2019年以色列資訊及資安產業參訪紀要

蘇柏鳴 / 金融聯合徵信中心 資安部

聯徵中心是國內唯一的跨金融機構間信用報告機構，同時蒐集個人與企業信用報告，並發展個人與企業信用評分、建置全國信用資料庫，不僅提供信用資料給金融會員機構，也肩負提供主管機關金融監理或政府金融政策擬訂所需資訊之角色，近年來Fintech 崛起，各金融機構爲因應Fintech帶來的挑戰，積極發展各式新型態的金融服務，聯徵中心身爲金融體系中重要的一環，也必須跟上這波時代潮流。

隨著資訊服務樣式多樣化，衍生出來的資訊安全是必須嚴肅面對課題，近年來銀行業資安重大事件爲「2016年第一銀ATM遭駭事件」及「2017年遠東銀行SWIFT遭駭事件」最爲嚴重，除此之外，政府機關個資外洩事件頻傳，光2019年就有「臺北市政府衛生局個資外洩」及「銓敘部59萬筆文官個資外洩」，代表資訊系統安全防護建置已是刻不容緩，爲強化本中心資安防護能力，聯徵中心安排此次參訪以色列資訊及資安相關廠商行程，近年來以色列資安及資訊新創產業發產蓬勃，美國市場研調機構CB Insights公佈了「2018全球科技中心報告」，以色列特拉維夫（Tel Aviv）被列爲全球25大科技中心之一，並與波士頓、倫敦、洛杉磯、紐約及矽谷一同列爲重量級中心，而此次由聯徵中心副總經理帶隊，與資訊、資安部門的三位組長拜訪主要廠商爲CyberGym、Cybereason、IntSights、Votiro、Facetrom及Cyberbit，希望透過瞭解目前以色列資訊安產業發產的狀況，可以作爲未來聯徵中心資訊安全藍圖建構的靈感。

一、參訪目的

本次參訪團係由聯徵中心與駐台北以色列經濟文化辦事處合作，規劃「2019年以色列資訊及資安產業參訪團」，赴以色列實地參訪多家國際知名金融科技與資安廠商，並拜訪「以色列出口與國際合作協會（IEICI）」及「網路星光園區（CyberSpark）」，藉此全面瞭解以色列在資訊及資安領域的最新發展及新創公司的特色。

本次參訪主要機構包含：CyberGym、Intsights、Cybereason、Votiro、Facetrom、Cyberbit 、CyberSpark、以色列出口與國際合作協會（IEICI）、 JVP venture等數個以色列著名科技公司與創新公司。

透過本次實地參訪，有助於本中心此次參訪團成員深入瞭解以色列在資訊、資安相關產業的最新發展及產品概況，尤其是在資訊安全實地攻防訓練體系、檔案無害化與重組技術（CDR）、暗網主動監控、資安流程自動化回應（SOAR）…等領域，更有本中心值得借鑑的價值。

二、參訪過程

(一) 以色列國家介紹

以色列自1948年建國至今，人口增長近10倍， 人口2018年統計為844萬，組成為猶太人、阿拉伯人及其他族群，其中猶太人口佔全國人數的3/4，根據國際貨幣基金組織（IMF，International Monetary Fund ）2018資料統計，以色列人均GDP為41,267美元[1]，為台灣的1.56倍。如今的以色列是新創企業培育的搖籃，世界上最早出現的即時通訊軟體ICQ，就是1996年誕生於以色列的Mirabilis公司所做，那個時候還沒有LINE跟MSN，在這個人口才不到千萬、國土面積剛過2萬平方公里的國家，目前已育成了超過6千家新創企業，這些數量眾多、技術領先的新創企業，自然也吸引了創投機構和跨國公司的注意力。

表一 以色列國家概況

首都	耶路撒冷
面積	21,946平方公里，南北長約450公里，東西寬由53~135公里。
地理位置	位於阿拉伯半島西北角，北接黎巴嫩，東北處接敘利亞，東鄰約旦，南及西南連接西奈半島，西面地中海。
人口	884.4萬(2018年) (猶太人74.7%，阿拉伯人20.5%，其他族群4.2%)
宗教	猶太教、伊斯蘭教、基督教
語言	希伯來語、阿拉伯語
幣別	New Israeli Sheker (新謝克爾)。1 USD = 3.5 ILS
簽證與入境	凡持有效期6個月以上之中華民國護照的國人，得免簽證入境以色列，惟180天內停留時間不得超過90天。

1 2018年各國人均GDP資料。
https://zh.wikipedia.org/wiki/%E5%9C%8B%E9%9A%9B%E8%B2%A8%E5%B9%A3%E5%9F%BA%E9%87%91%E7%B5%84%E7%B9%94

（二）參訪行程

1. 參訪機構總覽

	參訪單位	位置	產品名稱/服務	產品類型	備註
1	CyberGym	哈代拉(Hadera)	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。		
2	Cybereason	特拉維夫(Tel Aviv)	EDR,MDR,NEXT-GENERATION ANTIVIRUS (NGAV)	EDR、MDR	入選CB Insights AI 100 2018名單。
3	以色列出口與國際合作協會(IEICI)	特拉維夫(Tel Aviv)	功能與臺灣的外貿協會相仿，由以色列政府和私有部門提供支持，做為以色列企業對國際市場聯繫平台，旨在促進海外企業和以色列公司建立業務關係、組建合資企業以及結成戰略聯盟，並透過會展、考察團等各式活動，協助以國國內企業將產品與服務帶向國際市場。		
4	Votiro	特拉維夫(Tel Aviv)	Votiro Disarmer	CDR	
5	Facetrom	特拉維夫(Tel Aviv)	AI人臉辨識。		
6	Cyberbit	賴阿南納	(1) CyberShield SOC 3D (2) Cyberbit EDR (3) Cyberbit Range	SIEM、EDR、資安攻防	
7	CyberSpark (網路星火產業園)	貝爾謝巴	以色列CyberSpark為最具代表性的科技聚落，結合本古里安大學及其創新研究室德國電信創新實驗室、國家緊急防禦團隊、資訊安全專門創投耶路撒冷創投，以及超過40間資訊安全企業。		
8	JVP venture	貝爾謝巴			
9	Intsights	特拉維夫(Tel Aviv)	致力於為用戶提供一個智慧解決方案，覆蓋多源網路情報，自動即時檢測開放網路、深網和暗網網路威脅，提供網路駭客和欺詐攻擊的預警		

2. CyberGym

(1)日期與時間：2019年5月26日，09:30~12:00。

(2)機構簡介：以色列電力公司（IEC）[2]是以色列最大的電力供應公司，也是以色列唯一的綜合電力公司，因為以色列國情的緣故，以色列電力公司（IEC）每天會遭到數以千計的網路攻擊，因此IEC也培養出了一批實戰豐富的網路攻擊防禦專家，在2013年IEC將這個團隊獨立成為子公司CyberGym 。CyberGym透過客製化建立與企業相仿之資

2 以色列電力公司（IEC）: https://www.iec.co.il/en/ir/pages/default.aspx

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)參訪內容：CyberGym為本次參訪行程的第一間廠商，因銀行公會參訪團本日未安排行程，所以由郭董事長帶隊參訪，CyberGym的總部地處哈代拉（Hadera）郊外，設施分布在園區內改裝後的小屋平房中，該園區為以色列電力公司所屬的場地，因以色列電力公司（IEC）為重要的基礎設施，所以走在園區時，時不時可以看到手持長槍的警衛人員在園區巡視。

我們聽取Oren Tepper對於該公司及他們資安攻防教育訓練的介紹，這家公司除了對各國賣出他們的網路安全實戰訓練平台，在以色列當地也幫軍方、警察、國安人員及其他關鍵基礎設施業者，培訓專業的資安人員。我們實地參觀他們培訓資安人員的教室與設備，包括了紅隊（Red team，在資安攻防中代表了攻擊方）、藍隊（Blue team，在資安攻防中代表了防守方）及白隊（White team，在他們的定義中為鑑識，裁判方）。因為他們是從電力公司獨立出來的，所以可以看的出來他們強調擬真的設施與設備，尤其在OT與IoT的教室中，就是真的配電盤與鍋爐在運作。

除正式介紹外，交流過程中Oren Tepper提到兩件有趣的訊息，第一訊息是攻擊以色列最多的來源國家並非我們想像的周邊阿拉伯世界國家，而是遠在有亞洲的另一區的北韓，他也說明實際上是中國透過北韓來攻擊以色列，因為以色列跟美國的科技及軍事的密切關係。另一則是2010年伊朗核電廠受到Stuxnet蠕蟲感染[3]，就是以色列利用USB方式讓核電廠感染病毒。

3. IntSights

(1)日期與時間：2019年5月26日，14:00~16:00。

(2)機構簡介：IntSights 創立於 2015年，總部位於特拉維夫，創始人團隊來自於以色列國防部情報和網絡安全部門，致力於為用戶提供一個智能解決方案，覆蓋多源網絡情報，自動實時檢測開放網絡、深網和暗網網絡威脅，提供網絡黑客和欺詐攻擊的預警。公司暗網數據的可視性，能夠在網絡攻擊發生之前就監控到這些潛在的威脅。威脅情報來源：Clear Web、Deep Web、Dark Web、Threat Intelligence Feeds、SIEM。

(3)參訪內容：參訪IntSights公司是由他們的CPO&Co-founder 的Alon Arvatz接待，IntSights提出的概念就是若要更早掌握相關情資，得知企業可能成為駭客攻擊的目標，可能就必須要往源頭追溯，而在現行的網路世界中，可能會蘊藏這些攻擊資訊的

3 伊朗核電廠受到Stuxnet蠕蟲感染新聞: https://www.ithome.com.tw/node/63565

地方，並不只是檯面上公開的明網（Clear Web）或是表網（Surface Web），還有地下的網路環境，也就是所謂的深網（Deep Web），以及位於其中的暗網（Dark Web），因此，有許多資安分析人員也會設法潛伏到這些無法直接存取的網路裡面，伺機觀察黑客彼此之間的互動溝通過程，打探各種非法的買兇攻擊與個資交易行為。

只要有公司提供基本相關資訊，例如公司名稱、公司Logo、高階經理人姓名或郵件，公司網站…..等，他們就可以提供監控暗網服務，並且如有非法的個資交易他們會通知客戶，此外還會提供監控官網Phishing攻擊，是一種新型態資安防護的概念，但暗網監控人員私下是否也是駭客，這些風險無法掌握，所以對於提供外部廠商聯徵中心資訊還是有一定風險存在。

4. Cybereason

(1)日期與時間：2019年5月27日，14:00~16:00。

(2)機構簡介及參訪內容： Cybereason的總部設在Boston，於2012年由以色列國防部8200部隊成員在以色列創立，在特拉維夫仍保留一家研發中心，並於2018年入選CB Insights AI 100 2018名單。它的軟體可收集電腦網路內任何活動方面的資料，如運行當中的程式、被使用者訪問的檔以及員工及任何獲授權使用網路中的電腦人的鍵盤輸入和滑鼠移動情況，相關產品只會記錄「與實際威脅的存在性」相關的資料，不會記錄任何機密或者私密資料，在發現幾個關聯的異常情況時才會發出警告，目的時為了避免發出錯誤警告，Cybereason的端點防護也有導入Machine Learning的分析，看來導入Machine Learning的分析已在EDR防護上已是顯學。

5. Votiro

(1)日期與時間：2019年5月28日，14:00~16:00。

(2)機構簡介：Votiro由以色列國防軍精英技術情報部門的退伍軍人於2010年創立，是一家屢獲殊榮的網路安全公司，專門致力於消除零時差與未知的目標攻擊。Votiro新世代受專利保護的 CDR技術讓使用者能安全無虞地開啓電子郵件附件、下載和傳輸檔案、共用內容與使用可卸載式裝置，同時保持效能與功能的完整性。Votiro在全球擁有超過500名客戶，在以色列、美國、澳洲和新加坡都設有辦事處。

(3)參訪內容：此次參訪是由Votire公司的CEO Aviv Grafi接待並解說，Votiro主要的產品是Votiro Disarmer，主打CDR功能，這裡所謂的CDR技術，全名為內容威脅解除與重組（Content Disarm and Reconstruction），簡單說就是檔案威脅清除，舉例來說，有些PDF檔本身會包含JavaScript，有些Office文件會包含巨集、Flash或OLE物件（檔案內嵌檔案），都是CDR技術可清除的對象。CDR這項技術其實並不是要偵測出惡

意內容，而是直接將這些可執行、有疑慮的元件失去作用，也就是不論惡意或非惡意的程式碼，通通要清除，以做到更徹底的保護。

6. Facetrom

(1)日期與時間：2019年5月28日，18:00~20:00。

(2)機構簡介：Facetrom是一間非常年輕的新創公司，該公司技術團隊致力於解碼人類面部表情中的隱藏資訊，可通過分析人類面部照片微表情建立人物「側寫」，這一新技術可用於提高企業銷售業績、客戶關係以及投資回報率，甚至可以用來預防犯罪。

(3)參訪內容： 這公司是此行參訪我認為最有趣的一間公司，從我與他們CEO Ido Peleg聯繫約拜訪時間，因為他本人去紐約出差不在以色列國內，而他回國時我們參訪團也已經回國，本來要放棄拜訪該公司，但因Ido Peleg提出希望用視訊方式介紹他們產品，所以我們配合拜訪時間延至18:00，可以感受到新創公司的積極性。

技術方也是覺得很神奇，他們公司產品主要是透過人臉的特徵值找出隱藏資訊，Predicts Users’ Risk Scoring Based on a Facial Phote，他在現場舉例說，他們的模型可以經由收集犯罪者的照片訓練後，用此模型可以判斷照片的人是否為犯罪者，號精確度有90.7%。他們Training Data主要是由3萬多位犯罪者的照片練出來的，當下我想到的應用為，收集信用違約的人的照片，使用該公司的模型來判斷照片內的人是否有違約風險，但因Feature 是無法解釋，且會有人權方面的問題，該AI不適合聯徵中心發展方向，但經由此次參訪也瞭解臉部應用的多樣性。

7. Cyberbit

(1)日期與時間：2019年5月29日，10:00~16:00。

(2)機構簡介：Cyberbit 是一家資安解決方案公司，該公司創立於2015年，由以色列埃爾比系統公司（Eibit Systems Ltd. 那斯達克證交所：ESLT）所成立，其創辦人亦為以色列國防軍8200部隊退役之將領，Cyberbit 於2017年已進入世界500大資安公司，其主要的資安解決方案有四項，包含有：Endpoint Detection and Response、SOC Automation and Orchestration、ISC/SCADA Security and Continuity、Cyber Range Training and Simulation。

(3)參訪內容：Cyberbit是本次以色列參訪的重點公司，所以我們安排了一整天的時間參訪該公司，而對方也派出亞太地區銷售經理Kobi Lezerovich全程解說Cyberbit公司的產品，也是這次行程中在技術細節上對我們最友善的公司，在這家公司我們大部分的時間主要關注該公司的兩項產品，一個是SOC 3D（資安流程自動化回應的工具），另一個則是Cyberbit Range（資訊安全實地攻防訓練的服務）。

① SOC 3D：這套產品主要是應用在資安事件的處理上面，比起傳統的SIEM跟SOC，他導入了自動化流程的workflow，產品聚焦在於：事件處理工作流程化、反應自動化、後續資安事件的調查。

運作方式主要是在各式各樣的「告警訊息」（例如：SIEM、Email、CRM、UEBA、EDR）和「回應處理工具」（Response Tools ，例如：IPS、FireWall、WAF、AD）之間透過SOC 3D來達到處理流程自動化。能夠就告警訊息，經過判斷之後，自動透過資安工具來處理各種資安事件的回應；除次之外，SOC 3D也提供數位儀表板就發生的事件、處理的狀況供調查使用。

這套產品最讓大的優勢，是他們把一般用在表單流程自動化的設計工具，用於資安事件的回應上面，而為了讓各式各樣的資安工具軟體也能協同作業，他們跟全球大部分的資安產商合作，透過API協作達到“自動處理資安事件”這個目標，而這個只有四個人的開發團隊，也因為自身定位很清楚，在資安這個領域透過與其他廠商的合作，達到了比單一產品運作更大的目標。

② Cyberbit Range：這是一套資安實地攻防訓練平台，一開始他們就對這個產品做出很明確的地位，他們訓練出來的人員能力是藍隊（攻防演練中的防禦方）的資安專業人員。他們提供環境讓受訓人員實地體驗，當發生特定的資安攻擊事件發生的時候，資安或系統人員應該要有那些反應動作，整個訓練過程中要求講師評估學員是否達到每個情境中的檢核點，Kobi也提到：在下一個版本中他們能夠由系統自動評估學員是否達到每個情境中的檢核點。在簡介中他們介紹，這套產品可以提供：

●額外的的訓練計劃與使用上的實例。（內建Machine Learning演算法）

●事件回應團隊的訓練

●滲透測試訓練

●資安攻防奪旗比賽

●OT關鍵基礎設施的訓練

●攻擊腳本和技術評估

●新進人員專業能力評估

Cyberbit Range這套產品，主要作為教育訓練是主要的用途。但在他們的客戶中也有人用這套產品來檢定資安人員的能力或資格， 因為這套產品提供客戶客製化設定環境功能，所以在美國有一家大銀行則是在他們的重大系統上線之前，將新的系統在此平台環境下做檢測，測試是否有資安漏洞，在台灣其實很缺乏類似的教育訓練課程和可做資安攻防的實作平台。（資策會在2018引進Cyberbit Range，並成立Range Seed智慧技術人才培育中心[4]，推出相關教育訓練課程）

4 Range Seed智慧技術人才培育中心: https://rangeseed.com/5

8. CyberSpark（網路星火 業園） & JVP venture

(1)日期與時間：2019年5月30日，09:00~15:00。

(2)機構簡介：以色列CyberSpark為最具代表性的科技聚落，結合本古里安大學及其創新研究室德國電信創新實驗室、國家緊急防禦團隊（Computer Emergency Response Team ,CERT）、資訊安全專門創投耶路撒冷創投，以及超過40間資訊安全企業。

我們還參訪的JVP venture，Jerusalem Venture Partners是一家成立於1993年的國際風險投資公司。該基金專注於創業公司的投資，專注於數字媒體，企業軟件，半導體，存儲和網絡安全，已經在9個基金中籌集了近10億美元。 JVP總部位於耶路撒冷的JVP媒體區，在Be'er Sheva，紐約市和巴黎設有辦事處，這次參訪他幫我們引薦itouch.io跟Valid Network公司。

三、心得及建議

以色列採取徵兵制，無論男女年滿十八歲均須入營從軍，女性服役兩年、男性三年，在軍中依性向能力給予系統性之訓練，退役再依個人志趣進入大學就讀，故相關產業具有豐沛高素質人力資源持續投入。以我們這次參訪的CyberBit為例，接待我們的Kobi本身就是一個少校，每年都還要回到軍中服役一段期間。其中的8200部隊更是因為只挑選前5%的人選，而被以色列人戲稱是軍方資訊界的PhD。產業和國家制度的結合，造成了源源不絕的人才投入產業界，不論是新創公司或者是將成熟的產品獨立成子公司，以色列在資安產業的積極態度，讓我們留下非常深刻的印象。

在我們這次參訪的過程中碰到的以色列人都非常務實，其中有一家新創公司一到會場就先問我們，我們公司的資料傳輸是不是用中文，一得知我們平常處理的資料都是中文，就直接表明他們公司的產品對我們而言不適用，他就不做正式的投影片簡報了，但是，後來還是興致勃勃的跟我們談論，他們家這個產品的思路及用途，過程中得知原來這家公司的產品是專門在公司內部處理個資外洩，利用網路監聽和Machine Learning的技術，從網路封包來判斷是不是有個資外洩，也可判斷外洩的流向及擴散的範圍，很有趣的想法但是他們的產品只支援英文。

以色列的新創公司都是拿出想法，經過扶植做成產品之後，就直接上市場拚搏，一方面賣出產品，另一方面也爭取創投的挹注。重實際的態度也讓他們產品的定位很明確，一個產品就是解決一個問題，這種模式造就以色列每年大量的新創公司的成立，他們不怕失敗，畢竟新創就是用新的思維解決新的問題，目前Fintech的興起造就銀行業大量的資訊需求，聯徵中心在這波浪潮中勢必會被強迫升級，雖然在這波浪潮中大家還是會顧忌新的創新模式是否會帶來風險，但潮流是不會停止的，聯徵中心應培養人才，並提升整體資訊技術能力，做好面對挑戰的萬全準備，才能在這波挑戰中生存。