出國報告（出國類別：研究）

107 年組團出國專題研究資通安全班

服務機關：行政院等 17 個機關
姓名職稱：徐副處長嘉臨等 22 人
派赴國家：以色列、德國
出國期間：107 年 8 月 31 日至 107 年 9 月 16 日
報告日期：107 年 11 月 15 日

摘要

本班係以資通安全為主題，並就「資安政策規劃及發展策略」、「關鍵資訊基礎設施之資安防禦機制」、「資安產業發展」、「資安人才培育」及「IoT 與資安防護」等 5 個研究重點，遴選相關業務機關中高階研究人員參與，藉由研習以色列國家網絡安全生態圈、培育網絡專業人才及資助網絡產業等議題，並實地參訪資安攻防人才培訓及物聯網安新創等資安產業；與德國聯邦資訊安全局就國家資安作業推動進行交流，並參訪資安相關的研究中心，了解德國資安研究趨勢及人才培育等，讓本班人員除增加本身業務職掌上更多元的看法與見解外，並能將學習成效具體回饋於業務推動，以持續規劃及推動我國資通安全管理政策，提升國家整體資安防衛能力。

目次

圖目次

本文

一、目的

當前全球先進國家皆將數位經濟視為國家社會進步暨經濟轉型的重要策略，蔡總統提出數位國家、智慧島嶼的國家發展戰略，行政院也於 105 年 11 月提出「數位國家・創新經濟發展方案」，在建構有利數位創新的基礎環境，鞏固數位國家基磐，打造數位國家創新生態系，提升我國資訊國力。

我國在 90 年 1 月成立行政院國家資通安全會報，截至 105 年已完成了 4 個階段資安相關整備作業，如資安責任等級分級、設置資安長、政府機關資安監控中心、資安事件通報應變及資安情報分享等機制，106 年啟動第 5 階段國家資通安全發展方案，以「完備資安基礎環境、建構國家資安聯防體系、推升資安產業自主能量及孕育優質資安人才」為推動策略，作為打造數位國家之碁盤。

107 年 5 月 11 日資安法經立法院三讀通過，奠定我國課予公務機關與特定非公務機關負擔資通安全維護責任之法治基礎，有助全面推動關鍵資訊基礎設施的資安防護作業；107 年 9 月 14 日亦公布我國第 1 部國家資通安全戰略報告：資安即國安，亦指出為突破資安防衛能力的困境，我國應進一步加強資安機制、資安人才培育及資安產業自主研發。

為持續規劃及推動我國資通安全管理政策，提升國家整體資安防衛能力，本班研究係以資通安全為主題，並以「資安政策規劃及發展策略」、「關鍵資訊基礎設施之資安防禦機制」、「資安產業發展」、「資安人才培育」及「IoT 與資安防護」等 5 個研究重點，遴選相關業務機關中高階研究人員參與，以瞭解先進國家經驗，透過國外參訪研習行程與主題研究，讓參與之機關人員，除提升本身業務職掌上不同的看法與見解外，並能將學習成效具體回饋於業務推動，作為後續業務規劃之參考，並落實於資通安全政策推動與執行。

二、過程

本班於 107 年 8 月 31 日至 9 月 16 日期間參訪以色列及德國之資安推展情形，以下分別就相關內容進行說明：

(一)以色列部分

由特拉維夫大學協助安排相關課程及參訪，課程包含了「以色列與中東概覽」、「以色列的創新和創業生態圈」、「從安全稜鏡看以色列生態圈:人力資本、

產業發展和國家基礎建設」、「未來的網絡安全:物聯網、智慧城市、人工智能」、「國家網絡安全：從策略到實踐」、「國家網絡安全生態圈」、「影響運營、線上社群媒體和資訊戰」、「網絡立法與歐盟一般資料保護法規」、「網絡教育：培育網絡專業人才」、「挑戰：培育網絡研發的人力資本」、「資助網絡產業：經驗教訓與未來趨勢」、「物聯網安全與防護：風險和機會-私營部門的觀點」、「網絡解決方案的演進-進進退退」、「網絡安全和國家安全」、「指揮你的思維邁向成功」，涵蓋了以色列的文化及歷史演進，導引該國走向高科技建國及推展高科技經濟為國本的政策方向與處理原則，也論述了未來的走向。

圖 1　政府參與資安之必要性

1、資安發展策略

以色列因與鄰國長期處於戰亂，以色列的高軍事預算、攻防武器研發及全民皆兵制度，被認為是目前資安技術及人力的重要關鍵基礎；以色列一開始是向各界尋找資源滿足他們的資訊化需求，同時引入了國際大廠在以色列設置研發中心，也帶來了大公司的經驗、知識、物流、人力資源及行銷全球的相關資源，輔以推動高科技經濟及全球行銷的政策方向，加上以色列重視教育並鼓勵思辨傳統，造就創新不怕失敗的民族性，是他們網安技術創新及產業發展亮眼之根源。

以色列打造國家級的網絡安全生態圈，主要由政府、企業及學校等 3 個面向來發展。在政府部分，目前是由國家網路安全指導委員會(Israel National Cyber Directorate, INCD)統管整體網絡安全的工作，直接對總理負

責，約250位成員，設有技術研發(Technology Uuit)、安全強化(Robustness Unit)及操作營運(Operation Unit)等 3 個主要單位，分別負責網安技術能量提升、各層面安全防護指引(如關鍵基礎設施防護、產業引導等)、資安事件資訊蒐集及處理；另設有支援單位，負責策略規劃、國際合作、法律諮詢、人事及後勤等。

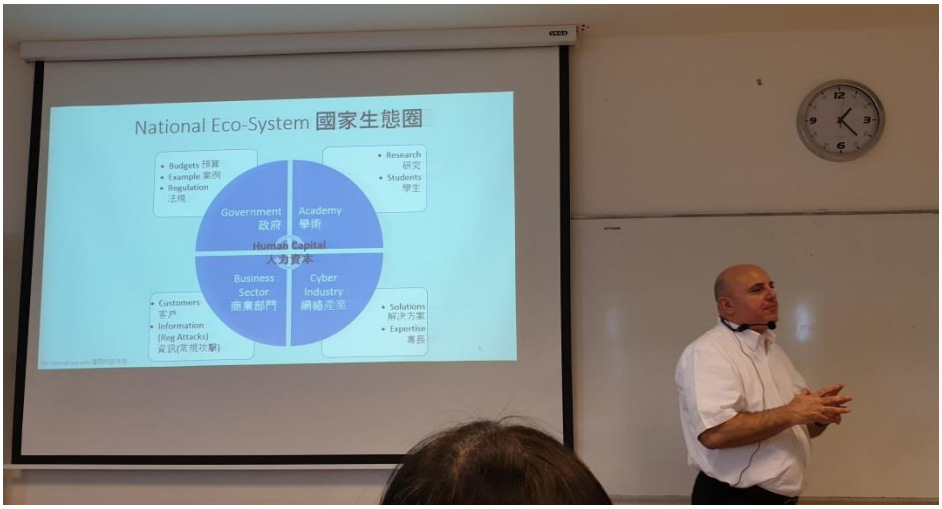

圖 2　打造國家生態圈

以色列自 2002 年即建立相關的資安組織進行業務推展，其相關演進及作業情形說明如下：

(1)國家情報安全局(National Intelligence and Security Authority, NISA)：

2002年成立，對資訊安全領域的關鍵基礎設施進行規範，其任務包括：認定特定基礎建設是否為關鍵基礎設施；關鍵基礎建設中資訊相關的人事任命同意權；指導資安相關的政府部門人員；管理轄下機關的關鍵基礎設施的業務面審查和財務審計。

NISA 的審查人員可依法對被監管單位在網路安全系統和關鍵基礎設施上的防護措施進行全面的風險評估和系統性的安全審查，被監管單位須配合辦理及時分享資訊，否則將受到處罰，在關鍵基礎設施保護上，NISA 扮演監管機構的角色。

(2)國家網路局(Israel National Cyber Bureau, INCB)：

於 2012 年成立，主要是以色列將資安發展視同作戰，自 2011 年起即視國家資訊安全為最優先政策，爰成立此一組織，負責協調該國的各政府機關和國防網路安全工作，保護國家基礎設施避免遭受網路攻擊，並就網

路安全領域的立法和法規問題提供總理諮詢意見。

(3)網路安全監管機構(National Cyber Security Authority, NCSA)：

2016 年於總理辦公室成立 NCSA，任務為制定國家網路政策，並促進國家安全方面的應用，亦即制定國家網路安全戰略。自 2017 年 3 月以來，NCSA 負責指導各關鍵基礎設施組織，包括以色列電力公司和以色列鐵路，如何應對網路風險。

NCSA 於 2016 年提出 4 項國內網路優先發展事項，分別為：提升針對現在和未來網路挑戰的能力；強化以色列國家基礎設施的保護能力；提升以色列作為全球資訊科技開發中心的地位；鼓勵學界、產業界、私人企業、政府部門之間的跨領域合作。

而針對 CIP(Critical Infrastructure Protection，關鍵基礎設施保護)，保護標的擴及全國大小設施，包含：政府機關、銀行、部分製造產業、石油、天然氣、水利、電力、醫院、通訊、航空、鐵路、海運、證券，和社會安全機構。同時，藉由以色列國防軍(Israel Defense Forces, IDF)建立符合當局要求的網路安全結構，協助偵防國內通訊系統。

(4)國家網路安全指導會(Israel National Cyber Directorate, INCD)：

於 2018 年成立，係以色列政府在 2017 年底將 NCSA 及 INCB 整合為一個機關，其任務包括保護民用網路空間、發展國家網路防禦能力，及提高以色列應對網路安全挑戰的能力。INCD 還負責推動提升以色列在網路領域的國際影響力，特別是在網路相關知識和技術發展方面，希望能佔據世界領先地位。

以色列政府部門網絡安全戰略採 3 層次架構，包含第 1 層「強化平時防護整備能力(Aggregate Robustness)」：強調各組織平日即須投注網安防護資源，當單一個體均能做好防護，國家整體防護能量自能提升；第 2 層「強化事件應處能力與防護韌性(Resilience)」：事件發生即時應處恢復運作，注重預警情訊分享及漏洞修補；第 3 層「國家層級防禦(National Defense)」：注重駭侵源頭追查及事件管理，與情報機關合作，嘗試找出攻擊者，以全面應對網安威脅。今(107)年 4 月委員會的重要決議要求各機關應投入 8%的資訊預算在資安相關工作上、各部會的網絡監管單位要向委員會彙報相關資安維護計畫及作業等。

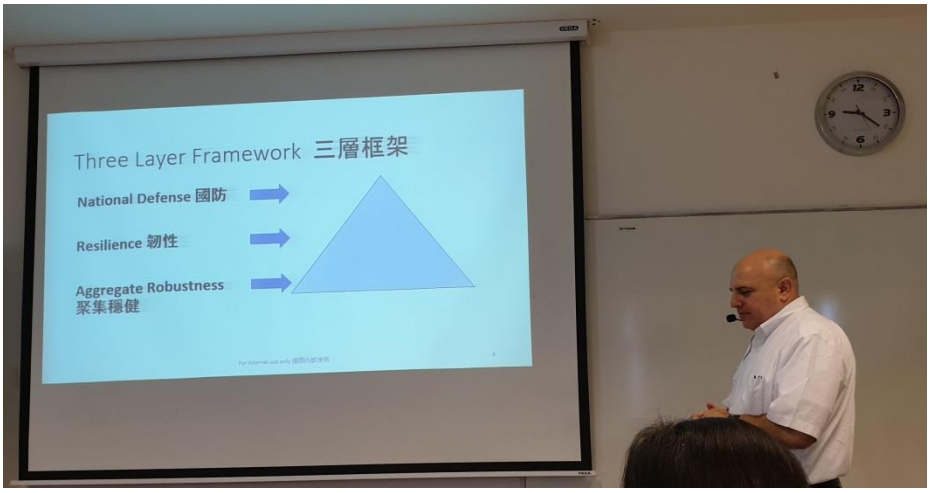

圖 3　以色列政府部門網絡安全戰略架構

因企業組織無法打造跟其他人分享資訊的機制，所以要打造一個國家級的電腦緊急應變團隊(Computer Emergency Response Team, CERT)機制，串連國家及產業之合作，此外也將各產業區分 CERT 出來，由各領域專家提供諮詢。國家級的資安監控中心(Security Operation Center, SOC)掌握國家網絡情況，而各企業依其自己的需求及資源是否成立 CERT 就不在強制範圍了。

本次行程中安排參訪以色列國家電腦緊急應變團隊(CERT-IL)，該團隊設立於 INCD 中，提供資安情報蒐集及分析。CERT-IL 非常重視提升民眾對訊息安全及隱私問題的認識和了解，強調對資安事件進行專業評估的必要性，並向民眾發布如何處理事件、防禦工具等訊息。鑒於全面性進行資安聯防作業的重要性，以色列也規定關鍵基礎設施如發生資安事件須強制回報至 CERT-IL，再依資安嚴重程度進行不同層級之通報，重要關鍵基礎設施如金融、能源等之資安事件則會進一步協調處理。CERT-IL 也與國際 CERT 進行合作，以發揮更大的聯防效果。CERT-IL 主要的任務有三：調查以及回應資訊安全的事件，進行公開的評估以及建議；協調及處理安全事件；公布威脅資訊以及防禦工具。

2、關鍵基礎設施資安聯防

此外，以色列政府部門也會就重要的關鍵基礎設施進行輔導及協助，與其共同進行資訊分享、安全防護及通報作業，提供經費給中小產業進行資安風險評估及資安概念的宣導。以色列因長年戰火使民眾對國家安全具有高度認知，在追求安全的目標下，民間團體較易形成良性競合關係，如 10 家業

者組成以色列網路聯盟 IC3，協助發展網安解決方案，這也是以色列推展網絡安全作業的關鍵因素之一。

有關關鍵基礎設施的資安攻防演練部分，本案安排參訪了 CyberGym 公司，該公司是由以色列電力公司和網路安全顧問公司 Cyber Control 共同出資成立，主要業務為替政府和私人公司提供網路資安實戰演練培訓課程，針對不同的產業客群，量身發展一套完整的資安教育訓練模式，提供仿真的場地及設備，複製實際工作環境流程，在為期數日的訓練過程中，培養學員在實務環境中防禦網路攻擊及反應能力。

圖 4　藍隊攻防演練場域

圖 5　紅隊攻防演練場域

該公司針對關鍵基礎設施資安攻防訓練，著重 2 個部份，分別是 SCADA 資安防禦認知的建構以及區分角色模擬各種資安事件的攻防演練。

(1)SCADA 資安防禦認知的建構

包含習慣養成，預期不可預期的事（Habit: expect the unexpected），將此認知內化到日常；經驗累積，模擬各種情境（Experiences: scenarios），例如：電力系統停擺、通訊環境的 DOS 攻擊、類似 Stuxnet 的可疑病毒；建立技術，透過動手做累積能量（Skills: Hands-on），在 SCADA 網路系統中搜尋各種可能的惡意程式碼，做 Pcap 檔案的分析；建構相關知識（Knowledge）。例如 Modbus 協定、PLC（Programmable Logic Controller）與暗黑能量（Black Energy）案例等專業知識。

(2)區分角色模擬各種資安事件的攻防演練

訓練團隊的技術能力並發展網路上戰術性技巧，及持續掌握最新威脅情資，同時也針對帶有較高風險的業務活動設計與實施攻防演練，該演練側重

於實際操演，而非紙上談兵。CyberGym 的攻防演練過程中配置有 4 種角色：

I. 紅隊(Red Team，攻擊員)：執行特定目標的攻擊，由來自以色列國防軍精英 8200 網路情報單位有經驗的攻擊和防禦駭客以及其他網路防禦組織的資安老手組成。其目標是在 Blue Team 防禦的技術環境中執行真實的網路攻擊，以挑戰受訓者。

II. 藍隊(Blue Team，回應員)：防禦、偵測和回應特殊網路事件，由跨組織的技術和非技術人員組成，其目標是保護組織的關鍵資產，同時盡量減少損失。

III. 白隊(White Team，引導員)：指派、評估與觀察，由以色列國家情報安全局(NISA)退休的專業老手組成，在保護和控制重大網路威脅和攻擊關鍵基礎設施方面擁有多年經驗，其目標是管理培訓課程並協調藍隊和紅隊。

IV. 灰隊(Grey Team，觀察員)：負責分析與深入鑑識檢查。

整體而言，紅隊利用各種技術和方法來挑戰藍隊，藍隊面臨攻擊則必須識別，捍衛和保護組織安全，白隊則負責管理培訓和彙報過程，評核藍隊的表現並提供建議。

圖 6　攻防演練 4 隊角色

在培訓過程則提供工業和 IT 真實設備並採用實際手動操作訓練(hands-on training)，如 PLC，防火牆，SCADA，HMI，SIEM，Snort 等。經過以上的訓練，政府機關或企業組織即可按下列步驟實施攻防演練：(1)確

認演練目標；(2)設計演練情境；(3)協調人員、資源與行程；(4)發展演練計畫與檢核表；(5)準備相關工具與環境；(6)動員 Red Team、Blue Team、White Team、Grey Team 等不同角色執行攻防演練；(7)產生計分機制及報告內容。

3、資安產業推展

資安產業在以色列佔有重要的經濟角色，其約有 50 多個加速器；300 多家創投，其中 230 家是全球基金，70 家為本土基金，政府也加入創投角色，投資國內新創，對於創投給與減稅優惠；超過 25 家跨國企業在以色列設立創新研發中心；資安公司有 300 多家，占全球 10%，年營收 40 億美金，占全球 5%，以色列約拿到全球 20%的投資，企業 2015-2016 年被收購價值約 20 億美金。

而政府也會協助企業，主要是媒合企業以全球作為市場，拓展國際合作，邀請海外投資及參與論壇以尋求合作伙伴等；另也扶助新創產業，補助有發展性的企業投資計畫，尤其是風險高的投資項目，由政府從旁協助支持，協助與國際大公司尋求國際合作的機會，補助金額甚至可以到 75%，協助承擔新創風險，若創業失敗亦無需還錢，但成功者則須回饋營利。

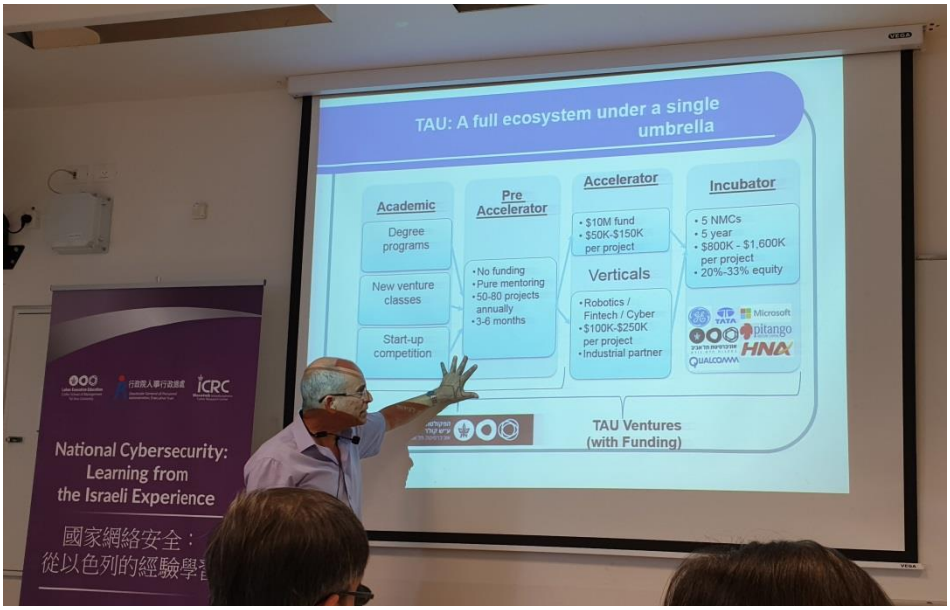

圖 7　以色列產業加速孵化機制

以色列資安創新創業生態圈是由政府-產業-大學形成「三重螺旋」產生交互作用關係。政府部門的主要角色是為打造創新創業生態圈的環境，例如投資資金、稅賦優惠、法規制定、群聚園區等。以色列經濟部創新局(前身

為首席科學家辦公室)，主導並支持產業研發政策，協助科技發展，利用其科學潛力，強化產業知識基礎，激勵高附加價值的研發和鼓勵國內及國際間的研發合作。

圖 8　資安生態群聚園區

同時政府也協助業者開發建立加速器和孵化器、創新園區、科學園區及加工出口區等，並由政府帶頭進駐，對本國企業不斷投入資源及資金，如加速器前期的專業指導(1 年有 50 到 80 個項目、3 到 6 個月)，加速器時期則有 1,000 萬美元的總投資資金(每個項目大約有 5 萬到 15 萬美金，另外，機器人/金融科技/資安領域獲投資金額較高，每個項目有 10 萬到 25 萬美金)；最後則是孵化器時期，每個項目有 80 到 160 萬美金的投資資金，可取得 20%-33%的股權。

其他協助資金投入本土企業的措施，如給予創投業抵稅、低稅率甚至免稅的優惠，在法規上，鼓勵產業研發，並減少金融業對創投公司融資的限制。創投公司對以色列資安新創公司的投資收益很高，2017 年達 230 億美金，也造就了創投公司對以色列的投資信心，全球僅次於美國。過去，以色列創投資金主要來自美國的創投公司，但近期已逐漸有亞洲資金注入，顯見全球對其資安新創的青睞。另外，出身資安新創公司的天使投資人踴躍投資資安新創公司，也是以色列能持續在全球資安創投市場取得多數資金的原因之一。

上一屆的 RSA 資安研討會有超過 550 家資安供應商參展，估計全世界約有 1300 到 1500 家資安公司，但大企業只跟其中 70 到 100 家供應商合作，新創公司的成長挑戰越來越大。在種子輪融資方面，單一公司的融資額增加，而獲得融資的新創公司數目卻減少，且大量資金湧入新創後期以推動增長和擴張，融資集中於頂尖的新創公司。這幾年資安新創公司已不再熱衷上市，而是追求快速從創投公司融資大量資金來顛覆市場或快速的退出。另外，新創公司也面臨聚焦利基市場與發展為整合產品與服務的兩難：聚焦利基市場容易被收購，但估值較低；發展整合產品與服務雖然估值較高，但時間較久、風險較高、潛在併購者也較少，目前是朝整合型產品與服務發展為主。

以色列市場小並無法支撐一個新創公司太久，所以以色列新創公司多以 Born Global 為目標，成功案例如研發世界第 1 個防火牆的 Check Point，現已是世界最知名的資安公司之一。美國幾乎是所有以色列資安新創公司的首要目標，一則因為美國約占全球資安市場 60%，而大多數的資安巨頭都是美國公司；二則因為全球投資資安新創公司的資金大多來自美國的創投公司，且英文對多數以色列人來說是第二語言，美國又有很強大的猶太或以色列人的社群關係網絡，自然使得美國為首選目標。另外，日本與英國的資安市場成長速度也十分強勁。

跨國大企業也支撐著以色列的資安生態圈，許多跨國企業如 Motorola、IBM、Intel、VMware、Cisco 等均在以色列設立網路安全創新研發中心，看重的就是以色列所培養的人才，但其實這些跨國企業帶來新觀念與技術，一方面可以把專業知識引進以色列國內，提供創新和技術想法，同時也讓年輕人有好的發揮舞台，提供歷練機會，造就了以色列的國際人才。

此外，在以色列不論男女，在完成高中教育後皆需服兵役，服役期間至少 2~3 年，除了培養獨立自主能力外，也提供了集訓與協同合作的實戰機會，戰爭講求速度，訓練快速反應及尋找成功捷徑的能力，雖不完美但符合創新所需的能力，所以其軍隊是人才培育的重要體系。軍隊裡的人員篩選機制會將入伍人員裡具有潛力者安排操作或研發高科技軍事武器，甚至納編至「8200 部隊（Unit 8200，網軍）」，退伍後，勇於創業者接受政府扶植成立新創公司，加上軍中資安專業及人脈，使其資安產業自然鏈結成形。

以色列軍事單位所研發之偵測及防禦武器，因國家安全考量，並不販售

給其他國家，但相關技術會轉型與民間公司擴大應用面向，如地對空偵測技術(含影像、定位)便應用在內視鏡膠囊檢查(Endoscopy capsules)的健康量測方面，由受檢者吞入，排出後由醫生再回收診視。

在公私合作部分，以色列政府也在國家網路局內建立網路戰情室，與網路防禦相關的社群、政府機構及私部門共享資訊。納入了學術界、網路研發、防禦等領域的專家，與大學合作進行網路安全防護研究與資安人才培養。

有關資安產業生態園，最具代表的就是 CyberSpark 生態園區，以色列以技術研發為核心，在南方貝爾謝巴(Beer-Sheba)打造此生態園區，結合了本古里安大學（Ben-Gurion University）、國家電腦緊急應變團隊(CERT-IL)、新創企業、學術研究機構及國防部等，吸引多家跨國企業研發中心進駐，形成產、官、學、研間一個自適應的完整生態圈。大學生在學習過程中可以就近實習，而畢業後也可進入企業或軍隊服務，實驗室研究成果則回饋國家或成立新創公司，CyberSpark 生態園區展現成功的營運方式及源源不絕的人才來源與技術能量。

圖 9　實地參訪貝爾謝巴園區

4、資安人才培育

面臨資通安全人才不足問題，以色列政府採取四要素策略：建立實用的課程、促進未來研發領袖、加強高中電腦學習項目及跨大資通訊科技管道，

透過教育向下扎根的方式，強化人才的培育。

以色列從小學教育即強調鼓勵理性思考，凡是質疑辯論，挑戰威權，鼓勵思考更好的想法與不斷地反省，讓創新成為生活的習慣與方式。在以色列中學階段，學校即教授資訊安全，另規定要專修網路安全，則另需要修習數學課程，以奠定強固的學習基礎。

另從高中開始即有計畫跨部會合作培育，如 Magshimim(Achievers)計畫，這個計畫是以色列國防軍聯合教育部、非政府組織(NGO)之間的人才培育合作計畫，重點放在訓練高中學生的網路技能。另外參與 Gvahim(高地)計劃的學生，會被要求 900 小時的學習時數。每天都必須學習程式撰寫、網路基礎設施，以及如何對抗網路威脅等。

以色列大學負責教育培養創新管理者的促進者角色，除了教學及研究外，更負責協調產業發展過程中之創新和創業活動。另以色列政府也選定 6 所大學做為推動資安人才培育的重點大學，補助一半經費鼓勵學校成立網絡安全的專責研究中心，並依各校專長領域進行研究及人才培育，分別是希伯來大學(網路和協議、國際法)、特拉維夫大學(跨學科)、海法理工大學(工程導向)、巴伊蘭大學(加密)、魏茲曼科學院、海法大學(隱私)及本古理安大學(應用研究)，提升人力品質，自然產出高品質的科技。相關研究並與產業合作，使研發成果進入既有產業或成立新創公司。以特拉維夫大學為例，其創造了完整的生態圈，包括學術方面的提供學士學位、新創企業課程、新創公司競賽等。

針對政府機關網絡人才培訓部分，主要區分為 3 級：第 1 級屬於基礎的人員，為執行網路安全從業人員，第 2 級屬於進階的人，可再細分為網路安全技術專員、網路安全方法專員、網路安全鑑識專員及網路安全測試專員，第 3 級為專業級的專家。

圖 10　各級資安人才培訓

不同級別的人力需求係透過國家或國際認證制度以獲得對應的相關人才，即建立資安人才證照制度，由以色列民間機構進行基礎、進階、專業網路資安證照制度之推動，且在未來必須要有執照才能擔任資安職務，每年依科技進展不斷更新知識，並透過實際執行業務自我成長，以因應網路資安環境的日益複雜。

另以色列的大學教育並不以就業市場所需人才需求為訓練重點，且私人公司大多喜歡聘用有經驗開發工程師，初入社會工作者顯少有機會進入資安相關公司，針對這問題，以色列資助成立 ITC(Israel Tech Challenge)，以編程集訓營(Disruptive Training Methods)的方式，約 2 至 5 個月完成訓練，為特定產業量身打造課程來訓練需求人才，也提供了不同背景的人能進入高科技研發領域發展的機會，填補學校到就業市場間的人才需求缺口。

圖 11　ITC 在職人力培訓

圖 12　特拉維夫大學 CyberHorse(由上千個中毒的電腦及手機零件組成)

(二)德國部分

1、資安發展策略

德國在 2005 年通過了 CIP 實施計畫，2009 年聯邦內政部(BMI)發布了「國家關鍵基礎設施保護戰略」，其中提到了關鍵基礎設施的特定資安風險和威脅。聯邦政府將關鍵基礎設施定義為「關鍵基礎設施是對國家社會和經濟重要的組織、物理結構和設施，其失敗或退化將導致持續的供應短缺，公共安全和安全的重大破壞或其他嚴重後果」。

由於德國關鍵基礎設施運營商多為民營企業，因此聯邦政府採取全面的關鍵基礎設施保護方法，2005 德國 CIP 實施計劃納入關鍵基礎設施運營商合作模式，2007 年公布的實施計畫，將這種現在被稱為“UP KRITIS”的公私合作制度化，其共同目標是改善跨部門關鍵基礎設施的保護及提高關鍵基礎設施的韌性。UP KRITIS 成員在互信基礎上交流想法和經驗，並在保護關鍵基礎設施方面相互學習，共同尋找更好的解決方案。在 UP KRITIS 的框架內，建立聯繫、舉行演習，並發展和啟動 IT 危機管理的聯合方法。另為了

確保更好的國際合作，KRITIS 成員亦定期了解歐洲有關保護關鍵基礎設施的相關活動，討論對德國的影響，並將自己的立場由聯邦資訊安全局轉達給歐盟委員會，這使得 UP KRITIS 成員有機會在早期階段影響歐洲層面的決策，進一步推動 UP KRITIS 和德國的利益。

在 2009 年時通過「聯邦資訊科技安全局法」(Act on the Federal Office for Information Security 2009)，正式指定聯邦資訊安全局（Bundesamt für Sicherheit in der Informationstechnik，BSI）為網路安全之聯邦層級主管機關，屬內政部下設機關，統籌推動資訊和通信科技安全工作。

2011 年發布「德國網路安全策略」(Cyber Security Strategy for Germany)，其目標為保護關鍵基礎設施、強化德國公民與企業的 IT 系統、建立「國家網路應變中心」(National Cyber Response Centre)及「國家資訊安全理事會」(National Cyber Security Council)。「德國網路安全策略」於 2016 年改版，強調對關鍵基礎設施的保護，同時要求公私部門建立更廣泛的網路威脅資訊分享機制，並針對政府機構與關鍵基礎設施面對的網路安全威脅做出立即回應。該策略將德國網路安全分 4 大行動領域，分別為在數位環境中採取安全而自主的行動；政府與企業間的共同努力；強固且穩定之網路安全架構；德國於歐洲及國際網路安全政策的積極定位等。

2015 年通過 IT 安全法案(IT-SiG)，保護 IT 系統及關鍵基礎設施，該法律適用於電信公司、數位服務提供商和關鍵基礎設施營運商，主管機關亦為 BSI，其下的 CK 部門即負責網路安全及關鍵基礎建設。依據該法規及 2016 年訂定之「關鍵基礎設施條例」，關鍵基礎設施包括能源、醫療、資訊科技及電信、交通運輸、媒體及文化、水、金融保險、食品、國家及行政等 9 類。

IT-SiG 要求關鍵基礎設施相關組織應維持規定的最低 IT 安全要求，並取得 BSI 許可，且須就其安全系統每兩年進行檢查是否符合規定，檢查結果應向 BSI 提出報告，BSI 有權就不足之處要求改善。針對強化安全性所採行之措施，雙方會進行協調。重要關鍵基礎設施及服務對象逾 50 萬人之企業如發生資安事件，須向 BSI 通報，BSI 會協助提供防範措施。BSI 依其職責僅就資訊安全部分進行處理，各行業之管理仍回歸其目的事業主管機關。前開 IT-SiG 法案預計 2019 年進行修正以強化規範。

德國聯邦資訊安全局（BSI）在 1991 年成立，目前是聯邦網路安全主管機關，隸屬於德國內政部，總部設在波昂(Bonn)，其下有 CK 部門(負責網絡安全及關鍵基礎設施)、B 部門(公私部門的諮詢服務)、KT 部門(公部門資安需求的加密及資訊管理服務)、D 部門(數位化政府、身分驗證及標準作業之網絡安全)及 Z 部門(與聯邦行政作業)等 5 個單位(如下圖)，員工 940 位，年度預算約 1.1 億歐元。BSI 負責管理資訊安全、關鍵基礎設施保護、加密演算法及反竊聽(尤其是對於軍事通訊)、安全產品認證和檢測實驗室之認證，基於安全的考量，BSI 會自行開發產品，進行公私合作(PPP)，由民間生產，政府採用，並由生產公司同時對外銷售。除維護數位環境的安全外，BSI 也積極與各部會及歐盟、北約組織(NATO)等國際社會合作並著重網路安全標準等政策討論。

(1)行動辦公之服務需求面向

德國推動數位化服務及行動辦公，也面臨如何提供安全、有效、友善的行動辦公環境議題，BSI 投入研發人力，提出相關的解決方案，一方面針對資料及系統面做出部分限制，另一方面又必須滿足實務使用的需求，期建構安全可靠的系統運作環境，相關考量重點如下：

I. 使用者業務需求：

資料能即時同步，使行動辦公能夠有效執行，如即時行動存取電子郵件(E-Mails)、行事曆、通訊錄，在行動環境下對組織內部網路的存取。

符合行動辦公的需求，在組織內部網路範圍外，也可以存取 Internet 網頁內容及資訊；可以存取通過檢核的 Apps。

滿足使用者期待的高可用性，如敏捷的設備操作與人機介面，語音應用能被安全地操作、運用。

II.系統安全性需求：

行動裝置須能提供安全的資料存取機制，即須存在加密機制以保護裝置上的資料；具有 PIN 保護機制及 Smartcard 認證機制，避免未經合法授權的存取；運用 VPN 連線到組織內部資訊基礎設施，以保護通訊管道和內部私有網路。

行動裝置須提供安全的語音通訊具有加密機制，簡訊服務具有加密機制，組織私有與外部公用資料須有嚴格隔離機制，具有 App 檢查機制，

避免裝置不慎安裝到惡意 APP 造成資安威脅。

III.智慧型手機面臨的資訊安全挑戰

軟體部分，現在的裝置需要使用複雜的軟體架構來滿足使用者期待的功能；軟體品質低落造成可運用來進行攻擊的程式漏洞是普遍存在的；軟體元件間的隔離非常脆弱，攻擊者有機會穿透脆弱的隔離取得裝置控制權。

硬體部分，市場上販售的現成裝置多數並不提供安全的輸入、輸出以及信任金鑰的儲存，為達到裝置的多功能性，其需要龐大的二進制韌體，但無法對這些韌體進行安全性檢視。

(2)行動服務之資安規劃

綜上需求及限制條件下，為解決前述脆弱隔離與程式錯誤等 2 個主要問題，已發展出建構可信任的智慧型手機架構，期達系統安全的目標：

I. 牢固的隔離：包含將系統中的硬軟體元件區分出需要被隔離的元件；與系統間的互動只能透過定義事先好的管道進行溝通；系統元件區分為可信任與不可信任。只有可信任的元件能夠進行處理有關資訊安全的作業。

II.建構能高度保證是可信任元件的機制：運用嚴謹的數學驗證方式做錯誤排除；進行功能屬性的驗證；能在短時間內對新版軟硬體資訊安全做評估、並能快速區分出可信任的元件。

III.符合資訊安全的可信任架構：讓被隔離、未經修改的 APP 在 Compatibility Layer 中執行。受信任的政策元件(policy objects)會對 app 與系統服務的互動做限制。受信任的裝置與驅動程式(Graphics、Touch)藉由 UI 多工器(Multiplexer)進行分享。受信任的 wrapper(VPN、Storage Encryption)讓使用不可信任的裝置與驅動程式變的安全。

在 BSI 裡的 KT 部門，負責產品的研發及認證，主要是針對政府部門使用的軟硬體設備進行資安設計或檢測，對政府部門使用的軟硬體，會先做檢測，提供使用建議，若有必須使用但有資安風險的情形時，會提供比較安全的使用建議；而在手機上的使用上，是採軟硬體搭配方式，由政府部門設計特定的 APP 作為使用服務的登入入口，用手機進入政府內部系統時，除登

打帳號密碼外，也須輔以另一實體設備進行使用者驗證，通過後才能順利使用政府的內部服務。

(3)電腦緊急應變小組

德國是由 16 個邦組成，各邦皆有電腦緊急應變小組(例如 Das CERT-Hessen)，聯邦政府亦成立電腦緊急應變小組(CERT-Bund)，歐盟機構亦設立電腦緊急應變小組(CERT-EU，該團隊由來自歐盟主要機構，它與成員國及其他地區的其他 CERT 以及專業 IT 安全公司密切合作)，原則來說德國的 CERT 屬階層式架構，各邦的 CERT 會將資訊整合回報給聯邦政府。

以 CERT-Bund 而言，其服務主要供聯邦政府使用，提供 24 小時服務，其目標為:創建並發布預防性建議以避免損壞。指出硬體和軟體產品之漏洞。提出已知安全漏洞的解決措施。遇到特殊威脅(與信息技術相關)時發出警訊並提供解決建議。

2、資安相關學術研究

德國大學除了研究與教學外，亦從事大眾資安教育的工作以及企業的教育，基於對學術自由的尊重，德國政府是讓各相關大學及研究機構自行選擇興趣領域進行研究，目前進行之研究分基礎及應用 2 類，注重跨領域學科研究是一大特色。

本次參訪之尤利希研究中心(Julich)，原為核能能源之研究機構，後轉移研究主題為資安、人腦、AI、網絡安全及數位證據分析等研究，與企業合作研究，如欲取得政府研究經費挹注，則研究主題需與德國科技部協商，提出 5 年合作研究計畫，5 年後專業機構鑑定該研究機構的績效。

圖 13　尤利希研究中心交流及合影

本次參訪的卡爾斯魯厄理工學院資訊安全應用技術研究中心(KASTEL,

KIT)，其所在的卡爾魯斯是很多企業聚集的地方，所以研究偏重在實際應用，如智慧環境、能源穩定性、智慧產權保護等，也自行研發網路隱私防護工具供大眾免費下載使用，並推廣大眾資安認知教育；而達姆施塔特工業大學及其高等資訊安全研究中心(TUD 及 CYSEC)則是專注在更安全的密碼演算法、量子電腦、網頁安全分析及虛實系統間的協作等方面之研究。

圖 14　KIT 交流及合影

圖 15　TUD 交流及合影

各研究中心除接受政府經費補助外，亦會與企業合作進行研發計畫，研發專利會移轉給企業或成立新創公司來進行市場應用。德國高科技學術研發能量豐沛，並積極推展國際合作。

(三)物聯網資安

本次在以色列參訪車聯網資安的新創公司 Karamba，該公司技術主要是結合網安及行車安全，該公司產品除偵測網路攻擊外，並有主動防禦機制，其產品機制即協助封裝後的 ECU(汽車微控制器，Electronic Control Unit)程式不允許未授權的更新，並可防阻記憶體的溢位攻擊(memory buffer overflow)，來達

到資安保護措施。

圖 16　karamba 資安公司說明物聯溢位攻擊

物聯網裝置、系統和服務都存在相關資安風險，主因多數物聯網裝置價格低廉且數量龐大，要求設計時加入資安防護意識或規劃，勢必增加成本。雖然各國深知物聯網裝置存在相關資安風險，然而國際間並未有相關裝置應經資安檢測合格，始得販售之共識，並落實在各國法規。

以色列及德國政府雖深知資安防護之重要性，但尚未如我國般規劃推動物聯網裝置資安檢測認證服務，惟為確保政府機關使用之連網設備具一定之資安防護能量，德國政府會依北大西洋公約組織或歐盟資安規定對其進行資安評估；以色列政府則要求應設置取得專業證照或經受訓合格之資安專責人員進行資安評估。

三、心得及建議

本次在參訪以色列及德國的各項課程學習、企業參訪及機關交流中，各組分別就所負責主題內容進行他國觀點與做法的了解及比較，以下分別從資安政策推動、關鍵資訊基礎設施防護、IoT 防護、資安產業發展、資安人才培育等面向，綜整提出本團之心得建議。

(一)資安政策推動

以色列跟德國的資安組織架構，皆有主要的統籌機關，掌握整體資安狀況、確認重要的關鍵基礎設施、結合情報機關進行資安防護作業，並有法規供執行依循，也結合大學或研究中心進行研發及人才培育，過程中結合理論與實務，

讓學生至企業實習，便利銜接人力資源需求，而研發成果也會轉化至企業進入經濟循環。另建構資安生態圈，有助於資安推動，而人力資源是最重要的核心關鍵，如何藉由短中長期的人才培訓及吸引外來人才等，都是我國後續可以思考努力的方向。

以、德2國都有國家級網路安全戰略方針，訂定產業發展方向及績效指標，投入大量資源及配套，殊值學習。我國國家安全會議甫於今(107)年9月14日發布首部資安戰略報告，推動總統所宣示「資安即國安」之政策，亦具備國家級的政策規劃，也期待能借鏡以色列及德國之經驗來持續發展執行。

1、在國家資安推動組織架構方面：

(1)我國刻正建立國家級資安聯防機制，資安法也已立法通過，各相關部會及關鍵基礎設施也積極配合辦理，是以整體的推動及範圍建議應明確並加以宣導，讓各界更清楚相關權責，有助於共同努力推動。

(2)資安推動作業應可評估納入白帽駭客貢獻所長，協助滲透測試、弱點掃描，甚至編成紅隊攻擊，應能提高政府資安強度及能力。

(3)我國中央政府組織有總員額法規定，不像以色列可以針對資安需要一直改造資安組織，因此若要如同以色列經常變動資安組織架構並不可能，是可擴大民間參與範圍 ，例如由民間公司代為進行驗證，以緩解公務機關繁重工作，且資安工作往往「高手在民間」，或能收取驗證報酬，民間公司就可能延攬白帽駭客協助，有利促進公私部門參與資安工作。

(4)以色列的首任國家網路局長，同時也是特拉維夫大學安全研究系系主任 Eviatar Matania 教授提到，大部分的網路安全都可以解決，但是最高級的駭客還是可能入侵，所以對於國安層級的攻擊要有不一樣的解決方案，除了必須快速恢復回到正軌，甚至要能反擊。因此，對於國安層級的駭客攻擊，我國亦應培養應變能力，以因應突發狀況。

(5)以、德的 CERT 資訊都向上集中通報，以掌握全國的資安訊息；國內目前係由行政院國家資通安全會報技術服務中心協助提供政府機關事前安全防護、事中預警應變、事後復原鑑識等技術支援服務，然各關鍵基礎設施須有不同的處理技術及因應方法，相關的資安攻防處理人力及技術需與時俱進，建議應以更彈性、更能吸納相關專業人才的組織方式(如行政法人)來補強此重要的基礎技術能量。

2、資安治理模式：

(1)為積極推動國家資通安全政策，加速建構國家資通安全環境，提升國家競爭力，行政院已設有「國家資通安全會報」，由行政院副院長兼任召集人，政府相關部會首長擔任委員，結合推動資通安全有關之機關、直轄市政府副首長及學者、專家，並由行政院資通安全處辦理本會報之幕僚作業，以成立跨部會之方式來推動強化網際防護體系、關鍵資訊基礎設施、產業發展、資通安全防護、 法規及標準規範、教育及人才培育、網際犯罪偵防等工作，然為發揮國家整體之資安政策，各單位應落實分級管理政策，設立緊急對應之支援團隊，加強內部資通安全策略和跨部會之協調合作，並進行策略施行前後的績效評估，以加強政府資通安全。

(2)我國政府部門目前多以兼辦人力辦理資安業務，資安威脅因行動化及物聯網服務而加劇，政府部門的資安人力及能力都應儘速補強以為因應，雖然目前每個機關都要有資安專責人員之規定，惟考量機關既有的組織員額及業務負擔，建議除機關配置具獨立之資安作業相關資源外，可由上級機關成立資安小組，統籌所屬機關之資安相關作業，逐步提升投入之資安資源，強化整體機關推動之可行性。

3、在政府資安人才培育方面：

(1)有關政府部門人員的資安訓練，除強化資安意識外，建議引入實務紅藍隊攻防訓練，讓政府部門的資安人力確實了解實際攻防作業，俾據以要求委託團隊的服務水準；亦可仿採購證照方式，就我國政府部門的資安人力進行能力認證(非現行的國際資安認證)，並鼓勵及獎勵同仁投入資安作業；除資安人力外，建議針對資安單位主管及機關內具資源協調權力之主管也規劃相關課程及調訓，以利機關對資安議題的重視及資源的投入。

(2)除引入企業或國外之外部資源進行師資及種子培訓外，另建議可由我國具攻防實務經驗之行政機關(如軍、警)，提供其訓練課程及師資，因其具實務強度，有利快速強化部會及縣市政府層級之資安攻防能力，再由上而下擴展。

4、在資安經費投注方面：

(1)以色列資安預算為資訊預算的 8%，民間企業負有強化本身系統的責任，資安部分通常也會參考政府的規定，編納不低於 8%的預算；德國機關(構)及頂尖大學預算，都是以億歐元為單位，我國政府機關資安預算，多從「資安旗艦計畫」及「前瞻基礎建設計畫」編列爭取，核列不易，建議擴大資安預算之投入。

(2)我國資安產業不乏新創公司(Startup)，然而臺灣市場太小，且大多不願購置國產品，造成國內新創公司難與國外代理商競爭，就算政府編列經費也難獲得政府採購，建議政府可提供輔助措施。

5、在個資保護方面：

資安法規持續配合實務修整中，而我國資安法及相關子法亦將於明(108)年施行，屆時亦可參考實務需求進行調整；然科技進步及網路普及也產生資訊安全發展之新走向，國際間亦紛紛重新規範資料保護之需求，諸如：歐洲議會及歐盟理事會於 2106 年 4 月 27 日通過歐盟規則第 2016／679 號「歐盟資料保護一般規則(General Data Protection Regulation, GDPR)」，已自 2018 年 5 月 25 日開始施行，其主要內容有：(1)擴大適用範圍，包括非設於歐盟境內但對於歐盟境內之個資當事人提供商品服務或對於歐盟境內的行為進行監控之個資控管者及處理者。(2)個資定義較廣，包括網路瀏覽器、網路 IP 位址。(3)須明確有效同意。(4)個資當事人具有更正權及刪除權(被遺忘權)、個資可攜權、拒絕權(拒絕自動化分析)。(5)書面委託歐盟境內代表。(6)個資保護影響評估。(7)指定個資保護長。(8)原則禁止個資跨境傳輸，例外取得適足性認定、提供適當保護措施、個資當事人明確同意始得傳輸至歐盟外。(9)提高罰則金額，最高將處 2000 萬歐元或全球營業總額 4%之行政罰鍰等，爰有以下建議：

(1)此次至以色列、德國研習，瞭解到該 2 國對歐盟 GDPR 亦重視以待，並檢視相關規範是否符合歐盟 GDPR 之要求，是我政府機關及民間企業亦應重視歐盟 GDPR 之規範，提早研議因應措施並研究是否修改個人資料保護法等相關法規，以與國際接軌。

(2)另為加強機密資訊與個人隱私保護，政府有責任阻止網路空間的濫用與侵犯隱私權與人權的行為，在各機關執行健全的隱私保障政策與作法，將民眾關心的身分安全及隱私保護列為推動電子化政府資通安全的工

作重點，以落實個人資料保護相關法令。

(3)又由於政府機關本身之公務機密或基於法令所蒐集的個人與企業資訊，以及關鍵基礎建設業者與企業所持有之商業機密或民眾個人資料等若發生外洩、被竄改或破壞等情事，多半會引起嚴重後果。因此對於開放外界連線作業之資訊系統，應視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之資通安全技術或防護措施，同時對於資料攜出與隨身碟等輸出入裝置須加以管理，方能維護機密資訊與個人隱私。

(二)關鍵資訊基礎設施

1、關鍵資訊基礎設施定義與範圍，應審時度勢並進行滾動檢討

首先，無論是以色列或是德國皆將關鍵資訊基礎設施(CIIP)列為首要之資安防護目標與重點，這點與我國作法一致，確符合當前國際潮流。然而，在關鍵資訊基礎設施的定義與選定的範圍上，仍依各國國情與政策略有不同。

以範圍選定而言，我國係以能源、水資源、通訊傳播、交通、金融、緊急救援與醫院、政府機關、科學園區與工業區等 8 項 CI 主要領域；相較之下，德國則多出「食品、文化與媒體」2 領域，但無「科學園區與工業區」領域。值得一提的是，德國採用一套 CI 評估方法論(MIKI Methodology)，除了以特性(Quality)決定上開領域外，還有定量(Quantity)方式，以影響是否超過 50 萬人為 CI 門檻值；以色列則強調應集中聚焦，並限縮目標的數量(如 5 個)。

考量駭客攻擊隨科技發展快速變異，且朝組織化目標性演繹，影響層面與領域勢必不斷翻新。另外，我國資通安全管理法預計自明(2019)年 1 月起施行，相關 CIIP 資安工作實際推動後，定會蒐集運作情形與改進建議，並進行滾動檢討與精進，建議屆時可將他國觀點與作法納入參考研商。

2、掌握整體資安情勢，研析國家資安健康指標有效性

延續上點說明，在以色列課程中，特別以圓桌工作坊方式，要求分析我國的網路安全與威脅，並限縮目標的數量，以 5 個 CI 為限。課堂上特別強調，應鑑別出國家真正的威脅在哪裡，以有限資源，集中保護 CI。後來參訪以色列 IL-CERT 時，看到以交通燈號協定(Traffic Light Protocol, TLP，

FIRST 標準)作為各項資安情資交換之揭露分級，並最後將相關事件依重要性、相依性、連動性、發生頻率等權重彙總後，呈現出整體國家資訊情勢指標(含顏色及百分比)，並以火車出軌事件為例子做說明。

限於參訪時間，無法對該項作法進一步了解，但可體會出以色列係以網路戰爭方式來看待，信奉實用與有效至上，只精準針對最關鍵系統進行保護監控。

建議後續可再對該項議題深入研析，瞭解實際上運作情形，並依我國現況及實務經驗，評估是否參考建立相關資安健康指標。並建議如有需要建立，公開與否也應列入研究，或以內外有別的展現方式。

3、建立 CII 資安攻防基地，兼具培訓與演練多功能

預計明年 1 月起資通安全管理法施行，相關 CII 的防護、通報、稽核、等工作將隨之展開，但現實面相關的人才與經驗亟需再加強。

本次參訪以色列 Israel Electric Corporation（IEC）CyberGym，特別為 IT、CI、IoT 等業界提供綜合性技術平台，作為資安防護專業培訓，並進行模擬資安攻擊演練與測試，以提升資安人員對外來攻擊之應變能力。

我國已納管 CII 八大領域，為深化關鍵基礎設施資安防護，建議在不影響正常運作前提下，評估擇定關鍵基礎設施領域，建立領域適用之系統攻防演練常態實測場域，培養人員應變能力，以厚植國家關鍵基礎設施網安的防護能量。建議可參考以色列 CyberGym 成功經驗，研究成立統一基地(是否結合民間資源可討論)或導入國際相關業界資源，進行第三方培訓與攻防演練，提供 CI 公私部門運營商之受訓環境及實兵演練，避免侷限於沙盤推演。

另可依據各領域之實際作業流程，可請各 CI 領域主管機關負責想定多套劇本，並研擬多重角色(紅隊、藍隊、白隊、灰隊等)，儘可能貼近實務，除保有獨特性外，可望更加深入模擬。

4、提升 CI 攻防演練擬真性，商議建立免責化共識

目前行政院國土安全辦公室或資通安全處每年會選擇 CI 進行演練作業，惟較偏向情境演練方式進行。為強化 CI 資安防護，建議可參考以色列演練之作法，就 CII 進行模擬資安測試，必要時更可進一步進行實際攻擊測試，甚至培育紅隊攻擊團隊，找出各種可能入侵的路徑，以提升資安人員對外來攻擊之應變能力。

但學習他國經驗時，如不細究國情文化，極易有盲點，甚至導致失敗。本班從出國前以色列在台代表，到以色列多名講師都不斷提及以色列人的特色之一，就是容許失敗，甚至鼓勵失敗(其實是勇於嘗試錯誤的思維)，進而型塑出以色列在新創業(含資安產業)發達的因素之一。且學員課堂提問：以色列是否對實際 CII 系統進行演練，如果造成服務中斷等結果會如何處置？講師更是強調，必須透過實際 CII 系統演練，才能真的找到潛在問題，沒有責任等問題。是以，如採行上開建議前，建議政府與 CI 公私部門運營商可以先形成免責化共識，以鼓勵性質，勇於找到問題，澈底提升 CI 資安保護能力

5、建立 CI 私部門信任感，營造公私共信協作機制

如心得所述，由於德國 CI 運營商多為民營企業，因此自 2005 年起德國 CIP 實施計畫納入合作模式，於 2007 年實施計畫將「UP KRITIS」公私合作制度化，並於 2013 進行組織結構及合作模式調整。在德國參訪時，喻稱 UP KRITIS 扮演「中間人」角色。

在 UP KRITIS 框架下，公私部門建立聯繫、舉行演習，並發展和啟動 IT 危機管理的聯合方法，成功促成參加 UP KRITIS 的產業與國家之間跨部門合作。

建議我國可以參照上開作法，營造合乎我國國情的公私合作機制。但要注意一點，因為涉及私部門或產業界，無論是以色列及德國都強調分享：必須要先建立信任感。以色列課程就曾經以「醫病關係」來比喻公私部門資安合作關係，病人生病了，不必要求他說明為什麼會得病？而是先負責醫好病。過程中，如果發現其他與病無關的，也不會另做處理。也就是說，當以色列資安部門（身分不是執法單位）進入產業時，假如發現漏稅、機敏資料，也信守保密規定，不向其他部門舉發，讓合作夥伴相信，與政府共享信息不會暴露敏感或商業資料。

6、提升民間 CI 資安防護能量，研議鼓勵或激勵機制

因 CII 具備的特性與一般資通訊設備稍有不同，例如 CII 非常著重在可用性及完整性、系統生命週期較長、作業平台除常見 Windows 與 Linux 外，還有嵌入式（Embedded）系統等。大略而言，CII 如果要強化資安防護時，除了進行安全漏洞修補或升級外，或許需要進行軟硬體汰換翻新、系統程式

改版重寫或實體安全強化等情形，可能增加運營商營業成本。依據以色列說法，民間 CI 運營商如需要協助，政府可提供資助。

資安防護是一體的，全靠政府與民間通力合作。固然民間 CI 營運商依「資通安全管理法」必須符合其所屬資安責任等級之要求，並向中央目的事業主管提出資通安全維護計畫及實施情形，並接受稽核，但是實務上如何提升民間 CI 營運商強化自身資安保護，將是執行與落實的挑戰，建議應再多蒐集國外做法，建立相關鼓勵或激勵機制。

(三)IoT 防護及資安產業

1、推動物聯網裝置資安產業標準

物聯網裝置所蒐集與傳遞的資訊可用以造福產業與廣大民眾，但數量龐大的物聯網設備，若無完善的資通安全防護機制，也潛藏著極大且多元的資安風險，並可能造成巨大危害。現行國際間並未有相關裝置應經資安檢測合格，始得販售之共識，並落實在各國法規，因此只有仰賴產業自主推動。業者將本求利，由業者自主推動恐緩不濟急，爰仍須政府介入，協助輔導，始得奏效。鑑於國家需求或關鍵基礎設施使用之連網設備，得由採購契約要求採購標的物須具備一定之資安防護能力，而民眾採購物聯網裝置時，端視其有無資安防護意識，爰建議優先推動多數民眾使用且為我國產業發展優勢之連網設備的資安產業標準。

2、催生物聯網裝置資安防護共通準則之國家標準

目前歐盟網路和資訊保安局(ENISA)及美國國家標準與技術研究院(NIST)都有發布物聯網相關資安防護共通建議。考量物聯網裝置多元，全數推動產業標準緩不濟急且不可行，但資安防護不可不為。為使政府機關、關鍵基礎設施設置者及廣大消費者，在採購尚未推動資安認證之物聯網裝置時，有一評核機制，建議我國可參考 ENISA 及 NIST，研議訂定物聯網裝置資安防護共通準則之國家標準。

3、推動物聯網裝置資安檢測環境及產品焠鍊場域，並提供物聯網裝置製造商資安防護技術輔導

建置物聯網裝置資安檢測生態鏈，包括檢測實驗室及實驗室資格之評鑑制度，完備物聯網裝置之資安檢測場域，並提供物聯網裝置製造商資安防護技術輔導及產品資安防護試煉場域。

4、推動物聯網裝置資安分級制度及認證機制

不同使用環境所需物聯網裝置資安防護層度不一，涉及國家安全者，應使用最高等級或另訂更高之要求;涉關鍵基礎設施設置者或政府機關則適用次高等級；一般環境則可選用具基本防護等級，如擬提高防護效果，則可選用高一等級之產品。

5、規定政府機關、關鍵基礎設施設置提供者、公營事業及政府捐助達一定比例的財團法人，使用之物聯網裝置須通過資安驗證或進行資安評估

由政府等相關單位率先使用經資安驗證之物聯網裝置，以帶動市場初期需求及引導物聯網裝置廠商、消費者重視資安防護之風潮，同時提高物聯網裝置製造商生產具資安防護能量產品之誘因，活絡物聯網裝置資安檢測體系。

6、催生物聯網裝置網路攻擊團隊，及早發掘資安漏洞

孫子有云知彼知己百戰不殆，如果只死守，而不思駭客想法，百密恐有一疏，一步錯至全盤皆輸。我國現已成立資通電軍，行政院亦有技術服務中心，可聯合其他白帽駭客或資安專業團體，在實驗場域，對我國具產業發展優勢之連網設備進行網路攻擊，及早發掘相關資安漏洞，並將其結果提供資安檢測推動單位及連網設備製造商，俾即時修正相關規定或發布修補程式。

7、宣導民眾物聯網裝置資安防護意識

物聯設備將充斥於生活周遭，民眾亦應有相關的資安防護意識，方能減少資安風險，可透由媒體或活動宣導民眾購買或使用物聯網裝置時，須注意相關產品的基本資安防護措施，減少個資隱私外露風險，保障民眾生命財產安全，也可藉由市場機制反映資安需求，帶動業者開發資安防護佳之物聯網裝置。

8、政府及關鍵基礎設施帶頭，帶動國內資安需求

需求導向是發展台灣資安產業的有效方法之一，政府如能創造國內對資安的大量需求，自然會吸引資金、人才投入資安產業。初期可以政府及關鍵基礎設施帶頭，導入資安解決方案，進而帶動民間資安需求，活絡國內整體資安產業。又臺灣內銷市場太小，除推動國內公私部門支持購買外，仍宜以國際市場作為發展目標。

9、建立資安攻防場域，發展新興資安技術

在智慧當道的現今社會，智慧城鄉、IoT 是未來趨勢，而關鍵基礎設施 OT 若遭駭，其影響亦十分重大，而這些場域及大型解決方案潛在的資安漏洞，仍有待進行資安攻防以及早發掘了解其弱點，除進行資安防護，進而確保國家安全外，並可藉機發展新興資安解決方案，形塑另項資安產業。

(三)資安人才培育

我國資安戰略係所謂「3x3x3國家級資安戰略」，做到三大整合、三大能力提升及三大目標，而參考以色列的經驗，當務之急宜加速培養資安人才及研發能力，並尋找適合師資及課程。以色列的資安教育向下紮根至高中，挑選優秀青少年培養網路專業，進而成為資安專業人才，由六大研究型大學(特拉維夫、理工、本古里安、巴伊蘭、希伯來、海法等六大學)參與資安領導產業，這個部分是臺灣可以學習的，亦即要落實在學培育與在職培訓兩大類之資通安全人才之培育。

1、資安教育紮根

根據資策會數位服務創新研究所「2017 年 4G 行動生活使用行為調查」報告，6 成以上台灣民眾每天使用手機 3 小時以上。數位科技如浪潮般改變產業樣貌，從生活、工作、產品到消費端徹底顛覆原本生活、學習和工作方式。然而我國中小社會或公民課程，僅教導自然人在實體社會應有之行為舉止，卻未教導如何成為適當的網路公民，更遑論如何藉由資安設備之選用，來防護自身隱私及安全，爰建議國中小社會或公民課程納入網路公民及資安防護教育。

另建議應從小開始落實資安教育，並奠定所需專業技能的基礎學科，如數學、程式編碼及英文。目前我國教育部已從 108 年起於中學課綱中加入運算思維素養的課程，並鼓勵開設程式設計的相關課程規劃，未來亦可參考以色列作法，進一步將高中數學及程式設計之成績列為申請大學資安相關系所之重要參考。

持續鼓勵大學增設資安系所，以培養更多專業資通安全科技人才，並延攬具實務業師，強調畢業即戰力。建議也可參考德國及以色列經驗及作法，從大學中選定重點研究大學，就資安再細分各相關研究領域，投入經費供其聚焦深入研究，提升我國資安技術水準。

2、資安職能培訓

(1)成立資安學院，培育資安專業人才：成立資安學院，加強與民間訓練機構合作辦理，建立長期資安專業人才培訓體系，連結各大學資安學程，整合民間資安培訓能量，提供職前、在職、轉業訓練來提高業界專業人力或提升在職人員資通安全相關知識，培訓各階層、不同領域的資安專才，並支援產業發展。

(2)資安首重實作，可師法以色列成立相關教育訓練機構，建立實戰培訓方式，課程設計內容應側重實作及演練，針對關鍵基礎領域並逐步建構產學研共用的國家級數位靶場，提供模擬環境或實驗室等全方位攻防演練的實戰場域，以驗證培訓成效及累積實戰經驗。

(3)物聯資安人才培育部分，建議亦可評估開設物聯網裝置資安攻防人才培訓場域及線上教育平臺，積極培訓相關技術領域的資安專業人才，以應未來萬物聯網資安防護所需。

(4)針對關鍵基礎設施資安人力，配置不同資安專業人力，建立人員職能地圖，並每年要求資安人才參加訓練，以提升關鍵基礎設施防禦能力。

(5)資安人才分級認證制度，就各種不同屬性及專長(如法律規範、標準制定、數位鑑識等)，提供資安人力分類分級制度，以培養出適合產業需要的人才；並建立資安人才資料庫，作為企業與人才媒合，輔導資通安全人才生涯發展，解決資安人才就業問題，進而鼓勵人力投入資安領域。

(6)擴大 CIIP 人才來源，評估軍方資源釋出管道：相關 CI 領域負責資安的人才來源不易，需具備該領域專業知識及技術，又需擁有資訊安全的專長。鑑於以色列軍方的成功案例，建議除了由產學研相關人員培養外，另可評估軍方人員，針對具備理工專長之屆退役人員，輔以資安在職訓練，提供退役後再就業與創業機會。

(7)善用資安防護專業之退休公務員資源：根據根據美國商業諮詢公司 Frost & Sullivan 指出，2022 年全球資安人力將短缺 180 萬人，比 2015 年增加 20%。目前各國對於資安人才之培育皆不遺餘力，我國大學、研究所雖有資訊系所已久，但其與資安防護專長仍有差異，現方急起直追，恐仍無法滿足市場所需。以色列學界、業界延攬軍中、政府機關現職或退休人士之案例不勝枚舉，在資安即是國安的世代，是否應適時檢討該

等退休公務員旋轉門條款，以避免我國具資安防護專業之公務人員於退休後，其專業隨著旋轉門條款而無法貢獻於其他領域。

3、強化資安生態系

加速資安新創園區籌設，鼓勵本國大型企業及資金投入資安產業，我國或可評估結合研究型大學及科學或工業園區的研發能量，建立生態圈，提供優質創新創業環境，配合提供園區完善的生活機能，提升於園區內的工作意願，並建立資安新創產業之生態系。

附錄一　研究人員名冊

學號	姓名	服務機關	職稱	組別
1	蘇俊榮	行政院人事總處	副人事長	團長
2	徐嘉臨	行政院資通安全處	副處長	學員長 第 3 組
3	張小梅	行政院資通安全處	科長	第 4 組
4	吳致仁	行政院人事行政總處	編審	總務組長 第 1 組
5	李崇偉	內政部警政署資訊室	科長	第 1 組
6	林豐裕	內政部警政署刑事警察局	簡任技正兼科長	副學員長 第 1 組
7	呂博章	財政部財政資訊中心	組長	第 2 組
8	王東琪	教育部資訊及科技教育司	科長	第 4 組組長
9	鄭健行	法務部調查局	調查專員	第 4 組
10	張春暉	法務部	參事	第 1 組組長
11	林俊秀	經濟部工業局	組長	第 3 組
12	黃貴麟	經濟部水利署	主任	第 5 組組長
13	曾信池	交通部公路總局	高級分析師	第 2 組
14	吳美琪	衛生福利部資訊處	科長	第 3 組
15	何昇龍	科技部資訊處	副處長	第 2 組組長
16	楊蘭堯	國家發展委員會資訊管理處	高級分析師	第 2 組
17	王麗惠	金融監督管理委員會銀行局	科長	第 2 組
18	廖水進	金融監督管理委員會資訊服務處	高級分析師	第 4 組
19	陳坤中	國家通訊傳播委員會基礎設施事務處	科長	第 5 組
20	鄭信一	臺北市政府資訊局	專門委員	第 3 組組長
21	林春吟	新北市政府研究發展考核委員會	主任秘書	彙整報告組長 第 1 組
22	閻俊如	桃園市政府資訊科技局	主任秘書	第 5 組
23	李春霖	高雄市政府資訊中心	科長	第 5 組

附錄二　國外參訪行程小組課堂發言紀錄

議題：9/2 從安全稜鏡看以色列生態圈：人力資本、產業發展和國家基礎建設(The Israeli Ecosystem through the Prism of Security: human capital, Industry development and national infrastructure)

Q：公部門要制定相關規定，但以色列最好的人才好像都去企業界了，不知公部門人員的任用情形？

A：政府部門很難衡量其表現績效，如國防、醫療保健、基礎設施、電力等，所以在管理上很不容易，而且基層公務員薪水很低，很難吸引人才，優秀人才大概 3 至 4 年就會離開；以前有企業界人才帶著實務經驗轉換到政府部門服務，但目前政府部門多是從大學教出來的學生，沒有經驗，僅少數是具有專業人才，是以色列公部門，有好的年輕人才，但較缺乏好的訓練及經驗。

Q：政府部門是由哪個單位在協助私部門進行網路安全管理？

A：6、7 年前以色列政府(非軍隊)就在管理網路安全，尤其是私部門；私部門間要互相交流網路安全訊息，主要是規範、串連訊息，告知企業已經被攻擊了，目前是 Lior 老師所在的委員會在管理並推動網路安全相關作業。

Q：我曾經讀過教授您在 2018 年出版的「國防與和平經濟學」(Defense and Peace economic)一書中讀過你的論文「Human and National Security」。該論文探討了人力資本與其實現有效國家安全的能力之間的關係。在您看來，如何為網路安全這個領域制定國家級人力資本戰略？

A：以色列政府機構已將網絡安全確定為主要國家安全的挑戰之一。因此，有關網路安全人力資本的政策和計劃均經過嚴格的審查。具體而言，國家應長期追蹤評估，發展整體國家資安人力，以提升當前網絡安全人力資本技能和能力。

議題：9/2 從網絡安全到數據科學與人工智能(From Cybersecurity to Data Science and AI)

Q：國家安全局的組織是否還存在？有無更好的運作機制建議？

A：2002 年時即由政府機關負責基礎設施網絡保護，當時是屬於以色列國家安全的一環，但人民對情報是有疑慮的，所以後來將民間使用網絡

空間的保護責任移轉到新機關，讓人民信任新的機關，並制定一些原則及方法，取得民間信任後即會樂於參與。新機關的處理並不進入資料層，且非執法機關的一部分，協助民間處理時若發現民間之秘密(即使犯罪)，也不會有通報問題，主要著重於檢測及處理，且績效不是找到多少資安事件，而是清除網絡世界的病毒與攻擊。

議題：9/2 特拉維夫大學奈米科技中心(TAU Nanotechnology center)

Q：如何選合作廠商進行技術移轉？

A：科技技術轉移中心研發之成果，可能會成立新的新創公司，如果是進階或特定技術取得專利，授權給企業，主要是評估其是否具市場潛力、技術能力、商品化及擴展能力。

Q：政府如何協助企業發展產業？

A：原則上政府不主導企業如何發展，但會有一些補助措施。

議題：9/3 國家網絡安全：從策略到實踐(National Cybersecurity：From Strategy to Implementation)

Q：如何讓企業將資源投注在資安防護上，以色列是如何推動的？從國家角度，如何提升整體資安防護的強度，有無類似的指標可以知道整個國家的強度情形？

A：由政府蒐集及分享資安訊息，協助企業建立警覺性及求救處理機制，建立國家級 CERT 串連政府與產業。指導委員會制定相關的規定、確認重要的關鍵基礎設施、各部會設有網絡監管單位提報網絡安全計畫及彙報網絡安全資訊給指導委員會、各部會 8%的 IT 預算投注在資安工作上等，政府部門以身作則，希望能帶動企業一塊前進。

Q: 特拉維夫大學是否為學生提供在網絡安全行業的實習機會？

A: 一般來說，我們學校均會提供學生各領域實習機會。但是特拉維夫大學目前並沒特別為學生提供在網絡安全方面的實習機會，主要是因為我們已網羅業界師資，並鼓勵學生經過在校淬練畢業後變成資安新創者。

Q:以色列的關鍵基礎設施係集中到極少數的設施或系統上，並集中資源以強化關鍵基礎設施之保護，不知台灣如何辦理?

A：而臺灣關鍵基礎設施則由主政單位指定到特定資訊系統，此作法與以

色列相同，而且台灣亦對關鍵基礎設施投入大量資源，加強保護。

Q：CyberSpark 新創園區是以色列國家網路技術生態圈的一個典範，依以色列實際運作經驗，是否需要實際把這些企業、學校及研發單位聚集一起，產生群聚效應，還是利用虛擬方式也可行？另外，國防軍 IDF 科技校區緊鄰在旁，是否也是成功因素之一？

A：其實沒有什麼必要性，在以色列本來就有一個虛擬的生態圈，以色列這麼小，如同美國矽谷一樣的小區，所以不需要具體把他們聚在一起。會成立園區，不僅是網路安全領域，事實上也是為了國土城鄉發展平衡，而軍隊也早就安排在該區域。

議題：9/3 網際網路：複雜的依賴性和新的解決方案(The Internet: Complex dependencies and new solutions)

Q：曾有利用海底電纜上的關鍵節點複製光電訊息並取走的攻擊方式，請問課程中提及的 A Hijack Detection System 可以偵測到哪些訊息是被複製過的嗎？

A：不行，本套機制主要是以蒐集、分析路由的方式來提出預警。

Q：Hijack Detection System 運用於物聯網系統之可行性及安置點？

A：可以，安置點適合在網路閘道器或系統端。

Q：提問：Hijack Detection System 的 Software agent 係佈設在他國及本國 ISP，ISP 這麼多要如何選擇？合作的 ISP 有什麼好處？

A：主要 ISP，好處是可收取服務租用月費，約 1~30 美元。

Q：以色列有無推動物聯網設備之檢測機制？

A：無此機制。

Q：邊界閘道器協議（BGP）是一個分配的演算法，用在網路之間的路由，但通常我們在追蹤國境之外的網路路由，涉及管轄權等議題，是很難做多國性跨境追蹤的，請教教材中所顯示的幾個例子，是如何做到？

A：目前我們有在日本、韓國、馬來西亞、新加玻、南非、紐西蘭及澳大利亞等國，以付費方式，洽詢當地安裝代理器（agent），定期資料蒐集分析。

Q：面對網路路由器的攻擊，國際上目前提出以資源公鑰基礎建設（RPKI）的解決方案，請問教授對這個解決方案的想法，目前以色列在推動路

由器攻擊的解決方式。

A：RPKI 是用於保護網際網路中，防止路由劫持和其他攻擊的作法，它主要利用憑證分層授權信任的方式，去檢驗路由起點授權（ROA），如自治區號碼和 IP 地址是否一致，但這種方式須所有路由都導入憑證才可充分獲得信任，目前全球導入比率約只 5%-10%，因此還有很長一段路要走，目前我不覺得可以解決路由器遭中間人攻擊的問題，以色列目前亦沒有推動計畫。

議題：9/4 網路立法與歐盟一般資料保護(Cyber legislation & GDPR)

Q：個資保護不完全是個人隱私的保護，而是追求個人隱私與公共利益間的均衡性，過度保護將妨害公共利益。GDPR 具有治外法權，其原則禁止境外傳輸，恐將造成非歐盟國家與其之間資料取得的困難，若各國都這麼做，大家的資料蒐集是否會造成封閉不流通情形？

A：個資使用與其他價值的均衡很難處理，國安工作必須處理個資，但從市民角度主張不希望再進入隱私權，所以討論出 GDPR。美國主流企業(FB, google, amazon, apple, MS)擁有全球很多個資，所以歐盟提出 GDPR 後也調整內容，且納入網際網路的情境。

Q：以色列因應歐盟 GDPR 有什麼協助產業的作法嗎？

A:若國家已通過的個資保護程度與歐洲差不多,則可以把歐盟轉到國內，以色列已被歐盟認證取得許可，所以以色列公司可以運作。由於 GDPR 已改變樣貌，所以以色列也在其監管之下，目前也在檢視現行法規有無需要一塊調整修正，以保持適當性。

Q：GDPR 被認為是史上最複雜且嚴格的規範，只要蒐集到資料就會受到 GDPR 的規範，是否意味著企業對於歐盟公民個資應該愈少蒐集愈好？

A：對，就數據分析而言，蒐集資料本來就不是愈多愈好，因此 GDPR 要求企業有關個資的蒐集、處理及利用不得逾越「特定目的」，並在最小範圍內蒐集、處理及利用。

議題：9/4 培育網絡專業人才(Cyber Education: Developing Cyber Professions)

Q：一個專業的網路安全團隊，人數大概需要幾個人？資安長（CISO，Chief Information Security Officer）需不需具備資安觀念？

A：通常 3 人以上就足以建立一個專業網路安全團隊（CSM）。另外資安長可能不是資訊專業，只是管理者，通常有專業人員協助諮詢，讓他可以做出正確判斷。

Q：韓國有 BoB，台灣 9 月亦將有資安學院，這些學院成立的目標在於訓練市場所需要的人才，以 BoB 背後有國家運作結果很不錯。ITC 是否有資助者，例如政府或大廠？目前已有 400 名學員，就業狀況？願景是為高科技產業提供 1 萬名開發工程師，各領域不同的知識，ITC 課程是否有考慮這部分的差異有提供不同的課程？

A：網路安全局及猶太相關組織，目前培訓各種背景有潛力的人，從特定領域開始，慢慢擴展領域，當發現市場有足夠需求時才開課，例如：資安產業、硬體設計，這些公司提供人才需求，與 ITC 合作。

Q：以色列資安人才培育訓練，如何能因應網路快速變化以及技術日新月異的挑戰？

A：以色列網路資安人才培育具系統化及專業化並分為三個層級，且每個專業資安人才須從第一級（基礎）開始，逐步提升至第二級（進階），再到第三級（專業），且須取得相關證照並於一定期間重新取得，以保持證照有效性，如下：

1、第一級（基礎）：網路安全從業人員（Cyber security practitioner）。

2、第二級之一（進階）：網路安全技術專員（Cyber security technology specialist）。

3、第二級之二（進階）：網路安全方法專員（Cyber security methodology specialist）。

4、第二級之三（進階）：網路安全鑑識專員（Cyber security forensics specialist）。

5、第二級之四（進階）：網路安全滲透測試專員（Cyber security penetration testing specialist）。

6、第三級（專業）：專家（Experts）。

議題：9/4 挑戰：培育網絡研發的人力資本(challenge: Developing Human Capital for Cyber R&D)

Q：TAU 很多教授都來自軍方，在台灣的大學教授多要有博士學位，請問

對大學師資應著重在學識或是實務經驗方面的看法？

A：知識是最先決的條件，但網絡安全課程需要比較多的實務經驗，在軍方或產業界的經歷可以加分，因以色列全民皆兵，所以很多學校的老師也有軍職背景，但還是需要自己有學習的經驗。

Q：台灣除了學校能量外，另外也有財團法人相關能量，以色列是否也有除學校以外的能量，如何合作？是否提供在學、在職、國防的訓練？

A：以色列僅有學校進行研究，沒有其他機關進行研究，學校基於現行優勢發展領域，不強求(軟公共工程)，缺的部分，與國際合作。必須引導學校產生自己願意成立研究機構的動力，且自己要投資一半經費。

Q：以色列政府對於大學研究經費的補助如何進行?

A：以色列政府對於各大學研究經費係採由對重點大學補助，由大學與政府各出資一半進行研究，以促使大學重視研究，並避免資源浪費，由大學與政府洽談後完成，決定投入經費。

Q：以色列高中畢業生畢業後立即服兵役，年紀還年輕，請問軍方如何選擇那些學生具有資安專才？可以說明如何培訓？軍方如何把人才留在軍中？或移轉到業界？

A：首先以色列有很大安全的威脅，需要很多高等級專業人才，軍方經過30 多年來發展出篩選機制，不同部隊有不同複雜與全面篩選程序，包括技能、智商、體力，還要去上課，已經可以很精確過濾出各類人才，分配出到適當部隊。如果是人才，其實民間的吸引力很大，軍方為了留才，只能開特別菁英課程，要求上課後，必須至少留幾年繼續服役。軍隊與民間留才的競賽還是持續進行中。

議題：9/4 資助網絡產業(Funding Cyber Industry)

Q：貴部門在 IOT 物聯網資安部分，是否有看好哪些關鍵技術的發展且已進行投資？

A：現有已投資的部分如數位化醫療手錶、數位化資產保護、還有一些交通部分的應用，像漁船上的安全保護。

Q：對於國家資助新創公司資金，請問以色列政府如何評估其績效？在多久的時間會進行衡量，如未達成預定目標之後續作法？

A：評估績效的方式很多，財務指標是其中一種，但不會是最終考量，主

要還是會看其發展潛力及市場狀況，如果產業上已經有很多這種產品，我們就會考慮轉投資，另外像專利申請數、團隊能力等亦會納入考量，一般來說大概 2 年就會進行評估。

議題：9/4 CyberGym 公司參訪

Q：Cyber Gym 以色列電力公司(關鍵基礎設施)網路安全顧問公司的資安技術訓練平台，係以紅隊(Red team)進行攻擊，藍隊(Blue team)測試防禦及復原能力，有時會有灰隊(Grey Team, 觀察員)支援分析，以及教練(Instructor)評估監控。請問藍隊(Blue team)在演練抵禦網路攻擊時，是否允許對於紅隊(Red team)演練具有反擊的能力？

A：紅隊演練的任務是攻擊，係在發現關鍵基礎設施的系統漏洞，藍隊任務是防禦，是在幫助組織發現潛在的問題，彼此的分工明確，不會混淆，也不會一成不變。如果國家有任務需要時，藍隊也可以轉變成紅隊，幫助國家發現敵國資安漏洞進而攻擊。

Q：如果關鍵基礎設已知道有安全漏洞，但無法執行漏洞修補或升級等工作，或需進行整體系統與設備更換，是否有建議處理方式？

A：只能利用隔離方式，將系統與外界連線區隔出來，降低網路安全之威脅。

Q：有關資安攻防訓練課程，一般會安排多長的時間

A：這不一定，看企業的需要而設計，有些基礎的資安觀念天數較短，只需 1-2 天，但像紅軍演練等課程，可能長達 2 星期，還是要依需求、預算，我們再設計課程內容供受訓單位選擇。

Q：Cyber Gym 提供給 Red Team 紅隊（攻擊員）進行攻擊時之演練環境，有無特別之限制，例如實體隔離等，以提高攻擊難度。

A：為求真實 Cyber Gym 提供給 Red Team 紅隊進行攻擊時之作業環境，無特別之限制，以符實際作業情境。

議題：9/5 以色列電腦緊急應變中心(CERT-IL)

Q：通常駭客攻擊時間多數為深夜或者週五晚上至週日等非上班時間，以色列 CERT-IL 內部有無輪班人員可以因應突發狀況？

A：CERT-IL 各部門每天都會有人在值勤，若安息日也會協調異教徒或不必守清規的員工留守。此外，突發事件也有資安緊急應變小組會處

理。

Q：IL-CERT 之網路事件管理中心及金融網路中心之關連性？

A：前者為一般資訊彙報處，如有涉及金融部分會進一步將訊息提供給後者處理（除金融外，該公司就能源及涉及政府等需特別處理事件另設有其他中心）。

議題：9/6 網絡權力(Cyber Power)

Q：展示的搜尋定位工具，看起來應該是使用 SS7 協定的漏洞去處理全球定位問題，有關非 SS7 協定的部分，可以處理嗎？另防禦系統可以在本國定位，但能處理外國的定位嗎？

A：這個工具沒有辦法，但可以運用其他工具來處理。

Q：請問老師你是否有為以色列軍方或國家設計相關課程？從駭客的人員特質來看，要如何培訓這樣的人才？

A：我寫了 15 個課程教材，也有核發 13 種證書，不過一般的認證或學位與駭客訓練是不相關的，有些駭客訓練課程可以在線上找到，挑選相關人員時，我不會問他是否有取得證書，主要是看他是否能跳脫框架去思考解決問題。

Q：老師您已棄暗從明擔任白帽駭客，請問和政府部門如何合作?一般請白帽駭客擔任守門員需要安裝 Agent，您的看法如何?請說明您曾經解決過的實績。

A：通常接到案子後，會做滲透測試，找出可能的漏洞，提醒業主修正。不建議安裝 Agent，除非做過安全測試才會安裝。安全防護軟體會選擇比較大廠牌的。必要時也會做紅隊測試。

Q：對於物聯網其中的智慧手機(以 google android 為例)，紅隊攻擊這些標的困難度，遠大於一般電腦系統，請問這方面的做法為何？

A：以駭客的角度，所有裝置都可以被駭。殭屍網路有很多被感染設備，接受指令做事。物聯網會讓殭屍網路攻擊更盛行，殭屍網路也很容易再發動 DDOS 攻擊。一般做法會掃描網路裡的裝置，先埋入其中一個再於網路中快速擴散(掃描、感染，自我擴張)，接著控制物聯網裝置，再往外擴。

議題：9/6 網路解決方案的演進-進進退退(The evolution of cyber solutions-there

and back again)

Q：多數企業會使用知名大廠之雲端資料庫，惟亦有評論表示知名大廠如發生安全問題，其資訊不會完整揭露，對此，以及針對銀行等更強調資料保護之行業使用雲端服務之看法？

A：企業使用雲端服務，內部仍需有資安專業人才隨時監控，才能確保使用之安全性。

Q：在 2016 年聯合國年度演講中，貴國總理宣稱：「如果駭客瞄準你的銀行，你的飛機，你的電網以及其他一切，以色列可以提供不可或缺的幫助」，以色列政府正在改變世界各國對以色列的態度，讓他們知道在網路的世界以色列可以幫助他們保護他們的人民，以色列發展資安國防已多年，至今有無前揭案例可供參考。

A：前揭宣言協助對象主要是針對第 3 世界國家提供協助，因其資安能力相對薄弱，現今網路攻擊猖獗，至今已有多項合作協助，此議題相對敏感，台灣與以色列有許多相似之處，資安能力也很強大，有機會兩國可相互合作。

議題：9/6 網絡安全和國家安全(Cybersecurity and national security)

Q：有關網絡安全，情報體系與網安部門是否有互相提供資訊的機制？

A：情報部門有責任提供國家網路安全指導委員會(INCD)所有的必要情報資訊，以協助其對民間部門提供服務，是依法的義務，但會以匿名方式處理。INCD 沒有獨立的情報來源，INCD 可決定要不要或提供什麼資料給情報部門。

Q：關鍵基礎設施的民間提供者也必須進行網路安全防範等工作，如涉及大規模系統與設備更換，以色列是否曾提供那些鼓勵措施，或是曾經資助過？

A：民間提供者如需要協助，以色列主要考慮提供租稅等優惠措施，如有特殊情況，是曾經提供過資助。

Q：以色列政府辦理關鍵基礎設施實兵演練時，有無攻擊方獲勝之紀錄或案例？

A：有攻擊方獲勝案例。以色列從小教育就是容許失敗，如果能從失敗中獲得經驗及技巧，並轉化成下次的成功，就是勝利。

議題：9/11 於利希研究中心(Forschungszentrum Julich GmbH)

Q：有關人腦相關研究是否與 AI 有關？主要是在哪個領域？

A：主要是超級電腦相關事務，用超級電腦來認識人腦，把人腦得到的輸入超級電腦裡，計算變成一個訊息，也跟人工智慧的深度學習有關係。

Q：簡報提到 security 的研究是屬於哪一方面的？

A：主要是大型集會的安全，如音樂會、足球場，不是網路安全。

Q：big data 的 5 年計畫，在哪些領域？

A：近年數據取得來源非常多，也要做處理，個人研究學者，是不可能處理這麼大量的訊息，所以需要用超級電腦來處理，一大群的科學家取得訊息，分析出哪些可用，訊息太多也是個問題，處理、儲存及分析解讀都是問題，如何讓第三者去取得訊息，也是需要研究的，儲存的數據轉化更新、個資隱私、如何取得訊息再加以利用等，是很大的研究主題。

議題：9/12 聯邦資訊安全局(BSI)交流座談

Q：GDPR 對企業有高額罰款，但對個人是沒有罰責，而在台灣是有包含對個人處罰，甚至是刑罰 ，不知歐盟如此規定的理由為何？

A：BSI 只處理網絡安全，不會對檔案的個資問題去處理，而重大案件的部分都是針對國際級的集團。

Q：有關公務同仁使用服務會經過監控機制，會不會有同仁對所有東西都須經過 BSI 的監控而有所反彈？

A：要進入聯邦部門的服務才會經過 BSI 的管控機制，如果是部會內的服務，就由各部會自行運作，並不須都經過聯邦層級的監控。

Q：德國聯邦資訊安全局（BSI）負責的職掌中有 1 項是身分識別，請問德國身分證是否有儲存民眾的生物特徵(如指紋、虹膜等)，如果有，請問政府如何防範網路攻擊或個人資料竊取？

A：我們的晶片身分證生物特徵資料以電子化方式儲存於晶片內，數位照片只有授權機關始能讀取，例如警察機關及海關單位，晶片為使用者資料和應用程式的載體，故晶片安全為重要的基礎，因此會有相關規範，因為這個業務是另一個部門負責，詳細的安全作法可向該部門詢

問，我們很樂意分享資料。

Q：德國政府對於大學或研究機構之研究經費的補助如何進行?

A：採由各大學或研究機構向政府申請，研究計畫以 5 年為期，由政府組成委員會予以審查，5 年期滿後由政府所組成之委員會，依照所訂之 KPI(如論文登載於知名學術刊物之數量)予以審查，並作為下一個 5 年計畫審查之重要參考依據。

Q：BSI 提供的手機安全連網機制，使用前需以無線方式與提供類似 Token 的裝置聯繫，以無線方式傳遞，還是有被駭的危險性，這方面應如何預防？

A：確實有，一直在精進，降低被駭可能性。

Q：德國政府有無推動民用物聯網設備之檢測機制？

A：無，只關注在政府使用之連網設備。

議題：9/13 卡爾斯魯厄理工學院資訊安全應用技術研究中心(Karlsruhe Institute of Technology, KIT)

Q：KIT 與律師及法律界的合作是屬於哪一方面？

A：主要是應用合法性的確認，如系統匿名性的做法是否適法等。

Q：德國政府如何向公眾推廣網路安全意識教育？是透過學校系統還是公共媒體管道？ 以台灣為例，中小學教師被要求教育學生如何在網路空間保護自己。 此外，教育部還開發了一個免費的網路過濾軟件，可以讓學生安裝在 PC 或手機上避免存取不當資訊。

A：基本上德國政府是透過公共媒體管道向公眾宣傳網路安全意識教育。我們希望所有公民都了解網路安全和隱私的重要性。這就是我們為公眾開發這些免費隱私保護工具的原因。

Q：物聯網環境初略可分為感知層、網路層到應用層三層，您認為哪一層進行資安防護最具效力？

A：這並非本單位專業，或許問其他單位較為合適。

議題：9/14 達姆施塔特工業大學(Darmstadt University of Technology, TUD)及其高等資訊安全研究中心 CYSEC & Fraunhofer 資訊安全研究所(SIT)

Q：有關德國資安相關議題，機關間是如何合作的？

A：各機關間會舉行會議進行協調。

Q：德國之資安相關研究，若涉及相關領域之整合研究，將如何產生主導之研究者? (參訪達姆施塔特工業大學及其高等資訊安全研究中心資訊安全研究所)

A：由各相關領域之研究團隊自行協調，以產生主導者，若有自願者多由自願者，但主導者極為辛苦，或是由研究領域中所佔研究份量較重者擔任之，通常協調後均能順利產生。

附錄三　研習行程表

一、　研習國家：以色列、德國。

二、　研習期間：107 年 8 月 31 日至 9 月 16 日（含途程）。

日期	行程
第 1 天 8/31(五)	臺灣桃園國際機場(TPE)出發
第 2 天 9/1(六)	抵達以色列特拉維夫班古里安國際機場(TLV)
第 3 天 9/2(日)	◎特拉維夫大學(Tel-Aviv University) ● 以色列與中東概覽(Israel and the Middle East at a Glance) **Prof. Uriya Shavit**, Head of The Department of Arabic and Islamic Studies and department of Religious Studies, TAU ● 以色列的創新和創業生態圈(The Israeli Innovation & Entrepreneurial Ecosystem) **Prof. Moshe Zviran**, Dean, Coller School of Managemen ● 從安全稜鏡看以色列生態圈：人力資本、產業發展和國家基礎建設(The Israeli Ecosystem through the Prism of Security: human capital, industry development and national infrastructure) **Prof. Asher Tishler,** former President of the College of Management and Dean of Coller School of Management, TAU ● 參訪特拉維夫大學奈米科技中心(TAU Nanotechnology center) **Yuval Kupitz,** Head of International Collaborations ● 未來的網絡安全：物聯網、智慧城市、人工智能(Future Cybersecurity: IoT, Smart cities, AI) **Major Gen. (Ret.) Prof. Isaac Ben-Israel,** Head of Blavatnik Interdisciplinary Cyber Research Centre
第 4 天 9/3(一)	◎特拉維夫大學(Tel-Aviv University) ● 國家網絡安全：從策略到實踐(National Cybersecurity: From Strategy to Implementation) **Prof. Eviatar Matania,** Director of the Security Studies Program, TAU. First and former Director General of the national Cyber Directorate in the Prime Minister office of Israel ● 圓桌工作坊–分析網絡安全：結構與威脅(Round Table workshop – Analyzing Cybersecurity: Structure and threats) Lead by **Prof. Eviatar Matania** ● 互聯網：複雜的依賴性和新的解決方案(The Internet: Complex dependencies and new solutions) **Prof. Yuval Shavitt,** Professor of Electrical Engineering, TAU ● 國家網絡安全生態圈(The national cybersecurity ecosystem) **Prof. Eviatar Matania**

日期	行程
	● 影響運營、線上社群媒體和資訊戰(Influence operations, online social media and information warfare) **Lior Tabansky,** Blavatnik Interdisciplinary Cyber Research Centre
	● 公司參訪：物聯網網絡安全(Company visit：IOT Cybersecurity, Karamba Security) **Assaf Harel,** Chief Scientist & Co-Founder and Amir Einav, VP Marketing
第 5 天 9/4(二)	● 公司參訪：在關鍵基礎設施的網絡安全(Company visit：Cybersecurity in critical infrastructure Israel Electric Corporation (IEC), CyberGym) **Ofer Rachman,** VP Global Sales
	◎特拉維夫大學(Tel-Aviv University)
	● 網絡立法與歐盟一般資料保護法規(Cyber legislation & GDPR) **Yoram Hacohen**, CEO of the Israeli Internet Association (ISCO-IL) ● 網絡教育：培育網絡專業人才(Cyber Education: Developing Cyber Professions) **Ziv Solomon,** Cyber Security Expert ● 挑戰：培育網絡研發的人力資本(The Challenge: Developing Human Capital for Cyber R&D) **Tom Ahi Dror,** VP Business Development at Israel Tech Challenge, Former Head of Human Capital Development at the Israel National Cyber Bureau ● 資助網絡產業：經驗教訓與未來趨勢(Funding Cyber Industry: lessons learned and future trends) **Zohar Rosenberg,** VP Cyber Investments at Elron Electronic Industries Ltd.
第 6 天 9/5(三)	◎貝爾謝巴 Beer-Sheva
	● 實地考察：發展一個新的國家網絡生態圈群集(Field study: developing a new cluster in the National Cyber Ecosystem) 網絡事件就緒團隊(CERT-IL Cyber Event Readiness Team) 內蓋夫高階技術科技園區(CyberSpark @ Gav-Yam Negev Advanced Technology Park) **Roy Zwebner,** CEO, Gav-Yam Negev Advanced Technologies Park ● 公司參訪：網絡安全解決方案-國家層級的解決方案(Company visit: Cybersecurity solutions - A country-level solution, Elta Systems Cyber division) **Dani Paslev**, Dep. Director Marketing & Sales Department
第 7 天 9/6(四)	◎特拉維夫大學(Tel-Aviv University)
	● 網絡權力(Cyber Power) **Guy Mizrahi,** white-hat, VP Cyber, RayZone ● 網絡解決方案的演進–進進退退(The evolution of cyber solutions - there and back again) **Niv David,** Department of political science and the Yuval Ne'eman Workshop for Science, Technology and Security, TAU ● 網絡安全和國家安全(Cybersecurity and national security) Major General (res.) **Yaacov Amidror**, former National Security Advisor to Prime Minister and Chairman of the National Security Council ● 指揮你的思維邁向成功(Conducting your mind towards success) Maestro **Roni Porat**, Orchestra conductor, facilitator, & Virtuoso

日期	行程
第 8 天 9/7(五)	文化參訪、整理資料及小組討論參訪心得
第 9 天 9/8(六)	搭機前往德國慕尼黑
第 10 天 9/9(日)	◎慕尼黑 文化參訪、整理資料及小組討論參訪心得
第 11 天 9/10(一)	◎慕尼黑-海德堡 文化參訪及交通移動
第 12 天 9/11(二)	◎尤利希研究中心(Forschungszentrum Julich GmbH) ● Round Table with Board of Directors **Prof. Sebastian M. Schmidt**, Member of the Executive Board Member of the Board of Director for Scientific Division I **Dr. Hyunji Park,** National and international relations, Corporate Development ● Visit to the Jülich Supercomputing Center, JSC **Dr. Thomas Eickermann,** Head of the Division “Communication Systems” at Jülich Supercomuting Centre ● Visit to the Peter Grünberg Institut, PGI-7 **Prof. Rainer Waser**, Head of the Institute, Electronic Materials at Peter Grünberg Institute
第 13 天 9/12(三)	◎波昂 Bonn ● 交流座談會：聯邦資訊安全局(Bundesamt für Sicherheit in der Informationstechnik, BSI) Dr. Welsch, Kryptotechnology Department
第 14 天 9/13(四)	◎卡爾斯魯厄理工學院資訊安全應用技術研究中心(KIT, Karlsruhe Institute of Technology) ● Introduction to KIT **Oliver Schmidt**, Deputy Head, Regional Strategy & Information Executive Officer Asia & Middle East, Business Unit International Affirs ● Introduction to the KIT Center of Information-Systems-Technologies, KCIST **Prof. Dr. Jorn Muller-Quade**, Head, Research Group：Cryptography and Security”. Institute of Theoretical Informatics ITI Director, FZI Research Center for Information Technology ● Cyber Security Research at KIT **Prof. Dr. Jorn Muller-Quade**, Head, Research Group :Cryptography and Security”. Institute of Theoretical Informatics ITI Director, FZI Research Center for Information Technology

日期	行程
	● Security-Usability-Society **Prof. Dr. Melanie Volkamer**, Head, Research Group "Security-Usability-Society:, Institute of Applied Informatics and Formal Description Methods AIFB
第 15 天 9/14(五)	◎達姆施塔特工業大學 Darmstadt University of Technology（TUD）及其高等資訊安全研究中心 CYSEC & Fraunhofer 資訊安全研究所（SIT）
	● Presentation：Cybersecurity Research at Fraunhofer Institute for Secure Information Technology ■ Cybersecurity policy & Development Strategy by **Dr. Michael Kreutzer** ■ Protection IoT & cybersecurity by **Dr. Ruben Niederhagen** ● Presentation：Cybersecurity Research at CYSEC/TU Darmstadt ■ Overview the Cybersecurity Research by **Prof. Johannes Buchmann** ■ International activities and emergent research directions by **Prof. Neeraj Suri** ■ CRISP update by **Prof. Stefan Katzenbeisser** ■ Overview CROSSING (DFG Collaborative Research Center CROSSING) by **Dr.-Ing. Johannes Braun** ■ Overview ENCRYPTO (Engineering Cryptographic Protocols Group) by **Prof. Thomas Schneider** ● Joint discussion TUD + Taiwan delegation on the way-forward on collaboration possibilities
第 16 天 9/15(六)	◎德國法蘭克福機場(FRA)出發返國
第 17 天 9/16(日)	◎抵達臺灣桃園國際機場(TPE)