出國報告 (出國類別：參加國際會議)

出席「第三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」會議報告書

服務機關：國家通訊傳播委員會

姓名職稱：科長 林尚楨

派赴國家：美國華盛頓特區

出國期間：96 年 10 月 8 日至 13 日

報告日期：96 年 12 月 28 日

出席「第三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」會議報告書目錄

壹、前言

近年來，政府大力推動寬頻通信基礎建設，不但使得國內網路通信環境漸趨完備，亦帶動了我國網路電子商務的蓬勃發展；而經營電子商務，最重要的莫過於運用傳銷工具以拓展行銷網絡，在眾多的傳銷工具中，電子郵件由於具有成本低廉、易於大量散播、傳送快速等多重特性，遂受到電子商務經營者(以下簡稱廣告主)青睞而大量運用，惟由於廣告主多未瞭解網路傳銷特性，僅以開信率或廣告點擊率計算廣告費用，加以欠缺法規規制，致使電子郵件遭不當濫用，而網路上大量流竄的垃圾郵件，不但造成廣大收信者信件處理資源及電子郵件服務資源的雙重鉅額耗損，向國外濫發的結果，亦使我國成為垃圾郵件之輸出大國，嚴重損及我國際形象。

為加強國際合作，宣示我防制垃圾郵件決心，以提升我國國際形象，國家通訊傳播委員會(以下簡稱本會)除努力爭取與他國洽簽雙邊、多邊垃圾郵件防制合作協議外，並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日以「台灣」名義正式成為「倫敦行動計畫」會員。本次96年10月9日至10月11日於美國華盛頓特區舉辦之「第三屆倫敦行動計畫及垃圾郵件主管機關聯繫網絡研討會」，已係我國加入該計畫後第2次參與之國際性工作會議，本會特指派林尚楨科長出席會議，為加強業界參與，並協調台灣網際網路協會邀請會員代表協同出席(參閱附件1)。

本次會議共有2個主軸議程，議程1係為倫敦行動計畫與反訊息濫用工作組，基於以協同企業合作向網路威脅對抗的聯合會議，研討議題包括對於濫發者的法律動作、制度回顧、新興威脅以及各相關組織地區資訊的更新等議題。議程2則為執法機構之網路威脅調查會議，研討議題包括認識垃圾郵件、e-Crime工具在網路上如何協助犯罪調查、行政機構如何協助追蹤濫發者、控制惡意程式等議題。本報告書首先就倫敦行動計畫現況及我國參與緣由加以簡介，再說明本次會議重要議題及內容。

倫敦行動計畫(London Action Plan , LAP)

(1) 倫敦行動計畫簡介

93年11月11日，美國聯邦貿易委員會（Federal Trade Commission, 簡稱FTC）及英國公平交易局（Office of Fair Trading, 簡稱OFT）等27個國家之資料保護、電信、消費者保護等政府機關及部分民間機構代表於英國倫敦集會，並共同簽署「執

行防制垃圾郵件國際合作」之「倫敦行動計畫」。

「倫敦行動計畫」揭示歡迎其他有興趣之相關政府機關、國際組織及適當之民間機構代表加入執行防制垃圾郵件之合作計畫，並揭櫫加入該計畫之相關政府機關、國際組織及適當之民間機構代表，應盡最大努力執行防制垃圾郵件合作之計畫項目及內容。

(2) 我國加入倫敦行動計畫之緣由

鑑於我國在國際垃圾郵件輸出國排名有居高不下之趨勢，政府為尋求國際合作助力，建立國際垃圾郵件聯防網，經瞭解「倫敦行動計畫」於 93 年底成立後，乃藉由多種管道積極爭取加入，嗣於 94 年 5 月 10 日我國駐美代表處函告，美國 FTC 支持我國參與「倫敦行動計畫」，以加強我國與各國主管防制垃圾郵件政府機構之合作，並建議本會逕以電子郵件方式將參與該計畫之申請書寄交美國 FTC 法律顧問 Ms. Elena Gasol Ramos，並於申請書中敘明我國執行防制垃圾郵件成效及未來計畫，俾利美國 FTC 轉致該計畫各會員爭取支持。

94 年 6 月 17 日我國以「台灣」之名義，請美國聯邦貿易委員會轉致「倫敦行動計畫」各會員有關我國申請加入該計畫防制垃圾郵件會員之申請書，並爭取支持。

嗣英國 OFT 於 94 年 8 月 4 日以電子郵件表示，基於目前「倫敦行動計畫」各會員並未反對我國參與該計畫(no objections from current members)，我國已被接受成為該計畫防制垃圾郵件之會員。附件 2 內檢附「倫敦行動計畫」防制垃圾郵件宣言中、英文版資料供參。

另關於中國大陸之參與狀況，經查「倫敦行動計畫」防制垃圾郵件網站，中國大陸亦於 94 年 7 月 20 日簽署加入。

貳、LAP/CNSA「第三屆倫敦行動計畫及垃圾郵件主管機關聯繫網絡研討會」

1、會議時間、地點及議程

時間：96 年 10 月 9 日至 10 月 11 日

地點：美國華盛頓特區

議程：詳附件 3、4

2、主要議程

本屆「倫敦行動計畫及垃圾郵件主管機關聯繫網絡研討會」會期 3 日，分為 10 月 9 日至 10 月 11 日舉辦的「反訊息濫用工作組協同企業合作向網路威脅對抗的聯合會議」(3rd Joint LAP-CNSA Workshop: Collaborative Ventures to Fight Online Threats Featuring Joint Sessions With MAAWG[1])及 10 月 10 日至 10 月 11 日舉辦的「執法機構的網路威脅調查會議」(Online Threats Investigations for Law Enforcement Agencies)2 個相異主題之議程，如下分別簡述各議程重要議題：

(1) 反訊息濫用工作組協同企業合作向網路威脅對抗的聯合會議

✓ 議題 1：不利於濫發者之法律動作

本議題主要分為兩個部分，第一部份由澳洲通訊傳播署（Australian Communications and Media Authority，以下簡稱 ACMA）資深調查員 Chris Duffy 介紹該國目前防制 SAPM 的手段及實際案例，第二部分由 FTC 律師 Steven Wernikoff 介紹美國《CAN SPAM ACT 2003》架構及該國執行反垃圾郵件之情形。

第一部分，澳洲 ACMA 資深調查員 Chris Duffy 首先介紹該國 SPAM ACT 2003 之規範架構，包括採取 OPT-IN(寄件者必須取得收件者同意，方得寄送商業電子郵件)機制之立法例、受傳送規制之郵件性質必須具有商業性等，另其報告亦指出澳洲政府依據該國 Telecommunications Act 1997 及

[1] MAAGE, Messageing Anti-Abuse Working Group, 反訊息濫用工作組

SPAM ACT 2003 執行行政調查之措施，內容包括向服務提供者取得資訊之權力以及向第三人取得資訊之權力等。

ACMA 有權接受澳洲國民對於 SPAM 案件之申訴，並進而為調查措施，惟對於類似網路釣魚（Phishing）及詐財之刑事案件，仍由澳洲政府之高科技犯罪中心或州政府警察局偵辦該等案件。另外 ACMA 也與州政府負責調查詐財案件之消費者保護機關保持緊密聯繫。

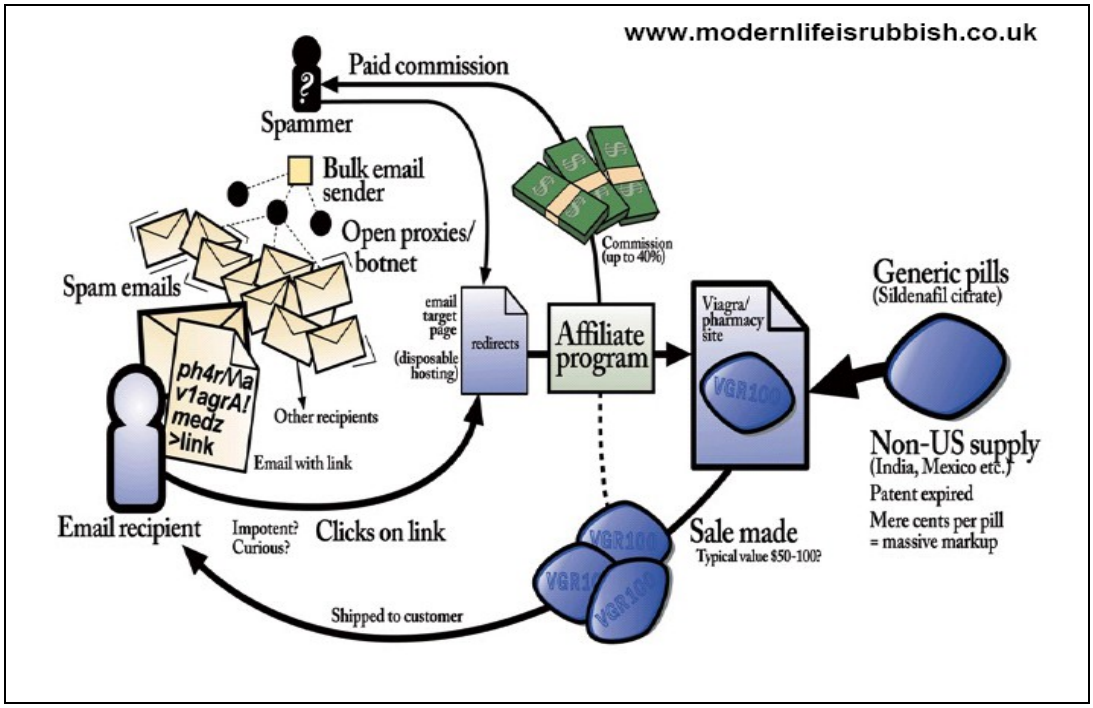
報告中介紹 ACMA 進行調查之工具包括：(1)Telecommunications Act 1997 中 Section 522 之法規授權部分，包括要求寄件者提出相關資訊、警告命令之簽發、對於不遵從警告命令或提出不實證據者之罰鍰規定。(2)以法院核發之搜索票進行搜索。其他尚包括是否有其他更適合之法規依據以行使其調查權之斟酌，以及應該與私人企業包括(但不侷限於此)如 Microsoft、Spamhaus、Sophos、Messagelabs、Symantec 共同合作調查 Spam 犯罪之執行等。

此外 Chris Duffy 亦介紹該國起訴 Spammer 之案例，於 2005 年 7 月，澳洲法院對於 Mansfield 及 Clarity1 公司濫發商業電子郵件之行為核發禁制令，於採行交互詰問的過程中，法院取得 Mansfield 以及 Clarity1 公司的確分別有蒐集電子郵件位址及傳送未經收件者同意之電子郵件等不法行為之心證，於 2007 年 7 月，該國法院對於 Mansfield 以及 Clarity1 公司共同判處 309000 澳幣之罰鍰。

第二部分之報告人為 FTC 律師 Steven Wernikoff，報告首先以圖示方式介紹商業電子郵件濫發及交易流程(如下圖)，一開始濫發者透過 Open proxy 或 Botnet 之方法散發大量商業電子郵件，收件者基於自身需要或好奇心點選郵件中的超連結，連結至濫發者早已製作好的網頁，而收件者可藉由該網頁所設定好的交易模式與廣告主進行交易，廣告主藉由該網頁所設定的模式，將商品銷售與收件者，同時濫發者也可抽取廣告主販售商品所得之利益作為佣金。

其次介紹美國《CAN SPAM ACT 2003》所賦予 FTC 之權責，調查權部分，FTC 得傳喚相關行為人，但無搜索之權力，

FTC ACT 中對於商業行銷者以不公平或欺騙方式為行銷行為亦有所規範，另外《CAN SPAM ACT 2003》所規範尚包括提供虛偽或引人錯誤之信首資訊、欺騙性的主旨欄、未提供選擇退出機制、未提供正確之寄件者郵件位址、明顯涉及「猥褻性」內容之郵件而未予特別標示等。此外，對於意圖提供特定訊息而引誘行為人按下連結或確認鍵（push the button），導致濫發者取得行為人特定資料之行為，該法亦有所規範。



Steven Wernikoff 緊接著介紹目前 FTC 執法現況，自從《CAN SPAM ACT 2003》實行以來，約有 27 個涉及 SPAM 的案件發生，超過一千二百萬美元的罰鍰處罰。自 2004 年 4 月 29 日起，FTC 接到超過 50 萬封申訴信，於是 FTC 加強展開執法行動，首先找出濫發者 Daniel Lin，並且判處 3 年有期徒刑。另一例濫發者 Creaghan Harry 在中國大陸境內架設郵件主機，使用加拿大的郵件信箱，並在哥斯大黎加申請 Domain name 及付費，全部皆冒用假名申辦，該位濫發者被逮捕後被判處五十萬美元罰鍰。另一例則為 FTC 控告 7 家公司違反《CAN SPAM ACT 2003》中，有關成人內容之郵件應為標示義務之規定，最後法院判決其中 5 家公司應負擔約 150 萬美元民事罰鍰。另外關於意圖提供特定訊息，引誘行為人按下連結或確認鍵（push the button），導致濫發者取得行為人特定資料行為之查緝，FTC 亦起訴了 3 人，其中一位

Button Pusher Brian McMullen 承認其所為違反《CAN SPAM ACT 2003》之相關規定，最後被判處拘禁 5 個月，以上為 Steven Wernikoff 所介紹 FTC 之執法概況。

✓ 議題 2：評估機制介紹

本議題由 MAAWG、Cert.br、Symantec、IronPort 代表分別報告他們使用各種不同的觀測法所觀察到的 SPAM 數量、種類、傳送方式、來源國等流竄於網路上之 SPAM 相關資訊。

❖ M AAWG

MAAWG 執行長(Executive Director) Jerry Upton 介紹該組織設計的「電子郵件評估計畫」(Email Metric Program)，該計畫從 2006 年三月開始發表第一份在 2005 年第四季所進行調查的報告，原則上每季會發表一份報告(若被觀察的信箱少於一百萬則不會發表季報告)，目的在於從郵件管理者(mailbox provider)立場，對電子郵件濫發情形提供一個不偏頗的觀點。該份季報告嘗試說明電子郵件到達使用者信箱之前，業者在防堵 SPAM 上所作的努力，並長期觀察相關趨勢之演變。

這個計畫一開始是為了回應 OECD 在 2005 年提出將「現有的評估機制」(existing metrics)以及「被測量的對象」(what was being measures)進行全面完整的研究。測量所得到的數據似可作為評估政策、法制、技術解決方案的「有效性」(effectiveness)以及決定策略及未來變化的「有效性」之用。

該計畫的參與者都是自願的，且必須為 MAAWG 的成員並負有管理終端使用者(end-user)信箱的責任。參與者可隨時加入此計畫，除有特殊狀況外，原則上須持續兩年提出季報告。所有提出的報告皆被視為機密資料，由執行長處理彙整所有的資料，並將結果公佈於 MAAWG 網站上。

會中公佈最近 2007 年第二季報告，該季觀測郵件信箱總數為 2 億 4 千 1 百萬個，被阻斷的連線及被阻擋/加標籤的內寄郵件(dropped connections & blocked/tagged inbound email)計有 2960 億封，未經變更的郵件(unaltered delivered email)計

有 460 億封。

Reported Metrics	Report #6 Q2 2007	Report #5 Q1 2007	Report #4 Q4 2006	Report #4 Q3 2006	Report #3 Q2 2006	Report #2 Q1 2006	Report #1 Q4 2005
Number of Mailboxes Represented	241 Mil.	230 Mil.	219 Mil.	216Mil.	170 Mil.	170 Mil.	138 Mil.
Number of Dropped Connections & Blocked/Tagged Inbound Email	296 Bil.	271 Bil.	268 Bil.	261 Bil.	265 Bil.	285 Bil.	233 Bil.
Number of Unaltered Delivered Email	46 Bil.	47 Bil.	58 Bil.	57 Bil.	55 Bil.	51 Bil.	43 Bil.

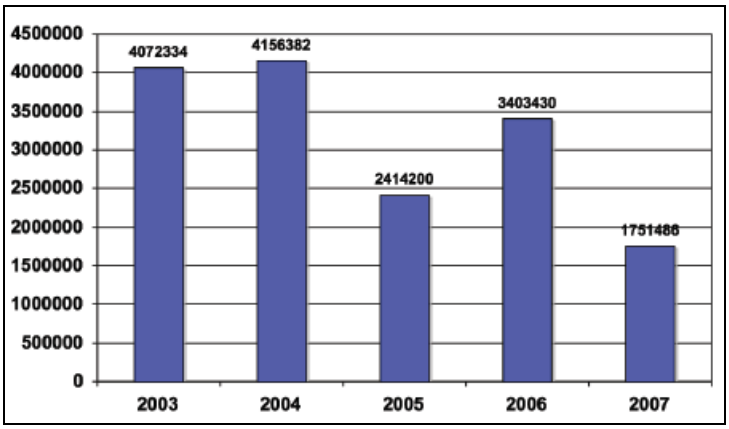
針對這些資料進一步的分析可以瞭解，每收到 1 封未經變更的郵件就會有 6.5 封被阻斷的連線及被阻擋/加標籤的內寄郵件，也就是說，在所有收到的郵件中，有 86.7%是被阻斷的連線及被阻擋/加標籤的內寄郵件。從表中可以看到這樣的一個比率是較前一季稍微提高的。

Selected Ratios	Report#6 Q2 2007	Report#5 Q1 2007	Report #4 Q4 2006	Report# 4 Q3 2006	Report#3 Q2 2006	Report #2 Q1 2006	Report #1 Q4 2005
Dropped Connections & Blocked/Tagged Inbound Emails per Mailbox	1230	1178	1221	1210	1562	1680	1697
Dropped Connections & Blocked/Tagged Inbound Emails per Unaltered Delivered Email	6.50 or 86.7% abusive email	5.77 or 85.2% abusive email	4.58 or 82.1% abusive email	4.51 or 81.8% abusive email	4.82 or 82.8% abusive email	5.58 or 84.8% abusive email	5.38 or 84.3% abusive email
Number of Unaltered Delivered Email per Mailbox	189	204	267	268	324	301	315

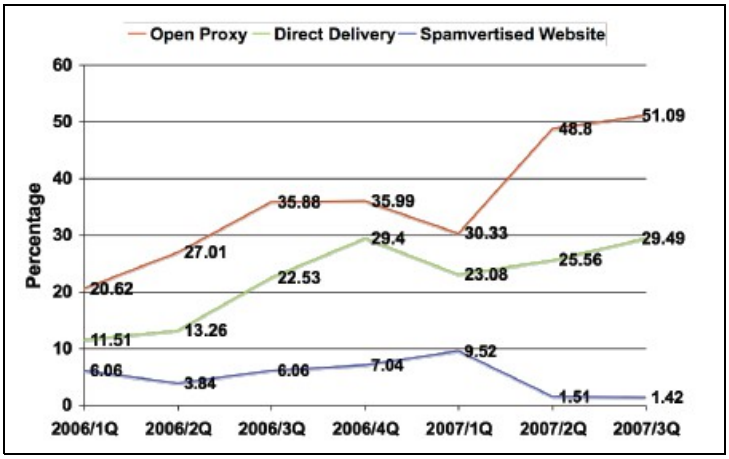
❖ Cert.br、NIC.br、CGI.br

由 Cert.br 經理 Cristine Hoepers 報告巴西在網路管理上的機制及架構。

Cert.br 從 2003 年起，逐步開始接受 SPAM 回報處理，直到 2006/2007 進入常規化。從 2003 年到現在，很明顯的可以看出巴西 SPAM 回報總量有逐年顯著減少的趨勢，從一開始的 400 萬封到 2007 年只剩下 175 萬封的 SPAM 回報數。



Cert.br 藉由 SpamCop 來分析這些經回報的 SPAM，可以知道有越來越多的 SPAM 是透過開放式代理服務(Open Proxy)的方式傳送，這方法在 2006 年時只佔 20.62%，到了 2007 年已倍增為 51.09%。位居第二的傳送方式為直接傳遞(Direct Delivery)，其所佔比率也是有升高的趨勢，在經過一年半的觀察發現其比率也從 11.51%向上攀升到 29.49%。而第三種透過 SPAM 做廣告的網站(Spamvertised Website)之傳送方式比率則是顯著降低，在 2007 年第三季時只佔 1.42%。



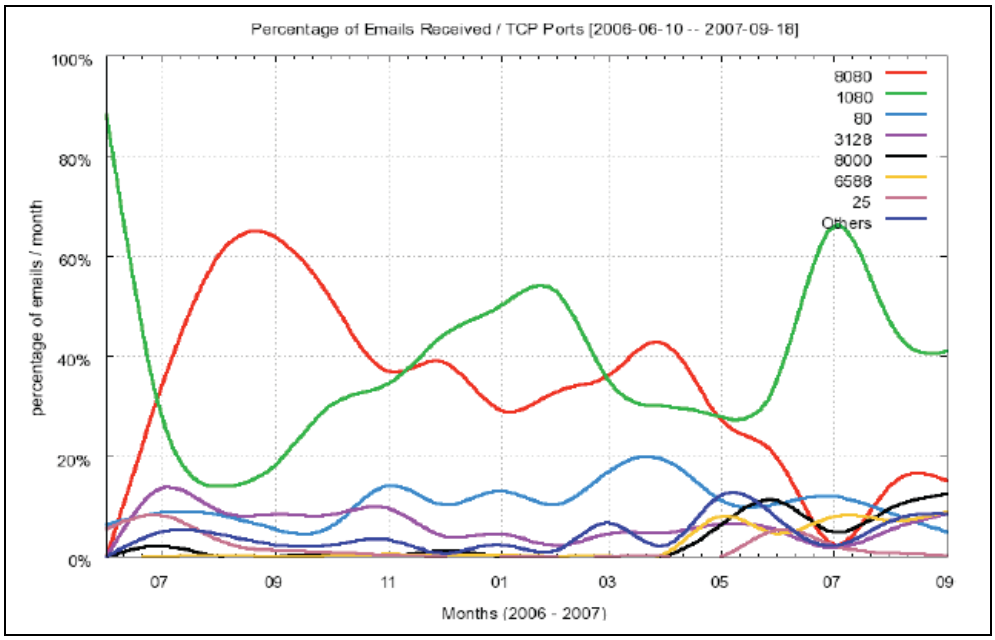
Cert.br 聽到的消息是：代理服務不再是主要的傳送方式，現今多已從殭屍電腦網路(Botnet)發送/轉送 SPAM。

但是，Cert.br 蒐集到的資料卻顯示：濫用開放式代理服務的 SPAM 在過去幾年有增加的趨勢！而且提供傳送 SPAM 的工具仍提供偵測代理服務的功能，其收集到的數據也顯示代理服務仍居於被用來傳送 SPAM 的前十名，使用的 TCP 埠位(port)中，1080、3128、6588、4480…等都是代理服務軟體常

用埠位。這些資料是從 CERT.br 的報告及 honetpot[2]中蒐集到的。

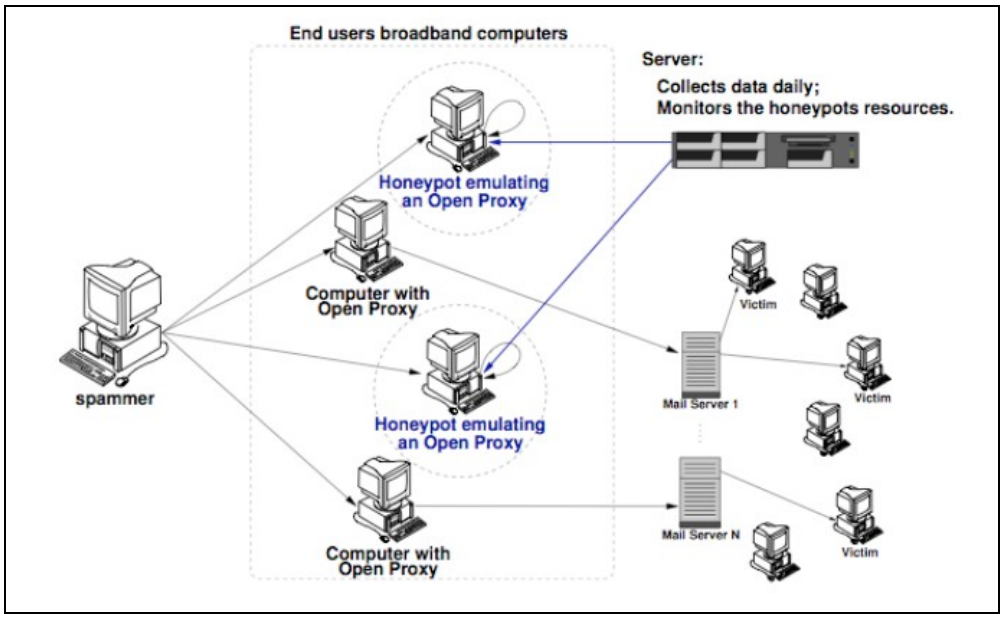
#	TCP Port	Protocol	Usual Service	%
01	1080	SOCKS	socks	37.31
02	8080	HTTP	alternate http	34.79
03	80	HTTP	http	10.92
04	3128	HTTP	Squid	6.17
05	8000	HTTP	alternate http	2.76
06	6588	HTTP	AnalogX	2.29
07	25	SMTP	smtp	1.46
08	4480	HTTP	Proxy+	1.38
09	3127	SOCKS	MyDoom Backdoor	1.00
10	3382	HTTP	Sobig.f Backdoor	0.96
11	81	HTTP	alternate http	0.96

從 2006 年六月到 2007 年九月這一年多的觀測中顯示，使用 8080 埠位的比率明顯降低，而 1080 埠位的使用率則一直都居高不下，走 Http 通訊協定的 80 埠位則居第三順位。



下圖為 Honeypot 的架構。此一 SpamPot 計畫是由 NIC.br 及 CGI.br 共同進行，為反垃圾郵件工作小組(Anti-spam Task Force)的工作項目之一。其係使用 OpenBSD、Honeyd 等軟體，分別在五個不同的寬頻網路服務提供者(Cable*2、ADSL*3)中放了十個 honeypot(每個網路設置一個家用及一個商用的連線)，並嘗試混淆 Spammer 企圖確認為 honeypot 的嘗試行為。

[2] 網址：http://www.honeypots-alliance.org.br/stats/



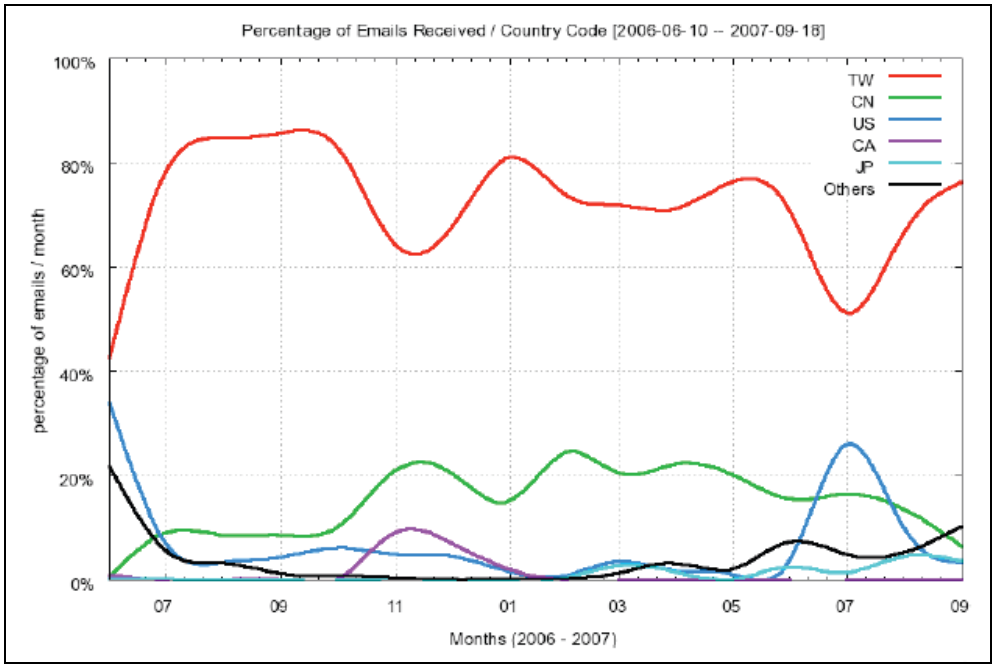
測試的期間為 2006/6/10-2007/9/18，計 466 天。從這十個 honeypot 中共收集到 5 億 2 千 4 百萬封電子郵件，收件對象共有 48 億 5 百萬人，平均每一封電子郵件寄給 9.1 個人，每日平均收到 120 萬封電子郵件。計有 21 萬 6 千多個來源 IP，3006 個 AS 碼 (autonomous system)，及 165 個國碼 (Country Code, CC)。

在蒐集到的 SPAM 中，來自亞洲的台灣(TW)其比率高達 73.43%，第二名是中國大陸 (CN)，在接收比率上只佔 15.80%，濫發程度遠遠低於台灣，第三名才是鄰近的美國 (US)。

#	CC	E-mails received	%
01	TW	385,189,756	73.43
02	CN	82,884,642	15.80
03	US	29,764,293	5.67
04	CA	6,684,667	1.27
05	JP	5,381,192	1.03
06	HK	4,383,999	0.84
07	KR	4,093,365	0.78
08	UA	1,806,210	0.34
09	DE	934,417	0.18
10	BR	863,657	0.16
		Subtotal:	**99.50**

下圖顯示個別國碼在每個月所接收到的 SPAM 的百分比。

很明顯的，台灣寄發的 SPAM 量遙遙領先其他來源國。

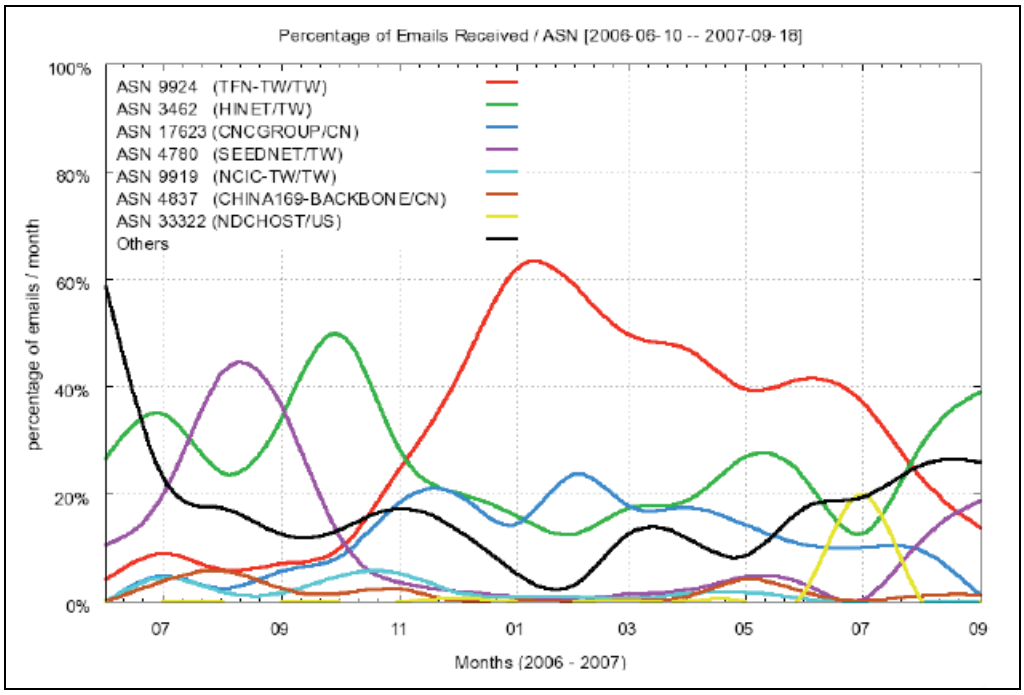


再進一步分析 AS 自動系統，以判別發送這些 SPAM 的來源網路服務提供者。前十名中，有五名來自台灣。第一名是台灣固網(TFN)，占 32.60%，其次是 HINET，占 25.04%，第三才是來自中國大陸深圳地區的網通(CNCGROUP)，其他來自台灣的網路服務提供者為第四名的 SEEDNET，第五名新世紀資通，及第九名億聯科技。

#	ASN	AS Name	CC	E-mails	%
01	9924	TFN-TW Taiwan Fixed Network	TW	170,998,167	32.60
02	3462	HINET Data Communication Business Group	TW	131,381,486	25.04
03	17623	CNCGROUP IP network of ShenZhen region	CN	65,214,192	12.43
04	4780	SEEDNET Digital United Inc.	TW	54,430,806	10.38
05	9919	NCIC-TW New Century InfoComm Tech Co., Ltd.	TW	9,186,802	1.75
06	4837	CHINA169-BACKBONE CNCGROUP	CN	9,025,142	1.72
07	33322	NDCHOST - Network Data Center Host, Inc.	US	8,359,583	1.59
08	4134	CHINANET-BACKBONE	CN	7,287,251	1.39
09	18429	EXTRALAN-TW Extra-Lan Technologies Co., Ltd	TW	6,746,124	1.29
10	7271	LOOKAS - Look Communications Inc.	CA	5,599,442	1.07
				Subtotal:	**89.26**

下圖顯示在資料收集期間，SPAM 的來源網路服務提供

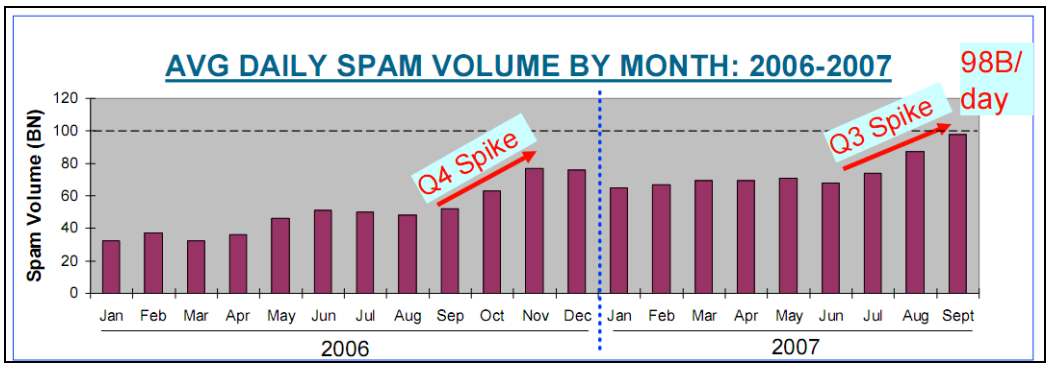
者每個月所佔的比率圖。紅色線為台灣固網、綠色線的 HINET、及紫色線的 SEEDNET 皆有超過 40%的 SPAM 發送量紀錄。



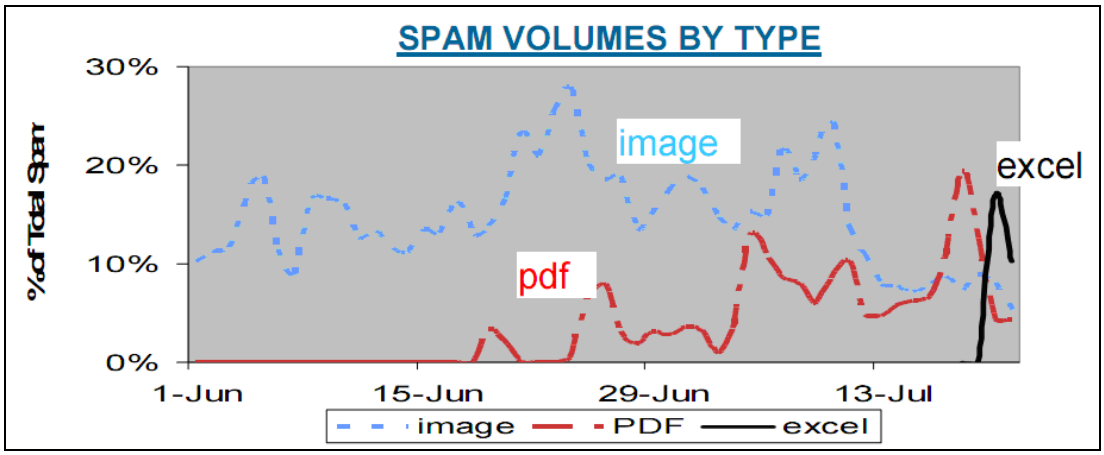
除上述分析方式外，未來則建議使用 Data Mining 技術來辨識 SPAM 的語言種類、包含的網址、及 Spammer 的活動，並偵查 Phishing 及其他線上犯罪活動，也會考慮以國際合作方式共同對抗 SPAM。

❖ IronPort

IronPort 是一家專門販售電子郵件及網路安全產品的業者，現為 Cisco 的部門之一。本部份由 IronPort 副總裁(vice Prisident) Patrick Peterson 報告。現今世界上每天約有 980 億封信是 SPAM，下圖顯示從 2007 年 6 月以來，SPAM 以每月增加 12%的速度快速上升。



緊隨著 Image SPAM 及 Pdf SPAM 而來的是在今年 7 月 21 日出現了 Excel 型態的 SPAM，在一個鐘頭內的量就衝到所有 SPAM 量的 17%。



✓ 議題3：生活中的一天

本議題則由AT&T、美國FTC、StrongMail、與Cablevision分別報告。

❖ AT&T

AT&T網路濫用中心(Network Abuse Center, 以下簡稱NAC)指派寬頻濫用(Broadband Abuse)部門經理Joel Casey提出本次報告。

NAC每天的工作包括：管理個人及企業用戶帳號、協助ISP電子郵件服務、接受專業的服務與安全諮詢、處理來自執法機關的要求，及侵犯他人著作權、客戶被釣魚網站竊取個人資訊等出庭需求及法務，建立自動化工具及維護，訂定使用及維護政策等事項。

從1996年到現在，NAC面對的是越來越大量繁複且多樣的客戶需求、安全問題，NAC持續改善流程，將程序自動化後便能夠減少大量需求的人力，並建立各種評量標準(ex. Abuse Ratio)以提高服務品質。雖然如此，NAC仍遭遇到以下的挑戰：當客戶的電腦受到感染時，該如何清除病毒？NAC在未來，勢必得不斷地發展新的防護技術，以對抗不斷發展的病毒問題。

❖ 美國FTC

由調查員(Investigator) Sheryl Drexler報告美國ISP與執法機關的合作情形。

FTC在反垃圾郵件的政策上採取三方面並進的策略：研究調查、教育大眾、及執行公權力。從1997年以來，FTC已經處理了90件spam的相關案例，其中包括了240個被告。FTC的Spam Database (spam@uce.gov)每天可以收到30萬封SPAM，透過偵查工具以及關鍵性的合作，能有效找出spammer。

在2003年CAN-SPAM法案出爐後，到了2004年FTC有了第一個案例：Phoenix Avatar，FTC指控被告利用spam

販賣假的減肥貼布。其後，在 2006 年 1 月 FTC 指控 William Dugger 在未告知的情形下，使用他人的家用電腦散佈關於性交易的電子郵件，在這個案例中，FTC 面對到以下的挑戰：需要具有專業知識的證人、須提出寄送郵件的證明、被告輪流使用不同的網域名稱發送同一封信、被告逃避過濾軟體的方法。

FTC 在執法上也面臨許多其他的挑戰，諸如：Botnets、惡意程式碼、機密性、對於假 ISP 的信任問題、對於下游 ISP 的販賣及移轉 IP 位址的問題、盜用信用卡資料、偽造付款資訊、Whois 資料庫及 IP 位址之處理、使用 Proxy 及相關機制隱匿行蹤等問題。

FTC 認為，並沒有所謂的「銀色子彈」可以一舉擊敗 SPAM，只有從強化執法者的力量(如 US SAFE WEB Act)、教育消費者、建立新的商業及技術方法，並透過公、私領域及執法者間的合作關係，才能有效減少 SPAM。

❖ StrongMail

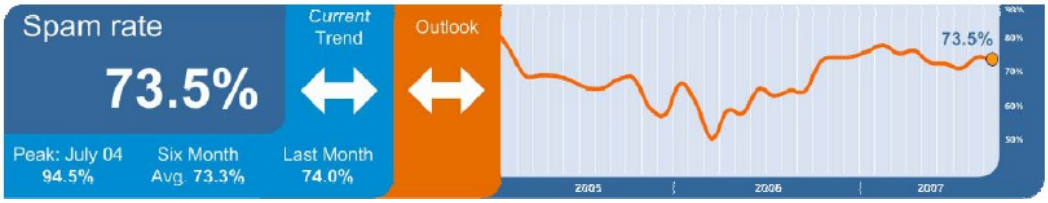
StrongMail 是一家提供企業在市場及交易上使用的電子郵件服務提供者。由傳送服務部門指導(Dir. Delivery Service) Spencer Kollas 報告。

StrongMail 的工作是向客戶說明什麼是最佳的解決方案(best practice)以及如何去執行這些作業方式，其必須瞭解 ISP 使用的系統以及執行的政策，才能減少聯繫 ISP 詢問解決方案的需求，對客戶而言，StrongMail 是他們的遠端雇員，與其內部人員一起工作，以確保商業上的成功。每天的工作就是要管理郵件遞送服務、到客戶端處理新系統、接受客戶諮詢提供最佳解決方案、向客戶解釋為何問題是出在他們的 ISP 上、與 ISP 合作以瞭解如何協助他們去對抗 SPAM，隨時瞭解最新的法令規範、審查潛在新客戶的背景紀錄。

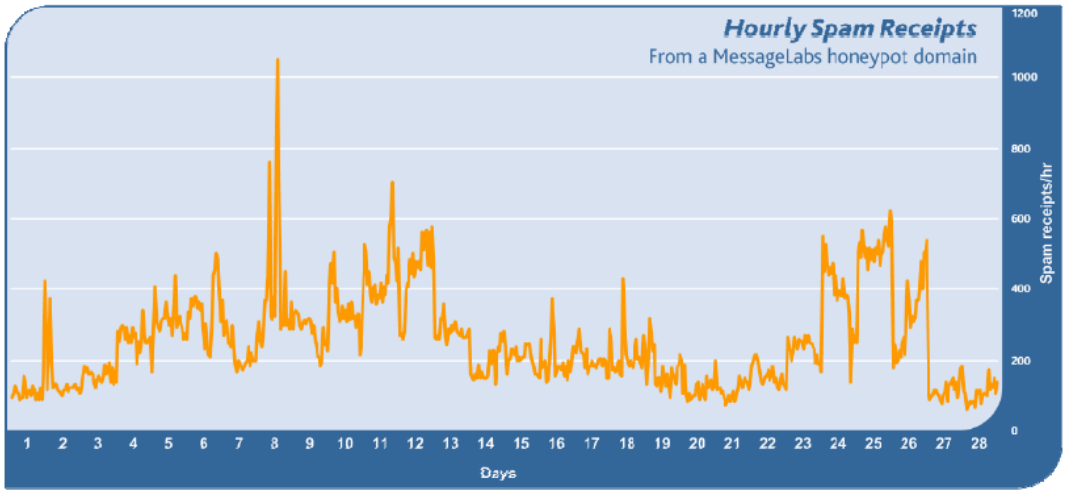
✓ 議題 4：新興的威脅

❖ MAAWG

首先 MAAWG 訊息實驗室首席分析師 Mark Sunner 在演講(如附件：2007 Deadly Sins: Emerging Technologies 簡報)中提到，2007 年 9 月所統計的正常郵件與垃圾郵件比率為 26.5%：73.5%，其每日統計數據請參考下圖所示。



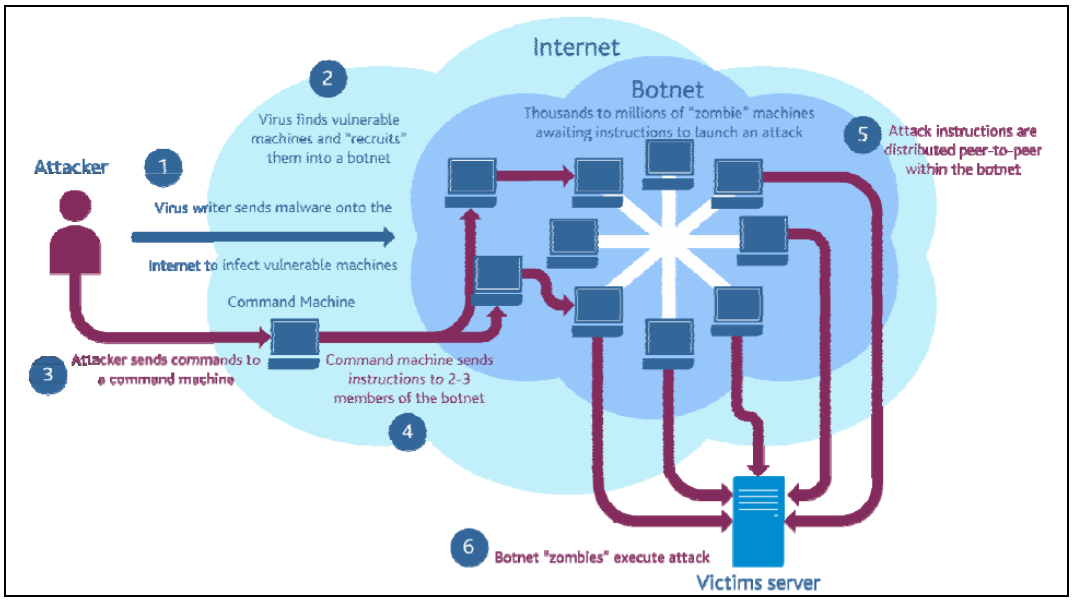
引用來源：簡報 Deadly Sins: Emerging Technologies, p.2



引用來源：簡報 Deadly Sins: Emerging Technologies, p.4

對於濫發者發送垃圾郵件時使用的手法，也透過下圖進行說明，其傳遞路徑如下：

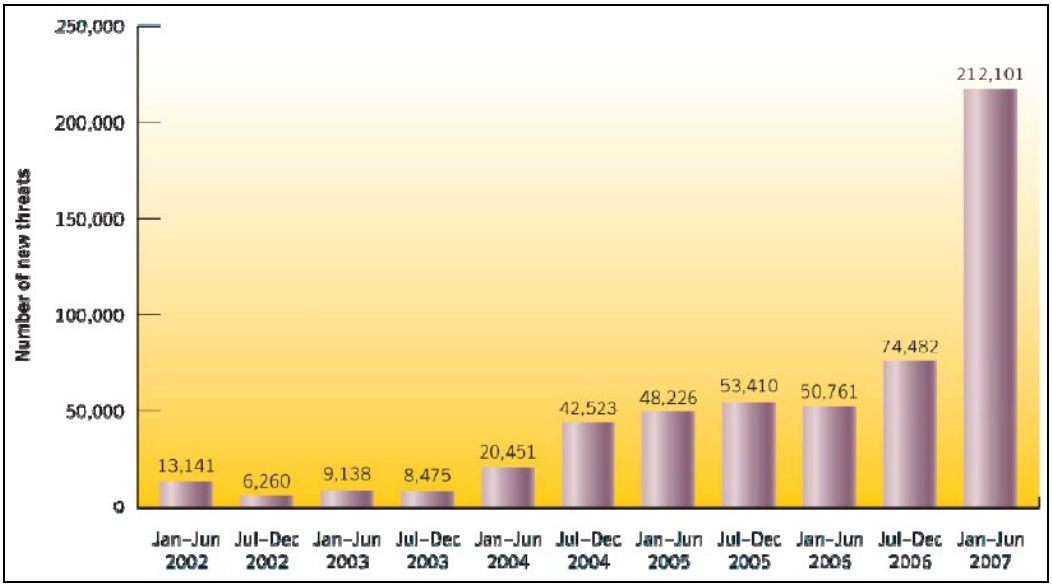
1. 以惡意程式透過網路介面針對具有弱點的主機進行入侵。
2. 將 Bot 程式植入入侵成功的主機。
3. 濫發者發送命令給訊息主機進行任務分派。
4. 訊息主機將任務指令分派給各個殭屍電腦/網路。
5. 殭屍電腦/網路收到只是進行分散式點對點的攻擊指令。
6. 郵件到達受到攻擊的祭品(郵件主機)。



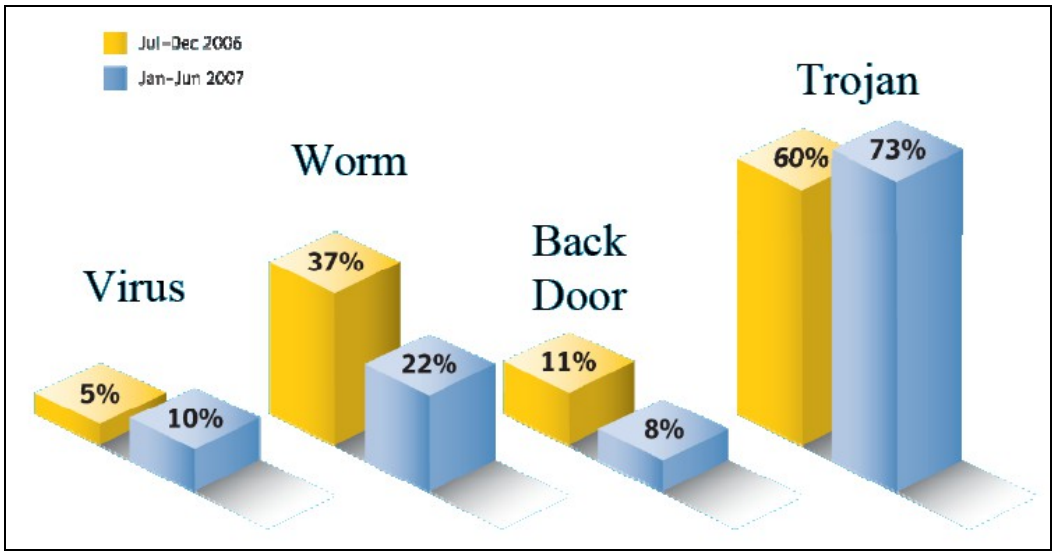
引用來源：簡報 Deadly Sins: Emerging Technologies, p.10

❖ 賽門鐵克

緊接著由 MAAWG 賽門鐵克資深管理師 David Cowings 針對惡意程式議題進行演講(Malware Threat Landscape & Emerging Threats Overview 簡報)。經觀察，惡意程式威脅有逐年上升的傾向，尤其在 2007 年 1 到 6 月所統計的資訊較前半年增為 3 倍；種類以特洛伊木馬占 7 成 3 最為嚴重。另外目標為郵件密碼、通訊錄與信箱位址合計占 22%。相關統計數據請參考下圖。



引用來源：簡報 Malware Threat Landscape & Emerging Threats Overview , p.3



引用來源：簡報 Malware Threat Landscape & Emerging Threats Overview , p.5

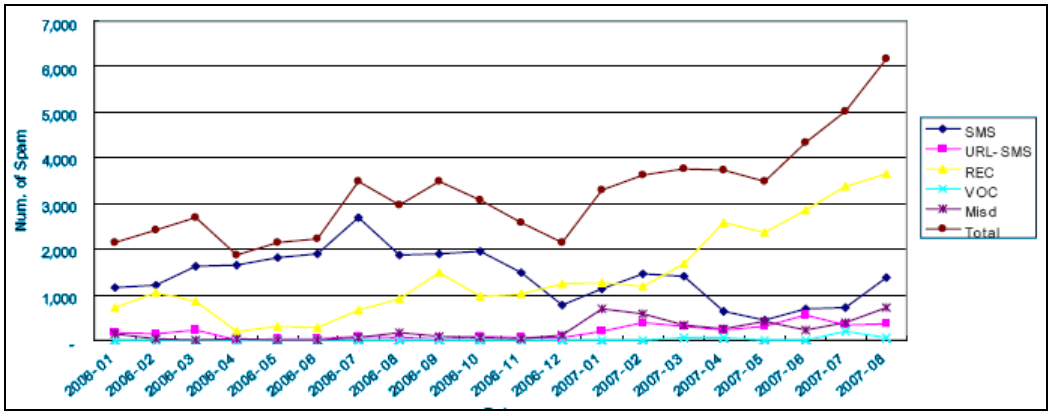
Rank	Item	Percentage	Range of Prices
1	Credit Cards	22%	$0.50–$5
2	Bank Accounts	21%	$30–$400
3	Email Passwords	8%	$1–$350
4	Mailers	8%	$8–$10
5	Email Addresses	6%	$2/MB–$4/MB
6	Proxies	6%	$0.50–$3
7	Full Identity	6%	$10–$150
8	Scams	6%	$10/week
9	Social Security Numbers	3%	$5–$7
10	Compromised Unix Shells	2%	$2–$10

引用來源：簡報 Malware Threat Landscape & Emerging Threats Overview , p.9

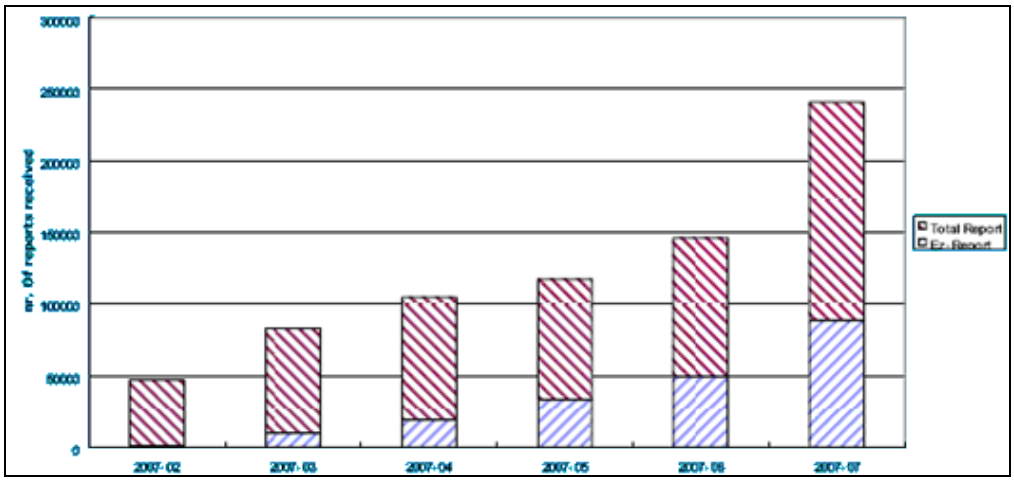
❖ KISA

而後由韓國 KISA 資安分析師 Joon Kim 針對韓國垃圾簡訊(Mobile Spam)議題進行報告(Mobile Spam in Korea 簡報)，在韓國簡訊使用量日益增多，其內容統計在成人資訊佔首位、其次為金融類型。於 1999 年 9 月開始在法律上採取選擇退出(OPT-OUT)機制進行立法規範，2004 年 10 月又將垃圾簡訊修法為選擇加入(OPT-IN)機制，在 2006 年 7 月進行舉報數量統計，平均約每 1000 封簡訊會有一封被民眾舉報濫發，下圖顯示韓國提供民眾使用的「EZ-Report」機制反應舉報的情形，明顯看出將垃圾簡訊回報功能嵌入行動裝置內的回報機制，已漸

漸被民眾所接受及使用。最後以「資訊安全工作永無止境」作為結語，期許與會代表一起努力。



引用來源：簡報 Mobile Spam in Korea, p.5



引用來源：簡報 Mobile Spam in Korea, p.9

最後幾個議題依次為 NEUSTAR 資深副總裁 Rodney Joffe 針對分散式阻絕服務攻擊(DDoS)的議題演講(The Real Damage Caused by a DDoS 簡報)、網域保證理事會 John R. Levine 針對網域測試與威脅議題演講(Domain Tasting and other domain threats 簡報)、MAAWG 反垃圾郵件技術主任 Matt Sergeant 針對經濟上的陰影議題演講(Shadow Economy At Work 簡報)、Spamhaus 產業公會聯合會 Richard Cox 針對組織工作進行介紹(The Spamhaus Project 簡報)，其資料均收錄在附件內，由於內容龐雜，將不另說明。

✓ 議題5：各組織或國家資訊更新

在討論本議題時，分別由各國際性組織、地區或國家等，提出各該相關資訊更新報告，大致上有CNSA（The European Union Contact Network of Spam Authorities）、OECD等組織提出更新報告，另外，巴西、韓國及保加利亞也提出其國內關於管制SPAM的更新資訊。

其中CNSA於2007年6月才舉行過相關會議，亦在本議題討論時提出更新報告。CNSA係因2004年歐盟《網路隱私指令》生效，再加上歐盟需要有一個可以針對SPAM問題，促進跨境合作、抱怨處理以及補救措施之機構等因素而成立，其成員大多係歐盟各國之資訊保護主管機關、電信事業主管機關或消費者保護主管機關(部門)，每年於布魯塞爾舉行三次會議。

CNSA之任務，大致上有下列幾點：

1、為國際間主管機關或主要產業間，提供資訊交換平台。

2、可在CIRCA[3]網站散佈及交換資訊。

3、對於各主管當局管理SPAM官員之聯繫細節。

4、和其他組織如OECD、LAP合作。

在該組織於2007年6月會議中提出，CNSA對於未來之展望，在於發展防制間諜軟體的方針，並且在消費者保護法建構內，加強主管當局之合作力量。

在各國資訊更新中，巴西提出其國內反垃圾郵件工作小組工作成果。該工作小組之任務為：

1、提供反制SPAM之技術規則。

2、提供關於SPAM之資訊給不同層面的使用者。

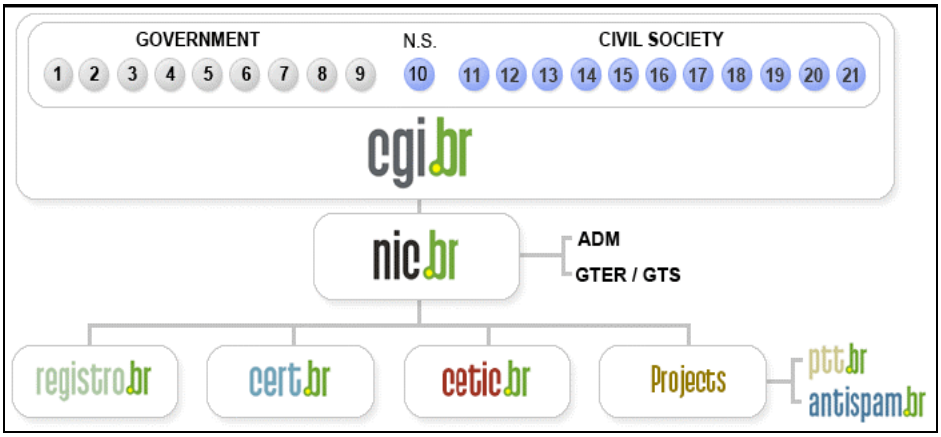
3、提出新法的建議方案。

4、為國際合作之連結點。

該工作小組之組織架構可分為政府機關及民間團體，政府機關大致上有科技部門主管機關、通訊部門主管機關以及

[3] Communication & Information Resource Centre Administrator

國際貿易主管機關等。民間團體則有ISP及軟硬體製造業者等，其詳細內容如下圖及表列所示。



1 – Ministry of Science and Technology (Coordination)
2 – Ministry of Communications
3 – Presidential Cabinet
4 – Ministry of Defense
5 – Ministry of Development, Industry and Foreign Trade
6 – Ministry of Planning, Budget and Management
7 – National Telecommunications Agency
8 – National Council of Scientific and Technological Development
9 – National Forum of Estate Science and Technology Secretaries
10 – Internet Expert
--（以下為民間機構）
11 – Internet Service Providers
12 – Telecommunication Infrastructure Providers
13 – Hardware and Software Industries
14 – General Business Sector Users
15 – Non-governmental Entity
16 – Non-governmental Entity
17 – Non-governmental Entity
18 – Non-governmental Entity
19 – Academia
20 – Academia
21 – Academia

在立法方面，目前在巴西國會及參議院報告中，係採取OPT-OUT機制，但仍有許多爭議。而該工作小組的貢獻，在於與FGV law school[4]合作，提出一份立法研究，在評估所有項目後，建議立法代替方案為軟性OPT-IN機制。

除巴西外，保加利亞亦提出其國內關於SPAM防制的立法架構，其報告中指出，保加利亞對於SPAM之定義，仍限定在不請自來的商業性訊息，並將管制SPAM之法律，分別

4 Fundação Getulio Vargas Law Schools.

散佈在電子商務法及電子通訊法中，並非成立SPAM專法加以規範，為保加利亞立法的特殊之處。

✓ 議題6：跨境執法的合作

跨境執法的合作，一直是防制SPAM最重要的議題，主要係因網路無國界之特性，垃圾郵件跨國濫發行為的猖獗，使得國際合作益發重要。本議題中，由歐盟代表Jean-Charles報告歐盟「網路犯罪公約」[5]之規範，該公約為網際網路犯罪之國際執法合作中，最具代表性的公約之一。

「網路犯罪公約」係由歐盟及加拿大、日本、南非及美國等國共同制定，於2001年開放簽署，並於2004年7月生效。該公約一共有4個章節，第一章係名詞定義，第二章則規範公約簽署國應採取之措施，分三部：刑法、刑事訴訟法及司法管轄權規範之。第三章係關於國際合作之規範，第四章則規範歐盟會員國及非會員國對於該公約之簽署及加入條款。

另外，在該公約的基礎下，前述歐盟及加拿大、日本、南非及美國等國，於2003年又開放簽署「經由電腦系統進行種族歧視及迫害議定書」[6]，該議定書於2006年3月生效，使得跨國網路犯罪執法合作，有更進一步的發展。

(2) 執法機構的網路威脅調查會議

✓ 議題1：認識垃圾郵件

由MAAWG資深技術顧問John Levine進行演講，其議題集中在：

1、分析郵件資訊的基本技術，學習到有關郵件標頭基本結構及其意義。分析電子郵件標頭時，其資訊可分為手動增加的部份(包括寄件者、收件者、主旨、寄送日期等，當然也包括偽造的資訊)和自動填入的部份(由郵件主機新增的資訊，包括Received、Delivered-To及Message-ID等，此部份也包括濫發者偽造的資訊。)

[5] 「The Convention on Cybercrime」
[6] 「Protocol on racism and xenophobia committed through computer systems」

2、MIME[7] 型態及其相關格式介紹，並依照濫發者可能拿來利用的部份進行說明。它是一種網際網路上的標準規格，制定的動機是要在只能可靠地傳輸純文字資料的電子郵件裡可靠地夾帶多媒體訊息，以擴充其功能，但是目前這些可供夾帶的多媒體訊息，也成為夾帶惡意程式或廣告的途徑。

3、標頭資訊哪些是真實或偽造之判定參考，並利用正常與偽造的範例做說明，範例包括 Outlook、Web mail、Hotmail、Yahoo、Gmail、Non-web Gmail 以及 Generic web mail 等 MUA 的正常標頭資訊；Script mail、Script/web 及 Zombieware 等經過偽造後的標頭資訊。

4、利用網路共享(舉例：WHOIS 和 DNS)資源，進一步稽核解析的說明。WHOIS 提供 IP 位址擁有者或是註冊者的相關資訊查詢；DNS 是提供主機網域名稱及其 IP 位址鏡像查詢服務。

✓ 議題 2：e-Crime 工具在網路上如何協助犯罪調查

由 IronPort System V-P 技術部門 Patrick Peterson 進行演講，其議題集中在：如何使用一些網路散發(網路流量、封包擷取、目標 IP 位址、來源與目的地埠號等)的資訊來幫助取得您所感興趣的資料，並透過儀器設備進行實例說明，讓與會人員透過監控螢幕來看到針對這些資料流蒐集後得到的資料一覽表。這所被分類整理後的資料，即可利用其他的工具或技術來進一步解析。

✓ 議題 3：行政機構如何協助濫發者追蹤

由 ACMA[8], AntiSpam Team 資深研究員 Chris Duffy、FBI[9] 特別代理人 Thomas X. Grasso 及 FTC 法律顧問 Steven Wernikoff 進行演講，此部分議題係探討關於調查及追訴濫發者之實務執行作為，尤其著重於討論執行機關於執行調查作為時之法律面議題，包括從 ISP 業者取得資訊、與外國之對等機構分享資訊，及提起民、刑事訴訟之立論基礎等。

✓ 議題 4：控制惡意程式

[7] MIME, Multipurpose Internet Mail Extensions
[8] ACMA, Australian Communications and Media Authority, 澳洲通訊與媒體的主管機關
[9] FBI, Federal Bureau of Investigation, 美國聯邦調查局

由 Dutch OPTA[10] 數位資訊研究員 Marcel van den Berg 進行演講，其議題集中在如何去控制惡意程式與快速分析。這一系列包含介紹利用工具以及方法，去針對筆記型電腦中用 Vmware 執行 Windows XP 系統的分析。

[10] Dutch OPTA, Dutch Post and Telcommunications Authority, 荷蘭郵政與通訊管理機構

叁、檢討與建議

甫於兩年前，我國即以交通部名義加入倫敦行動計畫（LAP）成為正式會員，隨即於同年10月由前電信總局派員參與第二屆「垃圾郵件主管機關聯繫網路研討會」，開始在防制SPAM的國際合作上嶄露頭角。

歷來我國外交處境艱辛，中共時藉機干預、阻撓我國參與國際組織之機會，然未遭LAP會員國反對而能順利加入此一國際組織，諒亦係各國深刻體認到我國資訊科技與網路產業發達，在國際合作促進網路安全、打擊網路犯罪及防制垃圾郵件工作上極具重要地位之故。

現今，適逢我國通訊傳播新紀元之始，本會身為管制垃圾郵件之主管機關，首度以「國家通訊傳播委員會」名義出席LAP第三屆研討會議，時值本會初建，萬務蓬興之際，而能在研商網際網路秩序維護相關議題之重大國際場合上，代表我國列席與會，此對本會而言更具有特殊意義。

2007年春，倫敦行動計畫組織曾向我方捎來一封電郵，內容指出，2月8日荷蘭警方與美國FBI合作，於阿姆斯特丹逮捕21名spammer，其中四名奈及利亞籍spammer將被引渡至美國，LAP組織以此一案例在國際合作打擊SPAM及網安犯罪上，具有象徵性意義，乃通報所有LAP會員國參考，除證SPAM現象為禍之烈外，更彰顯了跨國合作在維護全球網路秩序上之重要性。

本次會議，涉及之網路安全議題相當廣泛，當中針對垃圾郵件防制，秉持LAP設立宗旨，除冀圖震聾發聵、警醒世人SPAM現象之嚴重性，尚積極就對抗濫發行為之可能措施進行整合、磋商，遍觀其內容，包含三大主題：規範架構與執法案例、技術演進與調查工具、數據統計與歸納分析，為凝聚共識，擬針對上開會議內容提出檢討事項如下：

一、借鑑外國立法與執法經驗

會議中，美、澳兩國與會人員在介紹該國法規時，詳細說明其主管機關之執法權限，並針對相關執法情形加以簡介，FTC 更坦言不諱道出其執法與舉證上的諸多困難，FTC 最終認為，對抗 SPAM 並無一蹴可幾之捷徑，透過多面向、公私部門合作之策略，始可有效消弭電郵濫發現象。

所謂他山之石，可以攻錯，外國之立法與執法經驗殊值參考，此次美、澳兩國在會議中所提供之立法設計與寶貴執法經驗，適足以供各國日後執法措施之借鑑，務應積極汲取相關資訊。

二、建立政策與法律評估機制

此次議題中，為回應 OECD 於 2005 年提出之評估機制（existing metrics）研究，以求透過數據測量之方式，評估政策、法制、技術及未來變化之「有效性」，除 MAAWG 發表其「電子郵件評估計畫」外，巴西 Cert.br、Symantec、Ironport 之代表均透過數據分析之方式，從 SPAM 各種觀察角度，量化其嚴重程度，具體言之，目前有高達 86.7%郵件屬垃圾郵件，且多數係利用 OPEN PROXY（51.09%）之方式進行，值得警惕的是，從巴西蒐集的資料顯示，來自台灣的 SPAM 數量高達 73.43%，甚至前十大發送 SPAM 之網路服務提供者，竟有半數來自台灣，且第一、二名分別是台灣固網與 HINET。

透過數據之統計調查，除可知悉目前 SPAM 之濫發現象外，尚得藉以設定立法項目之優先順序，或分析既有管制手段之效益，甚或以此作為日後各國法規影響評估之參考，均屬適切之分析途徑，務應積極掌握。

三、技術演變與調查手段進化

會議中指出，目前日趨嚴重之兩種攻擊型態包括 BOTNET（殭屍電腦）與散佈惡意軟體，其他尚在演進者尚有分散式阻絕服務攻擊

（DDoS）、網域測試與威脅等項，鑑於技術手法不斷精進，與會者亦引介相關之調查技術，包括郵件資訊基本分析技術、信首資訊真偽判定、利用網路共享資源進行稽核、e-Crime 犯罪調查工具的使用、控制惡意程式，甚至論及行政機構如何追查濫發者等相關議題。

以上各種技術實務，各國均已投入相當的研究人力著手瞭解中，日後宜配合法律施行，透過強化追查技術以及提升舉證能力，以佐立法成效。

四、跨境執法與國際合作之重要性

本次會議，CNSA 針對 SPAM 事項提出資訊更新報告，歐盟等國亦針對「網路犯罪公約」及「經由電腦系統進行種族歧視及迫害議定書」進行報告，由於 CNSA 之設立目的在於提供資訊交流平台，作為各國主管機關聯繫管道，鑑於其與 LAP 間之密切關係，各國宜在 LAP 的基礎上與 CNSA 保持合作關係，另各國應積極簽署加入上開兩大國際多邊公約，以收跨國合作管制 SPAM 之成效。

在與各國代表共同參與本次會議諸多議題討論後，獲得相當多的啟發，謹提出下列建議以供本會制定政策與修法之參考：

1. 積極推動相關立法：考目前世界各國 SPAM 立法，均涵括前階行為、發送規範、違法效果、業者權義與配套制度等五大重要規範要素，我國「濫發商業電子郵件管理條例」草案之研擬，亦依照上開要素，積極強化制度設計，業經行政院通過送請立法院審查，主管機關應積極推動立法，使濫發行為之管制有法可據，亦可宣示我國阻絕 SPAM 之決心。
2. 鼓勵業界防制作為：網際網路服務業者之防堵機制，影響整體垃圾郵件之管制成效甚鉅，為激勵業者主動、積極過濾或阻絕垃圾郵件之能量，主管機關宜採行適當之行政措施促使業者配合，以強化業界自律作為。

3. 加強教育宣導事宜：主管機關應透過各種管道對民眾進行教育宣導，從灌輸正確之 E-Mail 使用規範著手，配合發信行為之立法管制，藉由全民防制，從收信端抵制濫發者之不當發送行為，除可消弭濫發現象外，並可有效降低個人資料外洩風險及減少殭屍電腦（BOTNET）之發生率。

4. 持續深化國際合作：我國宜在 LAP 之基礎上與 CNSA 保持合作關係，另應謀求簽署加入各種防制垃圾郵件國際多邊公約之機會，並積極與各國洽簽防制垃圾郵件合作瞭解備忘錄，以建立跨國合作管制 SPAM 之聯防網絡。

我國外交情勢艱難，LAP 為少數我國得以成功加入之全球性國際組織之一，基於網路全球化、國際性之特性，我國得以在「網路治理」（Internet Governance）此一範疇內，在國際組織內深化我國之影響力，主管機關應予以重視，尤其網路世界發達以來，已漸促使傳統之國家、地域概念稀薄，我國既已在此領域獲取一定之外交空間，更應把握契機，透過將國內之立法、執法與國際合作事項交相運用的手段，配合全球網路化之浪潮，開展我國寬宏之外交戰略縱深。