出國報告（計畫類別：訓練）

112 年度新購行動通訊偵查系統升級案原廠教育訓練

服務機關：　臺北市政府警察局刑事警察大隊科技犯罪偵查隊

姓名職稱：　隊長鄭國隆、副隊長謝其瑾、偵查佐許豪全、偵查佐吳仁庭、偵查佐曾竣傑

派赴國家：　以色列

出國期間：　112 年 5 月 1 日至 112 年 5 月 5 日

報告日期：　112 年 7 月 20 日

摘要

依據升級案契約，廠商應提供本隊同仁 3 名前往系統原廠供應商進行教育訓練及技術交流，最終廠商願意提供 5 位名額參加，相關期程為 112 年 5 月 1 日至 5 月 5 日。

本次預計前往位以色列臺拉維夫的 Cognyte Technologies Israel Ltd (係由 Verint Systems Ltd 集團獨立出來，成為一家獨立的安全分析軟體公司，惟原有負責行動通訊偵查系統之部門均不變，僅作公司名稱更名)，主要業務為提供各種網路情報資訊調查與分析平台(系統)的客戶解決方案。

教育訓練過程包含：(一)了解本案系統設備之功能及相關應用技術。(二)分享提供目前有利於提升國安、資安與通訊監察技術等科技發展之新型設備技術。(三)了解網際網路犯罪手法趨勢與分析、網路輿情分析、資訊安全系統相關技術。

預期效益為：(一)增進相關 M 化專責人員操作知識及技巧。(二)了解國際間關於國安、資安與通訊監察技術發展現況及未來趨勢。(三)探索是否有相關系統及技術有助於提升本隊突破 APP 通訊加密軟體及整合蒐報特定對象網路公開來源情資。

圖片說明：案內人員於 Cognyte 公司前合影

本文目次

本文

一、計畫緣起

依據採購案合約，廠商提供系統製造商以色列原廠教育訓練與技術交流，針對新購行動通訊偵查系統之原理、功能及相關應用層面，提出相關疑問與原廠技術人員探討，並分享該公司目前有利於提升國安、資安與通訊監察技術等科技發展之新型設備技術。

二、目標

增進相關 M 化專責人員操作知識及技巧。

了解國際間關於國安、資安與通訊監察技術發展現況及未來趨勢。

探索是否有相關系統及技術有助於提升本隊突破 APP 通訊加密軟體及整合蒐報特定對象網路公開來源情資。

三、過程

（一）參訪行程

本次教育訓練與技術交流計畫時間自 112 年 5 月 1 日至 5 月 5 日(因應往返以色列交通時間，案內人員提早於 112 年 4 月 29 日晚間出發，實際交流時間為 5 月 1 日至 5 月 4 日共 4 天，相關行程於 5 月 4 日下午結束即返程，並在 5 月 5 日回國)。

圖片說明：致贈 Cognyte 公司營運長 Sharon Chouli 與亞太區技術長 Gilad Ben-Aried 紀念品

(二) 第 1 天(112 年 5 月 1 日)

【Gi2 系統原理介紹與說明、Gi2 應用理論說明及實務經驗分享】

Gi2 系統為 Cognyte 公司針對基地台蜂巢式網路與目標對象使用之手機間往來訊號做攔截與控制之產品，運用其獨家技術破解基地台與手機於空中傳遞之訊號，大量攔截該系統位處地點周邊手機訊號進而判斷縮小目標對象範圍，並對其發射訊號鎖定並追蹤。

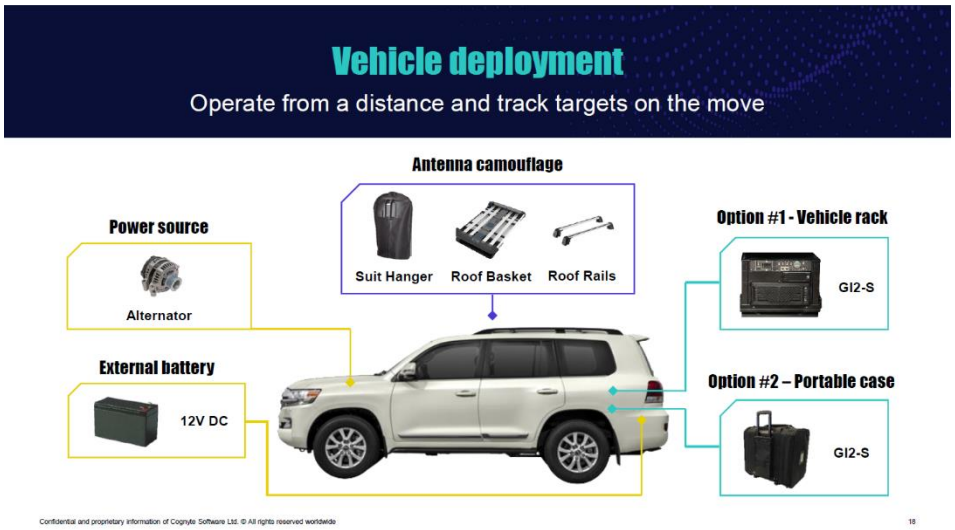
圖片說明：介紹各式應用 Gi2 系統類型

戰術指揮中心 TCC(Tactical Command Center)透過整合各式行動通訊系統如行動電話、衛星、WiFi 等相關主被動設備，蒐集與分析所取得之行動裝置訊息，掌握目標作息及藏匿處所，以及潛在共犯，甚至在機場及邊界偵測來自於他國之信號，達到提供預警情資的作用。

圖片說明：介紹各式戰術型行動通訊系統類型

Cognyte 公司之 Gi2 系統產品相當多元，本案採購標的為 Gi2-S 及 HIVE BACKPACK 兩種。

其中 Gi2-S 為車載式 Gi2 系統，相關設備所需電力均要透過更改電路，經由車輛本身發電機供電，因此對於車輛怠速發電量十分要求，並加裝並聯數具額外 12V 電瓶以應對車輛無法對設備供電之情況，來增加其使用時間；因其電力來源為車輛發電機，故在設備使用時間上除發電機故障外，未有限制，惟偵蒐範圍囿於地形限制，對於車輛無法進入之狹小巷弄或幅員遼闊之賣場等相類處所，屬其偵蒐之盲點。



圖片說明：車載式 Gi2 系統相關組成元件

Cognyte 公司架設於其辦公大樓樓頂之 Si2 衛星偵蒐系統，亦為 Gi2 系統相關產品，有別於均屬主動出擊偵蒐目標對象手機訊號之車載式 Gi2-S、背負式 HIVE BACKPACK 背包系統，其屬於架設於固定地點之設備，主要針對建築物及重點區域周邊往來人員手機訊號加以蒐集並加以分析。

圖片說明：位處於該公司樓頂之被動式 Si2 衛星偵蒐系統相關元件及發射與接收天線

(三) 第 2 天(112 年 5 月 2 日)

【Gi2 在 GSM/UMTS/LTE/5G NSA/5G SA 的原理、應用說明】

Wi-Fi 及 Bluetooth 套件（Nano Sniper），可偽裝為可供手機或裝置連線網路之設備，並能實際提供網路，惟其擔任連接網路之中繼將可取得手機相關軟硬體資訊，並針對手機本身做操縱。

圖片說明：介紹 Wi-Fi 及 Bluetooth（Nano Sniper）套件

Mucom 為 Gi2 系統的歸向設備，顧名思義即為歸納目標手機訊號方向之設備，可搭配增益型天線加強對於目標手機訊號來源之指向性與讀數，依操作人員經驗判別目標手機訊號所處位置。

圖片說明：介紹 Mucom，為 Gi2 系統的歸向設備，透過聲音及圖像解讀訊號來源強弱及方向

(四) 第 3 天(112 年 5 月 3 日)

【HIVE 在 GSM/UMTS/LTE/5G NSA/5G SA 的原理、應用說明與操作技巧】

劃時代的創新：背負式 Gi2 系統的誕生，解決因巷弄狹小或地物遮蔽訊號，針對車輛無法到達之處所或過往無法偵測之高樓層，執行搜尋。

HIVE BACKPACK 為背負式 Gi2 系統，也是本案除了車載式 Gi2 系統外，另 1 個採購標的，其設備大小為普通尺寸背包，重量約 10 公斤，電力來源則為本身所攜帶之電池，受限於背包大小、重量及人員體能狀況，因此設備續航力僅 1 至 2 小時，所能同步發射頻段數量亦較車載式少，但能針對車輛無法所及之處，以人力步行方式進行重點地毯式偵蒐，相對地也能解決車載式系統鞭長莫及之窘境。

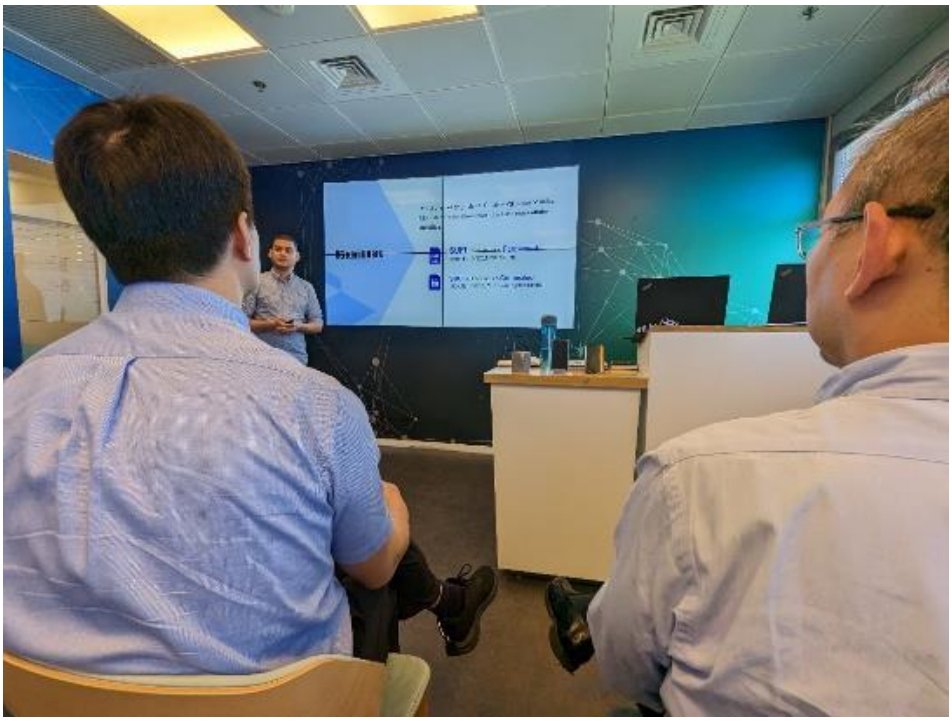
此外 HIVE 還有可以裝載於外送箱大小之 MOTORCYCLE BOX，搭配各國盛行之外送業者偽裝，因可搭載雙倍於背負式背包的雙倍電池量，兼有汽車之高機動性及行人可徒步穿梭狹小巷弄之靈活性。

圖片說明：介紹各式應用 Gi2 & HIVE 系統類型

5G(第五代行動通訊技術)為 4G 系統之後的演進，由於行動通訊網路安全以身分認證與金鑰管理做基礎，在用戶端與網路之間進行雙向身分認證，產生加密金鑰保護相關用戶資料，而 5G 相對於 4G 其中的變革，基於現代社會對於資訊安全的重視下，即為認證安全機制的重大改進。

就前面所提到的，Gi2 系統係針對基地台蜂巢式網路與目標對象使用之手機間往來訊號做攔截與控制之產品，那麼攔截到空中加密的通訊訊號後，如何得出可個化目標對象持有手機門號之資訊，則牽涉到破密的層面。

有別於 4G 中用戶設備 UE(User Equipment)在身分認證過程中，會被要求以明碼形式發送國際移動使用者辨識碼 IMSI(International Mobile Subscriber Identity)來識別，過程中極有可能產生被竊聽攔截風險，而 5G 在認證安全機制中，則以可識別用戶身分的訂閱永久標識符 SUPI(Subscription Permanent Identifier)加密保護產生之訂閱隱藏標識符 SUCI(Subscription Concealed Identifier)進行認證，大大改善了前述 4G 安全認證機制的風險。



圖片說明：5G 加密技術原理及相關認證機制(SUPI、SUCI)介紹

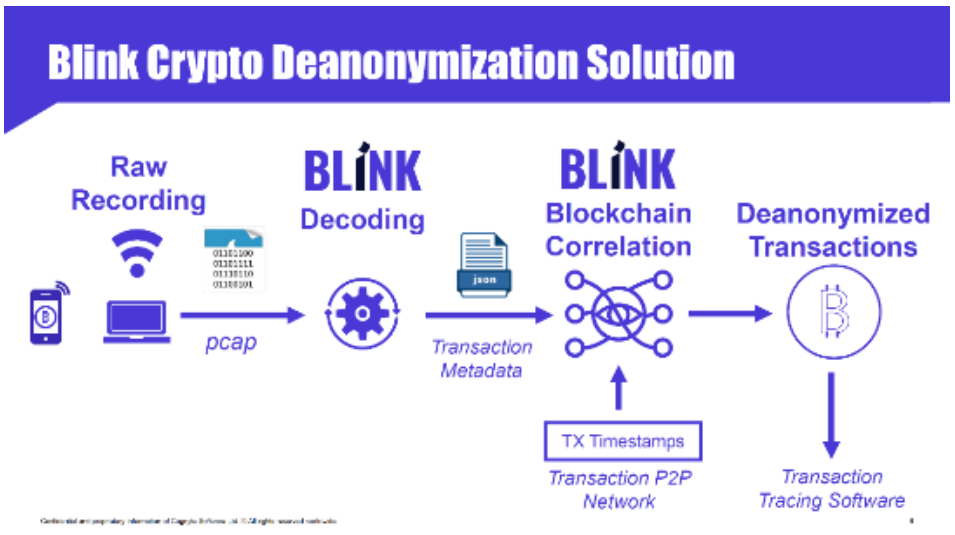
(五) 第 4 天(112 年 5 月 4 日)

【針對加密貨幣與區塊鏈的突破方案、說明與展示】

相對於警方查緝方式的進化，嫌犯對於如何規避警方在各個偵查階段試著調查出得以個化嫌犯真實身分之證據，往往都是兩者針鋒相對的一場角力。跟著金流走，一直以來都是警方追蹤嫌犯的重點，犯罪所得最後總會回到犯嫌手上，而使用區塊鏈技術的加密貨幣來交易，則大大提高了查緝的難度。

圖片說明：闡述針對加密貨幣的金流查緝方式，突破傳統偵查方式無法突破的困境

介紹並演示 BLINK 相關系統，針對所擷取的封包資訊解碼並分析，找出其關聯性，達成去匿名化進而達成追蹤流向的目的。



圖片說明：針對加密訊息如何去匿名化的流程

四、心得及建議

(一) 隊長鄭國隆

心得：

1.本次與同事們遠赴以色列 Cognyte 公司原廠參訪及受訓行程，可謂是本局科偵工作之一大突破，為刑事局以外第一個警察機關派員出訪以色列，本人及團員們均甚感興奮，短短五天參訪行程在原廠精心安排及授課者清晰解說下，我們不僅對採購標的之 5G 系統 M 化設備其架構、原理及未來發展有更進一步認知外，也對該公司其他如 Hornet、Nano-Sniper、PI2、SI2 等主、被動偵蒐設備、加密貨幣區塊鏈去匿名化工具 BLINK、網路公開資訊分析 CLARIAN、假訊息溯源系統 Orbis 及對目標手機位置進行即時定位之 FirstMile 等產品，有更完整之了解，也真正了解一個長年在戰火威脅、多元宗教、民族及地緣政治等複雜環境的狹小國家，如何不斷運用科技創新與發展，並融入實際的運用，幫助以國在世界科技、經濟及軍事地位中站穩一席之地。

2.此外，本次參訪也啟發了個人應設法與國際科技偵查領域之夥伴多交流以汲取新知，並強化語文溝通能力，始能持續進步，為本局「智安警政」發展貢獻更多心力。

建議事項：

1、建議出訪原廠每年安排參加該公司全球客戶大會，據統計該年度大會皆有超過七十個國家熱烈參與討論與實務交流，在我國外交困境下藉此拓展與他國治安領域進行科偵技術交流，不失為一個突破外交困境之絕佳機會。

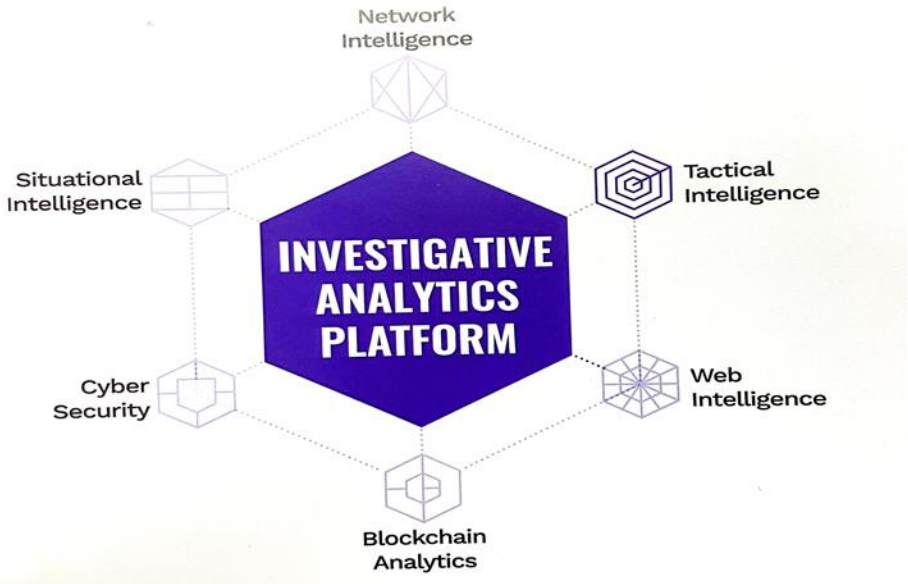
2、建議跨國參訪之部分課程，在無資安及機密疑慮下，可利用線上課程增加國內人員參與之機會。

3、建議本局可針對跨國犯罪偵查或科技偵查訓練，編列出國差旅費，以增進本局科偵人員技術能力及新知。

(二) 副隊長謝其瑾

心得：

本次 M 化設備系統升級前往以色列 Cognyte 公司原廠進行參訪，雖然短短數日，但在我心中對以色列這個國家人民及愛國心震撼我的思維，該公司不只針對我們採購的 5G GI2 設備做詳細的講解，並實際展示該公司對目前全世界高科技偵查全方位完整的提供他們解決方案，這些產品讓我比較興趣的是有關 Investigative Analytics Platform 調查分析平台，以 Network Intelligence（網路情蒐）、Tactical Intelligence（戰術情資）、Situational Intelligence（動態情報）、Block chain Analytics（區塊鏈分析）、Web Intelligence (智能網路)，該平臺打造各種科技偵查面向之工具，是目前全球科技戰略安全分析軟件的領導者，讓人對該公司打從心底不得不敬佩，該平臺使用開放軟件大量監控線上即時網絡資訊在規模上融合、分析大量異質數據集及多語系即時組合解譯和強大的整體空間視覺化、地理空間、時間軸方式呈現，並結合暗網大量資料蒐集，精準打擊全球恐佈活動和分析潛在犯罪資訊，這是最讓我佩服的，藉由 Cognyte 公司專業工程師深入淺出的講解，啟發我們爾後系統開發，分析思維能更全面更精準。



圖片說明：該公司調查分析平台各種面向之工具

建議事項：

建議針對本局本次採購價格昂貴之 Gi2 系統功能，能更全面性的瞭解學習，因該系統功能其實非常強大，目前僅針對手機即時定位進行運用，其中還有非常多的系統功能等待發掘運用，期盼多做交流可掌握系統最新發展狀況與掌握世界恐怖活動的趨勢。

建議全球反恐或科技偵查產品商，舉辦年會新知或新產品發表會或最新教育訓練課程，能編列出國參訪或訓練差旅費，以提升本局科偵人員技偵查素養機會。

(三) 偵查佐許豪全

心得：

本次以色列 Cognyte 原廠公司受訓及參訪，除了瞭解 5G-M 化系統體驗，更多是學習國際趨勢打擊犯罪的新知識，也改變了一些既有的觀念與想法，不但增廣了國際視野，更提升了國際觀，落實打擊犯罪國際化的培育目標。

本次採購標的 M 化系統(Gi2-S)及背負式 M 化系統(HIVE)新系統講解操作，讓我們在未來面對系統的任何問題都能迎刃而解，另外介紹說明加密貨幣區塊鏈去匿名化的 BLINK、增進網路公開資訊分析威脅效率的 CLARIAN，被動型偵蒐的 PI2、SI2 等設備等都有詳細的介紹，從這次難得的機會中，有很多方面的收穫。最後要再度感謝 Cognyte 公司原廠安排，您們的用心我們都有感受到。

建議事項：

本次參訪主要是參觀 Cognyte 公司原廠最新研發設備，其作法不外乎運用各項最新之科學技術，設備或作業方式等方法，以達到破解犯罪手法之目的,，這次講師替我們做詳細解說其中有一句話讓我印象非常深刻：「所有的進步都來自於需求」，事實也是如此，每個國家環境都不相同，建議設計課程時若能帶入我方需求作更深入的探討，更能貼近此次參訪目的。

(四) 偵查佐吳仁庭

心得：

管中窺豹，時見一斑。能夠前往本採購案位於以色列的 Cognyte 公司原廠參訪，不失為增廣見聞的機緣，一則見識了風格迥異的異國風情，二來也更深一層地對於自身工作上的相關知識有所增益。

除了另外介紹說明加密貨幣區塊鏈去匿名化的 BLINK、增進網路公開資訊分析威脅效率的 CLARIAN 等，最有興趣也是印象最深的，莫過於本案的採購標的 M 化系統(Gi2-S)，以及和其能夠互相搭配的背負式 M 化系統(HIVE)。

針對現有僅支援截取 5G NSA(類 5G 模組)系統，以及本案採購未來能夠及時支援 5G SA(5G 基地台核心)的新系統做比較，新系統將可針對其新增加密之 SUPI 與 SUCI 做截取並有效解譯取得目標門號之 IMSI，惟因 5G SA 網路的加密特性，目前技術仍受限於在 4G LTE 及其以下之 3G UMTS、2G GSM 網路做 Silent call(靜音呼叫，亦即針對目標發送並回收訊號，透過歸向設備來判讀目標訊號來源，但持機人未能察覺異狀)，該授課技師於課程中亦提到，該公司仍在對 5G 的 Silent call 做測試，未來若能於 5G 模式建立 Silent call，將可避免目標無法強制移至 4G 及其以下之網路時，無法定位之窘境。

建議事項：

本次目的地遠在中東的以色列，因路程遙遠且原廠人員於教育訓練及技術交流部分課目數量繁多，以至於在交流過程中不論是受訓人員或者授課的講師都略顯匆忙，未能追本溯源實在可惜，建議日後與原廠在討論設計課程時若能針對其中幾項作更深入的探討，讓受訓人員不只是「Know-What」，而能進一步「Know-How」、「Know-Why」，相信能讓大家在 M 化系統的操作上有更深的理解與進益。

（五）偵查佐曾竣傑

心得：

這趟到以色列 Cognyte 公司原廠受訓受益良多，除更了解本次所購買 5G 系統的 M 化設備的架構及原理以外，還發現 M 化設備只是 Cognyte 公司所研發的偵蒐系統的其中一環，有主動型偵蒐的 GI2-S、Hive、Hornet、Nano-Sniper 跟被動型偵蒐的 PI2、SI2 等設備，最後整合到 TCC 電腦設備中讓整個偵蒐的結果可以顯示出來，讓指揮官可以第一時間判斷該如何進行下一步，甚至連往往要跟電信公司三催四請才要到的即時定位資訊，該公司都能透過所研發的 FirstMile 直接告訴你目標所在的基地台位置，不愧是能在眾多國家攻打還能存活下來的實力。

建議事項：

本次雖然有額外購買該公司研發的 Hive 設備（背負式 M 化設備），以因應 M 化車物理上或先天地形上的限制，理論上確實可以提升偵測目標的成功機率，惟目前係以人工方式背著設備移動，如可以換成以機車當作 Hive 設備的載體，讓機動性可以更加提升，相信會更符合台灣多小巷子導致 M 化車無法進入的情況，讓偵測效率提升。