出國報告（出國類別：開會）

「國際資訊安全會議（DEF CON 31）」及「黑帽駭客大會（BLACK HAT USA）」

出國報告書

服務機關：數位發展部資通安全署

姓名職稱：鄭欣明副署長

許書瑜高級分析師

楊玲芬高級分析師

翁健瑋資安系統分析師

派赴國家：美國

出國期間：112 年 8 月 8 日至 15 日

報告日期：112 年 12 月 28 日

摘　要

每年的「國際資訊安全會議（DEF CON 31）」與「黑帽駭客大會（BLACK HAT）」是全球著名的駭客大會，本次參加的 DEF CON 31 與 BLACK HAT USA 會議時程相連，地點亦位於美國拉斯維加斯，主要是為了讓各界方便共襄盛舉。

在國際資訊安全會議（DEF CON 31）進行之「美國網路政策綜觀」網路政策座談由六位來自不同行業但工作與網路安全相關的專業人士(任職律師事務所負責網路安全及相關法律和政策領域的律師及網路安全與隱私服務資深總監、白宮國家網路辦公室負責戰略和研究團隊的主任、FDA 放射健康設備中心戰略合作夥伴和技術創新辦公室負責監管醫療設備網路安全的主任、全國國務卿協會負責網路安全和選舉安全的副執行主任、美國網路安全和基礎設施安全局(CISA)網路安全部門的高級顧問)分享在網路政策中的角色。技術領域的議程，包括愛達荷國家實驗室 Digital Twin 等，以及技術面及其衍生的安全性，甚至隱私問題，在各式各樣的 VILLAGE 也有一些領域各別介紹。

而在黑帽駭客大會（BLACK HAT USA）中，美國代理國家網路總監 Kemba Walden 以「美國之網路安全策略及人才培育」為題討論「國家網路安全戰略實施計劃」和「國家網路人力資源和教育戰略」相關細節。藉此機會相互學習，進一步瞭解資安相關國際標準與規範推動進程，並掌握相較的規範及因應對策。

目錄

細目

壹、 目的

近年來網路資通安全問題，已是國際關注之重要議題， BLACK HAT 及 DEF CON 即是全球最知名的駭客重要技術會議之一。 BLACK HAT USA 及 DEF CON ，每年定期於美國拉斯維加斯舉辦，除了受矚目的 DEF CON 奪旗攻防賽(Capture the Flag, 簡稱 CTF)，會議內容也包含豐富的資安技術與策略監管等資訊，還有最新資安軟硬體設備展場，亦有各式各樣不同領域與資安相關 VILLAGE，都是本次會議重要內涵。

全球許多專業領域代表、頂尖資安駭客、資安廠商、學術領域等，都會熱烈參與 BLACK HAT 及 DEF CON 此一年會，藉此掌握新興的資安趨勢。當然，在新興資安技術發展趨勢之外，這次會議更是提供一個資安結合產業領域之交流分享場域。

本次參加 BLACK HAT USA 、 DEF CON 31 會議之目的，包括 DEF CON 奪旗攻防賽，也期望可以瞭解最新資安動態、資安產業、國際資安政策等新訊，汲取一些新想法跟觀點，未來有助於機關業務推動。

貳、 會議紀要

「國際資訊安全會議（DEF CON 31）」與「黑帽駭客大會（BLACK HAT）」都源自 JEFF MOSS 創立。依創立時間序而言，1993 先成立 DEF CON 駭客大會，接著於 1997 年成立 BLACK HAT 黑帽大會。

每年的「國際資訊安全會議（DEF CON 31）」與「黑帽駭客大會（BLACK HAT）」是全球著名的駭客大會，前者比較像是駭客型的派對；後者則定位於電腦安全性質的會議，屬較正式的企業或者資安產業的盛事大會。2023 年的 DEF CON 與 BLACK HAT USA 都在美國拉斯維加斯舉辦，通常是接連著舉行，且舉辦地點毗遴。

一、 國際資訊安全會議（DEF CON 31）

(一) DEF CON 31 介紹

今年的 DEF CON 31 會議在美國內華達州拉斯維加斯 CAESARS FORUM 會議中心舉行，為期四天(8 月 10 日至 13 日)的活動提供許多資安領域政策、技術等豐富多元的議程內容，講授者多為資安領域的專家。

除了 CTF 搶旗賽之外，各式各樣的 VILLAGE 活動也是 DEF CON 亮點，VILLAGE 通常是組織或個人主辦的工作坊，提供對特定領域感興趣的參與者相互交流與探討。

(二) DEF CON 31 會議及議程

DEF CON 官方網站已備妥各式議程、徽章、音樂、照片等公開資源，提供連結下載使用。The DEF CON® Media Server - Archives of the conferences，相關連結：https://media.defcon.org/DEF%20CON%2031/。

本年度會議徽章由 Mar Williams 設計師製作，其已有多年的 DEF CON 藝術設計經驗。本次會議徽章為聚碳酸酯塑膠材質，由胖瘦菱形共同組成，意謂 human badges 與 inhuman badges（inhuman 有 11 類）。徽章背面有個線上 URL 搭配 Spux.art 前端開發的應用設計巧思，方便現場人員回饋資訊（包括顏色、形狀、留言、暱稱或暱名），隨著時間推展，登錄人數可呈現出漂亮的拚圖。相關連結：https://www.youtube.com/watch?v=Vx0TPGutROo

圖1.DEF CON 31 會場

圖2.DEF CON 31 會場

圖3.DEF CON 31 會場

圖4.截自官網之圖像設計、會場 Badge

圖5.截自影片之 Spux.art 的設計拚圖

圖6.截自影片之 3D 塑模徽章

相關連結：https://www.youtube.com/watch?v=Vx0TPGutROo

(三) 本次會議參與之重點

1. 技術分享：低功耗藍牙與電動車安全漏洞

(1)綜合充電系統

綜合充電系統（Combined Charging System，CCS）是電動車廣泛使用的直流快速充電技術之一，但容易受到無線攻擊的威脅。充電電纜可能洩漏電力線通訊（PLC）信號，駭客得以使用現成的無線電設備輸入自己的信號。DEF CON 會場展示了竊聽充電通訊的過程。這些漏洞已提出多年，但仍存在於 CCS 標準，而新的北美充電標準（NACS）也有相同的漏洞。

(2)安全問題

最著名的漏洞與低功耗藍牙（Bluetooth Low Energy，BLE）安全漏洞有關，駭客藉由連結層中繼攻擊（Link Layer Relay Attack），攻陷所有以 BLE 作為接近身分驗證（Proximity Authentication）的裝置。

Proximity Authentication 用於使用者靠近且為信任對象時進行身分驗證，通常透過可信對象與正在解鎖、登錄或啟動的設備之間的無線通訊來實現，其中電動車的無鑰匙解鎖是這項技術最常見且顯而易見的運用，類似技術也用於其他領域，包括電子鎖、建築物存取控制系統及筆記型電腦和手機。

低功耗藍牙(BLE)並未提供飛行時間測量或基於多載波相位距離的測量方式，且距離必須透過 RSSI 及 AoA 三角測量法來確定，導致 BLE 容易受到連結層中繼攻擊的影響，藍牙技術聯盟(Bluetooth SIG)指出：「『兩個設備可能被欺騙以為彼此距離很近』，且 BLE 的近距離身分驗證『不應該作為對有價值資產的唯一保護』（詳「Proximity Profile v1.0.1」第 17 頁）」，以免駭客藉由便宜的硬體設備發動攻擊，理論上，此方法可於地球任意處駭進他處之電動車。

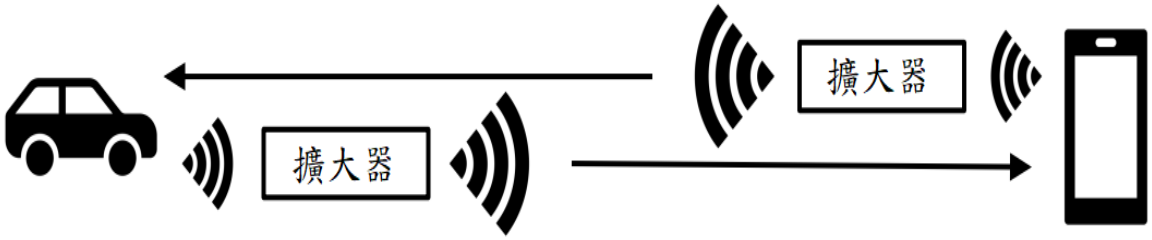

圖7.駭客攻擊手法圖示

(3)中繼攻擊

綜上，BLE 中繼攻擊可使用低成本硬體達成攻擊目標，單憑 RSSI 並不能作為近距離證明的唯一依據，且 BLE link 層加密無法防止中繼攻擊。研究人員透過實驗辨識系統可容忍來回通訊延遲為 80 毫秒，因此，駭客有機會透過 Wi-Fi 網路執行遠距離的攻擊行動，中繼的 BLE 通信的延遲可以調整與未中繼的通信相匹配。

2. 愛達荷國家實驗室所採用虛擬數位技術

主講人介紹：Kolton Heaps，任職於愛達荷州國家實驗室

相關連結：https://www.youtube.com/watch?v=Gc56q16RAGg

日常生活依賴的關鍵基礎設施，如水、電領域設施，可能存在安全性威脅。愛達荷國家實驗室的 CELR Group，透過微電網等不同的基礎設施，進行網路安全、混合實境（Mixed Reality，簡稱 MR）及虛擬實境（Virtual Reality，簡稱 VR）等研究。

圖8.截自影片之 3D Modeling and VR

(1)虛擬數位技術

虛擬數位技術正悄悄的改變人類與數位領域的互動模式，擴充實境（Extended Reality ，也有稱 X - Reality 或 Cross Reality ，簡稱 XR）係包括虛擬實境（Virtual Reality ，簡稱 VR）、擴增實境（Augmented Reality ，簡稱 AR）和混合實境（Mixed Reality，簡稱 MR）功能。

A.虛擬實境（Virtual Reality，簡稱 VR），用戶與實體世界的互動是分開的，VR 描述使用者使用虛擬環境，完全取代實體環境，使用者可藉此查看所有數位內容，通常是藉由攝影機，以及辨識相關技術結合，利用投攝而顯示出來的影像擴充虛擬物件，讓使用者得以與其互動。

B.擴增實境（Augmented Reality ，簡稱 AR），AR 是使用者在實體世界，多了虛擬疊加的效果，但使用者幾乎未與數位內容互動。

C.混合實境（Mixed Reality，簡稱 MR），MR 是實體世界與數位世界的融合，仿如置身 3D 世界，與電腦和環境間自然的互動。簡單而言，MR 是 AR 和 VR 的融合，通常都會搭配頭戴式的顯示器，如同看到現實環境，另外再疊加虛擬。下圖係利用頭戴式顯示器 Microsoft HoloLens 在混合實境系統的示範。

D.擴充實境（Extended Reality ，也有稱 X - Reality 或 Cross Reality，簡稱 XR），XR 包括 VR、AR、MR 的功能。

圖9.截自影片之 MR 示意圖

相關連結：https://www.youtube.com/watch?v=Gc56q16RAGg

(2)DIGITAL TWIN

DIGITAL TWIN 概念在工業界引起廣泛討論，其整合資料視覺化、人工智慧和機器學習，以及與實體模型形成一個有凝聚力的 DIGITAL TWIN。國家實驗室嘗試對 DIGITAL TWIN 重新定義，DIGITAL TWIN 是不同技術的融合，包含實體資產的感測器、儀器連接的數據整合。從系統取得數據回饋至視覺化、人工智慧、機器學習的演算法中。

(3)下一代 XR 技術

愛達荷國家實驗室正使用一套工具來增加視覺化應用、數位分析能力，並將整合到支援能源、核能甚至國土安全相關項目。這套工具具有視覺化捕捉和數位數據分析能力，以現今科技尚須依賴領域專家手動收集、檢查及解讀異常數據。更深入的研究議題在於 XR 與訊號分析結合，簡單解釋數據與呈現複雜數據更是重要。能在空間上查看所獲得的數據，識別和描述數據的過程，會讓應用更加簡化。

(4)進階應用

實驗室引進 XR 技術，透過視覺化設施中的組件，提高空間效率。也讓每個組件項目在實際創建前能即早發現錯誤。舉例說明，某系統採人工智慧預測分析技術，可使用學到的數據預測未來 15 分鐘內可能發生的數據。這對操作人員來說，除可瞭解現況之外，亦可提早預測系統可能產生的問題，方便人員將系統調整為手動控制，讓系統維持正常運作。

圖10. 截自影片之人工智慧預測分析

相關連結：https://www.youtube.com/watch?v=Gc56q16RAGg

3. DEF CON 31 主題 VILLAGE

(1)POLICY VILLAGE

DEF CON 的 POLICY VILLAGE 除談論網路安全漏洞外，本年度政策亮點包括資料外洩法律政策、監督管理等，除了資安駭客外，更有來自法律政策等不同領域的專業人士聚集在 101 會議室。

(2)AI VILLAGE

AI VILLAGE 會場提供八個供應商提供的模型，也提供筆電讓參與的 AI 工程師測試這些模型或合組紅隊攻擊供應商提供的模型。

(3)CAR HACKING VILLAGE

CAR HACKING VILLAGE 會場停放一台特斯拉電動車，駭客可透過破壞無線電數據系統來干擾廣播電台，藉由調整電動車行動電腦的頻率，將可以看到系統資訊，如果開始對其進行模糊測試，可能會導致某些電動車的系統無法正常運行。會場的電動車，本質是一台帶輪子的電腦，如果電動車系統無法運行，整台電動車將無法按照駕駛指示正常運作。CAR HACKING VILLAGE 除了讓大家了解電動車的網路安全問題之外，也希望藉由這個場域找到漏洞、回報給車商。

(4)LOCK PICKING VILLAGE

還有一些與資訊安全無直接關聯的活動，如 LOCK PICKING VILLAGE，會場聚集許多感興趣的人參與撬鎖，參加活動並非為了就業，純粹是挑戰和競爭，參加者無不想方設法，期望在最短的時間內打開桌上面的鎖，獲得勝利。

(5)XR VILLAGE

XR VILLAGE 會場上有 AR 的介紹，分享相關研究、專業見解和政策建議，此外，宣導具安全性設計的 XR 體驗，以及 XR 在行動安全方面的安全性及隱私問題。AR 分為定位型態與非定位型態。在應用上，也非常多元，如建築領域、導航、心率監測器、化妝應用、換臉技術、遊戲、軍事消防等用途。在 AR 的行動安全方面，也提及 OWASP 行動安全測試指南等，可再另行深入研析。

圖11. 截自影片之 CAR HACKING VILLAGE

圖12. 截自影片之 CAR HACKING VILLAGE

圖13. AI VILLAGE 展場

相關連結：

https://www.youtube.com/watch?v=rH_s0SpUQTM&list=PL9fPq3eQfaaCb7d8v5OZDAFUWHcq0V3Fq&index=3

https://www.youtube.com/watch?v=jDgYDNqDPI0&list=PL9fPq3eQfaaCb7d8v5OZDAFUWHcq0V3Fq&index=7

https://www.youtube.com/watch?v=2YyyTkMdWik&list=PL9fPq3eQfaaCb7d8v5OZDAFUWHcq0V3Fq&index=10

https://www.youtube.com/watch?v=nCEGBQyMxK4&list=PL9fPq3eQfaaCb7d8v5OZDAFUWHcq0V3Fq&index=2

https://www.youtube.com/watch?v=Xu8pR8DaO0o

https://www.youtube.com/watch?v=DsTEbsNM2G0&list=PL9fPq3eQfaaCb7d8v5OZDAFUWHcq0V3Fq&index=5

4. DEF CON 31 CTF 搶旗攻防競賽

(1)預賽準備

DEF CON 31 CTF 搶旗攻防比賽，預賽係採線上 48 小時不間斷的連線競賽，全球有 1,828 隊參賽，排名前面 12 名的隊伍才能晉級參加現場決賽，並於美國拉斯維加斯舉行決賽。代表我國參加的台灣聯隊 TWN48 ，除了平時不斷練習精進實戰技能，也有舉辦選手見面交流，先培養彼此間的默契。

再者，預先準備比賽用之軟硬體環境，不可或缺的則包括網路建置及賽事期間的穩定性之掌握，都非常重要。備妥在競賽期間可能會使用到的軟體工具，包括封包分析工具、程式修正工具、計分統計工具等等。

(2)DEF CON 31 CTF

賽事期間的解題過程，大會即時新訊的瞭解，最新題目及當下的攻擊封包、流量等態樣及數據分析，亦須隨時掌握跟因應。在連續三天的比賽中，會場之動態成績顯示器不斷的更新排名與成績。在比賽結束時，台灣聯隊 TWN48 嶄露頭角，攻擊面 Atk 績分 5,128 分、防禦面 Def 績分 370 分，Koh 績分 758 分，Live CTF 績分 500 分，取得總績分 6,756 分，決賽第 3 名的好成績，總成績揭曉如下：

表 1 總決賽成績圖示

名次	隊名	績分
1	Maple Mallard Magistrates	9,801
2	Blue Water	7,428
3	TWN48	6,756
4	Hypeboy	5,794
5	StrawHat	5,465
6	Norsecode	5,415
7	P1G_BuT_S4D	5,393
8	SuperDiceCode	5,315
9	Orgakraut	4,753
10	Mhackeroni	4,562

Name	Atk	Def	KoH	LiveCTF	Total
Parliament of Ducks	6436	329	1699	1337	9801
BlueWater	4879	208	1741	600	7428
TWN48	5128	370	758	500	6756
hypeboy	3545	163	1086	1000	5794
StrawHat	3788	115	662	900	5465

圖14. DEF CON 31 CTF 奪旗賽成績

圖15. DEF CON 31 CTF 奪旗賽 12 個隊伍

Final Scoreboard

Only the 535 teams that scored. Can't find your team? Check on the teams page.

Place	Team name	Score	Time of Last Solution
1	Blue Water	3753.0	2023-05-28 19:13:50 UTC
2	The Parliament of Ducks	3499.0	2023-05-28 21:22:55 UTC
3	orgakraut	3466.0	2023-05-28 23:48:11 UTC
4	SuperDiceCode	3398.0	2023-05-28 23:37:32 UTC
5	TWN48	3236.0	2023-05-28 22:41:55 UTC
6	Straw Hat	3204.0	2023-05-28 22:25:51 UTC
7	Norsecode'23	3090.0	2023-05-28 23:54:24 UTC
8	mhackeroni	2920.0	2023-05-28 22:32:12 UTC
9	P1G BuT S4D	2745.0	2023-05-28 23:48:49 UTC
10	Shellphish	2500.0	2023-05-28 23:52:24 UTC
11	undef1ned	2481.0	2023-05-28 23:17:23 UTC
12	HypeBoy	2417.0	2023-05-28 22:28:44 UTC

圖16. Scoreboard

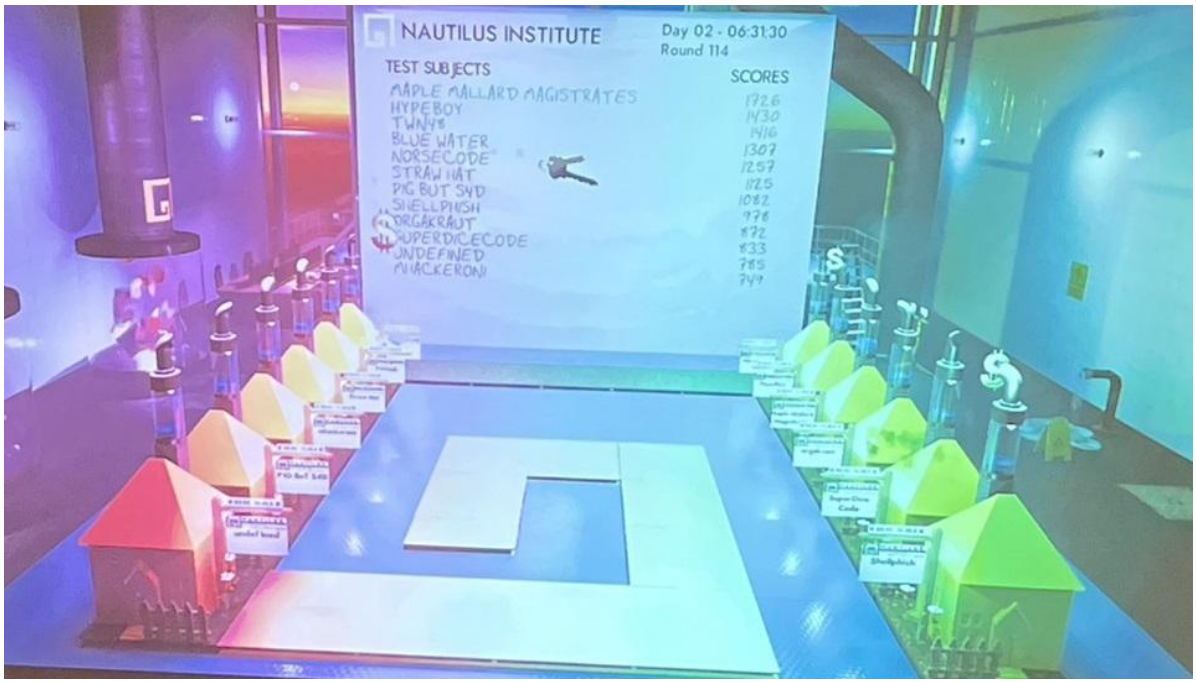

圖17. 動態成績不斷更新

參考來源：2023 世界駭客大賽 DEF CON 31 CTF

相關連結：https://DEF CON.org/

圖18. Challenge Coin

圖19. DEF CON 31 閉幕會場情況

圖20. BLACK HAT USA 識別證、DEFCON 徽章

二、 黑帽駭客大會（BLACK HAT）

(一) BLACK HAT 介紹

BLACK HAT 是國際公認的網路安全活動，會中提供最具資訊安全技術及相關性研究。業內最優秀的人才會經此管道聚集在一起，藉此可以瞭解最新的技術研究、發展和趨勢。

來自世界各地的相關人員，每年都會藉由大會舉辦時，分享最新的漏洞資訊，而與會者，則可獲得開創性的研究體驗。 BLACK HAT 提供以下資訊通安相關技術性資訊，並設立評審委員會之審查機制，致力吸引頂尖人才及研究。BLACK HAT 提供簡報及個人技術課程，讓有興趣出席者可以參與。在簡報部分，資安專業人員得以瞭解最新資訊安全風險、研究和趨勢，包括一系列的熱門設備漏洞、關鍵性基礎設施威脅等。邀請各領域專家講授個人技術課程，包括最新的滲透測試、利用 Web 應用程式之保護，如何攻擊和防禦未來的資訊安全格局等精心設計的主題。

BLACK HAT 大會的評審委員會，就每個提案的獨特性、整體內容專業知識和精確性進行審查。分區設置簡報評審委員會、培訓評審委員會、諮詢評審委員會，由逾 100 名最可信、最傑出的業界人士，更涵蓋資訊安全的各個領域的專業人士組成。而審查委員會具有相當的研究洞察力，會就其策略方向、審查和程式設計會議內容提供建議。就簡

報評審委員會再細分，亞洲、歐洲與美國三個評審委員會。查美國評審委員會之委員部分，包括 SHEILA A. BERTA（HEAD OF RESEARCH、DREAMLAB TECHNOLOGIES）、DAVID ADRIAN（GOOGLE）、USTINE BONE（PARTNER、RIDGE PARTNERS）等，逾 60 名委員。

藉由 BLACK HAT 密集的技術及相關簡報培訓、座談會議、社交活動、展場大廳會議等，提供與會人士專業的互動以及學習的交流跟機會。參加成員，常見有：資安相關行業人員、資安主管、廠商、業務開發人員、求職者和招聘廠商、學術界師生等，藉此拓展互動和交流的機會。

(二) BLACK HAT USA 議程及會場

圖21. BLACK HAT USA 會場_贊助商名單

圖22. BLACK HAT USA 展場_未來將進行之場次

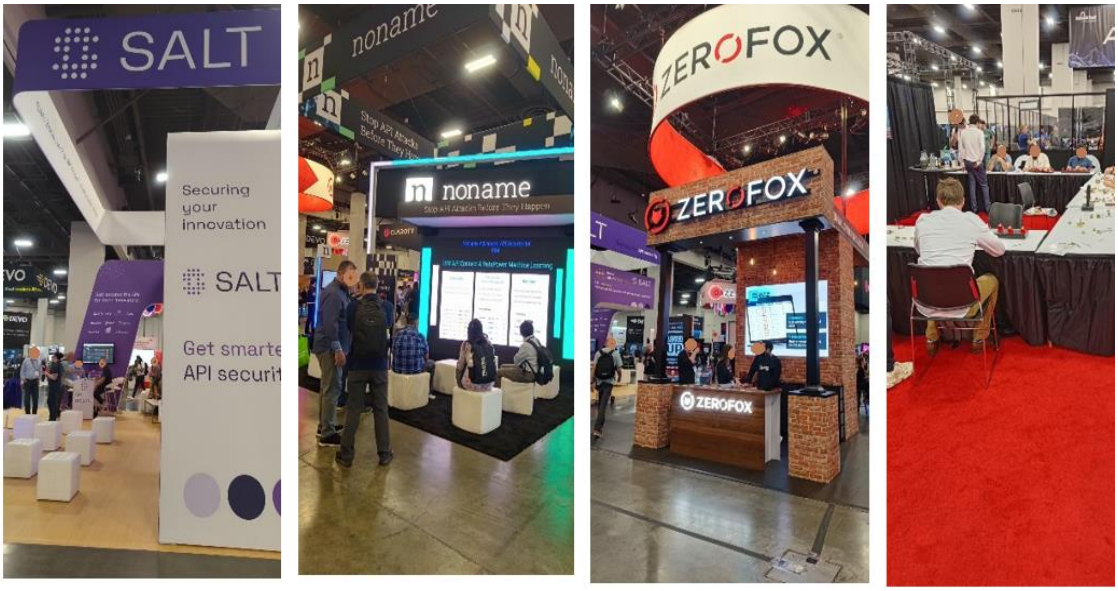

圖23. BLACK HAT USA 展場

(三) 本次會議參與之重點

1. 美國之網路安全策略及人才培育

主講人介紹：

Kemba Walden，美國代理國家網路總監(Acting National Cyber Director, Executive Office of the President)

Jason Healey，哥倫比亞大學國際與公共事務學院高級研究學者(Senior Research Scholar, Columbia University's School for International and Public Affairs)

時間：2023 年 8 月 10 日 09:00~10:00

演講介紹：代理國家網路總監Kemba Walden討論「國家網路安全戰略實施計劃」和「國家網路人力資源和教育戰略」的細節。

相關連結：https://www.blackhat.com/us-23/briefings/schedule/

就美國網路安全策略及資安人力培育方面，分別以策略的透明度、監測策略的成功、開源軟體安全、監管和法律法規、策略背後的價值觀、人工智慧（AI）及其防禦方面的應用、技術的用途、人才培育及養成策略等做分享。

(1) 美國網路安全策略訂定與成果監測

關於策略的透明度，其策略之實施計劃已經在白宮網站上公開，包含 69 個行動項目，由 18 個部門和機構負責。該項計劃中，明確列出了每個行動項目的截止日期、主導機構和支援機構。

監測策略是否成功，非常重要。然而如何確定策略是否成功是一個重要問題，特別是如何確定數位領域是否變得更具防禦性。監測指標包括預算使用情況、平均檢測時間、開源軟體的漏洞數等。政府正在積極尋找資金來支持策略的實施，包括聯邦政府、國會撥款、國家科學基金會等。

(2) 美國網路安全策略相關之法律規範

法律法規部分，政府的管理方法是提高最低的資訊安全基準要求，而不是隨意的監管。白宮希望實現法規的協調和互惠性，以減少企業需遵守的不同規則和法規。目標是建立一個協調一致的監管環境，提高資訊安全水平。

策略背後的價值觀而言，策略的主要目標是提高數位領域的防禦性，減少使用者端的負擔。政府不是出於監管的目的，而是為了提高資訊安全要求。

(3) 人工智慧在美國網路安全策略之角色

人工智慧（AI）部分，AI 對各方面產生影響，包括工作、人才培養和防禦。AI 關注的焦點包括數據保護、隱私保護、晶片供應鏈安全和人才培養。AI 既可以用作工具，也可以用作攻擊工具，必須在使用中加強保護和設置適當的管理措施。AI 在防禦方面的應用上，AI 除了可以用來增強防禦，例如用於快速修補漏洞。更是可以善用其潛力發揮，可以利用 AI 改變防禦策略，但需要制定適當的規則和協議來確保安全使用。

在技術的用途方面，技術本身是中性的，取決於人們如何使用它。需要考慮如何合理、有效地利用新技術，並確保技術的用途符合道德和價值觀。

(4) 開源軟體及技術應用對美國網路安全策略之影響

另外在開源軟體安全部分，白宮已經提出了有關安全開源軟體的訊息請求，希望了解如何提高開源軟體的安全性，以確保記憶體安全（Memory safety）。目標是實現軟體開發生命周期的安全性設計，以減少軟體漏洞和需要修補的情況。

(5) 人才培育及養成

在人才培育及養成策略方面，眾所皆知，人才是數位領域的重要組成部分，政府正在制定相關策略，包括提高數位素養、計算素養、教育體系中的數位素養、職業技能發展、軍事和農村的人才培養等。通過不同的法律法規和項目，政府正在提供資金來支持人才培養和培訓。另外，現就 AI 領域觀之，AI 對人才需求產生影響，需要培養具備適當技能的工作人員，以有效地應對新技術。人才培養不僅關注人數，還關注工作內容的變化，以確保人才能夠適應新環境。技術可以減少一些工作的需求，但同時也可以創造新的機會和需求。

2. 美國網路政策綜觀

主講人介紹：Harley Geiger，Venable 律師事務所網路安全律師

(1) 關鍵基礎設施

2022 年 7 月公布的「國家網路安全戰略」點出關鍵基礎設施的重要性，其攸關國家安全、民生經濟。2022 下半年是美國政府納管關鍵基礎設施網路安全的轉折點，在此之前，除金融及電力領域之外，多由各領域自行管控風險，許多領域尚無網路安全規則。政府採取與相關領域合作方式，共同制定各領域之計畫，採行相對彈性的管理方式。2022 年底之後，政府更透過國會立法，明確要求關鍵基礎設施制定網路安全規則。

水資源領域、交通鐵路、航空領域、金融業等陸續展開新監管模式，醫療領域也開始新措施。在國家網路安全戰略中，關鍵基礎設施是第一優先事項，預期未來幾年會有更多的領域持續發展其網路安全政策。

(2) IoT 安全標誌的興起

另一個重點是 IoT 安全標誌，也被稱為信任標誌。IoT 安全標誌為聯邦政府推動的新計畫，目的是讓消費者了解物聯網設備的安全性。標誌上會標示產品是否達到某些網路安全基準及安全功能。

聯邦通訊委員會已提出 IoT 安全標誌的法規草案，該法案目前為徵詢意見階段，預計最快 2023 年完成訂定。安全標誌將擴大適用於路由器、監控攝影機等消費級連網產品、工業物聯網等其他領域。通過國家標準與技術研究院(NIST)制定的安全基準測試，產品才能使用此標誌。安全標誌採用多層次設計，兼顧普通消費者和安全專家之需求。如果產品未達標準卻使用了標誌，該廠商將面臨假廣告之法律責任。

(3) 漏洞揭露的監管趨勢改變

漏洞揭露始終是 DEF CON 期間廣泛討論的主題，良好的漏洞揭露提供開放的管道，讓揭露者提交漏洞資訊，廠商或系統開發商則進行初步分析及採取行動，甚至經由雙方討論後，揭露者可在社群媒體上分享漏洞資訊。然而，越來越多的法規傾向將漏洞揭露給政府機構的監管趨勢，其中，歐盟網路韌性法案(Cyber Resilience Act)刻正訂定且深

具影響性，一旦通過將產生類似 GDPR 的影響，該法案要求企業在發現產品漏洞被利用後的 24 小時內通知政府機構，這適用於歐盟出售的任何軟體，其他重點如下：

A.2022 年 9 月由歐盟執委會提出，目的是建立歐盟共同的網路安全規範，提高歐盟的網路韌性。

B.適用對象包括必要服務的提供者，如能源、運輸、銀行、衛生、數位基礎設施等關鍵領域。

C.引入網路安全風險管理措施，要求企業進行風險評估並採取預防措施。

D.加強關鍵基礎設施的安全要求，並建立安全弱點揭露機制。

E.設立懲罰機制，違反法案規定者將面臨高額罰款。

F.法案預計於 2023 年底正式通過並開始實施。

中國政府亦有類似的漏洞揭露規定，其要求每個組織制定協調漏洞揭露(Coordinated Vulnerability Disclosure，CVD)政策，揭露報告最終必須提交給中國政府，漏洞發現者可選擇向漏洞所屬的公司揭露訊息，再由該公司通報中國政府，或由漏洞發現者直接通報中國政府，漏洞資訊不得私下再至其他組織或社群討論。

法國(Military Programming Legislation，軍事計畫法)、美國(Federal Information Security Management Act，FSMA)均已制定漏洞揭露相關法律，礙於時間本次會議並未詳述。最後，主講者語重心長的表示，會議提及各國的漏洞揭露時限與通報對象規定，要求廠商或系統開發商短時間內揭露系統未緩解的漏洞及向政府機構通報的要求，可能導致更大的風險。

(4) 事件通報之法規要求

除了漏洞揭露之外，事件通報(Incident Reporting)亦有相關法律規定要求，

A.關鍵基礎設施網路事件通報法(Cyber Incident Reporting for Critical Infrastructure Act，CIRCIA)：適用於關鍵基礎設施擁有者和運營商、承包商，若其發生重大事件，必須於 72 小時內通知 CISA。

B.美國證券交易委員會(Securities and Exchange Commission，SEC)要求上市公司遭遇重大資安事件的四天內，透過 8-K 文件上傳 EDGAR(Electronic Data Gathering, Analysis, and Retrieval System)系統對外界揭露事發細節。

(5) CISA 補充說明

主講人介紹：Lauren Zabierek，網路安全和基礎設施安全局網路安全部門高級顧問

針對即時威脅採取強化安全措施(如阻擋、應對、預防等)，確保攻擊者無法輕易侵入關鍵基礎設施，可確保關鍵基礎設施和國家安全受到適當的保護，此為 CISA 的重點任務。正如 Harley 先前提到的，通報事件並不等同於韌性。因此，作為國家網路安全戰略的一部分，確保產品、軟體和硬體的安全性，才是真正提高韌性與安全性的關鍵因素。

今年三月提出的國家網路安全戰略(National Cybersecurity Strategy)主要係透過國會立法授權、資金挹注，及國家網路安全主任辦公室的戰略方向指引。未來一年，CISA 將致力於數據合作、網路響應、恢復基金等工作項目，其來自網路安全戰略計畫，以提高可視性與減輕威脅之能力。

3. 美國推動醫療設備網路安全

主講人介紹：Suzanne Schwartz，FDA 放射健康設備中心戰略合作夥伴和技術創新辦公室主任

(1) 醫療設備安全漏洞展示的危險

多年來，BLACK HAT 和 DEF CON 現場經常展示醫療設備的安全漏洞，這些安全漏洞可能產生重大、甚至導致患者死亡的傷害。即便白帽駭客、安全研究人員已事先聲明可能的影響，但醫療業及相關製造商仍持續要求停止展示，並向美國食品藥物管理局(U.S. Food and Drug Administration，FDA)投訴，強烈建議禁止類此活動，以免將病患置於危險之中，也避免大眾對這些設備產生信任危機。

(2) 醫療設備之網路安全發展與管理宗旨

站在 FDA 的立場，醫療設備如不具網路安全性，該設備便無法確保醫療安全。為使患者得以安全使用，醫療設備必須具備基本的網路安全設計、保護功能，尤其是具連網功能或內建軟體功能的醫療設備。FDA 以保護與促進公共健康為使命，後續將透過監管活動實踐公共健康保護，包括監督醫療器材網路安全發展。

(3) 醫療設備上市前指南

先前的合理安全與有效保護，並不一定符合網路安全。因此，在未明確制定政策之前，推動或加強網路安全顯得困難重重。

首先，要求醫療設備製造商向 FDA 提出系統數據或證明文件，證明該設備係合理安全與有效保護，經過 FDA 審核同意後，醫師才能給予患者使用。2013 年至 2014 年期間，首次發布指引，期望製造商先設計符合安全的基本要求。

這段期間，藉由與業者的溝通、互動，許多利害關係人的共同參與，包括醫療機構、醫護人員、安全研究人員、社群、患者、醫療設備製造商。迄今，已成立一個第三方安全供應商組成的利害關係群組，共同努力嘗試改變醫療部門及醫療業的文化，讓大家了解新興的安全威脅、醫療領域免受攻擊的重要性。在推動前期，製造商先確保設備的安全性。此時，已有許多行政命令、政府開始重視相關議題，為推動整體醫療領域網路安全奠定基礎。

(4) 售後市場指南

2016 年發布的售後市場指南，指出設備在上市後須確保安全性。在設備的生命週期內可能出現安全漏洞，這些漏洞可能被識別、揭露，製造商負有保持和維護設備風險管理之責。

就網路安全而言，售後市場指南應包括漏洞揭露。製造商須先建立流程及政策，一旦收到漏洞訊息，應就該漏洞進行必要之評估與分析，以確認風險類型。若風險涉及關鍵性質、無法緩解之漏洞，製造商必須透過相關的補救措施來降低風險，之後，再與 FDA 協調讓大眾周知，以降低依賴此類設備(如心臟相關設備、植入式設備、胰島素相關設備等)患者家屬的信心危機。

為推動醫療設備的網路安全，美國 2018 年 4 月 17 日發表一份名為「醫療設備安全行動計畫：保護患者以及提升公眾健康」，內容已包含網路安全。藉由檢視「產品生命週期」(Total Product Life Cycle，簡稱 TPLC)，以提升醫療設備之安全性。同時，進一步要求醫療設備的網路安全，包括漏洞揭露、軟體材料清單的強制要求，並要求製造商主動提醒醫療機構。在漏洞揭露前期，製造商必須提供適當的證據，證明設備已進行修補或更新安全性，確認不會影響該設備性能。

4. 美國國家網路工作和教育戰略

主講人介紹：Michaela Lee，白宮國家網路辦公室戰略和研究團隊主任

(1) 網路定義各異

網路政策面臨的挑戰，部分來自各方對網路的不同理解，一方認為網路是攻擊對手的工具及方法，企業應妥善保護網路，或展開關鍵基礎設施的防禦。對某些人來說，網路是一種工作分類，以幫助聯邦政府確定部門和機構需要的技術技能類型。

白宮國家網路主任辦公室(Office of the National Cyber Director，ONCD)是新設組織，專門研究網路政策、技術及相關問題，可提供政府決策制定者有關網路戰略的資訊。

(2) 國家網路安全戰略

2023 年 3 月總統簽署並發布的國家網路安全戰略，提出二個基本變革，其一為監管與協調，其二是對網路安全長期投資的激勵思考。

在網路監管部分，重點在負擔轉移，亦即轉移負責網路安全風險管理者的負擔。希望從終端使用者移轉至最具能力、可負責的實體，包括監管和監管協調。其中，也希望改善弱勢狀況，要求小學、鄉鎮醫院診所與跨國組織抗衡是不公平的。

對網路安全的長期投資非常重要，國家網路安全戰略的另一個變革就是思考如何激勵網路安全的長期投資。無論公、私部門，在選擇解決方案時，鼓勵選擇長遠的解決方案，避免簡單而暫時性的解決方案，期待形塑此等文化。即便政府立法並已投入數百萬預算於基礎設施，若對潛在風險了解不足，未能於初始建立網路安全措施，數年後才發現基礎設施的漏洞風險，屆時再拆除或汰換，需要的預算會更多。

然而，為確保重要的基礎設施一開始即是安全的，必先納入相關的安全設計。以長遠來看，激勵長期性的投資，除可避免未來產生風險，整體經費也較為撙節。

(3) 國家網路工作和教育戰略

今年度發布的「國家網路工作和教育戰略」，突顯人才及專業知識長期被低估。為確保國家整體網路生態系統安全，需要培訓專業人才，共同協防關鍵基礎設施、思索 IT 與 OT 相關的問題，甚至共同參與相關決策。此戰略即是美國政府為解決上開問題，並培育下一代人才的計畫。國家網路安全戰略包括可防禦性、強韌性及價值觀一致性，礙於時間並未深入探討價值觀一致性。

5. 各國在人工智慧方面的網路安全政策

主講人介紹：Weather West，Venable 律師事務所網路安全與隱私服務資深總監

(1) 人工智慧與網路安全的競合

今年的人工智慧（Artificial Intelligence，簡稱 AI）非常熱門， AI 與網路安全產生微妙的影響。AI 對許多領域的發展舉足輕重，座談中提及部分政策低估 AI 對網路安全的重要性。各主要國家逐漸意識到 AI 的重要性，部分領域業界也著手與政府合作，努力確保 AI 的安全性，讓使用者更安全的使用 AI。

(2) 各主要國家的人工智慧法案

美國開始意識到人工智慧（AI）的重要性，有大量的國會和州提案，各有不同的觀點。有些觸及安全問題，有些涉及公平及偏見(如，有些州提案關於招聘偏見)。隨著資通訊科技的高度發展，人工智慧逐漸成為發展其他技術或應用的基礎，DARPA 也在本次大會宣布「DARPA AI Cyber Challenge」，呼籲電腦科學家、人工智慧專家、軟體開發人員等踴躍參加人工智慧網路挑戰賽(AIxCC)，這是一項為期兩年的競賽，旨在推動人工智慧和網路安全之創新，期待能創造新一代網路安全工具。

歐盟的 AI 法案正進行協議、最終談判，談判代表計劃依據即將推出的 AI 法案，對最大的 AI 系統實施額外管制。來自不同國家提出約 50 個國家戰略，顯示各國開始思索與人工智慧的應對，並設法讓人工智慧更安全。

另查英國在 AI 監管上，採取指導原則；歐盟在 AI 監管採立法方式。無論是英國的人工智慧監管規範政策報告、歐盟的人工智慧法案等，都可以再深入瞭解。

(3) 駭客法律責任

「數位千禧年著作權法」(Digital Millennium Copyright Act, DMCA)第 1201 條要求規避軟體技術保護措施前應獲得軟體版權所有者之授權，先前尚無例外情形，近年來稍加鬆綁，惟仍禁止安全研究人員將安全工具公諸大眾。「電腦詐欺與濫用法案」（Computer Fraud and Abuse Act，CFAA）禁止未經授權或逾越授權存取美國政府、各類企業及個人的電腦，美國司法部 2022 年 5 月 19 日宣布修改政策，將不會依據美國電腦犯罪相關法令控告進行「善意」安全研究的研究人員，但倡議團體認為修改幅度仍遠遠不夠。

6. 選舉安全與網路安全

主講人介紹：Lindsey Forson，全國國務卿協會副執行主任

全國國務卿協會 (National Association of Secretaries of State，NASS)是美國歷史最悠久、跨黨派的公職人員專業組織，會員包含 40 個州的首席選舉官員(多為國務卿、副州長)，該協會提供選舉和投票、國家商業服務、網路安全和檔案/記錄管理等服務。NASS 下設網路安全委員會，該委員會致力於促進 NASS 成員分享有關州、地方和聯邦層級網路安全政策相關資訊。NASS 另設選舉委員會，該委員會提供 NASS 成員有關州和聯邦層級選舉管理相關政策和實踐的教育和資訊，設置論壇討論促進選民參與的策略與分享選民教育和外展的創新實踐。

自 2016 年美國總統大選以來，選舉安全一直是人們關注與爭論的焦點，隨著選舉被指定為關鍵基礎設施，國務卿協會的角色更形重要。美國的選舉管理制度高度分權，選舉是州和地方選舉機構的憲法責任，例如國務卿、選舉管理員、縣書記員或其他地方官員，包括全國 6,000 多個地方政府。NASS 積極推動「Cyber Navigator 計劃」，派遣各州雇用人員前往縣、市政府，與當地政府工作人員合作，該計畫也讓 NASS 了解，多數地方選舉辦公室通常由縣或市政府，甚至是託管服務提供商(MSSP)獲得 IT 和網路安全協助。

(1) 建立州辦公室網路安全團隊

網路安全工作不再僅由資訊長處理，許多州辦公室正在聘用資安長(CISO)，並在 CISO 領導下建立團隊。

(2) 建立漏洞揭露政策，與駭客社群合作

透過各州辦公室 CISO 領導網路安全工作，努力與駭客社群建立聯繫、改善關係，引導州政府建立漏洞揭露政策，另鼓勵資訊長也進行類似工作，即便是研究資訊安全的社群亦可。近年來，除與地方政府合作外，亦向地方政府、州政府要求提供網路事件報告。在供應商合作方面，透過契約要求供應商共享漏洞評估、供應商建立協調漏洞揭露政策等。

參、 心得與建議事項

目前，我們正處於資通訊科技高度發展的世代，隨著資通訊科技日益普及，資訊化、網路化、數位化帶給個人、企業、政府許多優勢、機會，如改善個人日常生活品質、優化企業核心經營模式、提升電子化政府服務綜效等。看似美好的現況也帶來一些隱憂，設計不完善的資通訊科技產品(軟、硬體)可能導致不安全的使用風險，這相當值得我們留意，任何資通訊產品的設計缺陷都可能成為駭客發動攻擊的入侵點。水能載舟亦能覆舟，惡意軟體也帶來個資外洩、加密企業營運資料、攻擊政府關鍵基礎設施等衝擊個人生活、社會經濟、國家安全之危害。

「國際資訊安全會議（DEF CON）」與「黑帽駭客大會（BLACK HAT USA）」是全球著名的駭客大會，除了技術導向的議題之外，也有探討網路政策的座談。由於本署執掌「國家資通安全政策之研擬、規劃及執行」，出國期間也參加「US Policy 101」座談會議，瞭解美國及世界主要國家在資安政策、法規與重要措施之推動現況及未來規劃，他山之石可以攻錯，有助於本署推動相關政策之評估與參考。

「US Policy 101」網路政策座談提及美國近年來對「關鍵基礎設施」、「事件通報」及「漏洞揭露」之監管趨勢，我國目前則透過資通安全管理法、資通安全通報及應變辦法等法規與國家資通安全通報應變網站(N-CERT)、台灣電腦網路危機處理暨協調中心(TWCERT/CC)等機制進行管理。雙方雖有類似的監管機制，由於美國的行政區劃及法律制度多元發展，監管的侷限性也有所不同。此外，美國聯邦政府為管理物聯網(IoT)的網路安全，正試行物聯網網路信任標誌計畫，我國或可參考電腦設備「能源之星(Energy Star)」標誌之作法，評估於資通訊設備張貼網路安全標誌，透過 QR Code 提供設備安全的相關資訊(如製造商、產地、韌體版本等)之可行性。有關醫療設備網路安全管理部分，衛生福利部業於今年 10 月 27 日公布「衛生福利部醫療領域資通系統資安防護基準」，針對醫療儀器進行資安分群分類管理，其中，「資安列管醫療儀器」終端儀器群邊界主機與控制系統群為醫療儀器資通系統防護基準之防護標的，應依該防護基準執行控制措施。礙於「US Policy 101」座談時間有限，上述項目都值得再深入了解。

最終，他們對 AI 的應用也進行了深入探討，特別是在數據保護、計算能力和演算法方面。 AI 對工作力量的影響被視為重要議題，包括對人員的招聘、培訓和保留，以

及如何使 AI 成為有用的工具。主講人就AI技術所帶來的潛在風險與優勢進行了討論，並對如何運用 AI 技術提出了一些初步想法。其中可供我國參考的部分，包括建議可要求承辦人員不可向生成式 AI 提供公務上應保密、未經個人或機關同意公開的資訊，亦不得向生成式AI詢問涉及機密資料、個人資料的問題，以維機關資訊安全。

會議亦有就關鍵基礎設施的網路安全的探討。在關鍵基礎設施部分包括，醫療設備的網路安全推動，保護患者以及提升公眾健康。激勵長期性的網路安全投資，除了可避免未來風險產生，綜觀整體經費也相較節約。

競爭激烈的2023世界駭客大會（DEF CON 31）CTF（搶旗攻防賽）決賽結果出爐，在全球 12 支進入決賽的隊伍中，臺灣聯隊 TWN48 嶄露頭角。打敗了來自日本、韓國、中國、丹麥等國駭客高手，勇奪第 3 名的佳績，僅次於奪冠的 Maple Mallard Magistrates隊。 Maple Mallard Magistrates 隊，是由傳統強隊美國卡內基美隆大學的PPP成員以及韓國的 The Duck 組成），亞軍則是 Blue Water 國際聯隊。查我國歷年所取得最高名次為第二名（103年、106年及108年），103年至110年皆有進入決賽前五名, 本次則是獲得第三名的佳績。

有關美國代理國家網路總監 Kemba Walden 之座談談到的資安人才培育之議題，在聽完主題演講後，建議本署未來擘畫我國人才培育政策時，可考慮透過公私協力擴大培育資安人才，並提升資安課程開發及培訓量能，以強化資安人員專業職能，可藉由定期調訓各機關資安（訊）人員之方式，協助公務機關資安專職人員建立所需之專業能力。就整體國家的資安人才培育而言，可自學齡期間向下紮根，讓更多學子從小培養資訊安全的重要意識及興趣養成。在職部分，可鎖定各項產業及不同專業領域培育所需資安人才，投入具潛力的資安專業人才養成。亦可多舉辦各種不同年齡層或領域之資安競賽，結合獎勵及升學加分等誘因，以收培育人才之效。另以資安競賽類型觀之，可發現國內跨校際、區域性大型競賽及各項國際級的競賽，係頂尖之國際資安競賽選手展現實力之場域，除此之外，大型資安交流活動亦可提升資安專業技能，並促進跨域資安人才間交流。

考量政府機關資安人力尚有補充空間，建議可考慮規劃公務人員高等考試三級考試的資訊處理職系下新增「資通安全」類科，開設符合轉任資訊處理職系課程或專班。增設資安類科之外，建議鼓勵各大專校院多納入資通安全類科相關課程，並加強資安技能的廣度與深度，提供青年學子更多學習途徑，在從事資訊（訊）領域工作時，亦得以更貼近實際工作與業務需求。

轉任職系課程，是讓有意願之非資訊處理職系現職人員，於課程完成後，取得符合轉任資訊處理職系專長資格，從事資安（訊）相關業務。建議在課程規劃面，學校可考慮多納入資安相關技術與實作、加強問題分析處理的廣度與深度，培養資安領域銜接能力。