出國報告(出國類別：參加國際會議)

出席「第五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：副研究員　李德玲
派赴國家：葡萄牙里斯本
出國期間：98 年 10 月 5 至 11 日
報告日期：98 年 12 月 25 日

摘要

網際網路自 1950-60 年代發展以來，快速演進之趨勢，影響全人類各個層面的生活。隨資訊科技、寬頻服務及網路電子商務蓬勃發展之同時，垃圾郵件、惡意程式、網路病毒及跨國網路犯罪等問題湧現，衝擊全球，國際社會對於共同合作以促進網路安全、打擊網路犯罪及防制垃圾郵件之必要性，已形成共識。

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，自 94 年 8 月 4 日以「臺灣」名義加入「倫敦行動計畫（LAP）」成為正式會員以來，逐年派員參與「倫敦行動計畫及垃圾郵件主管機關聯繫網絡(LAP/CNSA)研討會」，積極展現國際合作防制垃圾郵件之決心。

本次會議之主題為「打擊垃圾郵件」（Spam-Fighting），會議之宗旨有提升網際網路發展、建置周全法規機制、善盡保護消費者、資訊安全及執行法規之責任、加強資訊分享、意識提升、建立全球性合作夥伴關係等項。鑒於會議討論事項相當廣泛，本報告僅就會議議程、議題內容、檢討與建議等擇要撰擬，至期可對相關業務之推動有所助益。

出席「第五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 1

貳、「第五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」 3

一、會議時間、地點及議程 3

二、開幕式 3

參、「第五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」 5

一、2009/10/7 議程 5

議題一：網際網路調查之教育及訓練 5

議題二：美國 FTC 國際案例介紹 8

議題三：殭屍電腦網絡之追蹤 11

議題四、以網際網路消費者防禦觀點進行之調查方法 13

二、2009/10/8 議程 17

議題一、垃圾郵件之趨勢及統計 17

議題二、垃圾郵件計量及葡萄牙垃郵案例介紹 18

議題三、新興的威脅 19

議題四、電子郵件行銷與垃圾郵件 20

議題五、馬來西亞防制垃圾郵件之立法 22

議題六、奧地利有關反制垃圾郵件之報告 24

議題七、歐盟線上隱私權及資料保護議題 27

議題八、加拿大反垃圾郵件法規 29

議題九、荷蘭之公私合作關係 32

議題十、自願性資料交換所涉隱私問題 34

三、2009/10/9 議程 35

議題一、打擊垃圾郵件之技術方案 35

議題二、OECD 2006 年跨國反制垃圾郵件法規建議之檢討 36

議題三、日本反制垃圾郵件之成效 38

議題四、RIPE NCC 簡介 41

肆、檢討與建議 45

一、借鏡外國立法與執法經驗 45

二、持續加強國際合作.....45
三、主動積極參與防制事務.....46
四、擴大防制機制並共同努力.....46

附件：「第五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」會議議程

壹、前言

網際網路自 1950-60 年代發展以來，快速演進之趨勢，影響全人類各個層面的生活。依據經濟部技術處委託財團法人資訊策進會 FIND 進行之「我國網際網路用戶數調查」顯示，截至 2009 年 6 月底為止，我國有線寬頻用戶達 487 萬戶，電話撥接用戶數為 63 萬戶，學術網路(TANet)用戶數為 444 萬人，行動網路用戶數為 1,661 萬戶。將上述各個連線方式用戶數經過加權運算，並扣除低用度用戶、一人多帳號與多人一帳號等重複值後，估算我國經常上網人口已達 1,060 萬人，網際網路連網應用普及率為 46%。足見，我國已達資訊化社會之程度。

網際網路、寬頻服務及網路電子商務蓬勃發展之同時，隨之而來的並不全然是正面的影響，眾所周知，垃圾郵件、惡意程式、網路病毒等，正以其成本低廉、易於大量散播、傳送快速之特性，衝擊著人們的正常生活，也讓每個國家的主管機關有所省思。近年來，國際情勢顯示，垃圾郵件已成為網際網路經濟發展之嚴重威脅，各國為解決垃圾郵件帶來之層層問題，無不提出通力合作及共同努力之呼籲。

有鑑於垃圾郵件氾濫情形嚴重，亟待政府加強管理，國家通訊傳播委員會(以下簡稱本會)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)，以作為建構我國商業電子郵件法制環境之基礎；復以濫發行為之防制，除須聯合國內業者組成技術防制網絡，亦應加強國際合作交流，並持續關切國際性事件及活動，以期強化技術防制網絡，宣示我國防制垃圾郵件之決心，並提升我國國際形象。

為善盡國際社會成員之責任，本會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「臺灣」名義加入「倫敦行動計畫」，並派員參與其年度會議，以蒐彙各國防制垃圾郵件之策略及經驗，同時尋求建立國際合作交流關係。本次 98 年 10 月 5 日至 10 月 11 日於葡萄牙里斯本舉辦之「第五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 4 次參與之國際性工作會議，本會特指派法律事務處李副研究員德玲出席會議，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。

本次會議研討之議題，面向廣泛並極為專業，其內容涵括：電子郵件管理法規、主管機關職責、各國防制機制、案例探討、網路安全、網

路犯罪及網路詐騙等多項主題。本報告書謹就以上諸議題予以說明。

貳、「第五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」

一、會議時間、地點及議程：

時間：98 年 10 月 7 日至 10 月 9 日

地點：地點：葡萄牙里斯本（Lisbon, Portugal）

議程：詳附件

- 10 月 7 日：會員國會議
- 10 月 8 日：會員國及業界會議
- 10 月 9 日：會員國及業界會議

二、開幕式：

本次會議係由垃圾郵件主管機關聯繫網絡（the Contact Network of Spam Enforcement Authorities, CNSA）成員之一的葡萄牙通訊主管機關 Autoridade Nacional de Comunicações（National Authority of Communications, ANACOM）主辦，參與會議之國家包括歐盟、美國、加拿大、澳洲、法國、德國、愛爾蘭、紐西蘭、葡萄牙、奧地利、丹麥、日本、馬來西亞及我國。

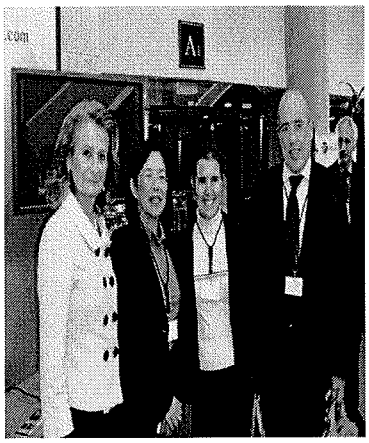
CNSA 為歐盟設立之官方網絡，提供歐盟各國職掌垃圾郵件事務之主關機關聯絡平台，以分享會員間絕佳之經驗，並共同合作打擊存在於不同國家濫發垃圾郵件及訊息之人及事件。

歐盟支援倫敦行動計畫（the London Action Plan, LAP），並為該計畫之觀察員，每年 CNSA 與 LAP 皆共同召開會議。LAP 之目標在促進國際間垃圾郵件及相關議題如網路詐欺、釣魚及散佈病毒之主管機關，共同合作及討論行動議題之機會。

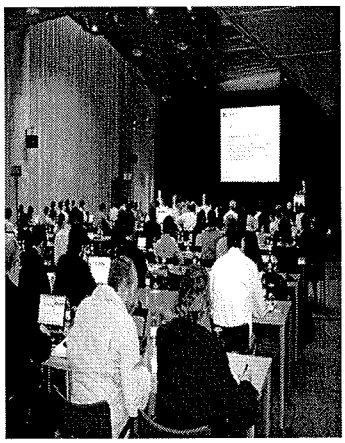
本次會議之主題為「打擊垃圾郵件」（Spam-Fighting），並由 ANACOM 管理委員會委員 Teresa Maury 女士致開幕辭，其內容揭櫫本會議之宗旨及目的如下：

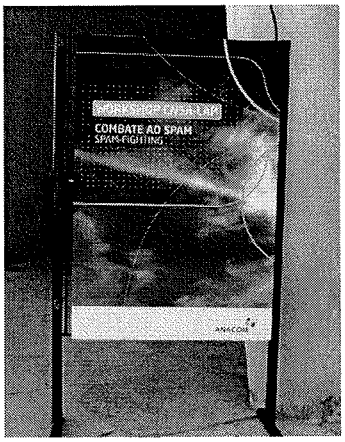
- 促進網絡、科技設備、運用及服務之整合。
- 提升網際網路發展、使用及運用之創造性。
- 強化信心及安全，並確保網路經濟全球化。
- 建置周全法規機制。
- 善盡保護消費者、資訊安全及執行法規之責任。

- 呼籲業界共同行動。
- 加強資訊之分享及意識之提升。
- 建立全球性合作夥伴關係。
- 共同致力未來網路經濟之發展。



Ms. Teresa Maury
Mr. Manuel Pedrosa de Barros





LAP/CNSA WORKSHOP
Spam-Fighting

參、「第五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」

議題討論

一、2009/10/7 議程

議題一：網際網路調查之教育及訓練

本節由愛爾蘭都柏林大學（University College Dublin, UCD, Ireland）網際網路犯罪調查中心主任 Joe Carthy 主講網際網路犯罪之調查。

圖片來源：http://www.ucd.ie/colleges.htm

◆ 背景：

年 代	情 形	內 容
2001 年之前	1、歐盟未有協調網際網路犯罪訓練之整合力量	
	2、LE 不同領域之訓練課程	1、無公認性。 2、無明確學習成果。 3、議題廣泛。 4、常變動先前課程版本。 5、對於參與者或其資格未加以檢測。
	3、歐盟各國尚未致力於創造所謂 LE 社區。	LE 間各國極少或甚且不曾分享資訊。
	4、各國擁有不同層次之專業。	大國或有卓越之調查員，但於證據、罪犯、程序方面之網際網路基礎建設狀況貧乏： 1、無成功合作案例。 2、無起訴案件。
2001/2002 年	歐盟 Falcone 計畫啟動，此計畫之目的在幫助歐盟人民及機構打擊組織性犯罪。	1、建議更深入之協調。 2、建議進行學術性認證之基礎、進階及高階訓練。
2003/2004 年	AGIS 計畫啟動，此計畫係一基礎課程以幫	已發展之基礎訓練。

	助歐盟會員國及將加入歐盟之國家之警察、司法及專業人員，共同合作打擊網路犯罪。	
2005/2006 年	AGIS 計畫繼續執行。	發展 6 訓練課程，其內容包括網際網路及網絡調查。
2008/2009 年	ISEC 計畫啟動，此計畫係有關資訊安全教育及網路安全管理之認證課程。	1、更多之課程。 2、整合所有計畫之課程，創造出 UCD 之 MSc 課程。

◆ UCD 之角色：

（一）UCD 自 2001 年起即開始從事 LE 訓練之協調及認證，隨課程增多，對於訓練教材之管理愈嚴，並維護獲取相關課程之適當管道。2006 年，UCD 成立網際網路犯罪調查中心（Cybercrime Investigation, CCI），其目的在延續 LE 之重心，惟仍以學術為導向，並為非營利性單位。此中心之目標有下列數項：

- 與執法機關、司法部門、業界及相關機構共同合作，以因應網際網路犯罪調查及安全專家從事高科技犯罪之預防與調查工作：
  - ✓ 發展、傳授並建置認證之網際網路犯罪教育課程。
  - ✓ 進行網際網路犯罪之應用及理論研究。
  - ✓ 研發並認證相關工作之軟體。
- 藉由微軟公司之支持，將現行所有訓練具予以升級，此點有助於加速達成相關工作之發展。
- 提供電腦及網際網路犯罪調查碩士學位，並以網路授課，此舉證明有效，並成功塑造 LE 專家社區。
- 提供業者 MSc 數位調查課程。

（二）LE 之堅實網絡

- 提供學術性建議予歐洲網際網路犯罪調查訓練協調小組。
- 為歐洲高科技犯罪訓練工作小組愛爾蘭代表一員。
- 參與國際刑警組織 Interpol（The International Criminal Police Organization）高科技犯罪工作小組，並與該單位及 IMPACT (The International Multilateral Partnership Against Cyber-Terrorism)簽訂相互瞭解備忘錄 MOUs。

（三）AGIS（2003~2006）、ISEC（2008~2009）

- 從事許多歐盟計畫發展 LE 訓練：
  - ✓ 提供內容專家及訓練企劃師。
  - ✓ 協助確保計畫之持續及品質。
  - ✓ 提供學術性認證。
- 使資料得以經由歐洲警察局（The European Police Office, Europol）到達所有設於歐洲之 LE 機構。
  - ✓ 藉由 Interpol 而為全球性，並為歐洲網際網路犯罪調查訓練協調小組之正式會員。

（四）其他工作：

- 與歐洲反詐欺局（The European Anti-Fraud office, OLAF）及歐洲社會及合作組織（The Organization for Security and Co-operation in Europe, OSCE）合作以完成大規模訓練計畫。
- 與 Interpol 合作進行「培訓及培訓員」課程。

（五）2 CENTRE 計畫：

2CENTRE（Cybercrime Centres of Excellence Network for Training, Research and Education）為一訓練及教育計畫，並整合歐盟及相關國家之執法機關、學術界及產業界力量，共同合作，以處理全球網際網路犯罪問題。

◆ 結論：

- 網際網路犯罪向全球引進新挑戰，故須新型態之全球合作。
- 我輩身處此國際社會，各國皆須有合作及互助之想法。
- 建議以下至上之模式進行合作，同時由上提供支援（如政府機關、歐盟、聯合國、產業等）。
- 無國家或產業可獨立完成任務。

議題二：美國 FTC 國際案例介紹

本節由美國聯邦貿易委員會
（U.S. Federal Trade Commission, FTC）
律師兼垃圾郵件協調員 Ethan Arenson
報告「2009 年高科技執行行動」。
其稱 2009 年為所謂「抓大魚」之年，
並說明 FTC 近年所處理最重要的案例。

圖片來源：Ethan Arenson 簡報

一、FTC v. Innovative 行銷公司等（Winfixer 軟體）：

Innovative 行銷公司生產之產品 Winfixer 為透過網際網路廣告安裝於用戶電腦的間諜軟體，此案係屬惡意安全軟體（惡意電腦程式 Scareware）之詐欺案件，其涵蓋之範圍遍佈全球，造成消費者損失之金額，達美金一億元之多，其亦為 FTC 所起訴最大宗網際網路詐騙案件之一。

該軟體之詐騙方式係經由對話框，提醒電腦使用者注意其電腦如有較平常運轉慢之情形，即為可能受到病毒侵害，並提供反制病毒軟體供使用者免費下載。

（一）惡意電腦程式早期發展情形：

FTC v. Seismic 娛樂製作公司等一案，於 2004 年 10 月 6 日提訴，該案使用較原始之手法，消費者於力勸下，常被誘騙購買惡意電腦程式（Spy Wiper, Spy Deleter）作為反制病毒之用。FTC v. Max Theater 及 FTC v. Trustsoft 二案，分別於 2005 年 3 月及 6 月提訴，開啟所謂虛偽掃描時代，其手法係以彈出式廣告告知消費者其電腦可能被間諜程式感染並提供消費者免費下載掃瞄軟體檢查其電腦，一旦安裝後，該軟體會告知察測出有間諜程式，並提供消費者優惠價格，誘使其立即以信用卡付款購買上述之軟體（間諜刺客 Spyware Assassin; SpyKiller）。

（二）惡意反間諜程式之今昔：

早期惡意反間諜程式賣家之手法係以美國為基地，由一人負責小規模操作，一次僅行銷一項產品予美國之消費者，且消費者係受彈出式廣告引誘。至 Winfixer 出現，惡意反間諜程式進入新時期，此案使用複雜之虛偽掃描誘騙消費者。

FTC v. Innovative 行銷公司等案於 2008 年 12 月提訴，

其行銷策略係以分地方式，深入不同市場使用不同之語言進入當地市場競爭，被告之根據地可向外追蹤至美國以外地區，如總公司設立於烏克蘭之基輔，並於全球各地遍布分據地，如德國、法國、義大利、韓國、日本、中國大陸、西班牙、葡萄牙、阿拉伯、荷蘭、瑞典、挪威、芬蘭、丹麥、俄羅斯、波蘭、土耳其及泰國。僱用數百員工以專業化經營，銷售千種以上之產品至全球消費者，造成消費者之損失達到億元以上。

隨後 Winfixer 進化為惡意廣告（Malvertising），其係一含有自動下載惡意軟體或有害內容至電腦之設計，影響更為鉅大。為使消費者瞭解此些非法軟體並達成防堵之目標，FTC 於 2008 年展開消費者警示措施，積極宣導「免費及安全之掃瞄須花費時間與金錢」之概念，並於大眾媒體（如巴爾的摩太陽報，the Baltimore Sun）及網路上，配合推廣。

二、FTC v. Pricewert LLC (三光纖網絡案 Triple Fiber Network, 3FN)

本案為 FTC 2009 年執行高科技犯罪訴訟案件之代表，被告係一網際網路服務提供者（ISP），其於美國設置數百架伺服器，以募集、主動參與、網站託管、不公平散佈及侵入電腦等方式，非法散佈兒童色情、線上藥房、殭屍電腦網絡、盜版音樂、軟體、垃圾郵件工具及惡意反間諜程式等惡意及有害之電子內容。

本案之相關證據源自美國國家航空暨太空總署航天局監察長辦公室（NASA Office of Inspector General）、阿拉巴馬大學、國家失踪及被剝削孩童中心（National Center for Missing and Exploited Children, NCMEC）、反垃圾郵件組織 The SpamHaus（The SpamHaus Project, Ltd）、Shadowsever 基金會（The Shadowsever Foundation）、賽門鐵克（Symantec）及 FTC 內務調查員（In-House Investigator）等。相關內容簡要說明如下：

- 「發現」3FN
  - ✓ NASA 出現電腦侵入案件，經特別探員 Sean Zadig 調查追縱至 McColo 及 3FN 之資料庫所在，並發現 3FN 員工與客戶間一連串 ICQ 聊天紀錄，顯示 Pricewert 涉嫌直接參與創置殭屍網絡，此些紀錄成為全案最關鍵之證據。
  - ✓ 阿拉巴馬大學電腦取證研究學系主任 Gary Warner

指出 3FN 為美國最糟糕的 ISP，並提供 3FN 託管之惡意內容證據。他又發現 crutop.nu 為一垃圾郵件發信人論壇，並提出 3FN 寄送廣告信予罪犯之證據。

- ✓ 經分析 NCMEC CyberTipline 之報告，由 3FN 控制之 IP 位址，發現 700 件兒童色情案件，確定成立者超過 500 件。
- ✓ SpamHaus 與 3FN 直接取得聯繫，證明其與客戶合作並提供保護，同時發現 3FN 由國外控制之證據，並涉及巨型殭屍電腦網絡。
- ✓ Shadowsever 基金會蒐集 3FN 託管之惡意內容，發現 311 個 IP 位址涉入或幫助惡意活動，4576 件間諜程式/病毒樣本使用 3FN 之伺服器支援殭屍電腦網絡，惡意活動遍及之幅員廣闊。
- ✓ 程式/病毒樣本使用 3FN 之伺服器支援殭屍電腦網絡，惡意活動遍及之幅員廣闊。
- ✓ 賽門鐵克（Symantec）分析 3FN 重大網路攻擊案件及其類型，如殭屍電腦網絡、垃圾郵件、釣魚網站等攻擊活動。
- ✓ FTC 內務調查員提出之證據包括：由 3FN 網域發現聯繫至 Pricewert 之化名、美國境外控制證據、ICQ 對話紀錄譯文、線上申訴案之查證及 3FN 託管網站/病毒之揭發。

三、衝擊之評估：

（一）好消息：

- ➢ 關閉 3FN 之衝擊何在？
  - ✓ 難以精確衡量。
  - ✓ 案件重大但暫可減低垃圾郵件泛濫程度。
  - ✓ 對殭屍電腦網絡之衝擊重大。

（二）壞消息：

- ➢ 犯罪行為是學習及演化而來的。
  - ✓ 不再需要中央控制之伺服器。
  - ✓ 縱有執法，殭屍電腦網絡及垃圾郵件仍持續成長。
  - ✓ 關閉 ISP 證明僅為暫時性之方案。

議題三：殭屍電腦網絡之追蹤

本節由葡萄牙電腦緊急反應團隊 CERT-IPN（Computer Emergency Response Team - Unidade do Laboratório de Informática e Sistemas do Instituto Pedro Nunes - Coimbra, PORTUGAL）代表 Francisco Rente 簡介殭屍電腦網絡之概念、歷史演進、重要案例及防禦措施。

CERT-IPN亦稱葡萄牙電腦安全事件反應團隊（Computer Security Incident Response Team, CSIRT），其任務在維護該國之資訊安全，主要之業務包括宣傳服務、顧問諮詢服務及商業繼續性支援服務，相關服務項目包括滲透測試、系統及網絡安全評估、資訊安全方案之諮詢及設計、取證分析及資訊回覆、研討會及培訓課程、安全事件回應、資訊安全意識及宣傳及與葡萄牙電腦安全相關計畫合作等。

一、殭屍電腦網絡之概念及演進：

（一）殭屍電腦網絡係指由遠端攻擊者控制被感染的機器並執行攻擊之網絡，亦即駭客利用其編寫之分散式阻斷服務攻擊程序控制數萬個淪陷的機器，並可隨時按照其指令展開拒絕服務攻擊或發送垃圾信息。最普遍之攻擊方式除分散式阻斷服務外，尚有垃圾郵件、釣魚網站及大型識別資料之竊取等。殭屍電腦網絡之特性包括：(1)可修改及擴充之惡意軟體；(2)概念分層組織；（3）冗長強大之網絡；(4）大規模毀滅性武器；(5）組織犯罪最新產品；(6）政府最新武器等。

（二）歷史演進：

- 1980年代晚期：病毒概念出現（Morris 病毒, Robert Tappan Morris）。
- 1993年：通過「網際網路中繼聊天協定」IRC （Internet Relay Chat）Procotol。
- 1990年代早期至中期，間諜軟體開始增加網際網路中繼聊天功能。
- 1990年代晚期：開始利用遠端開發癱瘓公私網絡。
- 21世紀初：加密、模糊化、多形態、包裝能力、組合式設計、反攻擊、主動防衛、點對點網絡 P2P（peer-to-peer computing）、非集中式網絡、所有形式之惡意電腦程式能力（如駭客軟體、木馬程式、廣告軟體）、超強武器、

隱藏能力。

- 2007年：暴風病毒。
- 2008年：變種蠕蟲病毒（Conficker）。
- 決定之能力端視：使用者行為、機器及網絡規範。

二、重要案例：

（一）國際案件

- 愛沙尼亞（Estonia）
  - ✓ 2007 年 4 月間，愛沙尼亞出現數個以分散式阻斷服務攻擊（Distributed Denial of Service , DDoS, DoS）、垃圾郵件及網頁置換方式攻擊愛沙尼亞主要政府機關、軍事單位及銀行機構之事件。
- 聖戰殭屍網絡（Jihad Botnet）
  - ✓ 2007 年後期，於社區出現流言大肆宣傳聖戰組織將以間諜程式建置殭屍電腦網絡。
- 喬治亞（Georgia）
  - ✓ 2007 年後期，於社區出現流言大肆宣傳聖戰組織將以間諜程式建置殭屍電腦網絡。
- 鬼網（Ghostnet）
  - ✓ 2009 年 3 月，經發現大規模網路間諜活動滲透 103 個國家具高價值之政治、經濟及媒體單位（包括葡萄牙），此軟體據推測源自中國，並由一建置於開放來源之概念惡意軟體---「啞」間諜軟體支援。

（二）國內案件

- 宙斯殭屍網絡（ZEUS Botnet, ZBot）
  - ✓ 千禧銀行（Millennium BCP）列於網路釣魚目標前 10 名。
- CERT-IPN 蒐集之資料:Nonius 計畫、誘捕網路(Honeynet)

三、防禦措施：

方 式	類 型	目 標
C&C (Command & Control)	主動防禦	失能/摧毀殭屍網絡控制中心
更新系統	主動防禦	失能/摧毀殭屍網絡更新/同步系統能力
傳播管道	防禦	分析並定義過濾器瞭解表面管道技術

誘捕網絡	研究	瞭解並勘測殭屍網絡之來源、行為及組織
暗網	研究	瞭解並勘測殭屍網絡之來源、行為及組織

四、結論：

- 殭屍網絡並非新型之威脅。
- 現今之殭屍網絡係使用尖端科技。
- 殭屍網絡開始被當成戰爭武器、生財工具及大規模組織犯罪支援系統。
- 以 IRC 為基礎之殭屍網絡仍為最常使用者。
- 兩種防禦類型：主動及被動。
- 對於殭屍電腦網絡之瞭解及研究極其重要，防禦系統以之為賴。

議題四、以網際網路消費者防禦觀點進行之調查方法

本節由葡萄牙消費者政策及保護主管機關DGC（Direcção-Geral do Consumidor / Consumer Directorate-General）代表José Manuel Faísca介紹消費者保護合作網絡（Consumer Protection Cooperation Networks , CPC Networks）：

一、宗旨：

跨國詐欺活動行為日漸增多，使各國主管機關難以對其他國家之商家祭出刑責，故須國際間之行政合作。歐盟「消費者保護合作規則」（The Regulation on Consumer Protection Cooperation, Regulation (EC) No 2006/2004），要求各國主管機關共同合作執行消費者保護法規。

二、範圍：

侵害歐盟消費者保護法規之跨國案件：

- ✓ 侵害歐盟消費者保護法規及保護消費者權益轉換為國內法之歐盟指令（約 20 項，明定於法規附錄）。
- ✓ 廣義之跨國案件。
- ✓ 涉及消費者集體利益。

三、相關規定：

- ✓ 第 6 條：依要求之資訊交換。

- ✓ 第 7 條：毋需要求之資訊交換。
- ✓ 第 8 條：要求執行方案。
- ✓ 第 9 條：市場監督及執行行動之合作（網際網路消費者保護）。

四、Sweeps 提供調查之方法及數據：

（一）掃蕩日（Sweep Days）

- ✓ 歐盟掃蕩為一整合之歐盟調查及執行行動，以符消費者保護法規定，其針對一特定團體合力查明，俾以找出消費者何項權益受阻或有否損失。
- ✓ 發現案例後，各國執行機關持續追蹤，聯繫涉嫌非法之公司，並要求該等公司應符合相關規定。
- ✓ 對於牴觸歐盟法規者，祭出司法行動。
- ✓ 此方案由各國參與，設定時程、方法、報告及公開程序，並為一規律性之調查活動。

（二）掃蕩之執行

- ➢ 分二層面進行：
  - ✓ 合作性掃蕩行動
    - ● 國家執法機關系統性及同時查證牴觸歐盟法規之特定市場，所有機關使用共同的查證表，以找出不正常者。
    - ● 以下之行為違反全歐盟法規：

      1、不提供買家完整之聯繫細節。

      2、不明確告知線上買家有關撤銷交易之權利。
  - ✓ 執法行動
    - ● 主管機關進一步調查涉嫌違法之商人，並採取後續行動，以確保當事人改正其行為，並課以適當之處分。
    - ● 各國主管機關調查並執行各該國境內之案件，有關跨國之案件，執法機關可向其他國家之主管機關尋求協助。
    - ● 當事人有權回覆並更正非法行動，未能完成改正者，將面臨司法行動，並課以罰金及其他制裁，其網站甚且會被關閉。

（三）掃蕩日之問題

- ✓ 案件或對象之選擇。
- ✓ 不同國家市場之問題或申訴。
- ✓ 歐盟法規未完全協調：不同國家採取之方案不同。
- ✓ 公開報告。
- ✓ 法律行動。
- ✓ 重覆調查（持續掃蕩）。
- ✓ 調查之規律性。

（四）如何改進行動？

- ✓ 於歐盟層面，DGC 從事三項網際網路掃蕩，分別發生於 2007 年、2008 年及 2009 年(機票、手機鈴、電子商品)。
- ✓ 於國家層面，DGC 以其廣告觀測站，針對受法令規範之廣告電子商務及不公平商業交易，進行規律性之網路掃蕩。
- ✓ DGC 同時參與國際性掃蕩行動，此部分多由 RICC/ICPEN 主導。

五、「網路計畫」之調查

（一）於 2008 年早期由包括葡萄牙在內之 5 個歐盟會員國發起，迄今已有 14 個會員國。

（二）目標

- ✓ 創造特殊之調查網絡。
- ✓ 訓練具技巧之調查人員。
- ✓ 於 CPCS 網站提供互動式網頁予電子商務消費者。
- ✓ 提供特殊之資訊及訓練課程。
- ✓ 研訂科技手冊及程序，以供調查之需。
- ✓ 將調查導入更深入之領域，而非僅限於合法及公開之範圍。

（三）進展成效

- ✓ 常態性掃蕩行動呈現更佳的合作及規劃效果。
- ✓ 新手法及新時程之研發。
- ✓ 運用新智慧科技工具。
- ✓ 舉辦研討會及研究人員機動化。
- ✓ 提昇更多主動調查（如於網站設置虛擬帳戶、使用電子卡片鼓勵交易）

- ✓ 研究人員手冊之內容：
  - 各國之導引資料庫網域辦公室及特殊單位資料庫包括導引其他共同研究工具之聯結。
  - 跟綜網站。
  - 確認個人、網域及個人網址。
  - 電子郵件研究、來源確認、垃圾郵件。
  - 依據電子商務法令所訂之其他程序。
  - 為線上交易消費者提供之線上資訊及訓練：

    1、於 CPCS 網站提供互動式網頁 PORTAL。

    2、為消費者發展之互動工具。

    3、智力競賽節目、影帶、連環漫畫。

    4、小折頁、小冊（如「歐洲線上買賣須知曉之權利」）。

    5、線上交易影片（所謂之「病毒」行銷）。

    6、全國各地網站聯結。

六、FraudenaNet 計畫：

- ➢ 更安全之網絡＝有自信之消費者。
- ➢ 模式：一週行動研討會（2008 年 4 月開始）。
- ➢ 格言：確認、報告並終止網路詐欺。
- ➢ 以實例編撰簡易宣導手冊。
- ➢ 每天於網站批露一個真實案例。

二、2009/10/8 議程

議題一、垃圾郵件之趨勢及統計

本節由美國反訊息濫用工作小組(The Messaging Anti-Abuse Working Group, MAAWG) 董事會公共政策主席 Luc Mathan 主講 MAAWG 全球垃圾郵件量度。

一、MAAWG 量度計劃

- 季報告係作為認識產業界阻擋濫用電郵成果之指南，以及確認經過一段時間後之相關趨勢。
- 第一份報告涵蓋 2005 年第四季。MAAWG 僅於超過一億個信箱被檢舉之情形方予報告。
- 以信箱經營者之觀點，提供客觀面向說明預防電郵遭受濫用之方法。
- 計量法被視為評估政策、立法及技術解決方法有效性，以及決定策略及未來改變的有效性之關鍵。

二、基本規則

- 自願參加。參加者必須是 MAAWG 會員，且為負責經營終端使用者電郵信箱。
- 保證每季回報計量達二年，儘管一間公司當有回報困難時可能退出。
- 公司可隨時加入，為達一致性，需提供至少二季回報。
- 所有回報皆屬機密。由執行長(Executive Director)接收並合計數據。
- 公布於 MAAWG 網站。

三、哪些數據將被收集？

- 具代表性信箱之數量。
- 未被改變傳送郵件之數量。
- 遺漏連結及被封鎖或被標記入站郵件之數量。

**目前 MAAWG 只公佈數據百分比或比例，由於原始數據經常修正，故不顯示原始統計數據。

四、量度報告

MAAWG 量度報告未顯示垃圾郵件，但指出被認定為”濫用”之電郵數量。

Key Historical Ratios	Report #11 Q2 2009	Report #10 Q1 2009	Report #10 Q4 2008	Report #9 Q3 2008	Report #8 Q2 2008
Dropped Connections & Blocked/Tagged Inbound Emails per Unaltered Delivered Email	8.11 or 89.0% abusive email	9.43 or 90.4% abusive email	12.12 or 94.2% abusive email	10.65 or 92.4% abusive email	11.49 or 92.0% abusive email

圖片來源：Luc Mathan 簡報

議題二、垃圾郵件計量及葡萄牙垃郵案例介紹

本節由葡萄牙 AnubisNetworks 公司 Francisco Fonseca 主講，該公司於 2006 年成立於葡萄牙里斯本，主要研發電郵安全機制。

一、垃圾郵件計量

・2009 年 1~9 月垃圾郵件百分比：

平均 96%上下，3 月明顯下降至 92%，8 月則增至 97%。

・2009 年 9 月每日垃圾郵件百分比：

平均垃圾郵件量 96.42%。

・2009 年 1~9 月美國、巴西、中國、俄羅斯、土耳其、印度及南韓等七個國家每月垃圾郵件量百分比：

9 月份排名依序為美、巴、中、印、韓及俄。

・2009 年 9 月各國寄送至葡萄牙之垃圾郵件：

唯一未寄送垃郵之國家為梵蒂岡；葡萄牙 75%的垃郵來自前 18 大濫發國。

二、統一資源識別碼 (Uniform Resource Identifier, URI)

・統一資源識別碼係由一串字元組成，用以辨識或命名網路資源。例如：.org、.pt、.com 等等。

・自頂層網域 (TLD) 之垃圾郵件，「.cn」占 64.1%，「.com」占 16.7%，「.org」占 12.7%。

・來自各個頂層網域垃圾郵件排名：

93.5%來自前 3 大頂層網域，99%來自前 9 大頂層網域。

三、葡萄牙語垃郵案例

・葡萄牙語垃圾郵件係指以歐洲葡語或巴西葡語所寫成之垃圾郵件，或是與葡萄牙公司有關之垃圾郵件。

・歐洲葡語垃圾郵件案例：

- ✓ 分為非詐欺型及詐欺型(鎖定葡萄牙公司)。
- ✓ 詐欺型垃郵通常為小公司藉以兜售產品或服務，來自殭屍電腦的歐洲葡語垃郵並不常見，絕大多數為非詐欺型。
- ✓ 詐欺型電子郵件主要使用巴西葡語或粗劣語言(自動翻譯)寄送，極少英語垃圾郵件攻擊葡萄牙公司。

議題三、新興的威脅

本節由荷蘭獨立郵政及通訊監理機關(Onafhankelijke Post en Telecommunicatie Autoriteit , Dutch Independent Post and Telecommunications Authority, OPTA）消費者事務處副處長 Danyel Molenaar 主講垃圾郵件之新型態－社交網絡垃圾郵件。

一、OPTA 簡介

・係獨立郵政電信署。

・於 1997 年依據行政法設立。

・依歐盟指令執行荷蘭電信法。

・2004 年開始執行取締垃圾郵件及惡意軟體。

・獨立調查機關。

・科以罰金(每一案件最高可處罰€450,000)，無監禁刑，違法者無案底紀錄但罰金判決公開。・

二、概分 4 種類型之垃圾郵件

・走起路來像隻鴨子 (If it walks like a duck)

- ✓ 傳統的垃圾郵件係透過殭屍網路，而具攻擊目標 之垃圾郵件係透過其他傳播媒介，諸如藍牙、簡訊服務或社交網絡。

・游起水來像隻鴨子 (…swims like a duck)

- ✓ 使用多個外國電腦。
- ✓ 於荷蘭排名第一的社交網站以字母創造 26,000 個偽 造帳戶，鎖住該帳戶並予登入。
- ✓ 隨機選取社交網絡會員並寄送 3,100,000 垃圾圖文，以促銷 RPS 遊戲。
- ✓ 上述事項於 9 天內完成。

・呱呱叫聲像隻鴨子 (…and quacks like a duck)

根據荷蘭法律，垃圾郵件係指下列電郵：(1)透過公開通訊網絡寄送之電子訊息、(2)含商業、慈善及觀念論內容、(3)寄送給公共電信服務訂戶（非自然人或法人）及(4)未經同意、未含寄件人身分或無有效退訂機制。

・他看起來似乎是隻鴨子 (...it just might be a duck)

- ✓ 它並非電子郵件：垃圾內容非寄至或儲存於電郵信箱，其意在混淆守法民眾。
- ✓ 垃圾內容為公開的：但僅於一個人登入社群網站後，垃圾內容本身方成為公開。
- ✓ 用戶非自然人或法人：此係調查工作極困難所在，1300個申訴案僅 3 個對 OPTA 有用。
- ✓ 此乃荷蘭新型態之垃圾郵件，顯而易見，OPTA 將此視為垃圾郵件，最大之挑戰則是找出有效之申訴。

議題四、電子郵件行銷與垃圾郵件

本節由網站代管公司 Eurotux S.A 之 Ricardo Oliveira 主講。

一、垃圾郵件

根據線上數據統計，94%的電子郵件為垃圾郵件，唯一能作的就是防堵，或是停止點閱郵件。超過半數的垃圾郵件發送源在中國註冊區域網名，並從位在中國的電腦發送，或以在中國的電腦為主機。

二、網站代管公司的角度

- ✓ 從網站代管公司(hosting company)的角度出發，電子郵件行銷代管(email marketing hosting) 對網站代管公司發生一些影響，如：

(一)增加頻寬的需求。

(二)伺服器與儲存的要求。

(三)額外服務的可能性。

(四)服務可為顧客帶來立即的收益。

- ✓ 垃圾郵件的防制亦對網站代管公司產生一些影響，如：

(一)龐大的頻寬需求。

(二)分散式伺服器的需求。

(三)回饋顧客。

(四)額外的服務變成強制性；處理客訴；從其他 ISP 業者感染電腦病毒 blackholes，及濫發郵件的黑名單等問題。

(五)處理名譽問題、

(六)對顧客的網路連線無法控制。

✓ 過濾垃圾郵件的軟體（雲端技術）是另一個令網站代管公司愉快的服務：

(一)給予顧客立即的滿足及擴大顧客群。

(二)保護顧客免受垃圾郵件騷擾為主要關切項目。

(三)處理垃圾郵件攻擊及顧客抱怨案件 2。

(四)管理極難，故須發展/更新探索之規則、靜態封鎖垃圾郵件來源並除去閒置之資源。

三、結論

Eurotux S.A 公司比喻此為同一枚硬幣的三個面向，即從電子郵件行銷、垃圾郵件防制、及過濾垃圾郵件軟體三個面向來看。該公司認為，不可能同時促進電子行銷商務，又保護用戶不受垃圾郵件的干擾，或者至少是說，同時採取促進電子商務及保護電子郵件服務安全的措施是沒有效率的。相關建議如下：

(一)將傳統、類垃圾郵件之解決方法提升至現代、選擇進入（opt-in）與選擇退出（opt-out）之技術。

(二)注意可疑之行為（關於網路安全）。

(三)將電子行銷資源予以分類，並創造顧客規則，以影響過濾層之訊息分析程序。

(四)創造本地垃圾郵件捕捉器及誘補系統。

(五)增進服務以幫助顧客免於典型垃圾郵件之攻擊，如形成濫發、錯誤電子郵件伺服器的配置及郵件位址蒐集等。

(六)調查國外申訴案件。

(七)公布濫發郵件者。

(八)確保違反「允許使用政策」(Acceptable Use Policy, AUP)將導致違約。

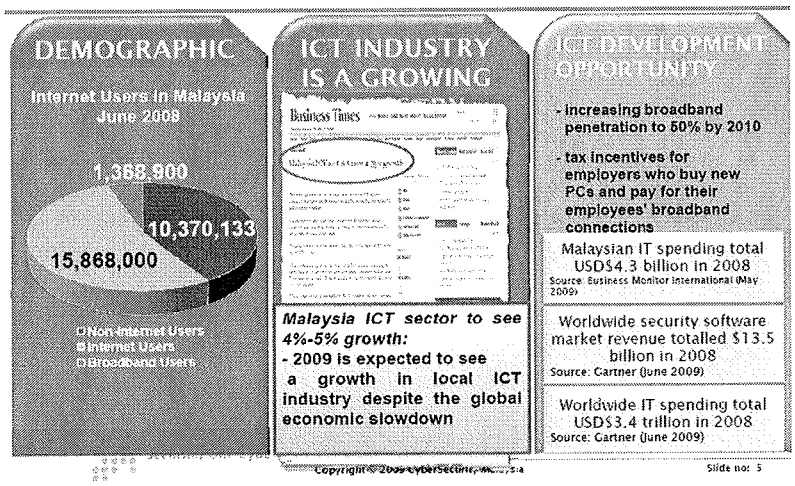
議題五、馬來西亞防制垃圾郵件之立法

本節由馬來西亞網路安全中心CyberSecurity Malaysia 業務部主管 Zahri Hj Yunos 主講該國防制垃圾郵件立法概況，該機構為政府設立，隸屬馬來西亞科學技術創新部（the Ministry of Science, Technology and Innovation, Malaysia, MOSTI）之國家級單位。

一、垃圾郵件（spam）之定義：

2006 年馬來西亞通訊與多媒體委員會定義垃圾郵件為「未經邀請寄送之電子訊息」，包括電子郵件、手機簡訊及即時訊息服務，發信人及收信人間事先並未有合意，而寄送之商業或非商業訊息（含惡意程式）。

二、馬來西亞使用網路人口統計及網路產業成長表如下：



圖片來源：Zahri Hj Yunos 簡報

經馬來西亞官方統計，2008 年 6 月馬來西亞使用網路之人口，大約為 60%；其通訊產業經外國雜誌預測在 2009 年仍有 4%-5% 的成長，政府預計於 2010 年之前將寬頻普及率達到 50%，並藉由稅率訂定鼓勵雇主購買個人電腦及支付寬頻費用。

三、垃圾郵件相關現況：

（一）馬來西亞於電子郵件位址蒐集活動中，排名世界前 40 名。

（二）尚未有防制垃圾郵件之法律---正由政府審議中。

（三）馬來西亞採取反垃圾郵件之措施包括：

1.用戶的自我防護（透過教育加強認知及技術解決）、對網路服務提供者的管理及國際合作。

2.網路安全防護公司 Borderware 連接濫發電子郵件的黑名單，並提供對抗電腦病毒、垃圾郵件及惡意軟體的防護。

（四）通訊與多媒體法案（Communication and Multimedia Act 1998）

馬來西亞 1998 通訊與多媒體法案第 233 條第 1 項適用於防制垃圾郵件。第 233 條規定不適當之網路設備使用或網路服務係指行為人以網路設備、網絡及應用服務等手段製作、創造、引誘或傳送任何含猥褻性、引人錯誤、恐嚇性或冒犯性之內容，意圖令人不快、毀謗、恐嚇、威脅及騷擾。

（五）違反之法律效果

行為人違反上述規定，經法院確定罪行後，應處以 50.000RM （相當新臺幣 50 萬元）罰金，或處以一年以下有期徒刑或兩者併罰。且在罪行確定後，行為人應就後續違法內容對其他人造成的損害時，每日處罰金 1.000RM（相當新臺幣 1 萬元）。

四、規範垃圾郵件所面臨之挑戰：

（一）過濾軟體難以偵測以俄羅斯語及馬來語編寫之垃圾郵件。

（二）類似 CAPTCHA[1]之破解工具亦被淪陷，使資訊安全之執行變得愈來愈複雜。

（三）殭屍網路的形成源於夾帶病毒的垃圾郵件，由於垃郵件數日益增加，使殭屍網路之改善，面臨難題。

（四）缺乏規範垃圾郵件的專法，且國際間反垃圾郵件法規不同，使垃圾郵件之防制益形困難。

（五）對有些用戶而言，某些垃圾郵件可促進合法經濟活動，故可被接受。

五、結論

（一）垃圾郵件乃一日漸嚴重的問題，並且造成困擾--- 此意味防

---

[1] CAPTCHA 之全名為 Completely Automated Public Test to tell Computers and Humans Apart，CAPTCHA 目前廣泛用於網站的留言板，許多留言板為防止有人利用電腦程式大量在留言板上張貼廣告或其他垃圾訊息，因此會放置 CAPTCHA 要求留言者必須輸入圖片上所顯示的文數字或是算術題才可完成留言。而一些網路上的交易系統（如訂票系統、網路銀行）為避免被電腦程式以暴力法大量嘗試交易也會有 CAPTCHA 的機制。請參閱 http://zh.wikipedia.org/zh-tw/CAPTCHA。

制垃圾郵件需要全球的合作。

（二）於處理垃圾郵件的問題上，教育、認知、遵從規範、執法及運用適當的技術為最重要的環節。

（三）須有最有效的執行程序與技術指導以防制垃圾郵件，並儘量最小化垃圾郵件量。

（四）防制垃圾郵件的規範需進行國際間協調。

議題六、奧地利有關反制垃圾郵件之報告

本節由奧地利運輸創新技術部（Austrian Federal Ministry for Transport, Innovation and Technology, BMVIT）電信辦公室 Nikolaus Koller 主講奧地利反制垃圾郵件現況。

一、法源基礎：

(一)歐盟有關隱私與電子通訊指令（Directive 2002/58/EC）

2002 年歐盟發布之隱私與電子通訊指令第 13 條明文規範主動提供之通訊：

1.必須事先取得用戶同意，始得利用自動發話系統、傳真或電子郵件傳送以直銷為目的之訊息。至於因出售產品或服務而取得顧客電子郵件地址者則被例外許可得利用該電子郵件進行其他類似產品或服務之直銷。

2.該制度不僅適用於自然人，各會員國得決定是否適用於法人。

3.禁止以虛偽或匿名之身份或未提供有效回覆地址方式發送以直銷為目的之電子訊息。

4.禁止以未提供有效回覆地址方式發送，即所有電子郵件須附上選擇退出的電子郵件回覆。

(二)奧地利電信法第 107 條（Austrian Telecommunications Act 2003, TKG）規範主動提供之通訊如下：

（1）禁止未經用戶事先同意，以行銷為目的之發話行為（包括傳真）。所謂用戶的同意係指經授意使用其電信線路。用戶可隨時撤回其同意，如用戶撤回同意並不影響契約關係。

（2）禁止於下列情形寄送未經收信人事前同意之電子訊息（包括手機簡訊）：

1.以行銷為目的之寄送。

2.收信人超過 50 位。

（3）於下列情形，發送電子郵件無須取得收信人之事先同意：

1.發信人已取得為締結買賣契約之聯絡細節。

2.因出售產品或服務而取得顧客電子郵件地址者，則可利用該電子郵件進行其他類似產品或服務之直銷。

3.於個人資訊被收集同時，發信人已提供收信人免費回傳機制以拒絕接收訊息，而其並未拒絕。

4.收信人已納入電子商務名單，即發信人第一次發送時未經拒絕接收。

（4）已廢除。

（5）禁止寄送以行銷為目的、信首資訊經偽造、隱匿或無清楚回傳機制之電子訊息。

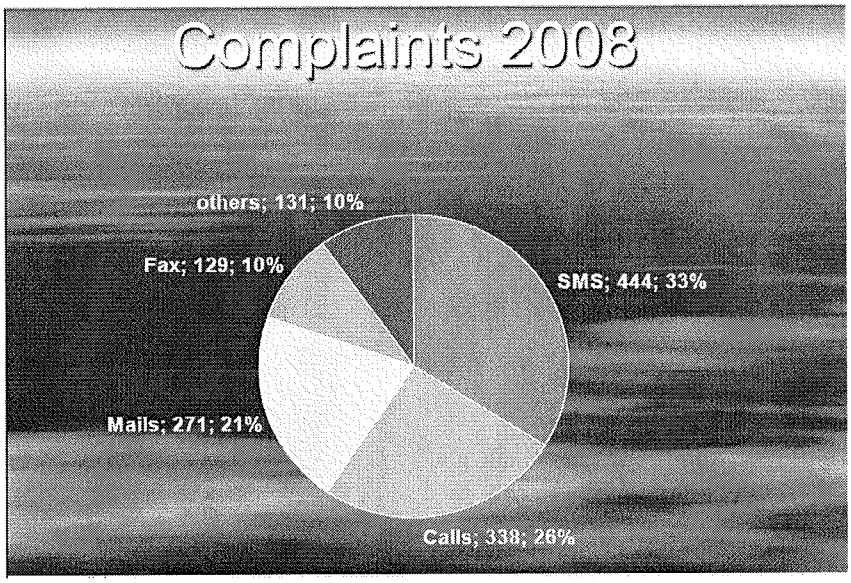
（6）如違反第 1 項、第 2 項、第 5 項之行為地不在奧地利者，應推定發信人已侵犯用戶之權利。

✓ 第 6 項係本於電子訊息發送常為跨國性，行為地不在奧地利時，應推定發信人依當地法規已侵犯用戶權利。實務上，奧地利對外國犯罪嫌疑人，從未採取法律行動，除非犯罪嫌疑人在德國，因奧地利與德國訂有雙邊協定，奧地利可對其進行法律程序。

二、管制垃圾郵件之主管機關：

奧地利設有隸屬於 BMVIT 之 4 個電信辦公室（Telecommunications Offices, TO），90%的員工皆負責無線電頻率之規劃，其中僅 4 名負責垃圾郵件之防制工作。該機構僅負責前述電信法第 107 條規定之執行，違反該條規定則處以行政罰，雖無監禁刑，但罰金可高達 37.000 歐元，且被告可上訴獨立行政法庭；又垃圾郵件如涉及詐欺或其他犯罪行為，則由警察局、公訴體系及法院共同管理。

三、接獲申訴之類型：



圖片來源：Nikolaus Koller 簡報

依奧地利官方統計，2008 年民眾申訴未經邀請之通訊情形，最大宗者為簡訊 33%，其次為電話 26%、電子郵件 21%、傳真 10%，其他類別 10%。

四、民眾申訴之處理

- ✓ TOs 負責所有違反 TKG 有關垃圾郵件之申訴案件。
  - 維也納權責中之申訴案件 90%係違反電信法第 107 條規定。
  - 大部分係申訴奧地利之" small fry "。
  - 迄今主要案件所涉垃圾郵件皆非源自奧地利。
- ✓ TOs 於處理民眾申訴案件時。面臨數項困難：
  - 對 TOs 有用的僅有主檔資料，號碼及 IP 位址皆須進一步之調查。
  - IP 位址之變動性造成極大之問題。
  - 依規定，案件應於接收電子郵件 6 個月內提起，惟因郵件常於接收後被刪除，導致不易保存證據以進行調查。
  - 人力缺乏。
- ✓ 與其他反制垃圾郵件主管機關合作：
  - 2008 年出現各種申訴濫發傳真（fax spam）案件，由於無法查知傳真來源，曾與荷蘭 OPTA 及英國 ICO（GB）合作。

五、期許未來：合作、合作、再合作！

議題七、歐盟線上隱私權及資料保護議題

本節由歐盟資訊社會及媒介總理事會政策發展及法規處代表 Merijn Schik 主講。

一、源起：

（一）2006 年，歐盟會員國召開垃圾郵件、偵測軟體及惡意軟體因應會議，會議決議如下：應加強利害關係人之認知、網路服務業者應採取”最有效措施”（BP）、主管機關須落實執行及國際合作。

（二）該會議內容包括界定執行成功之因素、中央政府之承諾、清楚的責任架構及適度的政府手段。相關細節包括：加快執行、應有明確的主管機關及確保有效的合作、有效利用網路服務業者之知識與技術、政府資源應有效利用、國際合作程序付諸實行及企業責任（如過濾技術、建立資訊標準等）。2006 年至 2008 年，各會員國根據該會議結論採取對抗垃圾郵件、偵測軟體及惡意軟體的措施。

二、2008 年歐盟研究報告：

2008 年針對 2006 年會議檢視會員國對垃圾郵件、偵測軟體及惡意軟體採取的措施。主要研究結果如下：

（一）歐盟已執行垃圾郵件及惡意軟體之立法。

（二）各會員國皆有介紹垃圾郵件及惡意軟體的相關網站及申訴管道。

（三）業者已執行並提供技術措施以防制垃圾郵件及惡意軟體。

（四）已有數個政府及企業間合作之範例，惟調查結果認為仍有下列問題存在：

- 政府間之合作及政府與企業間之合作層級應予提高。
- 有效的國際制裁並不總是被貫徹且獲起訴之案件量變化極大。
- 國際層級之合作計劃似不足夠。
- 政府應投入更多之資源（如預算、人力）。

（五）調查中發現，歐盟會員國調查之案件數超過 140 件，然而有些國家只處理少數的申訴案。荷蘭訂有最高罰金規定（1000.000 歐元）；義大利為 570.000 歐元；西班牙則為 30.000 歐元。然而在其他國家，某些濫發郵件者僅受到幾百歐元至幾千歐元不等的罰金。

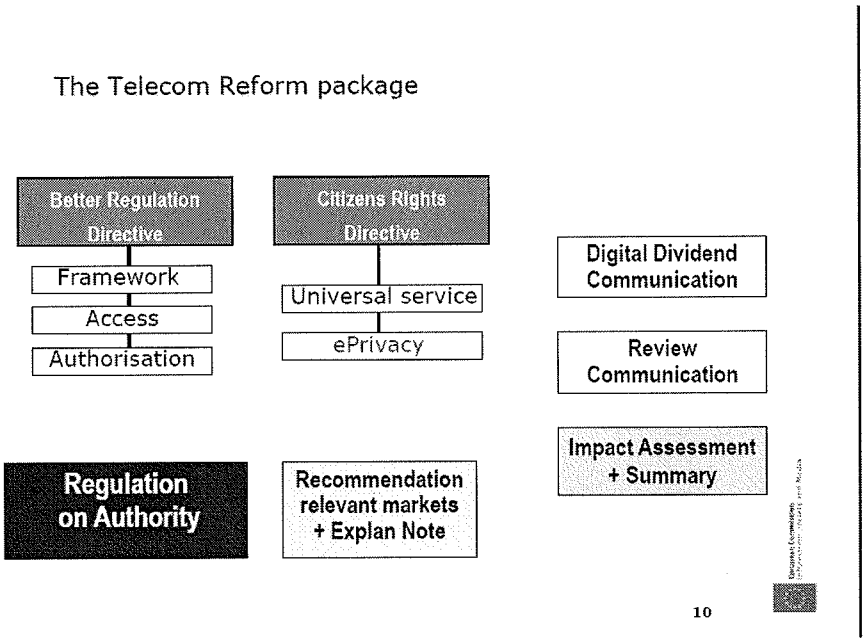
（六）調查同時發現數個優良合作計劃範例，如法國 Signalspam、比利時 eCops 及荷蘭 the Cybercrime Working group。根據以上之調查結果，歐盟執行委員會結論如下：

- 會員國及其他利害關係人應加強線上隱私權的保護，以免受垃圾郵件、偵測軟體及惡意軟體之威脅。
- 根據證據顯示，於程序進行中應投入更多資源，並加強國內與國際間之合作。
- 執委會於電信改革法案提出之新架構扮演重要角色，一旦此些電信規則被採用，將有助於防制垃圾郵件及惡意軟體工作。

三、2002 年線上隱私權保護指令（Directive 2002/58/EC）：

2002 年 7 月歐盟有關電子通訊中個人資料處理與隱私保護指令明文禁止發送垃圾郵件，相關規定詳如前述議題六介紹。

四、電信改革方案架構：



圖片來源：Merijn Schik 簡報

歐盟執委會提出之電信改革，針對公民權之指令，訂有電信普及化服務及隱私權兩項要求，其中電子通訊隱私權之要求與防制垃圾郵件相關，如採用蒐集電子郵件位址之措施，將使濫發垃圾郵件之情形獲得改善，並落實個人資料之保護。

歐盟執委會並加強垃圾郵件之規制如下：

（一）第 13 條明文禁止寄發”釣魚”訊息，即禁止寄發違反 2000/31/EC 第 6 條指令之電子郵件。

（二）第 13 條新增規定，賦予自然人及法人私法權利，以對抗濫發郵件者。

（三）跨領域執行合作之架構正式明文化，納入歐盟對消費者保護合作之規範。

議題八、加拿大反垃圾郵件法規

本節由加拿大廣播電視及電信委員會（Canadian Radio-television and Telecommunications Commission, CRTC）Lynne Fancy 主講加拿大反垃圾郵件法規之立法及電子商務保護法（Electronic Commerce Protection Act; ECPA, Bill C-27）。

一、加拿大總理聲明

加拿大總理於 2008 年 9 月作出聲明將反垃圾郵件立法納入消費者保護平台，保守黨政府將推行消費者保護計畫，包含之項目如下：(1)對於虛偽不實或誤導消費者之廣告增加民事罰鍰（civil penalty）及刑事追訴罰金或自由刑；(2) 透過立法降低網路垃郵，並且禁止竊取身分、散佈病毒、網路釣魚及其他詐騙方式；(3) 針對寄送危險、詐騙、具毀壞及企圖竊取個資之電子郵件，增加罰金；(4) 建立協調單位，用以確保立法有效執行，以及回應消費者申訴。

二、Bill C-27 及 Bill S-220 之立法進度

- Bill C-27 即電子商務保護法（ECPA），該法於 2009 年 4 月進入國會審查，目前該法案在下議院工業及科技常務委員會。
- Bill S-220 係參議員 Goldstein 繼 2008 年後，於 2009 年 2 月再次提出之關於商業電子訊息法（An act respecting commercial electronic messages），目前該法案在參議院交通通訊委員會。

三、ECPA 主要內容

- ECPA 係垃圾郵件工作小組建議之全方位法規制度，仿效國際最佳實務經驗，以經濟制裁取代刑事制裁來維護電子商務。內容包括擴大義務、收信人訴訟權（Private Right of Action , PRA）、行政罰鍰（Administrative Monetary Penalties , AMPs）及國際合作，另設輔助機制，如全國

性協調團體及垃圾郵件回報中心。

- 加拿大政府研擬該法案，係參酌澳大利亞、美國、英國及歐盟等國家法規，企圖建立最完整的機制。加拿大主要貿易伙伴皆透過行政法規機制來規範垃圾郵件，故 ECPA 將允許三個執法機關配合國際伙伴共同合作、分享資訊及完成調查。藉由與加拿大貿易伙伴相似的禁止規範，促進國際合作，收信人訴訟權在加拿大終結後亦可追溯至外國。

四、ECPA 禁止行為

- ✓ 濫發非經邀約之商業電子訊息。
- ✓ 網路上虛偽不實或引人錯誤之表示（含網站及位址）。
- ✓ 利用電腦系統蒐集未經同意之電子位址。
- ✓ 未經授權改變資料傳輸。
- ✓ 未經同意植入電腦程式。
- ✓ 未經授權進入電腦系統蒐集個資。

五、涉及之主管機關

包含 CRTC、競爭局（Competition Bureau）及隱私委員辦公室(Office of Privacy Commissioner, OPC)，其分工如下表：

主管機關	主管違法事項	管制作為
CRTC	1.發送未經邀約之商業電子訊息。 2.未經授權改變電信傳輸資訊及下載程式安裝於電腦系統或網路。	1.SPAM 2.惡意軟體與僵屍網路 3.網路釣魚
Competition Bureau	修訂競爭法中違法事項之規定，增訂誤導及虛偽的行為或陳述，例如虛偽不實之信首資訊、郵件主旨…等。	線上虛偽不實或引人錯誤之表示(包括網站及行為)
OPC	修正個人資訊保護及電子文件法(PIPEDA)違法行為之範圍： 1.未經同意收集或使用個人資訊。 2.藉由接取、使用或干擾他人電腦，收	1.電子郵件位址收集 2.字典式攻擊 3.間諜軟體(取得個人資訊)

	集個人資訊。	

六、重罰與合法程序

- ✓ CRTC 配合 ECPA 將採用行政罰鍰。
- ✓ 修正競爭法可課以行政罰鍰及其他處罰。
- ✓ 該法第 20 條第 4 項規定主管機關可課予個人最高 100 萬加幣罰鍰，個人以外之組織團體（any other person）1000 萬加幣罰鍰。
- ✓ 於課處罰鍰前，要求 CRTC 等主管機關必須考量第 20 條第 3 項所定諸項因素，以避免影響私權訴訟之法定損害賠償請求。

七、選擇加入（Opt-In）機制

- ✓ ECPA 採 Opt-In 機制，以規範任何電子訊息之寄發應經同意，此同意又區分如下：
  - 明示同意－係指發信人直接對收信人表達是否願意接收電子訊息，除非收信人明示同意接收，發信人不得為收信人已同意接收之假設。
  - 默示同意－既存商業關係、既存非商業關係及其他法律規定情況。

八、私權訴訟（The Private Right of Action, PRA）

ECPA 提供私權訴訟，無論企業、網路服務提供者或個人皆可對違反 ECPA 之人提起民事訴訟，而美國只保障網路服務提供者之訴訟權。

九、國際合作

- ✓ ECPA 規定三個執法機關間協商整合，但資訊分享及諮商不限於三個執法機關，亦包含國際間相類似之機構。
- ✓ 擴大加拿大連結，即電子訊息於加拿大收受、寄發或僅經過加拿大境內之伺服器。
- ✓ 就任何違法行為，相關組織應提供資訊予執法機關。

十、垃圾郵件回報中心

為支援 ECPA，政府將成立垃圾郵件回報中心，該中心允許企業或個人將所接收之網路訊息回傳至中央處理設備，此些網路訊息如經分析認定係構成 ECPA 所定違法行為，則移轉相關主管機關採取行政措施，並儲存分析資料以供證據或執法所用。該中心亦支援相關機關（如三執法機關）共同合作，並協助三

執法機關之調查及舉發事宜。

十一、反垃圾郵件協調機構

反垃圾郵件工作小組於 2005 年 5 月報告中，建議在政府部門成立核心或協調中心，統籌加拿大反垃圾郵件事宜，該協調機構將支援 ECPA 提供下列功能：檢視實際政策缺失、監督法令執行與成效、支援國際合作（如 LAP 或 OECD 等）、協助一般民間機構進行反垃圾郵件事務、監督垃圾郵件回報中心之運作、管理 Stop Spam Here 網站、從事研究與統計數據事宜及分析報告新興威脅與趨勢。

十二、新法結論

ECPA 融合垃圾郵件工作小組建議、法案 S-220 內容及其他國家反垃圾郵件措施，將以公平有效之措施，達成下列目標：（1）對抗危害行為（2）執法全方位及大範圍（3）加強適用之靈活度（4）利用現有專業技術進行多方面執法措施（5）促進國際合作（7）加強教育宣導。

議題九、荷蘭之公私合作關係

本節由荷蘭獨立郵政及通訊監理機關（Dutch Independent Post and Telecommunications Authority, OPTA）資深政策專員 Maarten Klijn 主講。

一、公私合作之範例

荷蘭執行公私合作共同對抗殭屍電腦之計劃，成效極佳，相關之情形如下：

- ✓ ISP 業者事前研究污染源、分享濫發郵件之經驗與實務操作並進行充分之資訊交流。
- ✓ 掌握污染源，如濫發平台、封鎖隔離、支援客戶並帶領消費者重新上網。

二、公私合作（Public Private Partnerships，簡稱 PPP）

（一）公私合作之內涵

相關內涵包括設定架構（特別是與主要網路業者）、可信賴的企業精神、消費者保護意味吸引客戶、認知（不過這並不長久）、行動打敗消極順從及明確的政府政策。

（二）運作之程序

- ✓ 公私合作之運作及如何使網路服務提供者與政府合作自如之要點，歸納如下：

  1.應立於業者角度思考，並創造安全的環境。

  2.證明 OPTA 係出於善意。

  3.應解釋計畫而非隱藏時程表。

  4.消除官方權威色彩。

- ✓ 自 2008 年 12 月起，荷蘭政府與業者試圖研商一個充分的計劃，但過程並不順利，其原因可能源自雙方對合作存有遲疑，並認為彼此畢竟互為競爭者。網路服務提供者不願洩露細節之原因，經分析可能是對主管機關不信任，且質疑該機關之企圖。直至某個夥伴推出成果，總算有所突破，而使運作步上軌道，至此，政府轉變而為監督及促進者角色。

- ✓ 其實，政府之目標如下：(1)促使業者使用封鎖(2)提供客戶脫離封鎖之方法(3)使受電腦病毒感染之民眾獲得相關資訊、學習技術及操作程序 (4)建立 4-5 家主要參與者合作機制(6)高度管理承諾等。

- ✓ 歸納 OPTA 與網路服務提供者的交涉重點如下：

  1.應仔細衡量自身之措辭。

  2.不要預設太多。

  3.互相信賴。

  4.分享歷史。

三、公私合作之準備

我們準備好了嗎？目前政府的目標與業者的承諾大致吻合，且有 14 家業者係出於自發性之合作，對業者而言，政府給方向比單純期待更為重要。再者，國際公約是一個出發點，我們應評估歐盟公約對荷蘭的現況會產生什麼影響，及如何界定污染源。就長期發展而言，我們要用最新的殭屍電腦偵測工具開拓荷蘭的技術。

四、結論--我們看到了什麼？

公私合作並不容易，但可行性極高。綜合而言，公私合作之要點如下：

- ✓ 應配合良好的程序管理。
- ✓ 勿過分管理，須有冷靜的期待。

- ✓ 策略性的討論。
- ✓ 一目了然。
- ✓ 找尋一個有策略思考的合作對象。
- ✓ OPTA 非常高興有此結果，特別感謝自發且熱心合作的網路服務業者，PPP 為現今世界第一個模型，此亦象徵一個新契機的開啟。

議題十、自願性資料交換所涉隱私問題

本節由荷蘭皇家 Kpn 電信公司合法監聽部(Royal Kpn N.V.)經理 GERT WABEKE 主講。

一、2008 年 9 月，荷蘭國外貿易部部長 Heemskerk 宣布該國開始執行海牙行為準則中之「通知移除機制」(Notice-and-Take-Down)。

二、2009 年 8 月，荷蘭 14 家網路服務提供者聯合發起對抗殭屍電腦行動及合作起草公約，並表明相互分享網路犯罪知識及資訊，依此方案，將可達成快速回應及增進對抗殭屍電腦措施之效能。

三、有關公私部門間之資料交換，可分享之資料類型為與社會有關之資訊，如威脅或病毒警報；公私部門資料之交換程序包含(1)ISP 根據可信任之申訴者，點對點回傳路徑指證垃圾郵件。(2)公部門依據受理之申訴案，發出正式請求資料等。

三、2009/10/9 議程

議題一、打擊垃圾郵件之技術方案

本節由葡萄牙國家科學計算基金會（Foundation for National Scientific Computing, FCCN）Pedro Veiga主講「垃圾郵件：一個無法避免的惡夢？」

一、背景：

- 1987年1月FCCN成立，其係受國家補助之私立非營利機構，在一些大學及私立非營利研究發展單位之支持下，研究有關葡萄牙網際網路之擴展業務，並負責葡萄牙學術及研究網絡「科學、科技及社會網絡」（Science, Technology and Society Network, RCTS）之設計及管理，其目的在提供更理想之網絡予有較大頻寬需求之單位，並建立高階通訊及服務業務運用之實驗平台。
- RCTS 網絡採用網際網路規範以保障教育、科學、科技及文化機構間得以建立一個通訊及合作平台。FCCN同時負責網域及次網域之註冊、虛擬校園及大宗郵件之服務等工作，它亦是Portuguese Foundation Centre（CPF, Centro Português de Fundações）之會員。
- FCCN為葡萄牙第一個CERT.PT，並負責訓練之工作。其亦致力於建立葡萄牙之研究及教育網絡，已完成1.000公里之暗光纖系統（dark fibre），學校機構之使用者逾1,500萬人。再者300.000網域已註冊於.PT。DNSSEC 系統於1年前建置，並於上週開放予所有持有網名者使用。

二、共同合作打擊垃圾郵件：

- 籌劃ISP論壇：第一次會議於2004年中召開，討論ISP控制垃圾郵件之技術、黑名單及阻欄客戶之困難等議題。
- 2007年建立正式關係，達成之成效包括：創造處理安全事件之能力、蒐集統計數據、交換資訊、相互合作及建立交換黑名單之中央系統。

三、科技之角色問題：

- 科技之合法性問題：
  - ✓ 知識（及意願）之欠缺。

- ✓ 高財務損失（如釣魚網站）。
- ➢ 客戶端解決方案：
  - ✓ 過濾軟體/規範。
  - ✓ 垃圾郵件量未減少。
  - ✓ 伺服器之下載未減少。
- ➢ 服務者端解決方案：
  - ✓ 依賴黑名單。
  - ✓ 「智慧」訊息之偵測。

四、科技仍力有未逮：

- ➢ 科技有效但仍有其他問題。
- ➢ 任何領域導入安全議題，面臨之問題如下：
  - ✓ 須花費資源及金錢。
  - ✓ 須變更程序及方式。
  - ✓ 須訓練。
  - ✓ 電子郵件科技須予進化。

議題二、OECD 2006年跨國反制垃圾郵件法規建議之檢討

本節由經濟合作暨發展組織（Organization for Economic Cooperation and Development, OECD）秘書處消費者政策委員會Brigitte Acoca主講。

一、OECD反制垃圾郵件之努力

- ➢ OECD反制垃圾郵件專案小組
  - ✓ 2005年反制垃圾郵件法規執行報告(彙整OECD會員國之問卷回應)
    - ● 負責執法單位之類型。
    - ● 國內執法架構。
    - ● 有效跨國執行之挑戰。
    - ● 面對挑戰之努力（包括資訊分享）。
  - ✓ OECD反制垃圾郵件建議之政策及方案
    - ● 呼籲政府機關建立國內反垃圾郵件政策並以下列方式與個別團體合作：
      - · 發展反垃圾郵件規範。
      - · 執行。

- 產業導向方案。
- 科技方案。
- 教育、自律。
- 公部門及私部門團體合夥伴關係。
- 評估。
- 全球合作。

✓ 2006年OECD垃圾郵件建議書呼籲會員國：

- 建立有效之國內架構。
- 經由妥適之合作架構(包括資訊分享及支援調查)，增進跨國合作能力。
- 改善合作程序。
- 與私部門團體之合作。
- 監督採行建議3年來執行跨國合作之進展。

二、2006垃圾郵件建議書之檢討：

- 2010上半年完成合作問卷。
- 2010年中回收回應。
- OECD秘書處準備分析報告。
- 2010第三季完成LAP及相關團體提出之評論。
- 報告提送2010年10月CCP及ICCP會議確認。
- 辦理後續聯合研討會事宜。

三、主要議題：

- 自2006年以來，有關垃圾郵件議題之國內法規有否變更以致影響跨國合作執法？有否需要新法規？
- 所設置處理跨國需求及個案之機制為何？
- 有否建立任何合作夥伴關係以備跨國公私合作之需？
- 跨國合作執法機制有否面臨任何挑戰？如何改善之？

四、優先考慮事項：

- LAP有否意願與OECD執行合作計畫？
- 如是，所提方案之範圍是否可被接受？
- LAP對於檢討報告有否其他欲加入之議題？
- LAP對於OECD未來處理垃圾郵件有否其他建議？

議題三、日本反制垃圾郵件之成效

本節由日本總務省（Ministry of Internal Affairs and Communications, MIC, Japan）、日本資訊及通訊協會（Japan Data Communications Association, JADCA）及防制電子郵件濫用團體（Japan E-mail Anti-Abuse Group, JEAG）代表主講該國防制垃圾郵件相關措施。

一、日本反垃圾郵件法（Japanese Anti-Spam Law）

（一）發信人之義務

1.「選擇進入」機制（第 3 條）

（1）禁止未經收信人的同意即寄發商業郵件。

（2）保存收信人的同意記錄之責任。

（3）禁止寄發給拒絕收到此類商業郵件之人。

2.標明義務[2]（第 4 條）

3.禁止以虛偽的發信人資訊寄發電子郵件（第 5 條）

4.禁止寄發電子郵件至虛假的電子信箱（第 6 條）

（二）防制流程

- ✓ ISP 接獲信件，發現其為垃圾郵件時，應依第 8 條規定，向總務省報告，並依第 11 條規定，對濫發垃圾郵件者拒絕提供網路服務以為抵制。
- ✓ 收件人如發現垃圾郵件，亦得依第 8 條規定，向總務省舉發。總務省接獲舉發垃圾郵件案件後，依第 28 條規定，得為實地調查、蒐集報告，並得依第 29 條要求 ISP 提供濫發者之相關資訊。
- ✓ 為促進防制垃圾郵件之國際交流，總務省依第 30 條規定，得提供垃圾郵件相關資訊予外國執法相關單位。

二、日本總務省採取之作法

（一）總務省對持續違反反垃圾郵件法之發信人，每周寄發郵件警告之，此行政行為係行政指導措施。

（二）總務省蒐集接獲警告但未改善之發信人情報。此些情報之提出可為強制性（依據防制垃圾郵件法第 28 條）或為任意性。

（三）自 2004 年反垃圾郵件法制定以來，總務省共發出 8 件行政

[2] 標明「此為 spam」之義務。

指示，要求發信人遵循該法，2008 年修正案通過施行後，共發出 2 件行政指示，2009 年，僅於 4 月及 6 月各發出一件行政命令。

（四）總務省發出之警告郵件統計數量如下：

年/月		警告郵件
2008	12	307
2009	1	330
	2	276
	3	234
	4	252
	5	396
	6	576
	7	507
	8	566
總計		3,444

（五）警告郵件之有效性

總務省對違法發信人寄發郵件警告後(一個月內)，約有 38%的發信人停止寄發垃圾郵件，且發送之郵件數已降低大約 1/3。

三、技術措施

（一）ISP 對於寄送郵件之限制（避免利用 ISP 本身之網路寄發垃圾郵件）

- ✓ 遮斷動態 IP 位址使用 25 埠，使之無法透過 ISP 伺服器發送垃圾郵件。
- ✓ OP25B 計畫亦可遮斷利用 bots 程式所發的垃圾郵件，JEAG 之努力，造就了 OP25B 計畫的廣泛普及。

（二）實際情況

- ✓ 引進 OP25B 之 ISP 數量逐年增加。
- ✓ 日本在垃圾郵件發送源國家的排名已由第 9 名下降至第 33 名。

四、垃圾郵件發送地在日本國內與國外之比較百分比

（一）電腦方面

2006 年至 2009 年間，由日本國內發出之垃圾郵件已由 28%下降至 5%，由國外發送至日本國內之垃圾郵件由 72%上升

至 95%。

（二）行動電話方面

2006 年至 2009 年間，由日本國內發出之垃圾郵件已由 98.3%下降至 3.1%，而由國外發送至日本國內之垃圾郵件由 1.7%上升至 96.9%。

五、國際間合作防制垃圾郵件

（一）目的：因應發送自國外之垃圾郵件急速增加的狀況。

- 2008 年反垃圾郵件法修正案：
  - ✓ 總務省可提供濫發垃圾郵件者之名單予外國執法單位。
  - ✓ 確認由國外發送至日本的垃圾郵件係日本反垃圾郵件法之規範範圍。
  - ✓ 延伸防制垃圾郵件之行政命令範圍，使總務省可採取方法對抗於日本下達指令給海外寄件人發送垃圾郵件之發令者。

（二）交換各國垃圾郵件發送源

日本資訊及通訊協會（JADCA）定期與中國、香港及臺灣相關單位交換垃圾郵件發送地 IP 位址之資訊。

（三）提升國際合作架構

1. 垃圾郵件接收者提供相關資訊予 JADAC 及總務省，此二單位人員分析垃圾郵件之相關資訊，並釐清發送垃圾郵件之位址。
2. 垃圾郵件發送地在國外之案件，其相關資訊將由 JADAC 提供予發送地相關管制單位。
3. 收到垃圾郵件位址之相關單位將提供該類資訊予 ISPs，業者並將採取對抗垃圾郵件發送者之措施，例如終止與垃圾郵件發送者之網路服務供給契約。

六、日本民間團體之作為

- 成立反制垃圾郵件諮詢中心（ASCC）
- 根除支援方案（ESP）：
  - ✓ 2005 年設置之政府與 ISP 間合作計畫，其內容包括：監督、攔截、通報 ISP、ISP 之處理程序（確認、忠告、警示、制止、刪除）。
  - ✓ ASCC 負責監督、調查及蒐集發送源資訊之業務，並

於每週將相關資料彙送 ISP 業者處理，同時要求其應予回覆。

- 日本垃圾郵件攔阻率：
  - ✓ 總攔阻率有大幅下降趨勢：
    85.2%(Apr.2005) →82.6%(Apr.2006) →24.8%(Apr.2007)→3.6%(Apr.2008) →4.1%(Apr.2009) →1.9%(Aug.2009)
- 與國外主管機關之聯繫：
  - ✓ 始於 2007 年。聯繫之對象包括：中國大陸、香港、臺灣。統計來自以上國家之垃圾郵件數量，亦有大幅下降趨勢：
    中國大陸：38.1%→25.0%；香港：0.1%→0.1%；臺灣：2.4%→0.5%。

七、JEAG 介紹：

- JEAG 成立於 2005 年 3 月，係一非營利私法人團體，並受 3 單位（MIC, METI, JADAC）之觀察。現階段該團體會員數 30，多數為 ISPs、行動電話公司及銷售商。並與反訊息濫用工作小組（MAAWG）及亞太防制濫發商業郵件聯盟（APCAUCE）保持聯繫關係。
- JEAG 建議書（2006/2/23）
  - ✓ OP25B 計畫（Outbound Port 25 Blocking）
  - ✓ 鑑定寄件人技術(Sender Policy Framework, SPF)
  - ✓ 行動電話”最有效措施”（BP）
- 防制垃圾郵件為無國界之議題，有賴國際合作。
- 各國甚難確認垃圾郵件是否係由本國寄發，故須分享資訊。

議題四、RIPE NCC 簡介

本節由歐洲IP網絡合作中心RIPE Network Coordination Centre（RIPE NCC）代表Jochem de Ruig等介紹該中心及其業務內容。

一、背景：

- 歐洲IP網絡RIPE（the Réseaux IP Européens, European

IP Networks）為一公開論壇，提供予所有對網路科技發展有興趣之團體使用，其設立目的在確保發展網路有關行政及合作事宜之運作。RIPE NCC（RIPE Network Coordination Centre)於1992年成立於荷蘭阿姆斯特丹，其亦為一提供關注網路科技發展團體之公開論壇，並支援RIPE之技術及行政事務。

- RIPE NCC 為全球五大區域性網際網路註冊中心之一（Regional Internet Registry, RIR)，其服務範圍涵蓋歐洲、中東及中亞部分地區。「RIPE社區」又形成數個工作小組（RIPE Working Groups）以處理各類涉及RIPE NCC會員及一般網路之議題。

二、組織及業務：

- RIPE NCC 係一獨立非法人及非營利機構，目前會員數6,000，遍佈於75國，現階段無官方會員。其運作模式如下：開放予所有人、無投票制度（以共識無主）、以工作小組及團隊從事業務及提供政策論壇、不參與政策制訂。
- RIPE NCC提供以下兩類服務：
  - ✓ 會員服務：分配資源（IPv4, IPv6, AS 系統）；提供訓練課程。
  - ✓ 公共服務:提供資料庫、DNS反查、ENUM(e164.arpa）機制、K-root域名服務器、線上學習等。

三、相關法制面介紹：

- 網際網路號碼資源（Internet number resources, INR)：依與會員成立之標準化契約進行相關事宜，如契約終止或資源自動歸回等。
  - ✓ 契約無縫隙、IP位址依需求設置、INR非私人財產。
- 終止LIR會員身分：
  - ✓ 終止之程序複雜、僅部分可能回復INR。
  - ✓ RIPE NCC可採取以下方式變更路由(Routability)：
    - ● 變更RIPE資料庫之管理者、移除RIPE資料庫紀錄及DNS反查機制、發佈”回收之INR” 訊息。
  - ✓ INR仍可使用。
- RIPE資料庫依據資料保護規定運作：
  - ✓ 所有紀錄由管理者管理、個資可應當事人請求移除、

大量資訊非包括個資。

- ✓ 所有資料皆可即時取得，且由管理者負責資料之品質。

四、RIPE NCC無法從事之業務：

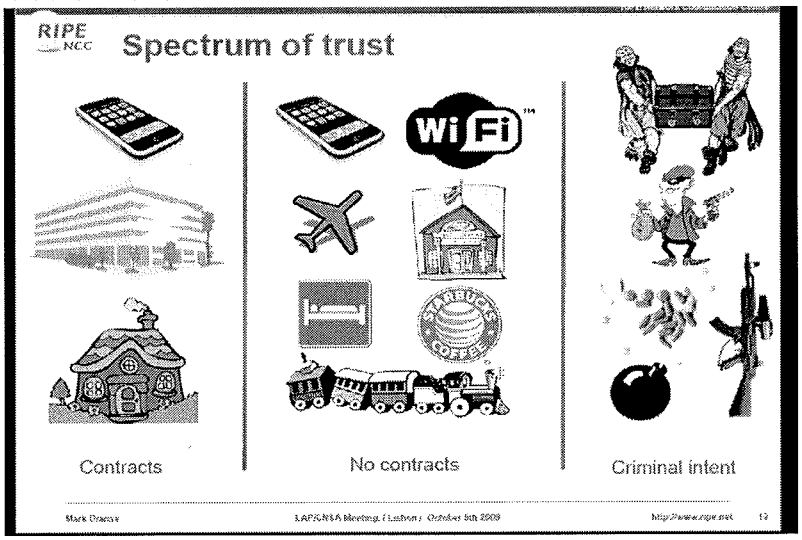
- ➢ 取消及回復INR。
- ➢ 查知INR實際使用者之位置。
- ➢ 以INR使用之內容提供資訊。
- ➢ 無正式荷蘭資訊要求來源，RIPE NCC不可提供任何非公共資訊。

五、網際網路認證介紹：

- ➢ 對象及資源之識別：

  如存取限制之內容(如BBC)、拒絕存取未經同意之內容(如中國)、搜尋目標或廣告(如搜尋之結果、本地新聞/天氣、航空公司、約會地點)及線上犯罪調查等。
- ➢ 果真如此簡單嗎？
  - ✓ 一言以蔽之：「不」。

    惟其係使用巨大 IP 範圍，故高層級數據（如國家/城市）之正確性相對提高，無根據之來源可予接受且錯誤容易修正。
- ➢ 網際網路信任關係如下表：



圖片來源：RIPE NCC 簡報

六、結論：

- ➢ 針對個案之分析教育有助加強瞭解相關問題。
- ➢ 所有原始數據應提供予調查之用。
- ➢ 防制技術之發展有賴整體力量挹注。

- 個案結果之解讀應提供支援。
- 數據之品質應予確保（如：安全儲存、保證來源、機構之可信度）。

肆、檢討與建議

隨資訊科技與網路產業快速發展之趨勢，垃圾郵件、惡意程式、網路病毒及跨國網路犯罪等問題湧現，衝擊全球，國際社會對於共同合作以促進網路安全、打擊網路犯罪及防制垃圾郵件之必要性，已形成共識。我國自 94 年 8 月加入倫敦行動計畫（LAP）成為正式會員以來，逐年派員參與「倫敦行動計畫及垃圾郵件主管機關聯繫網絡(LAP/CNSA)研討會」，積極展現國際合作防制垃圾郵件之決心。

本會議為國際社會重要交流平台，並為各國主管機關聯繫管道，除可蒐彙各國及業界防制垃圾郵件之法制規範、因應策略及實務措施，以供我國建構垃圾郵件防制體系之參考外，並能累積國際交流經驗及提升國家能見度，其意義可謂至為重大。展望未來，本會應加強與各國之密切合作並分享資訊，以善盡主管機關及國際社會成員之責。

本次會議涉及之網路議題極為廣泛，探討之內容涵括四大主題：法規機制與執法案例、防制技術與措施、調查與訓練、網路安全與合作。茲針對上開會議內容提出檢討與建議事項如下：

一、借鏡外國立法與執法經驗

鑒於垃圾郵件議題已逐漸融入網絡、資通安全、網路犯罪及消費者保護領域，本次會議由歐盟、奧地利、加拿大、日本及馬來西亞之代表介紹垃圾郵件法規機制，並由葡萄牙及荷蘭就主管機關之執法措施、消費者保護、公私部門合作及業界技術方案等，詳予說明。藉由深入瞭解上開各國所提供之立法設計與措施方案，適足以作為我國建置垃圾郵件防制機制之參考，以備未來執行之因應。

二、持續加強國際合作

誠如本次會議主席 Teresa Maury 女士於開幕辭所言，本會議之首要目的係在期許各國建立全球性合作夥伴關係並共同致力未來網路經濟之發展，隨垃圾郵件濫發行為及網路犯罪案件日漸增多，各國執法機關共同面臨處理跨國性違法案件之困境。有鑒於此，本次會議與會代表無不強調國際合作之重要，並由葡萄牙及愛爾蘭，針對國際合作事務議題，作深入之探討。我國為國際社會之一員，為配合處理跨國垃圾郵件產生之諸多問題，本會責無旁貸，應就推動立法、加強國際聯繫及積極參與國際事務等事項，持續進行審慎之規劃與檢討；並

針對國際合作之擴展及執行，考量合作各國平等互惠之原則，主動尋求合作伙伴，共同發展常態性國際合作實務交流平台。

三、主動積極參與防制事務

LAP 為我國現階段少數參與之全球性國際組織之一，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步建立合作關係，此成果得之不易；未來應於此基礎之上，持續加強配合執行，以彰顯我國總體發展之成效。又本次會議獲益良多，除討論及會談內容極具參考價值外，與會各國代表主動積極之態度，亦令人印象深刻。建議未來本會應積極把握國際合作交流契機，審慎規劃，或可於會議中提出報告，就我國防制垃圾郵件之成效與作為，分享各國。

四、擴大防制機制並共同努力

為因應垃圾郵件濫發與跨國性組織化網路犯罪日趨結合之情勢，現階段我國單一或分散式主管機關之型態，似已有不符需求之疑慮。當務之急，恐須考量擴大垃圾郵件防制機制，或成立跨部會合作小組互補不足，俾可整合政府機關、業界及民間團體之力量，共同努力，以期強化我國整體防制能量，並有效支援國際聯防機制，達成遏止垃圾郵件之目標。