出國報告（出國類別：進修）

國外碩士心得報告書

服務機關：國防部參謀本部資電作戰指揮部網路戰聯隊
姓名職稱：張書睿上尉
派赴國家/地區：美國賓夕法凡亞州匹茲堡
出國期間：107 年 7 月 31 日至 109 年 8月 3 日

摘　　要

本次受訓係奉國防部107年5月3日國人培育字第1070006979號令，核定赴美國卡內基美隆大學（Carnegie Mellon University）就讀「資訊科技與資訊安全學系」(Information Technology and Information Security）碩士課程，學期期程自107年7月30日至109年 8 月3日止，共計2年。

第一年的課程為通訊網路概論(Fundamentals of Telecommunications Networks)、資訊安全概論（Introduction to Information Security）、資訊確保應用（Applied Information Assurance）、惡意程式分析（Malicious Code Analysis）、主機鑑識（Host-Based Forensics）、資訊技術基礎架構庫導論（Introduction to the ITIL Framework）；第二年的課程為專題實作(Practicum)、網路鑑識(Network Forensics)。

目　　次

壹、目的

本次受訓係奉國防部107年5月3日國人培育字第1070006979號令，核定赴美國卡內基美隆大學（Carnegie Mellon University）就讀資訊網路學院（Information Networking Institute）下之「資訊科技與資訊安全學系」(Information Technology and Information Security) 碩士課程，學生可依需求挑選論文學程(Thesis Program)或非論文學程(Non-thesis Program)。

前揭資訊網路學院下設資訊安全學系（Information Security）、資訊網路學系（Information Networking）、資訊科技與資訊安全學系、資訊科技與行動裝置學系（Information Technology and Mobility），僅有碩士之教育學程，餘大學學程與博士學程納入該校之資訊工程學系（Computer Science）及電機工程學系（Electrical and Computer Engineering），使本科系更著重於資訊及網路安領域等，並置重點於理論與實務的結合。

本次出國期間係自107年8月3日至109年8月3日止，共計2年，職遵循非論文學程修畢指定學分數，並完成產學合作實習(Practicum)，由指導教授Patrick Tague及系主任 Dena Haritos Tsamitis完成認證，於 109年8 月3日返台後向資通電軍指揮部網路戰聯隊報到。

貳、學校簡介

一、學校概況與環境

卡內基美隆大學為美國私立大學之一，由 7 個學院所組成，包含卡內基工學院、藝術學院、迪特里希人文及社會科學學院、梅隆理學院、泰珀商學院、海因茨訊息系統和公共政策學院、以及電腦科學學院。學校主校區占地約 0.57 平方公里，在校人數約 14,000 人。校區內有數棟教學大樓，主要有學生活動中心（柯漢大學中心，Cohon University Center）、戲劇大樓（珀內爾中心，Purnell Center）、商學院大樓（波斯納樓，Posner Hall）、工學院大樓（多爾蒂樓，Doherty Hall）、電腦科學大樓（蓋茨·希爾曼，Gates Hillman Complex）、學生會活動中心以及周邊多個學生宿舍。校區內有販賣各國風格食物的學生餐廳、咖啡廳，以及郵局、銀行、體育館、游泳池、各類球場、學生宿舍等，校區附近亦有生鮮市場、速食店、書局、加油站等，生活機能完整。

該校有多項傳統活動，其中以手推車比賽(Buggy Race)最為著名(如圖1)，該項比賽於每年春季嘉年華活動中舉辦，由工學院的學生製作如魚雷造形的手推車，以接力方式完成。賽程中，選手可先以人力將手推車推上上坡後，任其自由滑落下坡及轉彎，再由隊友將其推上上坡，其過程不可有額外輔助工具，車子行進的方向由車中駕駛人員伸出前臂來控制，優先抵達終點者為勝。

圖 1：手推車比賽

二、地理位置

卡內基美隆大學位於美國東部賓夕尼亞州(如圖 2)，坐落於州內西南部的匹茲堡市，以北為伊利湖、以東為費城、以東南為首都華盛頓、以西北至克里福蘭。

匹茲堡曾為美國著名的鋼鐵工業城市，以「世界鋼都」之稱。近幾十年，轉型為以醫療（匹茲堡大學醫學中心）、金融（匹茲堡國家銀行）及高科技工業為主的都市。另外，亦為體育之城，以美式橄欖球之匹茲堡鋼鐵人隊(Pittsburgh Steelers)以及冰球之匹茲堡企鵝隊（Pittsburgh Penguins）為名。

圖 2：卡內基美隆大學地理位置圖

參、過程

一、旅行過程

本次去程於 107 年 7 月 30 日由桃園國際機場搭長榮航空公司啟程，至美國加利福尼亞州(California)舊金山國際機場(SFO)，經轉搭美國聯合航空(United Airlines)至賓夕凡尼亞州(Pennsylvania)匹茲堡市(Pittsburgh)，搭乘公車抵達住宿地點，隨後開始本學程第一年的課程。

由於本學程第二年自暑假課程起，授課地點為卡內基美隆大學矽谷校區，故於 108 年 5 月 19 日自匹茲堡(PIT)國際機場，搭乘美國聯合航空至美國加利福尼亞州(California)舊金山國際機場(SFO)，搭乘公車抵達住宿地點，隨後開始本學程第二年的課程。

回程自舊金山國際機場(SFO)搭長榮航空公司班機，於 109 年 8 月 3 日返台灣桃園國際機場。

二、課程內容

兩年內的學科包含通訊網路概論(Fundamentals of Telecommunications Networks)、資訊安全概論（Introduction to Information Security）、資訊確保應用（Applied Information Assurance）、惡意程式分析（Malicious Code Analysis）、主機鑑識（Host-Based Forensics）、資訊技術基礎架構庫導論（Introduction to the ITIL Framework）、企業管理導論（Fundamentals Of Business Management）、專題實作(Practicum)、網路鑑識(Network Forensics)、進階網路架構(Advanced Real-World Data Networks)、資安事件應變處置(Cyber Forensics Capstone)及資安新創與企業創新(Enterprise Innovation)及等 12 門課程。各學科內容簡介如後：

(一) 通訊網路概論(Fundamentals of Telecommunications Networks)

本學科係以開放式系統通訊（Open System Interconnection，OSI）參

考模型架構為課程架構主軸，於課程中逐一說明各層相關協議與規範，輔以每週文獻閱讀、7 個實機作業、以及期中與期末考試。

（二）資訊安全概論（Introduction to Information Security）

鑑於我們生活日益依賴網路訊息進行日常活動，例如從遠程通訊到金融交易，使資訊安全成為我們關鍵基礎設施的中心問題。故課程內容涵括所有的資訊安全領域，包含密碼學、通訊協定、緩衝區溢位、數位及虛擬貨幣、網路安全、常見軟體漏洞、隱私安全管理與確保等。主要目的是使學生能夠從安全工程的角度考慮訊息技術。此課程包含四項平時作業、以及期中與期末考試。

a. 實作 PGP 加解密電子郵件通訊：一般來說，電子郵件都只提供明文的傳輸，當要傳輸重要文件時，需要做加密，非對稱的加密技術是常見的手法之一。有別於傳統的對稱式加密，透過同一把金鑰進行加密和解密，非對稱加密採用兩把金鑰，分別為「公鑰」及「私鑰」，以作為加解密的基礎。公鑰是可以公開的，私鑰為使用者自己使用。透過公鑰加密，使用對應的私鑰解密，可減少傳統透過一組密碼加解密被截取密碼的風險。

b. 緩衝區溢位攻擊：在程式設計過程中，可能會不小心遺漏了檢查緩衝區的邊界，進而造成了這個程式在執行時可以寫超過緩衝區的大小，導致系統會執行攻擊者欲執行的攻擊程式，造成系統安全上的問題。緩衝區溢位實作方式，包含可分配釋放的堆疊溢位（Stack overflow）和不可分配釋放的堆疊溢位（Heap overflow），課程作業主要係搭配學校自建的平台實作之。

c. Secure Sockets Layer (SSL)和 Transport Layer Security (TLS)通訊加解密實作：SSL 即安全通訊端層，用於保持網際網路連線安全以及防止系統間發送的所有敏感資料被擷取。此技術可使用加密演算法以混淆輸送中的資料，防止駭客在資料透過連線發送時讀取。TSL 為傳輸層安全性，用以更新、更安全的 SSL 版本。此作業為實作 SSL 和 TLS，包含申請憑證，透過 SSL 加密，並於傳輸過程

中，透過 premaster 解密文件。

d. 智能合約攻擊與防禦實作：實作 Solidity 智能合約不當編輯導致的重入攻擊(Re-entrancy)與防禦，此攻擊為調用受害者合約，利用自己的 Fallback 函數，循環調用被害者的代碼。

（三）資訊確保應用（Applied Information Assurance）

此課程以實務應用為導向，包含每週線上實機作業、4 個分組作業與 1 次期末報告。實機作業多為開源或商業工具之應用，分組作業則係透過虛擬資安事故現場，由組員擔任第一線危機應變人員，執行資安事故調查，說明案情概況並完成處置。期末專題報告為設計環境，應用「使用 OWASP ZAP 與 ModSecurity 防護網頁安全」（Web Application Security Testing and Protection with OWASP ZAP and ModSecurity）。

OWASP ZAP，全名為 OWASP Zed Attack Proxy 攻擊代理服務器，透過置於用戶瀏覽器和外部伺服器之間，獲得兩者間交互的訊息，進行漏洞分析、滲透測試、代碼審計、掃描，甚至是訊息竄改重送，以幫助使用者在開發和測試應用程式過程中，自動發現應用程式中的安全漏洞。Modsecurity 則為一個開源工具以實作 WAF 網頁防火牆，可作為入侵偵測與防護引擎。其主要用途是用於網路程式應用，所以也被稱為 Web 應用程式防火牆(WAF)，主要是針對網頁應用程式攻擊深入分析之設備或軟體，可補足傳統 IDS/IPS 對網頁攻擊偵測效果不佳之問題，並保護網路程式以避免遭受來自已知與未知的攻擊。此專題主以透過 OWASP ZAP 模擬攻擊者，Modsecurity 作為防護端，進行雙方攻防演練。

（四）惡意程式碼分析（Malicious Code Analysis）

此課程內容涵括惡意程式碼分析、程式碼混淆技術、惡意程式偵測規則撰寫、惡意程式經濟效益分析至族群結構特徵判斷所構成，此課程包含 4 次平時作業及期末考試。

a. 關於中國菜刀（China Chopper）惡意程式研析：中國菜刀是一個開

源的 Web shell 工具，其特色是檔案小(僅 4 KB)且不易被發現，易於修改負載性。

b. 分析 UPX 加殼惡意程式，並解析其特性。

c. 分析使用 XOR 做模糊化而無法令編碼直接讀取惡意程式。

d. 使用 Ollydbg 進行惡意程式動態分析。

（五）主機鑑識（Host-Based Forensics）

可疑的駭侵行為主要分成主機端與網路端，此課程著重於主機端點的鑑識分析，包含硬體組成架構、檔案系統組態分析、自主機記憶體內切割可疑檔案、時間軸存取分析、RAID 鑑識等。本課程除 5 個平時作業外，另有 1 項案件調查報告撰寫與期末專題報告。

（六）資訊技術基礎架構庫導論（Introduction to the ITIL Framework）

資訊技術基礎架構為一套用於規範資訊科技相關產業服務管理的最佳遵循規範，藉由此套作業程序，最佳化流程與資源的應用，以提升服務水準，課程內容分服務策略、服務設計、服務移轉、服務實踐、服務持續等 5 大部分說明。課程的內容主要係介紹 ITIL 服務管理的關鍵概念及各種實踐方法，讓學生可以了解 ITIL 如何幫助組織推動及持續改善，以提升內部的資訊技術服務效率。

（七）企業管理導論（Fundamentals of Business Management）

課程內容主要分為五大主題：會計、財務、市場行銷、商務營運及策略分析等，課程較有趣之處為採分組方式，各組可登入虛擬貿易平台，以營運各自公司，每位組員有各自的任務職掌，分為操作營運面、財務管理面、市場行銷面與競爭對手分析面等。各組可依據每季營運結果據以調整下次策略，並於年度董事會中向股東報告說明。

（八）專題實作(Practicum)

透過與產業、學界的專題實作課程，讓學生了解課程內容的實際應用、遇到的問題及解決方法。實作的領域包括機器學習、人工智慧、資訊安

全、行動裝置安全等，遍及軟體與硬體層面。於此課程中，由卡內基美隆大學資訊網路學院副教授 Aleecia M. McDonald 指導，完成「網站暫存檔與同意使用說明之量化」（Quantifying Cookies and Consent）研究。研究成果顯示，相較於愛爾蘭等歐盟體系國家，美國等非歐盟體系國家，落實歐盟訂定之「一般資料保護規範」（General Data Protection Regulation，GDPR）之徵求使用網站訪客的地理位置、廣告識別碼、並告知使用者蒐集資料的目的、資料保存的期限等資訊比例較低。另外，提供使用者客製化之資訊運用選項較少。

（九）網路鑑識(Network Forensics)

此課程包括網路層面鑑識應用，包含網路封包與網路協定分析、入侵偵測系統記錄應用、資訊網路設備之紀錄同步與對照分析、無線網路封包分析與區塊鏈紀錄追查等。期末專題為與組員自行設計駭侵態樣與相關紀錄分析應用。本組使用 Cobalt Strike 工具為主，輔以 Snort 入侵偵測系統客製化規則、主機系統日誌紀錄與 Wireshark 網路流量封包分析。

（十）進階網路架構(Advanced Real-World Data Networks)

本課程以對網路原理的理解為基礎，研究如何在各種實際場景中採用這些原理來解決現代網路工程師面臨的問題。本課程探討現代和新興基礎架構的網路技術設計、實現和應用。主題可能包括，4G、5G 網路基礎架構、IPv6 應用現況、SDN 軟體定義網路、數據中心、網狀網路和嵌入式網路等。期末專題為基於 Multipath TCP 之多路徑路由演算法強化網路連線穩定性（Achieving robustness and performance with MPTCP in a mobile usage scenario）。隨著網路以及設備上多個網路接口的普及，存在多個路徑上劃分網路數據連線。這允許創建在節點之間具有多個數據路徑的混合接入網路，目的是提高影音串流和網路遊戲的可用性。

多路徑 TCP（MPTCP）是一種網路標準，它將連接分為多個 TCP 子流，以通過不同的路徑發送。以模擬器 ns-3 中建立仿真的網路環境，以模

擬具有 4G LTE 和 WiFi 的設備使用狀況，並新增兩個強化演算法，包含循環制演算法和 OTIAS（Out-of-order Transmission for In Order Arrival Scheduler），我們比較了各種演算法對應用程式的延遲影響，發現循環制演算法和最短的路程時間演算法（RTT）具有低延遲的優點。

（十一）資安事件應變處置(Cyber Forensics Capstone)

這堂課程透過實際案例教學研析。課程內容包含釣魚郵件追查研析、智慧型手機鑑識、依時間證物重建資安事件、反鑑識技術、人工智慧運用於惡意程式分析與資安事件查察等。透過既有的事件關聯分析和重建技術，找出資安事件脈絡，並模擬調查過程中的取證方法，提出完整報告。課程中包含數項作業：

a. 開源工具使用與分析：在網路取證和事件回應中，分析人員經常遇到需要研究或創新才能解決的新問題或陌生問題。所以，分析人員需要能夠在各種已知或未知的情況出現時適應並增加他們的技能。在這項作業中，選擇並研究 1 項開源取證工具，並將其設置在測試環境中，以了解該工具的作用。

b. 時間軸分析並還原現場：此作業擷取映像檔中所有事件的日誌紀錄檔，學生使用時間線分析技術來構建與事件相關的時間軸，並在無線索情況下，使用演繹推理來解釋所發生的事件。

c. 手機數位鑑識：提供來自多個 Android 手機的映像檔案，從這些設備中收集取證物，反證手機使用者是否有將公司機敏資料洩漏出去。

d. 反鑑識技術：情境假設犯罪嫌疑人具有顯著的資安技術能力，目前被一家高科技創業公司聘為系統工程師。深諳毒品是違法的，故運用隱碼術，將毒品資訊隱藏於各類檔案中，如果鑑識人員無法以反鑑識技術找到證物，嫌疑犯可能很快會被釋放，本次作業提供一個 USB 映像檔案，試圖於此檔案中，找到毒品相關交易資訊。

另有期末專題，題目情境假想為在過去的幾個月中，聯邦代理商一直在監視一間公司 Corpservices.io 的業務活動，強烈懷疑該公司與惡名昭彰的 U3 犯罪集團有聯繫。然而到目前為止，沒有任何證據可以證明兩者之間關係，為破獲此犯罪集團，近幾個星期，密切監視一個由 Corpservices 的偏遠倉庫狀況，在倉庫附近發現了兩位 Corpservices 人員，在該區域徘徊了 20 分鐘後離開，卻沒有與 Corpservices 進行任何明顯接觸。但是觀察到這行徑不久後，Corpservices 便失聯，鑑識人員懷疑這兩人跟 U3 犯罪集團相關，故取得搜索令後，對倉庫內的兩台電腦進行鑑識，此電腦硬碟的映像檔為 50TB，此專題為運用課程所學，對硬碟映像內的檔案逐一分析，找出兩者的關聯性。

（十二）資安新創與企業創新(Enterprise Innovation)

本課程重點為介紹公司在應對數位轉型、新興技術和競爭商業環境方面當前面臨的創新與挑戰。課程內容將專注於資訊長（CIO），數位長（CDO）和技術長（CTO）的管理與創新，從各個從事於企業風險投資機構的講者介紹實務現況。

課程主講教授為 Stuart Evans，過去 30 年在矽谷進行「超柔性」創新概念實務概念研究，並擔任阿聯酋航空-CMU 創新實驗室主任。其研究集中於企業如何開發創新戰略的靈活投資組合，以推動安全性並避免潛在威脅。期末專題報告為結合阿聯酋航空現況，以通訊軟體及社交軟體，開創其市場發展規劃。

肆、心得與建議

首先，由衷感謝各級長官的支持與協助，給職此次出國進修的機會，就讀以電腦及資訊等相關研究領域聞名國際的卡內基美隆大學，該學校在學習環境方面，校園內多處提供學生自習環境，各系所於中午不定時舉辦學術研討會，並歡迎在校師生參與。在課程規劃方面，學校碩士班旨在培育資訊安全的研究人才，然而此領域涵蓋範圍相當多元，學生必須要瞭解除了軟體與硬體領域的安全知識外，還需橫跨韌體、行動裝置、區塊鏈等不同的領域，實屬一門相當多元且需要整合能力的學科。

學校多元發展的概念，與我國資通電軍之編制相符，人員依據不同的專精領域，分成攻擊、防禦、情蒐與鑑識，使得資通電軍在精進不同領域的資安專業能量上持續茁壯滋長。職期許個人在經過國外學習後，能夠貢獻所學，於資通電軍未來跨領域整合上能站穩腳步，向前邁出創新的穩健步伐。另學程為美國雙岸合併學程，意即一年在東岸，賓系尼亞州之校本部；第二年在西岸，矽谷校區，旨在使學生同時接受充沛的學術與業界資源，以及應用所學，與實際產業發展現況接軌。

再次感謝國防部提供這次寶貴的赴美進修機會，除了修習相當多資訊安全領域課程，亦接觸不少實務上的訓練，更重要的是能體驗多元的文化，藉以增進外語、文化、國際觀、創造力、人際網路等能力；卡內基美隆大學電腦科學與資訊安全領域為國際進修學位首選之一，其紮實的教育訓練、多元的課程設計及豐富的學研資源，都相當值得我國借鏡，在美國，學生赴企業實習已行之多年，此亦為學生畢業後尋求正職工作之有效管道，反觀我國目前的教育制度，多著重於理論方面的知識，建議應鼓勵國內企業積極參與教育創新，藉由產官學教研共同合作以推動創新的教育模式，讓學生能學以致用並適才適所。人才培育決定國家未來，目前各國人才爭奪戰已開打，但該如何引才、留才、育才已成重要議題，我國應更積極思考如何針對在學、在職、在營等不同階段，培育所需各類人才。