出國報告（出國類別：開會）

2018年以色列國土安全暨資安大會
（Israel HLS & Cyber 2018）
出國報告

服務機關：國家通訊傳播委員會
姓名職稱：蘇思漢簡任技正
葉世湛分析師
林祐仲技正
派赴國家/地區：以色列/特拉維夫
出國期間：107年11月10日至17日
報告日期：107年12月28日

摘要

網際網路科技為人類生活帶來莫大的便利，同時也為現代資訊化社會帶來了前所未有的新世代威脅及衝擊。以色列以自身所處之艱困環境為警惕，強力發展國土安全及網際安全領域的科技；政府、集團、中小企業聚焦於相關領域，大量新創公司也致力於研發最新技術，垂直整合的創新力量促使以色列成為國際社會中國防安全及網際安全領域的翹楚。

駐臺北以色列經濟貿易辦事處邀請經濟部組團前往以色列，本會及各單位共同參與「2018年以色列國土安全暨資安大會（Israel HLS &Cyber 2018）代表團」，以拜會以色列多個重要關鍵基礎設施，並實地瞭解以色列之國土安全、網際安全與關鍵基礎設施防護等領域之應變處置規劃及相關措施，並與相關專家面對面交流。

本次國土安全暨資安大會之國際展會暨會議發表之科技範圍包括國土安全（Home Land Security，HLS）、網際安全（Cyber）、金融科技（Fintech）三大領域，本會成員在拜會公司及訪問展場攤位時，透過與專家之互動，學習以色列在資通安全方面的想法與解決方法。

目錄

壹、目的 1
貳、代表團行程 3
參、重點摘要 4
肆、心得與建議 13
伍、出國行程照片 14
陸、附錄 17

壹、 目的

蓬勃發展的網際網路科技為人類生活帶來莫大的便利，同時也為現代資訊化社會帶來了前所未有的新世代威脅及衝擊。面對現實生活及虛擬世界的資訊資產被侵略或滲透，以色列以自身所處之艱困環境為警惕，強力發展國土安全及網際安全領域的科技；不僅政府、集團、中小企業聚焦於相關領域，大量新創公司也致力於研發最新技術，而垂直整合的創新力量更已促使以色列成為國際社會中被定位為國防安全及網際安全領域的翹楚。

為提供拜會並學習以色列在國土安全、網際安全及金融安全發展的先進科技機會，駐臺北以色列經濟貿易辦事處特邀請經濟部組團前往以色列，透過經濟部國際合作處來函邀請本會及各單位共同參與「2018 年以色列國土安全暨資安大會（Israel HLS &Cyber 2018）代表團」，以拜會以色列多個重要關鍵基礎設施，並實地瞭解以色列之國土安全、網際安全與關鍵基礎設施防護等領域之應變處置規劃及相關措施，並與相關專家面對面交流。

本會出國成員則由負責國家通訊暨網際安全中心規劃建置、本會內部資訊業務、電信事業個人資料保護之單位共同派員參與，期能經由拜會及直接交流，學習以色列之相關經驗。

2018 年第五屆以色列國土安全暨資安大會之國際展會暨會議，總共集結了 160 家專業公司以及 60 位國際講者，為大眾演繹以色列備受肯定的新一代防衛科技；本次以色列國土安全暨資安大會之國際展會暨會議除了強調國土安全及網際安全二大領域外，也因應全球金融趨勢脈動特別增設金融科技展區及講座。大會發表之科技範圍如下：

一、國土安全（Home Land Security，HLS）：邊境管制、國家重要建設、網路資安保護、飛行保安、大眾交通運輸保安、大型活動及群眾管理、救護及緊急應變、執法管理等。

二、網際安全（Cyber）：國家安全、網路犯罪、交通安全、金融科技、工業

製造、企業管理及物聯網科技等。

三、金融科技（Fintech）：行動認證、數據及基礎設施、流程優化、詐騙預防及處理、法規監管、金融業區塊鏈解決方案等。

貳、 代表團行程

日期	時間	行程
11 月 12 日	10：30 至 12：30	拜會以色列電力公司 IEC
	14：00 至 16：30	拜會 Verint 公司
11 月 13 日	09：10 至 10：20	大會開幕式
	10：20 至 12：20	訪問廠商 Radiflow（攤位 C7）
		訪問廠商 CyberGym（攤位 C13）
		訪問廠商 L7 Defense（攤位 C64）
		訪問廠商 CORO.NET（攤位 C42）
		訪問廠商 Merlinx（攤位 H27）
	13：20 至 17：00	訪問廠商 GoldTec（攤位 H36）
		訪問廠商 TSG IT Systems（攤位 H60）
		訪問廠商 Barrel（攤位 F1）
		訪問廠商 Glassbox（攤位 F5）
		訪問廠商 OpenLegacy（攤位 F13）
		訪問廠商 COMMUNTAKE（攤位 C34）
		訪問廠商 KAYMERA（攤位 C14）
		訪問廠商 Intezer（攤位 C5）
		訪問廠商 1 touch（攤位 C47）
11 月 14 日	09：30 至 12：00	拜會 Radware 公司
	14：30 至 17：30	拜會 Leumi 銀行 SOC
11 月 15 日	10：00 至 12：00	拜會 Gav-Yam Negev 高科技園區
	14：30 至 18：30	訪問耶路撒冷古城區

參、 重點摘要

一、11 月 12 日：

（一）以色列電力公司（Israel Electricity Company，IEC）：

以色列電力公司（IEC）是以色列最大的電力供應公司。以色列政府擁有 IEC 約 99.85%的股權，故仍為國營事業。IEC 提供發電站的建立、維護和運行；送電和配電網等業務，也是以色列唯一的綜合電力公司，其裝機容量約占以色列總發電量的 80%，並且傳輸和分配以色列絕大部分的電力。

本會蘇思漢簡任技正詢問 IEC 是否有使用核能發電，IEC 人員回答，由於政治環境因素，所以不使用核能發電，主要是使用天然氣發電，少部分使用煤炭發電。由於以色列在北部的都市海法以西之地中海上發現了天然氣田，所以能提供充足的發電燃料。（註：2009 年，2010 年，以色列在海法以西的地中海發現了兩個巨型天然氣田，塔馬爾和列維坦氣田。2013 年，塔馬爾氣田開始供氣；2014 年，以色列和約旦簽署 150 億美元天然氣訂單，從列維坦氣田向約旦出口天然氣。）

IEC 是以風險為考量而研擬資安防禦策略，而且公司要求資安人員必須要比操作人員更瞭解各層面的技術細節。此外，IEC 也很注重員工的福利，因為員工的待遇及管理制度如果不健全，將造成員工士氣低落，容易洩漏機敏資料。

此外，IEC 的資安演練係建置實際設施及系統，對其實施攻防演練，以確保演練的真實性，但也花費許多的時間及人力，以期能達到系統不中斷及迅速復原的經營能力。

（二）Verint 公司：

Verint 成立了 20 餘年，係資安問題解決方案的專業顧問公司，並為其他組織提供重要的見解，使 Verint 的決策者能夠預測、應變及採取行動，Verint 的產品組合係利用機器學習技術和進階分析，將資訊轉化為洞察力。迄今已有超過 180 個國家、1 萬多家機構組織，包括財富雜誌所列的百大公司中 80%和政府機構，都在使用 Verint 公司的 Actionable Intelligence 解決方案。

Verint 人員介紹公司主要產品 TPS（Threat Protection System）時說明，TPS 係透過原有資安設備（如：防火牆、入侵偵測防禦系統、防毒系統）及額外安裝於終端設備（如個人電腦、伺服器）情報蒐集軟體所提供資訊及網路流量封包，經過系統的判斷機制（演算法、情報資訊資料庫等）處理後，產出有意義的資訊再供資安人員進行後續之判斷。

除了上述使用固定特徵判斷資安事件外，Verint 並使用人工智慧解析駭客行為模式，當網路行為符合更多的預設的行為模式時，就更有可能視為網路攻擊行為。而資安的基本要求，就是讓適當的人在正確的時間，用正確的方式存取適當的資料。

本會蘇思漢簡任技正在會後私下詢問研究人員，該公司是否使用中國大陸華為的產品，該研究人員表示 Verint 沒有也不會使用華為設備，因為經過檢測，有發現一些問題，但是並沒有舉出清楚的例證。

二、11 月 13 日：

（一）大會開幕式：

本次國土安全暨資安大會總裁 Shaul Mofaz（以色列退役中將，前國防部長）表示，由於網際網路無遠弗屆，已經成為在西方民主制度中一項活躍的非傳統武器，非常容易造成關鍵基礎設施遭到破壞，而且會產生無法逆轉的損害。

由於網際網路無界限，因此在物聯網時代，必須要能夠預測運用複雜演算法的網際網路攻擊，以及建立家庭中的感測器，亦即必須由實體到網際網路進行全面的防護。而 2018 國土及網際網路安全大會及展覽的目標就是對於各種問題及明日的挑戰提供解答，並建立一個企業間合作平臺，提供以色列的解決方案給各企業。

大會主席 Eli Cohen（國會議員，member of Knesset）則表示，以色列身處強敵環伺的環境，政治威脅和政治責任促使許多政府參與其網際網路安全戰略，因此網際網安全戰略必須能夠立即保護公民及其企業。

（二）代表團訪問廠商：

1. Radiflow：

Radiflow 提供國防基礎設施（如：電力、水庫與交通運輸系統）之安全評估服務，Radiflow 會先審視網路架構、相關設施，將潛在問題描繪出後，提出測試計畫，隨後啟動監控與分析網路流量，並提出可能被攻擊之弱點。

2. CyberGym：

CyberGym 透過客製化建立與企業相仿之資訊環境，並利用 Red team 實際找出已存在或潛在的資安威脅，將此邏輯以教育訓練方式傳授給企業資訊人員，使資訊人員擁有駭客思維，從攻擊角度思考如何防禦。

3. L7 Defense：

L7 Defense 產品監聽網路流量並使用人工智慧分析判斷出惡意行為後，以動態回饋機制調整阻擋規則。而 L7 Defense 為求達到良好效能，網路封包監聽數量每秒鐘僅取樣 5%，並卸載低使用率之阻擋規則。

4. CORO.NET：

CORO.NET 針對在家或非常駐辦公室工作者，提供一套確保工作者進行遠端連線時，亦能透過安全網路遠端工作。CORO.NET 提供之產品亦結合 Google map，以視覺化方式讓使用者理解附近的無線網路（Wi-Fi AP）之安全性，如果產生安全疑慮，將會對使用者示警。

5. Merlinx：

Merlinx 展出兩項產品，EAGLE 是利用中間人技術（Man in the middle，MITM），在使用者及 Wi-Fi AP 中間進行監聽，取得經過 Wi-Fi AP 傳輸的資料流，並可將木馬程式注入使用者端，對使用者進行監聽。（使用小到可放入被包裝的中間人攻擊套件取得經過 Wi-Fi AP 傳輸的資料流，就算是加密的資料也可經解密後萃取出有意義的資料。）而 MARS 則是可以遠端控制受感染的裝置並執行特定指令。但是這兩項產品只提供給政府的司法部門與警察機關使用，並不出售給民間企業。

6. GoldTec：

GoldTec 之產品光學 IFF（Identification Friend or Foe）主要是利用熱能信標（Thermal beacon）做到敵我識別，同時利用高功率的可見紅外線雷射指標器標示攻擊目標，以利友軍發起精準之飽和攻擊。GoldTec 也製造軍用高解析度之數位視訊記錄器，以及移動式軍用通信電臺車輛，該車輛可隨時隨地架起高 20 米的直立鐵塔，可架設發射機，鐵塔乘載重量可達 900 公斤。

7. TSG IT Systems：

TSG IT Systems 使用影像分析引擎分析監視器即時拍到的影像，再經過規則引擎分析切割出來的影像後，即可對可疑行為發出警示。該系統也可分析過去錄製的歷史影像。

8. Barrel：

Barrel 透過 Email、Uber 帳單等方式蒐集個人資料，經過切塊拆分成各種類型的資料並加密後，透過區塊鏈 smart contract 的方式提供給客戶分析統計使用。Barrel 的客戶並無法直接取得個人資料，僅能使用 Barrel 提供的介面分析出使用者的特性，以提供公司進行策略之運用。

9. Glassbox：

Glassbox 之產品主要目的為分析使用者在網站上之行為（例如：點擊 A 連結後，再點擊 B 連結）。Glassbox 分析之方法為建立相關腳本，並比對使用者行為與腳本是否有差異，若有不同，則提供使用者實際行為之所有相關資訊，回饋給企業，讓企業重新設計網頁之瀏覽流程，以期能達到精準訊息之傳遞或提高銷售業績。

10. OpenLegacy：

由於許多企業（例如：銀行）至今仍使用老舊大型主機（mainframe）系統，因此，對資訊人員而言，升級與維護是艱鉅的課題。OpenLegacy 之產品則提供一套中介服務，可介接在企業之舊系統上，讓企業可透過此中間層提供之介面進行系統功能之新增與修改。

11. COMMUNTAKE：

COMMUNTAKE 與 KAYMERA 提供類似之集中控管服務。差異在於 KAYMERA 專注在軟體面，而 COMMUNTAKE 則兼顧硬體，即使駭客拿到使用者手機後，亦無法破解入侵。

12. KAYMERA：

KAYMERA 提供一集中管理系統，管理使用者之手機（使用者手機需安裝代理程式 agent）。資安人員可透過此系統調整手機內 App 之使用權限，並建立相關的規則，以確保使用者不受資安威脅。

13. Intezer：

Intezer 將 DNA 概念引用至惡意程式中，並建立惡意程式 DNA 資料庫。分析系統將需要分析之惡意程式先採集其 DNA，並從 DNA 資料庫中比對，找尋該惡意程式是否源自某惡意程式家族。

Intezer 分析系統亦有脫殼（unpacked）技術，該系統會先偵測惡意程式是否使用加殼技術，若有，則將該惡意程式脫殼，隨後再採集 DNA 進行比對。若遇到無法偵測出之加殼技術，則該系統會動態運行此惡意程式，並將相關程序從記憶體中取出，再採集 DNA 進行比對。

14. 1 touch：

1 touch 利用獨特 PII（Personally identifiable information，個人可識別資訊）技術，協助客戶發掘公司資料庫中所持有之個人資料，並進行分類及分析，同時利用機器自動學習技術發掘或監控資料流向，確保資料庫安全。

三、11 月 14 日：

1. Radware 公司：

Radware 目標係協助企業建置網際網路安全和提供模擬資安防護的應用解決方案，並提供資安軟硬體服務及最安全的雲端服務中心服務等。

Radware 為本代表團做了兩份簡報，重點如下：

（1） 3G/4G 訊息集中在核心網路伺服器（Core Network Server），而 5G 把能在 Edge 處理掉的事情儘量留在 Edge 處理（稱為邊緣運算），好處是訊息可以不用經過層層關卡送回核心網路處理而造成塞車，壞處則是使用者容易因為誤動作或惡意目的對系統造成破壞，或者是邊緣伺服器容易被駭客攻擊造成資料洩漏。

在 5G 網路中物聯網（IoT）的運用將更為活耀，但也同時帶來威脅。IoT 裝置通常因為成本低，沒有良好的軟體設計，因此造成資安防護能力不足，容易淪為駭客跳板或變成殭屍網路（Botnet）執行 DDoS 攻擊的工具，也有駭客利用 IoT 來作為數位貨幣或虛擬貨幣（Digital Currency）的挖礦工具。

Radware 的產品 DefensePro 是結合 DoS 防護、行為分析、IPS 攻擊緩解的設備，DefensePro 透過行為分析技術來進行攻擊緩解，除了可防護網路層攻擊外，還可以針對第七層的內容進行檢查，並提供 IPS 防護功能，可說是一臺多功能的資安設備。

本會葉世湛分析師則提問，現今 DDoS 攻擊常達到 10Gbps 甚至 100Gbps 的流量，造成連外頻寬被塞滿，而不是網路設備被擊垮時，除了跟網際網路接取服務業者購買清洗流量的服務外，是否還有其他解決方法，該公司人員表示這事無法處理。

Radware 的產品哲學是迅速的 Mitigate（減輕）傷害，而不是要求完全地解決問題。因此在處理新型態攻擊產出新阻擋規則時，他們使用「修改規則-->量測-->修改規則-->量測」的反覆流程，在有限的時間內，最後產出一組可接受，但可能並非最佳的規則，在最大化減輕新型態攻擊造成之損害狀況下，讓使用者感受最少的限制使用服務。此一務實思維值得學習。

2. Leumi 銀行資安監控中心（Security Operation Center，SOC）：

Leumi 是以色列最古老的銀行，也是中東地區領先和最大的公司之一。該銀行如今在以色列全國擁有 250 家分行，並在主要金融交易點設有分支機構和辦事處。

Leumi 銀行為所有客戶提供銀行服務，包括家庭，中小型企業到大型企業。

這些服務通過專門的業務線提供，每一個業務線專門為具有類似特徵和需求的客戶提供銀行和金融服務。

Leumi 銀行建立了自己的資安監控中心（Security Operation Center，SOC），此 SOC 整合了四個監控部門，故亦稱為融合中心（Fusion Center），分別為負責銀行實體網路及 ATM 監控的實體中心（Physical Center）、負責銀行網路服務資安事件監控的網際中心（Cyber Center）、負責內部實體安全控管的安全中心（Security Center）、以及負責內部網路防火牆、IPS 等資安防護設備監控的監控中心（Monitoring Center）。

Leumi 銀行的融合中心在必要時，可以針對所有 ATM 進行遠端封鎖。此外，Leumi 銀行有培養自己的道德駭客，以協助銀行提升資通安全防護能力。

Leumi 銀行的網際中心任務宣言為：在提供有效及差異化防護及資訊情報風險管理（Risk Management），使資安威脅及風險容忍能達到一致時，促成及提升企業策略。

Leumi 銀行的資安監控中心建置廠商 ACID Co-Founder Yariv Maroely 表示，Leumi 銀行會從社群網路，網路聊天室，暗網（Dark Net）等來源，自動蒐集可能的新形態網路攻擊，並產出對應處理方式。

本會蘇思漢簡任技正詢問 Leumi 銀行的高階主管，以色列是否允許虛擬貨幣，例如比特幣（Bitcoin）在國內使用，該主管表示，以色列不允許使用虛擬貨幣。（Leumi 銀行的精神標語為：勇敢領導、謙虛學習。）

四、11 月 15 日：

1. Gav-Yam Negev 高科技園區

以色列為實踐其首任總理 David Ben-Gurion 的願景，要開發以色列南部地區，距離特拉維夫約 1 小時車程的 Be'er Sheva 地區成為高科技園區。經過以色列國防軍（Israel Defense Force，IDF）提出數位轉型及轉移至南部（Digital Transformation and Migration to the South）的計畫，要設計出一個新的國家生態系

統，包括推動六大目標：工業、數位校園、學校計畫、學術、資料中心計畫、IDF數位轉型。

在 2013 年 9 月 Gav-Yam Negev 高科技園區（Advanced Technologies Park）落成，本-古里安大學（Ben-Gurion University）負責發起並推展。此園區係結合了軍事科技（國防軍電信司及精英部隊）及先進科技產業，以及美國 KUD 公司共同成立。園區內有醫院、大學、鐵路、研究機構、公司等。

以色列規劃了數位演進之步驟是：數位化-->數位媒體-->數位企業-->社群-->社群媒體-->社群企業，最後在未來則要達成：連結（connected）+適應（adaptive）+情報（intelligence）的成果。

而成功的關鍵在於創新（innovation）：以協調（coordination）推動建設及資通訊技術、以機構方法（organization methodology）推動技術及採購；以有效率的決策推動策略夥伴及合作關係。以色列國防軍的未來願景是要建立起以色列的國家基礎建設、經濟、就業、福利、學術的全生態系統。

最後在參觀園區內一家設計製造小型機器人的新創公司，機器人的特性為低耗電、低成本，其中一種能因應各種地形改變自己的型態，目前的應用為外掛攝影鏡頭做為偵查用，以及自動採收蘋果。另一種微型機器人則已經能成功穿過實驗用的豬腸，進一步改良後可做為人類體內診查或微創手術之用途。

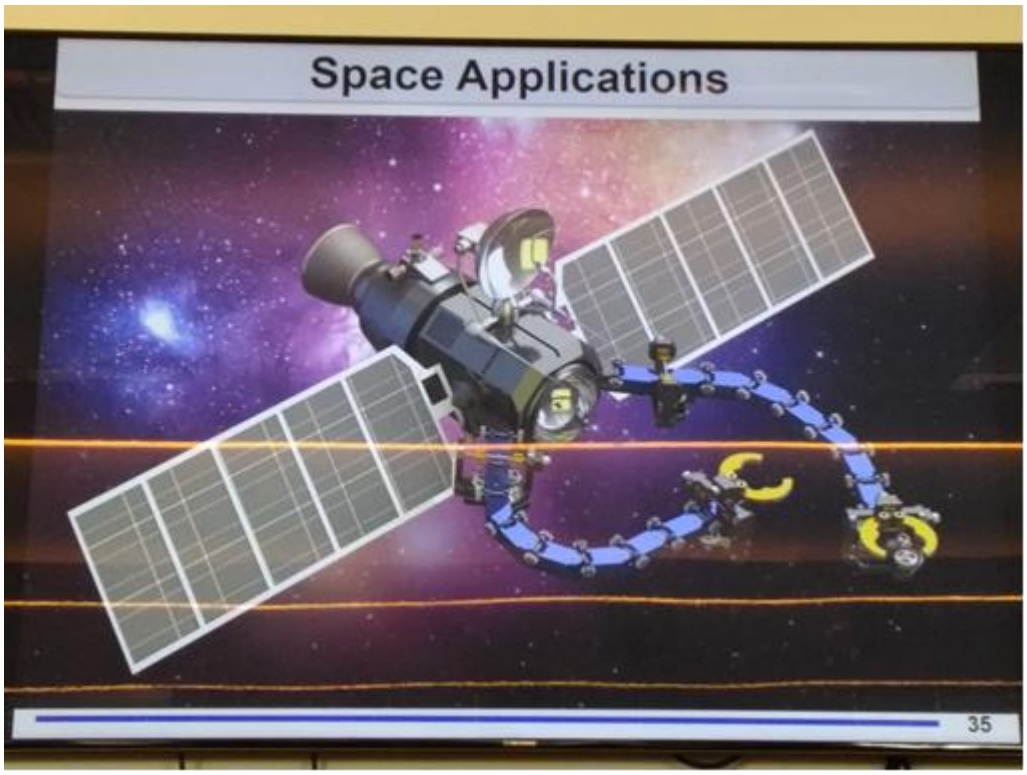

圖 1　機器手臂

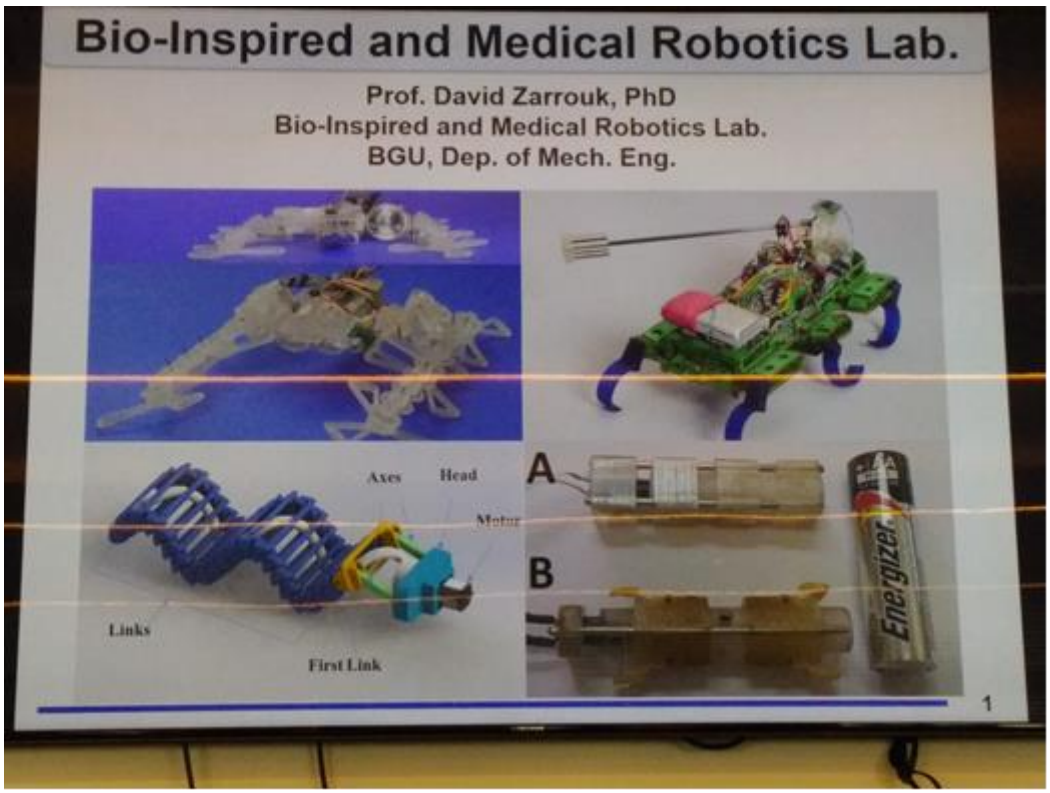

圖 2　機器蟲

肆、 心得與建議

一、心得：

以色列國土面積大約 22,072 平方公里，約為中華民國（臺灣）的 3/5，人口總數大約 852 萬，其中猶太人占 74.9%，約 638 萬人，約為中華民國（臺灣）總人口數的 3/11，其所處之西亞/中東地區，國際政治環境嚴峻。飛機航線必須繞道中國大陸、哈薩克、土耳其、塞浦路斯，才飛抵以色列。

但是猶太人卻發揮了強大的韌性、毅力、智慧，在農業科技、國防（國土安全、資通安全）科技、金融科技、觀光旅遊、能源開發的領域上，都發展出傲人的成績。

此次出國行程中，展場的主題包括國土安全、資通安全、金融科技，大部分的攤位是以色列國內的廠商。而在與訪問的公司及展場攤位交流時，發現猶太人對於解決問題，能夠大膽地假設，在完美與效能間取得平衡的前提下，將分析的結果落實為軟體的設計上（例如：針對網際網路攻擊行為的分析，為兼顧執行效能及流量監控，因此針對網際網路封包每秒鐘截取 5%的數量即可，而不是將全部封包都過濾；或者針對惡意程式抽取關鍵行為，建立所謂的 DNA 資料庫，進行比對、更新及調整，以簡化並加速程式的執行。）

二、建議：

臺灣所處之國際政治環境亦相當嚴峻，應當效法以色列猶太人的智慧與毅力，學習其優點，提升國民的資訊與資安教育，推動基礎科技的發展。本會也應持續參與以色列每兩年舉辦一次的國土安全暨資安大會，透過觀摩學習，讓資訊與資安人員互相交流。

以色列雖然是小國寡民，但是官方、民間與美國交流密切，義務教育從小學低年級起就有英語科目，而且電視、廣播充斥英語節目，因此，以色列人大多英語流利。我國也應朝此方向努力。

伍、 出國行程照片

圖 3　拜會以色列電力公司代表團合照

圖 4　拜會 Verint 公司代表團合照

圖 5　訪問展區攤位

圖 6　拜會 Radware 本會及 TTC 代表合照

圖 7　拜會 Leumi 銀行
（精神標語：勇敢領導、謙虛學習）

圖 8　拜會 Gav-Yam Negev 高科技園區

陸、 附錄

在一本名為「猶太教育」的書中，提到猶太人是重視思辨教育及經商賺錢的民族。因為教育的目的在於傳承文化，而賺錢的目的則是在逃難時能有效地疏通關卡。因此，猶太人在歷經顛沛流離的兩千年歷史中，以頑強的意志生存下來，造就了猶太人勇於思考、創新、解決問題的能力與個性。

全世界猶太民族約只有 1500 萬人，但是獲得諾貝爾獎的人數比例約占全部得獎者的 23%，是全世界最高的比例。而在個別獎項中，經濟和科學更是猶太人強項。猶太裔（包括 1/2 及 3/4 血統者）獲獎者人數，在經濟獎占有約 39%，醫學獎占有約 27%、物理獎占有約 26%、化學獎占有約 22%、文學獎占有約 12%、和平獎占有約 9%。