出國報告（出國類別：開會）

ONE Conference 資安研討會暨荷蘭資安生態系參訪

服務機關：數位發展部/數位產業署

姓名、職稱：莊裕智副組長

派赴國家/地區：荷蘭/海牙

出國期間：中華民國 112 年 9 月 30 日至 10 月 8 日

報告日期：中華民國 112 年 12 月 21 日

摘要

為推動臺灣資安產業在國際市場拓展，並強化臺灣與荷蘭及歐盟國家的合作關係，數產署特規劃此行，邀集資安院、資策會、工研院等法人團隊，並遴選出具國際發展潛力資安業者：指向科技、全景軟體、雷盾資安、來毅數位共 4 家業者共同訪荷。

荷蘭作為歐盟成員國之一，在歐洲資安領域有重要領先地位，且其素來與臺灣在資安領域交流熱絡，故藉此行持續深化合作面向。其重點拜會行程及目的摘要如下：

1. 觀摩海牙市政府主辦的"Hack the Hague"資安競賽，其允許駭客對市政府系統進行實際的滲透測試，臺灣或可考慮引進類似的競賽概念，加強國內對資訊安全的重視，培訓和發掘資安人才。
2. 鏈結荷蘭資安研究機構 Dcypher、恩荷芬科技大學等，未來可共同爭取歐盟研發計畫，將臺灣資安技術能量帶入歐洲市場。
3. 鏈結 HSD 等機構提供的落地軟硬資源，可以有效地推進臺灣資安業者落地發展。
4. 辦理臺灣資安廠商與荷蘭大廠 KPN 等媒合，加速歐洲商機拓展。
5. 參與 ONE Conference 及其週邊活動，協助臺灣資安業者了解荷蘭在地資源，利用 ONE Conference 平台曝光及建立合作夥伴網路等。

此次出訪荷蘭不僅推動臺灣資安產業國際化，同時亦以加強臺灣與荷蘭及歐盟地區合作為主軸。透過參與資安展會、與官方機構和企業的交流，以及商機拓展和媒合會議，期望實現資安政策、產業合作和應用技術方面的國際合作成果，進一步強化臺灣資安產業的國際競爭力。

目　　錄

圖目錄

表目錄

壹、 出國目的

為推動臺灣資安產業在國際市場拓展，並強化臺灣與荷蘭及歐盟國家的合作關係，數產署邀集資安院、資策會、工研院等法人團隊，並遴選四組具國際發展潛力之資安業者共同訪荷。荷蘭作為歐盟成員國之一，在歐洲資安領域有重要領先地位；且其素來與臺灣在資安領域交流熱絡，故借此行持續深化合作面向。

訪團重點行程之一，是參加在荷蘭舉辦的重要資安展會 ONE Conference，可為臺灣資安業者提供一個在國際舞台上展示技術和產品的機會，提高臺灣資安品牌知名度，並藉此與國際資安專家、國際產業合作夥伴進行深入交流。根據 Frost & Sullivan 於 2023 年 6 月的資料顯示，荷蘭每年在資安領域的支出持續攀升，預期於 2023 年達到 3 億 4 千 5 百萬歐元，顯示了政府及產業對於資安都高度重視，且有關資金與人才相關政策亦非常友善，而這也洽好是臺灣資安業者進入歐洲市場的重要契機。

另外，此行也安排拜會荷蘭官方資安組織和智庫，希汲取其在資安政策規劃和推動方面的寶貴經驗。荷蘭在資安立法和政策制定方面具有豐富經驗，特別注重保護數據隱私和網絡安全領域。這些經驗或能成為臺灣國家產業資安政策規劃和推動的重要參考。再者，荷蘭政府也積極整合資源鼓勵資安創新，臺灣資安業者也許能槓桿相關資源以加速在歐洲落地。

最後，訪團還將率領臺灣資安業者參與和荷蘭大廠商機拓展媒合交流會，旨在促進臺灣資安業者與荷蘭當地企業之間的商業合作。荷蘭是歐洲最大的資安市場之一，多元友善的國際貿易氛圍提供了大量的商機。此行另走訪了當地的產業生態聚落和產業發展園區，以發掘潛在的合作資源，並探索未來可互動互惠的機會，進一步帶動雙邊資安合作。

此次出訪荷蘭是以推動臺灣的資安產業國際化，同時加強臺灣與荷蘭及歐盟地區合作為主軸。透過參與資安展會、與官方機構和企業的交流，以及商機拓展和媒合會議，期望實現資安政策、產業合作和應用技術方面的國際合作成果，進一步強化臺灣資安產業的國際競爭力。

訪團成員

表 1 本署參訪人員名單

#	單位	姓名	職稱
1	數位發展部數位產業署	莊裕智	副組長

表 2 團隊參訪人員名單

#	單位	姓名	職稱
1	國家資通安全研究院	王家宜	主任
2	工業技術研究院	卓傳育	組長
3	工業技術研究院	何貞儀	專案經理
4	資訊工業策進會	蕭榮興	副主任
5	指向科技股份有限公司	黃文宏	副總
6	全景軟體股份有限公司	楊文和	總經理
7	雷盾資安股份有限公司	呂浩宸	執行長
8	來毅數位科技股份有限公司	林欣怡	總經理

行程表

表 3 行程表

日期	原定行程	所在地點	是否有異動
9/30- 10/1	臺灣桃園起飛/泰國曼谷轉機/抵達荷蘭阿姆斯特丹	臺灣桃園 荷蘭阿姆斯特丹	無差異
10/2	1. Security Delta (HSD)/Innovation Quarter 2. The Hague海牙市政府/Hack the Hague	荷蘭海牙	無差異
10/3	1. ONE Conference 2. National Cyber Security Center	荷蘭海牙	因訪團行程安排，變更為： 1. ONE Conference 2. ASML 3. Cyber Resilience Centre in Brainport Eindhoven 4. International Business Event
10/4	1. Innovation Quarter 2. Cyber Investor Day	荷蘭海牙	因訪團行程安排，變更為： 1. National Cyber Security Center(NCSC) 2. Dcypher
10/5	1. ASML 2. Cyber Resilience Centre in Brainport Eindhoven	荷蘭海牙	因訪團行程安排，變更為： 1. KPN 2. Cyber Investor Day
10/6	Dcypher	荷蘭海牙	因訪團行程安排，變更為： TU Eindhoven
10/7- 10/8	荷蘭阿姆斯特丹起飛/曼谷轉機/抵達臺灣桃園	荷蘭阿姆斯特丹 臺灣桃園	

貳、 工作內容

一、拜訪 Security Delta (HSD)及其上屬單位 Innovation Quarter

(一) 會議資料

- 日期：2023/10/2
- 時間：10:45-14:00
- 地點：Security Delta
- 荷蘭方與會者：Marijn Fraanje, Head of Economic department of the City of The Hague、Martijn van Hoogenhuijze & Philip Meijer Account Managers, Cyber Security InnovationQuarter、Joris den Bruinen Director, Security Delta
- 臺灣方與會者：全體訪團成員
- 其他出席者：2023 荷蘭資安周國際訪團，包括加拿大、瑞典、臺灣、法國、西班牙、德國及國際記者

(二) 議程

1. 歡迎致詞 by Marijn Fraanje
2. 簡報 1：Doing business in The Netherlands & the Dutch cybersecurity landscape by Martijn van Hoogenhuijze & Philip Meijer
3. 簡報 2：Introduction Security Delta (HSD), the Dutch Security Cluster by Joris den Bruinen

(三) 背景

本活動為 2023 荷蘭資安周的開場活動，邀請各國訪團及國際記者參加。除了介紹資安周的各項活動，包括：ONE Conference, 國際商業晚宴、歐洲投資人媒合等，也介紹荷蘭投資環境、資安產業現況及相關配套機制，促進國際合作及貿易往來。

(四) 重點摘要

1. 關於海牙

海牙市為荷蘭第三大城，中央政府、議會與外國使館皆坐落於此地，被稱為「國際和平及法治之都」 (International city of peace and justice)，為國際法院 (International court of justice)及國際常設仲裁法院 (Permanent Court of Arbitration)及許多國際組織的所在地，也因此間諜活動頻繁，例如 2018 年四月荷蘭情報機構成功遏阻一起俄國情報人員以禁止化學武器組織(OPCW)為目標的網路攻擊。

海牙市特重視資訊安全以保障重要國際組織的運作，因此 2013 年市議會決議成立海牙資安三角洲 Security Delta(HSD)，也與中央政府合作共同舉辦名為 ONE Conference 的年度國家資安會議。Security Delta 成立的宗旨在於維護

和平，讓城市，國家更具有資安韌性，而非增加對於資安的恐懼。達到此目標的三個要素為：

(1) 合作：貿易是建立在三螺旋 (Triple Helix)的產官學合作機制，以及國家/地方/組織層級的通力合作。

(2) 知識及創新：知識是創新的基礎：沒有任何一家單一資安公司的產品和服務可以解決全部的問題，需要大家合作。

(3) 建立長期合作：跨國層級合作，例如協助加拿大及西班牙公司在荷蘭設點參與當地活動；在瑞典從事研發合作；與臺灣的工研院、荷蘭在台辦事處及臺北駐荷蘭辦事處有多年的合作，並透過軟著陸計畫 (soft-landing program)協助臺灣公司在荷蘭設點。

同時，因為荷蘭具備活躍的白帽駭客社群，海牙市政府於 2017 年起，舉辦第一屆的“Hack the Hague”競賽，與駭客社群合作共同找尋海牙市政府的資安漏洞。2023 年度為第 6 屆，在海牙市政廳舉行，有近 120 位駭客報名參加。Hack the Hague 目前已是全球極富盛名的駭客競賽活動，經訪談現場參與人員，其表示最大程度開放可攻擊系統的範圍，以及最小程度限制駭客攻擊手法，是其一大特色，也是該活動保持歷久不衰的主因。

2. 荷蘭商業及海牙資安現況

荷蘭在商業發展上有許多優勢，包括地理位置、商業環境、高生活品質、英語普及率、高技術人力、物流、醫療服務、創新能力等。荷蘭適合外資發展資安產業的特色包括：

(1) 重視外商投資：荷蘭政府非常重視外資在荷蘭的投資，有超過三百間國際企業在荷蘭設點，創造出超過 8,600 個工作機會，有約五分之一的荷蘭人在跨國企業工作。

(2) 創新研發能力：早期荷蘭著名的創新發明包括望遠鏡、藍芽、DVD 及 WIFI 等，近年來則以艾斯摩爾(ASML)獨步全球的半導體晶片微影技術聞名國際。

(3) 數位發展：荷蘭為歐洲的數位樞紐，具備世界級的先進數位基礎設施，為國際光纖海纜進入歐洲的中心，數位經濟全球排名第二到第三，設有近 300 個數據中心，有著快速的蓬勃發展的數位產業。其中有約 678 間公司以資安為核心營業項目，同時也積極參與資安立法。大學設有資安課程，研究機構也非常重視資安。

(4) 人才引進：即便具備了高素質 IT 人才，荷蘭也跟全球大多數國家一樣面臨人才短缺的問題，因此積極放寬法規限制，讓國際人才可以很快在荷蘭取得身份。

(5) 生活環境：荷蘭生活品質高，據研究海牙市是歐洲前二十名最適合外派人士生活的城市。

(6) 稅制：荷蘭與多國簽有避免雙重課稅之協議，此外雇用荷蘭當地員工，尤其是研發的人才，可獲得稅金的減免。

(7) 政府輔助：荷蘭政府針對重點市場執行「國際商業夥伴」(Partnership International Business) 的計畫，透過舉辦訪問團及商展等，協助拓展市場，目前計畫對象包括德國及北歐。

圖 1 全體團員於 HSD 大廳合影

圖 2 與國際訪團代表交流

圖 3 與 HSD 會議交流歐洲資安發展現況

二、拜訪海牙市政府及觀摩 Hack the Hague 活動

(一) 會議資料

- 日期：2023/10/02
- 時間：14:00-17:00
- 地點：海牙市政府
- 荷蘭方與會者：Jan van Zanen, Mayor of the Hague、Jeroen Schipper Chief Information Security Officer (CISO) Municipality of the Hague、Tona Belderbos Policy Officer International and European Affairs Municipality of the Hague
- 臺灣方：全體訪團成員

(二) 議程

1. 海牙市市長接見
2. 參觀 Hack the Hague
3. 簡報一：海牙市資安概況 by Jeroen Schipper
4. 簡報二：海牙市國際合作活動簡介 byTona Belderbos

(三) 背景

海牙市長 Jan van Zanen 過去擔任阿姆斯特爾芬(Amstelveen)及烏特列支市(Utrecht)市長期間，曾多次率訪問團拜訪臺灣，並與包括臺北、臺中及高雄等城市建立合作關係，合作領域包括生技、智慧交通及農業等。2020 年接任海牙市市長後，對臺灣仍保持高度友好關係。2022 年與臺北市進行「城市數位治理」視訊會談。2019 年臺灣資安團也曾參觀 Hack the Hague 活動，當時由海牙市資安長(CISO)接待。

圖 4 海牙市長接待臺灣訪團成員

(四) 重點摘要

1. 海牙資安長分享海牙市資安概況：

(1) 位置和重要性：海牙市是荷蘭的第三大城市，亦是政府政經決策中心，為中央部會、議會及皇室所在地。海牙市是歐洲最大的海岸城市，也是荷蘭的第二大觀光城市。目前有 95%的國際組織在該市設有據點，尤其是與和平相關的國際組織。

(2) 資訊安全挑戰：海牙市面臨資訊安全威脅，主要來自中國大陸、俄羅斯、北韓和伊朗。市政府採取了監控和防禦措施，以預防資訊外洩與被作為攻擊國際組織的跳板。

(3) 資訊安全團隊：海牙市政府擁有約 30 名資訊安全專業團隊成員。主要工作包括風險管理、安全意識提升和利害關係人管理等。

(4) 框架和文件：海牙市政府採用美國的 NIST 資安框架。此外，也制定多項資訊安全相關文件，包括風險計畫、世界經濟論壇和聯合國資安計畫等。

(5) 國際合作：海牙市政府積極參與如歐洲刑警、北約等國際組織，以共同應對資訊安全挑戰。此外，除了世界經濟論壇外，海牙市也與歐洲和美國大城市的首席資訊安全官建立密切聯繫，目前在亞洲則尚未有合作對象。

(6) 危機應對：海牙市政府定期進行兩次危機研習，一個為 Hack the Hague，每年 ONE Conference 前一天舉辦，邀請駭客實體攻擊市政府資訊系統，吸引專業駭客參與漏洞發現和修補，2022 年共有 206 名駭客參加，共發現了 125 個資安漏洞；今年度則有 116 名駭客實體參與，共發現了 65 個資安漏洞，其中 6 項漏洞在活動時間內已經由市府的資安團隊及供應商共同修復。另外，還有在每年 11 月的國家危機演習，除了市政府、中央政府外，也包括了共約 500 個商業組織共同參與。

(7) 資訊分享和教育：海牙市政府也建立了強大的資訊安全社群，與各種機構、大學和新創公司合作，分享資訊和培訓資源。

圖 5 進行中的 Hack the Hague 2023

2. Hack the Hague 2023

2023 年共有 116 名駭客出席，其中約 40 名為在職學生。海牙市希望透過這項競賽提高自身的資安韌性，激勵供應商確保系統處於最佳狀態，以保護資訊安全。為確保公平競爭，參與的所有駭客事須先同意將他們發現的漏洞通報到指定的協調平台，提供他們發現的漏洞證據、如何發現的以及可能的解決方案，並不將其公諸於眾。這些條件符合市政府的協調漏洞揭示政策。在今年為期六小時的駭客競賽中，共提交了 65 個獨特的漏洞報告。其中 6 個報告屬於高風險漏洞；另外 6 個報告在競賽當天內得以解決，許多報告涉及網路應用程序安全漏洞。

圖 6 活動中的即時監控畫面

3. 海牙市國際合作概況

海牙市人口約 57 萬人，為荷蘭第三大城市，僅次於阿姆斯特丹及鹿特丹市，同時為荷蘭中央政府的所在地，為高度國際化的城市，55%的居民都有移民背景。海牙為國際法庭的所在地，享有「和平及正義之都」 (City of Peace and Justice)之美譽。和平宮 (Peace Palace) 為海牙的著名地標，同時海牙有超過 480 國際組織，其中最有名的是國際法庭及國際刑事法庭。此外還有 22 個跨政府組織、超過 170 個非政府組織、31 個歐盟組織、13 間研究機構及 163 間大使館。

海牙的數位化活動跟歐盟的數位化政策有直接的關係。歐盟總部布魯塞爾立法後，由歐盟的 27 個會員國將其內國法化。在去中央化的趨勢下，70%的歐盟規範由城市執行立法。海牙市設有歐盟事務副市長，確保與歐盟規範的一致性。而因應歐盟的主要策略包括影響及儘早參與立法程序、有效的實施和運用歐盟研發補助計畫。市政府的歐洲團隊 (team Europe)是海牙市政府和歐盟的橋樑，重點領域包含數位化、社會衝擊及韌性、永續發展。

列舉的數位專案範例包含：

- Living Lab Scheveningen：贏得智慧城市大獎在地能源專案，透過能源使用的監控，以平衡能源的生產與利用。例如於離峰時間(晚上)為電動車充電，確保白天能源夠用。
- hack The Hague：與駭客合作找出海牙市政府的資安弱點。
- 透過 Council of Global Cities CIO (CGCC)與其他城市 CIO 合作

圖 7 與海牙國際合作團隊交流

三、參與 ONE Conference 研討會活動

(一) 會議資料

- 日期：2023/10/03
- 時間：09:00-17:00
- 地點：World Forum, The Hague
- 主辦單位：National Cyber Security Centre, the Ministry of Economic Affairs and Climate Policy, the Ministry of Justice and Security, and The Hague Municipal Authority.
- 與會者：全體訪團成員

(二) 背景

1. 過去 2018 年，就曾由國科會資安研究及教學中心 (TWISC) 率團參加，成員均為學術研究背景。2019 年訪問團由工業局負責，領域擴大為學術 (TWISC) 、研究單位 (工研院)及產業 (5 間新創公司)。

2. 今(2023)年為臺灣訪團第三次參加 ONE Conference 活動，首次由政府(數位部數產署) 帶隊，帶領法人 (資安院、工研院、資策會)及產業 (4 間資安公司)參加。

3. ONE Conference 為歐洲重要資安活動之一，有別於其他商業或技術導向之活動，ONE Conference 目的為建立政府、駭客、產業、研究單位等不同關係人之間的鏈結，彰顯資安議題的重要性。

4. 本次活動除了兩天的多場次同步論壇外，也包括了以”let’s collaborate”為議題的 28 個展覽攤位、人才網路 (Talent Hub)及媒合活動。

5. 難得的是，今年的臺灣訪團不僅做為活動的訪問者，也實際上成為了貢獻者。在 ONE Conference Lighting Talk 的部份，分別由工研院、來毅數位及指向科技展示臺灣自主研發資安技術，有望進一步帶動台荷資安合作。

圖 8 ONE Conference 2023 年開幕會場

圖 9 工研院於 ONE Conference 簡報法人研發資安技術

圖 10 臺灣資安業者來毅數位於 ONE Conference 簡報解決方案

圖 11 臺灣資安業者指向科技於 ONE Conference 簡報解決方案

(三) 重點摘要

1. DG Connect 專題演講 (Lorena Boix Alonso，Director for digital society , trust and cybersecurity, DG connect, European Commission)

今年是「ONE Conference」的十週年。十年前，歐盟開始認識到必須在歐洲層面採取資訊安全行動，並頒布了相關指令。在過去二十年中，資安攻擊不斷增加，由於這種增加是漸進式的，人們在逐漸習慣的同時，風險意識卻沒有相對提升。然而，在疫情期間，人們開始認識到沒有人可以免於駭客攻擊，甚至無論是醫院還是疫苗生產線，都有可能遭受攻擊。儘管資安問題可能對經濟造成重大影響，導致損失，但並非所有政治人物或公司主管都將資安視為首要問題。然而，對於駭客來說，破壞卻是他們的首要目標。

歐盟過去十年中的行動方式，包括預防、偵測、反應和嚇阻。歐盟在預防方面採取了積極的措施，最初將重點放在關鍵基礎設施的安全上，然後逐漸擴大到供應鏈安全。然而，法規的制定需要時間。有些行業已經具備資安意識和法規，例如電信業，但製造業則需要加速提高危機意識。資安需要資金，因此一些高級主管可能不願意進行資安投資，但必須確保公司高層對資安決策負責。無論投資決策如何，高層主管都必須對其負責。

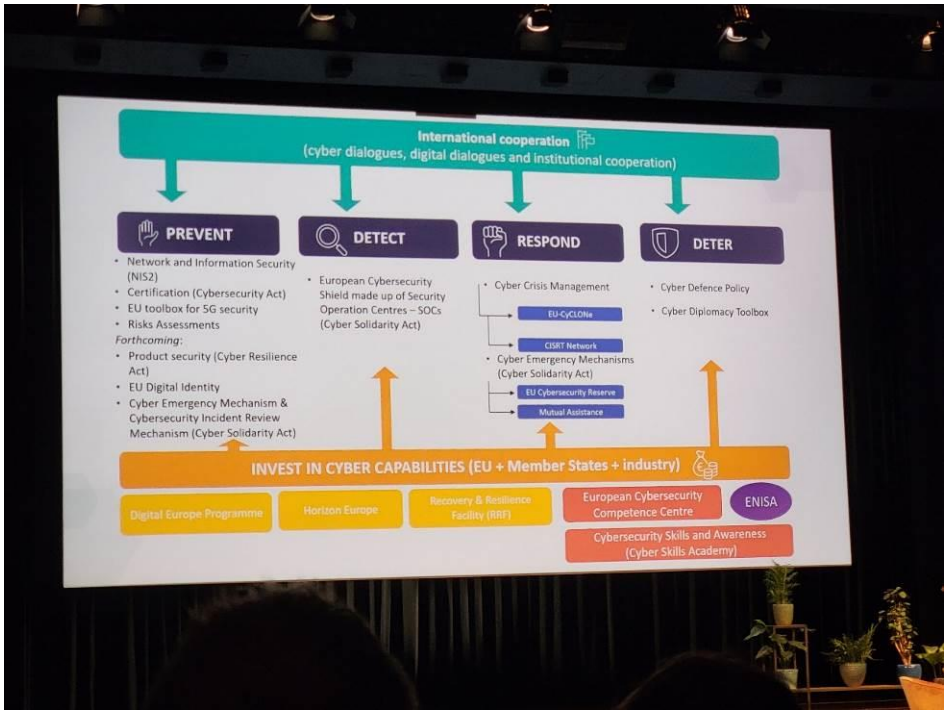

圖 12 歐盟資安推動框架

歐盟還在積極行動提升供應鏈資安，例如「Cyber Resilience Act」是規定供應鏈資安措施的法規，使其變成強制性措施。否則，私部門可能缺乏足夠動力來實施這些措施；或即使他們已經花費資金進行了改進，但他們的客戶可能不理解其價值。此外，還強調偵測和反應，並提出了「Cyber Solidarity Act」。

從俄烏戰爭中學到了重要的教訓，早期偵測至關重要。歐盟需要私部門的支持，以便在發生重大事件時能夠及時採取行動，並需要加強協調。

而歐盟成員國也可以自行選擇合作夥伴並建立合作關係，法律為這些行動提供法源。此外，法律也保留了一些來自私部門的力量，以便在危機發生時能夠迅速部署這些保留下來的私部門資源。接下來，歐盟將開始實施標準化和國際合作，並將加強垂直整合協調和危機管理。某些行業已經覺醒，並希望歐盟能夠針對這些行業制定相關法律，但歐盟需仍需要進一步謹慎評估。此外，歐盟也將從戰略性資安和技術性資安兩個角度入手，例如在考慮 5G 時，我們將以這種方式取得平衡。政策制定者也正在研究如何將人工智慧納入其中。

2. 專題演講 by Jaya Baloo, CIO, Rapid 7

在處理資安事件之前，還有一些重要的議題值得關注及討論：

(1) 資安道德： 需要重視資安道德，並要提案修訂「Cyber Resilience Act」，因為根據該法規，公司發現弱點後必須在 24 小時內通報，然而，弱點並不一定會被立即修復，可能導致弱點資訊落入不法人士之手。比較適當的作法是修改法律，讓公司有足夠時間找到修復的方法，而非過度強調即時通報的重要性。

(2) 資安事件： 以往許多資安事件都與勒索軟體有關，但很多企業並未通報，甚至越來越多選擇不通報。這需要建立更多的激勵措施，且企業被攻擊後，攻擊者掌控了情勢，建議企業應該以合作解決問題取代互相指責，並儘速釐清問題的嚴重性和擴散範圍。

(3) 美國法規： 美國的法規要求公司在遭受重大資安事件時必須在四天內報告，但實務上很難執行。此外，也需要釐清通報是否就等於安全？透明度可能導致企業面臨主管機關執法單位的嚴厲處罰，並且對於資安團隊來說並無實質好處。例如，Uber 的首席資安官被定罪就是一個明顯的案例。

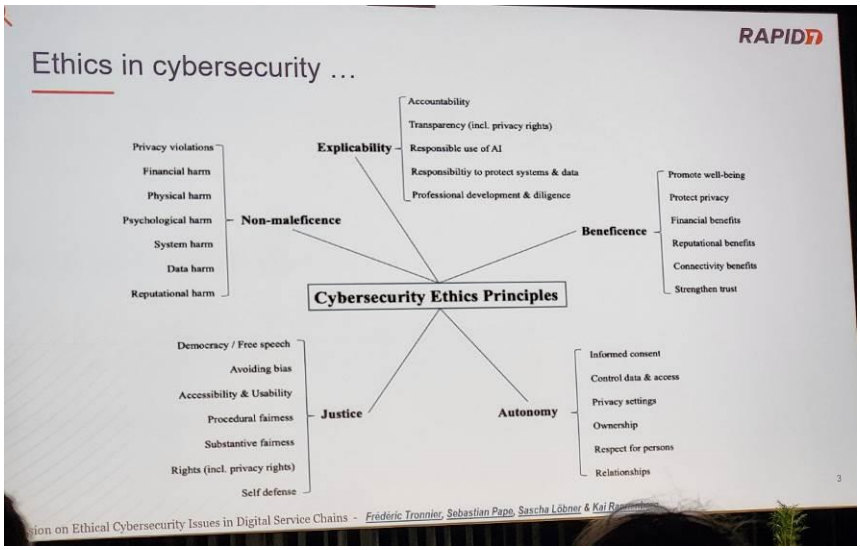

圖 13 資安道德議題被提出探討

四、拜訪 ASML 及 Cyber Resilience Centre in Brainport Eindhoven 交流

(一) 會議資訊

- 日期：2023/10/03
- 時間：15:00-15:45
- 地點：Room North America, World Forum, The Hague
- 荷蘭方與會者：
  Piet Bel, Senior Security Alliance Manager, ASML
  Angélique Staal, program manager, Cyber resilience center
- 臺灣方：數位部數產署、資安院、工研院、資策會

(二) 背景

"Cybersecurity Circle of Trust"（資安信任圈）是由高科技公司艾斯摩爾(ASML)所提出的一項倡議，共有十間大型跨國企業主導，旨在促進各種組織之間的合作和資訊共享，尤其是在資訊安全領域。其目標在於建構一個信任及合作的網路，加速資安認知及知識的擴散，進而提升整體產業之資安韌性，而非仰賴政府規範的推動。此倡議受到荷蘭政府單位例如 NCSC 及 Brainport Eindhoven 的支持，而 ASML 公司也積極地向外推廣此理念。

(三) 內容摘要

在荷蘭部分產業內部已積極合作，以金融業為例，當發生產業資安事件時，除了立即通報政府單位外，也會通知其他金融業者，以提升整體的資安韌性。但對於製造業而言，尤其是針對中小型的供應商，資訊安全被視為不必要的投資。以荷蘭連鎖超市 Albert Heijn 為例，2021 年 4 月因其物流廠商受被駭客入侵，使得大約一半的運輸卡車無法上路，導致部分門市無法正常供貨，不但影響公司運作也衝擊民生需求。因為企業的穩定運作需建立在完善的供應鏈資安上。

基於此理念，ASML 召集了包括飛利浦、殼牌石油等 10 間跨國公司，共同向政府提出” Cybersecurity Circle of Trust” 的概念。並已受到政府的支持。在此架構下，政府的角色為協調者，並由大型企業串聯中小型企業，共同建立合作網絡。大型企業利用其資源，除了蒐集全球資安資訊與政府分享外，也對於相關公共政策提出意見，建立起良好的合作關係。而中小企業也從中獲得相關的知識及協助。大型企業未從政府獲得任何資助，而是為了不同利害關係人對於資安的共同需求而努力。整體概念可分為下列重點：

- 合作網路：ASML 強調與工業、政府、用戶代表以及來自不同國家的會議代表團之間的合作。建立廣泛的關係網絡，可以更好地共享網路安全資訊和最佳實踐案例。
- 資訊共享：資訊共享為成功關鍵，尤其是在網路安全事件發生時。政府

和其他大公司之間的資訊共用協定，以確保網路安全事件的消息能夠快速傳播。

- 合作與非競爭：網路安全合作的意義，不僅在公司內部，還包括跨公司間合作，需透過不同規模的公司共同提升網路韌性。
- 政府協助：政府在網路安全策略和政策方面極為重要，尤其是協調和支援網路安全方面。
- 安全信任圈：這個概念強調建立一個安全的信任網路，將各個組織串連在一起，共同努力提高網路安全。
- 教育與資源：大公司透過教育和資源分享，特別是對中小企業，可以提高整個網路安全生態系統的韌性。

ASML 的“安全信任圈”概念凸顯了網路安全領域合作的重要性，以對抗不斷增加的網路威脅。這一概念將不同的組織和實體連接在一起，共同推動網路安全和資訊分享。

圖 14 荷蘭企業 ASML 說明大企業帶動中小企業建構資安合作

五、受邀參與 International Business Event

(一) 會議資訊

- 日期：2023/10/03
- 時間：18:00-20:00
- 地點：Leonardo Hotel, the Hague
- 主辦單位：海牙市政府、Innovation Quarter
- 荷蘭方與會者：全體 ONE Conference 與會者
- 臺灣方與會者：全體訪團成員

(二) 背景

社交是在荷蘭從事商業活動的重要一部分，而外來投資也是荷蘭經濟及就業的重要支柱，因此海牙市政府與 Innovation Quarter 在 ONE Conference 的第一天活動結束後，舉辦了 International Business Event. 活動中除了邀集了海牙市創業及投資相關單位，現場專人提供外國訪團在荷蘭拓展市場的資訊。此外，也邀請荷蘭本地企業，協助建立人脈及合作機會。

臺灣資安業者來毅數位近期在海牙 HSD 成立分公司，在活動中受到宣傳及表揚。

圖 15 International Business Event 活動現場交流熱絡

六、拜訪 National Cybersecurity Center (NCSC)

(一) 會議資料

- 日期：2023/10/04
- 時間：13:30-14:30
- 地點：Room Volga 1, World Forum, The Hague
- 荷蘭方：
  - Hans de Vries, Director, NCSC, Ministry of Justice and Security
  - Maartje Peters, Head of Department, International Cyber Policy Taskforce, Ministry of Foreign Affairs
  - Jurriën Norder, Senior advisor International Relations, NCSC, Ministry of Justice and Security
- 臺灣方與會人員：數位部數產署、資安院、工研院、資策會

(二) 議程

1. 荷蘭 NCSC 業務介紹
2. 臺灣資安院業務介紹
3. 綜合討論

(三) 重點摘要

1. NCSC 核心業務有三，包括

- 歐洲資安法規談判及溝通
- 營運合作:包括歐盟營運網路、交換威脅指標、資安攻擊量化、IP 位置、受害者通報等
- 大型企業戰略關係，包括蘋果及 google 等

2. 雙邊分享及討論業務範疇及運作方法之差異性，包括

- CERT, ISAC 及 SOC 的架構及運作機制
- 權責 (例如 NCSC 無審計之功能)及管理對象
- 協調功能
- 人力及培訓/徵才機制
- 特殊機制：
  - 漏洞披露機制 (Responsible Disclosure)
- 荷蘭透過 HackShield 的計畫，針對 8 至 12 歲的低年級學生，以遊戲化的方式解釋了網路安全的重要性並培訓孩童。進而，除了提升對網路安全的興趣及知識，也透過此計畫讓兒童教導高齡者了解資訊安全運作模式，目前除荷蘭之外，也在巴西及比利時等國家執行。
- 荷蘭 HackRight 計畫：針對未成年駭客，荷蘭政府的做法是請專業駭客解釋可能的後果，同時培養資安人才並納入政府資安體系，而非單純透過

懲罰的方式來遏止。

(四) NCSC 介紹荷蘭資安演練活動

- 11 月舉行為期 3 天的國家危機演練，共有超過 3000 人，約 200 個單位共同參與，各別組織將被賦予不同的危機情境。主要領域為港口、海事、能源及電信等
- 海牙市舉辦的“Hack the Hague”駭客競賽，允許駭客對於市政府資訊系統進行實際攻擊

圖 16 與 NCSC 互動交流

七、拜會 Dcypher

(一) 會議資料

- 日期：2023/10/04
- 時間：15:30-16:30
- 地點：Room Everest, World Forum, The Hague
- 荷蘭方與會人員：
  - Michel Rademaker, Program Director, Cryptocommunication (and deputy Director of the Hague Center for Strategic Studies)
  - Christian van der Woude, Strategic Adviser at dcypher
- 臺灣方與會人員：全體訪問團

(二) 會議議程

- 報告：Dcypher 介紹
- 綜合討論：雙邊合作重點及模式

(三) 重點摘要

1. Dcypher 簡介

Dcypher (Dutch CYbersecurity Platform Higher Education and Research, 直譯為荷蘭高等教育及研究資安平台) 為荷蘭政府依據國家資安策略 (national cybersecurity strategy) 及 頂尖產業政策 (top sector policy)，所建立的公共資安研發平台，其宗旨在於協助企業、研究機構及政府單位從事共同研究，增加知識的價值，進而促進經濟發展。Dcypher 透過夥伴關係建立、經費及專業知識協助：(1)提高基礎研究的經濟及社會價值；(2)培訓資安專業人員；(3)建立國際合作夥伴關係，強化荷蘭在資訊安全領域的知識地位。

Dcypher 目前所關切的議題包括後量子密碼學 (post quantum cryptography)、自動化弱點偵測 (automated vulnerability)、數位鑑識 (digital forensics)及 資安事故應變 (incident response)。Dcypher 透過價值鏈整合 (integral value chain approach)，將資訊安全引進高科技領域，例如離岸風電的新基礎設施及數據。Dcypher 亦協助：

- 探索可能資安漏洞
- 尋找可能的發展機會
- 分析其工業物聯網系統，例如船隻通訊及感測器
- 協助企業建立成長模式

2. 合作方向

Dcypher 提出三個可能的合作方向：

(1) 後量子密碼學：sustainability embedding expertise on PQC for society at large
(2) 台荷雙邊研發合作計畫（透過荷蘭政府的 Knowledge and Innovation Covenant, KIC 計畫)
(3) 建立雙邊合作路徑：擴大雙邊在高科技產業研發的路徑規劃

PQC 下的可能合作題目再聚焦，可能有

- 模組化元件的使用：檢視密碼學解決方案中常見的模組化元件的使用，以減少測試和認證時間；
- 最終用戶的需求：強調最終使用者對密碼學的認知有限，往往僅只知道他們需要安全解決方案，因此提到了一個名為 "檢查清單" 的專案，旨在更清晰和精確地定義密碼學需求，讓服務供應商能更明確掌握需求。
- 後量子金鑰遷移需求：討論了應對量子計算威脅的後量子金鑰遷移需求，並希望建立一個資源集散地以幫助社會進行遷移。
- 與晶片製造商的合作：提到了與晶片製造商（例如 TSMC 和 NXP）的合作，以在實際環境中測試密碼學解決方案。
- 密碼學在不同應用領域的使用：討論了密碼學在不同應用領域（包括國防、情報、基礎設施等）的使用，以及設備的計算性能和能源消耗等問題。

圖 17 與 Dcypher 交流資安技術合作

八、Meeting KPN 荷蘭皇家電信

(一) 會議資料

- 日期：2023/10/05
- 時間：09:30-11:30
- 地點：KPN Zoetemeer
- 荷蘭方與會人員：
  - Erno Doorenspleet, CTO, KPN
  - Remco van Oostrom, product owner digital Dutch Xperience at KPN
- 臺灣方與會人員：全體訪問團

(二) 會議議程

1. 簡報 1：KPN 資安活動介紹 by Erno Doorenspleet, KPN
2. 簡報 2：臺灣資安產業介紹 by 工研院
3. 簡報 3：四間臺灣廠商簡報 by 全景科技、指向科技、雷盾科技、來毅數位

(三) 重點摘要

1. 關於 KPN

   KPN 背景：公司擁有大約 140 年的歷史，最初為國營企業，負責家庭電信業務，後來逐漸發展出不同的服務。目前 KPN 為荷蘭最大的電信公司，擁有最完整的網路基礎設施。KPN 的資安服務涵蓋了政府及民營單位所需要的解決方案。

2. KPN 面對的挑戰

   (1) 永續發展：KPN 正在從單純地的網路安全轉向更廣泛的資訊科技和技術戰略。目前朝向永續的電信發展，透過光纖的鋪設、太陽能投資及降低數據中心能耗以因應成本上升及環境問題。

   (2) 新興技術：尤其是人工智慧和機器學習。過去兩年中人工智慧的討論發生了顯著變化，部分原因是 ChatGPT 等相關技術的進步。KPN 正主導荷蘭在量子計算和人工智慧交集的討論。由於 KPN 網路中擁有超過一百萬個感測器，維持如此複雜網路系統的資訊安全，勢必要仰賴人工智慧。然而，人工智慧已成為網路攻擊中的挑戰，加劇防守者和攻擊者之間的持續競爭。

   (3) 物聯網(IoT)：電信產業需正視物聯網快速發展以及工業控制技術(OT)的複雜性所帶來的挑戰。

   (4) 5G 網路： KPN 為因應 5G 網路所增加的頻寬需求，也需要提升基礎設施更的分布。從積極的一面來看，5G 能夠通過分層實現更強大的

網路安全，當與光纖相結合時，它成為 KPN 市場的有力組合。

(5) 永續能源和量子計算：KPN 公司積極參與量子計算最新發展及討論，包括是否會引起顛覆性變化以及何時會發生等。

(6) 複雜的威脅：新技術、人工智慧以及各種形式的攻擊如何使威脅形勢變得日益複雜。勒索軟體攻擊仍然是一個重大議題。儘管有人認為歐洲的 NIST2 指令將有助於解決這些挑戰，但積極的網路安全措施比僅僅遵守法規更為重要。物聯網的擴張和數位供應鏈風險也很重要。複雜化威脅的因素：包括物聯網的崛起、攻擊的擴展、COVID-19 對網路安全的影響以及員工行為的不可預測性，這些因素對於網路安全領域帶來了重大挑戰。

3. 合作及夥伴關係

KPN 強調合作對於荷蘭資訊安全的重要性。KPN 為各種關鍵領域提供服務，包括警察單位、重要港口和公共交通等。他們也透過設置監測感測器保護城市免受洪水侵襲，使城市安全成為共同的責任。

KPN 重視與關鍵合作夥伴的關係。與史基普爾機場、國防組織和其他重要機構均有長期的合作。合作關係是相互有益的，此關係激發 KPN 公司開發新的解決方案和想法，以增強安全措施並為合作夥伴提供關鍵服務，如國防和警察機構。服務內容包含：

4. 威脅情報：KPN 積極監控其網路，維護安全營運中心，進行自動漏洞管理，並部署快速應對小組，以應對內外部安全事件。提高意識和確保公司提供可靠的服務為重點。

5. 透明化：KPN 公司與合作夥伴以透明態度面對資安訊息，每週更新網路安全的當前狀態和潛在風險，以確保決策品質並及時因應。

6. 共同創造 (co-creation)和創新 (innovation)：KPN 在網路安全領域積極與客戶合作。他們提供各種服務，包括硬體、軟體和專業服務。透過與客戶的合作來掌握其獨特需求並幫助其成長。

7. 定制解決方案：
   - KPN 為大型企業和公司提供定制解決方案，以客製化彈性滿足特定需求。
   - KPN 為中小型企業提供由合作夥伴提供的網路安全解決方案。這些數位化解決方案可透過線上或到府服務。大約 70%的解決方案是由合作夥伴提供。

8. 核心服務： KPN 提供的核心服務，強調了他們對身份管理、威脅保護和專業服務的承諾。

- 威脅保護：KPN 公司積極監測他們客戶的環境，確保它們安全，並能夠進行操作而不擔心網路安全威脅。
- 專業服務：KPN 的專業服務包括風險管理和漏洞管理等。這些服務有助於組織規劃、評估其環境，並協作開發業務發展策略。

9. 對中小企業的支持： 中小企業服務是 KPN 成長最快的業務領域，在荷蘭大約有 170 萬家公司。所提供的服務包括安全網路標準、虛擬首席資安長、監測服務及定期報告，說明企業瞭解其安全狀況。

10. 額外安全互聯網 (extra safe internet)：KPN 的「額外安全互聯網」服務，企業家可以在他們的自助服務門戶中啟動該服務。這項服務有助於防止訪問惡意網站，並提供了適應不同需求的分級安全解決方案。由於網路安全要求不斷變化和新的法規，這是一個不斷發展的市場。KPN 正在積極與代表中小企業的組織互動，以收集回饋並使他們的服務適應這一領域不斷發展的需求。

圖 18 KPN 接待臺灣訪團

九、參加 Cyber Investor Day 活動

(一) 會議資料

- 日期：2023/10/05
- 時間：13:30-16:30
- 地點：Security Delta
- 荷蘭方與會人員：
  - Martijn van Hoogenhuijze & Philip Meijer Account Managers, Cyber Security InnovationQuarter；
  - Joris den Bruinen Director, Security Delta
- 臺灣方與會人員：全體訪問團

(二) 會議議程

1. 簡報 1：歐洲資安新創公司簡報
2. 商務交流：與荷蘭資安投資人交流

(三) 重點摘要

荷蘭投資資安新創公司的概況：

1. 資安新創公司數量：荷蘭是歐洲一個具有活躍資安新創生態系統的國家，擁有眾多資安相關的初創企業。這些公司涵蓋了各種不同的領域，包括網絡安全、數據保護、身份驗證、風險管理等。

2. 投資情況：荷蘭的資安新創公司吸引了國內外投資者的關注。一些知名的風險投資公司和創投公司可能會投資於這些企業，以支持其發展。

3. 創新生態系統：荷蘭的資安新創公司通常可以從當地的創新生態系統中受益。荷蘭有多個科技園區、創業加速器和孵化器，為初創企業提供支持和資源。

4. 政府支持：荷蘭政府也積極支持資安領域的創新和發展。這包括提供資金、培訓、法規和政策支持等。

5. 國際影響力：荷蘭作為一個國際性的商業和技術中心，有機會吸引全球客戶和合作夥伴，從而促進資安新創公司的國際影響力。

圖 19 進一步交流荷蘭資安投資概況

十、拜訪恩荷芬科技大學

(一) 會議資料

- 日期：2023/10/06
- 時間：10:30-15:30
- 地點：Eindhoven University of Technology
- 荷方與會者：
  - Sandro Etalle, Professor, TU/e
  - Harold Wafers, External Collaboration Coordinator, TU/e
  - Michelle Chong, Assistant Professor, department of mechanical engineering, TU/e
  - Tanja Lange, Professor, TU/e
  - Peter Boosten, manager cybersecurity monitoring operation center, TU/e
  - Jeroen van Woerden, Managing Director, The Gate Eindhoven
  - Cathy Song, Senior officer for Innovation, Technology and Science, Netherlands Office Taipei
- 臺灣方與會者：全體訪問團

(二) 議程

1. INTERSECT 計畫介紹 – Harold Waffers
2. 虛實整合系統的安全及隱私研究介紹 (Security and Privacy of Cyber-Physical Systems) – Michelle Chong
3. 後量子密碼學研究介紹 (Post quantum cryptography) – Tanja Lange
4. 恩荷芬科技大學資安計畫介紹 – Sandro Etalle
5. TU/e SOC 參訪 – Peter Boosten
6. 恩荷芬新創計畫 The Gate 介紹 - Jeroen van Woerden,

(三) 重點摘要

1. INTERSECT 計畫

恩荷芬科技大學資安領域涵蓋的資訊工程、數學以及機械工程等系所，均相互進行合作。資訊工程系以實務操作為導向，數學系注重理論、機械工程系則兩者兼備。

INTERSEC 為荷蘭過去 10 年來最大的資安研究計畫，其目的在於透過公私協力(PPP)的模式，建立安全物體的網絡 (Internet of Secure things)，以因應數位轉型所帶來的契機及威脅。下一階段的計畫規模為 5 億歐元。內容主要分為以下五個領域

- 監控及威脅情資 Monitoring the threat intelligence,
- 可信賴的人工智慧 Trustworthy AI,

- 物聯網資安 IoT security,
- 存取控制及政策符合性 Access control and policy compliance,
- 數位安全的實體層面 physical aspect of digital security.

其成立目的主要為了因應數位轉型 (digital transformation) 的趨勢，包括社會面及產業面。其中，物聯網為關鍵議題，尤其在於高科技連接系統內，可能串聯了電視或車輛等，均需要資安機制來提供保護。數位轉型發生在各個產業，而所有產業均為惡意攻擊者發揮的舞台，且多數人仍不知如何保護自身安全。有鑑於資安產業的分散性，INTERSECT 計畫把焦點放在產品上，確保產品在完整生命週期內的安全性。

全球各主管機關逐漸認知到在數位轉型及裝置聯網過程中，維持資安的重要性。物聯網涵蓋具備聯網及運算能力，且會產生資料的資通訊產品、感測器及觸動器等。許多產品在上市前並不內建資安功能，因此需避免沒有經過授權的資料存取及系統登入。資安標準在明年新法生效之後將變成強制性。物聯網內的資安威脅無所不在，尤其是現有建築物內已有太多的物聯網裝置及感測器，超出了使用者的掌握範疇。INTERSECT 的目標，是讓解決方案更容易為產業所採用，並建立新的系統生命週期。

INTERSECT 聯盟，其供應鏈是由上千供應商所成立的網路，所以要處理的很多。因此成功必須仰賴大規模的改變社會和產業。無論是終端消費者或者是供應鏈，均需要將資安納入每個環節的考量，且不能不能仰賴某個單位所提供所有的保障。聯盟成員除了學術界外，還涵蓋了：

- 物聯網系統的生產者 (Philips, Siemens, Bosch, …)
- 系統的生產者 (Centric, …)
- 驅動系統的生產者 (Synopsys, Verum, …)
- 特定領域的生產業者 (FME, NIDV, …)
- 產業代表 (CWCB)
- 政府

2. 簡報二：虛實整合系統(CPS)的安全及隱私研究介紹 (Security and Privacy of Cyber-Physical Systems) – Michelle Chong

機械工程系對於 CPS 的安全及隱私研究，主要應用於決策、學習、分析及控制等四個領域。CPS 可分為實體及虛擬等兩個層面，而資安漏洞可能存在於兩個層面之內。過去主要採用的是 IT 為基礎的解決方案，例如防火牆。但其效能有限。

CPS 安全及隱私的研究是建立在下列的方法上：

- 系統及控制理論 Systems and control theory
- 最佳化及機械學習 Optimization and machine learning
- 形式化方法 Formal methods

- 編碼理論 Coding theory

四個主要探討的問題為

- 敵對方可以從物理層面學到什麼？
- 他們能夠造成什麼樣的物理損害？
- 我們如何量化這些敵對能力？
- 我們如何減輕這種能力的影響？

CPS 的安全

- 目前研究範疇集中在實體層及兩層之間的通訊媒介，分為兩個面向
  - 偵測惡意入侵的監控機制
  - 安全 CPS 的持續性運作

目前的應用範圍包括了

- 關鍵基礎設施防護 (次世代自動車)
- 未來智慧能源系統防護 (50kv 或以下至低電壓系統)

目前參與了兩個歐盟補助的計畫

- Resili8 (Resilience for Cyber-Physical Energy Systems) (https://resili8-project.eu/)
- SELFY (Cyber-secure Cooperative and Connected Automated Driving) (https://selfy-project.eu/)

CPS 的隱私保護

- 為了保護在通信媒介上傳輸的數據，以及在運算單元中運行的算法
- 目前主要用途為：
  - 供雲計算所使用的數據和算法的同態加密：如何重新設計算法，使其能夠在加密數據上運行，並提供隱私保證
  - 隱私-效能綜合架構
  - 基於事件的編碼機制，用於控制和決策制定：僅在需要時發送關鍵信息

3. (簡報三：後量子密碼學介紹 – Tanja Lange

Tanja Lange 為國際知名的後量子密碼學學者，過去與臺灣大學及中研院有密切的合作，包括在 2020~2022 年間受中研院邀請，在臺灣從事的兩年的研究工作。

後量子密碼學之所以受到重視主要是基於 PW Shor 在 1994 年所發表的研究結果，內容顯示量子電腦在 5~10 年間能破解任何目前的加密方式。目前研究方向涵蓋編碼理論和密碼學

- 編碼理論
  - 錯誤檢測和修正碼(Error detecting and error correcting codes)

- 資訊理論 (Information Theory)
- 組合數學 (Combinatories)

- 密碼學
  - 後量子密碼學 PQC
  - 密碼學 Cryptology

4. 簡報四－恩荷芬新創育成計畫 The Gate 介紹

依據 TechLeap 的最新報告，恩荷芬的研究育成計畫排名全球第七，The Gate 的運作現況如下：

- 目前正支持 57 項商業計畫，並有 94 項計畫在規劃中
- 19 件計畫獲得經費補助，22 件計畫申請中
- 成立 4 間公司，5 間仍在成立中
- 23 件專利申請
- 44 件發明經過審核
- 目標在 2025 年時，每年協助 50 件新創計畫。

學校課程內已內含了基本創業理論，有興趣創業之教職員或學生可以參與進階的創業課程。同時學校可提供最高 25 萬歐元的種子研發投資。整體育成在正式進去 A 輪募資前結束。目標對象包括學生、科學家/研究人員及區域的企業家，提供初期所需要的經濟支援。The Gate 所提供的服務包括：

- 創新概念的驗證
- 制定商業計畫
- 智慧財產權協助
- 育成培訓
- 融資和募款
- 法律支持
- 住房和工作場所
- 輔導

圖 20 全體團員與主要接待者合影

圖 21 技術交流午宴

參、 結論

臺灣資安廠商走向國際，荷蘭是選項之一

國內內需市場有限，產業勢必向外發展，而國內廠商以往多向亞洲及美國發展，對歐洲較為陌生，而荷蘭已具備眾多資安產業發展優勢，同時積極協助外商拓展市場，可視為臺灣廠商未來進入歐洲市場的門戶。且台荷在過去已建立良好合作關係，未來應持續深化雙邊合作，以達到協助產業發展的目的。

荷蘭官方、研究機構、法人單位相對友善，具合作空間

拜訪海牙市，儘管現任市長對臺灣十分友善，但由於自疫情期間才擔任市長，尚未與臺灣有實體的交流活動；其國際合作團隊以歐盟為重點對象，可思考如何建立及提升雙邊的實質交流。例如邀請率團訪台等。另外其辦理的 Hack the Hague 為國際間極富盛名的駭客競賽，為海牙市推動資安發展亮點。臺灣每年舉辦不少駭客活動，可參考此型態以提升活動多樣性與吸睛度

拜訪 Dcypher，因雙邊技術發展的議題有交集，後續可能下一步包含量子安全遷移中心（QSMC）運作；如討論建立 QSMC 的重要性。目前歐洲包括德國、法國及荷蘭都積極發展 QSMC，但荷方認為臺灣目前在此領域的進度領先，希望能進一步了解目前的運作方式及未來可能的合作機會；

拜訪 TU Endhovan（TU/e）恩荷芬大學，其在工業控制安全、後量子密碼學及虛實整合系統資安均在全球領先地位。目前僅有後量子密碼學與臺灣大學及中研院有所合作，可思考如何協助產業及學術單位進行研發合作。此行我們還了解到，恩荷芬科技大學今年舉辦了第一屆的台荷半導體 Summer School，參加單位除了 TU/e 外，包括了陽明交通大學、臺灣大學、成功大學、艾斯摩爾（ASML）、台積電、恩智浦（NXP）及 Photon Delta；類似模式或可進一步拓展資安領域合作。最後，恩荷芬 The Gate 計畫為全球排名前段的學術研究育成計畫，其運作模式或可協助國內新創團隊於當地發展。

歐盟研發計畫為歐盟重要的研發機制，為荷蘭創新研發重要管道之一。臺灣具備參與歐盟計畫身分，可嘗試與荷蘭合作，提高獲得補助的機會。

荷蘭資安發展有大廠帶動

荷蘭經驗顯示提升整體產業資安水平不能僅仰賴政府制度的建立，尤其對中小型企業而言，資安成本不能反映在獲利上，因此往往被忽視，故需要大型企業與中小企業共同推動，且需要整體生態系成員共同參與。建立合作的基礎在於「信任」，而這正是產業/廠商之間所缺乏的。荷蘭透過不同類型的活動（例如由 ASML 帶動的 Circle of Trust），凝聚對資安的共識及對彼此的信任，可供參考。

在拜訪 KPN 時，其做為荷蘭及歐洲的重要電信商，採用開放式的態度積極與外界合作，以掌握新趨勢及需求，作為發展新產品及服務的基礎。其目前也積極爭取與國際資安新創合作，臺灣廠商可以借力與 KPN 合作，做為切入歐洲市場的重要合作夥伴。同時，KPN 技術長 Erno Doorenspleet 也是 KPN CISO 的顧問，本身在內部推動商業與非商業部門之間的資安合作。他同時也是 KPN 資安投資部門的委員。KPN 的投資策略是在不干涉經營權的情況下，針對具備潛力的資安新創提供資源、支持及指導。臺灣可積極爭取與 Erno 的緊密連結，做為具有指標性意義的國際顧問。

肆、 建議

此次出訪荷蘭規劃，依本署計畫目標、各法人任務導向以及廠商拓商需求等層面安排，參與多元活動、訪查多個單位、面談當地資安關鍵領導者，匯整結論依政策面、產業面及應用面，建議未來台荷資安合作下一步。

就政策面而言，”Hack the Hague”這項獨特的國際資訊安全活動，允許駭客對市政府系統進行實際的滲透測試，展現出荷蘭對於資訊安全的高度重視和積極態度。臺灣可以考慮引進類似的競賽概念，不僅可以加強國內對資訊安全的重視，亦能培訓和發掘資安人才，向世界展示臺灣資安實力。此外，不一定要限於市政府層面，部會或特定園區都可以作為可能的目標。另外，因歐盟特有的研發計畫，荷蘭獲得了充份的資源和支持，推動當地的資安技術和產業發展。目前臺灣也具備參與歐盟計畫的身分，宜積極尋找與荷蘭或其他歐盟國家的合作機會，帶動臺灣資安技術進入歐洲市場。最後，臺灣「量子安全遷移中心」計畫在荷蘭受到關注，如 Dcypherh 於拜會中即表達高度合作意願。後續可透過工研院及資策會的連結，或與法人進行技術合作，或與相關領域業者展開合作模式探討。

在產業面的影響，未來可持續參與 ONE Conference 及其周邊活動，協助臺灣資安業者深入了解荷蘭協助外商落地之政策資源、藉由 ONE Conference 平台曝光及鏈結合作夥伴，並利用荷蘭開放且友商的環境，做為臺灣業者進一步推進其他歐洲市場的關鍵據點。除此之外，透過與荷蘭企業合作建構跨國產業生態系，如此次拜會 ASML 及 KPN，荷方對於臺灣資安產業發展具有強烈的合作意向。不論是 ASML 在 Circle of Trust 的後續對談，或是 KPN 對於臺灣資安解決方案的進一步評估，都說明了雙邊產業生態存在合作潛力以進一步助攻臺灣資安產業發展的可能性。

最後在實際應用面層面，第一個拜會的 HSD 提供的落地軟硬資源，可以有效地推進臺灣資安業者切入歐洲市場。這次來毅數位落地 HSD 就是一個非常好的示範；HSD 有效為其在荷蘭當地做行銷宣傳、連結潛在客戶及投資人，提供辦公場所及商務社交活動。未來臺灣資安業者能循相同模式，槓桿資源、落地歐洲。而最後一站拜訪的恩荷芬科技大學，大學本身設置的資安創新育成中心，有效鏈結資安創新技術與其所在產業園區大廠協作及驗證。未來或能商議臺灣的資安創新亦透過其機制，將技術落地應用。

伍、 檢附相關資料

無