出國報告（出國類別：考察訪問）

數位發展部赴以色列參與 Cyber Week 2023 活動及比利時進行臺歐雙方數位合作交流出國報告

服務機關	姓名職稱
數位發展部	唐鳳部長、黃子維簡任秘書、李岳寅科長、顧荃專案規劃師
數位發展部數位產業署	林俊秀副署長、施偉仁副組長
數位發展部資通安全署	鄭欣明副署長

派赴國家：以色列及比利時
出國期間：112.06.25-112.07.2
報告日期：112.09.8

摘要

以色列 Cyber Week 主辦單位特拉維夫跨域網路研究中心（ICRC）創辦人暨以色列前國家科技及研發委員會主席 Prof. Isaac Ben-Israel 及總經理 Gili Drob－Heistein 邀請數位發展部（以下簡稱本部）唐鳳部長於參加「2023網路安全週」（以下簡稱 Cyber Week 2023）活動，就資安韌性及資訊產業推展進行交流，並將安排會晤該國政要；另為推動我國與歐盟進行電子簽章、AI 發展及分散式身分驗證合作，強化我國數位基礎建設韌性並連結國際民主網絡力量，銜接以色列行程續往比利時，拜會歐盟產、官、研界重要人士，因此於今（112）年6月25日由唐部長率本部及本部所屬數位產業署(以下簡稱產業署)及資通安全署(以下簡稱資安署）相關人員一同出訪。

本次訪團行程，唐部長首先受邀於以色列年度資安盛會 Cyber Week 2023國際論壇進行大會演說，成為我國部長級官員首度在以國公開演講，向與會各國政要及國際資安專家，分享臺灣因應境外網攻、捍衛民主的經驗，唐部長並本部產業署及資安署於圓桌論壇與各國專家就資安與 AI 議題進行對談，另部長亦就數位韌性（Cyber Resilience）分享臺灣正推動建立多元異質通訊網路，整合地面固定網路、無線網路、海纜、衛星等通訊方式，並持續強化網路資安防護，提升數位韌性。除參加 Cyber Week 2023相關活動，唐部長亦與以色列知名資安公司 Chain Reaction 及 Pentera 進行會晤，以了解先進資安技術。

唐部長結束以色列相關行程後趕往歐盟總部所在比利時，除拜會拜會歐盟執委會資通訊網絡暨科技總署（DG CONNECT）外，亦與包含歐洲民主基金會（European Endowment for Democracy, EFD）及 AI 學院（AI for the Common Good Institute, FARI）等非官方組織進行交流。本部產業署另由林副署長等人前往盧森堡拜會與資安產業相關人士。

期許透過本次出訪，與以色列、歐盟及比利時深化資通安全、數位政府、數位產業、應用創新等各面向合作，與國際民主夥伴攜手聯防，共同提升數位韌性。

目錄

壹、參訪目的

本次出國主要為應以色列 Cyber Week 2023之邀由本部唐部長率本部、產業署及資安署相關人員赴以色列台拉維夫與比利時布魯塞爾針對資安及 AI 等議題進行拜會交流，主要的目的包括：：

一、參加以色列 Cyber Week 並與資安新創 Chain Reaction 及 Pentera 交流合作：

(一)與以色列 Cyber Week 主辦單位 (台拉維夫跨域網路研究中心) 針對資訊安全技術與應用進行交流，了解以色列、美國等國家資安發展政策。

(二)拜訪以色列資安新創 Chain Reaction，除簽訂合作協議之外，並提出後續合作構想。

(三)會晤 Pentera 了解自動安全驗證（Automated Security Validation）等先進資安態勢管理技術，並針對如何增進數位韌性、控管網路風險進行深入討論。

二、拜訪比利時與歐盟數位產業相關官方機構、公協會與組織：

(一)拜訪資通訊網絡暨科技總署 (DG CONNECT)，掌握身分識別與信賴服務 (eIDAS)、AI Act 等之最新發展現況，並建立持續進行臺-歐盟電子簽章互通技術協商之共識。

(二)拜訪數位歐洲協會 (Digital Europe)、歐洲資訊安全組織 (ECSO)、電腦與通訊協會 (CCIA)、AI 公益學院 (FARI)等單位，了解比利時與歐洲對於資訊安全、人工智慧、數位政府等議題之發展現況，並尋求合作機會。

(三)拜訪盧森堡資安之家，針對臺灣-盧森堡之資安發展現況進行交流，並討論後續合作機會。

貳、參訪行程

本次以色列及比利時參訪行程自 112 年 6 月 25 日至 112 年 7 月 2 日合計 8 日，行程安排如下表：

表 1 赴以色列及比利時參訪行程表

日期	活動內容
112.06.25(日)	● 啟程前往以色列
112.06.26(一)	● 會晤台拉維夫跨域網路研究中心(ICRC)創辦人暨以色列前國家科技及研發委員會主席 Prof. Isaac Ben-Israel
112.06.27(二)	● 參加 Cyber Week 2023 ■ 大會發表演說 ■ 參加臺灣及以色列資安圓桌論壇 ■ 參加「Building Cyber Resilience at the organizational and national level」專題討論 ● 會晤以色列友台小組國會議員
112.06.28(三)	● 參訪以色列知名資安晶片新創公司 Chain Reaction
112.06.29(四)	● 會晤以色列資安公司 Pentera ● 前往比利時 ● 拜會歐洲資訊安全組織 (ECSO) ● 拜會電腦與通訊協會 (CCIA)
112.06.30(五)	● 參訪布魯塞爾自由大學 AI 學院（AI for the Common Good Institute, FARI） ● 拜會盧森堡資安之家(Luxembourg House of Cybersecurity) ● 出席歐洲民主基金會(European Endowment for Democracy, EFD)研討會 ● 拜會歐盟執委會資通訊網絡暨科技總署（DG CONNECT）
112.07.01(六)	● 返回臺灣
112.07.02(日)	● 抵達臺灣

參、參訪概要：

本次出訪行程以色列段雖由民間單位 Cyber week 主辦方出面邀請唐部長率團出席，但主辦方及我國駐台拉維夫台北經濟文化辦事處積極協調並安排下，所有以色列的行程安排皆具代表性，並取的豐碩成果。比利時段行程亦感謝我國駐歐盟兼駐比利時代表處細心安排下，與歐盟產官學端皆有正面接觸，以下謹就拜會過程分述如下：

一、 會晤台拉維夫跨域網路研究中心(ICRC)創辦人暨以色列前國家科技及研發委員會主席 Prof. Isaac Ben-Israel

訪團於6/26抵達台拉維夫後，於晚間參與由 Cyber Week 2003主辦單位台拉維夫跨域網路研究中心 (Blavatnik Interdisciplinary Cyber Research Center, ICRC)創辦人暨以色列前國家科技及研發委員會主席 Isaac Ben-Israel 教授主持的歡迎晚宴，雙方針對臺灣與以色列在共同面對全球資安威脅的各個面向進行交流。

席間也與 ICRC 的 Lior Tabansky 博士針對個人資料保護進行交流。對方提到，以色列有非常完善的全民健保制度，由政府主導，所有以色列公民和永久居民，都可以從4家民營非盈利的健康維護組織（Health Maintenance Organization, HMO）選擇1家來提供健康保險服務。也因為如此，這4家組織蒐集了非常完整的全民就醫相關記錄與資料，歷年來也進行了不少醫藥與健康相關的研究。而2018年以色列政府也開始推動整合這些資料來進行個人精準醫療的研究計畫，而這樣的做法也必然需要考慮到其個資與資安保護。除了讓民眾可以自由選擇是否要加入這個計畫之外，並對資料進行去識別化之外，以色列紮實的資安研究與產業能量，也讓這樣的計畫更能取得民眾的信任。

圖 1 唐部長、Isaac Ben-Israel 教授及駐以色列代表李雅萍（由左至右）

二、 參加 Cyber Week 2023

(一) 大會發表演說

以色列的 Cyber Week 是一個國際年度網路資訊安全盛會，每年在以色列台拉維夫大學舉辦，在過去的 12 年裡，已然成為領域專家、行業領袖、新創企業、投資者、學者、外交官和政府官員，在資安議題交流互動平台。在 2023 年第 13 屆依往例由 ICRC、Yuval Ne'eman Workshop for Science, Technology & Security 、Tel Aviv University、以色列總理辦公室國家網路安全局及外交部共同主辦。4天的議程中，有來自100多個國家/地區的11,000多名與會者，共同參與包含400多個講者，50多個圓桌會議、小組討論、研討會、論壇等。今年唐部長即應以色列資安教父 Isaac Ben-Israel 教授之邀，擔任 Cyber Week Main Plenary Keynote 講者。。

今年討論的主要主題是隨著新技術（主要是生成式人工智慧和量子運算）的進步，塑造網路安全產業的挑戰和機遇。大會由 ICRC 執行長 Gili Drob-Heistein

開場，她提到 Cyber Week 已成為吸引來自世界各地的思想領袖、專家、專業人士、投資者、新創企業、政府官員、軍事和學術界國際平台。Cyber Week 的影響遠遠超出了以色列國界，在塑造全球網路安全新局面上有著關鍵作用。

Gili Drob-Heistein 也介紹大會主席 Isaac Ben-Israel 教授進行開場致詞，他首先提到很高興能在以色列最大的大學舉辦這個年度盛會，也希望大家除了參加在大學內的各個專業的資安會議之外，也有機會多認識台拉維夫這個獨特的城市。其次，他也指出，雖然目前 Cyber 跟 AI 常常是被分別討論，但兩者之間已經有越來越強的關係。而明年2月 AI Week 也會持續在台拉維夫舉辦，也歡迎大家參加。

圖2 ICRC 執行長 Gili Drob-Heistein

圖3 大會主席 Isaac Ben-Israel

接下來的議程由 ICRC 的技術長、也是 Cytactic 資安危機管理新創公司合夥人 Menny Barzilay 來主持，他除了強調 Cyber Week 已經成為美國之外最重要的資安盛會之外，也一如往常指出了現場除了以色列當地的聽眾之外，還有來自美國、歐洲、亞洲、中東、非洲等國家的人士與會。他也提到希望大家在場內場外都能有充分的交流，在以色列以及在此會場的慣例就很直接，大家有任何問題或議題都可以直接對任何人提出來討論。

接下來由台拉維夫 Ron Huldai 市長會致詞，他提到台拉維夫是全球前5大高科技城市，對資安投資排名全球第3，在 EAME 地區 (Europe, Africa, Middle East)則排名第1。全球5.6%的新創投資是在資安領域，而在台拉維夫則高達20%。他也建議大家可以利用晚上10點之後的時間出門，體驗夜晚的城市風貌。

接下來由台拉維夫大學校長 Ariel Porat 教授致詞，他提到 ICRC 對台拉維夫大學有三個重要的面向。第一個是全球化，ICRC 跟全球各地的資安研究單位

有廣泛的而合作；其次是跨領域合作，ICRC 的研究議題不止資訊、電機等工程領域，還包括政治、社會、經濟等領域；最後是產業化，ICRC 結合了企業、新創等資安產業能量。他也表示，全球有40%的資安產業投資，是來自於以色列的公司。而這些也絕非偶然，很大的原因是因為以色列結合了其國防軍（Israel Defense Forces, IDF）對資安的重視，加上結合學校的人才培育能量，才能達成的成果。

Ariel Porat 校長也特別提到，就在1個月前，台拉維夫大學也邀請了 Open AI 的創辦人 Sam Altman，就在跟大會相同的這個會議廳進行演講與對談。雖然 ChatGPT 等生成式 AI 具備巨大的潛能，但大家也關注到這樣的新科技也會加速提升資安攻擊的能量，對資安的防護造成了嚴峻的威脅。所以我們也要更加關注並善用生成式 AI 來強化資安防護。

最後，Ariel Porat 校長也感謝籌辦此會議的 ICRC 工作人員，並感謝到場的來賓，尤其是提到來自臺灣的唐部長特別親自來參加此盛會，充分表現出對大會的重視，也希望大家都能有豐碩的收穫。

圖4 台拉維夫市長 Ron Huldai 致詞

圖5 台拉維夫大學校長 Ariel Porat 致詞

接下來由Gili Drob-Heistein執行長、Ariel Porat校長、以及Isaac Ben Israel教授共同宣佈並頒發今年由Cyber Week 執委會提名的 Cyber Shield Award 得主，Brig. General (Ret.) Pinhas Buchris，表揚他在以色列8200擔任指揮官時，以及退役後對以色列資安能量與生態系發展的貢獻。

圖6 表揚Cyber Shield Award 得主，Brig. General (Ret.) Pinhas Buchris

接下來由以色列國家網路安全局 Gaby Portnoy 局長發表演說，他首先引用數週前 Open AI 的 Sam Altman、Ilya Sutskever 提到資安防禦邊界的延伸：雖然 AI 帶來了更好的世界與未來，但也造成了新的挑戰。讓資安防護就像星際大戰中的企業號星艦，帶著大家探索未知的領域。憑藉著以色列過去的經驗與能量，更快的共同前進。包括：

1. 與多個國家的合作夥伴合作設計、建置、並擴展以色列網絡穹頂 (Cyber Dome)，作為國家和跨國合作的重要平台。

2. 與 Google 一起設計雲端 SOC 以及入口網，以便於政府與企業之溝通。

3. 與阿拉伯聯合國大公國合作，建立網絡調查和知識分享跨國協作平台 (Crystal Ball)，並結合色列微軟開發中心，為近40個白宮所領導的反勒索軟件計畫國家和組織提供服務。

他接著指出，在過去的一年裡，以色列一直在努力強化網路韌性並擴大檢測網絡攻擊的能力，揭露惡意活動，特別是伊朗的惡意活動，也成功阻攔絕大部分的攻擊活動。特別是 MuddyWater 與 Darkbit 兩個與伊朗情報部有關的網路攻擊組織，合作對以色列理工學院進行的網絡攻擊。而除了以色列，他們還攻擊土耳其、沙特阿拉伯、埃及、摩洛哥、印度、阿曼、巴林、科威特等許多國家的平民目標。以色列國防部門對伊朗的網路攻擊瞭如指掌，並正在努力以不同的方式阻止其破壞活動。

他也讚揚美國針對伊朗網路攻擊的活動，以及對情報和安全部兩名活躍網絡參與者實施制裁，因為他們共同創立了網路攻擊學院，專門培訓黑客進行惡意活動。Gaby Portnoy 局長最後表示，國際社會需要緊密合作，探索從沒有人到過的未知領域，阻止各種惡意的網路攻擊活動，這是我們共同的責任。

圖7 Gaby Portnoy 局長以企業號星艦比喻資安防護

接下來由美國總統辦公室代理國家網絡總監 Kemba Eneas Walden 律師發表演說。除了感謝大會的邀請，可以來分享她個人的經驗以及拜登政府的網路安全策略。她首先提到，隨著網際網路與數位工具的普及，網路攻擊已經擴散到政府、關鍵基礎設施、學術與教育機構，甚至連各個大中小型企業也都受到勒索軟體的威脅，網路安全的重要性與日俱增。比如過去如伊朗政府對沙烏地阿拉伯過去無理且不負責任的網路攻擊、俄羅斯將網路攻擊作為入烏克蘭的手段之一，並已擴散到其他國家，以及就在上週，國際網際安全組織對中國政府支持、以關鍵基礎設施為主要標的的網路攻擊發出警告。

而對這些網路攻擊的因應，也絕不能之著眼於短期的防護措施，需要針對網路的安全與韌性有中長期的規劃。所以拜登政府在與國際夥伴、民間企業、研究機構進行一系列的會談或磋商後，於今年3月發佈了網路安全策略。該策略以“建立一個安全、可靠、負責任的網路”為願景，期望能保障並支持目前與未來的數位科技（如生成式 AI）持續發展。其兩大基礎包括：

1. 重新平衡保障網路安全的責任：網絡空間中最有能力、最有利的參與者必須成為數位生態系的更好管理者，也就是網絡韌性不能依賴於少部分

的組織和個人的持續警惕。相反的，必須要求更多最有能力和最有利的政府與民間企業來確保我們的網路安全。

2. 重新調整激勵措施並支持長期投資：確保市場力量和公共計畫獎勵網路安全性和韌性的措施，建立 Security by Design 機制，強化對網絡安全的研發投資，並促進跨部門與公私協作。

最後她強調，基於全球的夥伴的共同的願景，需要大家有更為積極的作為，實現保障網路網路發展的安全韌性基礎環境。

圖 8 Kemba Eneas Walden 總監說明拜登政府的網路安全策略

接著由美國網路空間和數位政策無任所大使 Nathaniel C. Fick 進行演說。他從技術創新、負責任的網路行為、其他國際合作等三個面向來切入。首先，技術創新是我們未來的關鍵。它將推動我們的經濟成長，改善我們的生活品質，並幫助我們解決世界上最緊迫的問題。所以，我們必須投資於技術創新，以確保我們在競爭中保持領先地位。我們也需要持續支持研究和開發，培養技術人才，並鼓勵企業創新。

但是，技術創新也帶來了新的風險。網路攻擊、假新聞和其他網路威脅正在日益嚴重，對我們的安全和隱私構成威脅。所以，負責任的網路行為就顯得格外重要，美國會跟以色列以及理念相同的國家，共同找到應對這些新風險的方法，加強網路安全，保護我們的資料和系統。

最後，他提到幾個而未來可以跟各國持續合作的議題，包括：拜登政府在3月時簽署一項行政命令，並與10個國家共同宣佈，限制政府使用商業間諜軟體，並希望其他國家也能跟進、以及針對網路入侵的公開溯源(Public Attribution)。

圖9: Nathaniel C. Fick 無任所大使發表演說

接下來是加拿大聯邦政府網路安全中心 (Canadian Centre for Cyber Security, CCCS) Sami Khoury 主任的演說。他首先提到加拿大跟以色列雖然在地理位置跟氣候上有很大的差異，但面對的網路威脅並沒有太大的差異。CCCS 除了負責政府單位的資安防護之外，近年來也納入關鍵基礎設施、中小企業等。從2018年起，每兩年都會發佈加拿大國家網路威脅評估報告 (National Cyber Threat Assessment, NCTA)。最近一次於2022年底發佈的報告中，包括5大重點：

1. 勒索軟體仍然是加拿大面臨的最嚴重網路威脅之一，對經濟和公共安全造成重大威脅。

2. 對關鍵基礎設施的攻擊日益增加。就上週六 CCCS 的團隊還在處理一起針對關鍵基礎設施的資安攻擊。

3. 國家支持的網路攻擊是加拿大面臨的另一個重大威脅。其針對的目標除了政府，也包括商業、研究單位等。

4. 網路的威脅也會以影響對網路空間的信任，包括不實訊息、境外干涉等日益增加。

5. 新的技術帶來的機會與挑戰。先進 AI 等技術雖然帶來機會，但也對網路安全帶來新的挑戰。

面對這些威脅，CCCS 藉由堅強的資安防護能量、穩固的資訊分享網絡、國內與全球可信任夥伴的合作來共同因應，提升網路攻擊的成本，共同面對網路威脅、守護民主價值。

圖10: 加拿大網路安全中心 Sami Khoury 主任介紹國家網路威脅評估報告

接下來是壓軸的唐部長的演說，以「搶旗：捍衛臺灣民主不受境外干預」（CAPTURE THE FLAG: Defending Taiwan’s Democracy from Foreign Interference）為主題，分享我國應對複合式資安威脅、捍衛民主的經驗與因應措施。

唐部長以我國去年8月遭受的複合式網路攻擊為例，說明我國推動的重要資安政策，包括零信任架構（Zero Trust Architecture）和跨機關資料傳輸專屬通道（T-Road）。唐部長指出，去年攻擊導致部分政府官網暫時無法連線、回報超過150件資安事件，以及電子看板遭竄改；而在數位部成立後，迅速強化各項資安措施，今年蔡總統訪美期間，我國雖亦遭遇相當程度的網攻，但沒有政府官網或電子看板受到影響，回報資安事件大幅降至約40件。

唐部長並引用《未來網際網路宣言》(Declaration for the Future of the Internet)內容：「我們相信，我們應透過對於未來網際網路的共同願景，來迎向這些挑戰，重新令政府與相關機關，承諾捍衛人權及促進公平繁榮的經濟。」 呼籲各界攜手捍衛民主，對抗境外資訊操弄干擾(Foreign Information Manipulation and Interference, FIMI)。

圖11: 唐部長發表大會演說

(二) 參加臺灣及以色列資安圓桌論壇

同日下午的時段，訪團參與網路安全週圓桌論壇，就資安與 AI 議題與以國專家學者及業界領袖進行深度討論交流。論壇由唐部長及 Isaac Ben-Israel 教授開場，之後由以色列資安產業與研究機構代表分享在資安防護與新興技術發展的現況，包括：Yigal Una (INCD 前主任、CyFox XDR 公司顧問)、Assaf Kochan (8200部隊前指揮官，Sentra 公司創辦人)、Dorit Dor (Check Point 技術長)、Ronni Gamzu 教授 (台拉維夫大學 Sourasky Medical Center 主任)、Irad Ben-Gal 教授(台拉維夫大學 AI、機器學習、商業資料分析實驗室主任，CB4 Analytics 公司共同創辦人，2021年為 GAP Inc. 併購)、Lior Tabansky 博士 (台拉維夫大學安全韌性實驗室主任)。會議中主要針對新的 AI 科技對於資安防護所帶來的機會與威脅、健康醫療資料分析的機會與隱私保護挑戰、如何確保 AI 科技的正確性與透

明性等議題，進行互動的討論。

接續由數位產業署林俊秀副署長及資通安全署鄭欣明副署長，分別介紹我國建設產業數位韌性，以及推動關鍵基礎設施資安防護等重要政策。林副署長分享臺灣如何確保資安韌性的產業政策，包括推動半導體供應鏈資安國際標（SEMI E187）與導入零信任架構、App 資安檢測、晶片與物聯網資安標準，以及沙崙資安服務基地等，展現臺灣如何接軌國際，成為全球供應鏈安全可信夥伴的策略與階段性成果。

圖12：林副署長於圓桌論壇介紹臺灣資安產業政策

鄭副署長則分享我國以《資通安全管理法》為依據，建立跨部會資安聯防架構、逐步深化關鍵基礎設施防護、透過實地稽核驗證防禦措施有效性，並組織跨國攻防演練（Cyber Offense and Defence Excercise, CODE），邀集各國資安專家共同進行實戰演練，相互提升資安專業與應變能力，建立跨國聯防基礎。

圖13: 鄭副署長於圓桌論壇介紹臺灣關鍵基礎建設的資安防禦

(三) 參加「Building Cyber Resilience at the organizational and national level」專題討論

訪團並參加「建立數位韌性」(Building Cyber Resilience)會議，說明我國正推動建立多元異質通訊網路，整合地面固定網路、無線網路、海纜、衛星等通訊方式，並持續強化網路資安防護，提升數位韌性。

圖14: 唐部長針對「建立數位韌性」議題發表看法

三、　會晤以色列友台小組國會議員

晚間則與以色列國會友臺小組主席杜柏斯基（Boaz Toporovsky）等國會議員會晤，交流資安聯防、數位服務等議題，雙方皆期待促成更多數位相關領域合 作，進一步深化臺以雙邊關係。

圖15：會晤友台小組國會議員

四、 參訪以色列知名資安晶片新創公司 Chain Reaction

Chain Reaction 是以色列知名的晶片設計新創公司。其創辦人 Alon Webman 於 1999 年創立了 Mellanox Technologies，投入用於超級電腦、人工智慧、雲端運算和企業網絡等領域的高性能、低延遲和可靠的通訊產品，提供端到端 Ethernet 與 InfiniBand 智慧互聯解決方案、伺服器與儲存服務，並於 2020 年由 NVIDIA 以 69 億美元收購。之後 Alon Webman 即開始投入更具未來性的 區塊鏈/Web3、隱私強化技術。目前 Chain Reaction 的產品包括：

(一)區塊鏈系統硬體

1. EL3CTRUM ASIC: 以效率最高的雜湊計算設計的 ASIC，調整或優化在比特幣挖礦等應用實現高性能、高效能和低功耗。

2. EL3CTRUM HASHBOARD: 提供創建自己的雜湊系統所需的功率和靈活性。搭載 EL3CTRUM ASIC，同時具備 SPI 和 12C 接口、單一電源連接器、散熱器和溫度/功率監測功能，以提供高效能和穩定的運行。

3. EL3CTRUM SYSTEM: 比特幣雜湊系統具有專有的設計和即插即用功能。該系統高度反應迅速、可靠且易於使用，能夠完全掌控挖礦操 作，並顯著縮短回報時間。

(二)隱私保護技術

1. 3PU: 隱私保護處理 (Privacy Preserving Processing)是一款專用處理器/加速器，以 ASIC 與系統為用戶隱私和安全目的而定制，專為企業數據中心和雲端服務供應商設計，比市場上可用的處理器(CPU、GPU 等)更迅速的處理和加速性能。

2. 同態加密晶片: 預計 2024 年底 Tape-out。

由於工研院自 2012 年起即投入資料去識別化、差分隱私、聯合學習等隱私保護技術之研發，而針對目前 AI 以及 Web3 應用快速的發展，人們與機器的一舉一動，所產生的資料都蘊含巨大的價值，所以如何能善用龐大的資料促進社會與產業的發展，但又能避開可能潛在的安全與隱私的風險，成為數位社會與產業

首要的議題。而要防護資安、守護隱私，也就需要透過隱私強化技術確保資料應用時無關個資。

故工研院與 Chain Reaction 目前也都積極投入同態加密技術、零知識證明、安全多方運算等隱私強化技術。故工研院於 2023 年 5 月開始與 Chain Reaction 進行合作之洽談，並於本次訪團拜訪前完成合作協議之協商，並在 6/28 於 Chain Reaction 總部進行簽署。雙方將針對隱私強化技術、數位信任應用等議題，投入標準介面制定、技術研發、場域應用等項目。

在簽署 MOU 之前，首先由唐部長、李大使、Webman 執行長等開場，並由維中進行報告，提出以發展下一代隱私強化技術與應用為願景，聯結以色列、美國、以及臺灣等地在資安、晶片、應用等領域的人才與優勢，投入建立標準與介面，研發核心與應用技術，進行消費性，供應鏈、公共服務等場域試煉等之規劃。

報告後隨即進行合作協議簽署，由唐部長與駐以色列代表李雅萍共同見證，並由維中與 Alon Webman 執行長進行簽署，並結合臺灣包括：神盾（安全感測晶片設計）、帝濶（隱私強化軟硬體解決方案）、Authme（線上身分識別）等企業，以及中研院、陽明交大等學術機構，將攜手參與後續實證評估。期待這項合作能成為臺以共同投入、緊密鏈結產業生態系的典範案例。

現場參加的除了訪團成員之外，還包括駐以色列代表處科技組汪庭安組長、Chain Reaction 技術長 Oren Yoke 博士、財務長 Eran Cohen、營運長 呂學怡 (Richard Lu) 博士、資深處長 陳柏達 (Joseph Chen) 博士等

圖 16: 唐部長與李大使見證 ITRI-Chain Reaction 簽署合作協議

五、 會晤以色列資安公司 Pentera

Pentera 是一家以色列著名資安公司，提供先進的威脅發現和漏洞管理解決方案－「自動化安全驗證（Automated Security Validation, ASV)」平台，可持續發現企業的內部和外部攻擊面，並安全的驗證其對最新高級威脅的準備情況。該平台證明了利用每個安全漏洞可能帶來的潛在影響，並相應地優先處理漏洞修復。

6月29日會晤當日由 Pentera CMO（Chief Marketing Officer） Aviv Cohen 及亞太區負責人 Michael tan 負責向對方團利用實際系統畫面展示，說明 ASV 等先進資安態勢管理技術，並針對如何增進數位韌性、控管網路風險進行深入討論。

圖17 訪團會晤以色列資安公司 Pentera 相關人員

六、 比利時數位產業相關公協會

(一)拜會數位歐洲協會 (Digital Europe)

由協會貿易政策與國際事務處 Tsai-wei Chao-Muller 處長、Cristiana-Amira Cocis 專員接待，處長首先介紹了協會的主要目標：建立一個使歐洲企業和公民能夠繁榮與茁壯的數位技術的監管環境，讓歐洲能夠發展、吸引和維持世界上最好的數位人才和技術公司。

協會與成員一起研擬所有相關立法事項的產業政策立場，並為相關歐盟政策的製定和實施做出貢獻。協會會員代表了超過 45,000 家在歐洲經營和投資的企業，包括102 家在其業務領域處於全球領先地位的公司，以及來自歐洲各地的 41 個國家貿易協會。數位產業署林副署長則分享了臺灣在資訊安全與人工智慧方面的產業政策與發展現況。

(二)拜會歐洲資訊安全組織 (ECSO)

由秘書長 Luigi Rebuffi、資安政策法制與市場經理 Francesco Bordone、技術與自主供應鏈主管 Roberto Cascella 博士、應用人因與女性資及青年人培主管 Nina Olesen 等接待。Luigu 秘書長首先介紹 ECSO 是一個跨國合作的非盈利組織，致力於加強歐洲的網絡和資訊安全，以保護歐洲的數位經濟和社會免受數位威脅的侵害，是歐洲最具影響力的資安組織之一，匯集了來自大型企業、中小企業與新創、學術界和研究機構、歐洲國家或區域協會、以及地方、區域以及國家公部門的成員，共同致力於推動歐洲的資訊安全發展。

ECSO 自 2016 年成立以來，已有超過 290 個直接會員，以及數千個藉由公協會所聯結的間接會員，包括可信賴供應鏈 (WG1)、投資與市場發展 (WG2 & WG4)、網路風險管理 (WG3)、技能與人因 (WG5)、技術創新與防禦空間 (WG6) 等 6 個工作組。其主要投入議題包括：

1. 協調合作：ECSO 促進歐洲資安相關方的合作，包括政府、企業、學術界和研究機構等，共同應對資安挑戰。
2. 推動創新：該組織推動資安技術和解決方案的創新，並協助歐洲資安初創企業發展。

3. 政策倡導：ECSO 積極參與歐盟和國際層面的資安政策制定，為成員提供政策建議和指導。

4. 資訊共享：ECSO 促進成員之間的資訊共享，包括關於威脅情報、最佳實踐和資安經驗的交流。

5. 培訓與教育：該組織支持資安相關的培訓和教育活動，提高歐洲的資安專業人才水平。尤其是在女性與青年的資安人才，分別有 Woman4Cyber、Youth4Cyber 等計畫的投入。

2021 年 ECSO 並與歐洲投資銀行合作，推動了一個 20 億歐元預算的歐洲資安投資平臺。在 ECSO 介紹後，數位產業署林副署長也分享了臺灣在資訊安全與人工智慧方面的產業政策與發展現況。雙方並提到後續可以針對資安風險評級、資安人才培育、資安標準等議題進行合作洽談。

圖18: 與歐洲資訊安全組織秘書長(右3)等合影

(三)拜會電腦與通訊協會 (CCIA)

由協會公共關係處長 Alexandre Roure、協會政策經理 Boniface de Champris 接邀請 待，並 yaoGoogle 貿易政策與政府公共關係經理 Lenard Koschwitz、Intel 安全與技術政策處長 Riccardo Masucci、Cloudflare 公共政策資深經理 Petra Arts、AWS 歐洲事務公共關係處長 Arnaud David 等業界代表進行交流。Alexandre 處長首先介紹協會是一個總部在美國的國際性產業協會，成立於 1972 年。CCIA 是一個非營利組織，旨在代表和支持全球電腦、通訊、網際網路和數位創新產業。該協會的會員包括來自科技公司、數位平臺、軟

體開發商和網際網路服務供應商等各個領域的企業。CCIA 的使命是推動數位經濟的發展，促進創新和競爭，維護數位市場的開放和自由。該協會積極參與政策制定和立法過程，以確保數位技術在全球範圍內得到充分發展和應用。CCIA 著重捍衛數位權利和自由，維護企業的智慧財產權，並提倡公平競爭和開放的數位市場環境。其主要投入議題包括：

1. 政策倡導：CCIA 積極參與政策制定和法律立法過程，代表會員企業的利益，為科技產業發聲，推動數位經濟的健康發展。
2. 智權保護：該協會關注並捍衛成員企業的智慧財產權，包括專利、版權和商標等，為會員提供法律支援。
3. 數位市場開放：CCIA 倡導維持開放且競爭的數位市場，反對任何不合理的市場壁壘和封閉政策。
4. 數位隱私保護：該協會致力於保護用戶的數位隱私權利，支持制定和執行適當的數位隱私保護法規。
5. 創新推動：CCIA 支持科技創新，倡導激勵和獎勵創新的政策和措施。

本次與 CCIA 的交流主要著重在歐盟人工智慧法制規範的部分，尤其是歐洲議會剛通過 AI Act 議會版本，引起了全球各界的關注。與會的代表提到，目前產業界對此法案的看法分歧，尤其是去年底開始的 ChatGPT、大語言模型、生成式 AI 等風潮，讓各界覺得人工會智慧的監理需要更為周延的討論。

七、 比利時相關研究單位、歐盟 DG CONNECT

(一)拜會盧森堡資安之家(林副署長單獨前往)

由林俊秀副署長赴盧森堡與盧森堡資安處、盧森堡資安之家進行交流。對方出席的主管包括：盧森堡經濟部資安處處長 Francois Thill、資安之家執行長 Pascal Steichen。盧森堡資安之家 (Luxembourg House of Cybersecurity, LHC) 為盧森堡經濟部所資助的機構，其 5 年 (2021-2025) 佈局及目標策略包含：建立數位世界中的信任感並保護網路人權、加強盧森堡數位基礎建設的安全性及韌性、建立一個令人信賴、永續、安全的數位經濟。

資安之家為盧森堡各式資安相關活動之主辦者，強化全國資安韌性。其下屬單位包括：

1. Circl.Lu (電腦事件應變中心)：負責電腦資安威脅事件的回報：負責電腦資安威脅事件的回報。

2. National Cybersecurity Competence Centre, NC3 (盧森堡網路安全能力中心)：針對資源有限的中小型企業，協助其增強預防風險的能力，促使這些組織在網路安全領域，變得更有韌性。

此外，作為強化盧森堡與全球資安韌性的領航者，積極推動開展服務策略如下：

1. 推動盧森堡資安生態系：盧森堡資安生態系豐富並成長快速，能提供多元的資安解決方案。於327家資安參與者中，有73家新創公司；其中有93家以資安為核心事業的企業，共計8662名員工；其中有21家公司是過去5年間成立。共計有33家以資安為核心事業的新創公司。

2. 建立國家資安入口網，分別提供資安業者及使用者完善的資安整合服務，包括：

   (1)、 提供業者：曝光機會、專業課程、資安競賽等。

   (2)、 提供使用者：最新資安訊息、診斷、資安方案比價、工作

機會等。

3. 提供支援、加速成長、產業合作：與全國官方及民間重點產業及各式領域機構合作，包含：市府合作單位 (SIGI，提供國際及國內 IT 解決方案)、研究單位 (SnT 跨學科整合單位)、教育機構、新創加速器(Technoport)、國防單位、醫療體系等。

在資安之家的分享之後，林俊秀副署長亦分享臺灣推動資安產業與產業資安的政策，並交流雙方推動產業資安韌性強化的策略與做法，以及探討資安威脅觀測、情資分析、事件應變、資安新創與人才培育等議題。

(二)拜會 AI 公益學院 (AI for the Common Good Institute, FARI)。

FARI 為由 Vrije Universiteit Brussel(VUB) and Université Libre de Bruxelles (ULB)兩所大學及布魯塞爾首府在 2021 年比利時 AI4Belgium 活動期間，宣佈推出為共同利益而設立的人工智慧研究所。FARI 匯集超過300名人工智慧和相關學科的研究人員，圍繞著能夠造福於公眾利益的項目進行合作。該研究所將促進對可信、透明和可解釋的人工智慧進行研究。同時，它還將致力於幫助布魯塞爾地區及其居民應對各個領域面臨的挑戰。FARI 的研究人員將提供想法並參與交通、可持續發展、醫療服務、人工智慧和演算法的公民諮詢等項目。其項目將積極地讓市民參與並加強該地區關於人工智慧及其影響的教育。建立人工智慧專家、公民、企業和地方組織之間的橋樑。它將擁有三個中心：研究和創新中心、人工智慧、數據和社會智庫，以及人工智慧測試和體驗中心。

本次接待數位部訪團的 FARI 成員與介紹的主題包括：

1. Hans de Canck, Co-Director, VUB : 介紹 FARI 以及其與在地與歐盟創新機制

2. Carl Mörch, PhD, Co-director, ULB: 介紹永續與城市 AI 應用

3. Prof Gregory Lewkowicz, ULB Centre Perelman、Emilie van den Hoven, PhD, VUB LSTS: 介紹 AI 法制的未來，以及其對 FARI 等研究機構的影響

4. Julien Gosse, PhD, ULB Solvay: 介紹布魯塞爾地方政府的 AI

創新策略

5. Leon Denis, PhD, VUB ETRO imec research group: 介紹可解釋 AI 的技術

在 FARI 的專家介紹之後，唐部長也分享了分享數位部部參與國際非政府組織「集體智慧計畫」(Collective Intelligence Project, CIP)，與 OpenAI、Anthropic 等業界夥伴匯集公眾意見、凝聚各界共識，攜手處理「人工智慧對齊問題」(Alignment Problem)。

之後 FARI 為訪團導覽了其體驗中心的各項展示，包括：智慧能源社區、機器人的健康與社會福利應用、可解釋的電腦視覺技術、動物福利等。

圖19: 訪團拜會 AI 學院（FARI）

(三)唐部長參與歐洲民主基金會演講與座談

由歐盟大使館所安排由歐洲民主基金會（European Endowment for Democracy, EFD)與駐歐盟兼駐比利時代表處合辦的研討會，與各國產、官、學界與會人士分享我國去年8月遭受境外干擾的經驗，說明我方應變措施，包括零信任架構、通訊備援等關鍵策略，並呼籲與會者共同合作，攜手捍衛民主價值。

研討會由 EFD 會長波納莉（Roberta BONAZZI）女士主持，與會人士針對臺灣的資安態勢、通訊備援、我國如何與歐盟合作等議題踴躍提問，現場互動熱絡。

圖20 唐部長分享臺灣資安做為並接受提問

(四)拜訪資通訊網絡暨科技總署 (DG CONNECT)

6月30日拜會歐盟執委會資通訊網絡暨科技總署（DG CONNECT），就臺歐盟數位領域相關議題廣泛交換意見，期深化臺歐盟與臺比數位領域多元議題之連結。

肆、心得與建議：

以色列 Cyber Week 已成為全球知名的資安盛會，憑藉以色列政府與軍方、學術與研究機構、新創與資訊軟體與服務等三方緊密合作的生態體系，後續將在全球網路安全防護與資安產業發展持續扮演重要的角色。此外，Chain Reaction 藉由聯結以色列、美國、以及臺灣之人才，從區塊鏈跨入 Web3隱私防護技術與晶片之研發，對與臺灣合作亦抱持積極的態度。

歐盟 DG CONNECT 積極進行 eIDAS、AI Act 的法規調適，雖然兩者皆牽涉到非常廣泛的技術、政策與法規的議題，但可以預期其所建立的治理框架，勢必對全球數位產業與數位社會造成深遠的影響，需持續密切關注其進展。

本此訪團在八天拜訪了以色列及歐盟所在地比利時，針對資安政策、產業發展、AI 規範等議題與各界進行拜會交流，收穫豐碩，就本次出訪有下列議題建議：

(一)以色列資安生態與產業有其獨特之發展環境與優勢，尤其針對資安產官學研之合作，可作為臺灣資安展業發展之借鏡，但並不宜直接複製其發展模式，應思考是否有互補與合作之處。

(二)Chain Reaction 在新一代同態加密技術已有很好的基礎，後續可積極攜手開發用於全同態加密、零知識證明等尖端晶片之實證場域，結合臺灣產業共同發展新一代 AI 與 Web3 應用的安全隱私解決方案。

(三)除了持續跟歐盟 DG CONNECT 就臺-歐盟電子簽章互通進行規劃之外，亦須針對歐盟區塊鏈服務基礎設施（European Blockchain Services Infrastructure, EBSI）及歐盟數位身分（European Digital Identity Wallet, EUDI），加速了解並掌握現況與未來發展。

(四)針對盧森堡資安之家，後續可由資安署與產業署分別針對資安威脅觀測、情資分析、事件應變、資安新創與人才培育等議題，進一步進行交流與後續合作之洽談。

伍、附件：

一、唐部長 Cyber week 2023 Main Plenary 簡報

二、產業署林副署長簡報

三、資安署鄭副署長簡報

四、歐洲資訊安全組織（ECSO）介紹簡報