出國報告（出國類別：開會）

2024年辦理歐銀年度工作會議暨數位產業交流及參與荷蘭 ONE Conference 展會

服務機關：數位發展部數位產業署

姓名職稱：莊裕智 副組長

黃星富 科長

派赴國家/地區：荷蘭(海牙)、英國(倫敦)

出國期間：113 年 9 月 28 日至 113 年 10 月 6 日

報告日期：113 年 11 月 25 日

目錄

表目錄

圖目錄

壹、 前言（出國目的）

本次出國訪查係為維持與歐洲復興開發銀行（下稱歐銀）合作關係、並協助我國資安產業國際拓展，規劃前往歐銀總部、與對臺灣互動友善之荷蘭等地，一則參與當地主要數位轉型(DTX)、資安展會，二則拜會 Innovate UK、HSD 等機構與聚落，交流雙邊實務經驗及討論未來合作可能性。另此行也將率資安業者至荷蘭海牙，為其辦理商機拓展及在地資源媒合交流會，推廣臺灣資安品牌、帶動海外商機形成。針對資安商機擴展與歐銀、英國洽談合作之標的說明如下：

一、資安商機

近年，臺灣與荷蘭在資安領域展開多次深入交流，雙方在資安技術、政策研討及國際合作方面的互動日益密切。荷蘭作為歐洲資安生態系的重要一員，不僅擁有發達的資安產業，在政策上積極推動資訊安全的全球合作，這使臺荷之間的資安交流更具戰略意義。過去幾年，雙方透過技術論壇、商業媒合及政策對話，逐步建立起多層次的合作框架。臺灣的資安產業在全球擁有領先的技術優勢，而荷蘭的資安生態系則提供豐富的市場及技術合作機會，兩國的合作已逐漸深化。本次荷蘭訪團，正是為了進一步促進雙邊在資安領域的實質合作，並強化臺灣在歐洲市場的影響力。

此次荷蘭出訪的主要目的及任務包括官方拜會、國際主要資安活動參與、國際商機及資源媒合等面向。荷蘭作為歐洲資安重鎮之一，擁有完善的資安生態系，尤其是海牙市在全球資安界具有舉足輕重的地位。此次訪團旨在透過參加荷蘭的資安活動及高階會議，進一步強化臺灣與荷蘭企業、研究機構及政府單位的合作基礎以提升臺灣在國際資安領域的影響力，也將幫助臺灣資安業者與荷蘭的企業接洽合作。

二、英國與歐銀合作

為強化臺灣數位產業與歐銀的合作方式，本次與歐洲復興開發銀行

（EBRD）舉行了本年度第二次工作會議。此次會議延續 113 年 3 月份的工作會議討論內容，重點針對前次會議的進展進行說明與更新，並請歐銀就「數位成熟度評估方法」的推動模式、數位轉型顧問計畫的合作機會、以及歐銀的綠色城市計畫等議題說明並進行討論。會議重點在於探討臺灣企業如何具體參與這些數位轉型項目，並深入挖掘未來的合作機會，以促進雙方在相關領域的長期合作。

本次訪英行程亦參觀「Digital Transformation EXPO (DTX London)」展會及「2024 Frameless London Immersive Art Experience（Frameless Immersive）」展館，並拜訪與數位轉型相關的英方重要機構，包括英國創新局（Innovate UK）與 Connected Places Catapult（CPC）等。預計達成與歐銀洽談數位科技試點計畫合作機會，及臺灣企業與歐銀受援國的政府或企業建立顧問諮詢關係，以能協助臺灣企業爭取未來歐銀受援國之技術交流合作及參與專案計畫機會。

貳、行程表

本次荷蘭與英國參訪行程自 2024 年 9 月 28 日至 2024 年 10 月 6 日合計 9 日，行程安排如下表：

日期	地點	主要任務
9月28日 (六)	臺北、荷蘭	1. 啟程BR075 08:20起飛TW (TPE)/桃園機場搭機 2. 19:35 抵達荷蘭/阿姆斯特丹(AMS)
9月29日 (日)	荷蘭/海牙	1. 會議準備 2. 與團隊討論任務分工安排
9月30日 (一)	荷蘭/海牙	1. 參加International Kick-Off Cybersecurity Week 2. 荷蘭台商會晚宴活動
10月1日 (二)	荷蘭/海牙	1. 參加ONE Conference 2024研討會 2. 拜會海牙資安長 3. 參加International Business Event
10月2日 (三)	荷蘭/阿姆斯特丹	1. 考察Cyber Security & Cloud Expo Europe 2024 2. 搭機前往英國倫敦
10月3日 (四)	英國/倫敦	1. 參加2024 DTX Expo London 2. 拜會Innovate UK及Connected Places
10月4日 (五)	英國/倫敦	1. 辦理與歐銀工作會議 2. 參觀FRAMELESS Immersive Art Experience展館
10月5日 (六)	英國/倫敦	1. 資料整理 2. 回程：搭機返臺 CI 82 21:10
10月6日 (日)	桃園國際機場	回程：17:40抵達桃園國際機場(TPE)

參、團員名單

一、 數位發展部數位產業署

項次	單位名稱	姓名	職稱
1	數位產業署	莊裕智	副組長(團長)
2	數位產業署	黃星富	科長

二、 其他隨團成員

項次	單位名稱	姓名	職稱
1	資訊工業策進會	汪金城	組長
2	數位轉型研究院國際合作中心	蔡美青	副主任
3	數位轉型研究院國際合作中心	吳俐蒨	副分析師
4	工研院	卓傳育	組長
5	工研院	何貞儀	專案經理
6	工研院	羅翊萍	副經理
7	幻雲資訊(股)公司	邱德水	行銷副總
8	振生半導體(股)公司	李鳳凰	營運經理
9	池安量子資安(股)公司	朱庭葦	國際業務代表
10	池安量子資安(股)公司	池明洋	執行長/創辦人
11	來毅數位科技	林欣怡	聯合創辦人暨總經理
12	來毅數位科技	張嘉顯	首席技術長
13	臺灣圖靈鏈(股)公司	陳禹安	國際業務代表

肆、 工作內容

本次詳細行程之工作內容如下：

一、9 月 30 日(一) 整日 參與 International Kick-Off Cybersecurity Week

(一) 會議資訊

1. 地點：Security Delta(HSD)
2. 主辦單位：Municipality of The Hague, InnovationQuarter, Security Delta (HSD)

(二) 活動背景

本活動為 2024 海牙資安週的開場活動，除了荷蘭當地資訊安全的代表，現場還有多國代表團前來參與（包含臺灣、西班牙、瑞典等），由 HSD 介紹在荷蘭的資安商業經營模式，以及辦理與國際廠商快速交流活動，以促進參與者彼此資安技術、資訊交流、及商業合作機會。

(三) 行程活動摘要

1. 荷蘭資訊安全推動概況

荷蘭以其高度發展的經濟和創新環境條件，成為國際商業活動的重要中心。這裡擁有世界級的基礎設施，便捷的交通和物流網路，並以開放且具包容性的商業氛圍吸引了全球企業。荷蘭政府積極支持創新科技產業，特別是在資訊安全領域，已成為歐洲的領導者之一。荷蘭的資訊安全產業為企業提供全面的解決方案，涵蓋網路防禦、資料保護及威脅偵測等領域，並在國際間享有高度聲譽，成為全球資訊安全領域的先驅。

荷蘭為建立了完善的資訊安全生態系統，結合政府、企業和學術界的力量，於海牙設立「安全三角洲」(Security Delta, HSD)，亦為歐洲最大的資訊安全群集之一，匯集了各種資源和人才，致力於研究、發展和應用尖端的資訊安全技術。

圖 1 荷蘭商業活動與荷蘭資訊安全概況介紹

資料來源：2024 International Kick-Off Cybersecurity Week 會議

HSD 致力於促進國家與國際間的安全合作與創新。做為歐洲最大的安全生態系統之一，HSD 匯集了超過 300 家合作夥伴，涵蓋政府機構、學術單位、企業和非營利組織，共同致力於資訊安全、法治科技及智慧城市等領域的研究與發展。

HSD 提供了一個專業的協作平台，促進知識分享、商業連結和技術創新，並透過各種活動、研討會和培訓計畫，推動資訊安全領域的最新趨勢和技術應用。作為荷蘭安全產業的核心，HSD 不僅為合作夥伴創造商業機會，還積極推動國際合作，確保荷蘭在全球資訊安全領域保持領先地位，為應對未來的安全挑戰提供解決方案。

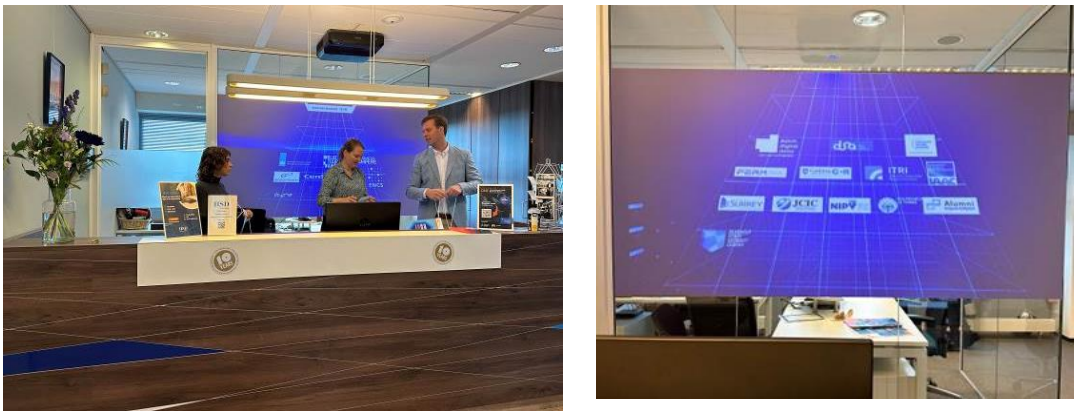


圖 2 Security Delta(HSD)會議現場

資料來源：2024 International Kick-Off Cybersecurity Week 會議

2. 立桌交流活動(Speed Dating)

立桌交流是鼓勵與會人員在短時間內與來自各地的參與者進行交流，來達到快速媒合產業的一種方式，本次立桌交流現場共有 20 桌，每桌 5~6 人，交流方式一共 5 輪，每輪 20 分鐘，每桌將有主持人引導發言與交流。

圖 3 立桌交流活動

資料來源：2024 International Kick-Off Cybersecurity Week 會議

3. 交流活動暨分組討論重點摘要

(1) Living Lab Scheveningen(Smart City)

HSD 在智慧城市(Smart City)領域積極推動多項創新項目，致力於將先進的科技應用於城市管理和公共安全，創造更智慧且更安全的城市環境。以下是一些 HSD 在智慧城市方面的案例：

- 智慧交通管理：HSD 與合作夥伴共同開發智慧交通系統，利用物聯網(IoT)和人工智慧(AI)技術，實時監控交通流量，優化交通信號，提高城市道路的通行效率，減少擁堵並提升道路安全。
- 公共安全監控：HSD 支援利用影像分析和感測技術，建立智慧監控系統，協助城市監控公共場所的安全狀況，及時偵測異常活動或威脅，並迅速採取應對措施，有效提升城市的公共安全水平。
- 智慧能源管理：HSD 參與推動智慧電網技術，透過資料分析和能源監控，實現城市能源的高效管理和分配，減少能源浪費，促進可持續發展。

這些案例展現了 HSD 在智慧城市領域的創新應用，成功地將資訊安全、資料分析和物聯網技術融入城市基礎設施，打造更安全、便捷和可持續的城市生活。

圖 4 Living Lab Scheveningen 分組討論

資料來源：2024 International Kick-Off Cybersecurity Week 會議

(2) HackShield

HackShield 是一款針對 8 至 12 歲兒童設計的資訊安全教育遊戲，旨在提升年輕一代的資訊安全意識和技能，培養未來的「網路英雄」(Cyber Heros)。透過遊戲化的學習方式，HackShield 讓兒童了解網路威脅、防範技巧以及負責任的網路行為，從而在早期建立對資訊安全的基本認識。遊戲內容涵蓋釣魚詐騙、密碼保護、隱私設定和網路禮儀等主題，並以互動任務、挑戰和故事情節引導孩子學習。

除了為兒童提供教育，HackShield 還鼓勵家庭和學校參與其中，創造一個全面的學習環境。該項目得到了荷蘭政府和資訊安全機構的支持，並與多個城市和企業合作，致力於將資訊安全知識普及到更多年輕人。HackShield 是一個創新的教育工具，不僅在遊戲中培養孩子的資安意識，還在現實中建立對網路世界的保護能力。

圖 5 HackShield 分組討論

資料來源：2024 International Kick-Off Cybersecurity Week 會議

(四) 小結

荷蘭的資安產業環境完善，政府、企業及學術機構之間緊密合作，尤其是海牙的 Security Delta (HSD)，作為歐洲最大的資安生態系統之一，提供了廣泛的合作機會。而臺灣的資安產業擁有世界級的技術創新能力，尤其是在物聯網安全、智慧城市與人工智慧應用領域，與荷蘭的技術需求高度契合。

在智慧城市方面，荷蘭積極推動智慧交通管理、公共安全監控及能源管理等創新項目，而臺灣的物聯網及 AI 技術可以有效支援這些智慧城市的發展。此外，針對兒童的資訊安全教育遊戲 HackShield 展示了荷蘭在推動全民資安教育方面的創新做法，臺灣可以考慮與此類教育專案合作，推廣資安教育至更多年齡層，進一步提升全民的資安意識。

二、10 月 1 日(二)參加 ONE Conference 研討會

(一) 研討會資訊

1. 地點：World Forum
2. 主辦單位：Municipality of The Hague, National Cyber Secuity Centre (NCSC), Ministry of Economics Affairs
3. 10 月 1 日各論壇議程：

	Main Stage KWA	Technical Amazon	Governance Yangtze	Law Enforcement Mississippi	Research Ariane	Lightning Talks Africa
09:00	09:00 - 09:25 KWA **Opening day 1** Michiel Boots, Saskia Bruines, Irene Rompa					
09:25	09:25 - 10:15 KWA **Digital Sovereignty Is Impossible Without Big Tech** Hans de Vries, Lokke Moerel, Freddy Dezeure, Jack Cable, Marty Smit, Andreas Rohr, Matthijs van Amelsfort, Bart Asnot					
10:15	Coffee break					
10:45	KWA **Bridging the talent gap** Lucinda Sterk, Anna Chung, Ariela Lopez, Noortje Henrichs	Amazon **Phishing for Tenants: From Simulation to Tenant Takeover** Vaisha Bernard	Yangtze **A Bridge to Secure by Design for OT** Matthew Rogers	Mississippi **Operation Endgame: case study for a broad approach in combating cybercrime** Fieke Miedema, Daan de Graaf	Ariane **The Future of Cyber Volunteering Across the Atlantic** Sarah Powazek, Stéphane Duguin, Matthew Grote, Max Smeets	
11:35	10 min break					
11:45	11:45 - 12:10 KWA **Unlocking Potential: Neurodiversity in Cyber Security** Jessica van der Ploeg, Sandra van de Bunt	11:45 - 12:10 Amazon **From DDosia with love** Talha Ucar	11:45 - 12:10 Yangtze **How do we communicate product security?** Sarah Fluchs	11:45 - 12:35 Mississippi **Panel discussion: A Comprehensive Approach is Crucial in Order to Effectively Fight Cybercrime** Koen Hermans, Dave Maasland, Caroline Sander, Esther Baars	11:45 - 12:10 Ariane **SOARCA: open-source SOAR for CACAO playbook automation** Jan-Paul Konijn, Maarten de Kruijf	
12:10	12:10 - 12:35 KWA **The history, future and importance of Dutch Hacker Camps** Nancy Beers	12:10 - 12:35 Amazon **Vulnerabilities: How to Patch When There is No Patch?** Jan Heijdra	12:10 - 12:35 Yangtze **ENSOC: Strengthening EU Cybersecurity Through Cross-Border Collaboration** Paul van den Berg, Javier R.		12:10 - 12:35 Ariane **Standardized Incident Reporting for a Stronger Community** Desiree Beck	
12:35	Networking lunch					12:35 - 13:35 Africa **Lightning talks day 1**
13:35	13:35 - 14:25 KWA **NIS2 Directive: the renewed cyber landscape of The Netherlands** Moshgan Wahedi	13:35 - 14:00 Amazon **Turning backups into gold: Backup Alchemy for OT** Stefan de Reuver, Earth Grob	13:35 - 14:25 Yangtze **Innovating Cybersecurity Education and Ethical Hacking** Astrid Oosenbrug, Barry van Kampen, Emily Jacometti	13:35 - 14:00 Mississippi **10 years of unique collaboration on (cyber)crime: The Joint cyber action Taskforce (J-CAT)** Ben Hitchcock, Marijn Schuurbiers, Bob Klaver	13:35 - 14:25 Ariane **Secure software: new guidelines beyond technology** Els De Busser, Olga Gadyatskaya, Cristina Del Real	
14:00		14:00 - 14:25 Amazon **Attacking OT Without Specialized Knowledge: a New Threat** Stash Kempinski		14:00 - 14:25 Mississippi **Tracking Transparency: Accurate labels in crypto tracing** Kelvin Lubbertsen, Rolf van Wegberg		
14:25	10 min break					

圖 6 ONE Conference 研討會 10 月 1 日論壇議程

資料來源：2024 ONE Conference 會議

(二) 研討會背景說明

ONE Conference 研討會自 2013 年開辦，其前身為 Govcert symposium，最早於 2002 年舉辦，隨著時間推移，ONE Conference 的影響力和重要性日益增長，荷蘭國家政府也在其中發揮了領導作用。

ONE Conference 為期兩天，包括全體會議，以及可選的分組會議和快速演講(lightning talks)。議程分為執法(Law Enforcement)、研究(Research)、治理(Governance)、技術(Technical)以及主舞台(Main Stage)等五個主軸。今年特別強調幾個重點主題，包含 OT(Operational Technology)安全、人才、地緣政治以及荷蘭的資訊安全。

除了促進知識與最佳實務的交流之外，ONE Conference 還提供網路應用程式，讓與會者或在休息時間和交流時間進行互動，

來擴展自己的人脈。會場還設有展示區，參展的組織展示它們在資訊安全領域的工作成果。此外，ONE Talent Hub 提供平台，讓參與的資安人才了解資訊安全領域的各種機會，同時也讓組織和公司能夠接觸並發掘人才。

(三) 研討會參與重點摘要

1. 展攤交流-Quantum Gateway Foundation

Quantum Gateway Foundation 專注於幫助企業和政府機構應對量子計算威脅，這些威脅可能破壞現有的加密協議。該基金會提供三大主要服務：第一是 Quantum Shield，一種加密檢測工具，為資安專家提供當前加密環境的量化分析；第二是量子安全測試平台，讓組織能夠模擬和比較不同加密協議；第三是 Quantum Path，一個專利申請中的量子安全通訊隧道技術，能夠在不影響現有應用程式的情況下創建量子安全的通訊通道。

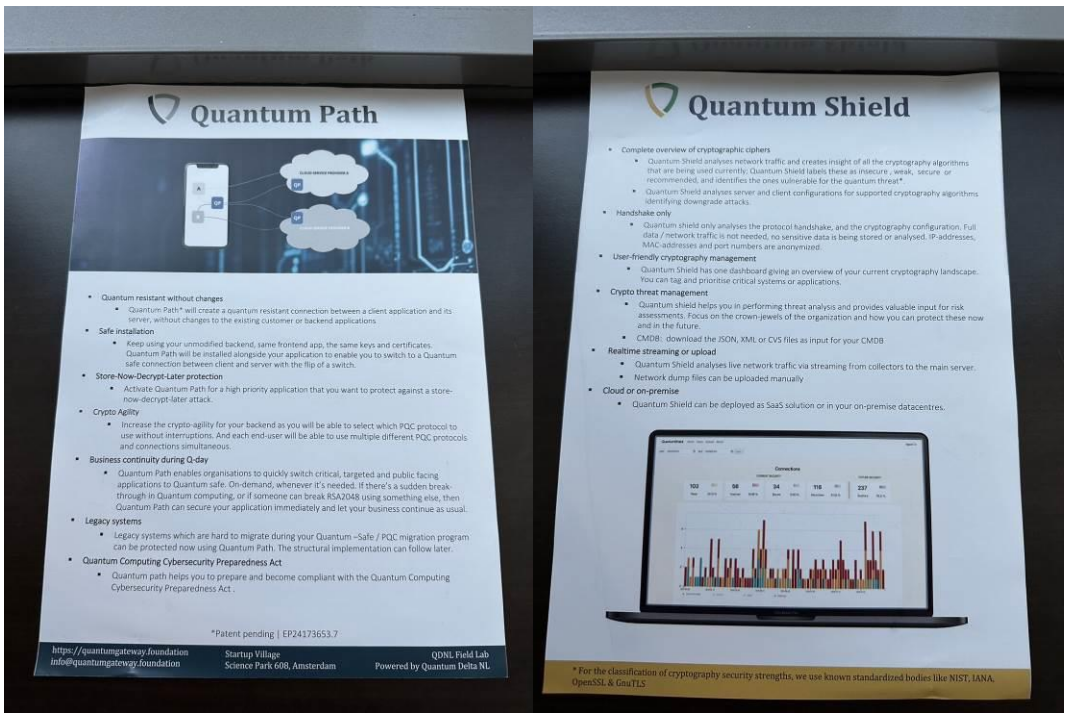


圖 7 活動交流- Quantum Gateway Foundation

資料來源：2024 ONE Conference 會議

2. 論壇專題演講-Bridging the talent gap

主講者：Lucinda Sterk, Anna Chung,

Ariela Lopez, Noortje Henrichs

該會議重點討論了資訊安全領域的人才短缺問題，由於資訊安全領域需求不斷增加，許多組織正面臨招募困難，討論強調多元化人才的必要性，並探討了如何吸引女性及不同背景的專業人士進入這個領域。會議提出了許多創新方案，目標是改進招聘方式，並鼓勵這些專業人才長期留在這個行業中。

會議中利用 AI 技術生成不同要應聘與招募的人才，來說明在自己求職過程當中會遇到的一些情況與瓶頸，再由會議上的與談人網路安全和危機溝通的專家 Lucinda Sterk，帶領各個頂尖單位如 Unit42、Fox-IT 及荷蘭國家網路安全中心 (NCSC-NL) 的領導者，為了縮小人才短缺與求職困境的這一差距，企業可以採取以下策略，歸納如下：

- 多元化與包容性：強調在網路安全領域中，吸引和留住來自不同背景的人才，特別是女性和少數族裔，能為行業帶來新視角和創新解決方案。
- 教育與培訓：通過教育和培訓計畫，提升現有員工的技能，並吸引新的人才進入網路安全領域，以應對不斷增長的威脅和漏洞。
- 產學合作：強調企業與大學之間的合作，開發適應行業需求的課程，確保畢業生具備實際所需的技能。
- 政策與宣導：討論政府和組織如何制定政策和宣導，支持多元化、教育和培訓計劃，以縮小人才差距。
- 職業發展與留任策略：探討如何為員工提供明確的職業發展路徑和支持，提升員工滿意度和留任率。

會議上提出許多解決方案，目標是改進招聘方式，並鼓勵這些專業人才長期留在這個行業中。

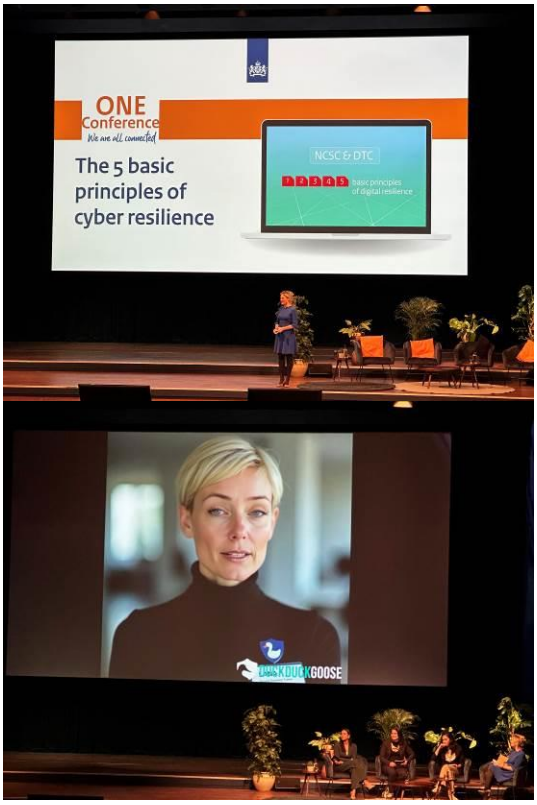


圖 8 活動照片- Bridging the talent gap
資料來源：2024 ONE Conference 會議

3. 論壇專題演講- Facing the EU digital compliance challenge

主講者：Hans de Vries, Michiel Steltman, Rudrani Djwalapersad, Joko Tenthog van Noorden, Kees Verhoeven

該會議主要探討如何應對歐盟日益複雜的數位法規，例如 NIS2 指令。NIS2 是歐盟於 2023 年實施的新網路與資訊安全法規，其於《網路與資訊系統安全指令》（Directive on Security of Network and Information Systems, NIS Directive）之基礎上，對監管範圍、成員國協調合作，以及資安風險管理措施面向進行補充，旨在加強和擴展對關鍵基礎設施和重要服務的網路安全保護。比原有 NIS 法規適用範圍擴大，規範更嚴格，目的是增強整個歐盟的網路韌性和應對能力。NIS2 主要內容說明如下：

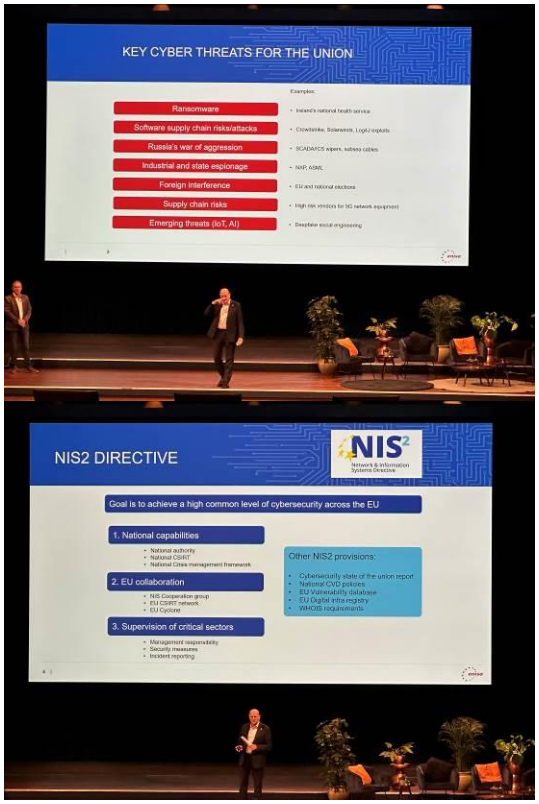
- 擴大適用範圍：NIS2 不僅涵蓋原有的關鍵基礎設施（如能源、交通、金融等），還包括更多行業，如供應鏈、醫療保健、資料中心和數位基礎設施等，甚至涉及一些被認為是「高風險」的數位供應鏈和第三方服務提供者。
- 強制性網路安全措施：要求受規範的組織（稱為「重要實體」和「必要實體」）採取強制性安全措施，包括風險管理、事

件應對、系統保護和資料備份等，以防範和減少網路安全威脅。

- 事件回報機制：NIS2 明確要求所有符合條件的組織必須向相關機構回報網路安全事件，並提供事件詳情。事件報告流程分階段進行，組織需在 24 小時內初步回報，72 小時內詳細回報，並在一個月內提交完整的報告。
- 高額罰款：違反 NIS2 法規的組織將面臨高額罰款。對於「必要實體」，罰款上限為年營收的 2%；對於「重要實體」，上限為年營收的 1.4%。此舉旨在加強合規意識，讓組織更重視網路安全。
- 跨境合作與資訊共享：NIS2 設置了多個監督和協作框架，鼓勵成員國之間更密切合作和資訊共享，提升跨國應對網路威脅的效率。歐盟成立了「歐洲網路安全聯盟」（EU Cybersecurity Competence Network），加強成員國間的合作。
- 國家主管機構角色加強：各成員國需建立或加強專門的網路安全主管機構，監督和推動 NIS2 的執行，並對網路安全事件進行協調和指導。
- 這些歐洲的相關法規旨在增強歐盟整體網路安全的韌性，但其覆蓋範圍廣泛，為企業帶來合規挑戰。本次會議與會者分享應對合規挑戰的策略，並討論如何在不同國家運營時維持合規性，重點說明如下：
- 歐盟數位政策的複雜性：過去 7 年，歐盟採納了超過 20 項新的數位法規，涵蓋從關鍵部門的韌性到個人資料保護、假資訊、線上恐怖主義和人工智慧偏見等多個領域。這些法規的多樣性和數量使企業面臨顯著的治理和合規挑戰。
- 企業面臨的合規挑戰：企業需要確定哪些法規與其業務相關，了解必須遵守的要求，以及在不同國家經營時這些要求

是否一致。此外，企業還需評估這些法規對其業務的影響和潛在的法律責任。

- 線上信任聯盟的角色：由荷蘭經濟事務和氣候政策部發起的線上信任聯盟（Online Trust Coalition，OTC）是一個公私合作的組織，旨在開發和定義方法，以簡化合規流程並提高法規的有效性。
- 綜合策略的制定：OTC 的參與者制定了一個詳細、實用且綜合的策略，協助組織及其領導者在面對大量歐盟數位法規時，建立強大的治理結構並展示合規性。
- 多方觀點的分享：會議中，來自歐盟、產業界和其他相關領域的專家分享了他們對數位合規挑戰的見解，並討論了應對這些挑戰的策略。



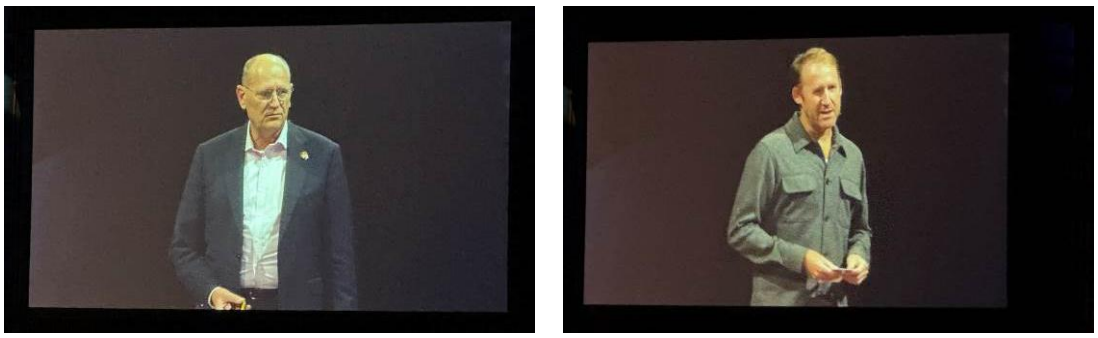


圖 9 活動照片- Facing the EU digital compliance challenge
資料來源：2024 ONE Conference 會議

4. 論壇專題演講- How the Dutch raise the security baseline：transparency

主講者：Elger Jonker

該會議探討了荷蘭如何透過提升透明度來增強其資訊安全基準，會議強調，透明度在荷蘭政府的資訊安全策略中扮演著關鍵角色，政府公開分享所有線上服務的安全基準數據，讓公眾能夠檢視安全性。這種做法不僅提高了政府的可信度，也促進了公共和私人領域之間的信任與合作，透過透明的政策，荷蘭能有效改善資訊安全並創建更安全的數位環境。

本次會議主要藉由說明利用 https://basisbeveiliging.nl/ 網站的搜尋分析結果，這個網站是荷蘭政府的數位安全政策組成部分，旨在評估並公布政府、醫療、教育、政治團體和網路安全公司等組織的基本數位安全狀況。該網站透過公開資訊，對網站和外部網路服務進行自動化檢查，評估其可用性、完整性和機密性。結果以地理地圖形式呈現，使用紅、橙、綠三色指示安全狀況，綠色表示安全，橙色表示中等，紅色表示存在問題。此舉旨在提高透明度，促使相關組織改進其數位安全措施，確保公眾對這些機構的信任。這個測量的指標包含 TLS 加密品質、DNS 安全性、未加密的 FTP 情形、電子郵件安全、RPKI 和相關安全檔的使用情形、非標準連接埠使用情形等，會議最

後還對最安全的組織頒發獎勵證書。

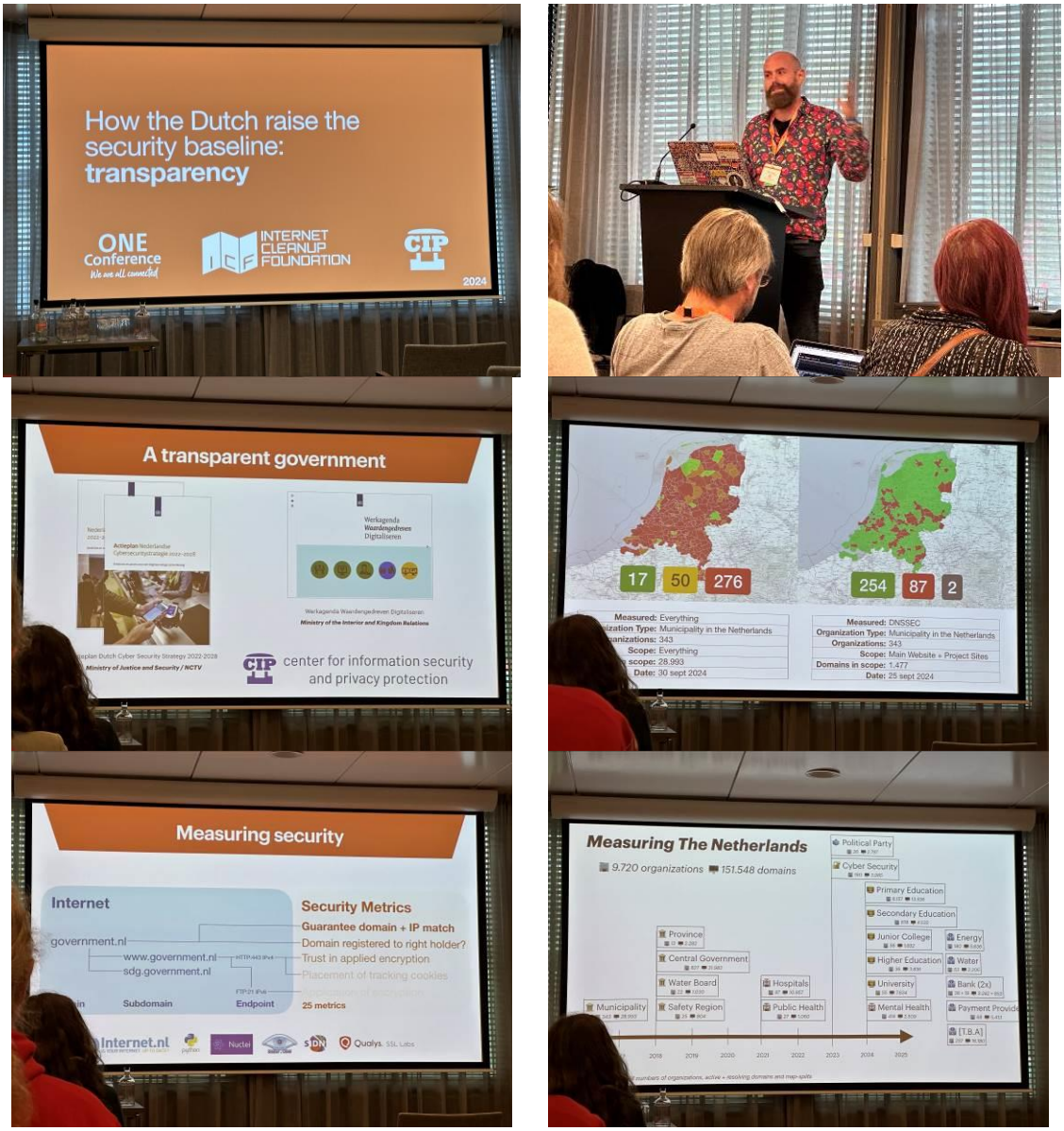


圖 10 活動照片- How the Dutch raise the security baseline: transparency

資料來源：2024 ONE Conference 會議

5. 論壇專題演講- Situation awareness through visual communication

主講者：Anni Tolvanen

該會議展示了如何透過視覺工具來提高資訊安全專業人員的威脅感知能力，會議中的討論強調，利用先進的視覺化技術可以幫助專業人員更好地理解資料含意，進而提升他們的即時決策能力，視覺溝通在資訊安全中的應用，能夠有效促進威脅識別和處理。

會議重點主要分為 4 個部分：

■ 減少認知負荷(reducing the cognitive load)

視覺化的呈現是可以最好的減少認知上的負荷，透過視覺化呈現方式，比嗅覺、聽覺、觸覺等感受，理解大部分的資訊。同樣的，視覺化呈現也更可以找到異常的資訊，透過字體大小不同的排版，也是抓住視覺重點的重要方法。

■ 讓事情變得容易理解(making things understandable)

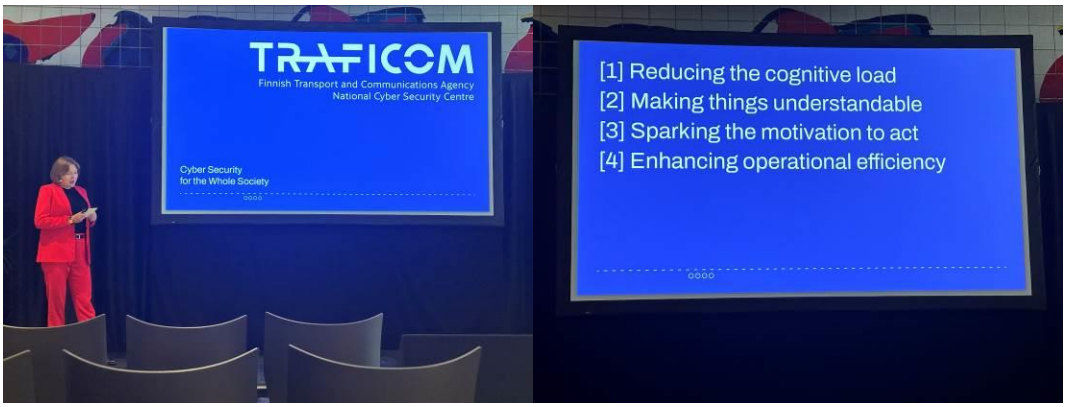
把相關資安事件用方法論呈現，或是以流程圖的方式描述攻擊過程，來幫助理解。例如一個勒索病毒的攻擊流程，可以先用 Mitre ATT&CK 的矩陣方式進行表達，然後用流程的方式說明其攻擊過程，來幫助理解整個資安事件的情形。

■ 激發行動動力(Sparking the motivation to act)

在這個部分可以利用比較的方式來激發行動力，例如圖表或是案例的比較。

■ 提高營運效率(enhancing operational efficiency)

最後就是利用自動化的工具來幫助提高與加快整體的運作流程。



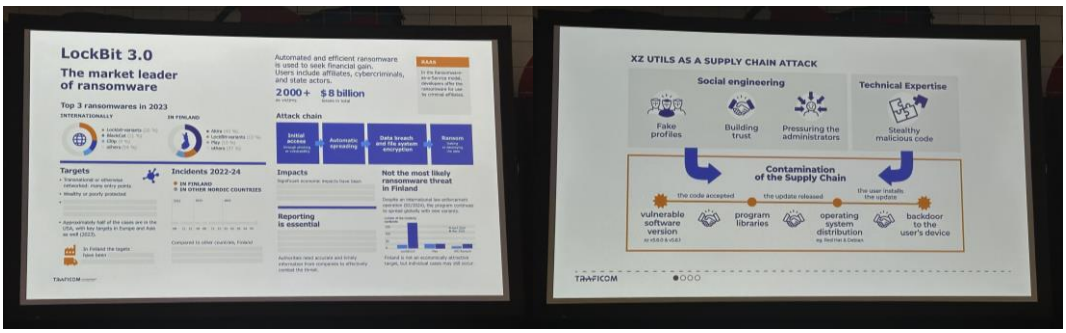


圖 11 活動照片 - Situation awareness through visual communication

資料來源：2024 ONE Conference 會議

6. 論壇專題演講-荷蘭工業自動化控制系統的威脅-Threat Landscape on IACS for the Netherlands

主講者：Rik van Dijk：Researcher, NCSC-NL

產業在工業控制系統中面臨什麼威脅？Rik van Dijk 和 Robin Staa 在此次會議提出了來自第一份 NCSC-NL 工業自動化控制系統威脅概況的研究結果，檢視了 2023-2024 年期間的相關事件和威脅和事件。

講者首先強調，隨著地緣政治事件的加劇，特別是俄烏戰爭等國際衝突，全球關鍵基礎設施受到的資安威脅不斷增長。工業控制系統(ICS)是當今社會不可或缺的部分，支撐著能源、水資源等基礎服務。然而，這些系統經常使用陳舊技術，且多數設計初衷是保障操作安全，而非抵禦網絡攻擊。隨著 IT 與 OT 系統的逐漸融合，ICS 的網絡暴露面變得越來越大，使得這些系統更容易受到攻擊。據統計，2023 年全球 ICS 系統的網絡威脅增加了約 20%，許多攻擊來自於使用簡單技術進行網絡滲透的駭客，而這些技術並不需要高深的技術背景，這些威脅的增長與全球政治局勢的緊張密切相關。

根據資料顯示，ICS 受到不同類型的攻擊，最常見的是經濟動機的勒索軟體攻擊。講者提到，僅在 2023 年，荷蘭就發生了大約 7447 起勒索軟體事件，其中涉及 ICS 的約占 1%。全球範

圍內，ICS 相關的勒索軟體攻擊導致的停產時間從一天到一個月不等，經濟損失相當可觀。儘管目前 ICS 系統直接受到勒索軟體攻擊的案例較少，攻擊主要透過 IT 系統滲透，但 ICS 環境中的 IT 和 OT 融合增加了勒索軟體影響範圍。這些資料反映了資安防護在工業控制系統中的重要性，尤其是在地緣政治緊張局勢下，攻擊可能不僅是經濟動機，還可能帶有政治目的。

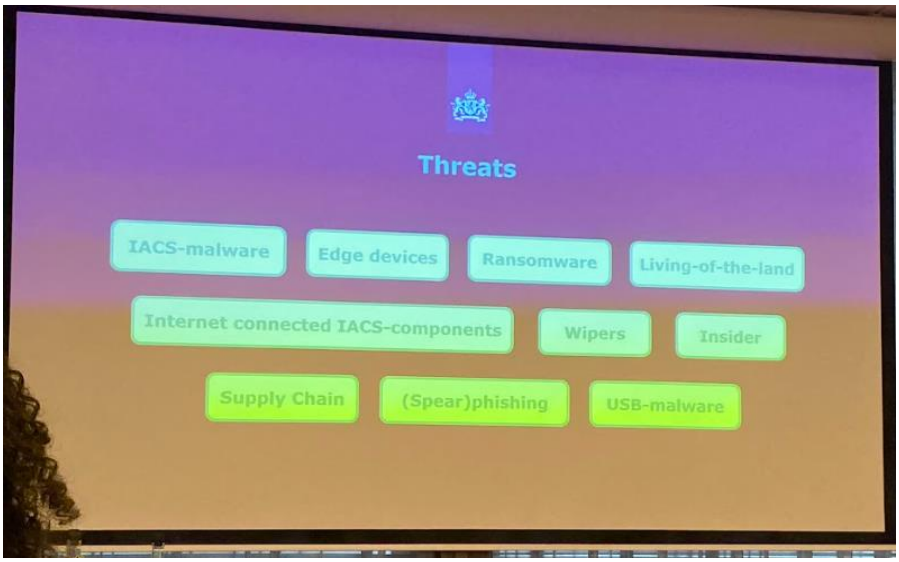


圖 12 ICS 系統面對的主要威脅來源
資料來源：2024 ONE Conference 會議

講者進一步闡述了與間諜活動相關的資安威脅。間諜攻擊多來自國家支持的駭客組織，這些攻擊主要針對工業系統以竊取機密資訊。根據資料，間諜活動的攻擊往往持續數月甚至數年，駭客會利用 ICS 系統中的本地工具進行隱蔽攻擊，這被稱為「依賴原生技術的攻擊」(Living off the Land)。俄烏戰爭爆發後，針對烏克蘭關鍵基礎設施的間諜攻擊明顯增多，2024 年發生了數起重大間諜事件，目標包括烏克蘭的電力和供水系統，這些攻擊不僅涉及訊息竊取，還為後續的破壞性行動鋪路。

除了間諜活動，講者還談到了與地緣政治高度相關的破壞性攻擊。儘管此類攻擊較為罕見，但當其發生時，影響極為嚴重。2024 年，針對烏克蘭的一次攻擊中，攻擊者成功控制了供

熱系統，導致數個城鎮在冬季斷供，影響了數千人的生活。這種攻擊通常需要對 ICS 系統有深入了解，並會使用特定的惡意軟體針對這些系統進行操作。講者指出，儘管破壞性攻擊相對較少，但在地緣政治局勢緊張的情況下，其風險顯著增加。隨著俄烏戰爭的持續，預計此類攻擊的頻率將進一步上升。

講者還討論了網絡激進主義者的興起，這些攻擊者出於政治或意識形態動機，對 ICS 系統進行攻擊。他們通常會利用 ICS 系統的互聯性漏洞來發動攻擊，這些攻擊多數是隨機的，目標往往是暴露在網際網路上的系統。例如，2023 年底，一個激進主義組織成功入侵愛爾蘭的一個水處理廠系統，導致當地兩天無法正常供水。雖然此類攻擊通常不會造成嚴重的生命財產損失，但對當地社區的生活秩序造成了嚴重干擾。講者強調，這類低技術門檻的攻擊正變得愈發常見，尤其是在政治動盪時期，對企業構成了實際的挑戰。

最後，講者強調了 ICS 惡意軟體的發展趨勢，這些惡意軟體的出現與全球地緣政治形勢密切相關。講者提到，2024 年出現的兩個新型惡意軟體「Cosmic Energy」和「Frosty Groupies」分別針對電力分配系統和市政供熱系統，這些惡意軟體的開發明顯受到俄烏戰爭的推動。儘管目前全球 ICS 惡意軟體攻擊事件較少，但講者預測，隨著地緣政治局勢的進一步惡化，ICS 惡意軟體的數量和複雜性將逐漸增長。這意味著各國和企業需要加強 ICS 系統的資安防護，以應對未來可能出現的更大威脅。

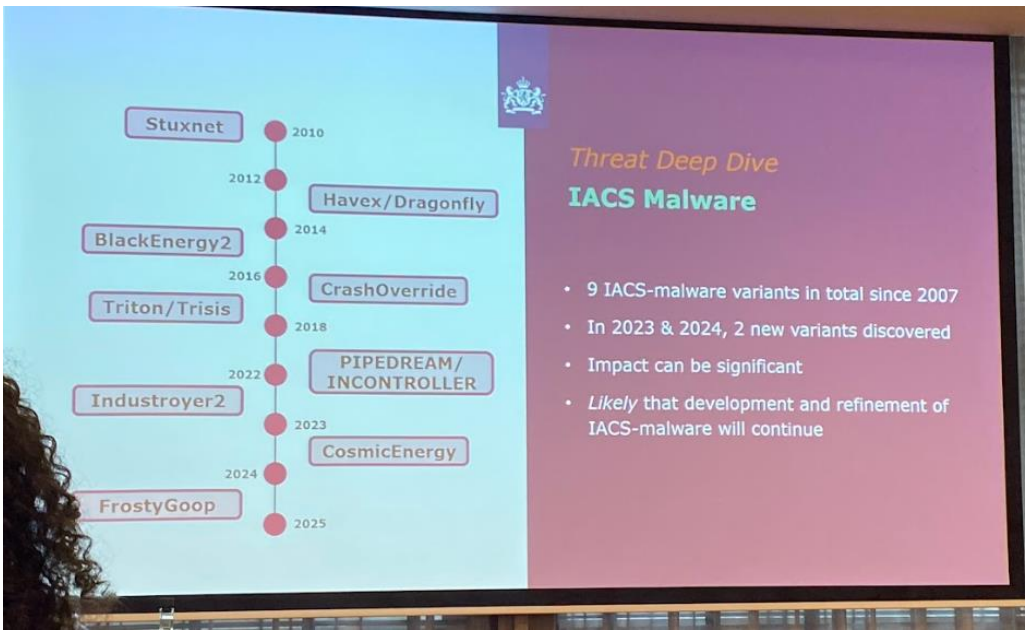


圖 13 種針對 ICS 系統攻擊之惡意軟體

資料來源：2024 ONE Conference 會議

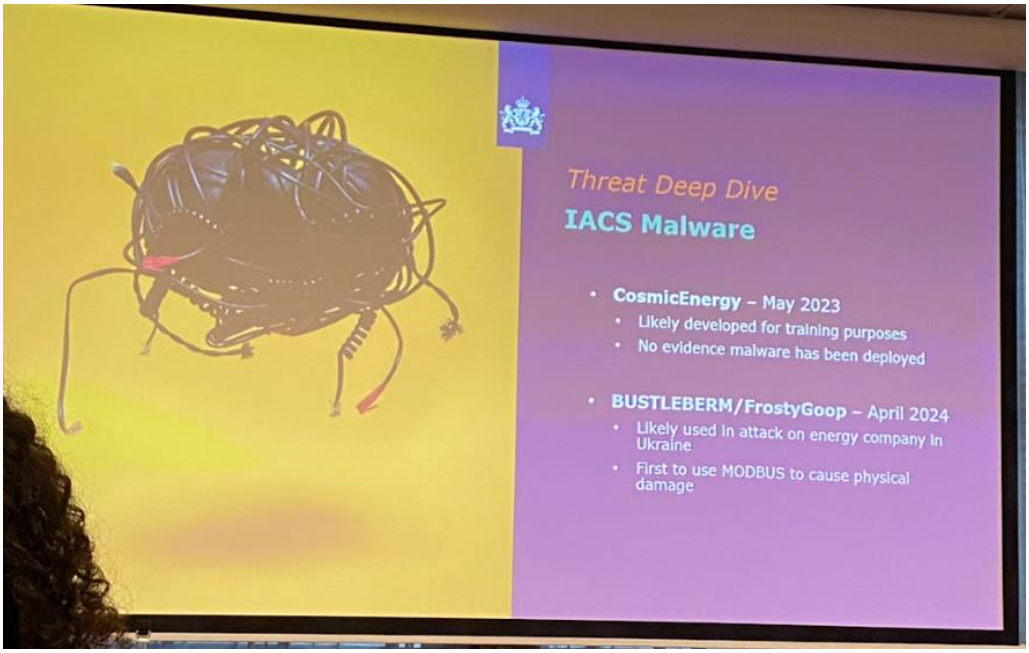


圖 14 近年發現之針對 ICS 系統之惡意軟體說明

資料來源：2024 ONE Conference 會議

7. 論壇專題演講-人工智慧和 CRQ 建構資安防護機制案例

-CISOs Building Defensible Business Cases using AI & CRQ

主講者：Douwe Mik：Director, Stratey & Risk,

Booz Allen Hamilton；Luke Simonetti

主要內容：講者首先介紹了如何應對當前資安領域日益增

長的複雜性。他提到，在管理公司的資安風險時，傳統的治理、風險和合規(GRC)工具雖然提供了基本的工作流程，但無法即時更新決策資訊，導致許多決策還是基於「點對點」的方式進行。針對這一挑戰，講者提到多家大公司已經開始採用新一代的風險管理解決方案。例如，某金融服務公司在 2023 年採用了一套整合風險管理系統（IRMS），該系統能夠將威脅情報、漏洞管理、以及滲透測試結果整合到一個單一頁面，從而實現即時的風險預測。據該公司反饋，透過這一系統的實施，他們將平均風險回應時間縮短了 35%，並且提高了風險預測的精確度，這是許多公司正努力實現的資安目標。

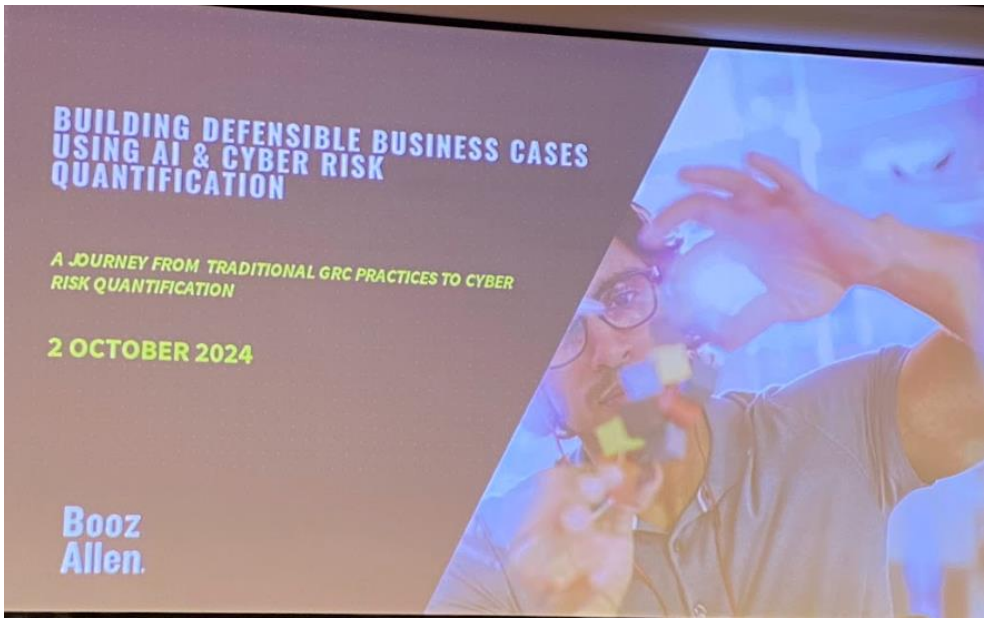


圖 15 人工智慧和 CRQ 建構資安防護機制案例首頁
資料來源：2024 ONE Conference 會議

講者強調了使用人工智慧(AI)技術來量化資安風險(CRQ)在實務中的價值。他介紹了一家全球製造業公司如何透過 AI 輔助的風險評估工具來量化他們的資安風險。這家公司的 IT 團隊透過這個工具進行了 500 多個場景的模擬，發現其中 15%的系統存在嚴重漏洞，這些漏洞可能在接下來的 12 個月內導致約 5,000 萬美元的損失。該工具透過資料建模和 AI 預測技術，幫

助該公司優先處理高風險區域，並採取具體的補救措施，從而將潛在損失降至 2500 萬美元。這一量化資料不僅幫助公司做出了更精確的風險投資決策，也提升了董事會對資安投資回報的認可度。

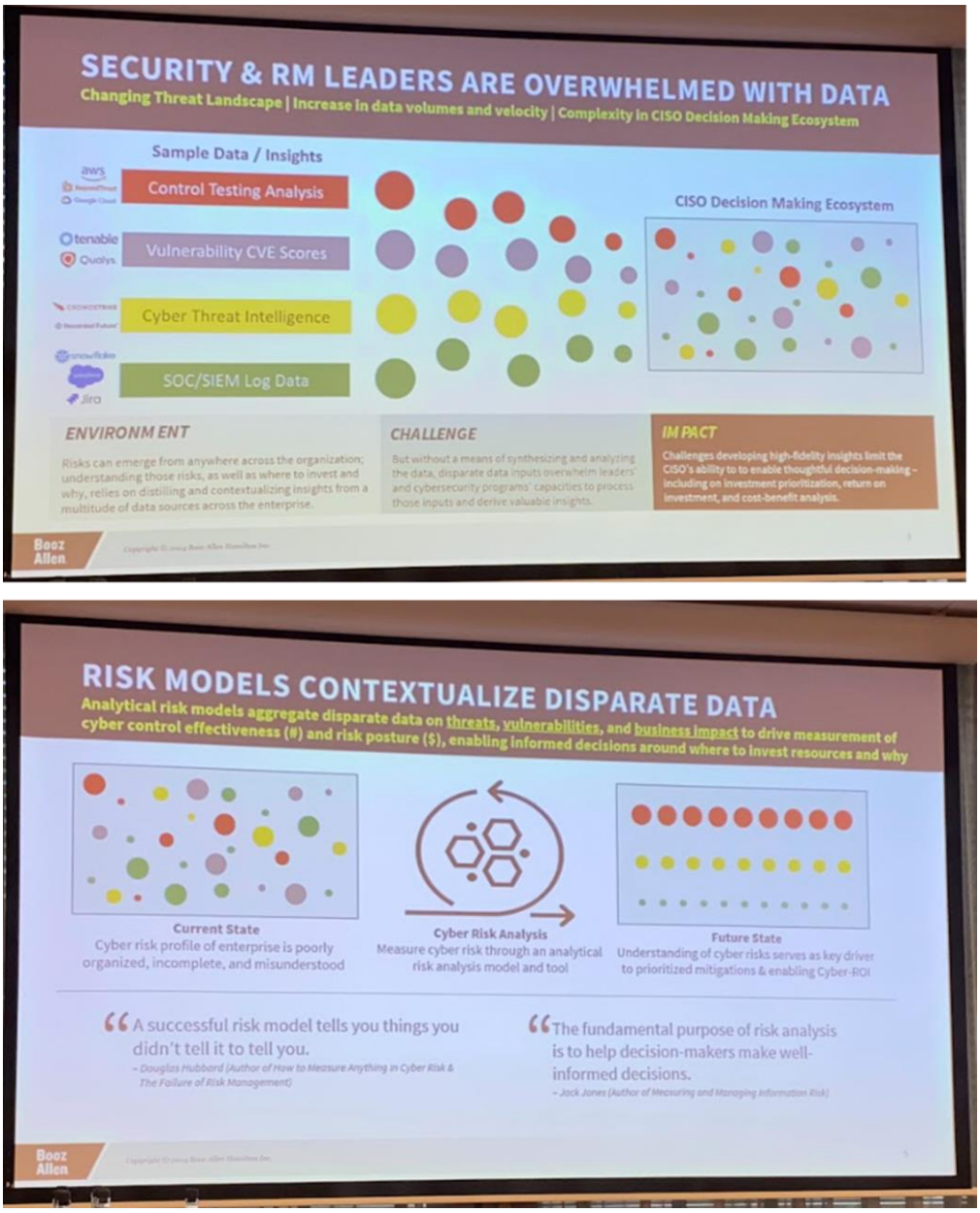


圖 16 資安風險分析模式

資料來源：2024 ONE Conference 會議

針對技術細節，講者提到，在實施 CRQ 時，關鍵是如何有效地整合和處理大量不同的資料來源。他舉例說明了一家科技公司是如何透過整合多種資料來源，包括威脅情報、漏洞報告、

控制評估和滲透測試，來實現全面的風險量化。該公司透過 AI 技術，自動化資料處理並生成即時的風險報告，這樣可以快速識別出威脅點。具體來說，這家公司成功將資安威脅情報的回應時間從原來的兩周縮短至 48 小時，並顯著降低了因攻擊而導致的停機時間。這個技術實作展示了如何透過整合技術提升風險管理效率，進而為業務帶來更大的價值。

講者介紹了一家醫療技術公司如何採用 AI 和量化風險評估技術來減少資安事件的發生。該公司透過分析其過去五年的資安事件資料，並結合 AI 預測模型，識別出最易受攻擊的系統。隨後，他們針對這些系統進行了安全補強，並實施了自動化的安全監控工具，即時檢測異常行為。據該公司報告，自從實施這些措施後，資安事件數量減少了 40%，而且 IT 團隊的維運工作量也顯著降低，從而節省了約 25%的營運成本。這一實例展示了量化風險評估技術在提升公司資安狀態和降低成本方面的巨大潛力。

講者表示量化風險評估不僅限於技術層面，也幫助公司在資安投資上做出更明智的決策。他舉例說明了一家零售公司在 2023 年進行了一次全面的資安風險評估，該評估顯示，如果該公司不採取進一步的安全措施，其在未來一年內可能因資料洩露損失高達 1 億美元。基於這些量化資料，該公司決定增加資安投資，採用了多層次的安全防禦體系，並部署了先進的身份管理和加密技術，這使其預期損失降低至 2000 萬美元。同時，公司透過這些資料成功說服董事會批准了更多的資安預算，以應對未來的挑戰。

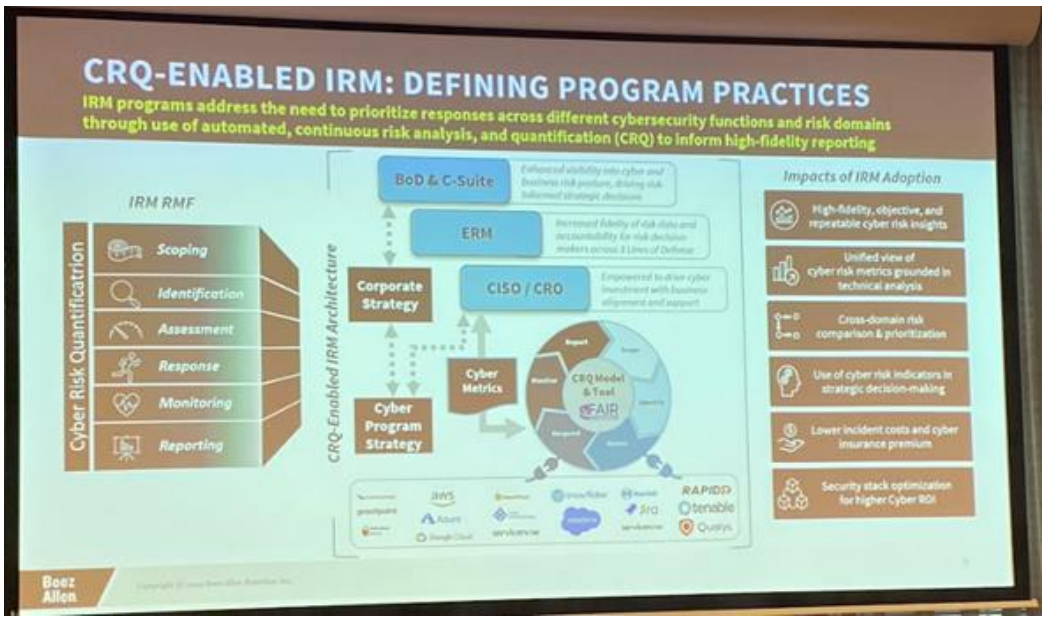


圖17 資安風險量化實際作法

資料來源：2024 ONE Conference 會議

最後，講者強調了量化風險評估技術對於公司戰略決策的重要性。他提到，許多企業現在正逐漸從傳統的合規驅動轉向風險驅動的資安模式。一家全球性金融機構最近採用了基於風險的資安策略，他們透過 AI 和量化風險技術，每季度進行風險評估，並根據即時資料動態調整資安資源的分配。這家公司發現，透過這樣的策略，他們不僅能夠更靈活地應對市場變化，還能在競爭激烈的金融業務中保持技術優勢。這一實際作法證明，將量化風險評估融入公司戰略，不僅可以提升資安防護水平，還能為企業創造可持續的競爭優勢。

8. 論壇專題演講-網路安全的遊戲改變者：RED 3.3 和 CRA-Gamechanger in cybersecurity: RED 3.3 and CRA

主講者：Brenda van der Wal：Senior policy officer Ministry of Economic Affairs

Brenda van der Wal 是資安和經濟安全領域的協調政策官員。她參與了歐盟網路韌性法案的談判，並將繼續參與荷蘭的網路韌性法案實施，依其簡報說明，《網路韌性法案》（Cyber

Resilience Act，CRA）的推出是歐盟數位安全框架的重要一步。根據該法案的計劃時間表，法案的生效預計在 2024 年第 4 季公布，並在整個歐盟內部逐步實施，至 2027 年第 4 季推廣至產品端。而《無線電設備指令 3.3》（Radio Equipment Directive3.3，RED3.3)則在 2024 年 10 月列為標準，並於 2025 年 8 月開始網路設備的稽查。

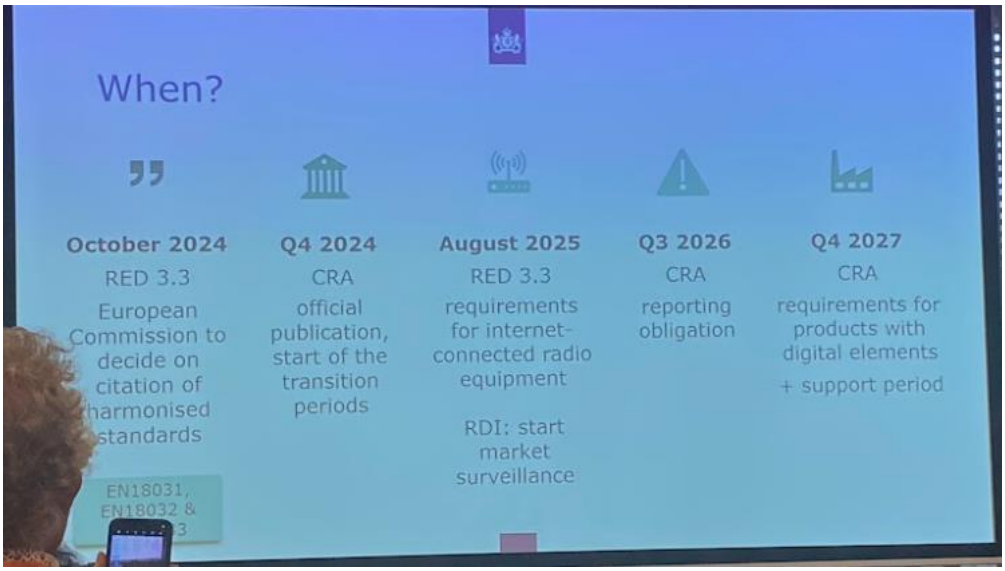


圖18 RED 3.3 和 CRA 推動時程
資料來源：2024 ONE Conference 會議

此二項法案旨在應對日益增長的資安威脅，尤其是針對具數位元素的產品，強化其從設計階段到使用全過程中的資安標準。這將帶來深遠的影響，因為該法案要求硬體和軟體製造商在產品開發過程中必須納入嚴格的資安控制。對於企業來說，這意味著需要提前投入資源以確保合規，尤其是在供應鏈安全和產品維護方面。然而，這也帶來了巨大的商機，尤其是對於資安解決方案供應商、認證機構和技術開發公司，他們將能夠提供專業的支援服務，幫助企業符合新法規的要求。

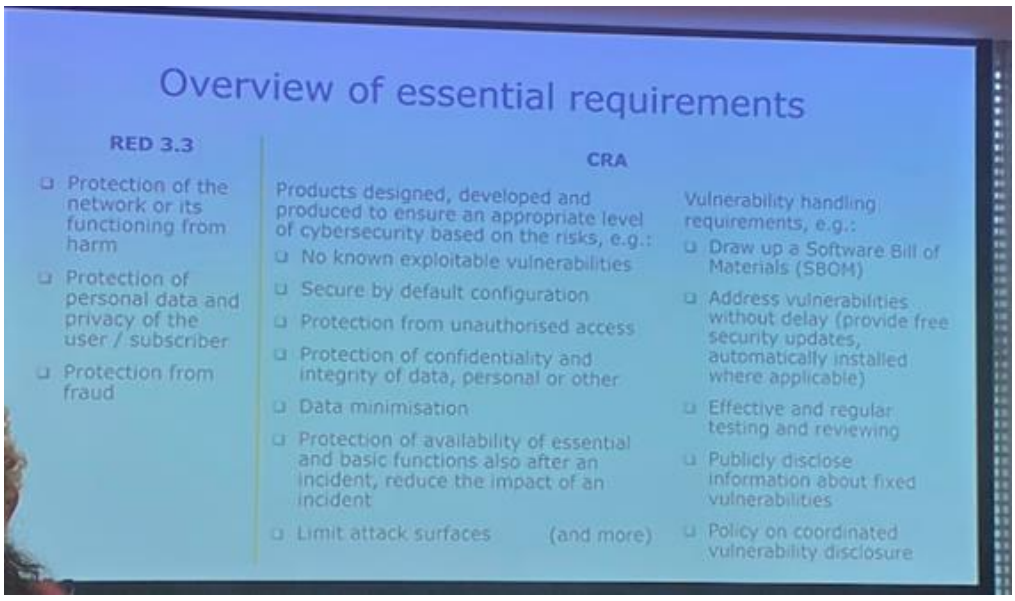


圖19 RED 3.3 和 CRA 規範內容

資料來源：2024 ONE Conference 會議

講者表示，法案的影響範圍廣泛，不僅限於大型跨國企業，小型企業也將面臨相同的法規要求。根據講者所述，許多中小型企業對於資安威脅的防護能力不足，這是當前數位生態系統中的一大挑戰。隨著法案的實施，這些企業將不得不加強其資安防護措施，這可能帶來一定的合規成本壓力。然而，對於市場來說，這也意味著新興的商機。例如，法案將促使市場需求增加，對於資安軟體、更新管理平台、智慧設備安全工具等技術解決方案的需求將顯著提升。許多公司，特別是中小型企業，可以利用這一法案所帶來的增長機會，透過提供針對特定市場需求的創新解決方案來佔據市場先機。

法案的時程安排還涉及合規性檢查和認證程序的落實。根據 CRA 的規定，歐盟內部的所有產品必須經過嚴格的資安審查，並且需要定期進行資安更新，以確保產品在整個生命週期內保持高度的安全性。這對於現有的產品監管機構和測試機構來說，是一個顯著的影響，因為將會有大量的產品需要接受審查和認證。這無疑將增加他們的工作負荷，同時也為他們提供

了增長的機會。市場中預計會出現更多的資安測試和認證需求，這將促使更多企業進入這一領域。此外，技術服務提供商也可以借此機會開發自動化合規工具，幫助企業降低合規成本並加速審查流程。

圖20 RED 3.3 和 CRA 推動之建議準備作法
資料來源：2024 ONE Conference 會議

隨著法案推進，另一個值得關注的領域是產品生命週期管理和供應鏈安全。講者表示供應鏈中的每一個環節都將受到法案的影響，特別是對於具有多層供應商的企業而言，必須確保其所有的供應商都符合資安標準。這意味著公司將需要重新審查其供應鏈，確保每個供應商都遵守資安規範。這對於供應鏈管理公司來說，提供了新的商機。供應鏈管理解決方案的市場需求將會顯著增加，尤其是那些能夠提供即時資安風險評估和監控的解決方案。此外，對於資安保險公司來說，這是一個拓展業務的機會，因為企業將尋求更多的保險來減少潛在的資安風險。

法案的時程安排還包括了對企業的持續資安維護要求。根

據法案，產品在整個使用過程中必須保持資安更新，並且製造商需要定期提供資安修補檔。這一要求對於軟體開發公司和技術支援提供商來說是一個潛在的商機，因為許多公司可能沒有內部資源來管理持續的資安維護和更新。提供資安維護服務的公司將能夠填補這一市場空白，尤其是針對那些小型企業和新創公司，這些公司通常無法自己完成這樣的工作。此外，提供自動化更新管理解決方案的公司也將從中受益，因為市場對於即時更新的需求將大幅提升。

最後，CRA 法案的全面實施預計將對數位市場產生長遠影響。根據法案，歐盟市場上所有的數位產品都必須遵循同樣的資安標準，這將促使整個市場向更高的安全性標準邁進。對於已經在資安領域有強大實力的公司來說，這是一個巨大的商機，因為他們可以透過提供資安諮詢、解決方案和認證服務來增加收入。此外，隨著全球市場逐漸關注資安風險，符合 CRA 標準的產品將具有更強的競爭力，不僅在歐盟內部，還包括全球市場。對於那些能夠提供創新解決方案的公司來說，這是一個在資安領域佔據領導地位的機會。

9. 論壇專題演講-網路攻防中的人工智慧-AI in Offensive and Defensive Cyber

主講者：Kris Oosthoek：Security Researcher - Delft University of Technology

講者說明目前的研究重點是人工智慧在資安和網路犯罪下的應用，人工智慧(AI)在資安領域的應用已經展現出強大的潛力，尤其是在強化防禦和預防網路犯罪方面。AI 透過其強大的學習能力，可以自動化地監控網路系統，檢測出潛在的安全漏洞。講者提到，許多企業利用 AI 來分析大量的網路流量數據，從中識別異常行為，這樣可以在威脅發生前就加以防範。例如，

AI 可以自動檢測釣魚郵件的特徵，並主動隔離這些郵件，防止網路攻擊的蔓延。這些 AI 技術不僅能減少人力干預，也提高了應對速度，降低了企業面臨的風險。

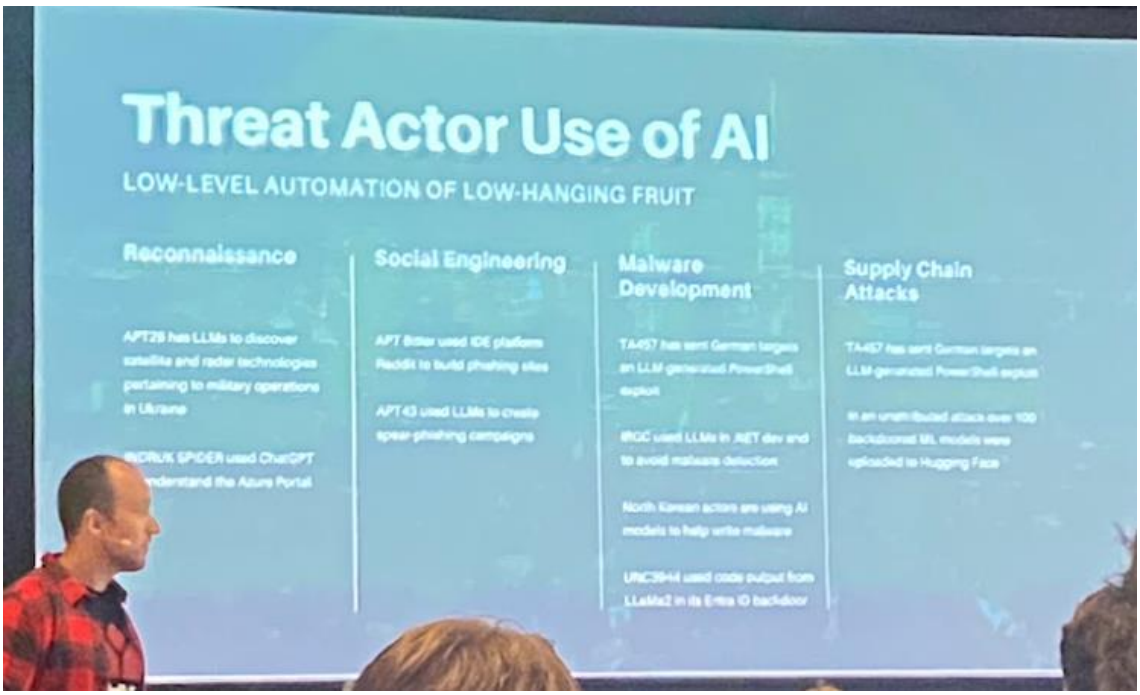


圖21 人工智慧可能的威脅說明
資料來源：2024 ONE Conference 會議

在防止網路犯罪方面，AI 的應用同樣重要。講者指出，AI 能夠透過分析多樣化的資料來識別出潛在的網路犯罪活動，尤其是像分布式拒絕服務(DDoS)攻擊這類攻擊。傳統的資安防禦通常依賴於事後響應，而 AI 能夠及時預測這些攻擊，從而採取主動防禦措施。例如，AI 可以透過持續監控網路流量來識別異常的資料包並主動封鎖，防止攻擊造成大規模的網路癱瘓。這類應用展示了 AI 在打擊網路犯罪中的關鍵角色。

講者強調，AI 在資安中的一大優勢是其自我學習和不斷優化的能力。與傳統的防禦技術不同，AI 系統能夠透過不斷學習新的威脅模式和攻擊方式來提高自身的防護水準。例如，AI 可以學習來自不同來源的資料，分析過去的網路攻擊，並透過自動化流程預測未來可能發生的攻擊類型。這樣的技術使得企業

能夠快速應對新興的安全威脅，同時減少依賴資安專家的時間和人力成本，從而更高效地保護其網路資源。

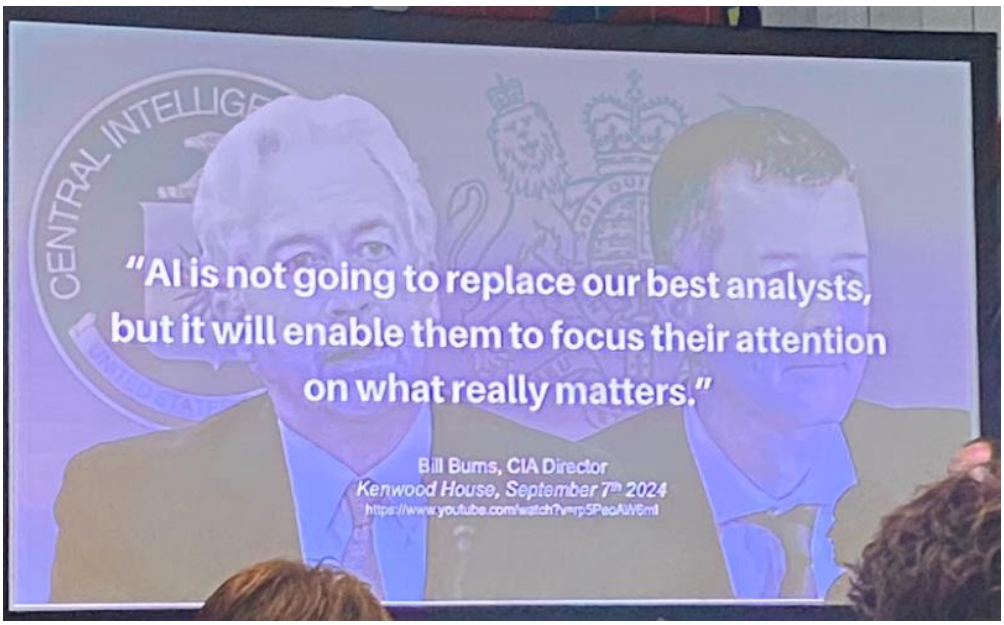


圖22 講者引述美國中央情報局對人工智慧應用的看法
資料來源：2024 ONE Conference 會議

然而，AI 技術本身也存在被濫用的風險，尤其是在網路犯罪中。講者指出，攻擊者可以利用 AI 生成更加難以檢測的惡意軟體或進行更加複雜的社交工程攻擊。例如，AI 可以模仿合法的用戶行為，讓傳統的安全系統無法辨別其是否為惡意行為。因此，AI 既是防禦者的有力工具，也成為攻擊者的潛在武器。為了應對這一挑戰，未來的資安技術必須進一步加強 AI 系統的安全性，並防止這些系統被惡意利用，這是資安領域未來發展的關鍵方向。

10. 論壇專題演講-資安作為經濟增長引擎的策略-Cyber as an Engine of Economic Growth – Strategy

主講者：James Caffrey：Head of Capacity Building - National Cyber Security Centre Ireland

James Caffrey 是愛爾蘭國家資安中心的負責人，他表示愛爾蘭在數位技術的採用和使用方面位居歐盟成員國前列地位，

這包括網路產業生態系統，該生態系統中有近 500 家公司參與，涵蓋跨國公司和中小型企業。

圖23 James Caffrey 開場說明
資料來源：2024 ONE Conference 會議

愛爾蘭在數位技術的採用和網路產業生態系統的建設中，展現潛力，特別是在政府的主導下，資安產業戰略成為經濟增長的引擎，而愛爾蘭政府在協調、推動和加速資安產業的發展方面發揮了核心作用，並且包含向後量子遷移的相關產業，政府的參與不僅是為了推動本地產業的增長，還在於建立一個具競爭力的國際市場。愛爾蘭政府積極投資於資安領域，設立了國家級研究發展中心，促進研發生態系統的建立。這種策略不僅強化了國家的網路防護能力，還提高了愛爾蘭在全球市場中的競爭力。

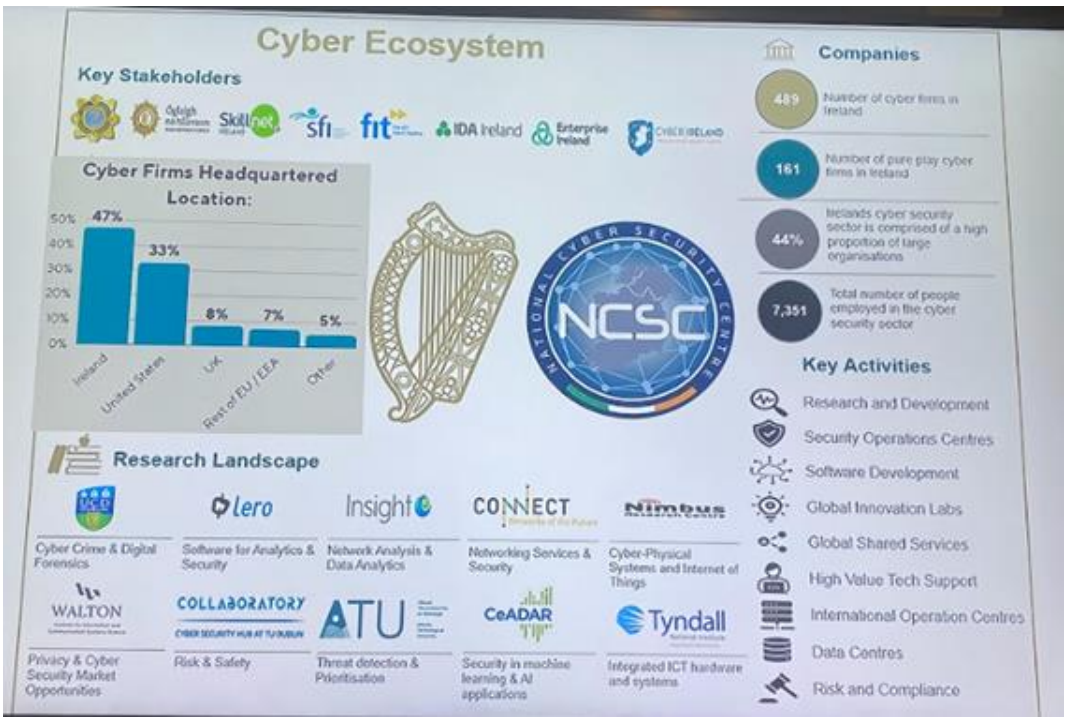


圖24 愛爾蘭資安生態系說明

資料來源：2024 ONE Conference 會議

愛爾蘭的資安產業戰略著重於解決本地資安人才短缺的問題。講者表示愛爾蘭 66%的企業表示面臨技能、招聘或人才留存的挑戰。為了應對這一問題，政府制定了一項戰略目標，即每年培訓和吸引 1000 名資安專業人才。此舉不僅有助於提高國內企業的競爭力，也為愛爾蘭吸引更多的外商直接投資（FDI）奠定了基礎。透過加強與教育和研究機構的合作，愛爾蘭致力於建立一個持續的人才培養體系，以確保資安產業的長期發展。這種全方位的支持將幫助本地企業應對日益增長的技術挑戰。

此外，愛爾蘭的戰略還強調了研發和創新的重要性。該國的資安產業在研發能力和投資協調方面存在不足，這對於愛爾蘭在國際市場上的競爭力構成了威脅。因此，政府正在推動建立一個協調良好的研發生態系統，並加強國內企業的研發能力。這不僅提升了本土企業的技術創新能力，也為全球市場提

供了更多的安全解決方案。歐盟的新資安法規對愛爾蘭企業來說是巨大的商機，尤其是那些具備數位解決方案的公司，可以利用這些法規來服務歐盟市場。

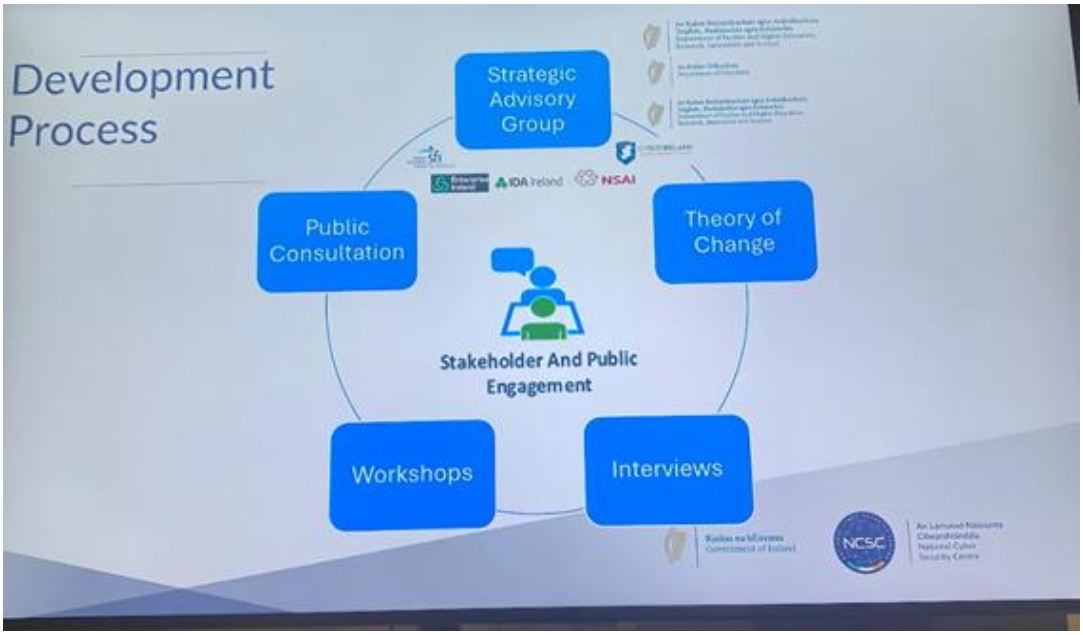


圖25愛爾蘭資安發展流程
資料來源：2024 ONE Conference 會議

最後，愛爾蘭的資安產業戰略與國際市場接軌，特別是與歐盟的數位市場戰略緊密結合，歐盟的數位市場正在快速擴張，而資安是支持這一市場增長的關鍵因素，愛爾蘭致力於成為歐盟內部具技術主權的國家，並積極吸引非歐盟的跨國公司來愛爾蘭設立基地。透過及早適應歐盟的法規，愛爾蘭企業將能夠利用這些新法規帶來的市場機會，佔據先發優勢。這樣的策略不僅增強了愛爾蘭企業在國際市場的競爭力，也為國家的數位經濟和社會安全提供了強有力的支持。

三、10 月 1 日(二) 下午 拜訪海牙市政府資安長

(一) 會議資訊

1. 地點：ONE Conference, World Forum, The Hague Oceania 會議室
2. 時間：下午 14:00 至 15:00
3. 荷方代表：
   (1) 海牙市政府資安長 Jeroen Schipper
   (2) National Cybersecurity Center 營運部門主管 Martijn Jonk
   (3) 海牙市政府資深政策顧問 Pepijn Zaaman

(二) 會議摘要

1. 荷方介紹「Hack the Hague 2024」活動

Jeroen Schipper 代表荷方詳細介紹了 2024 年「Hack the Hague」活動的主軸及其成果。今年的活動主題聚焦於測試海牙市的數位基礎設施和物理系統的安全性，特別是檢驗市政府的數位服務平台和實體基礎設施的防禦能力。活動吸引了來自全球的 100 多名白帽駭客，這些駭客透過攻擊模擬的方式測試了海牙市的網路與實體系統的脆弱性。

2024 年「Hack the Hague」的亮點在於，除了針對數位系統的傳統網路攻擊之外，活動首次擴展到對工控系統(OT)的測試，這些系統包括海牙市的供水、能源管理、以及智能交通控制系統。此次測試顯示，雖然市政府在許多方面已具備較高的資安防禦能力，但仍存在一些可以進一步加強的脆弱點。白帽駭客成功發現了數十個潛在的安全漏洞，這些發現將幫助市政府優化其資安防禦策略，進一步提升公共服務系統的安全性。

根據活動的成果，海牙市政府已決定將這些測試結果納入下一步數位安全強化計畫中，並計劃在 2025 年擴大活動範圍，邀請更多國際資安專家參與，持續提升市政府的安全水平。

2. 介紹 HITCON 相關活動

我方進行介紹了臺灣的 HITCON（Hacks in Taiwan Conference）活動。這是臺灣年度資安技術交流的盛會，匯集了全球頂尖的資安專家、白帽駭客和相關業界人士，旨在提升資安技術的創新和國際影響力。HITCON 以其專業性和開放性，為亞洲資安社群提供了重要的交流平台。

3. 互相邀請參與未來活動

會議中，荷方邀請臺灣 1-2 組白帽駭客團隊參與 2025 年的「Hack the Hague」活動，期待雙方在該活動中進行深度的技術交流與合作。同時，我方也邀請荷蘭的資安專家參與 2025 年的 HITCON CISO Summit，促進雙邊在資安領域的深入互動。雙方對參與對方的資安活動表示了濃厚興趣，並將在 2025 年活動的具體規劃出來後，進一步討論合作細節與參與方式。

圖 26　全體與會人員會後合影

資料來源：現場拍攝提供

四、10 月 1 日(二) 下午「臺荷資訊安全聯盟」的合作備忘錄簽署

(一) 會議資訊

1. 地點：ONE Conference, World Forum, The Hague Oceania 會議室

2. 時間：15:00 至 16:00

3. 荷方與會人員如下列名單(共 11 人)

No.	單位/Organization	職稱/Title	姓名/Name
1	Digital Economy, Ministry of Economic Affairs & Climate Policy	Director	Jos De Groot
2	Digital Economy, Ministry of Economic Affairs & Climate Policy	Senior Policy Adviser	Brian Huijts
3	Innovation Quarter	Senior Account Manager Safety & Security	Philip Meijer
4	Innovation Quarter 荷蘭創新中心	Senior Account Manager Asia	Xiaoling Sun 孫曉玲
5	Security Delta HSD	Deputy Director	Saskia Noordewier
6	Security Delta HSD	International Program Coordinator, Innovation Liaison	Paul (jr) Coumans
7	Dutch Blockchain Coalition & ECP Platform for the Information Society	Communications Advisor	Femke Bartelds
8	Dutch Blockchain Coalition	Innovation Manager	Nina Huijberts
9	EclecticIQ	VP Government Sector	Karen Sunderman
10	CFLW Cyber Strategies	Managing Director	Mark van Staalduinen
11	CFLW Cyber Strategies	Technology Director	Eljo Haspels

(二) 合作備忘錄簽署活動背景說明

CFLW 是一家致力於為數位社會提供安全可靠網路空間的專業機構，在 Mark van Staalduinen 博士的領導下，保障數位社會的繁榮與安全，透過提供全球策略見解和營運視角，來打擊網路

空間與新興技術中出現的非法活動。其採取使用者為中心的敏捷方式，與多方利害關係人共同開發先進技術，尤其是在暗網、加密資產、區塊鏈、去中心化密碼學和人工智慧等領域。CFLW 透過建立公私聯盟，應對迅速變化的網路威脅，並提供資料驅動的技術解決方案，協助調查人員開發新的調查技術，破壞犯罪者的商業模式。

荷蘭 CFLW 的創始人 Mark van Staalduinen 博士，基於其在亞洲，尤其是新加坡的工作經驗，提出了亞洲市場需要基於長期互惠合作的策略，以促進資安產業的持續發展。CFLW 的策略洞察力能夠支持政策制定者制定有效的防禦策略，而營運視角則為執法人員提供先進的技術，推動更安全的網路空間發展。

因此，本次訪團行前與 CFLW 展開了多次討論，探索臺荷雙邊的可行合作模式，最終形成「臺荷資訊安全聯盟」的合作備忘錄簽署共識。聯盟形成的主要目的是建立一個涵蓋產業、政府、學術和研究的合作平台，促進共同研發資安技術，並且在亞太地區和歐洲市場上共同推廣這些技術，推動台荷日益重要的隱私保護和數位安全領域中，建立相互信任的基礎，進行深層次的技術交流與協作。

「臺荷資訊安全聯盟」簽署儀式由荷蘭的 CFLW、HSD、Keypasco Europe，以及臺灣的來毅數位、池安量子、振生半導體、幻雲資訊和圖靈 5 家資安企業進行簽署。合作備忘錄的簽署只是台荷雙邊合作的第一步，未來雙方合作接下來預計透過網路研討會、面對面會議和技術展示等多種形式，持續推動合作的深化。並規劃雙方也將共同申請臺灣與歐盟的補助計畫，進一步強化雙邊資安技術的研發與推廣。

圖 27「臺荷資訊安全聯盟」的合作備忘錄簽署儀式圖組
資料來源：現場拍攝提供

五、10 月 1 日(二) 晚上 參與 International Cyber Business Event

(一) 會議資訊

1. 地點：Leonardo Royal Hotel Den Haag Promenande
2. 時間：18:00 - 20:00
3. 主辦單位：海牙市政府

(二) 活動說明

International Cyber Business Event 是一場在荷蘭 ONE Conference 期間舉辦的國際資安交流活動之一，旨在促進全球資安企業、政府機構及學術界之間的合作與交流。活動的主要目的是促進資安領域的商業合作，並為國際企業提供一個與潛在合作夥伴進行直接對話和商業媒合的機會。透過一對一的洽談、展示創新技術和分享專業知識，參與者可以了解最新的資訊安全趨勢，並尋找全球市場中的商業機會。

對於參與者而言，有機會展示其資安技術，還能與來自世界各地的合作夥伴進行交流互動，促進潛在的跨國商機合作。此活動將協助參與之企業進一步開拓全球市場，增強在國際資安領域的競爭力，並加強與全球資安社群的聯繫，從而促進資安技術的創新與發展。

在今年的 ONE International Cyber Business Event 中，本署首次參與籌設臺灣展位（Taiwan Stand），並帶領臺灣資安業者共同以國家隊的形式參加此活動。會場中播放臺灣 SECPAAS 資安整合服務平台(Security Platform as a Service)的介紹影片，展示了在資安服務平台上一站式的資源支持。此外，臺灣展位結合了科技創新展示與臺灣特色美食，營造出輕鬆的氛圍，吸引了眾多與會者前來交流，成功促進了與其他國際資安夥伴的互動。

整體來看，這次設置的臺灣展位宣傳效果良好，不僅提升了臺灣資安技術在國際上的能見度，也讓臺灣業者有機會與包括

ICTU Foundation 在內的歐洲機構進行深入合作的討論，為未來臺灣資安業者進軍歐洲市場建立初步基礎。

圖 28 臺灣展攤於活動中展示圖組
資料來源：現場拍攝提供

六、10 月 2 日(三) 參加 Cyber Security & Cloud Expo 2024

(一) 展會地點：RAI 國際會議中心, Amsterdam

(二) 展會介紹

Cyber Security & Cloud Expo Europe 2024 是歐洲最大的資安與雲端技術展覽之一，由 TECHEX 主辦，吸引了來自全球的資安專家、技術供應商及企業代表。此次展會的主題聚焦於四個核心技術領域，包括網路安全、雲端運算、物聯網(IoT)和大數據分析， 2024 年的主題著重探討如何透過整合這些技術來加強企業的資安防護，提升數據管理效率，並推動業界技術創新。

今年展會的亮點之一是針對企業應對新興資安威脅的討論。特別關注如何應對越來越複雜的網路攻擊，並強調混合雲環境中的數據安全性。展會還聚焦於如何運用 AI 和機器學習技術來提升資安防護，幫助企業主動偵測威脅並快速回應，保障企業在雲端與物聯網架構中的數據安全。

另一個主要焦點是雲端技術的最新發展，特別是在企業轉向混合雲環境時如何確保雲端資安的最佳實踐。會議期間，許多專家分享了他們在混合雲、零信任架構及自動化資安防護方面的應用經驗，強調企業應如何在加速數位轉型的同時，確保其網路和數據免受外部威脅。同時，展會也探討了物聯網安全的挑戰，展示了許多 IoT 設備管理的創新解決方案，強調如何應對分散式物聯網環境中的資安風險。這些討論對於計畫進入物聯網領域或目前正在擴展 IoT 應用的企業，提供實務建議與技術參考。

(三) 展會展攤參訪

2024 年 Cyber Security & Cloud Expo 吸引了多家全球知名的資安公司參展，各家廠商針對本年度的資安主流趨勢，展示了其最新的技術創新與解決方案。以下是部分參訪之場攤的主軸和亮點說明：

1. F5：F5 以其領導地位的 Web 應用與 API 保護解決方案在市場上享有盛譽。今年展會 F5 著重展示其新一代的應用程式安全與 API 保護平台，與 F5 洽談時，該業者強調如何透過其智能化的解決方案來應對日益複雜的應用層攻擊。另 F5 專注於提供整合性高的解決方案，確保企業能夠快速反應網路威脅，保護其關鍵的網路應用和 API 安全。
2. Perforce： Perforce 強調其針對高風險應用的 DevOps 解決方案，幫助企業加快技術交付的速度，同時提升資安合規性。洽談時，Perforce 展示了其創新的 DevOps 工具鏈管理方案，尤其是針對企業在開發過程中的安全性需求，協助組織實現更穩定的應用開發與部署。Perforce 專為複雜的技術挑戰而設計，並且已經受到眾多全球領先企業的採用。
3. ING：ING 作為全球金融服務領導者之一，在展會中展示了其針對金融科技應用的資安解決方案。今年 ING 的主軸聚焦於如何透過大規模應用技術來提升客戶體驗，特別是如何通過資安技術保護金融交易的安全性。洽談時，ING 進一步展示了其為 40 多個國家的客戶提供的資安防護技術，特別強調其數據保護和交易安全的解決方案。
4. Tenable：Tenable 在今年展會專注於其資產暴露管理平台的擴展，以為幫助企業全面瞭解並減少其網路風險。參訪時，Tenable 展示了其針對數位資產的全方位保護技術，特別是在多元計算平臺上如何有效管理漏洞。另作為 Nessus 的創建者，Tenable 展現了其在全球市場的領導地位，並強調其如何利用該技術來保護全球 43,000 多家企業免受網路攻擊。
5. IBM：IBM 今年的展出主軸是結合 AI 技術來達成企業的可持續發展目標，特別是透過數據和 AI 技術來強化資安防護。IBM 在展會上展示了其 AI 資安解決方案，洽談時，IBM 特別著重

於如何透過混合雲環境中的安全管理來保護企業的數據和身分識別。IBM 還強調其全球資安服務，並展出最新的企業數據保護技術，幫助企業同時管理財務與聲譽風險。

6. Globalstar：Globalstar 以其衛星通信服務聞名，今年展會展示了其最新的 IoT 硬體與軟體產品，這些產品能夠即時追蹤並監控資產，為消費者、企業和政府提供最安全的數據傳輸方案。與 Globalstar 洽談時，該業者強調其 LEOS 衛星技術，展示了如何在偏遠地區提供可靠的數據連接與保護，特別適用於需要安全通訊和數據傳輸的行業。
7. AAEON：作為全球領先的工業與嵌入式計算平台製造商，AAEON 今年專注於展示其智慧城市和工業 4.0 解決方案。洽談時，AAEON 展出了多款搭載 AI 技術的嵌入式系統與物聯網平台，並強調其針對智能工廠與自動化系統的資安應用。這些解決方案不僅能保護實體設備，還能保障數據傳輸的安全性。
8. Cloudflare：Cloudflare 作為全球領先的連接雲公司，在今年的展會上展示了其最新的網路加速與保護平台。此次展出的重點在於 Cloudflare 如何幫助企業透過統一的雲端原生產品和開發工具來保護其員工、應用程式和網路。洽談時，Cloudflare 強調其全球最強大的網際網路，展示其如何每日攔截數十億的威脅，保護來自世界各地的企業與組織。
9. Palo Alto Networks：Palo Alto Networks 是全球資安領導者之一，在本屆展會中展示了其最新的雲端資安技術。洽談時，該業者強調其在 AI、分析、以及自動化資安防護領域的創新，並展示了如何通過整合平台來保護跨雲、網絡及行動設備的企業資產，並分享其全球成功案例。

(四) 參訪小結

此次參訪 Cyber Security & Cloud Expo 2024 了解到這個展會參與對象，進而評估與歐洲潛在買家連結的機會。透過拜訪參展廠商，可讓資安業者可以了解全球資安技術的發展趨勢，並與歐洲市場的主要參與者建立聯繫，讓臺灣廠商有機會與全球主要資安品牌，如 F5、Palo Alto Networks、IBM 等大廠，除可提升了臺灣資安業者的國際知名度，有助於增強品牌的加值效果，另可讓臺灣業者能研議有效推進在歐洲市場的佈局，為未來的商業合作與市場拓展奠定了基礎。未來，將研議臺灣業者持續參與此類國際展會之可行性，以進一步提升在全球資安市場的影響力。

七、10 月 3 日（四）上午 參加 2024 DTX Expo London：

(一) 展會地點： ExCeL London, Royal Victoria Dock, 1 Western Gateway

(二) 展會介紹：

DTX Expo 為歐洲最大的數位轉型展會活動。自 2005 年開始辦理，邀請國際專家來提供正確的見解、及解決方案、發展創新及精確策略來幫助全球超過 150,000 多名 IT 專業人員。

DTX London 匯集並展示當今組織推動變革和創造價值所需的創意思維、技術專家和最新工具。無論在探索新的 IT 解決方案來執行組織的數位策略、制定應對下一次大型網路攻擊的計劃，還是對正在改變遊戲規則的新技術感到好奇，參加這個活動都將會受到更多啟發並獲得更多資訊。2024 年主題包括網路安全、雲端運算、人工智慧和數位轉型策略。

表 1 DTX London2024 主題列表

主題	說明
Cloud and Infrastructure	Addressing strategies for modernizing IT tools and maximizing legacy infrastructure to reduce tech debt.
Cyber Security	Tackling real-time threats and building secure ecosystems that protect operational continuity.
Data, AI, and Automation	Exploring AI use cases, effective governance, and architecture for responsible data management and automation.
Software Engineering and DevOps	Innovating software delivery practices and improving developer experience (DevX).
IT Service Management and Digital Workplace	Streamlining IT service desks and enhancing communication tools for both internal and customer-facing teams.

資料來源：DTX London 2024 官網：https://www.dtxevents.io/

表 2 DTX London2024 參觀廠商列表

廠商名稱與攤位號碼	中英文簡介
SenseOn (Stand: B-24)	SenseOn provides AI-powered cyber security solutions, essential for protecting smart city infrastructure and digital networks. SenseOn 提供 AI 驅動的網絡安全解決方案，對保護智慧城市基礎設施和數位網路至關重要。
BR One (Stand: F-22)	BR One offers change management services in technology, helping smart cities evolve through efficient project management. BR One 提供技術領域的變革管理服務，通過高效的項目管理幫助智慧城市發展。
BT Group (Stand: H-12)	BT Group offers telecom and networking services that form the backbone of urban digital transformation and smart city development. BT 集團提供電信和網路服務，構成城市數位轉型和智慧城市發展的骨幹。
Oracle (Stand: I-50)	Oracle is a leader in cloud infrastructure, offering solutions that support scalable and secure smart city technologies. 甲骨文在雲基礎設施方面領先，提供支持可擴展且安全的智慧城市技術的解決方案。
Cisco (Stand: K-70)	Cisco provides networking hardware and software solutions, integral to smart city infrastructure and digital transformation. Cisco 提供網路硬體或軟體解決方案，是智慧城市基礎設施和數位轉型的核心。

資料來源：自行整理

(三) 展會展攤參訪重點

1. DTX London 2024 年的主要議題涵蓋網路安全、雲端運算、人工智慧以及數位轉型策略。各廠商展出的技術亮點如下：SolarWind 的操作平台包括伺服器安裝、防火牆配置，並透過可自訂的警報系統監控網路運作狀況；Qlink 則展示了類似

ChatGPT 機制的生成式人工智慧(GenAI)，但其平台專注於處理私人資料，而非公開資訊，適用於高度重視個人資料保護的行業，如高等教育或金融機構。

2. DTX AI 專題演講著重於人工智慧技術在公共和私營部門的廣泛應用，並探討了安全性、偏見及全面測試的必要性等相關挑戰。演講強調了制定政策以確保人工智慧技術能夠負責任且有效部署的重要性，特別針對公共部門的應用進行討論。此外，演講還反思了人工智慧快速發展對產業的變革潛力，以及其可能帶來的社會影響，尤其是在如何確保系統安全與公正方面的關切。

(四) 參訪小結

DTX London 2024 展覽內容種類較單純，會依據展示類別分區分色，讓參訪者依據欲交流主題，較易找到合適參訪之展攤。另各展攤多有搭配實體展示說明，比較容易了解展攤技術內容。

在參訪 DTX 之展攤或是專題演講，如何搭配 AI 技術在歐洲國家是個重要議題，如未來參加歐洲展會時，可建議參展業者除展示原本自家技術外，另凸顯應用 AI 技術之面向，可吸引更多國外業者拜訪，增加商機交流機會。

圖 29 DTX London 廠商攤位參訪

資料來源：現場拍攝提供

圖 30 DTX London 會場側影

資料來源：現場拍攝提供

圖 31 DTX London 主舞台主題演講

資料來源：現場拍攝提供

八、10 月 3 日（四）下午 拜會 Innovate UK 及 CPC：

(一) 拜會地點： One Sekforde Street, London

(二) Innovate UK 單位介紹：

1. 英國研究創新局(United Kingdom Research and Innovation，簡稱 UKRI)負責指導英國科學研究預算與創新資金，所轄的 9 個組織中，英國創新局(Innovate UK)的主要任務為支持商業導向的創新研究，透過開發新產品、流程以及服務與商業化策略協助企業成長，促進更具包容性的創新生態系統。
2. 英國 Innovate UK 創立於 2018 年，是一個旨在促進創新、支持企業發展並解決社會挑戰的政府機構。在智慧城市領域，Innovate UK 扮演著推動技術創新、改善城市生活品質的角色。

表 3 Innovate UK 討論要點參考

討論方向	要點建議
Innovate UK 推動領域與其資金補助機制、範疇，能如何支持當地業者推動技術與創新之作法	•Innovate UK 相關數位化推動計畫推動領域如下: ■ 淨零(Net Zero) ■ 數位與技術(Digital and Technologies) ■ 健康生活 (Healthy Living) •上述領域在補助規劃上，是否設有補助資金適用範疇、場域大小規模，以及提案業者加分等事項?另是否有提案之英方業者與國外業者合作之標竿案例?
Innovate UK 與數發部數產署在產業領域推動計畫的潛在合作方向	•在產業合作領域如 Smart Transportation, Agriculture, Healthcare, AI, Cybersecurity….etc.)，相關延伸的商業機會為實場落地還是技術研發? 請益可以具體合作的模式。 •如何引入臺灣廠商的能量共同進行合作?
臺灣廠商如何參與至 Innovate UK 的推動項目	•國外廠商是否有能進行技術轉移或於當地進行與當地業者合作模式？

討論方向	要點建議
	•如何有恰當的合作機制，用以促進當地產業升級並帶來海外廠商技術交流的機會?

資料來源：自行整理

(三) CPC 單位介紹：

1. Connected Places Catapult (CPC)創立於 2019 年，Catapult 是由英國研究創新局(UKRI)成立的創新推動中心，扮演中介機構的角色以促進特定領域研究成果商業化，旗下 9 個中心中，Connected Places Catapult(CPC)是負責推動加速英國城市、交通和場域發展的組織，推動範圍包括提升地方領導地位、房舍與生活、共通基礎設施、陸海空交通與機場、海運港口、鐵路和車站等商業化發展。
2. Connected Places Catapult 主要為公共機構、企業和基礎設施提供公正的「創新服務」，催化加速改善城市民眾在居住、工作和通勤旅行等便利性，CPC 連結企業和公共部門領導者及尖端研究，藉此激發創新並開拓新市場。CPC 也運營技術示範場域及中小企業加速器，推動開發“以人為中心”，並擴展能提升經濟成長、傳播繁榮並減少碳排之創新解決方案。

表 4 CPC 討論要點參考

討論方向	要點建議
探詢 CPC 今年3月來臺參訪後，其有興趣的智慧應用服務或臺灣業者	•參觀臺灣場域後，針對如智慧城市與智慧交通等應用，CPC 是否有讓臺灣業者參與實際應用規劃或政策資源投入的合作建議，作為我方規劃參考？ •還有哪些領域 CPC 認為具備潛力能進行進一步深化合作？
建議臺灣廠商參與未來實際應用規劃，請益相關	•在未來政策投入的重點合作領域中，是否已有具體的領域或專案可以引介臺灣廠商?

討論方向	要點建議
資源與投入的合作方式	•臺灣廠商應如何在上述機會中，達到資源共享或有效的投入的特定合作模式？
參與支持與國際合作夥伴的合作，在大企業的帶領下，促進雙方中小企業(SMEs)的相關計畫。	•過往如CPC 與 Siemens Mobility 合作或CPC與 BT (British Telecom) 的 5G 協作，用以大帶小的合作方式支持當地中小企業(SMEs)的示範點計畫與加速器計畫(Arup 和 Mott MacDonald)等，幫助中小企業透過與大型企業的協作，資源會如何提供? •目前臺灣技術處(Industrial Development Bureau, IDB)與 CPC 進行協作， 數產署在數位領域可進行相關合作項目?

資料來源：自行整理

(四) 討論摘要：

1. Innovate UK 的使命是支持以企業為主導的創新發展，通過新產品及技術的商業化，協助英國各公司在未來的成長。執行的重要計劃項目包括創新貸款機制及對投資者合作夥伴關係，以利當地促進私人投資，並幫助企業擴展規模，優先關注的領域如淨零碳排放、健康生活及數位技術等。會議中更強調 AI 和綠色智慧城市合作項目的應用，並提及過往有超過 50 家英國公司訪問臺灣。
2. CPC 加速器中心一直以來聚焦於智慧城市的發展應用及城市公共基礎設施的數位創新，會議中舉例如 Bristol Temple Meads 火車站等合作項目中，使用數位雙生(Digital Twin)進行預測性的技術維護和相關能源使用上能如何更優化。另 CPC 的加速器計畫支持中小企業(SMEs)將技術推向市場，其中包括應對社會和技術挑戰的氣候韌性等項目的示範演示。
3. Innovate UK 與 CPC 經本次拜訪後，對於臺方業者的解決方案已有了解，惟現英國推動之數位創新計畫與方案，都已在進行

中，後續有適合專案將會研議臺灣參與機會，合作方式包含雙城對接方式，針對城市在推動數位轉型時所遭遇之問題，找尋臺灣業者提供解決智慧方案，但業者必需於英國設立公司。

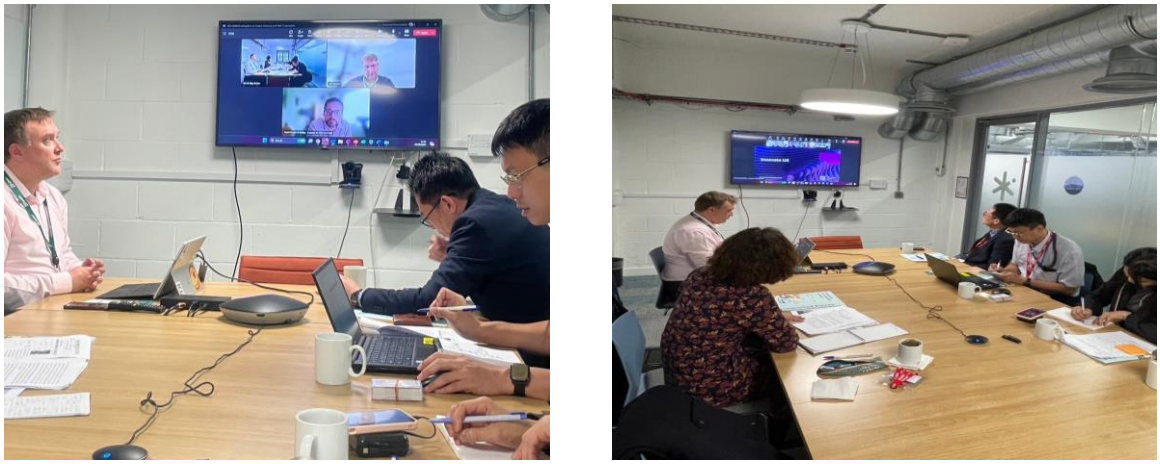


圖 32 Innovate UK 會議討論
資料來源：現場拍攝提供

圖 33 Innovate UK 會議討論
資料來源：現場拍攝提供

圖 34 CPC 會議後大合影
資料來源：現場拍攝提供

九、10 月 4 日（五）上午 辦理歐銀工作會議：

(一) 會議地點： Five Bank Street, London（歐銀倫敦總部）

(二) 歐洲復興開發銀行介紹：

1. 歐洲復興開發銀行((European Bank for Reconstruction and Development, EBRD)成立於 1991 年，總部位於英國倫敦，為歐洲區域性開發援助機構，其成立宗旨在協助中東歐及獨立國協國家由計畫經濟轉型為市場經濟，提升國家競爭力，邁向民主多元政治社會。
2. 歐銀計有 73 個成員，臺灣以特別觀察員身分參與理事會年會。財政部自 2006 年起派員赴歐銀貿易促進計畫處(Trade Facilitation Programme, TCP)工作，以利國際金融事務經驗交流，並積極協助我國廠商充分掌握歐銀釋出商機。
3. 歐銀於 2022 年成立數位轉型中心(Digital hub)，係協助受援國政府及民間奠定數位轉型基礎，包括法律規範、監管和體制框架，並建設基礎設施。旨在協助歐銀內部及受援國提升數位涵養，透過數位轉型作為提升各產業領域經濟發展之啟動引擎(enabler)。

表 5 EBRD 討論要點參考

討論方向	要點建議
數位轉型顧問計畫推動進度	•目前已推薦臺灣廠商擔任轉型計畫之顧問，是否有其他計畫或想合作的領域業者？可再協助找尋臺灣廠商參與。 •透過介紹我方簡報臺灣業者，並請益數位轉型顧問推動計畫參與的方式。
歐銀「數位成熟度評估方法」推動進度與合作討論	•分享目前規劃「數位成熟度評估方法」的進度，討論歐銀所使用的數位成熟度評估方法和指標，以及這些標準如何適應各市場的需求? •相關的評估模型如何讓臺灣業者加入合作模式，尋求可能的調整和改進方向?
其他議題分享	•是否有其他領域與項目能進行更多臺英合作，包括聯合研究、項目合作或專家顧問交流。

討論方向	要點建議
	•歐銀提出分享 AI Report 請我方參考

資料來源：自行整理

(三) 討論摘要：

1. 數位轉型策略

歐銀已將數位轉型策略訂為未來五年的發展重點，策略的核心在於透過數位化達成其他目標，特別是在連接性、企業適應和創新等領域方面發揮作用。會議上提及的議題包括智慧城市計畫、數位成熟度評估方法及 AI 整合，有助於發展與改善受援國等地區之相關計畫的成果。

2. 數位成熟度評估方法推動進展

數位成熟度評估方法已應用在多國進行試點計畫(Pilot Programs)。相關的試點計畫幫助確定各國的基礎設施及數位素養等關鍵因素的重要性，上述因素會影響各國在發展數位項目的成功與否。利用該方法學來分析各國的基礎設施及數位應用需求，如分析出該地區易淹水地區，如何應用數位來解決，促使防洪和水資源管理系統納入未來城市數位轉型項目的提案中。惟數位成熟度評估方法學是以個案專案組成專家群處理評估，目前並無有標準作業或技術文稿可供參考。

3. 其他議題交流與分享

(1) 我方簡介數位產業發展、專長領域、及案例，歐銀表達了解臺灣產業能量，如有相關需求將進一步聯繫並請我方推薦適合之公司或解決方案。

(2) 歐銀分享AI如何提升內部決策效率及針對計畫項目如何擁有影響力。至於所衍生出的 AI 風險，例如資料偏差、透明度不足及訓練 AI 模型所需的能耗問題，也被題提出作為討論；同時，歐銀在整合 AI 時，涉及到監管挑戰和策略風險也是未來

須注意的方向，如下說明：

- 策略風險：AI 的發展可能導致工作機會流失，且培訓模型所需的能源消耗對環境造成的影響不容忽視。此外，歷史數據中存在的系統偏見也可能在 AI 應用中持續延續。因此，如何謹慎管理 AI 的應用方式至關重要。目前，全球各國正積極制定相關的監管框架，美國、加拿大、中國等國的不同標準以及歐盟的《人工智慧法案》將成為重要的參考依據。
- 新興市場的機會：AI 在新興市場展現出突破既有技術的潛力，透過行動技術的普及性，協助達成與這些國家的經濟發展目標。目前相關市場仍面臨基礎設施不足、專業人才短缺及低品質資料集的挑戰，未來有望可推動如農業、能源、交通等多個領域的發展。
- 監管與治理：針對不同產業需求，應制定相應的監管制度以促進 AI 應用的發展。對於發展中國家而言，制定監管框架及投資支援技術（如資料數據中心及技能培訓）顯得重要，以確保其能夠有效利用相關技術。
- 銀行在 AI 中的角色：世界銀行、亞洲開發銀行及非洲開發銀行等國際開發銀行，已積極參與人工智慧驅動的項目，涵蓋交通、安全、家庭暴力應變及農業等領域。目前，這些機構正在加大對 AI 的投資，包括對 AI 企業的股權投資及基礎設施的支援。

(3) 後續合作機會：

- 數位轉型支援計畫(DTSP)：歐銀評估擴大在各國的試點計畫(Pilot Programs)和數位轉型支援計畫(DTSP)，後續可持續引介有量能的業者。並於下次工作會議追蹤推薦的業者進度，持續評估適合專案將會邀請業者納入轉型計畫之顧問團。

- AI 轉型計畫：目前歐銀之說明僅為初步規劃階段，尚未有實質推動轉型計畫，將持續洽歐銀之需求，找尋臺灣 AI 業者合作機會。

圖 35 EBRD 會議討論

資料來源：現場拍攝提供

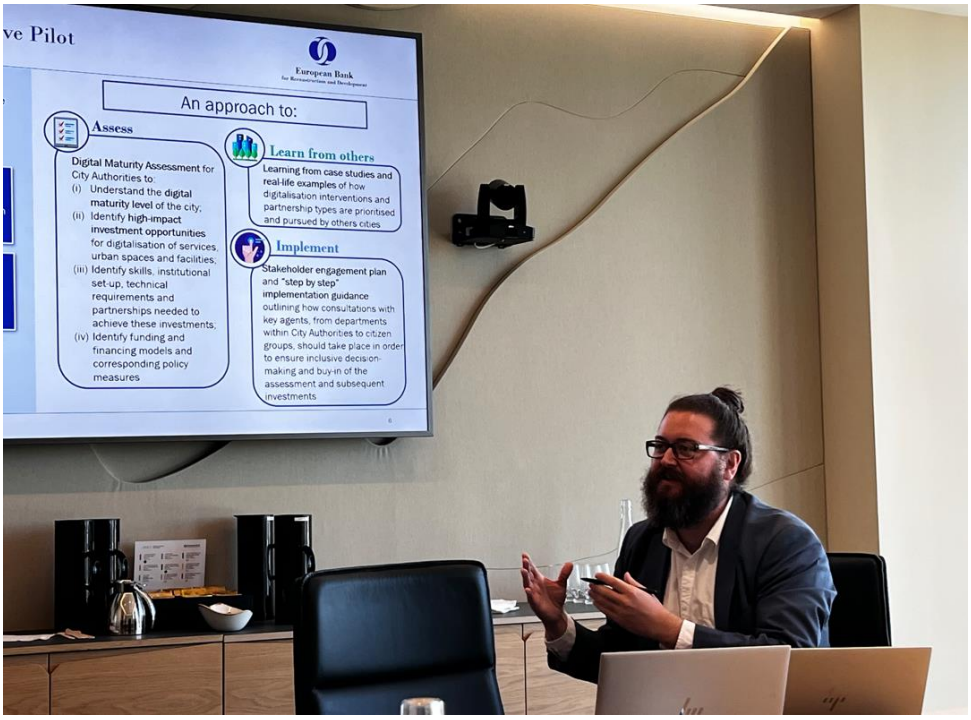


圖 36 EBRD 會議-數位成熟度評估方法討論

資料來源：現場拍攝提供

圖 37 EBRD 會後大合影

資料來源：現場拍攝提供

圖 38 EBRD 會後贈禮臺英雙方代表合影

資料來源：現場拍攝提供

圖 39 EBRD 門口大合影

資料來源：現場拍攝提供

十、10 月 4 日（五）下午參觀 FRAMELESS

Immersive Art Experience 展覽：

(一) 展覽地點： 6 Marble Arch, London

(二) 展覽說明：

1. Frameless 沉浸式藝術體驗是一場結合藝術與科技的創新展覽，位於倫敦市中心，將觀眾引入完全沉浸的環境中，重新詮釋知名的藝術作品。透過多維度的投影技術和互動元素，Frameless 將經典與當代藝術傑作轉化為充滿視覺、聽覺及觸覺等多感官的體驗。
2. 展覽以當前科技作為亮點，融合生成式 AI 技術與全球首創的沉浸式投影、互動裝置及雷射聲光效果場域，打破多人即時互動生成 AI 技術的限制。
3. 四大主題展區介紹：

(1)Beyond Reality 簡介：這個展區著重於超現實主義及抽象藝術，將現實重新想像並加以扭曲，帶領觀眾進入如夢似幻的異世界環境。觀眾將會看到來自薩爾瓦多·達利、勒內·馬格利特等超現實主義大師的作品，透過沉浸式的數位投影技術呈現。這個展區的目的是激發觀眾的驚奇感，讓物體看似打破物理法則與邏輯規範，探索一個充滿無限想像力的宇宙。

- 技術應用:
  - 高解析度的數位投影技術，將經典藝術作品轉化為動態、互動的視覺體驗。
  - 利用感應技術追蹤觀眾的移動，讓他們可以從不同角度觀看超現實作品的變化。
  - 3D 影像技術製作的場景讓參與者宛如置身於藝術品的異想空間中。

- 參觀重點：可以隨著自身的移動改變作品中的視角，感受到作品中不同的物體和元素以不符合物理規律的方式變形。在某些區域，者可以使用手勢或移動來觸發特定的視覺效果，例如改變顏色、形狀或觸發動畫效果，讓展區更具互動性。

(2) Colour in Motion 簡介：此展區專注於色彩的探索及其對情感的影響，呈現強調色彩與動態的視覺構圖。來自克勞德·莫內、梵谷及瓦西里·康丁斯基等藝術家的作品，透過流動的投影技術生動再現，將觀眾帶入一個色彩不斷變化與轉換的世界。觀眾將親身體驗到藝術家如何運用色彩的不同色調來喚起情緒、能量與氛圍。

- 技術應用:
  - 動態投影技術將色彩和光線結合，以動態形式呈現藝術品中的色彩變化。
  - 感應技術追蹤參與者的注視點和動作，調整色彩的變化與流動，提供即時互動的體驗。
  - AR 技術讓參與者能透過手持設備或穿戴裝置，與展區內的色彩動態互動。
- 參觀重點：可以通過移動或觸摸屏幕來改變展區中的色彩組合，體驗藝術家如何使用色彩來影響情感和氛圍，例如為牆面上的投影“上色”，並觀察不同色彩如何隨時間流動變化。

(3) The World Around Us 簡介：這個展區帶領觀眾進行一場視覺之旅，探索各種自然景觀、建築奇觀及風景名勝，捕捉世界的美麗。從 J.M.W.透納的壯麗自然景色到古斯塔夫·克林姆特的精細城市景觀，展區透過數位投影技術及環繞音效，

將觀眾帶到不同的時代與地點。不論是寧靜的森林還是繁華的大都市，觀眾都能在這裡感受到身歷其境的視覺盛宴。

- 技術應用:
  - 環繞式 360 度投影技術，創造出逼真的自然和城市景觀環境。
  - 結合擬真音效系統，讓參與者不僅能看到，還能聽到場景中的自然聲音，增加沉浸感。
  - 利用高解析度的數位重建技術，將各種名勝古蹟和自然奇觀栩栩如生地展現出來。
- 參觀重點: 走進模擬自然景觀和城市環境，感受到如同置身不同時空的感覺; 一些區域讓參與者可以透過互動裝置調整場景的時間和天氣變化，例如從白天變為夜晚或從晴天變為雨天，體驗不一樣的視覺與聽覺效果。

(4) The Art of Abstraction 簡介：這個展區專注於抽象藝術，讚頌那些脫離具象形式的藝術運動。觀眾將看到來自皮特·蒙德里安、卡濟米爾·馬列維奇及傑克遜·波洛克等藝術家的作品，這些作品透過形狀、線條與色彩，傳達超越字面意義的情感與想法。沉浸式的展覽設置讓觀眾能夠步入這些抽象構圖中，親身感受作品中的韻律、平衡與張力，在不斷變化的視覺空間中探索。

- 技術應用:
  - 動態投影技術讓觀眾可以進入抽象藝術世界，透過不斷變化的形狀和顏色感受藝術的情感傳遞。
  - 使用感應技術，觀察觀眾的移動，改變展廳中投影的構圖與色彩。
  - VR (虛擬實境) 技術，讓參與者能夠“進入”抽象藝術世界，親自探索藝術家的構圖。

- 參觀重點: 通過互動來改變投影的色彩、形狀和線條，親身參與抽象藝術創作的過程，並使用 VR 裝置，參與者可以走入藝術作品，感受抽象世界的立體感和動態變化，進一步了解作品背後的創作思路。

(三) 參訪小結：

該場域以跳脫過去傳統美術靜態展覽方式，利用科技體感設備增加與參觀者之互動，來增加民眾參訪之興趣，其分析利用之技術說明如下：

1. 高解析度投影技術

使用了 Panasonic 3-Chip DLP 雷射投影機，透過 4K 解析度技術，以極高的像素密度（479 百萬像素）將藝術作品以360度的方式呈現。這種技術讓觀眾仿佛置身於作品中，與藝術融為一體。參與者可以在大空間中自由移動，隨著不同角度的視角變化，感受藝術作品的每一個細節。

2. 互動式投影與動態追蹤技術

動態追蹤技術，讓觀眾能通過手勢或身體動作與數位藝術進行互動。例如，參與者可以用手或身體在空中揮舞，藝術作品會根據他們的動作進行即時變化和反應，讓每個人都能創造出屬於自己的藝術印記。

3. 鏡面投影技術

將投影包裹在鏡面箔片中，創造出無限的視覺效果。六面投影結合鏡面技術讓參與者感覺置身於一個無限延展的抽象藝術空間中，這種沉浸式的體驗讓觀眾感到自己成為藝術的一部分。

4. 聲光同步與 3D 音效

聲音與視覺效果的精準同步也是 Frameless 的一大特色。158個環繞聲喇叭構建了完整的 3D 音效，讓每個房間都

擁有獨特的聲音設計，觀眾的聽覺和視覺體驗相輔相成。例如，觀眾在欣賞畫作時，會聽到與畫作情境和氛圍相匹配的音樂或音效，這種多感官的技術增強了藝術的情感衝擊力。

本署目前亦由相關計畫推動文化數位轉型之工作，透過實驗性技術開發與數位服務設計，結合新興數位技術，打造新文化或藝術的實驗場域，除讓民眾意識數位科技的重要性，提高民眾數位素養外，亦幫助科技業者透過落地民眾體驗與回饋，調整產品設備優化，進而加速產品商模化。該參訪場域可供後續推動文化與藝術展時，透過增加民眾科技體驗之操作模式，作為科技業者之創新商機。

圖 40 Frameless 展覽門口合影
資料來源：現場拍攝提供

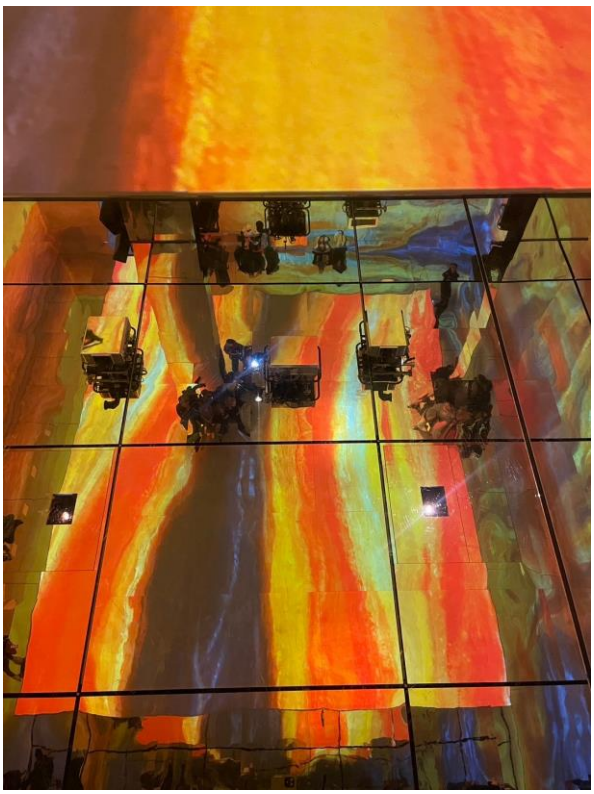


圖 41 Frameless 展覽展區內側影之一

資料來源：現場拍攝提供

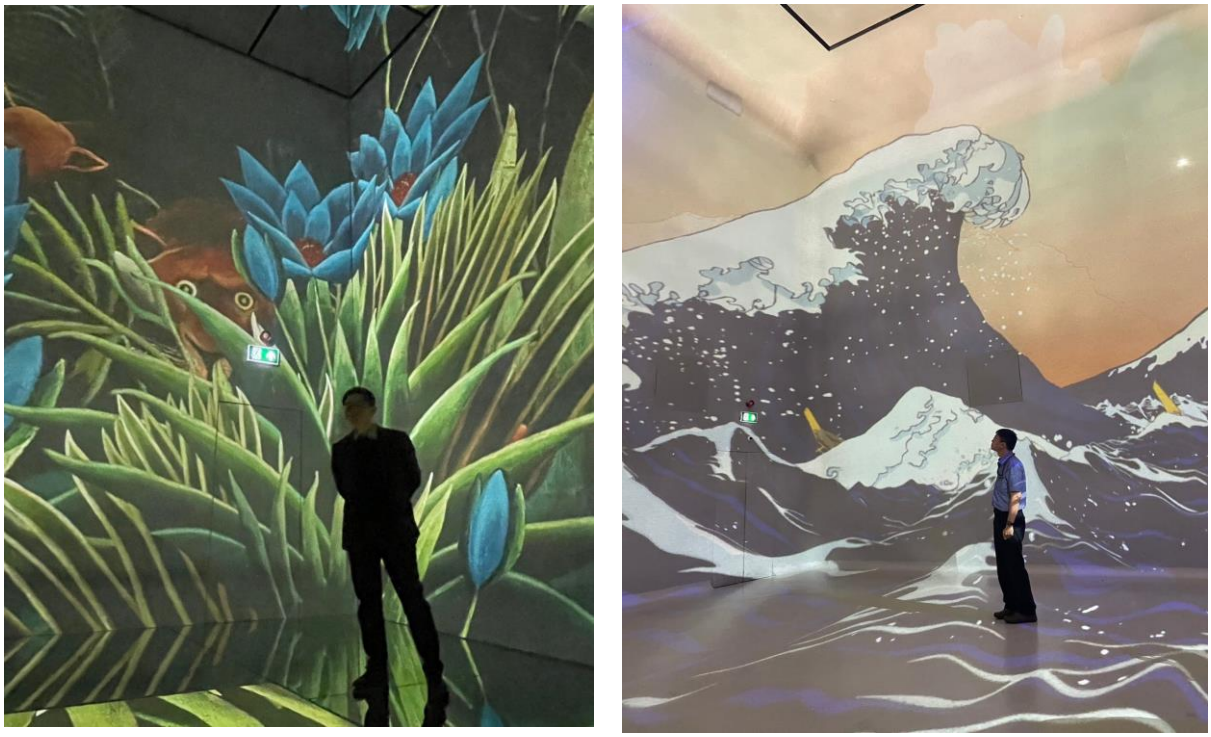


圖 42 Frameless 展覽展區內側影之二

資料來源：現場拍攝提供

伍、 結論

一、資安業者商機

本次參加荷蘭 ONE Conference 是此次訪團的核心之一。ONE Conference 是歐洲最重要的資安盛會之一，匯集了全球資安領域的專家、業者及學者，討論最新的技術趨勢與挑戰。本次訪團不僅參加論壇及專題討論，亦於展會週邊活動 International Business Event 設置臺灣展位（Taiwan Stand），展示臺灣資安產業的技術實力與創新潛力。透過這個國際平台，臺灣業者得以面向國際展示技術，進一步提升臺灣資安品牌實力。

另一重要行程是拜會海牙市政府資安長（CISO），會晤討論內容涵蓋邀請資安長參與臺灣 2025 HITCON CISO Summit，並探討臺灣白帽駭客團隊參加海牙知名的「Hack the Hague」活動的方式。透過高層次的官方交流加強國際合作網路，為未來雙邊技術與政策上的合作開創新契機。

此外，訪團還安排多場臺灣業者與潛在合作夥伴的商業交流活動，提供了一對一的媒合機會。臺灣業者藉此與來自歐洲的潛在合作夥伴進行洽談，包括由荷蘭 CFLW、HSD 等資安機構及臺灣 5 家資安廠商共同簽署合作備忘錄，討論合作的作法。未來預計將集中於資安技術的共同合作、產品市場擴展以及企業間的產品整合，為臺灣業者開啟更多的國際市場機會。

最後，透過考察 Cyber Security & Cloud Expo Europe 2024，評估其做為臺灣資安業者交流平台之一的可能性，讓臺灣業者不僅能夠展示技術，還能進一步推動其技術在歐洲市場的應用，創造更多商機。

二、英國與歐銀合作

本次訪團透過與英國創新局（Innovate UK）會議，討論雙邊合作的可能性，特別是在支持臺灣企業融入英國創新生態系統或產業合作

等專案方面，探討未來合作；與 CPC 會議則更了解英國在智慧城市與智慧交通方面的創新應用，希望強化臺灣企業進入當地市場、了解可行合作機會，CPC 亦分享支持中小型創新企業發展的重要性。後續將與 Innovate UK 及 CPC 探討研議英國在推動數位轉型計畫有關智慧城市基礎建設等領域的合作方式。並盤點臺灣具有技術能量之業者，評估投入計畫之可行性，以便協助臺灣業者快速進入英國市場。

在與歐銀工作會議除就數位成熟度指標、數位轉型顧問等議題交流討論外，歐銀亦分享區域夥伴關係和知識共享的重要性，持續專注受援國的基礎設施數位化計畫推動狀況，了解歐銀已在評估擴大在各國的試點計畫和數位轉型支援計畫，目前已有引介臺灣業者以專家身分參與歐銀數位轉型支援計畫，已獲得歐銀方初步肯定。

在 DTX London 展會，了解參展廠商在人工智慧(AI)、物聯網(IoT)及智慧城市應用等領域，數位化轉型技術與發展等最新趨勢，該展會上展示內容強調如何透過數位化與相關創新技術提升各企業競爭力。而 Frameless Immersive 展館則以當前科技與歷史、藝術、或文化結合，融合生成式 AI 技術與沉浸式投影、互動裝置，打造擁有全方位聽覺、視覺感受的雷射聲光效果場域。

陸、建議

一、 持續參與歐洲主要資安展會，讓臺灣資安業者技術與品牌受到歐洲市場關注，而 ONE Conference 是臺灣資安業者了解全球資安趨勢並推動技術與商業合作的理想平台，建議未來持續參與該會議及周邊活動，並進一步加強與歐洲市場的連結，推動臺灣資安技術進入歐洲。

二、 本次與海牙市政府資安長進行的會議進一步促成台荷雙方在資安領域的互動，雙方表達了對參與彼此資安活動的高度興趣，如荷蘭的 Hack the Hague 以及臺灣的 HITCON CISO Summit，這有望提升臺荷未來的技術交流與合作，促進臺灣的白帽駭客團隊在國際舞台上展現技術實力，並與荷蘭頂尖的資安團隊進行深度互動與合作。未來將評估臺灣團隊參與 Hack the Hague 活動，藉此展現臺灣資安技術實力，並與國際頂尖資安專家建立長期合作關係，並同步邀請荷蘭資安專家參加我國舉辦之HITCON CISO Summit，雙邊藉此分享技術經驗與資源。

三、 本次與歐銀會議洽談數位成熟度指標、數位轉型計畫議題進行討論與分享，目前已有引介臺灣業者參與歐銀數位轉型支援計畫專家團，建議後續除關切引介進度外，另協助業者提案適合之歐銀計畫專案。及持續引介有量能的業者目前已推薦探詢歐銀數位轉型支援計畫未來機會。