出國報告(出國類別：參加國際會議)

出席「第四屆倫敦行動計畫及垃圾郵件主管機關聯繫網絡（LAP/CNSA）研討會及第六屆德國反垃圾郵件高峰會」會議報告書

服務機關：國家通訊傳播委員會

姓名職稱：專門委員 黃文哲、

科長 蘇勇吉

派赴國家：德國威斯巴登

出國期間：97 年 10 月 26 日至 31 日

報告日期：98 年 1 月 20 日

出席「第四屆倫敦行動計畫及垃圾郵件主管機關聯繫網絡(LAP/CNSA)研討會及第六屆德國反垃圾郵件高峰會」會議報告書目錄

壹、前言

近年來，垃圾郵件肆虐於網路環境為害日深，除造成網路服務提供者系統極大之額外負擔外，對於一般網路使用人亦形成不小的困擾，94 年 11 月消費者文教基金會針對台灣地區的問卷調查表示，每個網路用戶一年要花費 30 小時刪除垃圾郵件，如以每人每小時新臺幣(以下同)100 元工資推估即達 440 億元，顯見垃圾郵件造成我國整體社會成本極大的損失。另一方面，由於電子郵件無國界的特性，大量的垃圾郵件亦不斷地對國外輸出，直接造成他國的困擾，使我國成為垃圾郵件輸出大國，嚴重損及我國科技矽島之國際形象。

國家通訊傳播委員會(以下簡稱本會)有鑑於垃圾郵件氾濫情形嚴重，亟待政府加強管理，除參酌各國立法例及國內網路現況，研擬「濫發商業電子郵件管理條例草案」，以作為建構國內商業電子郵件法制環境之基礎外，復審酌濫發行為之防制，一方面須聯合國內業者組成技術防制網絡，另一方面亦應加強國際合作交流，以阻斷跨國濫發行為。而藉由參與國際合作交流實務經驗，除可強化技術防制網絡，更可對國際間宣示我國防制垃圾郵件決心，提升我國國際形象。

本會為積極參與國際防制垃圾郵件相關組織及活動，於 94 年 8 月 4 日即以「台灣」名義加入「倫敦行動計畫」，並派員參與其年度會議，以蒐集各國防制垃圾郵件策略及未來發展，同時尋求建立國際合作交流關係。本次 97 年 10 月 26 日至 10 月 31 日於德國威斯巴登舉辦之「第四屆倫敦行動計畫及垃圾郵件主管機關聯繫網絡研討會及第六屆德國反垃圾郵件高峰會」，已係我國加入該計畫後第 3 次參與之國際性工作會議，本會特指派黃文哲專門委員及蘇勇吉科長出席會議，為加強業界參與，並協調財團法人電信技術中心派員協同出席(參閱附件 1)。

本次會議之研討議題極為廣泛，而由於垃圾郵件種類涵蓋面向除了商業用途外，亦不乏涉及犯罪之問題，且已有多項議題與網路詐騙及網路安全相關，除本會監理業務外，同時牽連其他主管機關之職責，較為重要之議題包括：網站安全、日本電子郵件管理法規之修正、網路犯罪、電子郵件管理法規之比較、網路(預付金)詐騙等多項議題。本報告書將就本次會議重要議題及內容加以摘要說明。

貳、「第四屆倫敦行動計畫及垃圾郵件主管機關聯繫網絡（LAP/CNSA）研討會及第六屆德國反垃圾郵件高峰會」

1、會議時間、地點及議程

時間：97 年 10 月 26 日至 10 月 31 日

地點：德國威斯巴登

議程：詳附件 2

2、主要議程

本次「第四屆倫敦行動計畫及垃圾郵件主管機關聯繫網絡研討會及第六屆德國反垃圾郵件高峰會」會期 3 天半，分為 10 月 27 日舉辦的「倫敦行動計畫及垃圾郵件主管機關聯繫網絡（LAP/CNSA）技術性訓練工作會議」(LAP-CNSA Technical Training Workshop)、10 月 28 日至 10 月 29 日舉辦的「第六屆德國反垃圾郵件高峰會」(6th German Anti Spam Summit)及 10 月 30 日上午舉辦的「執行會議」(Enforcement meeting - Technical mitigation)3 個主題之議程，其中，由於 10 月 27 日之部分會議資料，因涉及政府執行垃圾郵件結合網路犯罪之案件調查實務細節，並未對外公開，10 月 30 日上午議程因限於預算經費因素未能參加，及部分講者並未授權會議主辦單位得提供會議資料，是以，本報告將僅就得獲公開資料部分之議題加以簡述：

(1) 倫敦行動計畫及垃圾郵件主管機關聯繫網絡（LAP/CNSA）技術性訓練工作會議

本議程係主辦單位採納倫敦行動計畫多數會員之建議，鑑於垃圾郵件之防制工作，在許多國家仍在起步階段，然而垃圾郵件已漸漸與網路犯罪行為掛鉤，調查處理行動已趨於複雜化，並同時跨多個主管權責機關，為奠定執行人員之基礎素養，強化技術層面之專業判斷能力，同時參考先進國家之實際案例執行作法，乃辦理此項議程。

當日議程分為初級及進階兩種議程，初級議程包括：介紹網際網路運作基礎常識、垃圾郵件事件調查之基本要素及細節、如何透過法律手段針對垃圾郵件及間諜軟體加以行政管理(共同議程)。進階議程包括：跨國垃圾郵件結

合網路犯罪實例探討、間諜軟體之調查實務、被動式 DNS 複製(Passive DNS Replication)、如何透過法律手段針對垃圾郵件及間諜軟體加以行政管理。

✓ 議程 1：介紹網際網路運作基礎常識

介紹網路位址(IP 位址)及 IP 架構、網際網路與內部私人網路路由、traceroute 揭示訊息、網域名稱伺服器、DNS 查詢、PTR 紀錄與反解、常見之服務－HTTP、DNS、SMTP、FTP、網際網路屬性之登錄及 WHOIS 查詢、電子郵件與網頁之運作、惡意軟體、殭屍網路、垃圾郵件、網頁感染等常識。

✓ 議程 2：介紹垃圾郵件事件調查之基本要素及細節

透過主辦單位提供之軟體工具，實際分析垃圾郵件，比較垃圾郵件與正常郵件信首資訊之不同，並追蹤郵件訊息路徑，使用 WHOIS 查詢以取得訊息來源處之管理人員。

✓ 議程 3：透過法律手段針對垃圾郵件及間諜軟體加以行政管理

由加拿大工業部、荷蘭 OPTA、澳大利亞 ACMA、美國 FTC、紐西蘭 DIA 等機關代表，各以 5 分鐘分就其國家對於垃圾郵件及間諜軟體之現階段管理態度加以簡略口頭說明。

✓ 議題 4：跨國垃圾郵件結合網路犯罪實例探討

本議題分別由澳大利亞 ACMA 及美國 FTC 代表 Chris Duffy 及 Steven Wernikoff 報告 Herbal King 案例，說明目前 spammer 常利用殭屍網路、代理伺服器等方式隱藏發信點，同時網路犯罪已逐漸組織化、專業分工，網域名稱與廣告網站亦均互相隔離，且不與成員有所關連，整體案例之調查方向，由傳統之郵件追蹤調查，轉為網路金流流向追查，調查小組需整合多個主管機關之人力及專業，而未來之挑戰在於：需由大量電子或實體事證資料中分析有用資訊、事件 business model 越來越複雜、如何證明該等郵件為垃圾郵件。

紐西蘭 DIA 人員 Rob Hunter 則說明紐國在垃圾郵件之案件調查機

制，同時指出未來在結合金流之調查為突破之重點，在情資蒐集分析方面提醒應加強網路金流之調查及分析能力，在管理政策上亦應考量網路金流之管理是否存在缺失，於上述案例涉及多個國家情形觀之，亦可明確看出跨國合作之重要性。

✓ 議題 5：間諜軟體之調查實務

先由 Vigilo 顧問公司人員 Hein Dries 說明間諜軟體之概要，同時提醒某些廣告軟體不僅單純顯示廣告，在必要時，可搖身變為殭屍網路，平時可竊取使用人鍵入之帳號密碼，亦可在網頁瀏覽時執行網路釣魚，導引至錯誤網頁，並可暗中下載安裝病毒、蠕蟲或木馬，不應予以輕乎。

荷蘭 OPTA 人員 Martijn de Keizer 則報告 Dollar Revenue 案例，其表面為廣告軟體，標榜下載安裝後可取得一定網路回饋金，事實上為間諜程式，會將在被安裝電腦之任何使用資訊竊取回傳。

✓ 議題 6：被動式 DNS 複製(Passive DNS Replication)

由 BFK edv-consulting GmbH 人員 Tom Fischer 及 Florian Weimer 介紹被動式 DNS 複製技術及其用途，並介紹網域名稱系統可能存在之問題，如 Glue Record 因網域名稱伺服器內部訊息通知問題，可能造成不同步現象，致使新舊資料同時存在情形，亦使得域名伺服器可能被劫持，從而出現偽造之域名伺服器或名稱伺服器，以支持網路釣魚等犯罪行為。

(2) 第六屆德國反垃圾郵件高峰會

✓ 議題 1：垃圾郵件最新趨勢

由 eleven GmbH 人員 Enno Cramer 報告德國近年來垃圾郵件發展趨勢，2008 年起有暴增之情形(如下圖參考)，其中：殭屍網路是主要發信工具、大部分垃圾郵件具有散布木馬及擴張殭屍網路之主要目的、發信 IP 位址更換頻繁(80%以上 IP 僅使用 1 天)、大量使用合法電子郵件格式以混淆視聽。

以國家觀察，垃圾郵件來自 198 個國家，另外，各國送至德國之郵件中，90%國家的來信中有 7 成為垃圾郵件，僅 12 個國家之來信其垃圾郵件低於 5%。

殭屍網路之目的亦有小幅變動，如建立新帳號(主機、webmail)、竊取密碼等帳戶相關資料、顯示廣告及竄改瀏覽網站之路由。

垃圾郵件寄發者已逐漸成立公司形態架構，走向企業化經營，並建立大型網路服務事業架構及 webmail 服務，其觀察主要來自：垃圾郵件之寄送以上班日為主、合法位址退信情形增加、採用企業郵件格式有增加趨勢。

另外，垃圾郵件又開始回歸短文形態(short text spam)，自 2008 年 2 月之 PDF spam 風潮後，容器型垃圾郵件(container spam)已大幅銳減，2008 年 9 月起平均長度小於 3KB，使用引人注意或看似重要之主

題以吸引看信。其社交工程已逐漸具有多變化、專業及看似可信之特性，詐騙郵件比以往使用更佳之詞彙、具有令人信服之外貌，目前有兩大變型：釣魚郵件及木馬郵件，常用話題：契約、快遞訂單、銀行通知、提供假訂閱連結之新聞信、事件或假日訊息、假冒新聞發布。

冒用合法電郵位址退信亦為垃圾郵件之一大趨勢，自 2008 年第 2 季開始有大量增加之情形，尖峰時段可能抑制正常郵件之傳遞。

總體而言，垃圾郵件的發送量逐漸增加，已成為長久性之拒絕服務攻擊(DoS)，發送垃圾郵件具有高利潤、低風險性質，殭屍網路可確保匿名且發送垃圾郵件量之增加並不限於濫發者之數量，垃圾郵件之發展越來越專業，惡意軟體間(垃圾郵件、釣魚郵件、木馬程式)之互相關連性有增加之趨勢。

電子郵件安全議題應重視三個關鍵：反垃圾郵件方案、防制病毒方案及病毒發作偵測、電子郵件防火牆保護方案。

✓ 議題 2：管理法規與業務規則之比較

由歐洲網絡暨資訊安全署(The European Network and Information Security Agency，ENISA)人員 Pascal Manzano 提出 1 份管理法規與業務規則之比較報告，該報告之資料取材自 22 個國家或地區(包括 12 個歐盟國家-奧地利、比利時、法國、德國、希臘、愛爾蘭、義大利、荷蘭、葡萄牙、西班牙、瑞典、大英國協，及其他區域之澳大利亞、加拿大、中國、香港、紐西蘭、新加坡、瑞士、美國等)，涵蓋了 33 份法規文件(其中含 14 份管理法規、8 份營業規章)，而相關之機構有 15 家網際網路服務業者、8 個企業團體、5 個市場行銷機構、2 家行動通信業者、2 個政府會員、1 個歐盟機構。參考之文件中，有 18 份不具有強制力，1 份對於電子商務市場行銷活動具有強制力；其中有 21 份內容著眼於垃圾郵件之規範，4 份直接參照垃圾郵件事宜、3 份間接參照。有 10 份文件係於 2000 年至 2004 年間訂定，11 份在 2005 年訂定，7 份在 2006 年至 2008 年間訂定。

其中值得一提的有：

1.2003 年奧地利某網際網路服務業者之營業規章中，針對垃圾郵件之處理，明定對於內部用戶濫發行為之規制作為，並使用白名單機器。

2.2004 年德國網際網路商會(The German Internet Business Association，eco)對於垃圾郵件之白皮書，制定規範可信賴網路規範(含濫用管理、白名單)、立法建議案、對網路服務業者之建議(垃圾郵件之預防、對抗，如何降低對客戶之騷擾等)。

3.1999 年歐洲 IP 網路論壇(RIPE)對抗大量未經邀約郵件之業務規範，提出最佳行為準則：確認郵件伺服器未開放 Relay 功能、確認自身網路中之郵件發送源、保有追蹤郵件來源之能力、提供申訴處理系統、採取有效措施以預防客戶發送垃圾郵件、業者間資訊共享、用戶認知。

4.2005 年反訊息濫用工作小組(MAAWG)對於電子訊息系統業者之業者規範，認為業者應：提供可接受之訊息使用政策、能分辨訊息濫用類型、有權保護其系統被濫用、與其他業者溝通其保護措施。

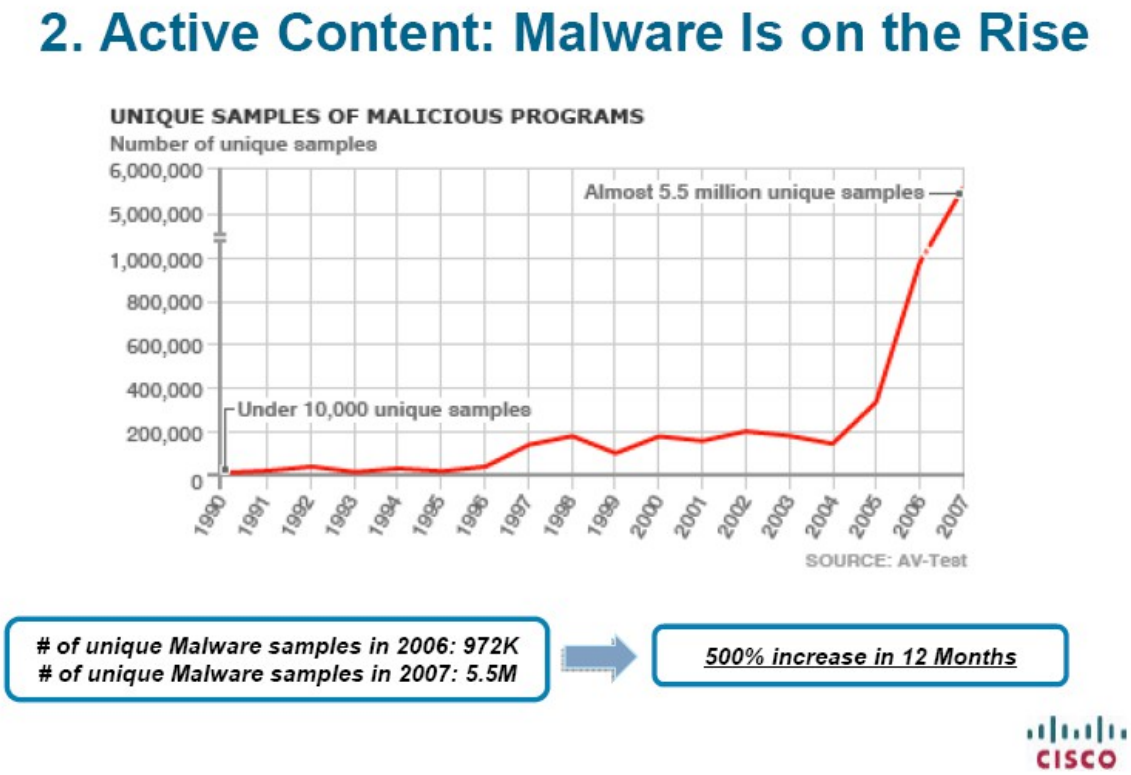
5.2005 年澳洲通訊媒體管理局(ACMA)對於電子行銷業者之營業規範，認為好的行為準則包括：明確傳送商業通訊之規則、取得同意之紀錄、對於第三方業者聯絡窗口之良好管理、病毒式行銷之預防、提供聯絡資訊、確保取消訂閱功能、申訴處理機制。

6.2005 年加拿大工業部 Task Force on Spam 報告中，最佳行為準則：使用 SPF(Sender Policy Framework)機制避免郵件偽造、管理 25Port、提供郵件附件過濾功能、監管郵件流量、個人電腦之檢疫及清理、申訴處理機制、對訂戶之通訊、具備郵件認證機制、維護 whois 資料。

7.2006 年 StopSpam 組織對抗垃圾郵件 4 條金科玉律：拒買任何垃圾郵件廣告之商品、絕不轉送垃圾郵件、千萬不要使用垃圾郵件中之「拒收」功能、對一切網際網路廣告抱持懷疑態度。

✓ 議題 3：網頁安全重要性

由Cisco公司IronPort部門人員Partick Peterson提出案例說明，許多網路犯罪行為均為透過瀏覽器為媒介，犯罪者以程式安裝可取得報酬或每天可取得固定酬金，或透過瀏覽器程式控制電腦硬體後欺騙當事人安裝其防毒程式等方式，吸引無知網民安裝其宣稱無毒之廣告或防毒軟體，以實際植入其木馬或殭屍程式，再伺機由受感染者之電腦發動網站或垃圾郵件攻擊，或者竊取其帳號密碼以對登入之網站瞭解其弱點，伺機對網站安裝惡意程式。



新型態偽裝成防毒程式之間諜軟體，多透過網站社交工程哄騙用戶安裝，亦透過垃圾郵件上附帶之網頁弱點、漏洞程式碼，或於瀏覽網址中加入不當SQL程式感染目前瀏覽之網頁。

網頁易遭受攻擊，主要因為：網頁瀏覽系統具有一定弱點、變種惡意程式擊敗防毒軟體、具有弱點之網站伺服器成為攻擊代言人。由於IE或Firefox等瀏覽器允許插件安裝，致使惡意有機可乘，另外由於MediaPlayer及視窗系統瀏覽協助物件(BHO API)存在一定管道，便於駭客將瀏覽者導至惡意網頁。

✓ 議題 4：DKIM 名聲計畫(DKIM Reputation Project)

由德國 Agitos 公司人員 Florian Sager 介紹其 DKIM 名聲計畫，該計畫蒐集已被成功辨認之垃圾郵件，並將其寄發人記錄至名聲資料庫中，以用於過濾垃圾郵件，並對於 DKIM 標示之濫發人給予極差之評分。

DKIM(DomainKeys Identified Mail，域名密鑰識別郵件標準)之應用範疇包括：提供一網域中之濫用情形、在擁有之網址內避免網路釣魚、提供 DKIM 名聲資料、可將正常郵件標示為高可信度。

該計畫之好處為：透過 DKIM 名聲資料，可顯著提升垃圾郵件過濾能力，在接收端可系統化過濾濫發者信箱之來信，在伺服器端可提升過濾能力以增加郵件遞送率。

✓ 議題 5：歐盟電子通訊管理架構之改革

由歐盟執行委員會人員 Merijn Schik 報告歐盟電子通訊管理架構之改革情形。改革提案係由執委會分別於 2007 年 11 月 13 日及 15 日向歐洲議會及歐盟理事會提出。歐洲經濟社會理事會於 2008 年 5 月 29 日通過歐盟執行委員會之提案，區域委員會則於 2008 年 6 月 18 日通過提案。歐洲議會於 2008 年 9 月 24 日一讀通過 155 條修正。歐盟理事會則準備在 2008 年 11 月 27 日進行政治協商。

目前歐盟電子隱私保護指令 2002 第 5 條並未針對單純資料攜出或為協助在電子通訊網路上進行傳輸，而進行之技術層次之儲存或存取予以防止，或做為明確由用戶提出請求之資訊社會服務之嚴謹必要程序。而第 13 條對於電子商務郵件之限制僅針對自然人而未擴及法人。

2007 年 11 月之電信改革提案，其中一個重點目標為加強隱私與安全，包括提高業者之責任義務以確保隱私與安全、強化用戶權利、增強主管機關之合作及執行。在業者之責任義務方面，除加強業者責任以確保其網路及服務之完善及安全外，為電子通訊服務之安全，用戶依服務契約僅需提供最少之資料，強制性中止通知－對主管機關運作上產生明顯之衝擊、對於消費者和主管機關間則為個人資料之危害。強化用

戶權利包括：散佈間諜軟體或惡意程式均屬違法，服務提供者對濫發者採取行動之權利，危及個人資料時之中止請求，由服務提供者針對資安事件採取之行動。增強主管機關之合作及執行方面則為：在資安措施方面增加具強制力之命令，並增加了通知及安全稽核之資訊，要求配置更多資源，及對消費者保護之管理。

另外提案針對第 13 條第 1 項亦強調包括簡訊(SMS)及多媒體訊息(MMS)兩種服務，同時包括「網路釣魚」，限制內含惡意或詐騙意圖之網站連結之郵件寄送，擴充對於全部隱私保護指令採取行動之權利。

✓ 議題 6：日本反垃圾郵件法之修正介紹

由日本總務省代表 Masahiko Kamiya 介紹該國反垃圾郵件法規之修正情形。首先對於日本 2007 年下半年垃圾郵件之主要類型提出說明：約有 80.9%為廣告及推銷約會網站、10.%為廣告及推銷成人網站、9.1%為其他；其他國家則 27%為商品郵件、20%為網際網路郵件、13%為財務郵件、10%為詐騙郵件、10%為健康方面郵件、40%為其他。另外對於源自日本或國外之垃圾郵件比較，在個人電腦方面由 2006 年上半年 72%源自國外，至 2008 年上半年一路上升至 96.9%，在手機方面則由 1.7%大幅攀升為 93.7%，可見日本當務之急在國際合作。

日本在 OP25B 計畫方面，以試行之服務提供者比較情形，明顯可見其防制所屬用戶濫發之效果，目前日本已有大量服務提供者均導入該項管制措施。

日本反垃圾郵件法規原採選擇退出(OPT-OUT)機制、郵件標示義務、禁止寄送虛假寄件者資訊或虛構收信位址之郵件、有正當理由時服務提供者得拒絕服務。另外，總務省針對濫發行為，得發出行政命令規制。

反垃圾郵件法規之修正，主要係因垃圾郵件數量不斷上升，且越來越惡意及技巧性，現有管制已然無效，濫發者多未遵守，且國外濫發數量巨幅增加。法規修正之重點在：導入選擇進入(OPT-IN)機制，維持法律之有效性，強化國際協調與合作。在選擇進入機制導入方面，最早的是歐盟相關國家(如大英國協，荷蘭、法國、德國則陸續導入)，美國則在手機方面導入此機制，澳大利亞、南韓、中國亦均已導入。

修正內容包括：釐清服務提供者得拒絕服務之狀況、制定規定使總務省可取得郵件訂約人之資料、擴充總務省行政命令之範圍、提高行政罰鍰額度達 30 倍以上。強化國際合作方面，增加可提供垃圾郵件資料予國外執法機關之規定，確認國外寄至日本之郵件適用本法規，擴充行政命令之範圍。

✓ 議題 7：外送垃圾郵件之分析

由 CloudMark 公司代表 Stuart Paton 及 Vincent Schonau 報告外送垃圾郵件之分析研究。首先說明的是－垃圾郵件損耗戰之特性在重複使用廣告網址及 IP 位址情形下，不斷變更其內容，其前提為濫發者找到在固定成本下對抗防禦策略之方法，而當濫發者發現新的目標時，其損耗方式將產生質變，以因應新目標。

對於質變之濫發攻勢，CloudMark 之因應策略為：採取彈性架構，隨著內容型態變動，快速整合指紋系統之防禦策略，並加速指紋防禦系統之運作，並透過工具之使用，維持安全措施之快速運作及反應。

建議之因應策略為：

1. WebMail 或離線 IP：認證措施為必要，限制 HTTP 連線客戶每天可發送之訊息數量。利用容量臨界值標示可疑之發送類型。
2. 線上 IP：合併殭屍名聲，饋入用戶矯正服務。使用主動過濾及紀錄掃瞄資料來辨識額外受到危害之 IP。
3. 開放 25Port 之 IP：使用透通式過濾阻擋 25Port 之外送通訊。利用結果來辨認額外受到危害之 IP，並結合用戶矯正服務。

✓ 議題 8：網路犯罪－執法單位與服務提供者之合作指導方針

由德國 Cologne 大學學者 Dr. Marco Gercke 針對執法單位與服務提供者之合作打擊網路犯罪，提出建議指導方針。本項研究肇始於 2007 年，並由一包含國際組織、執法單位及服務提供者組成之工作群組，指導方針係由此基礎透過密集的協商程序發展出來，並於 2008 年獲得通過。

報告首先對於有效率對抗網路犯罪提出基本需求條件：法律基礎、執法單位人員之訓練、足夠的設備，另外在國際層次上，尚需國際合作。之後並介紹犯罪者常用之手段－匿名通訊及加密。

匿名通訊具有「匿名的外觀」，亦為網路犯罪的關鍵行動方式，尤其是與色情連結之犯罪。此項科技足以妨礙執法者在網路上追蹤違法者之足跡。匿名通訊的好處通常與有效率的執法是針鋒相對的。透過搖控軟體，亦可能偽裝為他人。

加密則為混淆資訊，使之在不具備特定知識時便無法解讀，用以確保隱匿性。透過加密可隱藏被加密訊息已交換之事實。在犯罪上應用時，將導致犯罪必要事證難以蒐集。

本指導方針在立法本質上，建議採軟性法手段，不具有拘束力，不取代或凌駕硬性法，並應遵守相關硬性法之規定。其主要目標在釐定合作之可行途徑，並對於合作提出可行建議。主要原則為平衡性，指導方針對於執法單位與服務提供者雙方提出一套責任義務與限制之規範。透過國家間加強合作，可用來發展國際性合作架構。其係一般性的，而非直接可實施的，中間需有一轉換程序。而對抗網路犯罪需要持續的經費投入，在政府執法單位或服務提供者，誰應負責執行此一高成本措施，誰應補償此成本耗費？係為一重要課題。

企業方面多已實行一些技術保護及預防措施，而對於執行更進一步之責任義務(如資料保存義務)已被討論。對於用戶而言，通常羊毛出在羊身上，企業負擔之成本，一般均會被求諸於用戶身上。而透過提供執法服務，政府將負擔對抗網路犯罪之相關成本。犯罪者一般是一次獲利者，惟其利益並非一定等同於對抗網路犯罪所付出之全部成本。而受害者通常無法獲得財務上之補償以足夠支付其負擔之成本。「執法單位與服務提供者雙方均應注意，對要求之產生及回應所衍生之成本。」

- ✓ 議題 9：歐洲網絡暨資訊安全署(ENISA)白皮書－社交工程－利用最弱的環結

ENISA 代表 Kjell Kalmelid 就該署「社交工程－利用最弱的環結」白皮書作一概要報告，說明白皮書係由 3 項案例研究作為基礎，綜合了 179 名參與者，評估了一組 20 個訊息(11 個假造、9 個真實)，使用者僅能正確地分類 42%案例。而在一個具有 152 個標的收件者之參與機構中，有 23%的人可被技巧性地影響其執行易受惡意軟體感染之動作。標的收件者如再進一步改為大學肄業學生時，顯著的弱點可被觀察到，然而，如使用者加以訓練時，弱點情形即有下降之趨勢。

ENISA 建議，避免成為弱點，最佳的方式為提升可能成為標的成員其自我警覺能力。推薦提供用戶一個檢查表列，其中應包括一個他們被請求提供資訊時應審慎思考的因素列表：

1. 合法性：這個資料需求是否看來合法且平常？你是否應被要求提供資料？這個資料平常是由你提供的？

2. 重要性：你提供之資料或被要求執行之工作之價值為何？它將如何可能被誤用？

3. 來源：你是否確信該請求之來源為真？能否找到一個檢查方法？

4. 時間性：你有必要立即回應嗎？如果有所疑慮，花點時間尋求進一步檢查或協助。

✓ 議題 10：由美國觀察執法單位對於預付金詐欺之處理

美國司法部代表 Jonathan J. Rusch 針對預付金詐欺提出報告。在 2007 年 FTC 的消費者詐欺申訴資料顯示，由 2006 年 428159 件上升為 555472 件。已付出金額由 2005 年 6.83 億美元倍增為 12.37 億美元。其中與網際網路相關的申訴案有 221226 件(約占 40%的申訴案)。

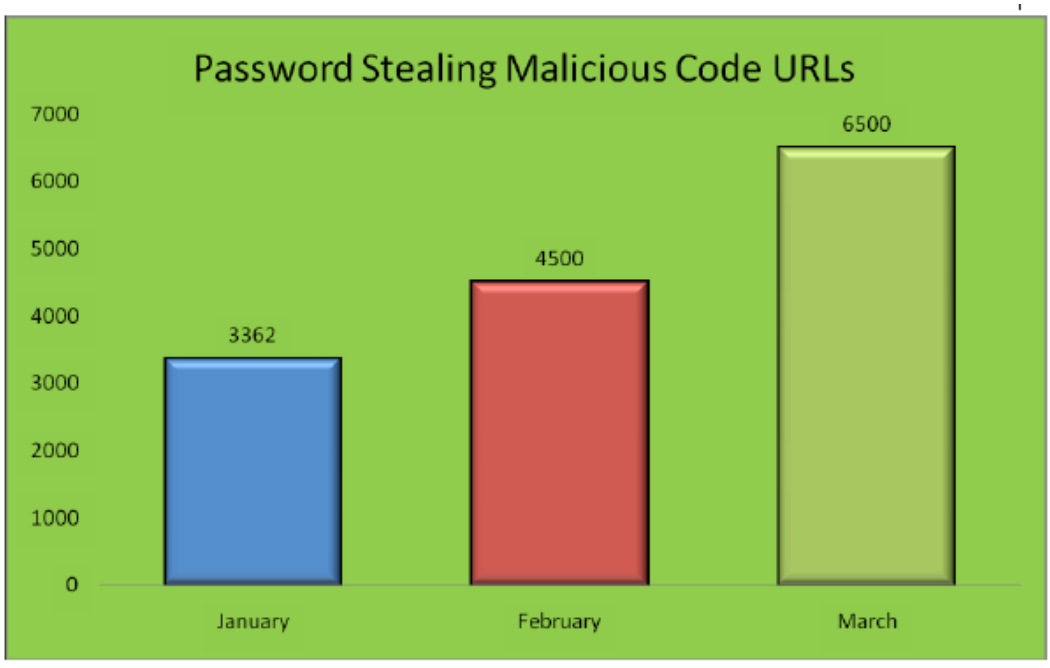
上升最快的詐欺類型包括：在家購物型錄銷售、網際網路服務、外國財產贈與、中獎/賭金/樂透、電腦設備/軟體、網路拍賣、衛生保健、旅遊/假期及分時渡假、預付金貸款、投資理財。

電話行銷詐欺方面，美國消費者聯盟(The National Consumer League)提出2007年前十大詐欺趨勢為：假支票詐欺、中獎/賭金/免費贈品、預付金貸款/信用理專、樂透/樂透彩券購買俱樂部、網路釣魚/詐騙、雜誌、信用卡發給、獎學金/學位授與、買家俱樂部、奈及利亞金錢贈與。其損失上升值得注意，平均每位受害者由2006年2036美元上升至3091美元(超過50%)。

網路詐欺方面，2007年前十大詐欺趨勢為：假支票詐欺、一般商品、網路拍賣、奈及利亞金錢贈與、樂透、預付金貸款/信用理專、中獎/賭金/免費贈品、網路釣魚/詐騙、甜心騙子、網際網路存取服務。其損失則為穩定狀態，平均每位受害者2006年1512美元、2007年1507美元。

美國網路犯罪申訴中心2007年間處理了超過219553件申訴，其中90008件移送法辦，詐欺總金額由2006年1.98億美元上升至2.39億，大多數加害者位於美國(約佔63.2%)，較顯著的有部分位於大英國協(約佔15.3%)，奈及利亞(5.7%)，加拿大(5.6%)等等。

網路詐欺/釣魚部分，由反網路釣魚工作小組2008年第1季統計顯示：釣魚網站有81215個(舉報數85630個)，被刼持利用的商標有141個，大部分以企業部門為主，其中金融服務占92.9%，政府及其他占4.3%，另外，竊取密碼的惡意程式碼因大量SQL injection攻擊而有大幅上升趨勢。



報告並針對假支票、外國財產贈與、獲審核通過的信用卡、投資理財、樂透、網路釣魚、金字塔型銷售/龐茲手法等案例作簡要說明，以供與會人員瞭解。

國際犯罪防制係為犯罪防制實務重要的一環，2008 年 4 月 23 日美國提出國際間系統化犯罪防制策略，宣示美國聯邦政府執法機關將分享國際間系統化犯罪事件情資，蒐集分析以將最重大威脅予以優先化，並施以美國專門技術及資源之處理，以有助於降低該等威脅。美國國際執法機關將加強與國際伙伴之合作，以將國際犯罪案件訴諸美國及他國法律。

1998 年美國與加拿大聯合成立特殊工作小組及策略伙伴關係，針對電話行銷詐欺，2004 年 10 月執行 Roaming Charge 行動，調查發現由犯罪組織進行組織化犯罪有上升趨勢，損害金額達 10 億美元；2006 年 5 月執行 Global Con 行動，在美洲及歐洲共逮捕 565 人，其中 96 件美國方面案件有 280 萬名受害者，損害總金額即近 10 億美元，FTC 在非法詐欺案中共對 140 名被告向法院提出 20 件民事訴訟。

以下為報告提出的 Global Con 行動的一些剪影：

目前推動國際大宗市場詐欺案件協調小組(International Mass-Marketing Fraud Coordinating Group)，成立於 2006 年 11 月，除針對詐欺案件的協調處理外，亦關注情資分析(聯合威脅評估)、分裂事件處理、教育及預防、執行方面等事務。

✓ 議題 11：世界性的詐欺

由澳洲消費者詐欺特別任務組(Australasian Consumer Fraud Taskforce，ACFT)代表 Louise Sylvan 對於流竄於世界的詐騙行為提出報告。該任務組係於 2005 年 3 月由 18 個澳大利亞及紐西蘭政府機關共同組成，2006 年加入警方成員。主要任務為加強澳大利亞與紐西蘭政府對抗詐騙行為，內部分為 3 個工作群組－拓廣服務組、預防組、研究組。

報告首先說明數個案例－阿德萊德一名農夫在西非國家馬利的網路詐騙案中被綁架折磨且詐取了 10 萬澳幣；昆士蘭網路愛情詐騙案中某男子被詐騙了 2 萬澳幣；美女於網站貼照片約會詐騙；電子郵件樂透詐騙，宣稱可獲得豐厚報酬，據統計大英國協約有 62%的垃圾郵件是樂透詐騙；提供在家或線上工作可賺取豐厚薪資的詐騙案；網路販售奧林匹克門票詐取奧迷數千澳幣。

目前常見的消費者詐騙有：技術層面的－惡意程式，吸引/詐騙－易於賺取之橫財、網路真愛、奇蹟式治癒藥效、中大獎等。

而在 ABS stats 之家庭式統調顯示，個人詐騙行為已造成約 9 億 8 千萬澳幣損失，在過去 12 個月內有 80 萬 6 千人受害，其中有半數為一定類型的詐騙(信用卡、電子郵件詐騙等)，32 萬人對於詐騙有所回應(電話、信件、電子郵件等)，其排名為：樂透、金字塔型銷售(老鼠會)、網路釣魚。

✓ 議題 12：起草對抗垃圾郵件之業務規範

希臘律師 Zoe Kardasiadou 就服務提供者研擬對抗垃圾郵件業務規範之實務，提出經驗分享。

在組織的措施方面，建議：提供用戶書面資訊或指導(包含服務提供者之管理策略、技術指導等)、防制垃圾郵件之規定條款及安全工具、申訴處理機制、在用戶服務契約中保有禁止垃圾郵件之條款或特定情形、察覺活動、維護正確網路資訊。

在技術措施方面，建議：除非在其他方面已同意，儘量阻斷 Port25 之通訊、公開 SPF 資訊、提供電子郵件過濾機制、在網路上隔離受感染的電腦、對於外送郵件加以發送速率限制、預測性的監控網路流量。

服務提供者的反應，由技術觀點而言，攔阻 25Port 是有效的，而由營業觀點來看，對於 25Port 之投資並無利潤可言，請主管機關配合制定強制法規，限制 25Port 之使用。

在法規層面應再詳加思考：

1. 業者被授予權利應採行相關措施，但他們是否也具有義務？是否可能就內部市場的服務自由條款，及監控依照電子商務指令第 15 條規定所為服務的缺乏約束力等而言，這些措施違反了業界法則？

2. 在 2002 年電子商務指令第 4 條之安全要求，是指向業者的責任義務，然而安全議題包括了整體電子郵件與網路服務效能，比如服務的可用度、對於拒絕服務的預防、預防業者與終端用戶的系統遭受感染。

3. 業者在用戶契約上具有提供良好效能的義務。

4. 用戶具有不寄送未經邀約訊息的義務。

5. 電子隱私指令第 4 條明定「安全措施應包括恰當的技術及組織上的措施，以保護網路及服務免於意外、違法或未經授權的使用，或干擾、妨礙其功能性、可用性。」

6. 提出的措施是否符合現狀需求？有否考慮垃圾郵件或其他如惡意程式？這些措施是否適切及恰如其份？是否為技術中立？是否應再提

出替代方案或組合方案？

7.推薦的措施是否有約束效應？技術性措施－是的，組織性措施則非全部－如提供業者營運策略的書面資料、在用戶契約的相關約定條款、維護正確的網路資訊等。

(3) 執行會議

✓ 議題1：Signal SPAM 垃圾郵件回報中心介紹

由Signal SPAM 計畫管理師Francis Bouvier進行演講，其內容主要說明Signal SPAM垃圾郵件回報中心之運作現況，及透過回報中心之資料彙整分析後，對於郵件中經常存在之防制預付金(advance fee)詐騙，具有一定之遏阻效用，值得業界共同善用此一機制。

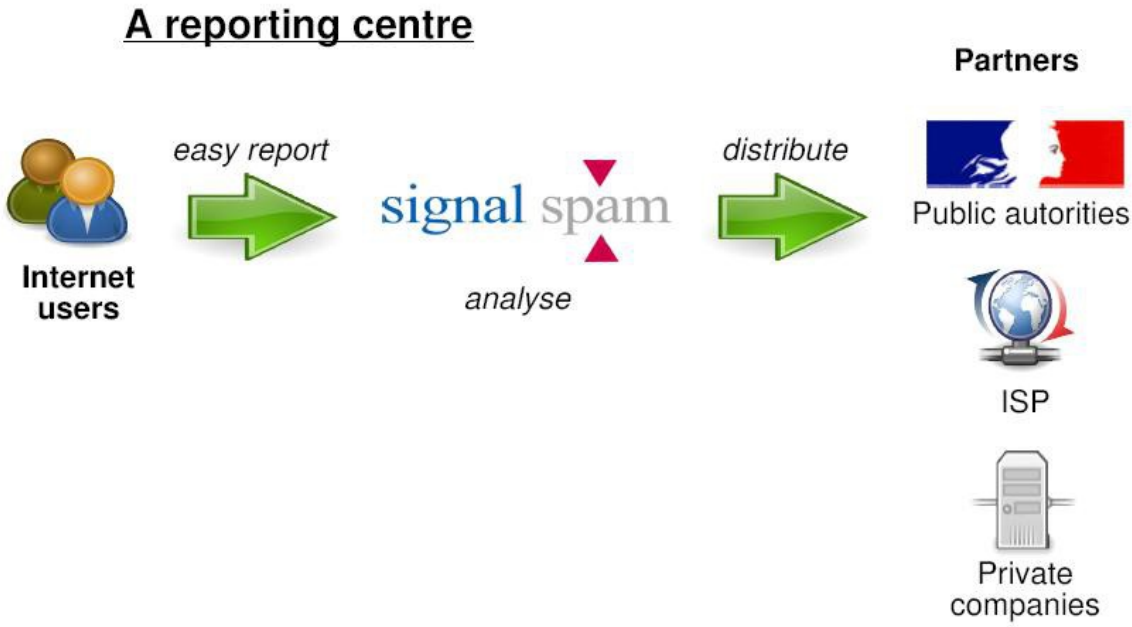
回報中心在預付金詐騙問題中可發揮下列功能：

1、 提供統計分析功能：基於用戶回報案例，針對特定類型詐騙郵件，可評估其影響。

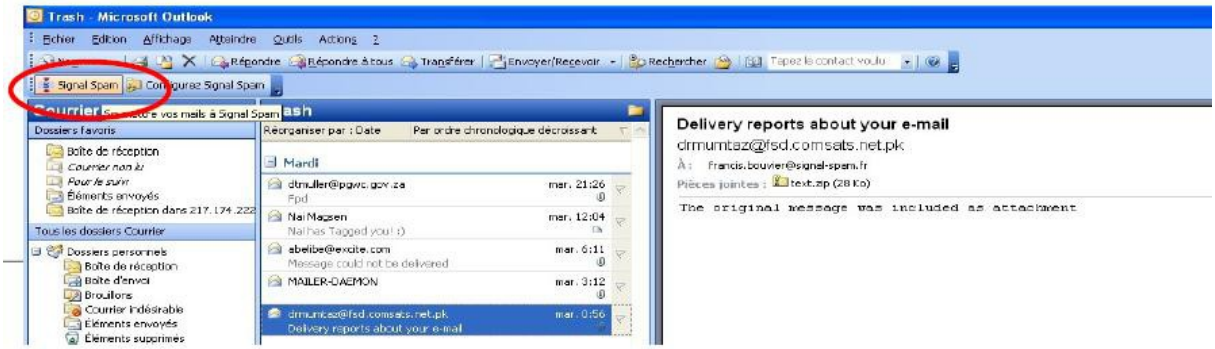
2、 先期告警功能：可於特定案例發生時，即時關閉受影響之伺服器，避免損害擴大。

3、 執行功能：提供用戶問題詢答、協助處理客訴。

Signal SPAM計畫係於2007年5月啟動，其組成包括相關主管機關(法國政府部門、個人資料保護主管機關、警方網路犯罪部門等)及民間業者(ISP業者、電子商務業者、市場行銷業者、銀行業者等)。其垃圾郵件之蒐集來源，主要為網際網路使用者透過Signal SPAM提供之簡易舉報程序，向該回報中心舉發，在回報中心將收到之舉發資料儲存至資料庫中，並加以比對分析後，再依其分類情形，分送給主管機關及相關業者，以利該等機構續為必要之處理，該回報中心之運作情形示意圖如下：



首先 Signal SPAM 係於其網站()上提供電子郵件用戶端程式之插件(目前支援 Outlook 2003、2007、Outlook Express、Windows Mail 及 ThunderBird 2.0)，以便用戶安裝使用，當用戶透過電子郵件用戶端程式瀏覽郵件時，如認為某一郵件可疑時，即可點擊工具列上「Signal Spam」按鈕，即可將此郵件向回報中心舉發(參考下圖)。



由於舉報方式簡便，18 個月內已有 4 萬用戶安裝回報用插件，且回報中心之蒐集速度驚人，每天約可收到 22,000 封舉報郵件，18 個月內已蒐集了近 1 千 2 百萬封舉報郵件，蒐集資料經過分析，約有 4%資料為樂透或預付金詐騙類型之垃圾郵件，單僅 2008 年內即有約 23 萬封樂透或預付金詐騙郵件。

回報中心在取得用戶舉報資料後，將透過系統程式自動分析資料

內之 IP 位址、網域名稱、ISP 業者、國家、主旨欄、Hash 值及包含之網址等。資料庫中之資料，可針對指定準則進行交叉比對搜尋，並依排序加以研究，更可即時向相關機構分發通知資料，系統亦可週期性提供摘要資訊。2008 年內即已分發了 20 萬封垃圾郵件資訊。

叁、檢討與建議

自 94 年 8 月我國加入倫敦行動計畫（LAP）成為正式會員以來，即逐年派員參與倫敦行動計畫「垃圾郵件主管機關聯繫網路研討會」，蒐集各國及業界防制垃圾郵件之策略與實務作為，以供我國建構法制規範環境之參考，同時建立國內垃圾郵件防制實務體系。我國在外交運作上雖時遭中國藉機干預及阻撓，然以加入 LAP 反垃圾郵件組織未遭反對而能順利加入之態勢觀之，國際間應已深刻體認到，打擊垃圾郵件單就各國本身力量已鞭長莫及，與其僅靠本國力量消極地進行技術防堵措施，尚不如在國際合作著力，強化國際聯防力量以減少跨國垃圾郵件來得有效。以我國情形為例，約有 95%之垃圾郵件係為跨國傳遞之型態，雖然國內調查已能確認幾近 100%之案件，然而難以介入調查的多數跨國垃圾郵件，仍有賴於健全的跨國合作始有解決之道。

本次會議，由垃圾郵件引發涉及之議題相當廣泛，除了資安議題受到重視外，詐欺事件亦為當前應合作解決之問題，由本次議程安排可看出，在各國防制垃圾郵件機制逐漸建立後，執法單位的工作重點已由單純垃圾郵件的防制，移轉至網路犯罪事件的調查與防遏，同時並跨越行政調查進入了刑事偵查範疇，爰擬就上開會議內容提出檢討事項如下：

一、應擴大參與層面以吸取外國立法與執法經驗

本次會議中，有部分議題係為垃圾郵件串連網路犯罪事件，而其犯罪手法則與資安議題息息相關，由主辦單位安排美國、澳大利亞、紐西蘭、荷蘭等國之多項議程廣及網路詐欺、網路安全等方面議題可見一斑，是以未來倫敦行動計畫工作小組會議之參與單位，建議應予擴大至資訊安全、犯罪防制或執法實務等相關部門，以配合深入瞭解其他國家之規劃、處理細節及聯合作業方式，同時預知未來執行上之困難因子，並仔細思考預為因應，透過吸取各國在會議中所提供立法設計與寶貴執法經驗，適足以供我國日後規劃政策及執法措施之借鑑，加速防遏不法行為。

二、垃圾郵件與網路犯罪掛鉤，防制機制趨於複雜及多面向化

在會議首日中，由澳大利亞與美國之 Herbal King 案例觀察，垃圾郵件之發送本身雖有極高利益，然而結合網路犯罪行為之獲利更為豐厚，並由犯罪組織之專業分工，及其本身透過公司化以合法掩護非法來看，未來防制工作面對的是有組織、有計畫、具專業能力的高級知識犯罪體，除大幅增加調查工作之難度外，如何防制亦為一亟待深入探討之議題，僅靠現有單薄的因應機制及分散由各執法單位依職掌處理已明顯不足，再依美國等先進國家組成工作群組的廣度觀之，未來我國亦應成立跨部會合作機制以互補不足，同時提高資源之利用度，以能因應處理各面向之案件。

審酌犯罪之原始目的即為取得金錢，透過金流之調查將可使犯罪者之核心及其架構無所遁形，未來在法規及調查實務能力上，亦應積極思考、規劃及擴充在調查及情資工作上，在金融面向之執法依據及可用工具，以積極掌握調查契機，由金流層面突破以瓦解犯罪者在通信技術上之層層防禦。而對於現有監管機制上具有管理弱點之網路金融，應早日釐清對策，以避免成為未來網路犯罪防制之絆腳石。

三、持續加強國際合作之重要性

國際合作之推動，一直以來便是倫敦行動計畫的重點，而越來越多的垃圾郵件濫發行為及網路犯罪事件，亦逐漸走向國際化，以提高執法單位之困難度，本次會議相關報告亦有多項論點涉及國際合作事務之探討。國家通訊傳播委員會有鑑於跨國垃圾郵件占絕大多數，已在推動立法核心業務外，將關注重點放在國際合作之加強，審酌國際合作之擴展與執行，須投入大量資源，並需考量合作雙方平等互惠原則，然鑑於目前由於法規尚未完備，國際合作之能量仍屬極為單薄，尚難以收跨國合作防制垃圾郵件之成效。為在完成法制環境建構前，厚植國際合作能量，本會將透過預算編列之方式，積極尋求合作伙伴共同發展常態化之國際合作實務工作平台，並與各國逐漸建立合作關係，藉由務實行政作為維繫國際合作管道，以便於未來完成立法後，即以之作為基礎，加強擴展國際聯防網絡。

藉由倫敦行動計畫及其年度工作會議的參與，本會已與其他國家逐漸建立合作

關係，其中更有如巴西等外交聯繫較弱之國家，由於垃圾郵件對於世界各國之干擾已久，與會各國均抱持積極擴展國際合作立場，係為我國在外交多方受阻情勢中，少數能逆勢發展者，本會雖積極投入行政資源配合執行合作實務，然仍屬杯水車薪期盼未來能擴大行政機關及民間機構之共同參與，以強化整體國際合作交流力量，除能更為有效防遏垃圾郵件外，更能藉由交流合作建立國際實質友誼關係，提升我國外交能量。