出國報告(出國類別：參加國際會議)

出席 2017 年倫敦行動計畫
(LAP:London Action Plan)年度會議報告

服務機關：國家通訊傳播委員會

姓名職稱：蘇簡任技正思漢、李技正福懿

派赴國家：加拿大 多倫多

出國日期：**106** 年 **9** 月 **30** 日至 **10** 月 **7** 日

報告日期：**106** 年 **12** 月 **21** 日

壹、前言

本會為配合行政院之政策，協助推動垃圾郵件防制，對外積極參與國際反垃圾郵件相關組織之活動以尋求國際合作之機會；在國內則係持續監督電信相關事業透過服務契約提供垃圾郵件技術防制，以確保民眾之通信權益。另因垃圾郵件與網路資訊安全議題已環環相扣，垃圾郵件防制工作已成為本會電信資安防護工作之一，本會除續辦垃圾郵件防制與跨國之合作事務，亦更積極推動電信資安的防護事務。本次派員參與倫敦行動計畫之目的，除藉由參與會議以瞭解並蒐集各會員國就防制訊息濫發及網路安全防護之機制與趨勢，以作為本會規劃與業務執行面之參考外，亦繼續垃圾郵件防制之國際交流與擴展任務。

本次會議乃係由「倫敦行動計畫」及「反濫用訊息、惡意軟體、行動通訊工作群組」(Message Malware Mobile Anti-Abuse Working Group， M3AAWG)兩大組織合併舉辦，M3AAWG General Meeting 主要為各國在訊息濫發防制上的議題提出討論、分享作法、及法規制訂與執行現況，在依照不同的領域性（垃圾郵件、廣告簡訊、廣告電話、Do Not Call、Robot Call）分別在依照技術面、政策面、各國現況等不同主題分別舉行相關會議。本會加入的會員組織為 UCENet（THE UNSOLICITED COMMUNICATIONS ENFORCEMENT NETWORK），該組織前身為 LAP（THE LONDON ACTION PLAN），組織成員主要為各國在垃圾郵件防制上的主責機關，共同致力於垃圾郵件有關之「情報」、「法規」、「溝通」、「訓練」等議題上建立共識與交流。

貳、會議議程

會議行程		
日期	上午	下午
10 月 2 日 星期一		• Hands-On Intro to Machine Learning to Identify Email Abuse • Hands-On With Advanced Topics in Machine Learning to Identify Email Abuse
10 月 3 日 星期二	• UCENet Sweep 2017 (OPEN) - Affiliate Marketing • 會晤日方代表	• UCENet & DNA-SIG & Public Policy GDPR Impact on WHOIS data • Combined Capabilities for Internet Security
10 月 4 日 星期三	UCENet (LE ONLY) - Emerging trends from ASIA / PACIFIC	
10 月 5 日 星期四	• Robocalls Regulatory Update, Successes and Challenges • CASL Enforcement Update from various Canadian Enforcement Agencies	• The Email Blocklist: An Introduction

參、議程活動

一、透過上機操作瞭解機械學習在辨識垃圾郵件防制之應用

Hands-On Machine Learning to Identify Email Abuse(106 年 10 月 2 日)

機械學習(Machine Learning)已廣泛使用在各項領域,並且在資安方面也積極發展,除了能夠更快速掌握重要資訊外,更重要的可以輔助人力在資料分析上效率的提升。一般企業或郵件服務供應商(Email Service Provide),已經導入機械學習的技術,其目的為了降低 Email 用戶在收到郵件前,就已經協助過濾出哪些是屬於垃圾郵件範疇,以確保用戶能夠避免接觸到過多不必要的資訊,甚至是惡意釣魚郵件(Phishing)。

過去在判斷垃圾郵件特徵的方式,習慣透過內容中的「關鍵字/詞」的邏輯組合進行分類,但是由於類型變得越來越複雜,規則組合開始變得難以掌控,包括如何記錄、傳遞以及處理這些郵件的分類,許多解決這樣問題的技術就必須仰賴機器學習這個範疇,協助完成建立分類的邏輯,亦即是要如何解決自動化方式從數據的某些特徵中學習他們之間的關係。

本次議程第一天的活動行程,主要是透過直接上機操作方式(Hands-on)初步瞭解透過機械學習,協助垃圾郵件的偵測與濫用。該場次共有兩個主題,分別是:「Intro to Machine Learning for Detecting Abuse」、「More Advanced Topics in Machine Learning for Detecting Abuse」,由 Dr. Victor Amin 來介紹、解說。

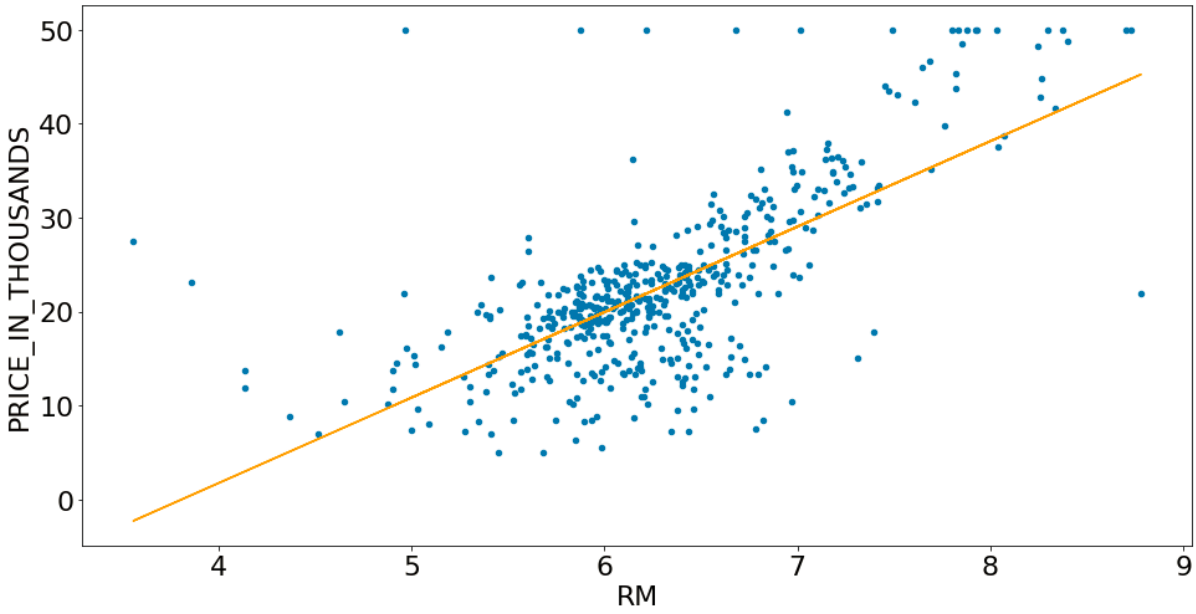
Victor 博士是任職美國 SendGrid 電子郵件服務公司的一位數據科學家,主要的任務就是增強電子郵件的可交付性,藉由數據科學的管理,阻止垃圾郵件、網絡釣魚和其他濫用行為的發生,並且協助重要的郵件發送到他們該去的地方。Victor 博士創建數據策略,構建機器學習的產品,並進行由 PB 級數據量的嚴峻分析研究。

首先,在第一場「Intro to Machine Learning for Detecting Abuse」過程中,Victor 博士透過 Microsoft Azure Notebooks 雲端服務方式,加上 Python 技術介紹如何透過機械學習來偵測垃圾郵件的氾濫情形。主題包含有:

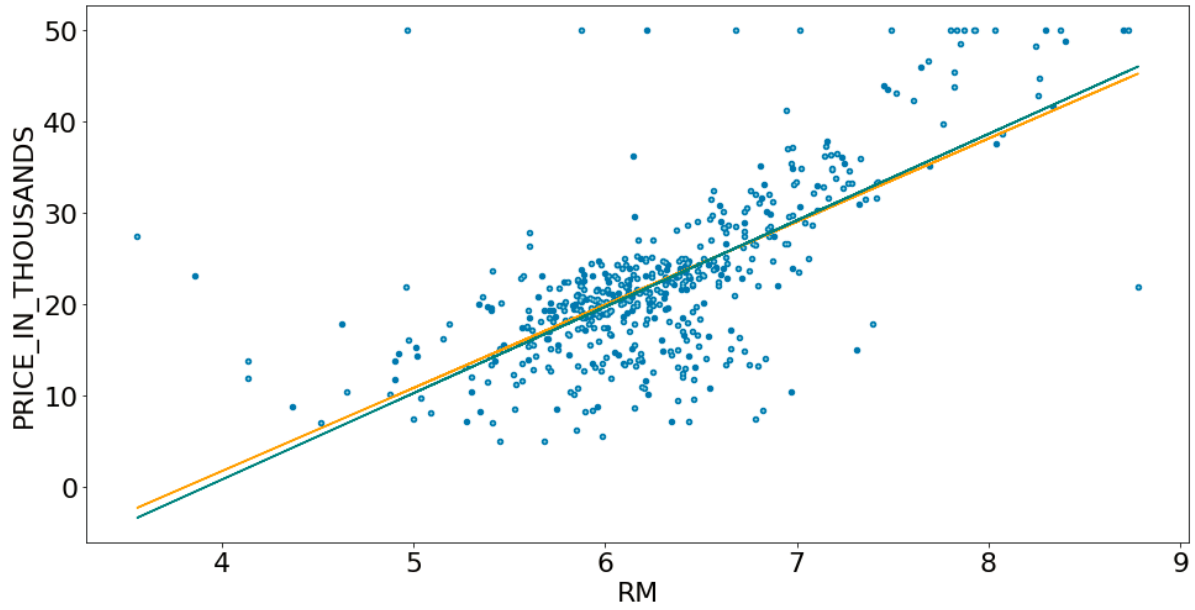
1. A quick intro to this coding environment.
2. A basic primer on machine learning.
3. A practical example of using machine learning to detect spam.

接著在第二場「More Advanced Topics in Machine Learning for Detecting Abuse」，透過實際數據資料訓練，來呈現如何應用機械學習輔助偵測哪些屬於垃圾郵件。

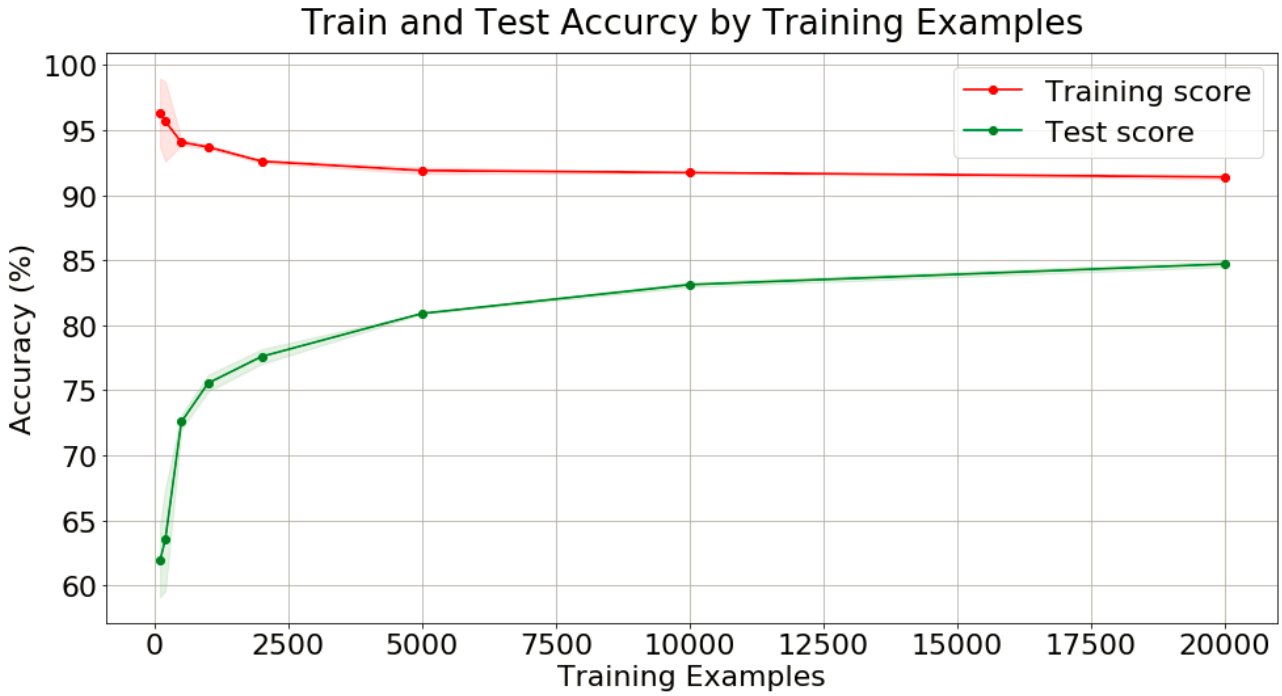
本次上機操作所使用的技術為 Python，Python 是目前廣泛被使用在數據分析技術領域上的程式語言，同時也是腳本程式工具（Script Language Tool），Victor 博士先以事先準備好的垃圾郵件資料，一步一步指導如何將數據以散點圖方式呈現，同時發現數據的趨勢，並建立數據模型，如下圖所示。



接下來透過測試資料的演算，繪製出趨勢，並透過與數據模型的比較找出差異，將這些差異進行修正，如下圖所示。



Victor 博士採用的是「Random Forest 演算法」，透過該演算法對電腦進行訓練與學習方式，反覆數次，同時提供資料量與樣本數越來越多時，電腦可協助判斷的誤差就會越來越低，分析出結果能力越來越貼近真實狀況，詳如下圖趨勢所示。



有鑑於機械學習應用領域越來越廣泛，亦可應用在判定偵測是否為垃圾郵件濫用的範疇，在未來透過 Spam 佈點主機的佈建，蒐集 Spammer 濫發垃圾郵件的行為特徵上，將有助於協助分析人員進行特徵判斷。

二、 聯盟營銷（Affiliate Marketing）掃描報告（Sweep）

UCENet Sweep 2017 – Affiliate Marketing（106 年 10 月 3 日）

本次會議主講人為 Adam Stevens ，該員是英國 ICO(UK Information Commissioner's Office)情報中心的團隊主管，ICO 組織主要的是英國針對訊息、資訊權力的維持與保護的獨立，維持公共利益，並促使國家立法的機構。

在2017年6月，UCENet(原為LAP, London Action Plan，於2016年9月更名為UCENet, Unsolicited Communications Enforcement Network)進行了第一次掃描（Sweep）報告。本次的掃描報告涉及許多組織，針對特定主題的資訊蒐集進行協調，其目的是為了追求各國遵守/執法相關活動，以及促使 UCENet 會員對變革後對組織發展目標主題的理解。2017 年的主題是與聯盟營銷（Affiliate Marketing）有關的項目。在本次會議中，專家小組成員將介紹他們從掃描過程中發現的高層次調查結果，其中包括他們發現的主題和趨勢，以及個別機關深入研究與結果有關的相關（公開）工作。產業專家還將介紹他們在聯盟營銷和垃圾郵件之間的關連經驗。

PSA(Phone-paid Services Authority Findings)組織 John Hodge 分享 Sweep 執行成果。PSA 採用自動化工具應用在 285 盜版內容網站、97 個新聞報紙與雜誌內容網站進行瀏覽次數分析，發現了 85 個潛在問題。其中資安威脅主要造成影響的包含：瀏覽器首頁綁架（Browser Hijacks）、下載潛在有害程式（PUPs）。調查結果發現，其中網站內容屬於約會詐騙網站類型佔 2%、賭博娛樂網站類型佔 4%、成人網站（包含成人聊天、成人遊戲）類型佔 6%、快速致富廣告網站類型 8%、網站直接發現 Ransomware（Microsoft Spoofs）佔 7%。該組織表示目前掃描成果仍有進步空間，未來將考慮進一步分析加盟型網站與運動型網站，同時考慮針對 Cookie 進行分析並針對新聞報紙與雜誌內容類型網站進一步深入分析。

三、 我國與日本 MIC 及 JADAC 交流會議

（106 年 10 月 3 日）

日方出席代表有：

總務省（Ministry of Internal Affairs and Communications，MIC）電信局第二電信消費者政策處（Second Telecommunications Consumer Policy Division，Telecommunications Bureau）：

企畫官（Director） 岡本剛和（Yoshikazu OKAMOTO）

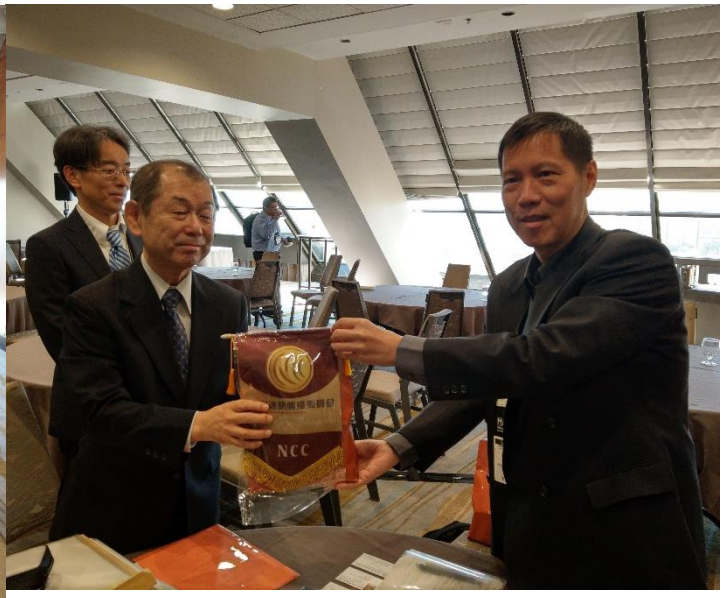
日本數據通信協會（Japan Data Communications Association，JADAC）反垃圾電子郵件諮詢中心（Anti-Spam Consultation Center）：

次長（Director） 西松 薰（Kaoru NISHIMATSU）

審議役（Deputy Director）谷原秀彥（Hidehiko TANIHARA）

由左至右為：西松薰、谷原秀彥、岡本剛和、蘇思漢、林高裕、李福懿

日本數據通訊協會(下稱 JADAC)代表西松 薰先生為 JADAC 垃圾郵件防制中心代表，其為日本垃圾郵件主管機關－總務省委託辦理防制垃圾郵件事務之主辦機構首長，主要擔任諮詢指導業務，負責 Honeypot 資料分析、對垃圾郵件資訊交換、國際合作及電話諮詢建議等垃圾郵件防制業務。本次會晤開始前，由本會基礎處蘇簡任技正思漢致贈日方代表紀念品，以表示友好關係。



本次台日雙邊討論主題，包含：垃圾郵件與垃圾郵件防制的最新訊息交流、電子郵件供應商回報國外移案的處置情形、未來進一步針對垃圾郵件防制的作法與規劃。針對上訴的相關議題向日方分享我國在垃圾郵件管理立法上遇到的處境，以及在今年將透過數位通訊傳播法的修訂，以期能向垃圾郵件防制更向前邁進。此外，因配合我國資安即國安的政策目標，概要性向日方介紹 NCC 在 SOC、ISAC、CERT 短期計畫目標，同時也透過簡報內容說明新一代 SPAM 管理系統運作架構規劃，包含垃圾郵件分析管理的運作方式，如何建立自動化機制、垃圾郵件誘捕系統研究方向與技術方式、以及透過事件追蹤管理的作法，將垃圾郵件通報業者採用事件管理進行通報及後續處置的追蹤，唯獨針對移案處置回報情形，因目前國內在管理辦法上缺乏強制力，針對惡意散播行為較難有進一步要求或罰則措施，因此將先從技術面著手，以強化系統能力與完整性為要務，並期能持續與國際接軌。

會談過程中西松 薰先生分享目前 JADAC 組織運作的一些近況，日本約有 1.2 億個 email 帳號，到目前為止，已經佈建了 200 個 honey pots，以供蒐集與分析垃圾電子郵件（spam），運作上編制有 3、4 人以人工方式針對無法自動判定之垃圾郵件，進行是否為垃圾郵件的判斷，每天總共要處理約 1,500 件電子郵件。

針對反垃圾電子郵件（anti-spam）日方已建立 8 個合作國家，包含：臺灣、中國大

陸、韓國、香港、越南、緬甸、巴西、印度（只送不收），針對垃圾郵件防制交換資訊。另外，中國大陸的 QQ 在特定日期，例如七七抗戰勝利紀念日、918 瀋陽事件日等，會連續幾天透過網路攻擊日本國會網站影響網際網路運作，日方想找中國大陸談，但是中國大陸不願接受邀約。同時日方也表示近期將進一步與加拿大建立合作關係，以拓展垃圾郵件情資交流的機會。JADAC 是致力於內容遭濫發防制的專責機構，有別於資通安全管理，因此有關於郵件中隱含惡意程式或惡意連結的部分，並不屬於 JADAC 所負責的範疇，而涉及內容濫發的部分，包含簡訊、廣告電話等議題，均是 JADAC 所負責的領域。此外 JADAC 在日本已經佈建行動電話的 spamtrap 系統，開始蒐集垃圾郵件，並向本會分享，南韓網際網路及安全中心（Korea Internet & Security Agency，KISA）是負責佈建電子郵件誘捕系統之機構，用來蒐集分析垃圾電子郵件資訊。

岡本剛和表示，日本的情報處理推進機構（Information-technology Promotion Agency，IPA）負責處理資訊安全事務，而國家資訊安全中心（National Information Security Center，NISC）負責處理網際網路濫用事務。此外在日本每個行動電話的 email 帳號大約被詐騙了 10 到 20 美元的金額。

近年在社群通訊工具逐步流行與廣泛被使用的狀況下（例如：Line），JADAC 已收

到越來越多的民眾的檢舉社群通訊工具的廣告濫發情形，因我國民眾在社群通訊工具的使用習慣上與日本相近，如何在這個領域進行有效的防制與管理，將是我國未來的課題之一，在這部分也將是本會未來可與日方進一步交流的議題。日本數據通信協會為財團法人性質組織，與電信技術中心屬性相當，未來有機會可以向日本方面有關垃圾郵件防制的作法，包含技術面、法規面，如何協助主管機關完成防制與管理事務，進一步合作與交流，日方積極表達未來可安排前往日本進行參訪 Spam 系統建置成果與雙邊交流的可能性，我方表示會考慮這項邀請。

四、 歐盟一般資料保護法規（GDPR）對網際網路的影響

UCENet & DNA-SIG & Public Policy GDPR Impact on WHOIS data（106 年 10 月 3 日）

由於歐盟會員國在個人資料保護相關法律缺乏一致性的架構，以及近年來雲端計算、行動互聯網、大數據等資訊科技的快速發展，對個人資料保護帶來新的議題與挑戰，歐盟對於 1995 年的資料保護指令（Directive 95/46/EC: the Data Protection Directive）進行大刀闊斧的改革。

歐盟執委會自 2012 年 1 月提出資料保護改革草案以來，其嚴苛的規範撼動資訊科技界的巨擘於歐盟經營的根基，紛紛投入龐大的資源向歐盟當局進行遊說，歐洲議會共計收到4千多份修正意見，經過4年多的討論，終於在2016年4月27日通過歐盟規則2016/679，即一般性個人資料保護規則（General Data Protection Regulation，GDPR），GDPR 自 2016 年 5 月 24 日起生效，1995 年的資料保護指令則不再適用。

GDPR 有 2 年的過渡期，直到歐盟各會員國均實施 GDPR 後，將自 2018 年 5 月 25 日起全面施行新法。GDPR 不僅適用於歐盟會員國境內註冊的企業，非屬歐盟企業體但在歐盟會員國境內營運，蒐集、處理或利用歐盟會員國人民的個人資料者，亦須適用。

此外，GDPR 除了提升個資保護強度，且大幅提高了罰款金額上限，最高可處 2,000 萬歐元或當年度全球總營業額 4%金額的罰鍰。

根據 GDPR 的規定，沒有特別目的，不需要保留太多的個人資料，要保留資料必須建置 Registry，才能為之，而且經過個人同意，才能使用個人資料。ICANN 了解歐盟的 GDPR 將於 2018 年 5 月全面實施，因此 ICANN 董事會成立了 EWG 要將 WHOIS 升級成 RDS（Registered Data Server），並提供具有安全防護的 DNSSEC 功能，因此，為了保護個人資料，未來的 RDS 只會提供最少量的資料（thin data）供民眾查詢，因此有可能影響到調查人員或警察人員的犯罪偵察辦案作為。ICANN 已經在密切的討論與尋求解決方法。

ICANN 根據關於 gTLD 註冊數據提出改革建議，提出「廣泛和有針對性的行動方案」（broad and responsive action），同時 ICANN 核定了一個流程框架，並規劃新一代服務系統的以便適當考慮所有相互依賴的政策領域，其評估與執行步驟如下：

步驟一：確定下一代通用頂級域名（gTLD）註冊目錄服務（Registration Directory Service，RDS）的需求，確認是否以需要取代現行的 WHOIS 系統。

步驟二：設計一個新的政策框架（Police Framework），詳細說明下一代 RDS 提供的功能以支援哪些要求。

步驟三：如何為下一代 RDS 系統落實執行這些政策進行指導，並最終取代現行的 WHOIS 系統。

五、 網際網路安全綜合能力報告

Combined Capabilities for Internet Security（106 年 10 月 3 日）

為了因應資安事件日益增長的需求，需要有機關執法的能力以及能夠被信任的團體協助減輕及處置資安威脅。例如 DNSChanger and Avalanche 組織間的合作關係是廣為人知的成功案例，但仍然有許多不同的組織或跨國聯盟更需要瞭解如何運作及情資的共享。105 年 12 月開始，在史丹佛國際安全與合作中心（Stanford's Center for International Security and Cooperation）在一場 LE and Trust Communities 系列活動研討會當中，針對情資共享與協作方面造成成功與失敗的關鍵因素進行討論。本場次會議中針對 UCENet 會員於該系列活動研討會中獲得相關的回饋資訊，希望未來能夠進一步分享，有助於 UCENet 會員在訊息分享上的參考。

六、 南韓 KISA 主辦的亞太地區發展趨勢會議

UCENet (LE ONLY) - Emerging trends from ASIA / PACIFIC（106 年 10 月 4 日）

本場次會議由南韓 KISA 主辦的亞太地區發展趨勢會議，邀請國家包含有：臺灣、新加坡、日本、南韓、香港等國家，分別針對各國現況進行報告，以下內容排序依當日報告順序。

由左至右為：主辦代表、新加坡代表、日本代表、南韓代表及我國代表

1. 新加坡

新加坡的個人資料保護委員會（Personal Data Protection Commission，PDPC）官員 CHUNG Sang Hao（Assistant Director of DNC & Tech Operations）表示，該委員會是在 2013 年 1 月 2 日根據 2012 年的個人資料保護法（Personal Data Protection Act，PDPA）成立的，後來在 2016 年 10 月移撥至資通訊媒體發展局（Info-communications Media Development Authority，IMDA）下，目前有 50 名員工，負責簡訊（SMS）、電話（phone call）的申訴處理，Do Not Call 的個人資料保護工作是在 2013 年開始推動，目前 PDPC 已經設置電話黑名單登錄資料庫（Do Not Call registry），分析黑名單的電話號碼。

PDPC 目前已經有法規（legal arm）及技術（technical arm）兩個面向的條件，協助他們的施政作為。不過 PDPC 只針對固定通信網路的電話及傳真、行動通信網路的電話進行監理，但不監理公務電話門號，且 SPAM 也不在 PDPC 的監理範圍。目前新加坡約有 800 萬門電話號碼，目前已有約 10%納入了 Do Not Call registry。

2. 日本

日本 MIC 的岡本剛和企劃官表示日本憲法第 21 條規定，任何通訊工具不可以違反秘密通訊原則，且電信業務法（Telecommunications Business Act）第 4 條規定，電信業者管理的秘密不可以被違反，是為保障通信內容安全的法源。而日本於 2002 年制定的「特定電子郵件傳送標準化法」，則是希望使網際網路使用人免於垃圾郵件騷擾，建構良好的電子郵件使用環境，俾促進高度資訊化社會健全發展。

他表示，日本已經規劃設置一套新的 DMARC（Domain-based Message Authentication, Reporting and Conformance）系統，它是一套以 SPF 及 DKIM[1]為基礎的電子郵件認證機制，可以檢測及防止偽冒身份、對付網路釣魚或垃圾電郵。

---

[1] DMARC（Domain-based Message Authentication, Reporting and Conformance）是一套以 SPF 及 DKIM 為基礎的電子郵件認證機制，可以檢測及防止偽冒身份、對付網路釣魚或垃圾電郵。
網域管理員可以在域名系統公布相關政策，讓外界得知旗下域名的電子郵件提供何種方式（SPF 及/或 DKIM）認證身份，以及如果寄件者身份未能百分之百確認時，收件者可以如何處理郵件（放進雜件箱或直接回絕）及回報。回報機制可以讓網域管理員了解是否有第三者正在偽冒其網域身份寄出電郵。
發件人策略框架（英語：Sender Policy Framework；簡稱 SPF；RFC4408）是一套電子郵件認證機制，可以確認電子郵件確實是由網域授權的郵件伺服器寄出，防止有人偽冒身分網路釣魚或寄出垃圾電郵。SPF 允許管理員設定一個 DNS TXT 記錄或 SPF 記錄設定傳送郵件伺服器的 IP 範圍，如有任何郵件並非從上述指明授權的 IP 位址寄出，則很可能該郵件並非確實由真正的寄件者寄出（郵件上聲稱的「寄件者」為假冒）。
DKIM（Domain Keys Identified Mail）是一套電子郵件認證機制，使用公開金鑰加密的基礎提供了數位簽章與身分驗證的功能，以檢測寄件者、主旨、內文、附件等部份有否被偽冒或竄改。
一般來說，發送方會在電子郵件的標頭插入 DKIM-Signature 及電子簽名資訊。而接收方則透過 DNS 查詢得到公開金鑰後進行驗證。

3. 南韓

南韓 KISA 的個人資料保護中心（Personal Data Protection Center）Bong Ki Hwan 經理表示，已經邀集國內如三星、LG 等手機製造商，於手機內建不請自來通信（垃圾郵件或簡訊等）的簡易回報功能（easy reporting function）軟體，將蒐集到的垃圾資訊直接傳到 SK、KT、LGU+國內三家電信業者，供該等業者分析處理。此外，KISA 表示，該中心建置的蜜網（honey net），其蜜罐（honey pot）系統可以偵測到全球的電子郵件。

4. 臺灣

本會蘇簡任技正思漢擔任最後一位講者，於會中簡要描述我國在關鍵電信基礎設施防護（Critical Telecommunications Infrastructure Protection）方面，已經規劃針對 6 個主要電信或網際網路服務，建置一套網路監看監控中心（Network Observation and Monitoring Center，NOMC），負責電信關鍵基礎設施的緊急事件應變處理。

另外在網際網路資安方面，將建置升級版的網際網路安全中心（Cyber Security Center），負責 SOC（Security Operation Center）、ISAC（Information Sharing and Analysis Center）、CERT（Computer Emergency Response Team），負責網際網路資安事件的應變處理。另亦規劃利用網際網路安全中心的蜜罐（honey pot），建置垃圾電子郵件（spam）誘捕蒐集與分析的 spamtrap 功能，以蒐集垃圾郵件資料，並進行後續的分析分享，同時規劃將可進一步分析 Spammer 的行為及 spam 的特徵，追蹤 spam 的發信位置、來源及可能的散播趨勢。

最後說明本會已經擬定數位通訊傳播法，這是一份網際網路的民法，管理行為但無罰則的法。其中也將處理 spam 的精神納入，例如發信者須於 spam 內提供 opt-out 功能、發信者在收到拒絕接收 spam 的回應後不得再次發送，發信者必須揭露真實資訊給收信者，被視為 spam 的要件，不被視為 spam 的要件。

七、 Robocall 的監理與執法近況報告

Robocalls: Regulatory and Enforcement Update（106 年 10 月 5 日）

本場次會議主要聽取數位政府的代表，包含澳洲通訊及媒體管理局（Australian Communications and Media Authority，ACMA）代表 Jeremy Fenton、美國聯邦通信委員會（Federal Communications Commission，FCC）代表 Micah Caldwell、英國資訊委員會辦公室（Information Commissioner's Office，ICO）代表 Adam Stevens，會議主席為聯邦貿易委員會（Federal Trade Commission，FTC）Janice Kopec，就監管、政策和執法措施等方面，以打擊不必要的來電騷擾，進行分享，包括統計數據，呼叫阻止次數，來電顯示認證治理

和執法趨勢等內容進行報告。

根據 AMCA 統計，自 2009 年 10 月至 2017 年 8 月，DNC（Do Not Call）以及 Robocall 抱怨次數逐年升高，此外拜輔助科技進步之賜，2017 年的抱怨次數以高成長比例的斜率向上攀升，2017 年 8 月的抱怨次數已創歷年新高。根據統計，2017 年 1 月至 8 月的抱怨次數，DNC 的抱怨次數平均每月達 691,024 次。

根據 FCC 統計，統計不想接的來電電話（Unwanted calls），每年收到的抱怨數量從 2015 年 1 月至 2017 年 9 月進行抱怨次數統計，2015 年有 172,000 次、2016 年有 150,000 次、2017 年統計至 9 月，已有 141,000 次抱怨數。FCC 根據所蒐集來的抱怨電話資料，依照蒐集資訊欄位（Date、Time、Type of device、Caller`s number、Type of call 等欄位）提供 API 服務供系統整合廠商應用，同時也提供給第三方開發攔阻 APP 的廠商應用其資料。FCC 在 2017 年 3 月，發佈了 Call Blocking NPRM/NOI 委員會文件，主要目的為針對和消除非法 Robocall 的治理，委員會通過了「建議規則制定通知」(Notice of Proposed Rulemaking，NPRM）和「查詢通知」（Notice of Inquiry，NOI），使語音服務提供業者能夠更好地保護用戶免受非法 robocall 侵擾。同時在 2017 年 7 月 FCC 發佈兩個 NOI，分別是：Caller ID Authentication NOI、Reassigned Numbers NOI，Caller ID Authentication 主要是探討是否實施電話認證標準，以阻止使用來電顯示欺騙的非法 Robocaller 欺騙用戶，Reassigned Numbers 主要是探討是否使用 ID 認證資訊，建立企業可以用來識別該企業已被分配的電話號碼資源。

根據 ICO 表示，統計 2016 年 1 月至 2017 年 8 月，最大宗的抱怨數來自於 Automated Calls（Robocall），其次是 Live Calls（Do Not Call），在英國 Live Calls 的抱怨數量月均值大約在 5K 左右，Automated Calls 部分起伏較大，但自 2016 年以來，已有良好成效，從高峰的接近 20,000 次，至 2017 年 8 月，已降為 10,000 次，在 2017 年 4 月是近年來最低，約 8,000 次左右的抱怨量。統計 2017 年 8 月的 Live Calls 抱怨類型當中，以事故索賠類型的廣告電話（Accident Claims）最高。在眾多類型因抱怨檢舉衍生違法罰款，自 2017 年統計至 2017 年 9 月總金額已高達 2,593,500 英鎊。

八、 加拿大反垃圾電子郵件法（CASL）

CASL（Canadian Anti-Spam Law）Enforcement Update from various Canadian Enforcement Agencies（106 年 10 月 5 日）

加拿大的反垃圾電子郵件法（Canadian Anti-Spam Law，CASL）已經由廣播電視及電

信委員會（Canadian Radio-television and Telecommunications Commission，CRTC）制訂發佈並實施 3 年。而 CASL 具有賦予政府機關與國際相關政府機關交換 spam 垃圾電子郵件之授權。加拿大競爭署（the Competition Bureau）及隱私委員辦公室（the Office of the Privacy Commissioner，OPC）已經實行法的效力及依據該法進行調查。加拿大此三個聯合執法的組織正在討論推動法律執行的不同案例、趨勢及計畫。Do not call 的推動，可以促進民眾提出申訴並蒐集資料，每天約有 2 萬件申訴案件。

加拿大 CRTC 下轄之垃圾電子郵件報告中心（Spam Reporting Centre，SRC）統計處理的五種主要申訴案件型態為：合法公司及產品（legitimate company, legitimate product）、半合法公司及產品合法性懷疑（legitimate company, product legitimacy suspect）、非法公司/賣家但無產品詐騙（illegitimate company/seller, no product scam）、釣魚程式（phishing）、惡意軟體（malware），過去 6 個月以來，已有超過 1 千個案件。

根據 2017 年 3 月至 2017 年 9 月的統計，以簡訊（SMS）進行釣魚有 3 種主要類型：第一種是假冒銀行業務（Banking），以簡訊提供假的銀行網頁連結，騙取用戶帳號密碼；第二種是假冒加拿大稅收局業務（Canadian Revenue Agency，CRA），偽裝是 CRA 寄給民眾退稅的假網頁連結。第三種是假冒電信業者（Telecommunications Service Providers，TSPs）發出有帳務錯誤的訊息，騙用戶點選釣魚網頁連結可獲得退款。CRTC 目前亦在探討執法的領域，包括其他平臺（SMS/OTT）、惡意軟體（malware）、惡意主機（malicious hosting）。

加拿大競爭署（CB）是依據競爭法執行聯邦法律的機關，另有 3 個法規命令。競爭局下轄 4 個局（Directorate），市場詐騙作為管理局（Deceptive Marketing Practices Directorate，DMPD）負責假造或誤導的報導，以及市場詐騙作為之管理，最近的處理的案例為調查 Hertz and Thrifty、Amazon、Avis and Budget 此 3 家公司此的不當行為。

加拿大隱私委員辦公室（OPC）資深顧問 Trevor Yeo 指出，CASL 修正了個人資訊保護及電子文件法（The Personal Information Protection and Electronic Documents Act，PIPEDA），PIPEDA 是用於私人機構的聯邦隱私法。2016 年至 2017 年共 95 份有關隱私的報告，有 55 份涉及偷取或未獲授權接取個人資料，因此，OPC 目前正針對個人隱私的保護進行探討分析。OPC 的優先目標有三項：持續更新於 UCENET 提出的掃描（Sweep）報告、與 CASL 授權共同執法的伙伴合作、持續與私人公司討論所見之電子威脅風險。

九、 電子郵件黑名單介紹

The Email Blocklist: An Introduction（106 年 10 月 5 日）

Slido.com 組織為本會議的發起與發表人，會議內容為針對垃圾郵件(Spam)攔阻電子郵件名單（Email Blocklist）進行說明，並以互動式網頁，由現場參與者提出問題，即時討論，主要說明的項目如下：

- 為什麼要使用雜湊（Hash）亂碼？

Hash 用於 DNS 的技術限制，允許在基於 DNS 的攔阻名單中，可使用 Hash 進行修改。Hash 不被視為個人識別資訊（Personal Identification Information，PII），因此需要保護 PII 的法律不適用於 Hash Blocklist（HASHBL）。

- 什麼是 EBL？

EBL（The Email Blocklist）及 HASHBL 均是 MSBL（The Missed Spam Blocklists）組織的一部份，這是一個非營利組織，其目標是鼓勵發展垃圾郵件的防制與管理，並藉此發展利基市場。EBL 運作是利用於允許垃圾郵件受害者對垃圾郵件發送者（Spammer）進行電子郵件地址的阻止列表之建立，蒐集所阻止之列表，並藉由 SHA1 Hashes 方式存儲再加以應用，這裡面也包含了合法的 DNS 網域，並允許 EBL 與現有的域名列表一起運作。EBL（Email Blocklist）是一個，包含 spam 中看到的郵件地址密碼散列，而 EBL 的目的是在攔阻垃圾郵件不能被 IP 或 domain-based 的攔阻名單阻止，是以 EBL 攔阻不會導致誤報。

EBL 上的其他類型的電子郵件地址包含直接發郵人（垃圾郵件直接從一個免費的網路郵件網站的帳戶發送）及批量發郵人（垃圾郵件通過批量電子郵件名單發送到免費批量名單提供商）。

EBL 功能：名單可以自動生成或手動鍵入。白名單和安全檢查不能繞過，除非以管理員身份登錄到主數據庫。EBL 可以自動清除，即在一段時間後，spam 中看不到電子郵件地址，或手動清除，即在誤報或持續列表的情況下，不得自動移除。刪除請求電子郵件刪除須到：ebl-removals@msbl.org，spam 刪除請求在 24 小時內進行審核。

EBL 也有防止誤報、電子郵件地址格式變化、創建 EBL 名單、安全和隱私及處理釣魚網頁（如假冒銀行網頁）的功能，其系統被設計用來協助安全無虞的阻絕垃圾郵件的干擾，亦可透過公開的 HASHBL 資料進行本地端的流量分析，但部分國家因公開的 HASHBL 資料恐有法律層面的考量，因此需藉由當地白名單與 EBL 進行比對的方式查詢使用，避免流量分析後的郵件地址遭到曝光。EBL 在未來的規劃朝向的目標包含有：

- 訊息公布週期的提升，內容將包含惡意郵件（malicious spam）及灰色郵件（graymail）
- 更多的類型及有效的資料蒐集，涵蓋面向更廣泛
- 即時通訊的 ID（例如:Skype）、甚至是電話號碼

肆、檢討與建議

近年來使用者習慣已改變，藉由手機接收訊息已成為常態且高度普及，加上使用便利性及依賴性均遠高於傳統使用習慣，因此手機上的訊息接收（email、簡訊、社群通訊軟體）所衍生的濫發衍生的問題將會更加嚴重，包含亦可能衍生資安、詐騙等問題。大量不請自來之商業電子郵件、垃圾短訊與惡意軟體為害日深，並已嚴重危害網路提供正常通訊的效能，造成個人、企業、國家乃的損失。世界各國已紛訂立專法管制，建議我國亦應加速推動訂定相關專法，以利有效推動垃圾郵件防制相關工作。

日本在誘捕技術的發展上，已開發建置手機裝置垃圾郵件誘捕系統，結合郵件、簡訊舉報功能，藉由 JADAC 組織對民眾的的宣導，未來在本會推動垃圾郵件防制上可借鏡其成功經驗，提升垃圾郵件防制能力。此外，機械學習、深度學習之應用等議題持續發酵，在與時間賽跑的資料分析過程中，如何應用科技輔助來完成大量人力分析工作的可能性，是值得未來在技術面上可以加以考慮的重點。

在過去除了已知巴西、日本普遍透過垃圾郵件誘捕系統蒐集垃圾郵件資料外，於本次會議中韓國 KISA 代表 Bong Ki Hwan 亦分享南韓透過垃圾郵件誘捕獲得垃圾郵件，並進一步進行分析、管理以及與其他國家進行資訊分享，本會在 106 年度已開始建置新一代垃圾郵件管理系統，以及垃圾郵件誘捕系統，建立我國垃圾郵件蒐集、分析之能量，將可與國際運作接軌，以強化我國在垃圾郵件防制積極參與。

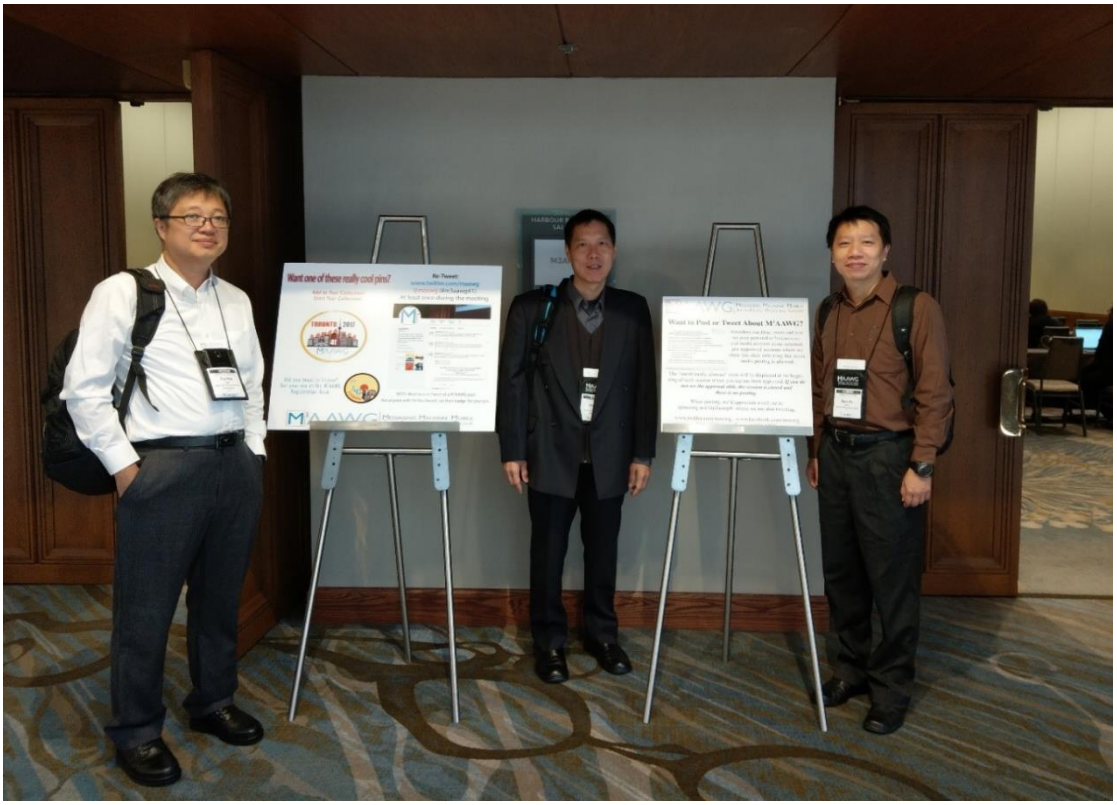
在本次出席 2017 年倫敦行動計畫年度會議中可以看到來自世界各地的出席者，不論是學術界、民間團體、政府，對於訊息濫發防制與管理上不遺餘力，從技術面的角度、法規面的角度、各國執行現況以及未來發展趨勢，為了就是能夠降低非自願性的訊息來源對使用者造成的干擾或影響。在此類國際會議場合中除了有機會可積極分享我國發展近況外，對於國際上對我國執行成效的認可也是一個很重要展現實力的舞台，未來除了提昇技術能量、完善管理規範與治理外，亦可透過實際治理成效與各國交流，促進國際合作以提昇我國國際關係，讓生活在科技發達環境中的網路使用者，能夠擁有安全、乾淨、便利的網路世界。

伍、附錄

與亞太地區發展趨勢會議南韓代表合影

與亞太地區發展趨勢會議香港出席代表合影

與加拿大隱私專員辦公室（Office of the Privacy Commissioner）Trevor Yeo 合影



本會出席人員合影