出國報告（出國類別：開會）

出席2018年不請自來網路組織（UCENet）年度會議出國報告

服務機關：國家通訊傳播委員會
姓名職稱：蘇思漢簡任技正
李福懿技正
派赴國家/地區：美國/紐約
出國期間：**107**年**10**月**6**日至**10**月**13**日
報告日期：**107**年**12**月**31**日

摘要

M3AAWG（Messaging Malware Mobile Anti-Abuse Working Group）是各國聯合起來共同打擊殭屍網路（Botnets）、惡意程式（Malware）、垃圾郵件（Spam）、病毒（Viruses）、服務的阻斷（DoS）攻擊和其他在線攻擊而合作的國際組織。也是一個以科技為主且中立的非政治性國際組織。

本次會議由不請自來網路組織（The Unsolicited Communications Enforcement Network，“ UCENet“）組織，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 “)兩大組織共同舉辦，本會係 UCENet 組織之會員國，其前身為 LAP（The London Action Plan），UCENet 的會員國主要為各國在垃圾郵件防制上的主政機關，共同致力於有關垃圾郵件之「情報」、「法規」、「溝通」、「訓練」等議題上建立共識與交流。

參加這次會議，除了在亞太地區會員國會議中說明我國在防制垃圾郵件上的努力及最新進度，並且安排了臺日雙邊會談，這個會談已經持續了幾年，對於雙邊的合作做出貢獻。在日方 JADAC 的持續邀請下，本會將安排 2019 年赴日進行參訪，以期能在垃圾郵件的防制工作上進一步合作。

目次

壹、前言

M3AAWG（Messaging Malware Mobile[1] Anti-Abuse Working Group）是各國聯合起來共同打擊殭屍網路（Botnets）、惡意程式（Malware）、垃圾郵件（Spam）、病毒（Viruses）、服務的阻斷（DoS）攻擊和其他在線攻擊而合作的國際組織。在全球擁有 200 多名會員國，致力於研究制定合作打擊網際網路資源遭濫用的有效方法。

M3AAWG 是一個以科技為主且中立的非政治性國際組織。主要關注網際網路資源遭濫用的議題，包括科技研發、產業合作和公共政策。會員國包括網際網路服務提供者（IASP）、電信公司、電子郵件服務提供者（ESP）、社交網路公司、硬體和軟體供應商、和許多資訊安全設備廠商。

M3AAWG 一般會議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，再依照不同的領域性（垃圾郵件、廣告簡訊、廣告電話、Do Not Call、RoboCall）分別再依照技術面、政策面、各國現況等不同主題分別舉行相關會議。本次會議由不請自來網路組織（The Unsolicited Communications Enforcement Network，“ UCENet “）組織，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 “)兩大組織共同舉辦，UCENet 的會員國主要為各國在垃圾郵件防制上的主政機關，共同致力於有關垃圾郵件之「情報」、「法規」、「溝通」、「訓練」等議題上建立共識與交流。

[1] Messaging：解決任何訊息傳遞平臺上的濫用問題，從電子郵件到簡訊系統；Malware：垃圾郵件和許多其他形式的傳遞平臺濫用只是傳播媒介，它們的主要目的是利用病毒、惡意代碼或是蠕蟲等惡意行為秘密地感染用戶系統。如果我們阻止上述行為訪問系統，對用戶造成的傷害或影響就會消失；Mobile：保護這個無處不在的平臺，免受惡意程式和訊息傳遞濫用的影響，包括文字和語音服務。

貳、議程

議程		
日期	上午	下午
10 月 8 日 星期一	• UCENet: Asia-Pacific Members Welcome Reception	• UCENet: Planning Workshop • UCENet ExCom
10 月 9 日 星期二	• 臺日雙邊會談	• UCENet: Country Updates • UCENet: Effective Government/Industry Collaboration • UCENet: Canada OPC Case Study
10 月 10 日 星期三	• UCENet: Asia-Pacific Region Updates	• UCENet: SMS Case Studies
10 月 11 日 星期四	• FTC Telemarketing Rules and Enforcement（UCENet Joint Session） • SS7 Attack Detection	

參、會議重點

一、UCENet Asia-Pacific Members Welcome Reception

UCENet Asia-Pacific Members Welcome Reception（亞太會員國歡迎會）會議係由韓國 KISA（Korea Internet & Security Agency）的 Bong, Ki Hwan 經理及 Jo, Insu 研究員共同主持會議，主要是邀集亞太地區的 UCENet 會員國，針對目前各會員國間的垃圾郵件（Spam）議題進行彙總與交流。

會議中提及規劃於 2019 年邀請亞太地區各個會員國共同簽署合作協議，其宗旨主要為協調和促進其他會員國及亞太地區與垃圾郵件有關的問題的國際執法合作和活動，如網上欺詐和欺騙、釣魚和社群網路服務（Social Networking Services，SNS）垃圾郵件，以及未經請求而來的電話和簡訊。

會中通過執行亞太地區業務計畫及採取情報或證據引導的方法，鼓勵和融合政府機構、監理機關之間的參與，以減少垃圾郵件，從而實施有效的合作與協調關係。

主持人並針對亞太地區的運作條款說明如下：

（一） 運作條款適用於亞太區合作國夥伴的 UCENet 運作計劃。

（二） 要求工作小組應盡最大努力制定和實施業務計劃中概述的合作工作項目。

（三） 運作計劃的期限為三年（2019-2021）年。

（四） 工作小組會員國資格的期限由會員國自行決定。

（五） 在 UCENet 年度會議期間（M3AAWG 會議），每年至少召開一次。而工作小組可自行決定舉行會議的頻率。

（六） 會員國們應保障以自己的身份收到的任何資訊不被公開披露，除非此類資訊屬於公共領域。

（七） 會員國可以在整個亞太地區的 UCENet 運作計劃中分享 Spamtrap

（HoneyPot）資訊和其他內容。

此外，KISA 提出以「區域性緊密經濟夥伴（RCEP，Regional Close Economic Partnership）協定」為基礎，由 16 個 RCEP 協定簽署國家，包含東南亞國協（Association of Southeast Asian Nations，ASEAN）10 國（印尼、馬來西亞、菲律賓、泰國、新加坡、汶萊、柬埔寨、寮國、緬甸與越南）以及韓國、日本、中國大陸、澳洲、紐西蘭，共計 16 國共同簽署防制垃圾郵件情資交流聯防計畫。因為少了 1 國，本會蘇思漢簡任技正詢問，主持人說明是印度（RCEP 簽署國），應該是主持人疏漏了。

另因中華民國是 UCENet 會員國，但未列在亞太區會員國清單上，於是本會蘇思漢簡任技正再度提出疑問，為何沒有中華民國，主持人解釋，中華民國不是東南亞國協中的會員國之一嗎？經蘇簡任技正說明中華民國並非東南亞國協之會員國後，主持人表示會將此議題帶回去再確認。

會議中日本代表也對於規劃 16 國簽署合約的討論代表是何人表示並不知情，韓國 KISA 代表則再度表示此議題將會一併帶回去確認相關資訊後，回覆日本及中華民國代表。

經會後以電子郵件詢問日本代表，韓國並未提供任何資訊，另澳洲及紐西蘭代表均表示有關利用 RCEP 協定簽署反制垃圾郵件協議，應該是外交部職掌，並非電信監理機關職掌。

圖 1　亞太會員國合影

二、UCENet Planning Workshop and ExCom

UCENet Planning Workshop and ExCom（規劃工作小組及執行委員會）主持人之一的 Adam Stevens 為英國 ICO（Information Commissioner's Office, UK）情報中心的主管。ICO 的主要工作是保護英國對於訊息、資訊權力之獨立性，維持公共利益，並促進立法的機構。另一位主持人 Sara DePaul 為美國聯邦貿易委員會（Federal Trade Commission, FTC）的職員，亦擔任華盛頓特區的國際消費者保護法律顧問（Counsel for International Consumer Protection Washington, DC）。

本會議對UCENet會員國及有興趣與政府或執法部門合作的M3AAWG會員國開放，主要目標在於減低未經同意的通訊對各會員國造成的影響與傷害。希望透過討論，確保網路的結構合理與有效運作。討論結果將做為下一次 UCENet 運作計劃（2019-2021）之基礎。

會中討論 UCEnet 2016 年至 2018 年之運作計畫，主持人報告運作計畫的內容、UCENet 完成什麼計畫，以及 2018 年至 2020 年需要關注的議題有哪些面向等。

UCENet 雖於 2016 年 9 月 9 日由倫敦行動計畫（London Action Plan，LAP）更名，但仍與倫敦行動計畫會員國共用資訊。UCENet 的運作計畫分為四大類別，包含情報（Intelligence）、執行（Enforcement）、溝通（Communications）及訓練（Training），說明如下：

1. 情報（Intelligence）：期望藉由收集、分析與傳播相關情報或資訊的方式，以利提高 UCENet 會員國間彼此合作效益，並期望可以理解彼此會員國間目前可能的法規資訊。最後希望能夠透過情報共用方式，讓會員國在遭遇事件時，能迅速識別風險與事件資訊，採取應對措施，以合作方式增加應對共同問題或挑戰的處理效率。
2. 執行（Enforcement）：對於所收集到的相關情報與證據，UCENet 需在允

許的時間內進行處置應對，採取適當的行動阻止、偵查及干擾刑事和民事之違法行為，以達成最大化 UCENet 集體權力與保護民眾的目標。

3. 溝通（Communications）：在 LAP 會員國間並與合作夥伴間共用訊息和情報，以促進與提供可靠、安全及有效的方法，包括透過 LAP 備忘錄，以便能夠執行行動計畫；透過文宣和推廣合規與執法之活動。經由促進 LAP 會員國的優勢，確保瞭解各轄區的不同環境，以增進彼此間的合作與協調關係。
4. 訓練（Training）：在年會上為調查人員和研究人員提供有意義的培訓，深入瞭解並規劃一個符合 LAP 會員國間需求與期待的培訓計劃。
5. 會議最後說明 UCENet 針對上述四大類別完成事項的探討與未來規劃，例如 KISA 進一步說明執行委員會會員國之名單，以及創建相關立法之權力等。

三、臺日雙邊會談

2018 年 10 月 9 日我方與日方進行雙邊會談，我方代表為本會蘇思漢簡任技正、李福懿技正、TTC 林高裕經理，日方出席代表為總務省（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）之 Deputy Director Kiyoshi Tokube，以及日本數據通訊協會（Japan Data Communications Association，JADAC）反垃圾電子郵件諮詢中心（Anti-Spam Consultation Center）之 Deputy Director 谷原秀彥（Hidehiko Tanihara）。

日本數據通訊協會（JADAC）為日本總務省委託辦理防制垃圾郵件事務之法人機構。谷原秀彥主要擔任諮詢指導業務之工作，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防制垃圾郵件業務。

本次會談主要討論三項主要議題：（1）日方提供予 HiNet 有關垃圾郵件時間戳記（Timestamp）資訊的運用成效；（2）中華民國數位通訊傳播法的立法現況；（3）關於 2019 年參訪 JADAC 的可行性及相關規劃事項。

（一） 日方提供予 HiNet 有關垃圾郵件時間戳記（Timestamp）資訊的運用成效

1、日方詢問：

JADAC 已經開始提供從 HiNet 發送到 JADAC Spamtrap 垃圾郵件的時間戳記相關資訊，JADAC 想瞭解提供這些資訊是否有相關成效出現。

2、我方說明：

(1) 中華電信是 HiNet 的母公司，表示這些垃圾郵件發送的確切時間與相關資訊，可協助中華電信進一步分析出正確的資訊。中華電信必須有這些確切的證據，才能阻止用戶濫發電子郵件的違規行為。因

此，我們仍建議必須提供有關垃圾郵件的時間戳記等內容資訊，包含發送垃圾郵件的時間以及發送垃圾郵件者的相關訊息。

(2) 若是 HiNet 於 1 個月內檢測到濫發垃圾郵件的行為超過 3 次以上，HiNet Spam 團隊將通過電話或電子郵件的方式先行通知發送垃圾郵件的用戶。通知後，用戶如果仍然持續發送垃圾郵件超過 3 次以上，HiNet 將拒絕用戶的 SMTP 服務（Port 25）。

(3) 說明自 2018 年 9 月 5 日起至 2018 年 9 月 12 日止期間之執行成效為，日方舉報之中華電信用戶濫發郵件 IP 數共 31 組 IP 位址，其中以電話通知用戶的有 6 組；以電子郵件通知用戶的有 12 組；被阻斷服務的有 7 組，而持續觀察的有 6 組。

（二） 中華民國數位通訊傳播法的立法現況：

1、日方詢問：

對於中華民國現在處理垃圾郵件的相關法律－數位通訊傳播法（草案）或濫發商業電子郵件管理法（草案）的發展，在總統交接之後是否有什麼改變？以及目前數位通訊傳播法的最新進度或是相關人的聯繫方式。

2、我方說明：

蘇簡正說明濫發商業電子郵件管理法（草案）已經被擱置，不會再提出，而是用數位通訊傳播法（草案）中的條文，對濫發商業電子郵件進行監管，立法進度為立法院已經在審議。

（三） 關於 2019 年參訪 JADAC 的可行性及相關規劃事項。

1、日方詢問：

JADAC 詢問我方於 2019 參訪 JADAC 的計劃，以及是否獲得核准。若是獲得核准，JADAC 希望確認參訪時間、預計與會者及規劃討論的議題。

2、我方說明：

考量日本的氣候，我方表示希望可以在 5 月或 6 月時參訪 JADAC。與會者則規劃為本會與 TTC 的人員。在討論參訪議程部分，則為本會對於垃

圾郵件議題的最新目標與相關計畫，另外 TTC 已開發有關 Spamtrap 的新系統，或許可以與日本針對此系統進行交流與討論，由技術人員負責軟體部署事宜，並請 JADAC 協助維護，以共享雙方獲得的垃圾郵件情資。

圖 2　臺日雙邊會談

四、UCENet Country Updates

UCENet Country Updates（會員國進度更新）會議安排有三位講者，第一位為 Peter Merrigan，他為紐西蘭防衛產業協會（New Zealand Defense Industry Association，NZDIA）高級調查員，第二位是 Adam Stevens，他是英國資訊委員辦公室（ICO）情報中心主管，第三位是 Sara DePaul，她是美國聯邦貿易委員會（FTC）華盛頓特區的國際消費者保護法律顧問。

本會議的目的是由各 UCENet 會員國說明各國與不請自來(unsolicited)通信內容有關的法律、法規、科技和其他進度之更新。在各國資安法規的陸續出爐情形之下，歐盟一般資料保護規則(General Data Protection Regulation，GDPR）與資料保護法（Data Protection Act 2018，DPA18）所造成的影響也逐漸明顯。從 Peter Merrigan 提供的數據可以瞭解因應的各種法規，例如數據保護違規(Data Protection Breach)的案件日漸攀升，從 2018 年 4 月的 485 筆，幾乎為倍數提高至 5 月的 806 筆，至 6 月甚至達到 1,855 筆。但是這些案件並非突然產生，而是在 GDPR 實施後才被發現，換言之，未被發現的事件應該大於表面呈現的數字。

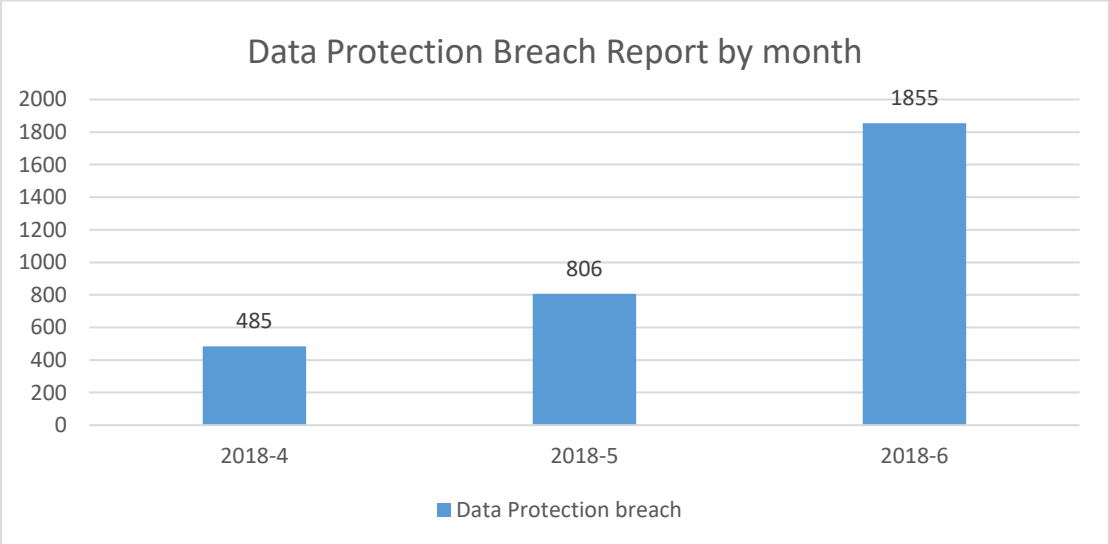

圖 3　資料保護違規月報數據

英國資訊委員辦公室(ICO)提供的數據則聚焦在隱私及電子通信法上，從下圖可知在總數 10 萬餘筆的資料中，簡訊（SMS）有 14,065 筆，佔總數約 13%；自動撥號（Automated Calls）有 40,993 筆，佔總數約 38%；直接撥號（Live Calls）最多，有 52,309 筆，佔總數約 49%。根據 ICO 的數據顯示，自動撥號與直接撥號的事件，更有逐月上升的趨勢，這些數據在在顯示因科技日新月異，導致這些不請自來的訊息只會不斷的增加，因此，如何有效防制已是需要關注的重點。

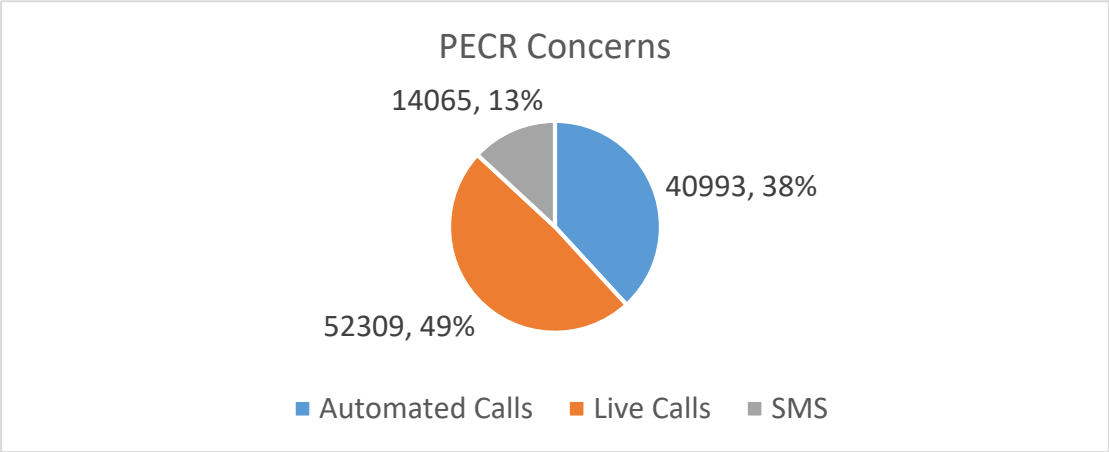

圖 4　隱私及電子通信法關切事件數量

五、UCENet Effective Government/Industry Collaboration

UCENet Effective Government/Industry Collaboration（政府或產業有效合作）會議主要在說明美國政府和各企業會員國間，以及紐西蘭政府與各企業會員國間，如何有效合作打擊非法不請自來的通信內容。會議主講者共有四位，分別為美國聯邦貿易委員會（FTC）的 Ian Barlow、紐西蘭防衛產業協會（NZDIA）的高級調查員 Peter Merrigan、美國電信協會的 Kevin Rupsy、美國聯邦通信委員會（FCC）的 Kristi Thompson。

會議中談及政府有時候會與特定企業合作，打擊或阻絕某些未經允許自來的通訊內容。合作方式包含分享某些特定的資訊及提供可能的證據來源。在分享某些特定資訊部分，FTC 於 2017 年起，就開始了一項新的措施，此措施會公告業者們發生或被利用來發送垃圾訊息的事件數量或頻率，期望能藉由公告數據的方式，讓業者可以自律並改進自身的運作機制。另外也鼓勵大家利用具阻擋功能的 APP 應用程式。

六、UCENet Canada OPC Case Study

UCENet Canada OPC Case Study（加拿大 OPC 案例研究）會議之講者為加拿大隱私委員辦公室（Office of the Privacy Commissioner of Canada，OPC）的 Tauqeer Shaikh，他介紹加拿大 OPC 最近對一家國內公司審理而且成功的案例，並說明運作的機制與原理。

案例中的公司開發了一個程式，該程式一旦安裝在個人電腦上，就會追蹤用戶的線上搜索查詢，並將結果與用戶的朋友和社交媒體網路上的各聯繫人共用內容的其他搜索結果作關聯分析，以獲得他們想要的資訊。此程式還會根據個人的線上搜索顯示有關連性的廣告。

散播方式主要是藉由協力的軟體開發廠商安裝，當用戶下載一些與此程式毫無關聯的免費程式時，該程式會假裝為一個附加的外掛程式被一同安裝在電腦上。Tauqeer Shaikh 針對此案例之運作原理及 OPC 後續的追蹤進行相關的說明與展示。

七、UCENet Asia-Pacific Region Updates

UCENet Asia-Pacific Region Updates（亞太地區進度更新）會議，是由韓國 KISA 發起並主辦的亞太地區發展趨勢會議，僅由會員國的監理機關參與，以分享最新進度。本次邀請報告之會員國包含中華民國、日本、韓國等，分別就各會員國的垃圾郵件處理現況進行報告。報告者的重點摘要如下：

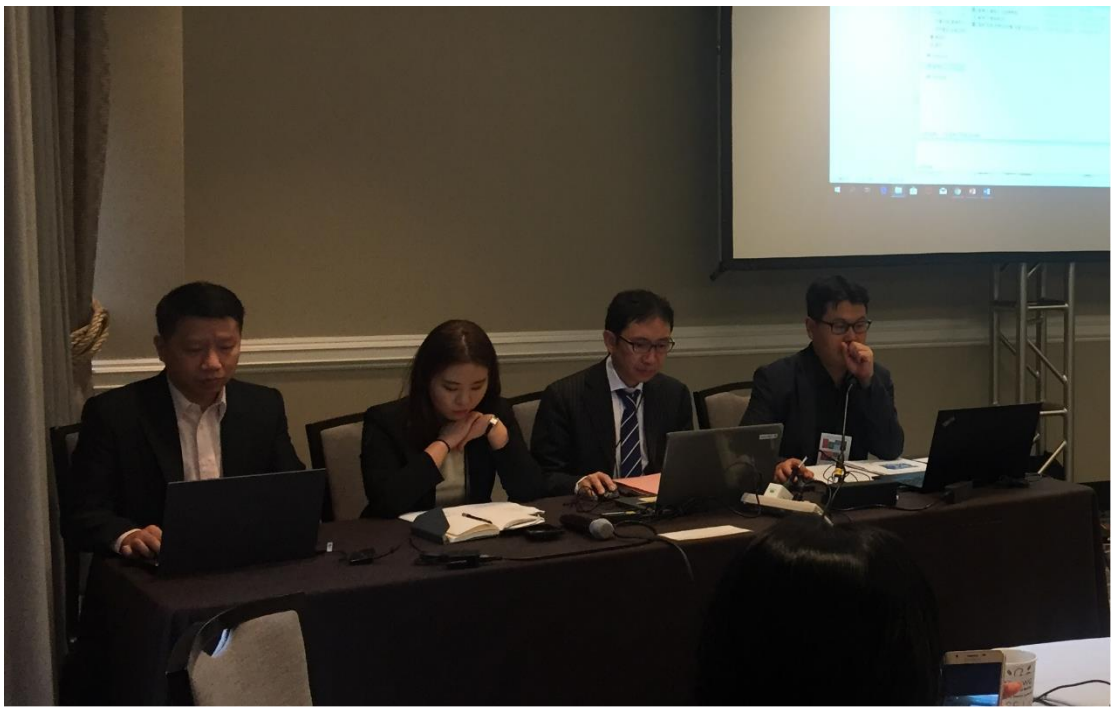

圖 5　左起為中華民國代表林高裕經理、韓國代表、日本代表及主辦者

1. 日本

日本總務省（MIC）電信局的 Kiyoshi Tokube 先簡單扼要地說明日本目前的垃圾郵件（Spam）統計情形，以及藉由誘捕系統取得其他來源國之垃圾郵件統計數據。Kiyoshi Tokube 提到，根據 SOPHOS 統計的數據顯示，亞洲地區是世界上發出垃圾郵件第二嚴重的地區。日本收到的垃圾郵件，以中國大陸和韓國為最主要的來源國，其餘亞洲國家，如菲律賓、印度和泰國，也位列前十名。因此，亞洲地區之防制垃圾郵件作為，已經成為一個非常重要的議題。

Kiyoshi Tokube 並提到日本現行的法規現況，反垃圾郵件法已於 2002

年開始執行，法規重點有，禁止未經收件人同意發送廣告郵件、禁止向拒絕此類廣告的人發送電子郵件、保留收件人同意紀錄的義務、禁止利用假造的寄件者資訊發送電子郵件、禁止向虛構地址發送電子郵件等。

在垃圾郵件的防制方式上，Kiyoshi Tokube 則說明有關 MIC 的防制流程，即是當垃圾郵件收件人或是反垃圾郵件諮詢中心（Anti-Spam Consultation Center）自身收到垃圾郵件時，收件人將相關資訊提供予反垃圾郵件諮詢中心以確認是否違反了反垃圾郵件法。若有違法事實，則 MIC 會先向垃圾郵件發送者發送警告郵件，如垃圾郵件發送者未發現或回應此警告郵件，MIC 接著會發出一紙行政命令，當垃圾郵件發送者違反此行政命令時，便有可能受到相關處罰。

在反垃圾郵件法的執行與影響上，近幾年統計中，當垃圾郵件發送者收到警告或相關命令時，大多會停止發送垃圾郵件，因此，當前的行政命令數量比以前減少許多，由於相關數據涉及機敏資訊，故不便提供。

最後，Kiyoshi Tokube 針對去年所提到的 DMARC[2]（Domain-based Message Authentication, Reporting and Conformance）系統執行現況進行說明如下：（1）第一項為各部會及機構制定其資訊安全政策和標準，這些政策和標準應符合政府安全局所制定之標準。（2）第二項為 DMARC 在 2018 年被推薦為符合標準的電子郵件技術之一，用於發送和接收更多合法的電

[2]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。網域管理員可以在功能變數名稱系統公佈相關政策，讓外界得知旗下功能變數名稱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瞭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。

子郵件。（3）第三項為根據 MIC 從 1 月份起調查的最新結果，日本政府部門網際網路域名 go.jp 的實施率約為 1%。目前 MIC 也正在努力敦促政府部門與相關機構採用 DMARC，並期望將其擴展到企業領域。

2. 韓國

韓國 KISA 的 JEESOO JEON 擔任講者，她說明 KISA 負責的事務包含了網際網路的推廣與網路安全的管理，像是韓國 IP 網址的管理、網路事件的處理、民眾個資的防護、網路安全人才的培訓，以及非法垃圾郵件的處置等。韓國期望藉由此種綜合管理的方式達到有效減少網路犯罪（如語音釣魚、網路詐騙）事件的發生，以減少對民眾的傷害。

韓國對於垃圾郵件的立法則注重下列幾項重點：（1）必須收件人同意才可以發送郵件；（2）應附上寄件人相關資訊（姓名或連絡訊息等）；（3）應提供拒絕接收的方式；（4）當收件人拒絕收到相關信件時，發信人不得向其收取其他額外費用；（5）當收件人拒絕接收垃圾郵件後，發信人便不得再向其發送垃圾郵件；（6）特定時段（晚間 9 點至早上 8 點）必須取得收件人的同意才可以發送垃圾郵件。

對於非法垃圾郵件的管理，韓國有三項實施策略：

（1） 善用具備「簡易回報服務[3]」的行動裝置提高民眾的便利性。

（2） 利用 CID 認證系統加強對偽造來電號碼的檢測，許多非法貸款、賭博等垃圾郵件，都會利用修改原始來電號碼的方式來躲過監測，因此會希望藉由網路營運商的角色，進行原始來電號碼的檢測並藉以規範垃圾郵件發信者的違法行為。

（3） 利用 Spamtrap（Honeypot）系統與垃圾郵件監控系統加強對垃圾郵件的偵測與應對處置。韓國建置了 18,000 組的虛擬號碼與 130,000 組的虛擬電子郵件帳號誘捕非法垃圾郵件。截至 2017 年底，共偵測到將

[3] 簡易回報服務（Easy Report Service）於 2007 年開始提供服務，在將近 30.28 億個 SPAM 案例中，有將近 99%的案例是利用此服務進行回報。（維基百科）

近 4,500 萬次的非法垃圾郵件發送行為。垃圾郵件監控系統會利用這些資訊，對於非法發送垃圾郵件的電子郵件之地址、IP 位址或電話號碼實施封鎖或撤銷作為。

3. 中華民國

中華民國負責簡報的講者為財團法人電信技術中心的林經理高裕，他就我國現行的法規與國家通訊暨網際安全中心（National Communications and Cyber Security Center，NCCSC）說明最新進度，包括我國關鍵電信基礎設施（CTI）及關鍵資訊基礎設施（CII）最新應處機制之 NCCSC，係由 C-NOC（負責 CTI 聯防），以及 C-SOC、C-ISAC、C-CERT（負責 CII 聯防），共計 4 個平臺組成。而針對垃圾郵件則為 CII 聯防的子平臺，包含下列三大功能系統：

（1） 監控系統：以 7x24 方式監控國內 IASP 業者與誘捕系統 Spamtrap 之垃圾郵件活動。

（2） 共享系統：針對國內各 IASP 與合作國間之垃圾郵件情資進行交換。

（3） 告警系統：當資安事件發生時，可即時通知處理人員，降低事件造成之危害。

透過其中的 C-SOC 與 C-ISAC 平臺，可以利用下列三種方式達成反垃圾郵件之目的：

（1） 監控、分析並通知 IASP 業者處理資安事件與垃圾郵件。

（2） 監控並分析惡意之郵件，以瞭解網絡釣魚網址（URL）和惡意程式 Hash 值等情資。

（3） 從 IASP 業者獲取有關資安事件處理結果之報告提供給 C-ISAC，以獲取更多情資。

為了讓協助 NCCSC 負責垃圾郵件的技術研究人員瞭解垃圾郵件資訊交換現況，我國開發了垃圾郵件分析管理系統（Spam Analysis Management System），可透過視覺化的方式顯示垃圾郵件傳輸狀態。

經過長時間的研究設計，我國產出一種利用 Relay 技術開發之誘捕系統，命名為 Spamtrap，用於檢測和收集垃圾郵件。其中與垃圾郵件發送者建立此系統之信任是 Spamtrap 最關鍵的問題，目前正在研究與垃圾郵件發送者建立信任關係的更好方法，所有垃圾郵件發送活動都可顯示在系統儀表板上，可同時顯示數量最多的前 10 名國家或地區。

八、UCENet SMS Case Studies

UCENet SMS Case Studies（簡訊服務案例研究）會議提供執法機構瞭解各會員國對於不請自來簡訊的監理、調查、執法、相關技術及案例研究的最新進展。紐西蘭 NZDIA 高級調查員 Peter Merrigan 一開始就針對前 5 名數量的簡訊為主題進行分析，垃圾簡訊與 5 種主題有關，分別為賭博、債務管理、銀行業務、事故索賠與金融貸款，而這 5 種就是目前最多的垃圾簡訊內容。

另外，他也提出三個案例：ppa-xplosion Ltd、514-ticket case selection 及 ic0-costelloe and Kelly limited 與大家分享。

第一個案例：ppa-xplosion Ltd 事件係 Xplosion 利用被稱為 clickjacking 的手法，讓成千上萬的用戶在瀏覽網頁時，因為隱藏的「同意收費」按鈕，造成在不知情的狀況下，訂閱了不感興趣或無意義的垃圾訊息，並向用戶的行動裝置每週強制收取 4.5 英鎊的費用。此案件讓這家名為 Xplosion 的公司被監理機關處以超過 100 萬英鎊的罰款，以杜絕防止這種造成大量用戶受害的情況再度發生。

第二個案例：2018 年 5 月 1 日加拿大廣電及電信委員會（Canada Radio and Telecommunication Commission，CRTC）以新聞稿宣佈，514-TICKETS[4] 公司已經承認涉嫌違反加拿大反垃圾郵件法（Canada Anti-Spam Law，CASL）。而負責營運 514-TICKETS 的公司承諾支付 10 萬美元的財務賠償金（向加拿大接管人支付 2.5 萬美元，向客戶提供 7.5 萬美元的退款優惠券）。

CRTC 的創新制裁形式，結合客戶賠款和罰款，目的不是要懲罰違法者，而是強迫他們採用符合 CASL 的做法，這是 CASL 實施合規計劃中強調的

[4] 514TICKETS 主要活動是轉售體育，文化和活動門票。

一種制裁方式。

第三個案例：ic0-costelloe and Kelly limited 事件則是有關 Costelloe and Kelly Ltd 違反了 2003 年隱私和電子通信指令第 22 條，即未經用戶有效同意，進行直接的簡訊行銷活動。

在一般民眾對於垃圾郵件的防制議題上，Peter Merrigan 說明了數種現行已於某些特定區域運作的建議方式，如 7726 門號、回報資訊給某些防制垃圾郵件的單位，如英國 ICO、美國 FTC 及美國 FCC，也可直接以用戶的手機 App 進行電話封鎖。

7726 的運作機制是利用大眾回報的資訊為基礎，將回報資訊彙整後，當作日後過濾垃圾郵件的標準。許多電信業者（包括美國四大電信業者 Verizon、AT&T、Sprint、T-Mobile）允許用戶利用將垃圾郵件轉發至 7726 門號的方式來提供是否為垃圾郵件的訊息。

雖然電信業者不一定會立即阻止垃圾郵件發送給用戶，但就像在 Gmail 中回報垃圾郵件一樣，它可以在未來幫助所有人過濾郵件。另一種選擇是報告給某些防制垃圾郵件的政府機關，這些機關可以對嚴重違反隱私和電子通信規則（Privacy and Electronic Communication Regulation，PECR）的違規行為罰款，最高額度為 50 萬英鎊。

2013 年，一家發薪日貸款公司被發現發送了數百萬條垃圾簡訊，因此被罰了 17.5 萬英鎊。英國的 ICO 可以查看在國內或代表英國公司發送的簡訊。不過有些消息是由英國以外的公司或以匿名帳號所發送，確實會提高預防或懲罰的難度。

Peter 也提到利用 App 封鎖的方式，來確保用戶不會從特定號碼得到垃圾訊息或不請自來的電話，最直接的方法是明確地封鎖該號碼。這樣也會阻止來自這些門號的呼叫。

但是仍有許多公司利用多個或隨機的模擬帳號及門號發送垃圾郵件，以增加發送垃圾訊息的效率與成功率。因此封鎖惡意的門號或帳號並不能保

證用戶不會再次收到垃圾郵件或訊息。不過若能確實對每個惡意來源執行封鎖，仍可阻斷一些已知的騷擾行為。

九、FTC Telemarketing Rules and Enforcement

FTC Telemarketing[5] Rules and Enforcement（電話行銷規則與執行）會議由 FTC 的 Ian Barlow 說明 FTC 對於 Robocall[6]、Do not call[7]與 Spoofing 之規範。

FTC 統計 2018 年至今最新的數據，有關 Robocall、Do not call 與 Spoofing 的案例總數為 139 筆，被成功解決的有 126 筆，其中 Robocall 佔 49 筆；Spoofing 佔 30 筆。

Ian Barlow 並提到在一些例外情形，例如建立書面協議、有業務關係之特殊情況下，上述方式的電話行銷是可以被允許執行的。

[5] Telemarketing（電話銷售）：電話銷售是一種直銷模式，一般是銷售人員通過電話向潛在的客戶推銷商品和服務。電話銷售有時候也使用電話自動撥號，然後錄音播放錄音的方式。電話銷售的消極方面是經常和各種詭計和詐騙聯繫在一起，比如層壓式推銷、價格不合理的劣質貨品或假貨，亦有電話行銷者頻密緻電目標顧客，令對方感到滋擾。（維基百科）

[6] Robocall：一種通過電話來達到宣傳目標的形式，通過電腦控制實施自動撥號，播放預先錄製好的音訊。這種方式大大提高了傳統電話宣傳效率，通常用於電話銷售，總統選舉等。（維基百科）

[7] Do not call：美國謝絕來電計劃（英語：National Do Not Call Registry）旨在讓美國消費者少收到錄音電話促銷。消費者可撥打 1-888-382-1222 註冊該計劃。謝絕來電計劃從 2003 年開始設立，但因有異議延誤至 2004 年實行。（維基百科）

十、SS7 Attack Detection

SS7[8]Attack Detection（SS7 攻擊檢測）會議由美國佛羅里達大學的教授 Brad Reaves 以「Sonar: Detecting SS7 Redirection Attack With Audio-Base Distance Bounding」分享研究成果。

目前全球電信網路之通訊量每日高達數十億筆，其運作之核心主要是透過 SS7（Signaling System Number 7）協定來建立通信、管理行動裝置連線、其他許多網路服務。而 SS7 協定的制定基礎是建立在少數可信任對象與核心網路基礎設施建立通信之上。

在 SS7 協定中，因行動裝置通信的特殊需求，故允許具有核心存取權限的使用者在世界任何地方可以攔截或重新轉向使用者的通訊內容，甚至任意修改語音通訊內容，新增噪音或中斷通信，得知使用者所在之地理位置資訊。但這也是 SS7 協定的弱點，因為會使整體仰賴此協定的電信網路與全球各地一般使用者面臨巨大的風險。

會議中，是由佛羅里達大學的教授分享如何安全的針對 SS7 協定的重新轉向與非法攔截等攻擊行為進行偵測之相關研究成果。他們研發了一套名為 Sonar 的系統，可針對兩個通訊端的語音往返時間進行檢測，能夠有效地偵測 SS7 轉向攻擊（Redirection Attacks）。

他們在研究中發現，SS7 轉向攻擊將無可避免的導致兩個通訊端的信號往返距離變長後，將導致延遲時間拉長，因此，若能進一步偵測出兩通訊端信號往返時間上產生異常，就能偵測出 SS7 轉向攻擊。

[8]第七號發信系統（SS7，Signaling System Number 7）是一種被廣泛應用在公共交換電話網、蜂窩通訊網路等現代通訊網路的共通頻道信號系統。第七號發信系統是國際電信聯盟推薦首選的標準信令系統。為了實現電信業務的互聯互通，不同通訊運營商之間，特別是不同國家的運營商之間都會採用第七號發信系統控制運營商之間業務交換的過程。許多的通訊運營商也在自己的通訊網路裡面使用第七號發信系統實現計費、漫遊或者其他電信業務。（維基百科）

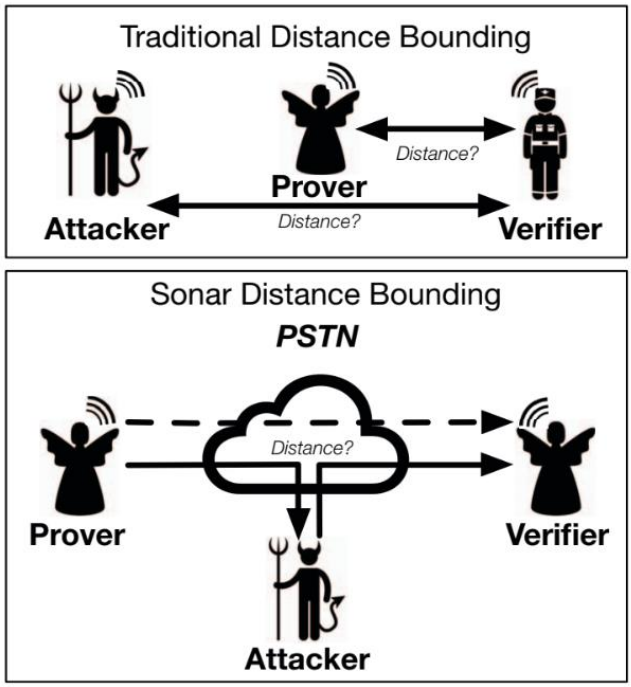

圖 6　SS7 轉向攻擊之檢測示意圖

在 TCP/IP 協定的網際網路中，要測量封包往返時間與距離，有許多軟體工具，例如 Traceroute、Ping 等可以利用，相較於 TCP/IP 的網際網路世界，SS7 協定的電信網路，就沒有類似的軟體工具可以利用，即使有，也不支援類似追蹤通信路徑的功能。

兩個通訊端之間傳輸的資料就僅有語音訊號，如何準確地測量兩個通訊端的語音訊號傳遞距離的差異是最大的難題。在跨網路的通訊中，如 VoIP 語音通訊與傳統電信網路間的語音通訊，本身就存在各種延遲時間，例如 TCP/IP 層的封包傳遞時間、邊界路由器的封包處理時間、既有公眾交換電信網路（PSTN）資訊傳遞時間等，都會產生延遲。而語音訊號的延遲問題不管是 VoIP 電話或 PSTN 中都是存在的，而 PSTN 的語音訊號延遲問題甚至高於 VoIP 電話。

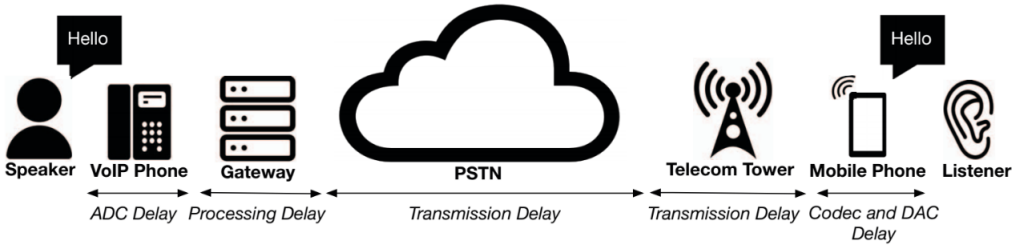

圖 7　語音訊號在各種網路之延遲示意圖

佛羅里達大學研究團隊於實驗室中建立了一個研究模型，藉此模擬 SS7 轉向攻擊。透過 VoIP 客戶端及 VPN 伺服器，並使用 PBX（Private Branch Exchange）用戶交換器與 GSM 閘道器（Gateway）連線後，進入公眾交換電信網路（PSTN），最終語音訊號透過 GSM 音訊迴路（Loopback）設備回送。在這個研究模型中，就是透過切換不同的 VPN 伺服器來模擬 SS7 轉向攻擊的語音訊號延遲狀況。

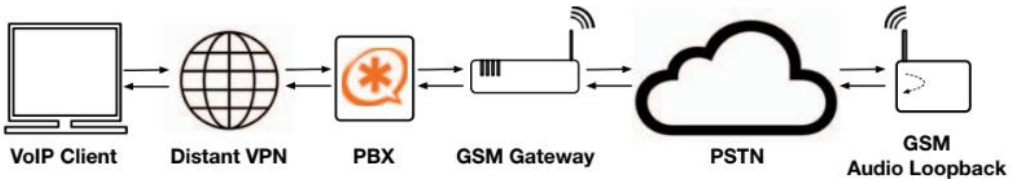

圖 8　語音訊號模擬的轉向攻擊模型示意圖

研究結果顯示正常的兩端通訊之間的語音訊號延遲，與模擬的 SS7 轉向攻擊語音訊號延遲有著顯著的差異。

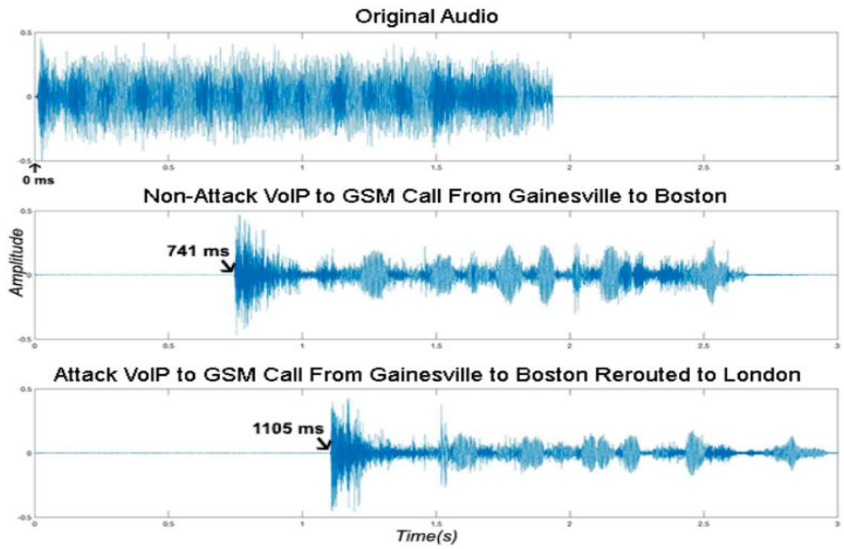

圖 9　語音訊號轉向攻擊實際與模擬的時間延遲

研究團隊進一步擴大研究規模，希望驗證這套偵測機制的可行性，因此利用特殊的儀器在電信網路終端，進行語音訊號延遲時間的監控，包含微控制器、LCD 顯示器、GSM 數據機、控制按鈕等，建構出一套名為 Sonar 的系統，並利用這套系統，在美國電信業者及以色列的研究夥伴在許可下，於真實的電信網路環境實現 SS7 轉向攻擊的實驗。

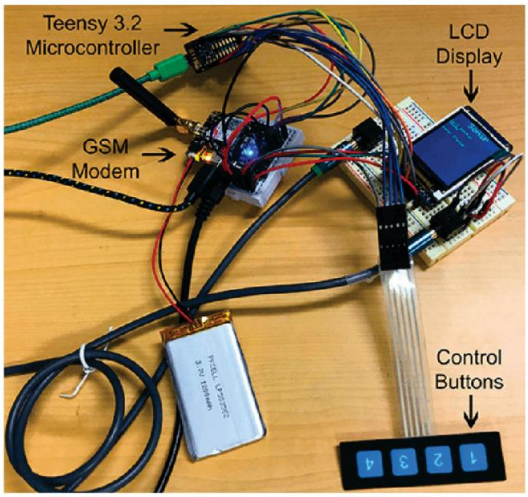

圖 11　語音訊號轉向攻擊的 Sonar 系統

在電信業者的協助下，研究團隊操作 SS7 轉向攻擊，將語音訊號從北卡羅萊納州轉向導到加州舊金山，再返回原先的通信路徑，並記錄整體語音

訊號的時間延遲狀況。

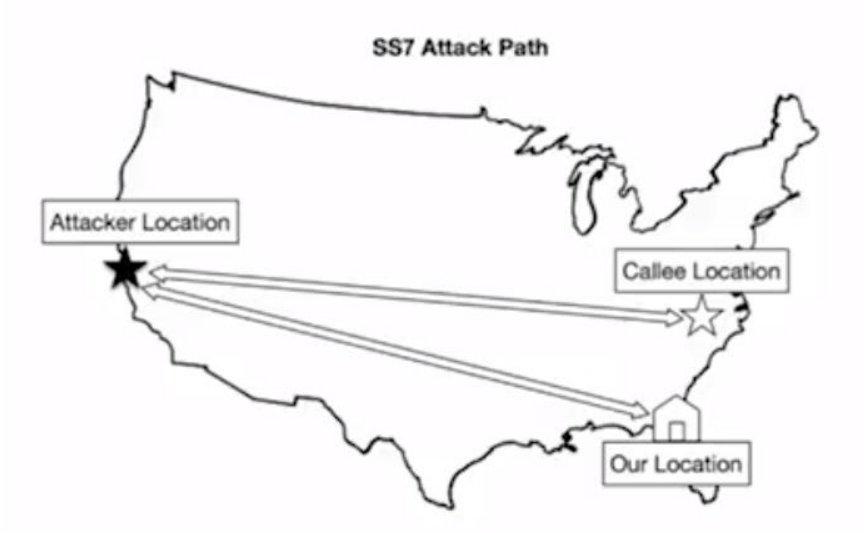

圖 10　SS7 轉向攻擊的導向路徑示意圖

研究結果顯示，在真實環境中重現的 SS7 轉向攻擊，確實能夠透過語音訊號的延遲時間中，判斷出明顯的差異，同時也驗證了這個偵測概念確實可行。除了部分特殊案例，例如攻擊者與受害者地理位置十分接近，導致無法從語音訊號的延遲時間中觀察之外，基本上，這項偵測技術在真實電信網路環境確實可行。

透過佛羅里達大學分享的偵測技術，除了讓我們更瞭解 SS7 轉向攻擊的原理與架構外，亦獲得透過不同角度，來思考防禦這類型攻擊的可能性，藉此提高我國整體電信網路的安全性。

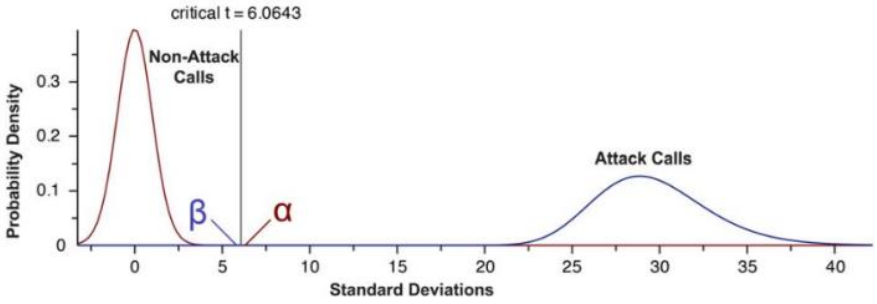

圖 12　SS7 轉向攻擊的機率示意圖

肆、心得與建議

拜科技的日新月異所賜，人手一機的生活方式已經默默改變人們的生活型態。近年來資訊產品使用者的習慣已經改變，傳統許多需要利用桌上電腦或筆記型電腦才能完成的事物，現今利用手機或平板電腦都可以完成，舉凡像是接受電子郵件、視訊通話及遠端會議等。

利用行動裝置接收多樣化的訊息已成為生活常態且已高度普及，加上便利性及依賴性均遠高於使用電腦的傳統習慣，因此，衍生出手機接收到濫發的電子郵件、簡訊、社群訊息等問題，也會日趨嚴重，而且也衍生出資安、詐騙等問題。

本次參與 UCENet 會議可以瞭解訊息濫發的議題，在各國都已經形成重大的問題，不僅僅是政府，民間團體與學術界針對類似的議題都在竭盡所能進行研究與管制。學術界與民間團體研究技術面的防制手法，政府機關則由法規面著手，並對各會員國目前與防制進度及技術情報進行交流，交換彼此的經驗，以期許各會員國都能夠更有效率地防制對用戶造成困擾及影響的濫發訊息。環顧世界各國已紛訂立專法管制，本會函報行政院送立法院審查之「數位通訊傳播法」草案對於商業電子訊息已納入規範，建議未來完成立法後應加速推動辦理。

與日本溝通交流，得知日本之垃圾郵件即時防制相關機制已相當完整，日方亦歡迎我國派員至日方相關單位進行訪問及技術交流，本會已於 107 年完成資安監控分析通報平臺建置，建議未來可就防制垃圾郵件及技術交流，適時雙方互訪，以加深雙方合作關係，並強化防制成效。

我國在此一國際會議場合上，則可增加與各會員國交流的機會，並藉此累積我國的技術專業與知名度，獲得其他國家對我國執行成效的認同。在與各會員國交流後，亦可持續吸收技術、法規、監理及經驗的新資訊，以加

強我國對於垃圾資訊的防制能量。期許在持續參與 UCENet 會議的過程中，加強與會員國彼此的合作關係，共同讓各會員國的民眾享有一個乾淨安全的網路環境。