生成內容時不會對公眾產生負面影響。除了技術能力外，講者認為需要建立更多的機制來識別和管理人工智慧生成的內容，需要來從政府和法律方面的角度切入，這也是為什麼人工智慧的防護需要跨界合作的重要原因，儘管我們有足夠技術工具和能力來解決人工智慧的風險，但像是隱私侵犯或是生成假信息等等，都需要制定政策和法律來防護，人工智慧在安全性和實踐方面存在諸多風險，涉及到安全性和隱私之間相互關聯性，以及不使用人工智慧帶來的新風險。我們需要提出相應的政策和規範。

主持人提到，對我們而言，最重要的是對人工智慧保持警惕，即

便它帶來了許多好處，但也帶來了使用及管理上的挑戰，確保人工智慧的使用是安全且永續的，需要技術、政策和社會各方的共同努力。本場討論，深入探討人工智慧技術的發展和應用中面臨的風險和挑戰，特別是如何在隱私、安全和創新之間找到平衡，強調使用所有人工智慧技術前，都需要仔細地做好風險管理。

四、關於水下：保護海底電纜免受資安威脅和外國干擾（Under Water: Protecting Subsea Cables from Cyber Threats and Foreign Interference）

（一）主持人：Daniel Bagge, Senior Intelligence Specialist, Strider, Czech Republic

（二）與談者：

1. Herming Chiueh, Deputy Minister, Ministry for Digital, Taiwan
2. Jaakko Wallenius, Vice President, Chief Security Officer, ELISA
3. Jack Shis, Head of Strategy Branch, NATO CCD COE
4. Grace Koh, Vice President, Government Affairs, Ciena

（三）重點摘要：

主持人提到，海底電纜對於全球安全和經濟至關重要。同時，海底基礎設施面臨越來越多的破壞、干擾和網路攻擊。本場次討論探討海底電纜日益增加威脅，以及各國如何從國家安全的角度來加強保護海底電纜，未來共同合作努力，研擬降低風險的策略，並專注於重要的技術和政策問題，在這次大會有副總統和技術政策中心的專家，還有白宮國家經濟委員會的代表都會參與討論。

主持人介紹本次講者有來自政府、民間部門、軍事和各行動領域的代表背景，其中有一位電子工程系的副教授，在國際上非常有影響力，還有是芬蘭最大的營運商的副總裁兼首席執行官擔任講者，在海底電纜的攻擊事件中具有豐富的經驗，將共同講述海底電纜的重要性以及電纜在各個領域都有重要意義。

1. 海底電纜面臨的當前威脅是什麼？

瞭解海底電纜的威脅前，必須先了解過去十年對海底電纜的挑戰和未來針對海底電纜攻擊趨勢。從2008年到2022年，國際海底電纜保護委員會（International Cable Protection Committee）共記錄了2,000多起攻擊事件，皆以海底電纜為攻擊目標，影響了國際通訊。

在臺灣，海底電纜攻擊事件有些對電纜的破壞行為，這些攻擊對國家關鍵基礎設施構成威脅，也對臺灣應對海底電纜攻擊所應對能力提出了挑戰，針對海底電纜的攻擊對國家的經濟和安全的影響是非常大的，因此需要加強政策以及應對攻擊的技術手段、國際間的合作及建立安全措施，以確保海底電纜的穩定運行。

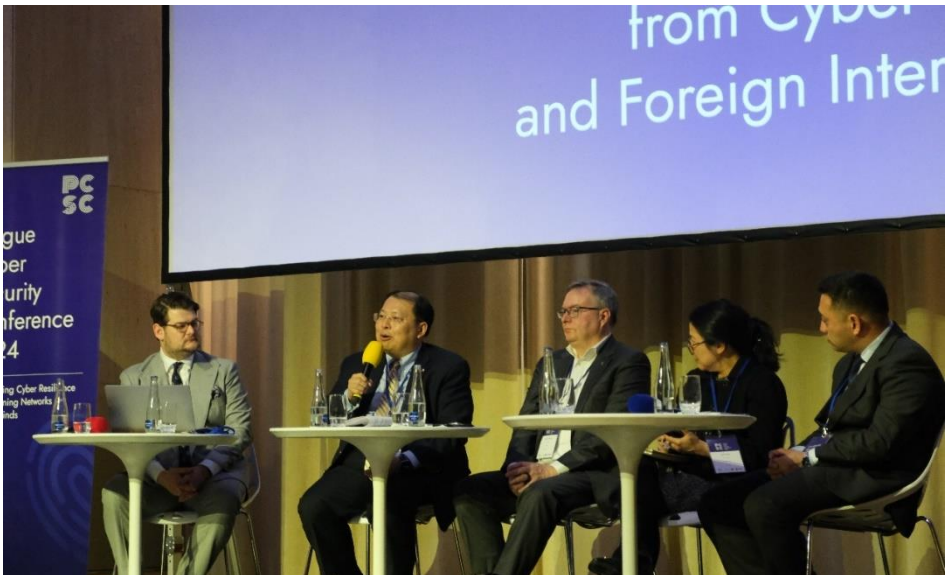

圖 11 分享臺灣海底電纜攻擊事件

目前沒有任何證據表明有具體的方法可以完全阻止海底電纜攻擊威脅，各式攻擊具備高效能及先進的技術能力，所以，從技術角度來看，這是無法避免的，因此國家間分享各式海纜攻擊的情報（包括電力網路和高壓線）顯得至關重要，在本次研討會希望討論國際社會對海底電纜攻擊事件的回應，特別是涉及跨國攻擊的事件，討論解決跨國海纜的攻擊事件，能幫助各國理解海底電纜防護所遇到的問題。

臺灣講者提到，當海底電纜連接到一些偏遠島嶼時，離島地區的通訊安全性變得更加重要，需要更加確保這些島嶼電纜的安全，並在必要時發佈相關訊息。臺灣必須應對很多挑戰，包括國際合作和技術困難，必須採取國際合作和技術創新措施，確保這些電纜的安全性和穩定性、關鍵基礎設施免受各種威脅。

2. 海底電纜位置的重要性

芬蘭講者提到，我們現在所發送的訊息都可以在一到兩個小時內

完成傳遞，傳遞資訊的速度與電纜的傳輸最大數據量具有一定的關聯性，傳輸最大數據取決於電纜的年齡和耐久性，這些因素都屬於可預期範圍內，電纜無論是在海底或是其他地方，通訊系統應該對於各類攻擊應具有足夠的應對能力，電纜是整個通訊系統的一部分，通訊系統需要具備能夠承受損害的能力，並且應該有足夠的容量來應對需求，問題在於，一旦電纜的位置被公開，對那些攻擊者來說，會發生不可避免的攻擊情況，芬蘭講者舉例，例如，去年十月，有一條重要的電纜被損壞，這條電纜深埋在1,600米處，整個通訊系統仍正常運作，但仍然顯示出電纜的重要性，當時的電纜受到了風暴的影響，芬蘭意識到這不是一個普通事件，開始採取行動進行修復及調查，調查期間，愛沙尼亞和芬蘭的海岸防衛隊也積極行動，提供了重要的訊息和協助，芬蘭講者認為這是非常成功的國際合作案例，使芬蘭能夠成功應對當時的危機，並可以在事後進行深入調查，充分展示國際間海底電纜在面對攻擊時的準備和應對能力，展示國際間訊息交流和協調能力。

Ciena 公司講者提到，必要時發布海底電纜位置資訊給相關人員（例如漁民）很重要，讓他們知道海纜位置能預防漁民捕魚時不會意外地把錨拋到海底電纜上，例如，在新加坡，已經清楚地標示出漁民可以投錨的位置，而這在其他地區並沒有做到，這實際上與如何設置標識，同時讓相關人員感到方便，並且能夠輕易清楚記住這些標識，需要更多的長期努力。

NATO 講者指出，關鍵基礎設施的電纜對惡意攻擊者具有吸引力的原因之一，在於它是一個容易評估攻擊的目標。因為電纜的位置和功能通常是公開的，攻擊者可以相對容易地找到和定位它們，使得它們成為潛在的攻擊目標，例如：即使英國的海底電纜圖沒有公開，但關鍵基礎設施的電纜位置在內部可以得到相關資訊，惡意攻擊者知道在哪裡找到這些電纜，他們有能力在波羅的海定位這些電纜，這是一個相對簡單的任務。

NATO 講者認為，根據國際法，海纜地圖不應該被公開，這樣做會引發更多問題。不幸的是，現代國際社會中海底電纜已倒退數百年或數千年，我們需要有一個完善的法律制度，依據現行的國際法律，最近期的國際法規定了海底電纜的處理方法，是《聯合國海洋法公約》，在1982年通過的立法。因此，我們需要繼續改進和完善相關法律。

3. 海底電纜防護的未來

芬蘭講者提到，海底電纜問題的未來，需要討論的不僅僅是法律或基礎設施的問題，也需要考慮到電纜在地面與地方的連接情況，有幾個要注意的地方，首先，當談到技術方面時，電纜有許多保護方式，有硬體保護方式，也有軟體保護方式，保護措施中最重要是即時更新，因此，讓專家能夠及時應對各種可能的問題和風險。這對於任何組織來說都是非常重要的，然而，不幸的是，對於年輕的專家來說，攻擊電纜的技巧會日益複雜，防護工作可能會變得更加困難，因為我們無法完全控制情況，也無法預見它的走向。

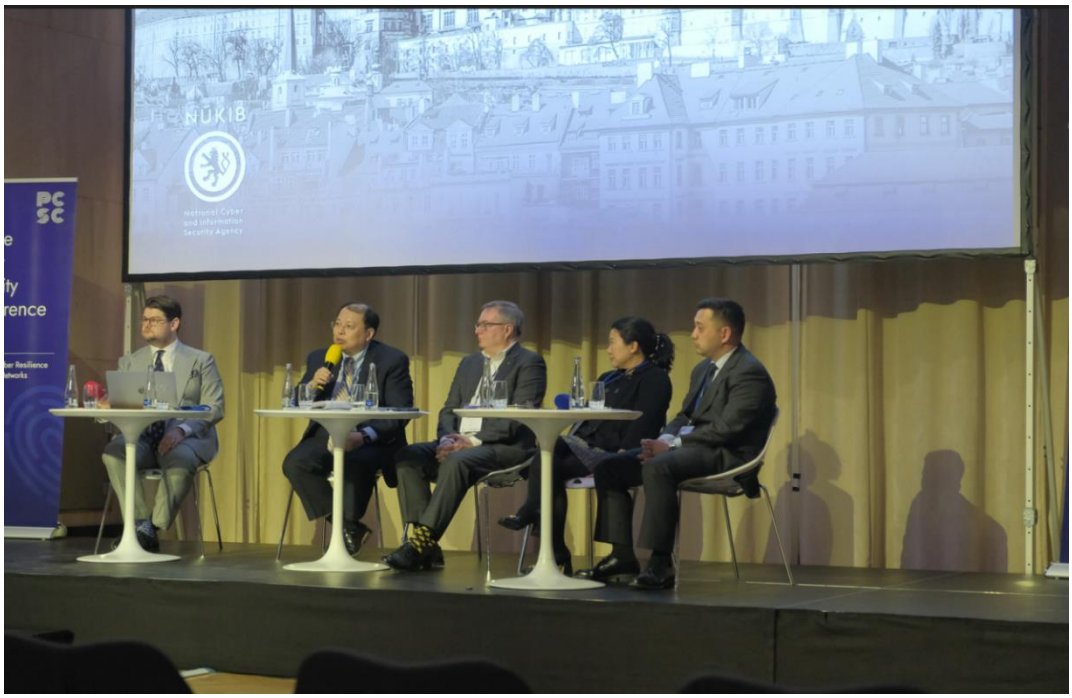

圖12　討論海底電纜防護的未來

海底電纜將數據送至歐洲或其他地方數據中心進行傳送，通過跨

海底纜線進行路由，然而，數據中心設備通常設置於地面，但具體的位置通常不為人所知，某些地方可能會提供數據中心防禦設施之細節描述，包含防禦設施的具體情況及位置，甚至還有技術的圖片，任何人那裡得到攻擊海底纜線的方法，因此，無論是實體或虛擬的數據中心站點都需要被保護，假如從數據中心洩漏海底電纜系統的方法和技術細節是相當危險的。

海底電纜的重要性和保護措施需要各界高度重視，對於某些國家來說，海底電纜是潛在的威脅，並且某些國家已經顯示出他們能夠一再地發現威脅，海底電纜涉及不同層次的挑戰，無論是在海洋還是在陸地上，研究如何保護這些電纜是非常困難的，需要投入大量資源和精力，政府和企業需要合作，採取措施確保關鍵基礎設施的安全，包括注重物理安全和監控系統的每一個細節。

海底電纜是全球互聯網基礎設施的重要組成部分，電纜承載著大量的數據流量，保護海底電纜免受損害或干擾，同時可確保互聯網的穩定運行和數據安全傳輸，此外，預防措施與海底電纜安全性也息息相關，當我們使用這些電纜時，需要確保陸地的基礎建設已經足夠完善，當使用預防設施時，涉及到與其他國家的合作，其中存在許多複雜的問題，我們需要高度警惕。在海底電纜預防設施的做法與其他互聯網保護措施沒有太大不同，但政治層面上的問題尤為重要，尤其是當我們在進行跨國合作時。應加強實體安全和建立自己的監控系統。

Ciena 講者提到，除了海底電纜的防護以外，訊息傳輸也存在一種風險是通訊被劫持，這會導致通訊方向的改變，從而使得訊息可能被引導到意外的地方或被轉移，導致訊息的泄漏或被不正當地使用，無論對於這傳送方或是接收方而言都是危險的，劫持只是從根本上改變了通訊的方向，這只是一個簡單的操作，就能夠掌握這一切，因此我們需要考慮到一點，就是有一些正在建立的網路，它們也可能會被利用，需要去觀察它們，確保它們的安全，在2018年，有一段時間，有

一個事件導致真實的流量被轉移，但不確切知道原因，Ciena 講者認為這不一定是針對這條電纜的攻擊，通常最大的問題幾乎都與電纜本身有關，這是真實的物理問題，它可能並不是因為遭受攻擊而轉移，現在有多種感染形式，我們需要仔細研究並解決它。

海底電纜避免遭受攻擊後無法通訊的窘迫情形發生，技術替代方案為何，現場分享臺灣曾透過即時將訊號傳輸切換成微波及衛星通訊，並盤點不同情境對通訊網路的風險，規劃和落實多元異質的通訊備援網路措施，從海、陸、空多維度強化通訊韌性與資安防護作為；講者們認為國際間在海纜的防護上應該保持相互合作，而不是相互競爭，而關於通訊電纜的問題如何利用新技術建立更好的協調和通訊頻道，以應對突發事件，是各國政府在保或國家的安全和利益時都應該處理的問題，本場討論充分反映各國對海底電纜防護不同觀點和看法。

五、 網路無國界：實現全球夥伴合作關係（No Distance in Cyberspace: Operationalizing Global Cooperation and Partnerships）

（一）主持人：Mike Bareja, Deputy Director of Cyber, Technology and Security, ASPI

（二）與談者：

1. Tomomi Maeda, Deputy Director, Cybersecurity Division, Commerce and Information Policy Bureau, METI, Japan
2. Stefano De Crescenzo, Head of Operations and Situational Awareness at ENISA
3. Eric Goldstein, Executive Assistant Director, U.S. Cybersecurity and Infrastructure Security Agency

（三）重點摘要：

國際合作在處理持續存在的資安漏洞、不斷增加的資安事件和不斷演變的關鍵基礎設施威脅，扮演至關重要的角色，世界各國政府越來越多地在進行跨國合作，主持人開場提到本場討論將聚焦於，如何將各國全球合作的戰略轉化為實際操作，討論的範圍不僅僅是合作協議和原則，而是如何將跨國合作付諸實踐，達到實際效果，把國際間的原則轉化為行動，從「我們應該做什麼」的層次昇華為「我們該如何做」，主持人認為國際合作的重點會放在資訊的共享上，各國如何聯合制裁和打擊網路犯罪，以及像北約和其他聯盟演習在愛沙尼亞塔林所舉辦的演習，建立國際一致性的標準、法規，以及共同努力保持資安治理，資訊共享上是關鍵。

1. 遵守國際標準的困難

日本講者提到，日本經濟部目前有兩個主要願景，首先是保護日本產業免受網路威脅，另一個較新的使命是幫助日本產業提供安全的產品滿足日益增長的市場需求，日本代表認實踐國際安全，「設計即安全」是一個很好的原則，日本正在努力與各方合作將「設計即安全」

付諸實踐，並認為國際標準化是安全的關鍵，在日本目前的優先事項物聯網安全，數據顯示，三分之一的可疑攻擊是針對物聯網設備的。因此，日本目前正在確保工業產品的安全性，打算將其用於未來的政府和關鍵基礎設施，然而國際間存在許多標準，例如，ISO 標準、NIST 標準，國際標準使設計這件事情變得複雜，日本經濟不需要與製造商和這些產品的最終用戶進行了大量討論，這背後需要消耗很高的成本和時間來遵守不同國家的標準。

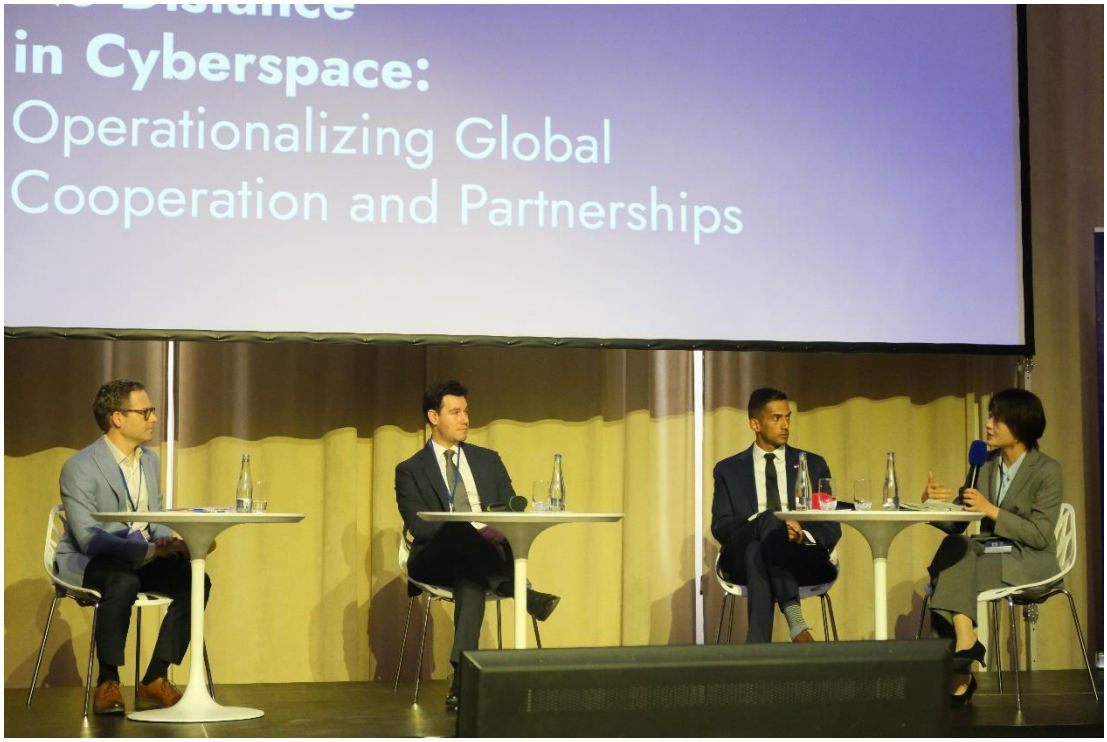

圖13　日本代表討論國際合作的作法

澳洲講者同意「設計即安全」政策確實是網路安全領域的一個重點，在去年八月發布的澳洲網路安全戰略中，也提倡「設計即安全」的計劃，此刻，這項計劃正在與各界進行諮詢，確定如何將其納入立法，這是一個非常困難的領域。有些相對簡單的設備，例如物聯網設備，較容易進行管制，但對於複雜的設備和軟體，幾乎不可能管理，如何設立標準，如何實施這些標準也成為一個問題。

2.　資訊共享在跨國資安聯防的成功案例

美國講者認為要完全理解資安事件及產品的資安漏洞，需要來自

不同角度的視角，有時候，私營部門對資安事件的掌握，甚至比政府部門更廣泛，民間公司在軟硬體、情報都有不同的資安可視性，在各國的狀況皆是如此，因此美國希望在國際舞台上與私部門資訊交流，所採取做法為聯合網路防禦協作機制（Joint Cyber Defense Collaborative，JCDC），試圖吸引民間企業加入計畫，能夠即時共享訊息，並與美國政府共同開展資安聯合防禦行動，美國希望能夠在戰略上將 JCDC 與全球各地的合作夥伴聯繫起來。

美國講者提到資訊交換的方式通常來自於具體資安事件情境，舉個例子，早期的 JCDC 活動中，一些最成功的案例之一是 Log4j 漏洞，這是一個開放源碼的漏洞，漏洞影響了各種產品和服務，JCDC 計畫透過協調民間部門共同開發，成功識別受影響的產品中的版本漏洞，這是一個非常具體的戰術例子，展示了跨國界如何和私部門共享訊息來應對現實世界中的挑戰。

在俄羅斯入侵烏克蘭這樣的事件中。美國藉由國際和民間部門的共享訊息，迅速與歐洲和全球伙伴合作，識別俄羅斯的惡意軟體和入侵行為，顯示出我們如何通過共享訊息來加強全球安全，也藉此突顯國際合作在日益增加的挑戰之重要性和效果。

六、資安人才：建立和保留資安人才是一項共同責任（Cyber Workforce: Building and Retaining Cyber Talent as a Shared Responsibility）

（一）主持人：Liina Areng, Director LAC4, Estonia）

（二）與談者：

1. Christopher Porter, Head of International Security Cooperation, Google
2. 山口勇 Isamu Yamaguchi Counsellor, International Strategy, National Center of Incident readiness and Strategy for Cybersecurity, NISC
3. Ilir Daka, Director of Monitoring and Strategic of National Authority on Electronic, Albania
4. Gert Auväärt, Director of the NCSC-EE, RIA, Estonia

（三）重點摘要：

主持人提到資安防護中所有元素，資安人才是最重要的元素，各國如何解決資安人力短缺的問題，全球估計有4百萬資安專家缺口，不幸的是公私部門皆沒有投入足夠的資源培訓，AI 席捲全世界，人類還能做什麼發揮作用，以及所謂的資安人才需要具備何種能力？皆會在本場次討論。

1. 無論何時都有新資安人才需求，公私部門可以採取哪些措施？可以做些什麼來吸引更多資安人才？

隨著時代的進步，網路攻擊的速度越來越快，每個組織、每家公司都需要專業的資安人員支持他們的服務和營運。但不幸的是，在許多行業、關鍵基礎設施，都沒有足夠的資源投入到資安專家的培養。主持人提問所有與談者：「隨著人工智慧風靡全球，在你們的組織中，現在特別需要哪些特定技能？當你們看到不同行業的特殊性時，你們能否詳細說明哪些行業特別缺乏這些技能？比如學校、醫院、釀酒廠等等。我們如何影響這一情況？」。

在公私部門都在尋找資安人力缺口的同時，儘管每年都有新的學生從大學畢業，但無論何時都有新資安人才需求，政府可以採取

哪些措施？可以做些什麼來吸引更多資安人才？這是一個各國重要的問題。

愛沙尼亞與談者提到，我們唯一可以做的事情是盡早開始，提早接觸大學一年級或二年級的學生，讓他們參與部分資安工作，然後慢慢培養成我們需要的專家。這是唯一的解決方案，愛沙尼亞正在努力實現，在這方面還有很多工作要做，這需要時間和努力，去深入了解威脅並試圖模仿惡意行為者，這些技能是必不可少的，能夠為各公司提供資安服務的人才是非常重要的，需求也是存在的。可以從這裡開始，再規劃下一步該如何進行。

圖14　討論吸引資安人才的作法

Google 與談者提到，舉例來說 Google 或其他公司，即使是雇用了成千上萬名世界頂尖的技術專家，仍始終都在尋找一流的技術人才、努力聘請頂尖的技術人才，即使雇用人才是足夠的，也仍會持續這麼做，特別是在尋找技術人才方面，因為問題是在於網路攻擊者，會試圖解決資通安全防禦的問題，公司必須阻止攻擊者對軍事情報服務用戶、公司或政府進行攻擊，會不斷尋找技術專家。

2.　資安人才所需的技能為何？團隊中所需的人員知能為何？

無法成功防禦資安攻擊的原因並不是全然因為沒有足夠的工程師或類似的原因，而是內部人員需具有正確的溝通技巧及方法、擁

有足夠的技術、知識和理解資安威脅，且需要有與工程師、開發人員、網路分析師和逆向工程師溝通，並且能夠提出正確的問題，並理解技術人員的答案的人才。

但是，對於一個成熟的大公司來說，即使是最好、最安全的公司或國家，總是有相同的問題，不理解資安威脅的重要性，也無法將其傳達給非專家。例如：當在金融業發生銀行資訊系統受到網路攻擊時，資安人員可能會說：「中斷網路，阻止一切攻擊。」，然而，這樣的舉止可能難以說服其他非資安人員，因為他們會考慮到網路攻擊造成的損害與金融損失之間的權衡。這並不是因為他們不理解安全威脅，而是因為雙方不理解彼此工作的業務。

因此要制定有效的資通安全政策，也必須向不熟悉金融業務的資安人員，傳達資本考量的重要性。同時具備熟悉業務及資安重要性實際上是一種較罕見的技能，當人工智慧使用變得更加普及時，我們需要更多有很多具備能同時瞭解資安及業務重要性，並能夠有效說服團隊之溝通人才。

團隊需要優秀的溝通者和良好的團隊合作者，善於與他人合作的，也擁有某種程度的知識基礎，另個具體的例子，當有間製藥公司正在遭受入侵時，稽核單位關注的是資安防禦措施，關注如何詳細描述基礎設施的運作情況等等，包含是否有人竊取訊息或準備進行勒索，是否有製劑被改變，藉此評估藥廠是否需要召回所有藥品並關閉公司，這種狀況下，軟性的溝通技能和將技術操作及熟悉業務的能力對於公司來說是非常重要的，但隨著業務營運變得更加複雜，公司將無法再只是一個需要純技術人才，需要其他溝通技能，而這些技能往往不是當學生上大學好工作時所考慮的。

3. 各國採取哪些措施，試著解決資安人力缺口？有無特別針對女性資安培訓的項目？

（1）愛沙尼亞

愛沙尼亞會著重於基礎技術的發展，現今每個人都在使用手機、平板及電腦這些設備，每天累積基礎技術，也給了孩子們這些技術

設備，並詢問會議中有多少人在給孩子們第一個手機或平板電腦時，教導他們有關資通安全的基本知識，這是愛沙尼亞在學校要做的事情，會跟更年輕的孩子談談資安相關的故事和所需的知識，激發他們的興趣。最近愛沙尼亞正在舉辦的一項活動是為了提高公眾的意識，開始針對目標群體為 13 到 16 歲女孩的舉辦黑客課程，因為女孩在這方面的興趣比男孩少，希望平衡性別不一的情況，有許多孩子想參加活動、想學習，我們過去做錯的一件事部分活動是以競賽形式舉行，但並非所有人都想競爭，愛沙尼亞目前專注的是，如何提高孩子參加資安活動之意願，希望孩子能慢慢學習資安，逐步獲取知識。

愛沙尼亞也教導學校的資安老師，無論是小學還是中學，這些老師在教 IT 基礎方面很有經驗，但在資通安全方面幾乎沒有關注。沒有教授如何資安防護。我們現在與十位老師合作，儘管這是一個小數目，但對愛沙尼亞這個小國來說，十位老師已經是一個群體。我們將繼續這樣的步驟，教導孩子們一些資通安全知識，讓他們對這個領域感興趣，然後當他們決定在大學學習什麼時，這是愛沙尼亞的第一步，謝謝。

（2）阿爾巴尼亞

阿爾巴尼亞針對女性的資安培訓，則是與不同的專業人士合作，目前在亞美尼亞進行對女性資安學員進行短期培訓，是為了讓學員瞭解資通安全的想法對資通安全感興趣；另一項培訓是與合作夥伴合作，在高中辦理資安意識活動，目前沒有在國中進行。

對孩子們進行一些培訓，瞭解基礎資安知識，開始信任資通安全，原本很多原本不想參加的高中生，在參加後有了改變，現在有更多關於資通安全的訊息，青年從思維上跟成年人有所不同，阿爾巴尼亞看到對資通安全感興趣的人越來越多，但現在阿爾巴尼亞國家面臨的問題是，許多大學的課程中並沒有涉及資通安全這一科目，大多數人學的是計算機科學。

阿爾巴尼亞目前正在透過與大學合作辦理短期的培育計畫，未

來將會納入長期五年的新計畫中，目前正在尋找真正的資安專業人才擔任講師，並對於各行各業的專業人才來進行人才培育，並開始與私人部門合作培育人才及講師。阿爾巴尼亞也十分積極地為在職員工提供資安培訓，鼓勵從高中畢業後已經工作了四年之工作者，進入資安領域，希望在職員工接受一到兩年的資安技術培訓計畫，並且安排在地之資安人培訓。

（3）Google

從 Google 講者個人的經驗來看，女性人才在資通安全方面不足的問題。雖然個人經驗僅是小小的樣本，但在 Google 團隊的首席工程師是女性，講者的老闆及大部分的同事都是女性，女性投入資安工作是一個趨勢，對於一家大型成熟的私人組織來說，資安工作性別比例不均的情形不明顯，但女性資安人才不足的問題還是存在。

（4）日本

在日本資安領域中存在許多女性管理者及傑出的領袖，不僅在資通安全專業領域，還包括在議會和政府中都有傑出的女性領袖，製造出女性能夠在議會中參與重大資安決策的環境；至於創新方面，日本人非常擅長硬體製造術開發，因為過去的價值觀，硬件製造技術被高度重視，因此在教育中，軟體創新技術的理念沒有得到充分發展，現在日本正在努力追趕國際社會的腳步，希望未來在軟體創新技術方面面能夠與國際社會競爭。

日本面臨了資安技術人才短缺的挑戰缺的問題，日本在這方面的需求預計達到十萬人，另外對於那些沒有高級學位但具有軟體開發能力的人才需求也在增加。

4. 免費課程資源的重要性

在職業發展上，許多在資通安全方面表現出色的人最初並不是從事明確的資通安全職位，他們一開始可能是工程師的某種類型，或者他們可能在完全不同的領域工作，但在他們職業生涯的某個時候對資安技術產生了興趣，然後轉換到資安領域工作。但由於他們技能的組合或個人態度，讓他們在工作中表現出色。所以 Google 講

者的觀點是，當我們考慮制定資安技術人才職業發展計畫時，要考慮來自各種不同的職業背景的對象，在 Google 公司的經驗中，所有人並非都上完高中，然後進入大學，取得學位，開始資安技術培訓，許多人來自不同行業，帶來了各式各樣的想法以及職涯軌跡，Google 講者認為培訓資安人才比較好的作法是提供公眾免費的資安課程內容，或是提供免費的證書課程認證。

免費或相對低成本的課程與大學訓練課程相比是很好的方案，因為可以吸引在其他領域就職，但對資通安全感興趣之工作者學習，可以在取得認證後開始從事資通安全相關的工作；即便在獲得認證後決定不轉行，所學習到資通安全方面的知識，仍然可以運用於原來的工作中，從公共安全的角度來看，這是一個雙贏的情況。

為了通過吸引不同類型的人才來擴大潛在的資安勞動力。所以，Google 歐洲有各種類似免費課程計畫，還贊助進大學就讀的讀書計畫，我們不會要求保留所有計畫所訓練的人才來為 Google 公司工作，另外特別希望訓練後的人才能夠至小型的初創公司發展，因為這些公司通常尚未建立基礎資通安全設備，方便於初期建立正確的資安觀念。提供免費資安學習資源是一種公共服務，對我們的整體環境是有益的，因為隨著 Google 公司是在歐洲推出針對小型企業計畫，

圖15　主持人分享資安人才培育作法

產生良好的回饋，因此很快就將資金從一千萬歐元擴大到了一千五百萬歐元。Google 講者認為不預設從資安相關科系畢業並非進入資安領域的唯一方式，我們可以建立清晰且非正式的高等教育來完成資安人才的培訓。

5. 培育資安工作所需的基本技能

資安人員須具備最基本的技能之一是打字，許多人並不具備基本的打字能力，只能使用兩指打字，進而影響在執行資安工作的效率，使用十指打字，需要長時間的學習過程才能熟練掌握，這是一個非常基本但又非常重要的問題，假如不具備基本的打字技能，也沒有能力在資安方面進行有效的操作。所以，打字問題是首要被解決的，然後再談其他的技術問題，提升人員基本的打字技能，這是我們需要努力的方向，澳洲的一些公司正在通過遊戲來解決這個問題，比如 Tommy Q Game 這款遊戲就是一個例子，能讓孩子從小累績打字技能。

另一項基本知識是有關如何使用基本的資通安全技術，在目前學校所教授的知識中沒有基本的資通安全技術相關知識，因此建議在基礎教育中，不應該僅是教導孩子們使用電腦，還必須包括教他們如何安全地使用電腦。

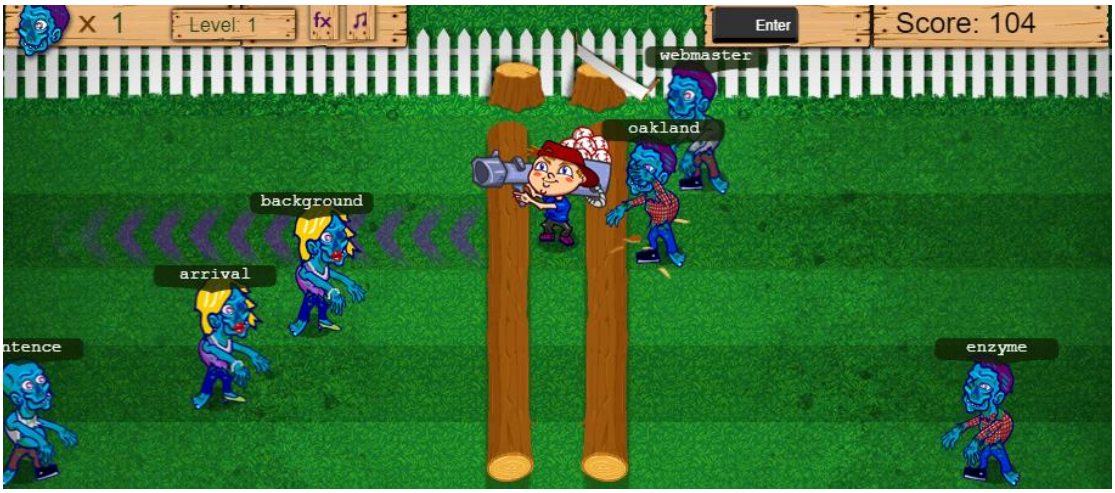

圖16 Tommy Q Game 遊戲畫面

6. 對於普通公民、公司客戶或非資通安全職業的員工，我們如何提高他們的安全意識和能力？

（1） 愛沙尼亞

在愛沙尼亞目前正在嘗試在希望將資安防護基本知識納入大學課程中。比如，對於醫學系的學生，除了醫學課程外，他們還需要修一門資通安全的課程，愛沙尼亞目前正在推動這個計畫，但針對教育界和機構的變革是緩慢的，目前正在努力推動。

此外，愛沙尼亞建立一個基本的資通安全學習平臺，內容不僅僅是關於社交工程之釣魚攻擊的課程，而是涵蓋更多面向，未來計劃將其作為小學的必修課程，讓孩子從小學開始就應該學習資安課程，並獲得相應的認證，也要求成人完成學習這些課程，未來將是公共和私人機構都可以使用的學習資源，並且會有法律上的要求人民學習，讓這些課程更加普及，內容未來更容易理解。

愛沙尼亞所進行大量的教育工作，皆有其必要性，期待下一世代軟體和互聯網的設計將是以安全性為核心，不再將負擔放在用戶手中，更像是維護房屋安全，而不是記住各種複雜的密碼，但仍然需要繼續教育人們，讓他們知道網路威脅是存在的，這些事情可能會發生在他們身上的，所以應該使用安全的資通系統，就像在過去，我們會教育人們在走出家門時，要小心可能有人會搶劫您的財物。我們需要保持這種警覺性，讓人們知道威脅的存在並做好準備。

（2） Google

用戶教育很重要，並且將永遠重要。但是，讓我們回想當初汽車剛普及時，駕駛人需要知道如何自行進行一些維護和保養，駕駛汽車曾經是一件危險的事情，就像極限運動一樣。同樣地，過去買肉也是一件冒險的事情，如果您不知道肉是否安全，那就很危險。當時的政策管理者可能會說，您需要知道如何確保肉類安全，然而，現代社會中，食物和汽車應該都是安全的。

期待是每個人都需要具備一定的技術知識才能使用最先進的技術，這是一種奇怪的期望，教育很重要，但這不是我們未來應該走的方向。人類的本性不會隨著這些技術的變化而改變，騙局和犯罪仍然存在，威脅不會消失。但這應該更像是知道如何安全駕駛汽車

或基本的食品衛生，而不是將所有的負擔放在個人身上，我們應該期待軟件本身是安全的，用戶使用它時也是安全的，異常情況應該是罕見的，但現在它們並不罕見，這是不正常的，我們需要讓軟件製造商和政府共同承擔這些責任，在汽車方面，仍然會有一些問題，比如司機會出事故，但這並不意味著我們應該將所有安全責任放在個人身上。同樣地，我們應該對軟件製造商施加壓力，使其設計出更安全的產品。當我們談到未來的技術時，可能需要像駕駛執照一樣的東西來確保我們能夠應對未來的高級技術威脅，人們應該提高對技術的理解和期望，這樣可以促使開發者提高標準，不必等到事故發生後再去解決問題，而是在事前做好預防。

然而，對資通安全以及網路威脅的認知，世代間是存在差異的，在互聯網時代成長起來的人，後來才接觸到互聯網的人不同；在社交媒體的使用上，不同世代也有不同的風險認知，因此在教育用戶資安相關知識時我們必須考慮到世代間的差異；希望人們生活在一個安全的世界裡，就像去超市購物時，不需要擔心食品中毒一樣。我們不應該期待普通人了解所有的技術細節，設置足夠強的密碼來防止加密破解。

目前很多社交工程及網路釣魚攻擊之所以有效，是因為它們模仿了真實的商業行為，用戶很難區分真假，現今我們將安全責任推給了個人，講者認為這是不可行的，我們應該設計自動安全的軟件，並施加合理的監管來保護隱私，提供更安全的身份驗證方式，資安防護不應該是個人的責任，技術應該自動提供安全設施，人們不應該被要求成為資安專家，這是我們應該共同努力的方向。

7. 如何提高全社會意識和應對能力，在發生資通安全危機時，社會該如何準備並應對這些危機，並利用外部資源來應對這些挑戰？

愛沙尼亞講者認為，一種方法是提高用戶的安全意識，在愛沙尼亞的官方網站上提供「全民網路健康測試」的免費測試，能幫助用戶了解自己的資通安全知識，目前有專門針對公司和組織開發更進階的測試，可以讓用戶了解自己的弱點，並提高他們的資通安全

意識，希望這些測試能夠幫助我們建立一個更安全的網路環境。

然而，政府可以做什麼來保護關鍵基礎設施，公私合作如何在一個國家內運作以保護系統和生活方式，其中一個選項是制定計畫，愛沙尼亞有一個叫做國家網路預備役的計畫，已經實施了兩年。這個預備役系統分為多層級，第一層是專家，隨時準備應對各式對公司、政府組織或其他受網路攻擊的單位，成員包含政府內的 IT 專家和網路專家，他們自願參加，這些人實際上在各種私人公司工作，他們利用業餘時間來幫助社會，這是一種回饋社會的方式。曾經測試了這個系統兩次，一次是與國防部門合作，另一次是與電力供應商合作，模擬國家遭受重大網路攻擊的情景。

透過執行計畫就像是知道火災時警鈴在哪裡，知道在需要的時候可以使用。雖然希望永遠不會用到它，但至少有這個計畫在那裡，不僅需要有計畫，還需要測試這些計畫，以確保它們在實際情況下有效。

在阿爾巴尼亞公共和私部門的合作也是關鍵，民間公司與政府合作，不僅在國內或是國際上，全球的資通安全都有幫助。分享威脅情報和技術知識對於防禦是至關重要的。這樣的合作使得我們可以共同應對大規模的攻擊，因為攻擊者通常不會只針對一個目標；在日本，知識往往集中在大型企業中，因此，我們需要促進企業與政府之間的合作，以及國際間的合作，來加強資通安全。

在過去十年中，Google 培訓項目在愛沙尼亞和新成立的公司中取得了很大的進展和成功。這些項目是用來測試並提高資通安全意識的，其中一個例子是愛沙尼亞邊境附近的一個小鎮，叫做 Narva-Jõesuu，這是一個完全跳出傳統培訓框架的學校。在這裡，學員需要學習18個月，唯一的入學要求是通過邏輯測試，不需要任何其他的學歷證書，可以在這裡學會編碼並成為一名資通安全專家，畢業後可以為公司提供服務，這是一種不同尋常但非常有效的方式，展示了如何通過傳統教育體系的思維來提升能力。

在國際合作方面，參與跨國演練非常重要，在許多其他國家的

經驗，例如：歐盟組織的各種演練，這些演習不僅僅是讓私人公司參與，還包括政府部門，政府人員在這些演習中展示他們的知識，並與民間部門的專家進行合作，對於建立公私部門以及國際間信任和提升整體資通安全水平非常有幫助，透過跨國界合作，讓資安演習不僅僅局限於一個國家內部。更好地利用資源，並創造一個更大規模的創新環境，這樣可以更好地吸引和培養頂尖人才，並在全球範圍內提升資通安全水平。

肆、心得與建議事項

一、建立替代的通訊頻道，以應對海底電纜斷線等突發事件

目前沒有具體的方法可以完全阻止針對海底電纜攻擊威脅，各式攻擊具備高效能及先進的技術能力，我國經常遭遇連接離島的互聯網電纜經常被切斷風險，造成離島全面斷訊，然而，從技術角度來看，針對海底電纜的攻擊是無法避免的，因此建置替代的通訊頻道顯得至關重要，我國已積極布建備用衛星網路，規劃和落實多元的通訊備援網路措施，與本次大會分享經驗，並受各國認可。

二、加強海底電纜的國際合作分享國際間的攻擊案例

海底電纜承載著超過95%的國際數據流量，支撐著從金融交易到軍事行動的一切，對海底電纜攻擊技術多變，為確保電纜的安全性和穩定性、基礎設施免受各種威脅，國際間在海纜的防護上應該保持相互合作，是各國政府在保或國家的安全和利益時都應該處理的問題，海底電纜的安全和保護應該由各國政府、國際組織以及相關行業共同合作來確保的，資安大會提到可經由七大工業國組織（Group of Seven）建設海底通訊電纜網路，為發展中國家和新興國家提供資料傳輸服務， 加強發展中國家電信基礎設施建設。

對海底電纜進行破壞活動、針對基礎設施的犯罪活動以通過篡改電纜資料傳輸的方向或是挾持訊息，各式攻擊發生的可能性越來越關注，因此國家間分享各式海纜攻擊的情報，將無法避免的海纜攻擊所產生的傷害降到最低。

三、培育具備跨領域溝通之人才及提升資安人員溝通能力

談及資安人才的短缺，往往會著重在策略面、管理面及技術面三個面向的專業能力發展，在本次資安大會裡開始注重資安人員的溝通能力，在公私部門中皆需要優秀的溝通者，同時具備某種程度技術知識基礎以及熟悉業務，資安防護技術知識固然重要，但需要依據遭受攻擊的真實狀況來權衡該實施何種控制措施來降低損害，因此需要培育資安人員溝通能力或是訓練具備資安及業務基礎知識之跨領域人才，公、私部門無法只是一個需要純技術人才，需要其他溝通技能，而這些技能往往不是在傳統教育中

所要求的。

目前公部門的資安培訓當中，也將積極培育資安人員的溝通能力及團隊合作的精神，將透過各式情境及團隊合作的設計，加強資安人員與業務單位非資訊背景的人員溝通，以及跨單位資安人員彼此間的溝通，加強公部門間資安聯防的能力，避免發生攻擊時無法正確且迅速地傳遞訊息，並能夠在業務執行以及資安防護控制措施，透過與業務人員溝通找出權衡點。

面對網路威脅，理解人類行為是非常重要的，這不僅僅是技術問題，未來可考慮加入技術以外的基礎能力項目，包括良好的溝通技能，基礎能力會隨著時間變化，並提早幫助學生想像未來的職業規劃，更好地適應未來的挑戰。

四、 增強建立資安工作與生活平衡之職場

面對資安人員的短缺，資安人員留才跟攬才都非常重要，本次資安大會討論到各國資安人才如何從小建立資安意識，減少資安人員的兩性差距，同時各個講者也提到擁有良好的工作生活平衡職場對所有職員都有好處，實現良好的工作生活平衡，能有效提升女性願意繼續在資安領域中工作，建立資安意識的部分我國已透過「GiCS 尋找資安女婕思」，從教育年輕女學生對資安正確觀念著手，鼓勵女性投入資安科技領域。

針對資安人才留才的部分，建議未來可多思考如何在組織制定公平、包容的政策，建立友善職場，能夠包容不同生活方式的工作環境，在留住資安人才，是除了提高薪資及補助以外可以考慮的方向，也能成為吸引女性投入資安相關領域的誘因。

五、 積極參與資安跨國演練，提升國內資安人才技術量能

本次大會提到提高資安韌性，資安人才扮演中大角色，根據某些公司的研究數據發現，大多數針對性的攻擊都是國際性的，因此提升資安韌性不單純是各國國內應討論的話題，而是國際間的合作問題，為了提升資安韌性，我們需要與其他主要國家合作與協調，所做的資安防護行動也應該是全球彼此互項合作的。

在資安人才實戰演練上，國際合作參與跨國演練非常重要，在演練過程中可以學習許多其他國家的經驗，例如：歐盟組織的各種演習，讓成員

國的公、私部門人員在這些演習中展示他們的知識，達到公私協力及國家間的協力，讓資安演習不僅僅局限於一個國家內部。而是創造一個更大規模的演練場域，能更好地培養頂尖人才，並提升全球資安水平。

本次大會認為需要跳出國家與國家間的競爭關係，透過跨國界合作，資通安全是國際間共享責任，基於信任和國際合作，我們需要超越自己的組織和國家，並支持那些沒有資源進行培訓或應對威脅的國家，才能共同提升全球的資通安全水平，才能更好地應對未來的資通安全挑戰。

六、 提供學習成本較低之資安培訓資源，增加不同背景人員接觸資安專業知識的機會。

在本次大會講者的經驗中，成為資安人才人員的背景，許多是來自不同的背景透過各式方式學習及經驗累積而成為資安人才，而 Google 公司也意識到這點並積極推出 Google 資通安全證書（Google Cybersecurity Course），並通過補助的方式讓沒有相關背景的人也能低成本接觸到資安知識，取得認證後可從事資安相關工作，建議我國在職業訓練或是資安人員相關訓練上能與學界或是私部門就現實生活中所遭遇到資安問題及所需之技能，共同合作研發線上學習資源，並提供學習後投入資安工作之學員補助，提升不同背景的人員學習資安專業知識的誘因。

伍、參加布拉格資安大會之額外效益

2024年布拉格資安大會邀請全球各地資通安全專家學者，本次訪團藉由場邊會議交流時間邀請各國專家參加數位發展部舉辦之2024年「前瞻資安探索會議」（Advanced Cybersecurity Exploration Conference, ACE），成功建立與捷克駐澳洲大使館的印太網安協調官、日本內閣網路安全中心（National Center of Incident readiness and Strategy for Cybersecurity, NISC）及新加坡網路安全局（Cyber Security Agency of Singapore, CSA）人員互動，相互提供跨國資安聯防資訊，並邀請捷克、日本及新加坡資安專家學者與我國分享及交流資安防護經驗，深化與各國資安防護之友好關係。

附錄－2024布拉格資安大會議程

19 March, Main Hall

8:00 - 9:00 | Registration and Welcome Coffee

9:00 - 9:30 | Opening Ceremony

- **Petr Pavel**, President of the Czech Republic (pre-recorded speech)
- **Věra Jourová**, Vice President of the European Commission for Values and Transparency (pre- recorded speech)
- **Anne Neuberger**, United States Deputy National Security Advisor for Cyber and Emerging Technologies, United States National Security Council (pre- recorded speech)
- **Chad Woolf**, Vice President for Security Assurance, Amazon Web Services
- **Lukáš Kintr**, Director, NÚKIB

9:30 - 10:30 | Five Years Since the Prague Proposals on 5G: ICT Supply Chain Security Beyond Telecommunications

- **Katharine Brooks**, Global Cybersecurity Policy, Aspen Digital, *the moderator*
- **Pavel Štěpáník**, Deputy Director, Strategic Affairs and Engagement Division, NÚKIB
- **Brendan Dowling**, Ambassador for Cyber Affairs and Critical Technology, Australian Department of Foreign Affairs and Trade
- **Isamu Yamaguchi**, Cabinet Counsellor, Japanese National Cybersecurity Center
- **Dan Cimpean**, Director of Romanian National Cyber Security Directorate
- **Jennifer Bachus**, Principal Deputy Assistant Secretary, Bureau of Cyberspace and Digital Policy, U.S. Department of State

11:00 - 12:30 | Countering Cyber Aggression & Building Resilience

- **David van Weel**, Assistant Secretary General for Emerging Security Challenges, NATO, *the keynote*
- **Steen Simonsen**, Principal Strategic Security Consultant, Mandiant (part of Google Cloud), *the moderator*
- **Ory Schein**, Executive Director for Intelligence & Threat Assessment, INCD, Israel
- **Ilir Daka**, Head of the Operational Center and Red Team, National Authority on Electronic Certification and Cyber Security, Albania
- **Inga Žukauskienė**, Director of Regional Cyber Defence Centre, NCSC, Lithuania

12:30 - 13:30 | Lunch Break

13:30 - 15:00 | Ensuring Safe and Secure AI: Do We Need Principles, Guardrails or Regulation?

- **Evi Fuelle**, Director, Global Policy, Credo AI, *the moderator*
- **Nicole Foster,** Director of Global AI/ML & Canada Public Policy, Amazon Web Services
- **Priscilla Delgado Argeris**, Chief Counsel, U.S. Federal Communications Commission
- **Daniel Všetečka**, Director of Digital Economy Department, Ministry of Industry and Trade, Czech Republic

15:30 - 17:00 | Under Water: Protecting Subsea Cables from Cyber Threats and Foreign Interference

- **Daniel Bagge**, Senior Intelligence Specialist, Strider, *the moderator*
- **Jaakko Wallenius**, Vice President, Chief Security Officer, ELISA
- **Jack Shis**, Head of Strategy Branch, NATO CCDCOE
- **Grace Koh**, Vice President, Government Affairs, Ciena
- **Herming Chiueh**, Deputy Minister, Ministry for Digital, Taiwan

20 March, Main Hall

8:30 - 9:00 | Welcome Coffee

9:00 – 10:00 | No Distance in Cyberspace: Operationalizing Global Cooperation and Partnerships

- **Mike Bareja**, Deputy Director of Cyber, Technology and Security, ASPI, *the moderator*
- **Yukako Kaneda**, Director for International Affairs, Cybersecurity Division, Commerce and Information Policy Bureau, METI, Japan
- **Stefano De Crescenzo**, Head of Operations and Situational Awareness at ENISA
- **Eric Goldstein**, Executive Assistant Director, U.S. Cybersecurity and Infrastructure Security Agency

10:00 – 11:30 | Same Goal, Different Approaches: Harmonizing Incident Reporting for Critical Infrastructure

- **Věra Mikušová**, CSIRT Representative, CZ.NIC, *the moderator*
- **Lorena Boix Alonso**, Director for Digital Society, Trust and Cybersecurity, DG CONNECT, European Commission
- **Iranga Kahangama**, Assistant Secretary for Cyber, Infrastructure, Risk, and Resilience, U.S. Department of Homeland Security
- **Alice Bonne Reeh**, Deputy Head of Cyber, Danish Ministry of Defence
- **Carlos Leonardo**, Director of the National CSIRT, Dominican Republic
- **Miguel De Bruycker**, Director General, Centre for Cyber Security Belgium

11:30 – 12:30 | Lunch Break

12:30 – 14:00 | Cyber Workforce: Building and Retaining Cyber Talent as a Shared Responsibility

- **Ivan Bartoš**, Deputy Prime Minister for Digitisation and Minister of Regional, *the keynote*
- **Liina Areng**, EU CyberNet Project Director, *the moderator*
- **Christopher Porter**, Head of International Security Cooperation, Google
- **Jarle Eek**, Regional Director Mainland Europe, RiskRecon, Mastercard Company
- **Albert Antwi-Boasiako**, Director of Cyber Security Authority, Ghana
- **Gert Auväärt**, Director of the National Cyber Security Centre, Estonia (NCSC-EE)

14:30 – 16:00 | Disrupting Ransomware Ecosystem Together

- **Allan Liska**, Recorded Future, *the moderator*
- **Phua Puay Li**, Senior Director, Policy and Corporate Development, Cyber Security Agency, Singapore
- **Enrique Hernandez**, Head of Cybercrime Operations, Interpol
- **Břetislav Brejcha**, Director at National Headquarters Against Terrorism, Extremism and Cybercrime, Czech Republic
- **Jakub Souček**, Researcher, ESET
- **Terry Rice**, Vice President, CISO of Merck and MSD

16:00 – 16:30 | Closing Remarks