出國報告（出國類別：研究）

108 年度行政院選送公務人員出國專題研究「政府資安治理模式」報告

服務機關：行政院資通安全處
姓名職稱：周智禾 科長
派赴國家：美國(維吉尼亞州費爾法克斯、加州舊金山)
出國期間：108 年 5 月 3 日至 108 年 7 月 31 日
報告日期：108 年 10 月 14 日

摘　　要

我國自 103 年起，參考國內 CNS、國際 ISO 及美國 NIST 等標準，建立資安治理架構 4 大面向與 18 個流程構面，發展國內政府機關資安防護能力指標與分析，並推動資安治理制度成熟度自評；惟目前推動上仍有部分困難點，包括如何明確定義資安治理各評核問項之內涵及確保評核結果之一致性，釐清資安治理所訂面向與流程間相互關係，可否研析設定各面向權重之可行性，不同政府機關是否應訂定其優先實作流程項目等項，前揭相關問題期可透過本次出國專題研究，瞭解先進國家目前作法及相關實務經驗。

本次出國研究擇定美國喬治梅森大學(George Mason University, GMU)，研究主題為「政府資安治理模式」，與資訊科技及公共政策具高度關聯性，期藉此短期專題研究期間，瞭解美國對資安治理、政策及法規之相關研究及實務，並透過交流互動方式，持續精進我國資安體制。

目　　錄

壹、目的

藉由本次出國專題研究，透過相關經驗分享及實務交流，持續精進我國資安治理制度，針對目前所訂面向與流程構面，精簡相關內容，讓各機關人員能以更客觀方式填報相關問項，後續可針對機關弱項提供協助，提升整體制度實質效益，並有效分配資源與訂定政策方向。

為建構國家資安聯防體系，提升整體資安防護機制，強化資安自主產業發展，以保衛數位國土安全，行政院訂定「國家資通安全發展方案(106 年至 109 年)」，該方案擬具 4 項推動策略，分別從「完備資安基礎環境」、「建構國家資安聯防體系」、「推升資安產業自主能量」及「孕育優質資安菁英人才」等面向著手，逐步推動我國資安縱深防禦及聯防體系，打造安全可信賴的數位國家。

其中，推動策略「完備資安基礎環境」下之具體措施「建立政府資安治理模式」，主要係建立國家層級資安風險管理機制及推動政府機關導入資安治理制度，期透過公正的第三方評審，引導各機關強化資安治理作為，朝制度化型(Established)、可預測型(Predictable)，甚至是創新型(Innovating)組織邁進，規劃於 109 年推動資安責任等級 A、B 級政府機關資安治理成熟度達第 3 級(含以上)，以健全整體政府機關之資安體質。

貳、過程及重點議題

一、過程

本次出國專題研究於本(108)年 5 月 3 日抵達美國喬治梅森大學(George Mason University, GMU)，除校園腹地廣大外，最令人印象深刻是綠意盎然的環境(如圖 1)，由於正值春季課程結束，校內學生均忙著準備期末考試。

圖 1：GMU 校園

此外，當行走於校園內，最吸引人的是隨處可見到擁有 6 個輪子的無人小車(如圖 2)，此為愛沙尼亞新創事業星艦科技(Starship Technologies)所研發的星艦快遞機器人(Starship Delivery Robot)，相較於近年國際大廠紛紛推動無人機送貨，星艦科技認為無人車送貨的

安全性及可行性更高，因此從 2015 年開始積極測試運作，其特點為具防水功能，可在雨中或雪中行駛，時速與行人速度相同，使用人工智慧、超音波感應器及攝影機等來進行導航，收貨者必須透過手機行動 APP 所收到密碼開啟，後端亦有人員進行監控，可於必要時介入操作，或於意外發生時即時處理。

GMU 於 2019 年 1 月 22 日開始與星艦科技合作引入 25 部無人小車，用來提供送餐服務，同時 GMU 也是全美第一個導入無人小車的學校，校內職員及學生可以於上午 9 時至下午 8 時間，透過手機 APP 點餐(Blaze Pizza, Second Stop, Dunkin' Donuts 或 Starbucks 等)，並支付 1.99 美金的運送費，即可於 15 分鐘內收到食物(每次運送最多 20 磅，且具有保溫及保冰功能)。

比較有趣的是根據調查結果，有 88%的大學學生會忽略早餐，一般的原因通常是沒時間，在 GMU 引入無人小車第一天運作時，大量的晚餐訂單讓無人小車疲於奔命，然而經過 2 個月後，已經接到超過 1,500 筆早餐的訂單，其數量已經取代晚餐的訂單，這項服務也影響了學生用餐的習慣。此外，這些無人小車也為學校提供了有價值的資訊，它可以顯示學生吃飯的時間，食物的種類及飲食規劃的使用方式，這也可能會使大學為學生所提供的餐飲服務方式產生變化。

圖 2：GMU 校園內的星艦快遞機器人

依指導教授 Auffret, Jean-Pierre (the director of the Research Partnerships and Grants Initiatives in the School of Business and associate director of the Center for Assurance Research and

Engineering in the Volgenau School of Engineering at George Mason University)安排於 5 月 8 日辦理報到手續，自 5 月 9 日開始研讀指導教授所提供之各國 Cybersecurity 策略相關文件，並不定期安排會議參與討論，詳細議程詳見表 1，研究室位置如圖 3。

表1　議程

日期	與會者及主題	參考資料
5/9	Meeting with German Perilla (Director of Honey Bee Initiative, School of Business and College of Science) for the topic of Honey Bee Initiative	https://bees.gmu.edu/
5/14	Meeting with Jo Ann Henson (the business and economics librarian at Mason) for the topic of library resource	https://library.gmu.edu/
5/17	Meeting with Dave Jordan (Vice President, Mission Security and former CISO, Arlington County, Virginia)	https://www.missionsecure.com/
5/20	Meeting with Jeff Matsuura (Attorney, Alliance Law Group) for the topic of technology law and intellectual property rights	https://alliancelawgroup.com/jeffrey-h-matsuura/
5/22	Meeting with Kerry Bolognese (Director, Federal Government Relations, George Mason) for the topic of the US government	✓https://relations.gmu.edu/contact-us/kerry-bolognese/ ✓https://www.fda.gov/medical-devices/digital-health/cybersecurity
5/22	Meeting with Dan Fleck (Research Associate Professor, Computer Science, George Mason and Penn State) for the topic of DDoS and medical devices	✓https://ieeexplore.ieee.org/document/7433335 ✓https://www.altrixmedical.com/
5/23	Meeting with Christopher D Magee (MS MLIS, Social Sciences Librarian, George Mason University Libraries)	https://www.zotero.org/
5/24	Meeting with David Bulova (a member of the Virginia House of Delegates)	http://www.davidbulova.com/
5/28	Meeting with Joey Hutcherson (the U.S. Data.gov and open data programs)	✓https://www.opengovpartnership.org/about/about-ogp ✓https://www.opengovpartnership.org/participants ✓https://www.data.gov/

日期	與會者及主題	參考資料
		✓https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/us_open_data_action_plan.pdf ✓https://project-open-data.cio.gov/ ✓https://www.ctg.albany.edu/media/pubs/pdfs/USopendatapolicy.pdf
5/31	Meeting with Marilyn Smith (Vice President and CIO, and Curtis McNay, Director, IT Security George Mason)	https://its.gmu.edu/about-its/strategic-plan/ https://its.gmu.edu/member/marilyn-t-smith/ https://its.gmu.edu/
6/3	Meeting with Duminda Wijestera (Professor Computer Science, George Mason)	https://volgenau.gmu.edu/profile/view/13535
6/5	Duminda Wijestera, Professor Computer Science, George Mason	https://volgenau.gmu.edu/profile/view/13535
6/5	Joy Suh, George Mason Library	https://dsc.gmu.edu/gis/
6/5	Meeing with Prof. J.P. and Serge to sharing my thesis and dissertation about cryptography.	
6/6	Meeting with Falahyar Fatmi (Falahyar Fatmi is the Chief Information Officer at Air Force Association. Falahyar provides leadership for the continued development of an innovative, robust, and secure information technology environment throughout the Air Force Association. The primary responsibilities for this office encompass a wide variety of strategic technology issues: governance and policy, resource allocation, IT protocols, and the Air Force Association Information Technology organization. IT provides support for field operations and technology, delivery of IT infrastructure and services, information security systems and compliance, administrative systems, and client support services. Falahyar spent 20 years in IT roles in both For-Profit and Non-Profit sector.	https://www.afa.org/

日期	與會者及主題	參考資料
	Falahyar holds two Masters in Technology Management and Information Systems from George Mason University.)	
6/6	Meeting with Christine Pommerening (Professor in the Political Science department at George Mason University)	
6/6	Meeting with Rich Kauzlarich (Distinguished Visiting Professor at the Schar School of Policy and Government at George Mason University)	https://schar.gmu.edu/about/faculty-directory/richard-kauzlarich
6/7	Meeting with Kevin Yin (Chief Executive Officer, Sitscape Inc)	✓https://www.sitscape.com/homepage/ ✓https://www.sitscape.com/homepage/leadership/
6/17	Meeting with Joseph Nolan (Principal, Multi-Discipline Systems Engineer at MITRE Corporation)	✓https://www.linkedin.com/in/joseph-nolan-256a4110 ✓https://www.csiac.org/
6/19	Participating GMU Cybersecurity Innovation Forum	✓https://www.eventbrite.com/e/3rd-2019-george-mason-university-cybersecurity-innovation-forum-registration-53960625684
6/20	Meeting with Linton Wells II (Executive Advisor for the C4I & Cyber Center)	✓https://c4i.gmu.edu/2016/02/3604/ ✓https://inss.ndu.edu/Media/Biographies/Article-View/Article/977343/linton-wells-ii/
6/25	Meeting with Sebrina Blake [Chief Information Officer (CIO) Administration for Children and Families (ACF) U.S. Department of Health and Human Services (HHS)]	✓https://www.acf.hhs.gov/about/leadership/sebrina-blake

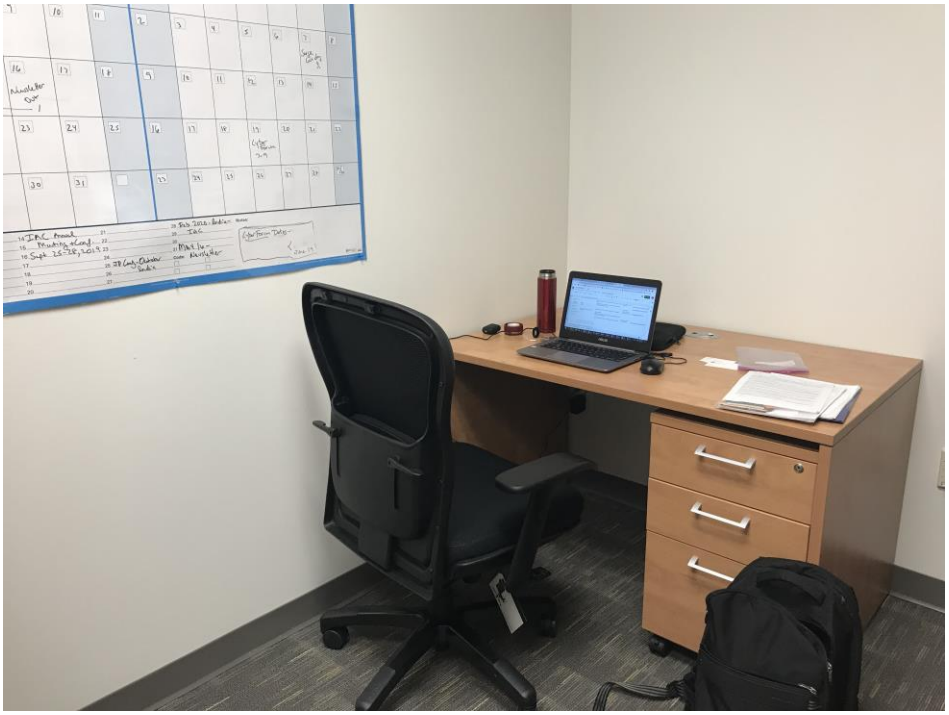

圖 3：研究室位置

續於 6 月 28 日搭機至美國加州舊金山，原訂安排參訪北加州地區情報中心(Northern California Regional Intelligence Center)及相關組織機構，惟經多次聯繫未果；期間，指導教授 Auffret, Jean-Pierre 亦協助聯繫灣區及矽谷多間政府機關及新創公司，於該處進行資料蒐整與研究，並至 Google 舊金山公司參訪數次，了解其工作內容及型態。

二、重點議題

(一) DDoS and medical devices

阻斷服務攻擊(Denial of Service, DoS)目的在於使目標電腦的網路或系統資源耗盡，使服務暫時中斷或停止，導致目標用戶無法正常使用。而分散式阻斷服務攻擊(Distributed Denial of Service, DDoS)即為 DoS 的延伸，透過 2 個或 2 個以上電腦對外進行攻擊行為，致使目標電腦無法正常運作，即稱之為 DDoS。由於 DDoS 需使用資源較大，因此通常伴隨操控僵屍網路(botnet)進行攻擊，近年來 DDoS 攻擊越來越嚴重，不管是攻擊流量或是手法複雜度都日益提升，而我國亦面臨類此威脅，為能有效強化我國政府機關 DDoS 防

護能量，爰於 105 年訂定「政府機關分散式阻斷服務防禦與應變作業程序」，提供各機關參考運用，該程序書綜整政府機關層級應變防護機制，並供資訊人員進行相關資訊設備防護設定之參考，期望機關依內部設備與資源，發展 DDoS 攻擊之防禦與應變作業程序，當機關遭受 DDoS 攻擊時，資訊人員能參考適當的應變處置措施，儘速減緩 DDoS 攻擊影響，使資訊設備或服務能儘速恢復正常營運。

GMU 的 Dan Fleck 教授向我們介紹他們所提出一種使用雲端架構的 DDoS 防禦機制(Cloud-Enabled DDoS Defense)，其方式為基於雲端架構，使用伺服器自動複製及智慧型使用者分流等方式，將攻擊流量集中至某一(或多)部伺服器上，並使用其所提出的 shuffling 技術為受攻擊伺服器上的使用者計算出最佳重新分配策略，系統會不斷變更受攻擊的伺服器，以有效地將正常的使用者從攻擊者中區分開來(如圖 4)，而不需要瞭解攻擊者所使用的攻擊手法為何(因攻擊手法日新月異，在實務上相當難逐一辨識出來，只需要知道伺服器回應變慢，可能就表示遭到 DDoS 攻擊)，針對在系統運作期間，他們提出相關演算法將 client-to-server 重新分配機制進行最佳化，期望能有效減少 shuffle 的次數，以在最短時間內減緩 DDoS 攻擊，其方法已在 Amazon EC2 上實作並完成概念驗證，目前刻正於 GMU 進行導入。

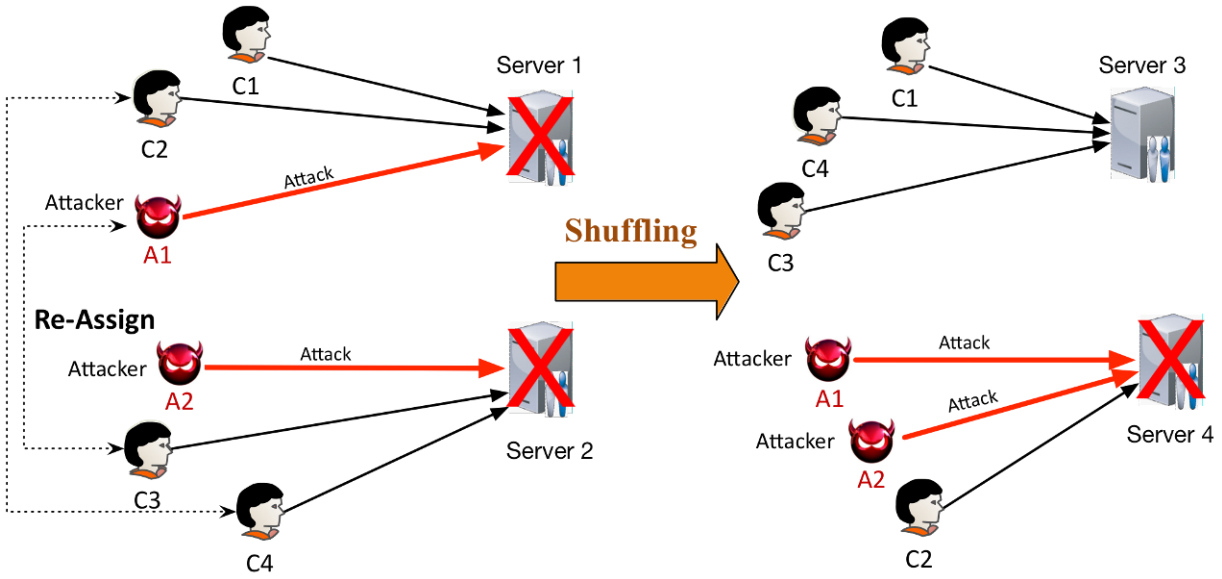

圖 4：client-to-server shuffling 範例

(二) AltrixMedical

Dan Fleck 教授同時也任職於 AltrixMedical 公司，並說明該公司研發提供 2 款醫療用的實用工具，分述如下：

1、 NaloxoFind：在美國每天有 175 人死於鴉片類藥物服用過量(Opioid Overdoses)，而有部分原因是因為無法即時使用納洛酮(Naloxone)，因此開發 NaloxoFind 這款行動應用程式(APP)，允許任何人在 2 英里範圍內識別和定位哪裡有可用的納洛酮，並與攜帶這種救命藥物的人直接溝通。這個免費的 APP 允許第一個回應者及好撒馬利亞人(Good Samaritan)註冊為納洛酮攜帶者，使其在緊急情況下可由 NaloxoFind 的 APP 用戶聯繫。

2、 Smartphone AED：自動體外心臟去顫器(Automated External Defibrillator, AED)為一種攜帶型的醫療設備，主要自動診斷特定的心律不整(非針對心臟停止跳動的狀況)並給予心臟電擊，專門用來針對瀕臨猝死的病患進行急救，使用時機為突發性心臟停止跳動患者搭配心肺復甦術(CPR)使用，目前國內多數公共場所(如機場或車站)均有配置。但假如發生地點找不到 AED、距離太遠或是附近剛好沒有 AED，於是該公司研發一種可與智慧型手機整合的 AED(如圖 5)，主要著眼點為現代人手機不離身的特性，於發生意外時可進行即時現場診斷和治療，該產品的特性如下：

(1) 比一般智慧型手機稍大

(2) 可設定向緊急救援服務進行自動撥號或發送簡訊，讓救護人員能儘速抵達現場

(3) 提供全功能的遠距醫療

(4) 支援多種語言的操作介面

(5) 能夠傳送所在的 GPS 地理位置給救護人員

圖 5：Smartphone AED

(三)文獻管理軟體(Zotero)

為利蒐集及管理相關參考文獻，GMU 圖書館員(Christopher D Magee)介紹文獻管理軟體(Zotero)，該軟體可至 https://www.zotero.org/網站下載，其為開源的免費軟體，主要針對撰寫論文時，可用該工具來管理參考文獻及其相關資訊(如分類、摘要、作者、標題、出版社、年份、頁數等)，並可製作筆記(Note)及標籤(Tag)便於管理及搜尋，其軟體介面如圖 6。

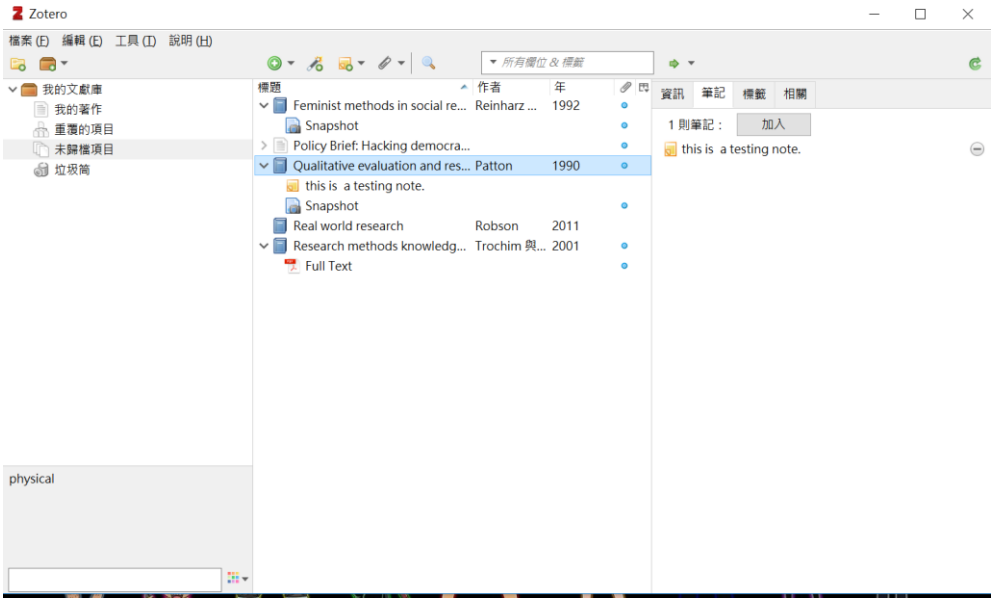

圖 6：Zotero 軟體介面

此外，Zotero 亦提供 Connector 可以整合於瀏覽器，目前支援 Chrome、Safari 及 Firefox，Zotero 可以自動偵測所瀏覽的網頁內容，只要簡單點擊一下即可儲存網頁快照(Snapshots)及相關資訊，如果網頁包含 PDF 檔亦會一併下載，不管是在 arXiv.org 搜尋預印本(Preprint)、在 JSTOR 搜尋期刊文章(Journal)或在 New York Times 搜尋新聞，Zotero 已經支援上千個網站。例如在 scholar.google.com 搜尋 cyber security 相關文章，約有 681,000 筆結果，每頁列出 10 筆，點選瀏覽器右上角的 Zotero Connector，出現 Zotero Item Selector 視窗，使用者即可以選擇所要下載的文章，如圖 7。

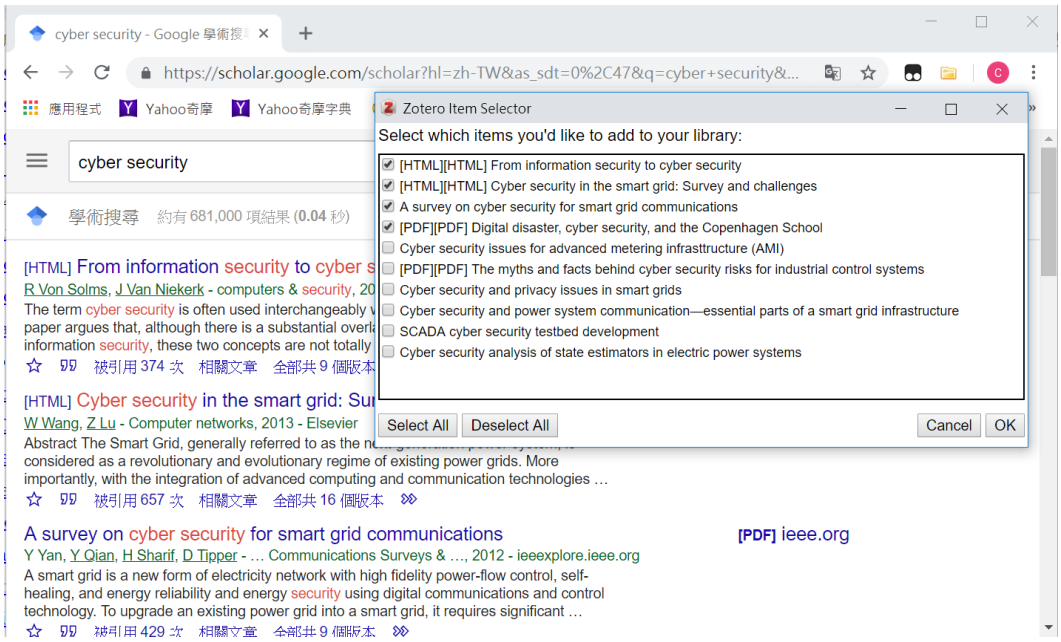

圖 7：瀏覽器使用 Zotero Connector 下載文章

最後，Zotero 提供外掛程式可整合至文書處理軟體，目前支援 Microsoft Word 及 LibreOffice，當使用者在撰寫文章時，如需要引用其他期刊論文時，可使用 Zotero 外掛程式產生文內引用、腳註或文章最後的參考文獻(bibliographies)，其支援共 9,390 種期刊論文參考文獻引用樣式，如圖 8。

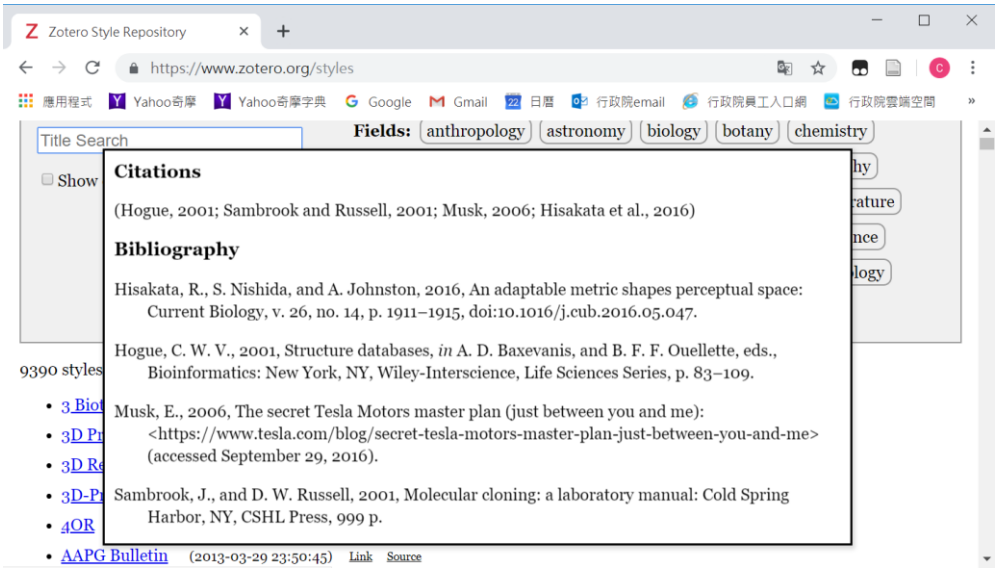

圖 8：Zotero 支援共 9,390 種期刊論文參考文獻引用樣式

(四)維吉尼亞州法規現況

首先參考美國國務院出版的「How the United States is Governed」(https://web-archive-2017.ait.org.tw/infousa/zhtw/PUBS/AmGov/overview.htm)，美國政府體制為憲政聯邦共和制(Constitutional Federal Republic)，憲政(Constitution)指美國政府為建立在美利堅合眾國憲法(1789 年)的基礎上，並透過憲法創立三權分立，即立法(Legislative)、行政(Executive)及司法(Judicial)的相互制衡體制，而聯邦(Federal)表示美國是由全國政府及 50 個州政府所組成，最後，共和制(Republic)則說明人民掌握根本權力，並由人民選出的代表協助執政；我們可以簡單將美國分為三個部分，即聯邦政府(Federal government)、州政府(State government)及地方政府(Local government)，以下簡單說明重點：

1、聯邦政府：主要負責州際貿易、國防、貨幣、移民等，並與州政府合作推動相關規定，聯邦政府可分為立法、行政及司法等三部分，由憲法賦予其職權，簡述如下：

(1) 立法：由參議院(The Senate)及眾議院(The House of Representatives)組成國會

(Congress)，主要負責制訂及審查所有的法案，包括起草、聽證、審定及投票等過程，經參、眾兩院通過後，由總統簽字方可生效。除前揭立法外，國會亦負責監督行政部門，可透過聽證會調查行政部門的運作。

上開的參議院亦稱為上院(Upper Chamber)，比起眾議院擁有較高的審議權，副總統為參議院主席，其成員為每州經選舉產生 2 名議員，共計 100 位議員，任期為 6 年，其職權與眾議院不同在於，參議院負責批准總統提名的大法官、法官及內閣人選，可否決總統所簽署的國際條約等。眾議院則按聯邦所轄各州的人口數目比例分配，但保障每州至少一人，總計為 435 人，任期為 2 年，也只有該院具有提出彈劾的權力。

(2) 行政：總統為行政機構最高領導，由全國人民選舉方式產生，但比較不一樣的是總統選舉結果取決於選舉人票數，而非人民選票，選舉人票數相當於該州參議員及眾議員的人數總和(535 票加上首都哥倫比亞特區 3 票，共 538 票)，即贏得一個州多數人民選票的候選人可囊括該州的所有選舉人票數，最後由贏得最多選舉人票的候選人當選總統。總統的權力包括任命最高法院(The supreme court)大法官及下級聯邦法院法官，任命行政部門及機構的首長，發佈行政命令(Executive order)等。

前揭行政部門及機構包括國務院(Department of State)、財政部(Department of the Treasury)、國防部(Department of Defense)、司法部(Department of Justice)、內政部(Department of the Interior)、農業部(Department of Agriculture)、商務部(Department of Commerce)、勞工部(Department of Labor)、衛生與公眾服務部(Department of Health and Human Services)、住房及城市發展部(Department of Housing and Urban Development)、運輸部(Department of Transportation)、能源部(Department of Energy)、教育部(Department of Education)、退伍軍人事務部(Department of Veterans Affairs)、國土安全部(Department of Homeland Security)，除了上述 15 個部之外，尚有許多獨立的機構跟委員會。

(3) 司法：負責憲法、聯邦法律、條約、外交等案件及州際間訴訟等，其組成包含一個最高法院(The Supreme Court)和多個下級法院，下級法院包括 13 個上訴法院(Courts of Appeal)負責裁定聯邦司法管轄區對地區法院判決的上訴、94 個聯邦地區法院(Federal District Courts)負責初審各州的民事及刑事案件，為確保司法獨立，憲法明文規定聯邦法官為終身職，且其薪水於任職期間不得削減。

2、州政府：美國第一級行政區劃為州，擁有相當的自主權，美國從一開始最早的 13 個州，到目前為 50 個州，另外還有一個哥倫比亞特區(District of Columbia)不屬於任何一州，其為美國的首都，也就是大家所熟知的華盛頓 DC 特區。州政府與聯邦政府體系類似，擁有立法、行政及司法，但並非隸屬於聯邦政府，簡單說明如下：

(1) 立法：立法機構的州議員係透過選舉方式產生，任期多為 2 至 4 年，負責制定州法律、批准州預算及監督行政體系運作等，大多數州的立法機構與聯邦政府一樣由兩院組成，上院為參議院，下院則可能稱為眾議院(House of Representatives)、代表院(House of Delegates)或州立法大會(State Assembly)，在較具規模的州，其州議員為全職工作，其餘多為兼職性質，每年僅工作數週以進行立法議事。

(2) 行政：負責州內的各項公眾教育、交通運輸、公共安全、健康醫療、選舉等與民眾相關之服務，各州擁有一位經選舉產生的行政首長稱為州長，任期為 2 至 4 年。

(3) 司法：負責各項違反州或地方法律之民事及刑事案件，以及違反州憲法的案子，各州擁有相當的司法自主權，州政府有自己的憲法及法律，但前提是不能凌駕於聯邦政府及美國憲法，其州憲法亦不得超過國家整體主權。州內設有最高法院(State Supreme Court)或稱上訴法院(Court of Appeals)，但其法官並非終身職。

3、 地方政府：各州地方政府的層級、名稱、職權等依其各州憲法規定有所不同，通常根據各州的憲法，會將州內劃分成不同的行政區，一般會下設郡(或稱縣，County)或同等地位的行政區(County-equivalent)，負責登記註冊、選舉、公共建設及治安等，而郡通常會下設鎮區，另外尚有擁有自身行政和稅收權的市、鎮、村，稱為自治行政體

(municipality)，以及不屬於任何地方政府的特區政府(special district government)。

在 5 月 24 日與維吉尼亞州眾議院(Virginia House of Delegates)的議員 David Bulova 會面，維吉尼亞州於每兩年期的預算年度期間，議會通常開議維期 15 天，眾議院議員每年因其服務獲得 17,640 美金的薪資，因此，對大多數議員來說，擔任議員並非個全職工作，而議員必須每兩年在行政區內競選連任。David Bulova 為維吉尼亞州第 37 行政區(GMU 位於該行政區)的代表，其本職工作為擔任 Wood Environment & Infrastructure Solutions, Inc.的專案經理，致力於協助政府和企業遵守聯邦及州的環境相關法規。

於本次會面期間，David Bulova 討論到維吉尼亞州相關法規環境，包括目前刻正討論有關教育制度的發展，係要以考試來評鑑學生能力，抑或注重在學的技能培養；針對汽車駕駛人尚無禁止使用手機的規範；選舉改採電子方式進行；以及針對無人機的安全，目前無相關法規規範。針對討論內容除進行簡單的意見交換外，亦分享我國於 107 年修正民用航空法(如圖 9)，將無人機的管理法規納入至該法第 99 條，並依其飛行高度劃分權責，四百呎以上由中央負責，四百呎以下歸地方管轄。

收件者: Jean-Pierre Auffret <jauffret@gmu.edu>;
副本:

Dear Prof. JP

It's very nice to meeting with Davide Bulova. (http://www.davidbulova.com/)
There are many interesting talk about education, legislation, election, and etc.
And, I mentioned that Taiwan had related rules to restrict the drones.
Sorry, I remember the wrong number.
The correct one is 400 feet instead of 600 meters.
We amended the Civil Aviation Act on April 25 2018.
The Chapter 9-2 applied to the activities of drone in the open space outside of the buildings.
Articles 99-9 through 99-19 are detailed, and you can see that on the below website.
https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=K0090001
I abstract the content from Article 99-13 as follows:
Central government (Civil Aeronautics Administration, MOTC) is responsible for the drones above the height of 400 feet.
On the other hand, Local government is responsible for the drones under the height of 400 feet.

By the way, Taiwan proposed the draft on articles of "Regulations of Drones"recently.
But it seems to be under the legislative process.
You can see the detail on the website. (https://www.caa.gov.tw/Article.aspx?a=2292&lang=1)
Unfortunately, it is only available in Chinese currently.

May I ask you for helping me send the above content to David?
Thanks and best regards,

圖 9：分享我國民用航空法針對無人機管理之規定

(五)開放政府資料(Open Government Data)

由美國商務部(the United States Department of Commerce)退休官員 Joey Hutcherson 說明美國開放政府資料(Open Government Data)，緣起於 2017 年 12 月，30 名開放政府的提倡者於加州 Sebastopol 共同研擬了開放政府資料的 8 項原則，主要強調使用技術方式讓所有資料可用(Available)，但隨後面臨的是可用的資料不一定是有用(Usable)的資料，而只強調技術解決方式應為多加考量終端使用者的立場，因此成立跨機關工作小組來解決此問題，將短期目標訂為公私部門合作，並徵詢公私部門共同訂定長期目標。

2009 年 12 月，美國行政管理和預算局(Office of Management and Budget)發布一項開放政府指令(M-10-06)，要求執行部門和機構採取具體行動，納入總統於 2009 年 1 月 21 日提出的透明度(Transparency)、參與(Participation)和合作(Collaboration)等原則；有關資料公開部分，應該在法律允許的範圍內盡可能公開，並滿足隱私、機密、國家安全及其他等限制。

- ✓透明度(Transparency)：透過向民眾公開政府正在做什麼以推動可歸責性(Accountability)。
- ✓參與(Participation)：讓民眾貢獻想法及專業知識，以便政府可以參考社會大眾的想法來制定政策。
- ✓合作(Collaboration)：通過鼓勵與聯邦政府、跨政府機關、民間組織和民眾之間的伙伴關係和合作，提高政府的效率。

在 2019 年 1 月 15 日，美國總統川普簽署開放政府資料法(Open Government Data Act)，該法通過後，將促使美國聯邦政府開放政府資料將更加順暢，並能設立資料長(Chief Data Officers, CDO)，後續美國聯邦政府所開放的所有非敏感資料必須預設為機器可讀格式(machine-readable formats)。

美國於 1967 年所頒布之資訊自由法(Freedom of Information Act, FOIA)，旨在規定民眾

獲得行政情報方面的權利，以及政府機關在向民眾提供行政情報方面的義務；而 FOIAonline 為處理及發布 FOIA 請求及回應的集中點，提供多機關(multi-agency)的 FOIA 處理及追蹤工具，允許讓民眾可以線上提出 FOIA 請求，該系統為免費平臺，民眾僅需註冊後，即可於 FOIAonline 網站上提出請求，查詢之前公布之紀錄、產出報告以及自動以電子郵件收取紀錄，並可直接聯繫相關機關，收到任何查詢狀態的異動通知等，

(五) 國家網路戰略(National Cyber Strategy)

2018 年 9 月美國川普總統公布「國家網路戰略(National Cyber Strategy)」， 針對網路將採取主動方式，確保對手明確知道如進行駭客攻擊、網路入侵及任何其它形式的攻擊行動需付出代價，川普總統表示美國行政當局將採取一切手段保護美國不受網路威脅，新戰略為美國政府保護各部門網路資料，以及美國民眾隱私的最佳方向。

美國國家網路戰略實現國家網路安全，包括 4 大構面(Pillar)、10 項目標(Objective)及 42 項具體措施(Priority Actions)，其架構圖如圖 10，各構面之目標、重點及具體措施如表 2。

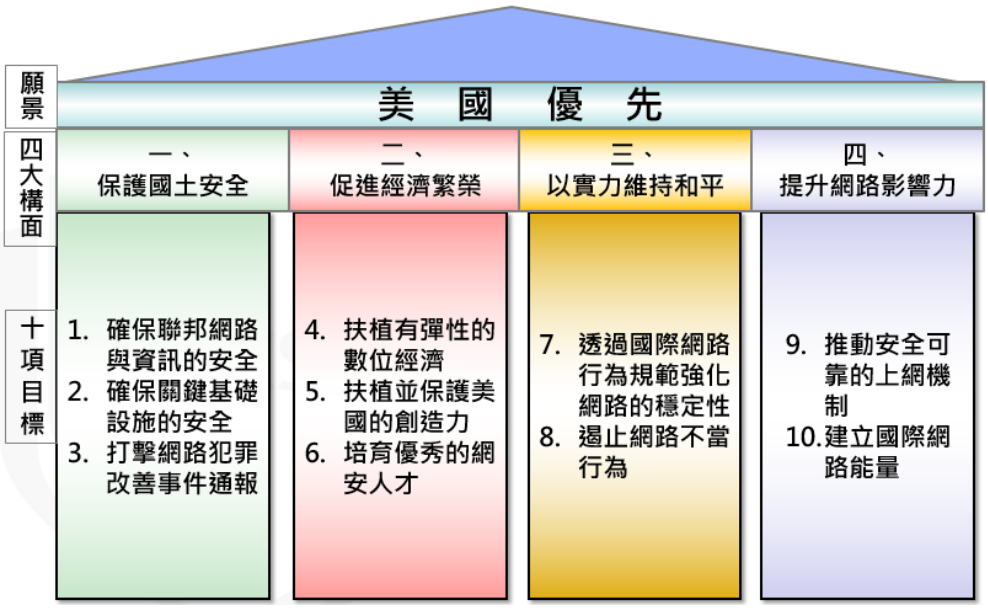

圖 10：美國國家網路戰略架構圖

表 2：美國國家網路戰略之構面、目標、重點及具體措施

構面	目標	重點	具體措施
一、保護國土安全	1、確保聯邦網路與資訊的安全 (Secure Federal Networks and Information)	✓ 保護聯邦網路的安全（包括聯邦資訊系統與國家安全系統） ✓ 釐清各部門與跨部門資訊系統 ✓ 確保聯邦政府的安全制定網路安全風險管理標準 ✓ 聯邦將採集中式管理，強化跨部門的合作，並改善供應鏈的管理 ✓ 加強美國政府承包商系統的安全	1、採取集中管理，以確保聯邦網路安全 2、風險管理與資訊技術活動 3、提高聯邦供應鏈風險管理 4、加強聯邦承包商網路安全 5、確保政府領導與創新實踐
	2、確保關鍵基礎設施的安全 (Secure Critical Infrastructure)	✓ 政府與民營企業都有對國家關鍵基礎設施與其網路安全的責任 ✓ 政府與民營企業合作，使用風險管理方法來修正關鍵基礎設施的弱點，提高網路安全 ✓ 確定依事件嚴重性優先處理，以降低關鍵基礎架構可能造成重大損失 ✓ 政府利用起訴和經濟制裁等行動，作為更廣泛的戰略的一部分	6、重新定義美國政府在網路的角色與責任 7、根據國家風險採取的優先行動 8、協調資訊與通信技術提供商及網路安全服務提供者在網路安全的責任 9、保護國家民主發展 10、鼓勵網路安全投資 11、優先投資關鍵基礎設施的研究與開發 12、改善通信傳輸與海運網路安全 13、改善網路空間安全
	3、打擊網路犯罪和改善事件通報 (Combat Cybercrime and Improve Incident Reporting)	✓ 政府將與各地方政府合作，針對國家的網路的威脅與破壞進行檢測、預防及調查 ✓ 執法部門致力逮捕與起訴違法者，打擊跨國網路犯罪活動與經濟間諜活動 ✓ 執法部門將與私人企業合作，阻止對網路犯罪活動	14、通報網路事件並快速回應 15、現代化電子監理電腦犯罪法 16、降低網路跨國犯罪組織的威脅 17、改善對跨國犯罪嫌疑人的接觸 18、強化國家合作夥伴的

			網路執法能力
二、促進經濟繁榮	4、扶植有彈性的數位經濟(Foster a Vibrant and Resilient Digital Economy)	✓ 建立保護經濟安全的標準 ✓ 強化美國市場與創新的活力	19、政府提供先進與安全的技術市場激勵制度 20、網路生態鏈的創新 21、投資次世代網路基礎設施 22、鼓勵資料自由交換 23、維持美國新興技術的領導地位 24、政府促進網路安全產品的生命週期
	5、扶植並保護美國的創造力(Foster and Protect United States Ingenuity)	✓ 培養與保護美國的發明和創新力 ✓ 反對壟斷性併購，並抵制侵犯智財權的行為 ✓ 將鞏固新興技術的領導地位，加強技術的認證，包括人工智慧、量子密碼及次世代電信基礎設施	25、定期更新外國投資與經營的審查機制 26、智慧財產權保護制度 27、保護美國思想的機密與完整性
	6、培育優秀的網安人力(Develop a Superior Cybersecurity Workforce)	✓ 充分應用豐富的人才資源，同時招攬國際最優秀、最聰明的人才	28、建立人才培訓管道 29、增加美國在職人員訓練與教育 30、加強聯邦網安專業人力 31、獎勵公私機構資安人才
三、以實力維持和平	7、透過國際網路行為規範強化網路的穩定性(Enhance Cyber Stability through Norms of Responsible State Behavior)	✓ 美國將在國際法基礎上，建立一個屬於網路空間模式的規範 ✓ 減少惡意網路風險以建立使用者的信心 ✓ 這些規範將成為網路合作應對的基礎，以對抗與該模式不同國家的不負責行為	32、鼓勵全球加入網路規範
	8、遏止網路不當行為(Attribute and Deter Unacceptable Behavior in Cyberspace)	✓ 美國與網路開放的國家達成共識外，對惡意攻擊國家採取報復行動 ✓ 應用所有的國家力量與工具來預防與阻止網路惡意活動，包括外交、資訊、軍	33、鼓勵情資合作 34、及時制止不良後果 35、組織國際網路聯盟 36、處理網路誹謗與假消息

		事（行動與網軍）、財務、情報、公共輿論及執法能力	
四、提升網路影響力	9、推動安全可靠的上網機制 (Promote and Open, Interoperable, Reliable, and Secure Internet)	✓ 美國堅持網路應受到保護，並以開放、可操作、可靠及安全的原則 ✓ 確保開放網路對應的國際標準 ✓ 防止專制國家將網路當作政治威脅，以反恐為藉口，將開放的網路變成的專制制度下的控制工具	38、與網路聯盟國、產業、學術機構進行網路策略合作 39、鼓勵不同利害關係者共同治理網路 40、促進關鍵基礎設施使用可靠的網路 41、促進與維護全球市場的獨創性
	10、建立國際網路能量(Build International Cyber Capacity)	✓ 美國與戰略夥伴建立開放、可操作、可靠及安全的網路安全的共同願景，鼓勵投資與開闢新的經濟市場 ✓ 共享網路威脅信息，更能夠保護國內關鍵基礎設施與全球供應鏈，使政府更加專注網路協定 ✓ 建立合作夥伴網路安全能力，使美國主導的網路主張發揮功效	42、提高建置網路能量

(六) 國防部網路戰略(Department of Defense Cyber Strategy 2018)

美國國防部於 2018 年公布「Department of Defense Cyber Strategy 2018」，該份文件整體策略重點在於向前防禦(Defense Forward)，並針對近年來所面臨的網路威脅，以具體行動來實現國家安全戰略(National Security Strategy)及國家防禦戰略(National Defense Strategy)。

美國的戰略競爭對手刻正展開網路攻擊，用以減弱美國的軍事優勢、威脅基礎設施、降低經濟繁榮，國防部必須透過揭露(expose)、中斷(disrupt)及降低(degrade)威脅美國利益的網路攻擊，強化主要潛在目標的網路安全和復原力(resilience)，以及與其他部門、機構及夥伴密切合作來回應這些網路攻擊。

首先，必須確保美國軍隊在任何領域(包括網路空間)均能對抗並贏得戰爭的能力，這是美國國家安全的基本要求，也是確保我們能阻止對美國、盟友及夥伴進行侵略的關鍵，當然包括使用武力的網路攻擊。國防部必須保護其網絡、系統和資訊以免於遭受惡意網路攻擊，並於接獲指令後，準備好防禦那些國防關鍵基礎設施(Defense Critical Infrastructure, DCI)和國防工業基地(Defense Industrial Base, DIB)之網路及系統，我們將向前防禦(defend forward)以阻止或降低那些針對國防部的網路攻擊，同時也將透過合作模式來強化國防部、DCI 及 DIB 網路和系統的網路安全和復原力。

其次，國防部嘗試先發制人、擊敗或阻止那些可能導致美國關鍵基礎設施發生重大資安事件的的惡意網路活動，無論該事件是否會影響國防部的作戰準備或能力，其在國土防禦任務中的主要角色是透過向前防禦，在威脅尚未碰觸到目標前將它阻擋下來，同時與其他聯邦政府部門和機構協調，向公私部門等合作夥伴提供惡意網路活動的指示和警告(Indications and Warning, I&W)。

第三，國防部將與美國盟友及夥伴共同合作，以強化網路防護能力，擴展聯合網路空間，增加雙向資訊分享，以促進彼此雙方共同利益。

國防部的網路空間防護目標為確保聯合部隊(Joint Force)能完成其在網路空間的任務，強化網路空間作戰能力以提升美國軍事優勢，防護美國關鍵基礎設施免於遭受惡意網路攻擊，提升國防部的資訊及系統之安全性(包括那些存放在非國防部轄管網路的國防部資訊)，擴展國防部與各政府機關、企業及國際夥伴的網路合作。

美國國防部網路戰略是建立在相互強化的方針上，用以建立更致命的力量，在網路空間的對抗及制止，擴大聯盟和夥伴關係，改革部門並培養人才，其戰略方法摘述如下：

1、建立更致命的聯合部隊(Build a more lethal joint force)

(1) 加速發展網路能力(Accelerate cyber capability development)：國防部將加速發展作戰和打擊惡意網路行為者的能力，其重點放在可擴展、適應性強且多樣化的部署能力上，以提供為聯合部隊指揮官最大的靈活度，聯合部隊將能夠在從日常活動到

戰爭時的各種衝突中使用網路空間作戰能力，以促進美國的利益。

(2) 創新以加速敏捷(Innovate to foster agility)：國防部必須進行創新，以跟上網路空間中迅速發展的威脅和技術，將以謹慎方式來接受及管理維運及計畫的風險，從「零缺陷(zero defect)」的文化轉變為促進敏捷性和創新的文化，因為在這領域成功的關鍵在於要比戰略競爭對手更快地創新。

(3) 衡量自動化及資料分析以改善有效性(Leverage automation and data analysis to improve effectiveness)：國防部將使用商業用的網路解決方案，以機器運算速度及巨量資料分析方式來識別不同網路和系統中的惡意活動，將衡量其優點以改善自己的防禦態勢，並確保自身網路能力可持續有效地對抗擁有尖端技術的競爭對手。

(4) 使用網路相關商業現貨(Employ commercial-off-the-shelf [COTS] cyber capabilities)：國防部擅長為特定的維運問題量身訂做網路能力，除此之外，也將大量使用可針對國防部所需功能進行最佳化的商業現貨。

2、在網路空間的對抗及制止(Compete and deter in cyberspace)

(1) 阻斷惡意的網路活動(Deter malicious cyber activities)：美國試圖利用所有國家職權來阻止對手進行那些威脅到美國國家利益、盟友及夥伴的惡意網路空間活動，國防部將優先保護敏感的國防相關訊息，並阻止對美國、盟友或合作夥伴使用武力的惡意網路活動，如果阻止失敗的話，聯合部隊隨時準備利用各種軍事能力作為回應。

(2) 在日常競爭中持續對抗惡意網路活動(Persistently contest malicious cyber activity in day-to-day competition)：國防部將透過向前防禦以攔截和制止網路威脅，並加強支持國防部任務的系統和網路之網路安全，來打擊威脅美國軍事優勢的網路活動，這包括與私部門、外國盟友及夥伴的共同合作，對可能威脅聯合部隊任務和洩露敏感國防訊息的網路活動提出質疑。

(3) 增加美國關鍵基礎設施的復原力(Increase the resilience of U.S. critical infrastructure) ：

國防部針對美國關鍵基礎設施的惡意網路活動，將與其他機構及私部門合作以降低可能帶來災難性或連鎖性後果的風險，並簡化公私部門的資訊分享機制，以及加強關鍵基礎設施網路和系統的復原力及網路安全。

3、強化同盟並吸引新夥伴(Strengthen alliances and attract new partnerships)

(1) 建立可信任的合作關係(Build trusted private sector partnerships)：私部門擁有並經營美國大部分基礎設施，並處於網路空間競爭的前線，國防部將與其他聯邦部門及機構協調，與作為軍事行動關鍵推動因素的私部門建立信任關係，並完成嚴謹規劃和合作訓練，以實現相互支持的網路安全活動。

(2) 實現國際合作關係(Operationalize international partnerships)：許多盟友和夥伴擁有先進的網路能力，可以補充美國的能力，國防部將努力加強這些盟友和夥伴的合作關係，利用其獨特技能、資源、能力及觀點來提升該部的能量，與盟友和夥伴的資訊分享關係將提高網路空間聯合作戰的有效性。

(3) 加強負責任的國家網路空間行為準則(Reinforce norms of responsible State behavior in cyberspace)：國防部將在和平時期將針對負責任的國家網路空間行為，加強其自願、非約束性的規範，美國贊同聯合國國際安全資訊和電信領域發展政府專家組(the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security)所做的工作，即制訂網路空間負責任的國家行為框架，其原則包括禁止在和平時期破壞民間關鍵基礎設施，並禁止將國家領土用於非法網路活動，國防部將與其他機構及國際合作夥伴共同努力，促進有關網路空間行為的國際承諾，以及發展和實施網路信任建立措施(cyber confidence building measures, CBM)，當網路活動威脅到美國的利益時，將準備與合作夥伴一起採取行動以捍衛美國的利益。

4、改革部門(Reform the department)

(1) 納入網路認知至國防部組織文化(Incorporate cyber awareness into DoD institutional

culture)：國防部將調整其組織文化以利各級人員了解網路空間領域，並將這些知識納入日常活動中，主管及其員工需要 cyber fluent，以便他們能夠充分了解其決策對網路安全的影響，並利用網路空間領域以獲得戰略、維運及戰術優勢的機會。

(2) 增加網路安全的可歸責性(Increase cybersecurity accountability)：為減少攻擊面(attack surface)，需要提高整個部門的網路安全認知和可歸責性，國防部人員和其他私部門合作夥伴應對其網路安全實施和選擇負責。

(3) 尋求可負擔、有彈性且健全的解決方案(Seek material solutions that are affordable, flexible, and robust)：縮短軟硬體採購所需的時間以跟上技術的快速發展，我們將採購可擴展服務(scalable services)，如雲端空間及可擴展計算能力，以確保系統能與商業資訊科技保持同步，並在必要時進行擴展以滿足不斷變化的需求，同時還將在可行的情況下使用 COTS 功能，以減少對費用昂貴且難以維護或升級的客製化軟體依賴。

(4) 擴展群眾外包(Expand crowd-sourced vulnerability identification)：國防部將繼續執行群眾外包，例如黑客松(hack-a-thons)和獎金獵人(bug-bounties)，以更有效地識別和減輕弱點並促進創新。

5、培育人才(Cultivate talent)：

(1) 維持準備就緒的網路部隊(Sustain a ready cyber workforce)：國防部員工是重要的網路資產，我們將投資建立未來所需的人才，招募廣受歡迎的人才，並維持我們現有的網路人才，於機關內外部提供充足的機會，以促進網路人員的專業及職業發展，我們將建立流程，以維持整個軍事和民用網路人員的能見度，並將軍事部門和指揮部的人員輪調最佳化，包括最大限度地利用後備役(Reserve Components)，國防部亦將確保其網路需求由武職人員、文職人員及合約人員的最佳組合以滿足任務要求。

(2) 強化國家網路專業人才(Enhance the Nation’ s cyber talent)：為進一步提升公私部門

的網路防禦力，國防部在強化國家網路人才資料庫方面發揮扮演重要角色，該部與其他聯邦部門和機構共同努力，以促進美國中小學教育的科學、技術、工程、數學及外語(STEM-L)等訓練，同時亦將與產業界及學術界合作制定訓練、教育和認知等標準，以促進美國網路人才的發展。

(3) 深化軟硬體專業技術為國防部核心能力(Embed software and hardware expertise as a core DoD competency)：為吸引相關人才，國防部將針對電腦科學相關專家(硬體工程師、軟體開發者及資料分析師)建立職涯發展軌道，提供有意義的挑戰，跨部門的輪調機制，專業教育訓練機，以及特殊網路崗位服役(Cyber Excepted Service, CES)的薪酬激勵措施。

(4) 建立網路頂尖人才計畫(Establish a cyber top talent management program)：國防部將建立一個網路人才管理計劃，為熟悉網路的人員提供集中的資源和機會，在其職業生涯中培養關鍵技術，並採取競爭方式，包括個人和團隊競賽，以找出最有能力的國防部軍事和民用網路專家，並授權這些人員協助解決其最棘手的挑戰。

(七) 資安治理

我國自 103 年起，參考國內 CNS、國際 ISO、美國 NIST 等標準以及我國資安相關規範，包括行政院及所屬機關資訊安全管理要點、行政院及所屬各機關資訊安全管理規範、國家資通訊安全發展方案(102 年至 105 年)、國家資通安全發展方案(106 年至 109 年)、政府機關(構)資通安全責任等級分級作業規定、國家資通安全通報應變作業綱要、資訊系統分級與資安防護基準作業規定等，建立資安治理架構，發展國內政府機關資安防護能力指標與分析，並推動資安治理制度成熟度自評，資安治理推動歷程及如圖 11。

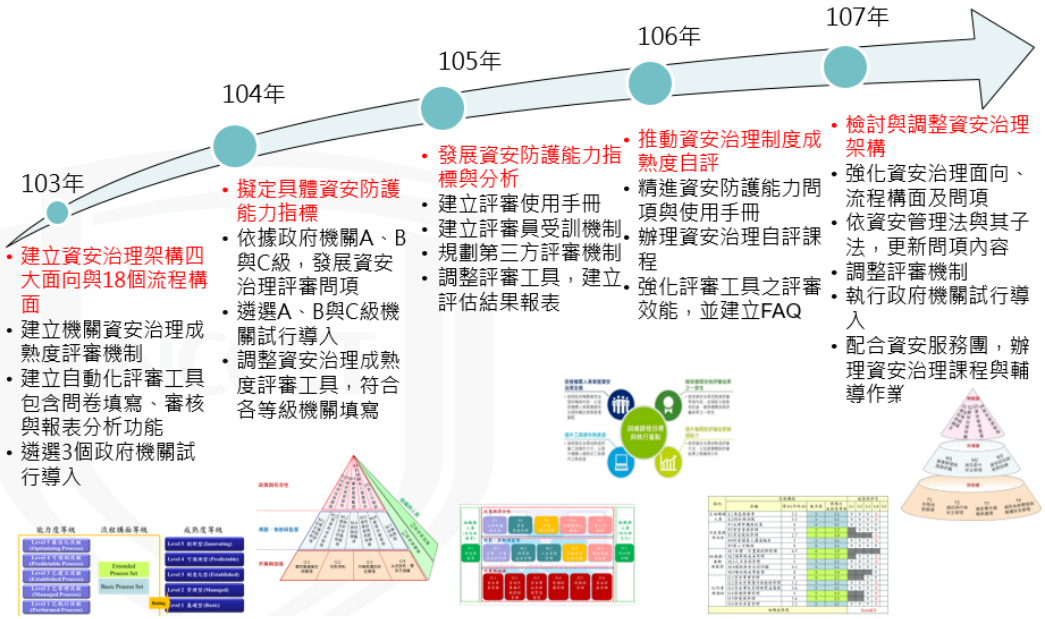

圖 11：資安治理推動歷程

依我國「國家資通安全發展方案(106 年至 109 年)」(發展藍圖如圖 12)，其推動策略「完備資安基礎環境」下之具體措施「建立政府資安治理模式」，已規劃下列分年里程碑：

- ✓ 106 年推動 A、B 級政府機關試行導入資安治理成熟度
- ✓ 107 年精進資安治理成熟度評審機制，完成 3 個 A 級政府機關導入資安治理成熟度自評作業
- ✓ 108 年推動 30 個 A 級政府機關落實資安治理成熟度自評作業，成熟度達第 2 級以上
- ✓ 109 年推動所有 A 級政府機關落實資安治理成熟度自評作業，成熟度達第 3 級以上

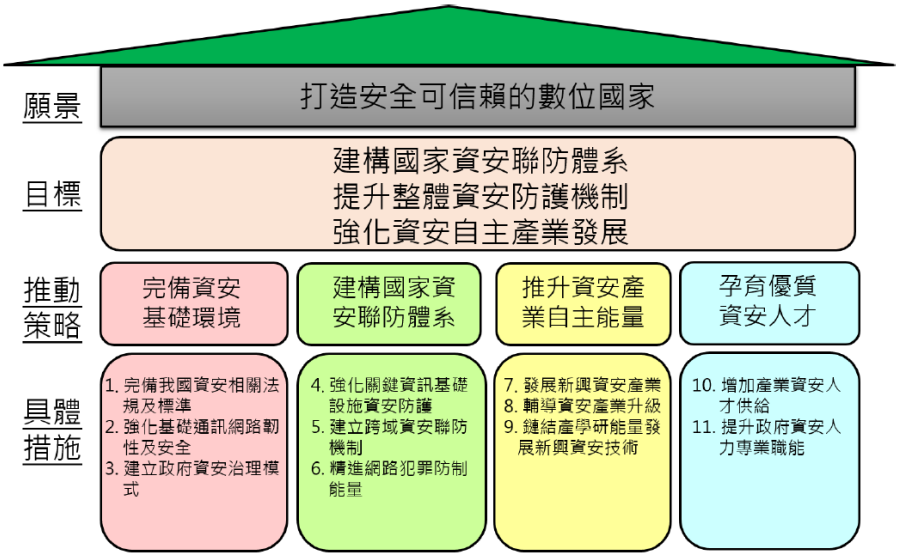

圖 12：國家資通安全發展方案(106 年至 109 年)發展藍圖

依資安責任等級分級辦法之應辦事項，資通安全責任等級 A、B 級之公務機關，每年辦理一次資安治理成熟度評估，如圖 13

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級妥適性。
	資訊安全管理系統之導入及通過公正第三方之驗證		初次受核定或等級變更後之二年內，全部核心資通系統導入CNS 27001資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置四人；須以專職人員配置之。
	內部資通安全稽核		每年辦理二次。
	業務持續運作演練		全部核心資通系統每年辦理一次。
	資安治理成熟度評估		每年辦理一次。

圖 13：資通安全管理法子法要求

有關資安治理與資安管理的關係(如圖 14)，我們參考 ISACA COBIT 5 方法論，定義資安治理架構的三項主要活動，以評估(Evaluate)、指導(Direct)、監督(Monitor)建立治理架構，向下監督、管理資訊安全管理執行機制，並透過治理架構向上溝通，回應組織利害關係人之要求；而資安管理則是遵循治理架構所形成之指導原則，規劃與建立組織適用之管理機制，並透過日常維運執行與監督的過程確保其持續改善，並提供組織得以再次評估之管理回饋。

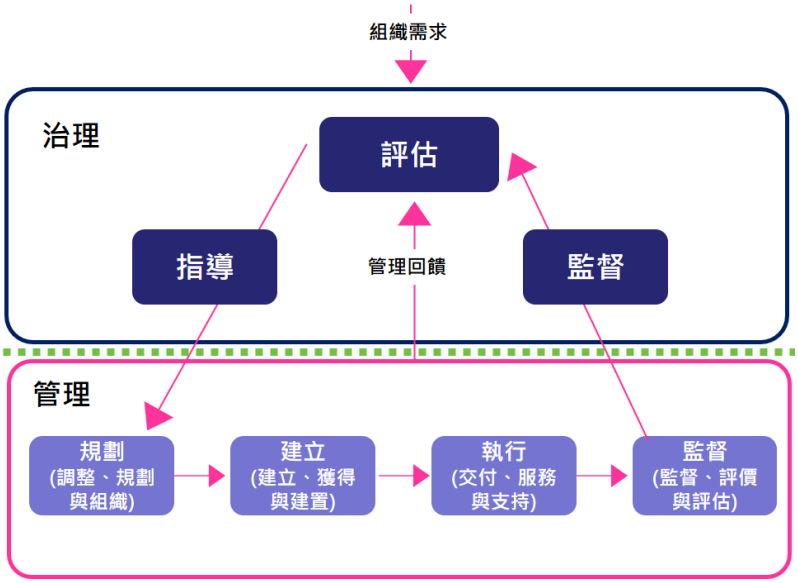

圖 14：資安治理與資安管理關係

資安治理架構原定為「政策與符合性」、「規劃、推動與監督」、「作業與技術」、「組織與人員」等 4 大面向，18 個流程構面，近年為配合我國所推動各項資安政策，進而強化資安治理面向、流程構面及問項，並依資安管理法與其子法，更新問項內容，將資安治理架構調整為策略面、管理面及技術面等三大面向，共 11 個流程構面，新舊版資安治理架構流程構面如圖 15，

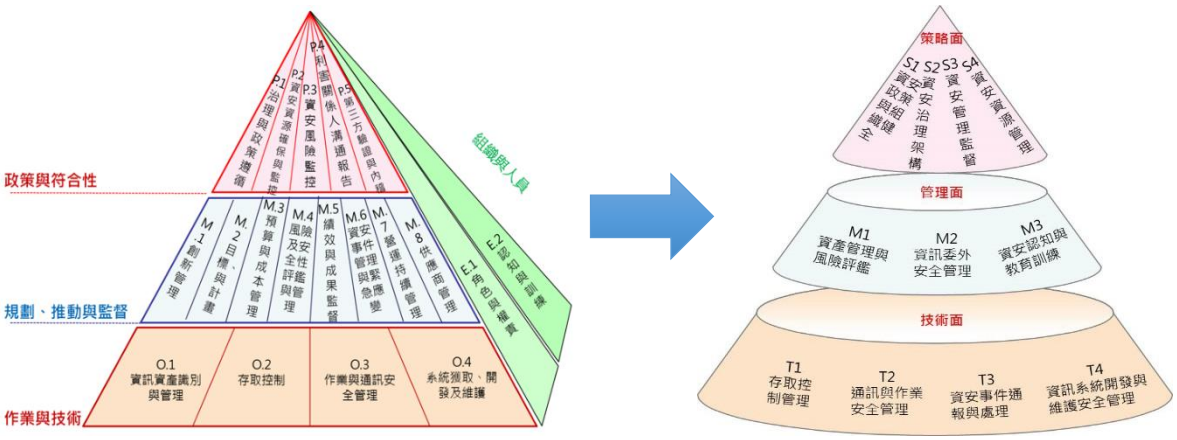

圖 15：資安治理架構流程構面

目前我國所推動資安治理之流程構面目標範圍詳如表 3。

表 3：流程構面目標範圍

面向	流程構面	目標範圍
策略	S1 資安政策與組織健全	• 資安政策建立 • 資安組織與管理審查 • 資安相關法規遵循
	S2 資安治理架構	• 資安新興議題評估 • 利害相關者溝通
	S3 資安資源管理	• 資安資源確保 • 資安專職人員配置
	S4 資安管理監督	• 績效與成果監督 • 業務持續運作管理
管理	M1 資產管理與風險評鑑	• 資安風險管理 • 資通系統分級與防護
	M2 資訊委外安全管理	• 委外廠商資安專業能力 • 委外廠商資安管理 • 委外資安稽核
	M3 資安認知與教育訓練	• 資安認知與教育訓練
技術	T1 存取控制管理	• 網路安全管理 • 權限管理 • 加密管理

	T2 通訊與作業安全管理	• 惡意軟體管理 • 遠距工作管理 • 電子郵件安全 • 實體環境控制措施 • 資料備份 • 儲存媒體處置 • 資通安全監控 • 資通安全防護 • 安全性檢測
	T3 資安事件通報與處理	• 資安事件通報應變 • 日誌紀錄保存
	T4 資訊系統開發與維護安全管理	• 安全系統發展生命週期(SSDLC)落實

經與相關人員訪談，並徵詢意見，其所提出較具體建議包括：成熟度評估完後所得到之分數或等級，是否用來與其他機關比較？各個問卷調查皆會面臨問項過於主觀(Subjective)，而不夠客觀(Objective)；在執行完資安治理成熟度評估後，應有相對應的正面激勵因素(positive incentive)，以鼓勵機關落實辦理。

(八) Google 參訪

在舊金山短暫停留的一個月期間，透過介紹有機會進入到 Google 公司，得以體驗美國矽谷 Google 工作型態，並學習到部分技術新知，包括 GCP(Google Cloud Platform)、go lang、terraform 等。

網路巨擘 Google 兩位創辦人在因緣際會下相遇，因個性及觀點不同而有所爭辨，卻也逐漸醞釀情誼，間接改變了他們的人生，而 Google 以人為本的創新文化，強調無所畏懼、幽默互動、博感情、飆創意的樂趣文化，著實令人驚訝！在矽谷充斥著創新創業生態，新創團隊在這能浸淫在全球最具創新氣氛的生態圈，與來自世界各地的創業者交流，逐步連結國際市場；矽谷另一特色在於充滿著大格局、合作、截長補短、開放創新的文化生態，可多元探索創新人才培養模式。爰此，政府近年提出亞洲・矽谷推動方案，期望建立一個以研發為本的創新創業生態系，由物聯網及新創 2 大主軸，輔以連結國際、連結未來及連結在地的 3 大連結，期以物聯網促進產業轉型升級，並以創新創業驅動經濟

成長。

圖 16：Sunnyvale 的 Google 公司

圖 17：舊金山的 Google 公司

圖 18：Mountain View 的 Google 公司

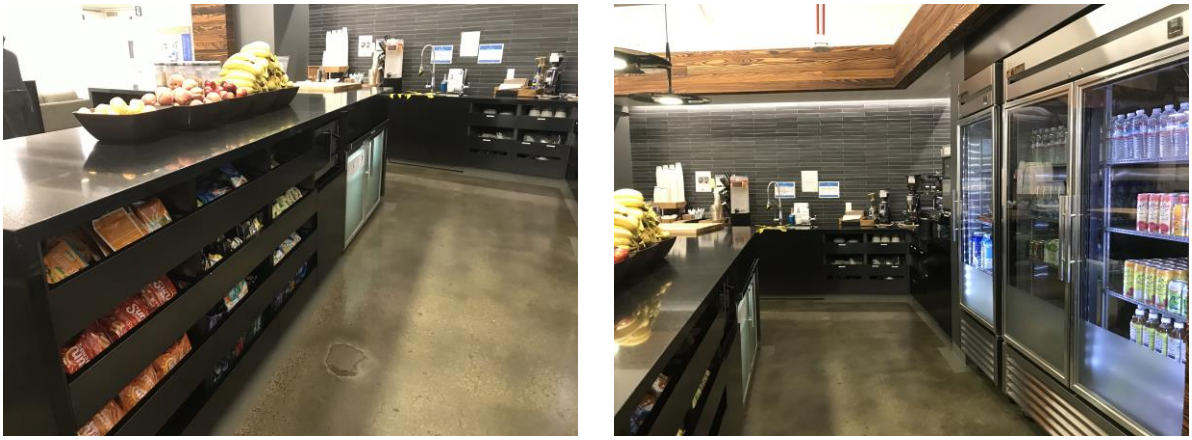

圖 19： Google 公司隨處可見的 MK(Micro Kitchen)

參、心得建議

本次出國專題研究實為人生難得經驗，除體驗到美國校園生活及當地文化，與教授及企業討論了解到美國與臺灣之間的異同處，不管是政策、法規或是實務經驗；當然最特別的是能有機會到矽谷感受創新創業生態圈，也參觀 Apple Park、NASA 園區及 Stanford University 等著名研究重鎮。

面對未來下一代人才培育，觀察我國現行教育體制著實令人憂心忡忡，在美國許多知名學校要求所有學生應至企業實習，這同時也是學生畢業後尋求正職工作的有效管道，我國應鼓勵國內企業參與教育創新，產官學教研可以合作推動創新的教育模式，讓學生學其所愛、愛其學，適時發揮其資優才能。

另根據研究，接觸美國文化越多，創造力的表現越高，主要係因多元文化促進創造力的培養，或許未來可視臺灣是家鄉，世界是校園，到國外學習或服務，以習得外語、文化、國際觀、創造力、人際網絡等能力；目前各國人才爭奪戰已開打，企業中最重要的資產肯定是人才，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。