出國報告（出國類別：參加國際會議）

出席「第八屆倫敦行動計畫暨訊息、惡意軟體和手機反濫用工作小組(LAP/M3AAWG)年度共同會議」報告

服務機關：國家通訊傳播委員會

姓名職稱：蘇科長思漢、林技士湛翔

派赴國家：加拿大蒙特婁

出國期間：2013 年 10 月 22 日至 10 月 25 日

報告日期：2014 年 1 月

摘要

本次倫敦行動計畫年度共同會議與訊息、惡意軟體和手機反濫用工作小組(M3AAWG；Message, Malware, and Mobile Anti-Abuse Working Group)聯合舉辦，M3AAWG 為全球性的國際組織，其目的希望透過產業合作、技術、公共政策等三方面的領域，來解決各種形式的電子訊息濫用，例如可能帶有惡意軟體的垃圾郵件、病毒以及其他攻擊等，目前本會尚未加入該組織。

由於通訊技術的日新月異，垃圾郵件所帶來的不再只是因「大量」的塞滿信箱導致可能的重要訊息被忽略或是流失的「困擾」，隨之而來的是資訊安全的風險，許多的駭客利用電子郵件進行「網路釣魚」、「社交工程」等手法竊取敏感的個人資料牟取不法利益，甚至造成網路用戶的名譽受損與財產損失，或是利用挾帶惡意軟體的方式，植入不知情的用戶電腦形成「殭屍網路」遂行不法行為，由資訊安全方面的專家公佈統計數據顯示，上述行為每年造成以「億」與「美元」為單位的經濟損失，然而撇開資訊安全議題單純從經濟角度來看，在垃圾郵件的背後，已經形成具有一定規模的市場經濟，擁有完整的供應鏈，在一定程度上破壞了「合法」市場的規則，對經濟產生影響，且大多數的垃圾郵件供應鏈為國際性合作模式，造成查緝上的困難，甚至出現提供垃圾郵件濫發服務的公司，他們與國際駭客合作，藉由駭客操控所屬「殭屍網路」大量濫發商業電子郵件，並與駭客分享利潤，同時卻也在背後為提供「反垃圾郵件」服務的公司創造不少利潤。由於垃圾郵件牽涉的層面複雜，查緝難度高，有關「反垃圾郵件」的法令規章一直頗受爭議，國際皆然，舉例來說，加拿大已制訂「反垃圾郵件法」並預計於 2014 年 7 月正式生效，其中對於違法的個人或法人用戶皆處以高額之行政罰鍰，但法案是否能有效落實尚待考驗，亦可提供本會相關立法之參考。

以通訊科技發展的趨勢來看，電子郵件不再是駭客入侵或商業廣告的主要媒介，隨著行動通訊裝置普及，許多非「郵件」的電子訊息也成為當前資

訊安全的隱憂，例如「Line」、「Facebook」、手機簡訊等，垃圾郵件事實上僅是資訊安全中的一環，網路用戶權益的保障除了加強認證機制與國際合作之外，還是必須透過宣導，建立正確的資訊安全防護觀念，培養良好的網路使用習慣。

目錄

壹、 前言

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、多邊防制垃圾郵件合作協議外，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)年度會議」。在本次會議中，本會在會議中上台報告，以「目前臺灣防制垃圾郵件之概況(The Status Quo of Combating Spam Emails in Taiwan)」為主題進行約 15 分鐘的簡報。本次會議主題以「加拿大反垃圾郵件法的立法與規範」、「垃圾郵件之經濟結構」、「防範垃圾郵件的新方式」、「網路詐財、手機網路監聽及詐欺–濫用支付系統的世界」、「行動裝置的威脅」等為中心，會議之宗旨有促進國際合作、建立全球性夥伴關係、呼籲公協會及業者參與、提升公眾防堵資安事件意識、建立周全法規機制、加強資訊分享及追蹤技術之研發、共同致力於未來網路經濟之發展等項。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、檢討心得與建議、附錄等擇要撰擬，期望對於相關業務之推動有所助益。

貳、 第八屆倫敦行動計畫暨訊息、惡意軟體和手機反濫用工作小組(LAP/M3AAWG)年度共同會議

一、 會議時間、地點及議程

時間：102 年 10 月 22 日至 10 月 25 日

地點：加拿大蒙特婁(Canada, Montreal)

議程：詳附錄

二、 開幕式

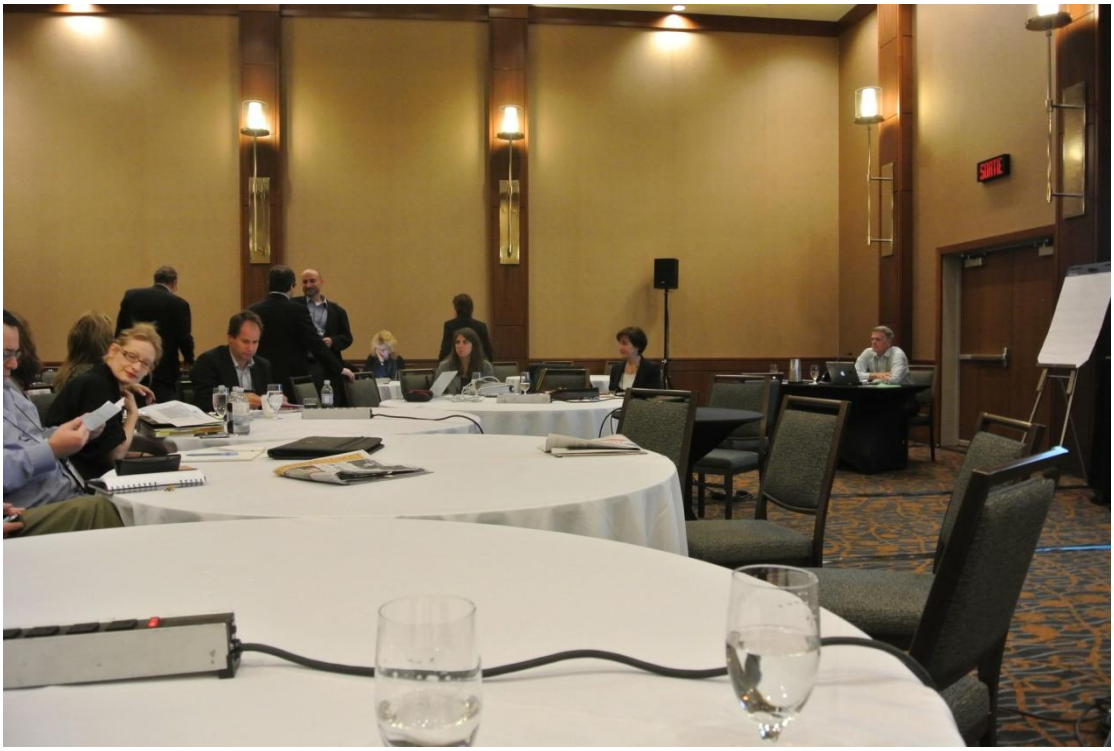
本次會議係加拿大工業部(Industry Canada)主辦，參與會議之國家包括歐盟、美國、加拿大、澳洲、英國、荷蘭、法國、紐西蘭、日本、南非、香港、南韓及我國等。倫敦行動計畫（the London Action Plan, LAP）之目標在促進國際間垃圾郵件及相關議題如網路詐欺、釣魚及散佈病毒之主管機關，共同合作及討論行動議題之機會。

開幕式由 M3AAWG 的執行長 Jerry Upton 致開幕辭，揭櫫本次會議宗旨及目的在於：

1. 積極拓展國際合作、保障網路用戶資訊安全。
2. 建立網路用戶正確之資訊安全觀念。
3. 提振網路消費者信心，促進網路經濟發展。
4. 綜合各國經驗，建置完善法律機制。
5. 資訊分享與資訊安全技術交流。

三、 會議剪影

上、下圖：蘇科長思漢上台報告我國防制垃圾郵件之概況。



會議即將開始，與會成員入場就座。

會議中場休息。

各國代表上台報告相關議題。

會議期間互動討論狀況。

參、 討論議題資料整理

議題一、加拿大反垃圾郵件立法與規範

加拿大訂定反垃圾郵件法案之目的，在於遏止藉由垃圾郵件所衍生出的資訊安全問題，諸如惡意軟體、網路釣魚、電腦病毒、社交詐騙、殭屍網路以及誘導性的商業行為等，建立規範機制與罰則標準，以降低與日俱增的資訊威脅，促進電子商務之健全發展，加拿大的反垃圾郵件法案包含下列部分：

1. 違法態樣

加拿大反垃圾郵件法案，立法禁止下列六種態樣：

(1) Spam

未經同意寄發商業電子郵件(第六條)。

(2) Traffic Rerouting

未經同意擅自變更資料傳輸路徑(第七條)。

(3) Malware

未經同意逕行安裝之電腦程式(第八條)。

(4) Fraud

在網路上利用假網址導引的釣魚方式，進行詐騙行為(第七十二條)。

(5) Harvesting

未經同意使用電腦系統進行電子郵件地址的蒐集(第八十二條第二款)。

(6) Privacy Invasion

未獲許可而進入電腦系統來蒐集個人資料(第八十二條第三款)。

2. 選擇加入(Opt-In)機制與發信郵件格式

採用「選擇加入」機制，任何商業電子郵件之寄發應事先經過同意，發信人不得預先假設收信人同意接收，此外，並區分為明示同意與默示同意：

(1) 明示同意

發信人不得預先假設收信人同意接收，同時，若收信人拒絕再接收，發信人不得繼續發送郵件。

(2) 默示同意

為避免矯枉過正，在下列的情況下，即使收信人未表示接收電子郵件之意向，仍可視收信人為同意接收：

a. 有既存商業上往來的關係。

b. 有既存非商業往來的關係(非營利性質)。

c. 顯著的公開資訊

例如因特定聯絡需求，而在網站上公開的電子郵件信箱地址。

d. 顯著的資訊揭露

例如事先交換名片，名片中所提供的電子郵件信箱地址。

電子郵件的發送，必須符合下列格式：

(1) 可清楚辨識郵件由何人所寄出(寄件人)。

(2) 提供能夠確實聯絡到負責寄發電子郵件者之方式。

(3) 提供可退出同意之機制，並符合下列要求：

a. 至少 60 天內有效。

b. 須免費，不得收取任何費用。

c. 除非方法不可行，否則必須提供相同替代方式。

d. 須包含電子郵件信箱地址或相關連結。

e. 在執行上不得有任何延遲的情形。

3. 私人訴訟權

無論私人企業、網際網路服務提供者或個人，皆有對違反規定者提起民事訴訟之權利。

4. 行政罰

Spam、Traffic Rerouting、Malware 之主管機關為 CRTC(Canadian Radio-television

Telecommunications Commission；加拿大廣播電視及通訊委員會)，違反規定者，個人罰鍰加幣 100 萬，法人罰鍰加幣 1,000 萬；行政罰與私權訴訟並行，最高罰鍰金額為個人 100 萬，法人 1,000 萬。

Fraud 之主管機關為 Competition Bureau(加拿大競爭局)，違反規定者個人第一次罰鍰加幣 75 萬，個人累犯罰鍰加幣 100 萬；法人第一次罰鍰加幣 1,000 萬，法人累犯罰鍰加幣 1,500 萬。

Harvesting、Privacy Invasion 之主管機關為 Office of Privacy Commissioner(加拿大隱私公署)，違反規定無行政罰，但有法定損害賠償。

加拿大垃圾郵件通報中心(Spam Reporting Centre)原規劃委由民間機構經營，但截至 2012 年 12 月底仍無人得標，故目前由加拿大廣播電視及通訊委員會負責營運。

5. 國際合作

鑒於網路屬於跨國性質，僅在國內執法難有實質成效，加拿大亦加入國際合作相關宣示條文，類似我國「濫發商業電子郵件管理條例」行政院版第十九條、立法委員葉宜津版第二十二條、立法委員陳亭妃版第十條，明文規定主管機關因執法需求，得與國際相關組織進行垃圾郵件來源、追蹤方式及其他相關資訊之交流。

6. 延伸責任(follow the money)

法案中加入了延伸責任的概念，並非只針對垃圾郵件的實際發送者，即不論是實際發送垃圾郵件的行為人或是授意人，只要屬於不法行為的共犯結構，或是直接、間接的不法行為受益者，均適用本法案的相關規定。

加拿大廣播電視及通訊委員會於 2012 年 3 月通過 Opt-in 機制的「識別資訊」與「同意要求」之規範，並因應第一次對外意見徵詢之要求，詳加定義「默示同意」之條件，將反垃圾郵件法進行更有彈性之適用。

加拿大工業部規範(Industry Canada Regulation)在 2011 年定義了下列：

1.「家庭關係」與「個人關係」。

2.「社團、機構和公益團體」，以及「非商業性」關係。

擁有「個人關係」和「家庭關係者」，原則上可不經由同意向其發送電子郵件，除非對方有「明示拒絕」之表示。

在法案相關對外徵詢意見時，有多方意見表示此反垃圾郵件法會嚴重阻礙商業法展，甚至會波及到其他原先不欲管制之寄發客體，例如銀行的聲明等，因此在法案中加入下列四項「同意義務豁免」條款：

1. 法人對法人間，持續性商業關係的往來訊息。

2. 對於有關要求、徵詢、客訴方面的回應訊息。

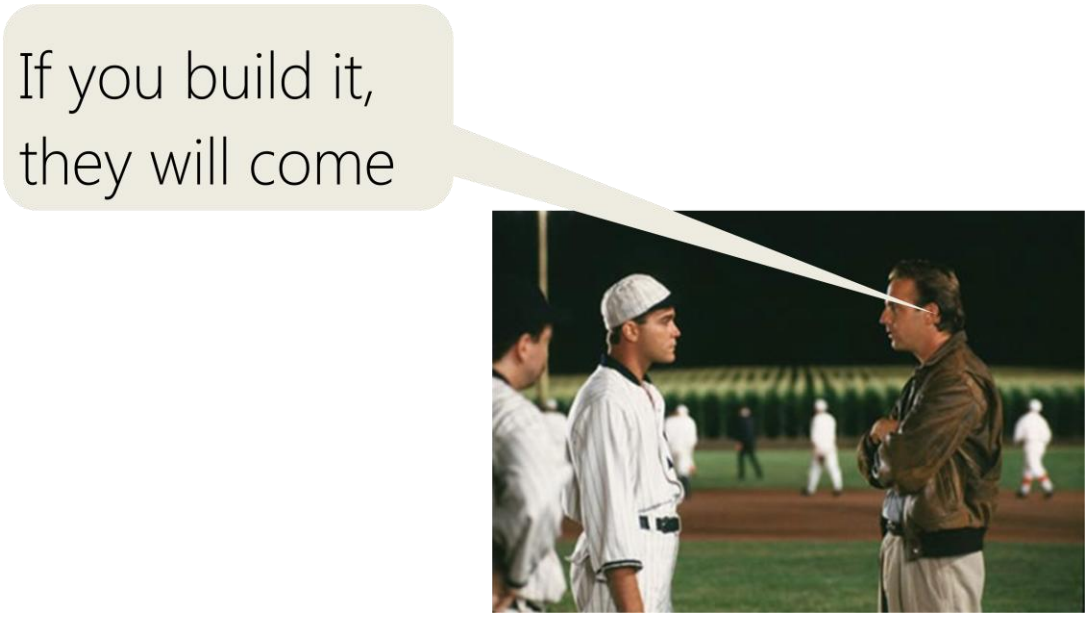
3. 執行法律權利的訊息，例如授權、債務等。

外國發信人寄發電子郵件給外國收信人，郵件經過加拿大，但非在加拿大境內收到電子郵件之情形；此條款是為了避免寄件者在不知自己所寄發的郵件會經過加拿大時，所可能會帶來訴訟之風險。

議題二、垃圾郵件之經濟結構

根據 2010 年的統計，全球每天的電子郵件流量約有 1,000 億封，而其中約有 88%是「垃圾郵件」，在此所稱的「垃圾郵件」定義為「不請自來的商業電子郵件」，而絕大多數的「垃圾郵件」均屬於此類型。

形成「垃圾郵件」的定律就有如在 70 年代的知名電影「Field of Dreams(夢幻成真)」情節，該電影的名言：「If you build it, they will come(如果你蓋了，他們會來)」，也間接反映了「垃圾郵件」形成的主因。



電影情節中，蓋了球場，則熱愛棒球的「靈魂」就會來，同樣的，提供了便捷快速服務的平台，有興趣的「靈魂」也會不請自來，例如網頁郵件(web mail)、社群網站(social)、簡訊服務(sms)以及其他傳統的服務(old school)等平台。

web spam

social

sms

old school

在報告中僅針對「垃圾郵件」方面進行探討，並把「垃圾郵件」視為商業廣告的一種形式，不考慮以網路釣魚、惡意軟體或其他詐騙性質的電子郵件，此類性質的電子郵件約佔整體「不合法的電子郵件(不請自來)」數量的 1%。

網路上的商業宣傳行為，可區分為符合規範的商業廣告與被定義為「垃圾郵件」的不請自來之商業電子郵件，兩者的差異如下：

1. 同樣都會提供完整明確的商品內容，但是「垃圾郵件」很有可能與實際商品不符，形同對消費者進行詐欺行為。
2. 兩者行為都屬於營利性質，但「垃圾郵件」會影響其他符合規範之商家所提供商品服務的合理利潤。
3. 兩者提供消費者資訊的機制不同，符合規範的商業行為被動的由消費者依據自身需求，決定是否接收廣告訊息，「垃圾郵件」則是不在乎消費的需求為何，主動且帶有強迫意味的讓消費者接收廣告訊息。
4. 合乎規範的商業廣告，其主要強調其商品本身帶給消費者的價值，例如強調所銷售的軟體具有之強大功能來吸引消費者，而「垃圾郵件」著重商品以外

的其他價值，例如以一套軟體的價格，可同時取得一系列的眾多軟體等誘導消費者。

在本篇報告中，關注下列問題：

1. 垃圾郵件發送者可以賺取多少利潤？
2. 因「垃圾郵件」著重的商品外其他價值，對個人和企業造成多大的影響？
3. 網際網路使用者因「垃圾郵件」而增加多少無形的成本？
4. 「垃圾郵件」的市場結構為何？
5. 「垃圾郵件」專業化到何種程度？
6. 公權力介入「垃圾郵件」的政策面為何？
7. 公權力介入「垃圾郵件」的法律面為何？
8. 公權力介入「垃圾郵件」的經濟與技術面為何？

將「垃圾郵件」與「市場經濟」作為議題並一同探討之。

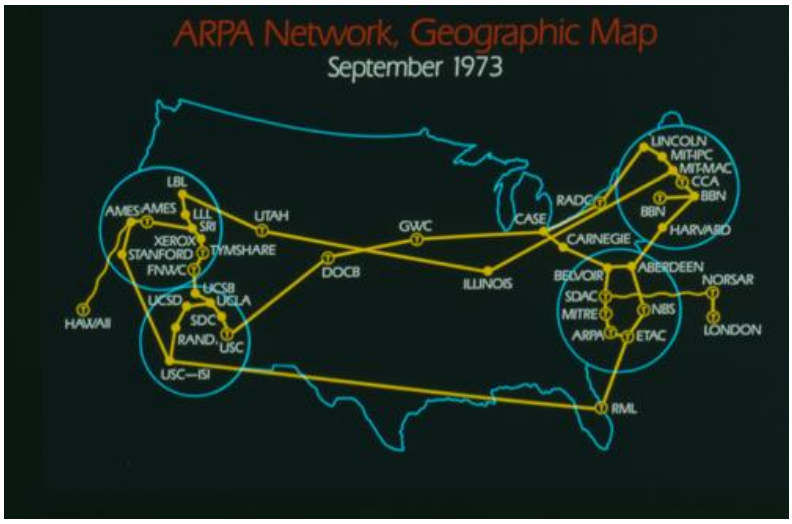
一、 垃圾郵件的商業生態系統

假設我們今天提問，「垃圾郵件」是不好的嗎？「竊盜」是令人厭惡的嗎？對我們大多數的人來說是肯定的回答「是」，然而並非全部的人都是肯定的，事實上對某些人來說是否定的，諸如下列：

如果你所經營的公司與保全、門鎖相關，則「竊盜」或許就不是你所厭惡的，公司主打這些「竊賊」，但是間接的從這些「竊賊」中獲得利潤，甚至可以說，因為這些「竊賊」的存在，才使公司得以維繫，形成「竊賊」與「防盜」兩者間競爭的市場機制，同理，此市場機制亦可套用在對使用者的電子郵件信箱保護上，競爭的對象換成了「垃圾郵件」濫發者。

二、 貓與老鼠

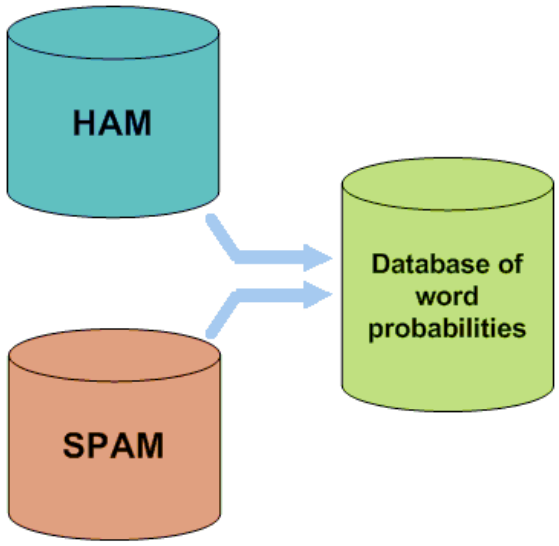
我們可以大膽的斷言，「垃圾郵件」市場是由成熟的專業濫發者和反「垃圾郵件」服務提供者之間持續以「貓捉老鼠」型態存在的遊戲；電子郵件是以SMTP(Simple Mail Transport Protocol)通訊協定進行傳輸，標準埠號為 25(Port 25)，該協定定義用戶端(Client)與郵件伺服器(Mail Server)以及郵件伺服器與郵件伺服器之間的通訊，為上世紀 80 年代所制定，信任層級設定為「高」等級，這是因為在 80 年代「美好時光」的背景下所定義，在當時寄送電子郵件有如傳統上由郵差送信般的單純。



由於電子郵件屬於相對免費性質，不需要附上郵資且便捷迅速，很快的在1995 年出現了第一個商業電子郵件濫發軟體，軟體名稱叫「Floodgate」，且開始為有心人士所利用，並開始出現被稱為「垃圾郵件之王」的固定大量濫發源，其「垃圾郵件」充斥在使用者的開放式中繼上，所謂開放式中繼意指任何人皆可利用此部主機的 SMTP 服務將郵件寄到目的地，也就是任何人的主機都有可能成為「垃圾郵件」寄送的跳板伺服器，為避免成為跳板，解決方式有兩種：

1. 透過認證機制，不接受要求開放中繼的訊息。
2. 經由機器學習、檢測、攔截步驟。

使用字詞機率資料庫(Database Of Word Probabilities)的方式來過濾「非垃圾郵件」與「垃圾郵件」。

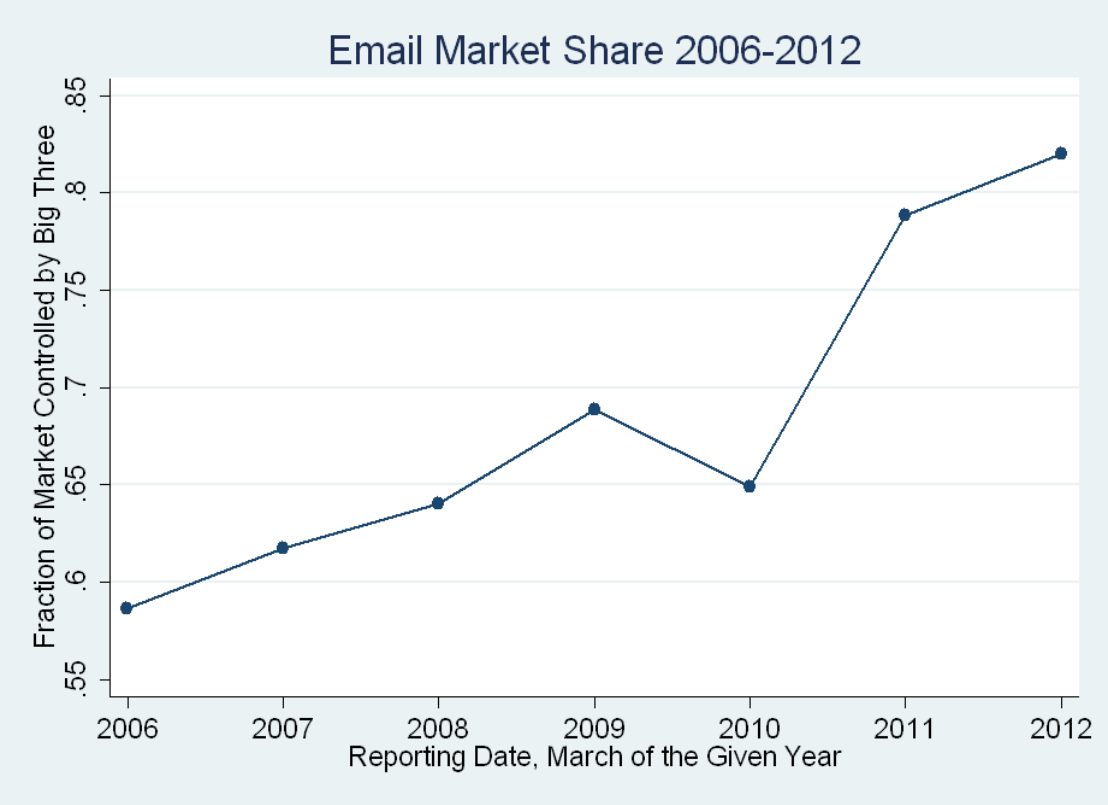


此過濾方式是利用字詞出現的機率演算法，利用統計技術來計算並推定是否為「垃圾郵件」，著名的方式如「貝葉斯郵件過濾(Bayesian Spam Filtering)」，過濾器事先並不知道出現在合法郵件中字詞的機率，必須經過「訓練」加以建立。

監督式學習(Supervised Learning 或稱 Machine Learning 101)為「機器學習」中的一種訓練方法，藉由資料中學到或建立一個學習模式(learning model)，

並依此模式推測新的實例，換句話說，就是利用「實際狀況」和「訓練資料」找出並建立「規則」，反覆進行之，再利用「規則」與「使用者輸入」形成「群眾外包(Crowdsourced)」機制，所謂「群眾外包」為一種新的商業模式，即企業利用網際網路來將工作「發包」，使用網際網路的群眾可根據本身技能，自願性的承接工作，發揮創意或解決技術問題，並獲取小額報酬，亦可視為一種組織勞動力的全新方式；藉由「群眾外包」不斷的回饋「垃圾郵件」與「非垃圾郵件」的判定資訊，即可形成準確性高的「垃圾郵件」過濾器，由於「群眾外包」的判定資訊不間斷的進行，故可隨時更新「垃圾郵件」過濾器。

下圖為個人電子郵件集中率的年度統計：

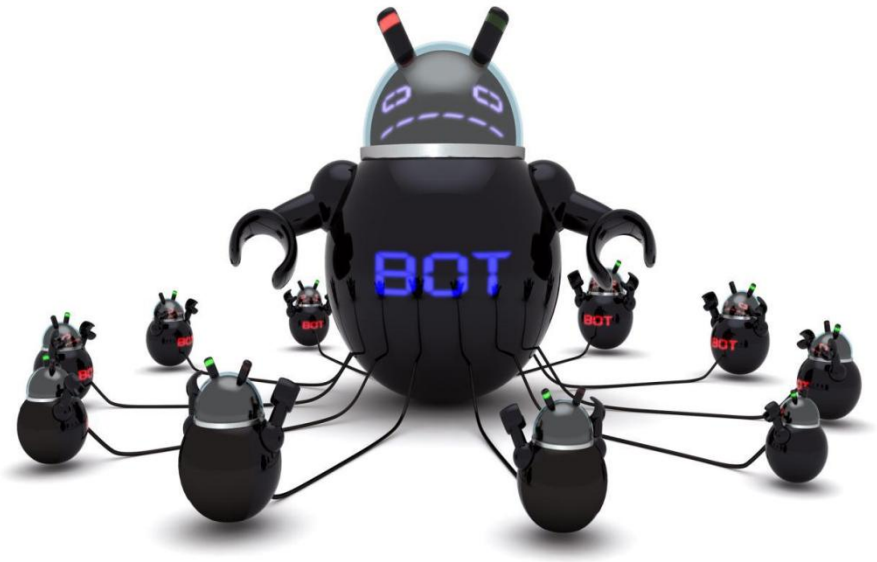


其橫軸為年度(西元)，區間為 2006 年至 2012 年，縱軸為商業電子郵件集中在前三大提供網路郵件服務的企業(商業電子郵件排行)比率，除了 2010 年稍有降低外，從 2006 年的不到 60%躍升到 2012 年的超過 80%

「垃圾郵件」是如何配送的？由於當時發展 SMTP 通訊協定的環境單純，因

此 SMTP 有太過於信任使用者的弱點，使得在早期「垃圾郵件發送者」利用此弱點進行大量發送，為了反制，採取了「黑名單」機制，網際網路所使用的通訊協定為 TCP/IP(Transmission Control Protocol/Internet Protocol)，因 TCP 協定無法偽造 IP 位址，所以可利用「垃圾郵件過濾器」、IP 位址以及共享資訊來建立「黑名單」藉以防堵「垃圾郵件」，這也使得「共享 IP」變成不是一個好的使用方式，因為只要其中一個虛擬 IP 用戶大量濫發「垃圾郵件」，就會因為實體 IP 被列入「黑名單」而讓所有的虛擬 IP 用戶均被封鎖，但是如果大部分的虛擬 IP 都在執行濫發的任務，反而也使得「垃圾郵件」過濾的效果更好；舉例來說，Spamhaus 即是一個跨國且非營利性質的反垃圾郵件組織，其網站 pamhaus.org 定期更新並公佈「垃圾郵件」濫發源的黑名單的相關共享資訊，作為進一步防制「垃圾郵件」的重要參考資料。

「垃圾郵件濫發者」為了因應「黑名單」機制，採用「殭屍網路(Botnet)」作為濫發「垃圾郵件」的手段，「殭屍網路」崛起於 2003 年。



「殭屍網路」主要透過散佈惡意軟體(Malware)的方式來達成，使用者通常

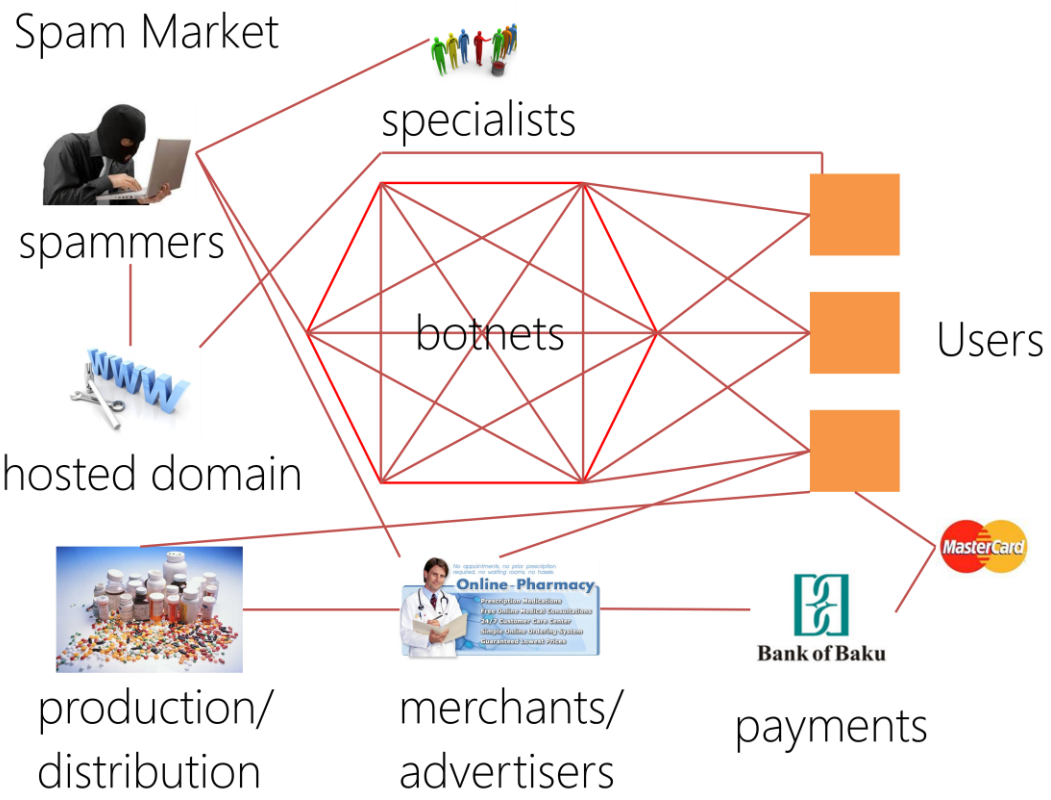
在不知情的情況下遭到植入，例如點選不知名超連結、檔案等，使得使用者的電腦遭遠端有心人士所操控，俗稱「殭屍電腦」，一群「殭屍電腦」所形成的網路，即俗稱「殭屍網路」，可被利用來大量濫發「垃圾郵件」，此方式不但成本低廉，而且具備「可移動」性，一旦某部「殭屍電腦」被查獲封鎖，可立刻轉移到下一部「殭屍電腦」繼續濫發，有高達 85%受感染的「殭屍電腦」濫發「垃圾郵件」超過一整天之後才被發現，而一般電腦主機取得 IP 上網所使用的為 DHCP(Dynamic Host Configuration Protocol；動態主機配置協定)通訊協定，自動將 IP 指派給登入 TCP/IP 協定的網際網路主機，由於是動態的，每日登入後所獲得的 IP 位址皆不固定，因此當原濫發的 IP 被發現後，隔天該部「殭屍電腦」又被配發新的 IP 位址，同樣又遭利用來濫發「垃圾郵件」，因此對濫發者來說，這又是「新鮮的 IP」而加以濫用；一項根據 2009 年的資料統計，超過 90%的「垃圾郵件」由分佈全球的 6 個「殭屍網路」所濫發，其中一個名為 Rustock 的「殭屍網路」由 2006 年開始運作，每小時能從被感染的主機發送 25000 封「垃圾郵件」，直到 2011 年 3 月才由全球性的網路安全公司 FireEye、微軟(Microsoft)、美國華盛頓大學以及美國聯邦執法人員聯手瓦解，全球電子郵件流量即時下降了 35%，即使到了今日，其流量仍未上升到當時的水平。

為反制「殭屍網路」所濫發的「垃圾郵件」，有人提出了封鎖 25 通訊埠(Port 25)的方式，因為電子郵件採行的是 SMTP 通訊協定，標準通訊埠號為 25，但是即使封鎖了 25 通訊埠，仍無法阻止利用網頁郵件(webmail)所大量發送的「垃圾郵件」，因此在網頁郵件的發送介面，設有「文字輸入驗證」機制，以防止大量濫發。

然而，「垃圾郵件」需要靠大規模發送，接收者愈多愈好嗎？是的，答案是肯定的，一個組織良好的市場已經有如雨後春筍般的湧現，此類圖像文字的廣告寄送服務，市場中每千封電子郵件的寄送成本，從 2007 年的美金 7 元，在 2009 年下降到美金 1 元，到了 2012 年已經降到美金 0.7 元，其濫發源已經由東歐，漸漸轉移到發送成本較低廉的印度、中國和越南等地，同時濫發「垃圾郵件」在當地並不違法。

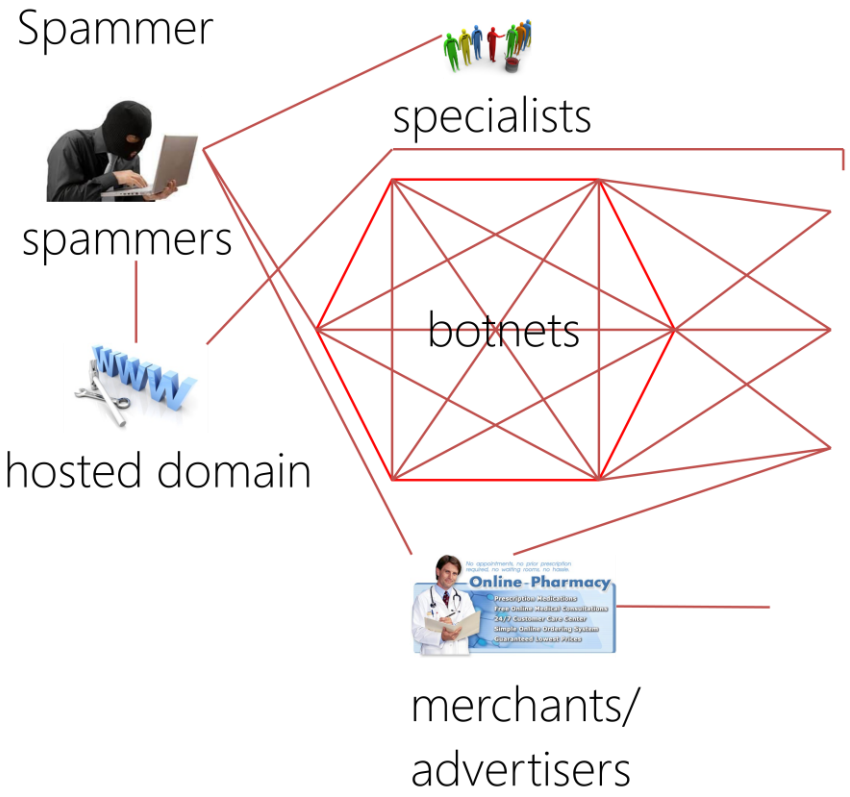
發送「垃圾郵件」到用戶信箱，其成功機率依序為：可信任網域的可信任帳戶、可信任網域的新帳戶、不知名網域的既有帳戶、不知名網域的新帳戶，由於資訊安全的漏洞導致帳戶遭劫持的情形不斷增加，因此垃圾郵件過濾器最好的做法是加入「白名單」

垃圾郵件市場經由拼湊之後，其全貌大致如下圖：



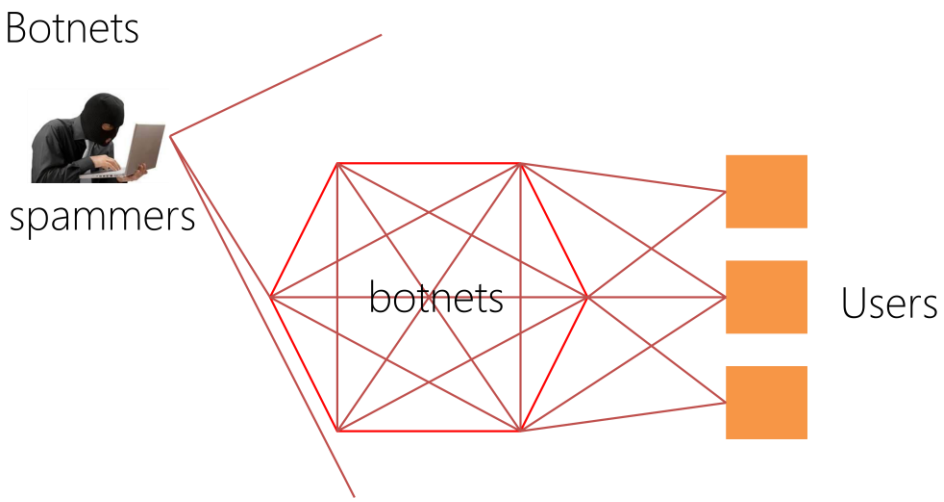
其全貌由下列結構所組成：

1. 垃圾郵件濫發源(Spammers)



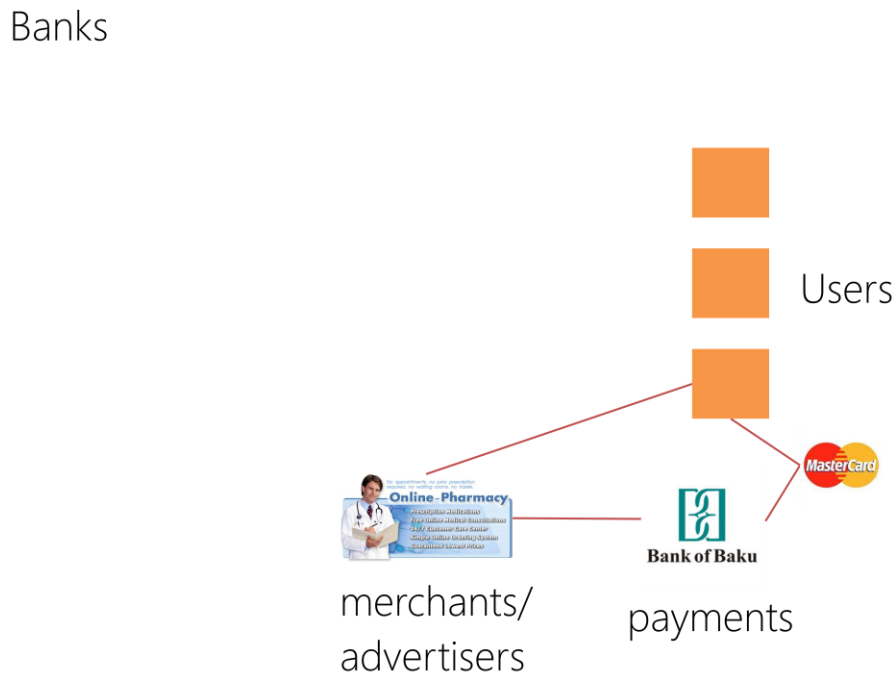
「垃圾郵件」濫發源在實際上是一個操控者的角色，「垃圾郵件濫發者(Spammers)」以網域代管(Hosted Domain)的方式架設商業網站，並且自行尋找商家合作，然而商家並無法直接與專家聯繫商討營運相關細節，僅能將商品或服務項目提供給「垃圾郵件濫發者」透過濫發者與專家聯繫，並操控所佈建之殭屍網路，進行大量的商業電子郵件發送。

2. 殭屍網路(Botnets)



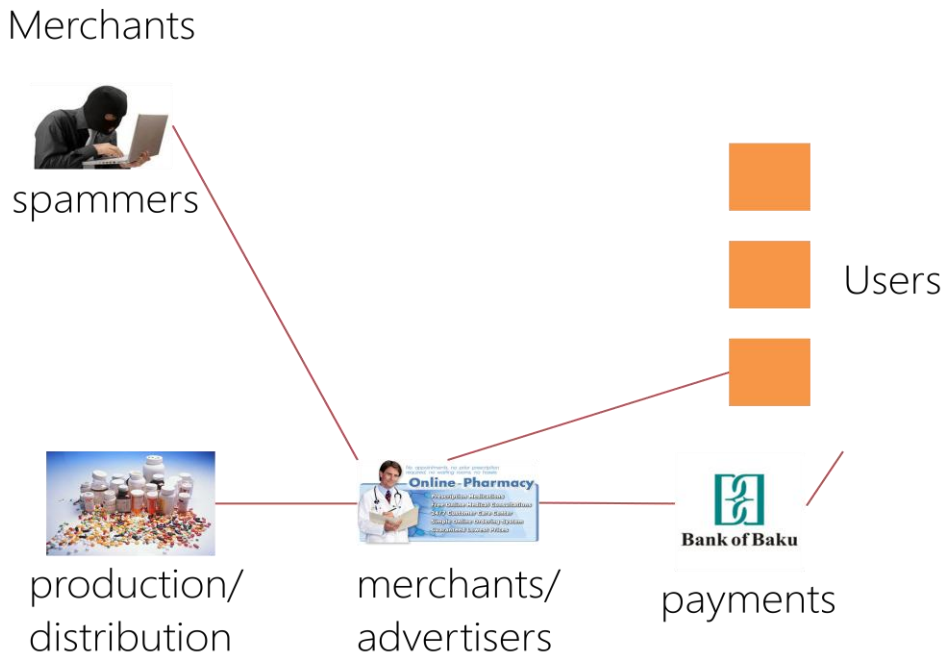
「垃圾郵件濫發者」藉由「殭屍網路」向網際網路使用者(Users)大量寄發「垃圾郵件」。

3. 支付系統(Banks)



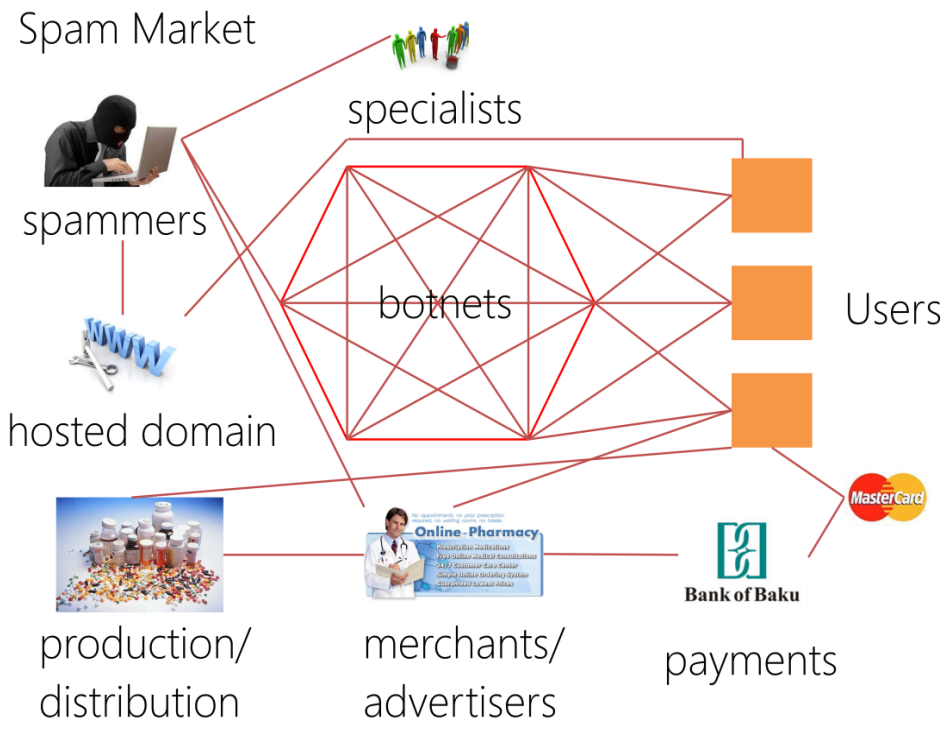
合作的銀行也是由「垃圾郵件濫發者」所指定，消費者透過第三方支付的方式消費，取得商品或服務。

4. 商業模式(Merchants)



其商業模式由商家製作或發行相關商品服務，在使用者消費購買後，分享利潤給「垃圾郵件濫發者」作為報酬。

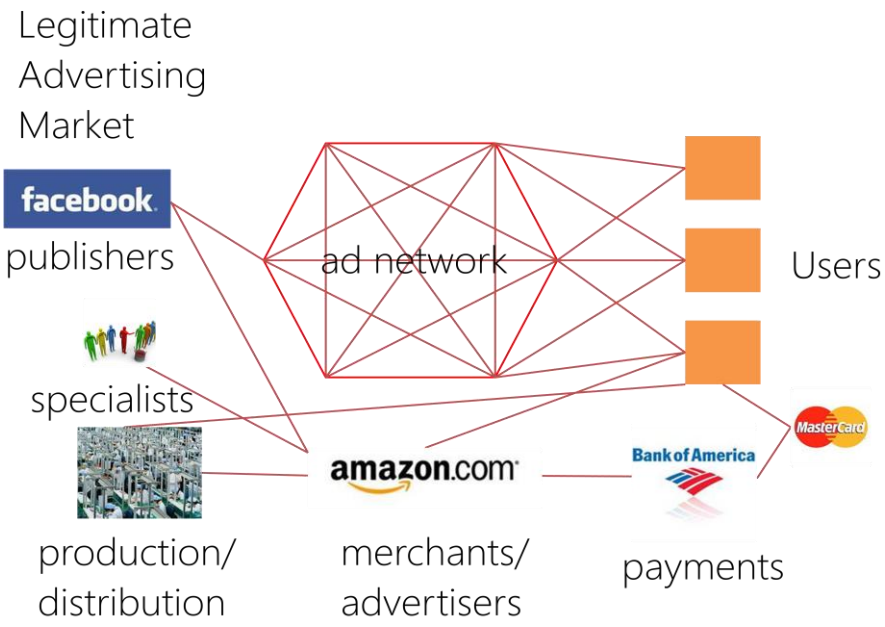
5. 「垃圾郵件」市場(Spam Market)



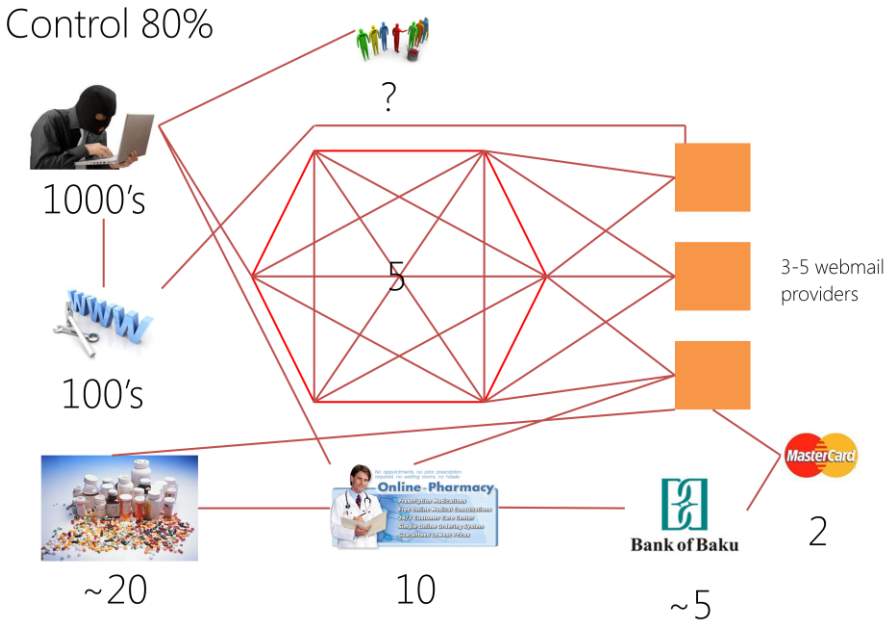
經過拼湊之後，推敲出「垃圾郵件」市場經濟的面貌，可以說是一個完

整的經濟結構。

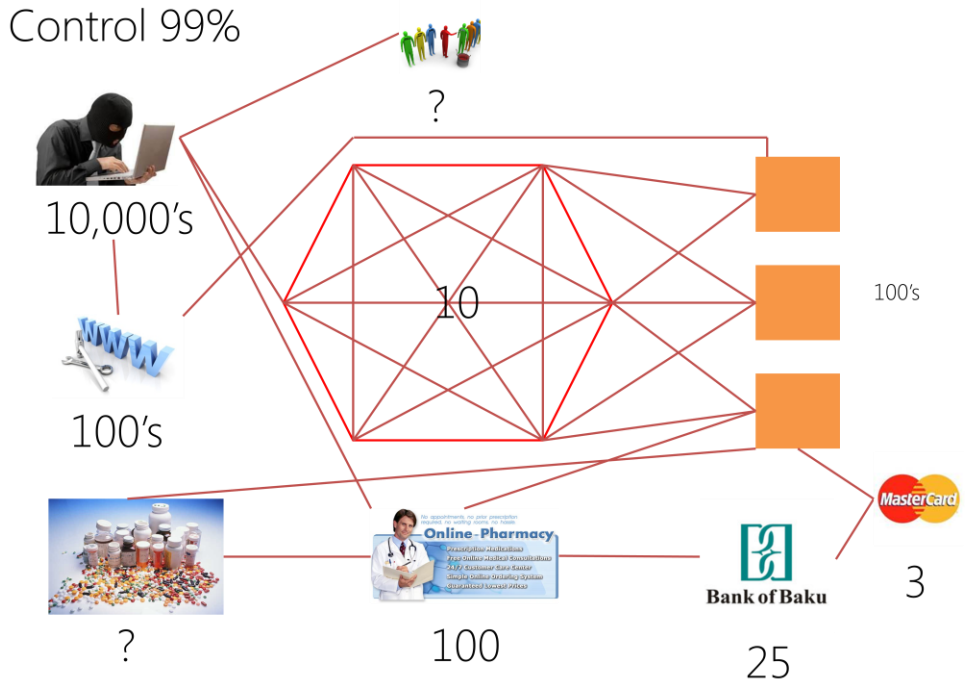
6. 「合法廣告」市場(Legitimate Advertising Market)



終端的使用者可以透過網路搜尋，或稱廣告網絡(ad network)，自主性的連結到相關社群網站(如 facebook)取得所需要的資訊，商家直接與專家和銀行接洽商業上的相關細節，而非前述的「垃圾郵件」市場般而需透過「垃圾郵件濫發者」主導，若消費者需要購買商品，同樣可透過第三方支付的方式消費，以取得所需要的商品或服務，為一種良性的互動關係。就如先前所提到，「垃圾郵件」很容易因過濾機制而被阻擋，因此僅有少數的「垃圾郵件」會順利到達網路使用者手中，就以下圖來說，假設有80%的「垃圾郵件」被過濾：



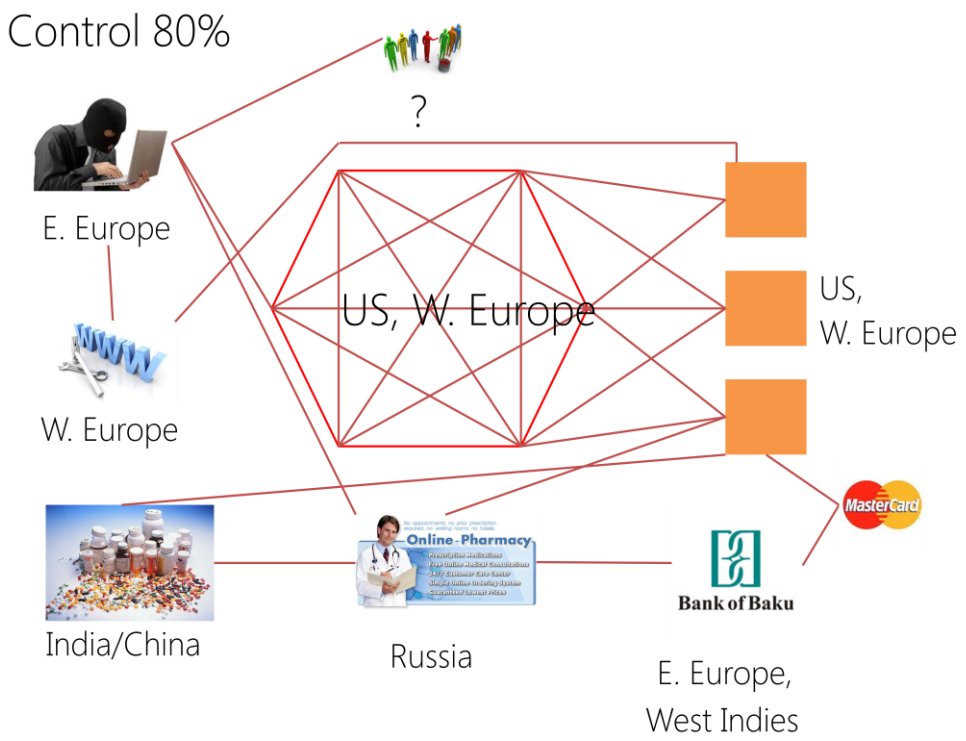
「垃圾郵件濫發者」假設操控所屬的 5 部殭屍電腦發送了 1000 封垃圾郵件，經過統計推測其中有 100 封「垃圾郵件」成功引導使用者連結到商業網站，因為風險較高，通常大約有只有 5 家銀行願意配合，在此數量下與濫發者合作的商家大約有 10 間，強迫推銷大約 20 項商品或服務。下圖為假設有 99%「垃圾郵件」被過濾的情況：



同理，假設有 10000 封「垃圾郵件」經由 10 部殭屍電腦被濫發，因為量

大，會有較多的銀行願意承擔些許風險合作，可能達到 25 家，與濫發者合作的商家可以到100家，至於可以推銷多少種商品？肯定很增加很多，但答案未知。

「垃圾郵件」的商業模式多為跨國組織：



舉例來說，操控殭屍網路的「垃圾郵件濫發者」藏在東歐，其網域設定於西歐，所操控的殭屍電腦位於美國和西歐，與東歐和西印度群島的銀行合作，商家選定在俄國，而商品在印度和中國行銷。

合法的商業廣告，其商品通常與品牌連結，而「垃圾郵件」所利用的「聯盟行銷」廣告通常會混淆商品與品牌的連結，因為其商品通常為仿冒商品，因此目的在刻意讓使用者混淆引誘消費。

根據監視殭屍網路活動的研究，在一份 2011 年由 Levchenko 等人追蹤 45 個與濫發者合作的商家進行研究的統計數據，其中光是藥品相關商業廣告的郵件，就有高達 3.5 億個不同的單一網址進行發送，其所屬的網域有 5.4 萬個，同時每一種藥品的商家通常會設計多個不同的「店面風格

(Store-front styles)」，用來混淆並吸引使用者消費，然而消費者並不知道商品皆來自同一店家，其數量據統計有 968 個，也就是說這 45 個商家在藥品的行銷上，提供單一用戶 968 個不同風格的介面連結，而 45 個商家中，與藥品相關的產品佔 30 家，其餘的軟體 5 家、仿冒品 10 家。

Table 1

Breakdown of the Spam Supply Chain

Stage	*Pharmacy*	*Software*	*Replicas*	*Total*
Unique URLs	346,993,046	3,071,828	15,330,404	365,395,278
Domains	54,220	7,252	7,530	69,002
Store-front styles	968	51	20	1,039
Merchants	30	5	10	45

Source: From a study of 45 merchants tracked by Levchenko et al. (2011).

「垃圾郵件」屬於規模效益(Economies of scale)性質，即隨著郵件濫發數量的增加，平均成本可不斷下降，其中「垃圾郵件過濾器」為其所面對的固定成本，其他如服務控制器、網路郵件、殭屍網路等，均屬於規模效益，但整體來說，雖然「垃圾郵件濫發者」可以自由進出已經註冊網域名稱和租用網路服務的殭屍網路，但畢竟為非法活動而存在著整體供應鏈中斷的風險，因此只有少數銀行願意承擔相關支付風險，即使有銀行願意合作，合作的商家所要付出的固定成本必定增加，然而，「垃圾郵件濫發者」到底可以從中獲取多少利潤呢？

假設「垃圾郵件濫發者」發送 10,000,000 封郵件，扣除因無法傳送而被退回的有 8,000,000 封，剩餘 2,000,000 封成功傳送，然而，再扣除被過濾掉的 1,850,000 封、被忽略直接刪除的 149,625 封，實際上會被點擊瀏覽的大約僅有 375 封，但是與其他方式的商業廣告比起來，以「垃圾郵件」的廣告方式，每曝光 1000 次所需要的成本(CPM)僅約美金 0.03 元。

Media	CPM	Conversions per 100,000 to break-even with MP=$50*
US Mail	$250-1000	500-2,000
Primetime TV	$20	50
Online Display	$1-5	2-10
Spam	$0.03	0.06

我們根據下列的參考資料估計「垃圾郵件」市場的銷售和收入總額：

Temporally Separated Orders (“accounting attacks”): Levchenko et al. (2011), Savage et al. (2011), Kanich et al. (2008)

botnet/market infiltration: Stone-Gross et al. (2011), Motoyama et al. (2011)

botnet monitoring: Symantec 2011, John et al. 2009/2011

“found data”: McCoy et al. (2012)

大約介於 1.8 億美元到 3.6 億美元之間。

GlavMed、SpamIt 和 RX-Promotion 為最知名且惡名昭彰的供應鏈代表，皆來自俄羅斯，提供「垃圾郵件」樣板、網址、網站設計、付費機制、產品接單、客戶支援等服務，再利用「垃圾郵件濫發者」操控殭屍網路大量發送「垃圾郵件」宣傳自行接單架設的藥品(非法)網站，並且「垃圾郵件濫發者」可取得不法獲利的 40%作為酬勞，自 2007 年至 2010 年底止，每週銷售量的統計圖如下(以千為單位)：

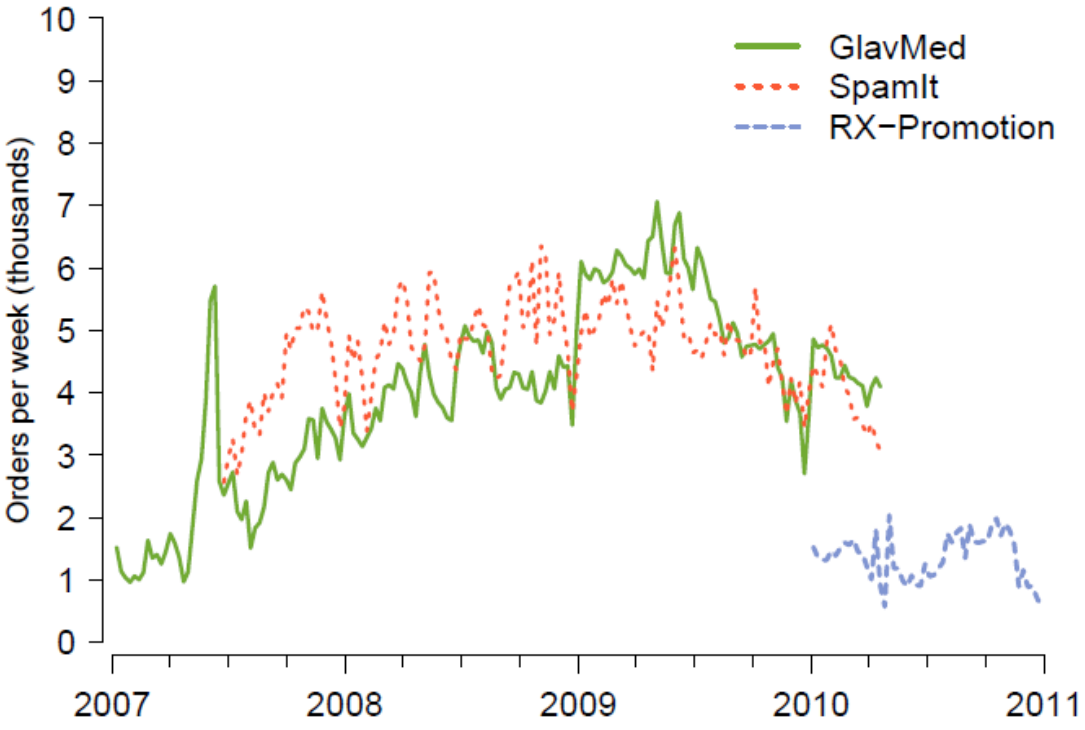
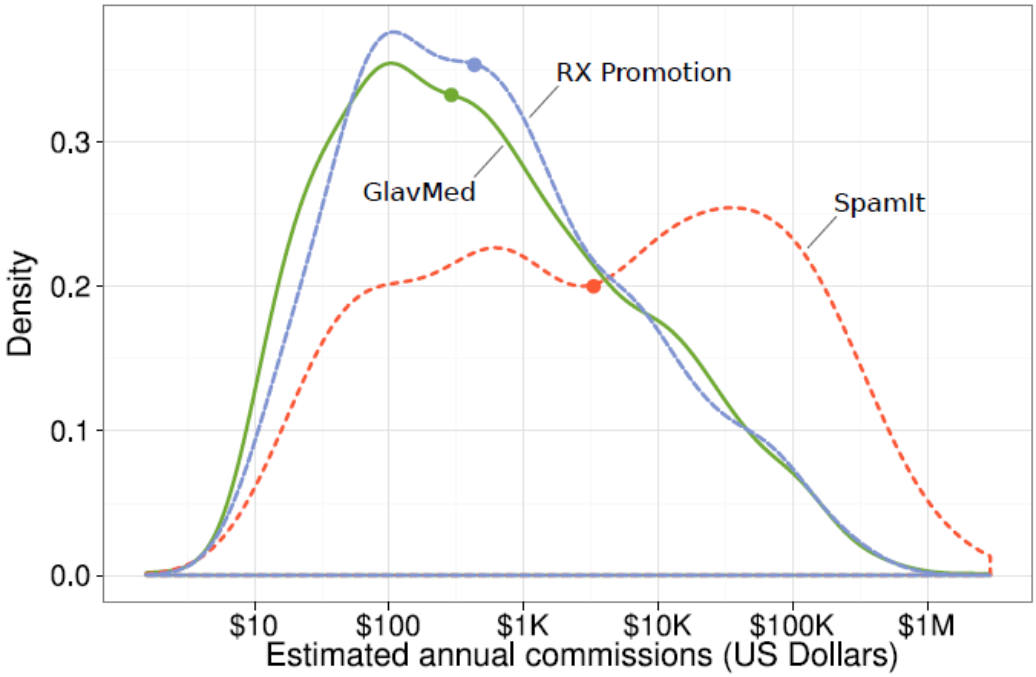


Figure 1: Weekly sales volume for each of the programs.

而「垃圾郵件濫發者」的收入分佈如下圖，橫軸為全年度佣金的估計，以美金為單位，縱軸是「垃圾郵件濫發者」的分佈密度。



在此我們所估計的收入，並非單指從事「垃圾郵件」行為所獲得的利潤，而是指由「垃圾郵件」效應所產生的總盈餘，然而，消費者大多不希望透過「垃圾郵件」購買商品，而是希望透過自己的意願上網搜尋商品，因此我們可以假設消費者的「獲利」遠低於「垃圾郵件」效應所產生的總收入，「垃圾郵件」將成本轉嫁給個人使用者或企業。

對個人使用者而言，大量的「垃圾郵件」造成電子郵件信箱塞爆無法收信導致重要訊息流失，或者因大量塞滿的郵件影響導致誤刪或疏忽重要郵件，此皆為個人使用者可能付出的隱形成本，在此我們不考慮帳戶入侵、帳戶轉換、帳戶挾持、窘困帳戶等成本。

我們利用下列參數來估計在美國每年因「垃圾郵件」加諸在個人使用者上造成的成本損失：

1. 總「垃圾郵件」量。
2. 通過「垃圾郵件」過濾器成功到達用戶端的比率(%)

3. 「垃圾郵件」過濾器的設定方式

5. 使用者平均花費在篩選上的時間成本

6. 實際上的時間損耗

據此我們估計美國在 2010 年,每天的「垃圾郵件」總量大約是 700 億封，其中有 1.2%的「垃圾郵件」通過過濾器到達用戶端，假設處理每封「垃圾郵件」所需的時間為 5 秒，以時薪 25 美元計算,「垃圾郵件」造成的個人用戶成本損失大約為 60 到 120 億美元之間。

對公司(法人)而言，付出的成本為購買並安裝反「垃圾郵件」軟體、伺服器的頻寬下降影響服務品質、員工刪除大量「垃圾郵件」耗費的時間等隱形成本，在此我們不考慮因「垃圾郵件」改變商業模式，而流失的廣告機會成本。

我們利用下列參數來估計每年因「垃圾郵件」加諸在公司(法人)上所造成的損失：

1. 支援第三方支付的相關服務支出

2. 硬體設備的支出

3. 員工在處理「垃圾郵件」所花費的時間

據估計，第三方支付服務支出成本約 50 億美元，硬體設備方面的支出少於 10 億美元，員工花費在處理「垃圾郵件」所花費的成本已納入個人使用者估算，不重覆併計。

因此，整理所得到的數據如下：

公司(法人)所浪費的成本約 60 億美元。

個人用戶所浪費的成本約 60 至 120 億美元之間。

因此「垃圾郵件」在美國帶給最終用戶端將近 200 億美元的成本，同樣是用戶端，產生這些「垃圾郵件」的最終用戶端因發送「垃圾郵件」每年賺取 2 億美元的獲利，所付出的社會成本相對於私人利益的比值，大

約是 100：1 左右，而我們可以做一個對照：

駕駛汽車產生的空氣汙染，其社會成本比值為 0.03 至 0.41 之間。

竊取汽車的行為，其社會成本比值為 6.7 至 30.3 之間。

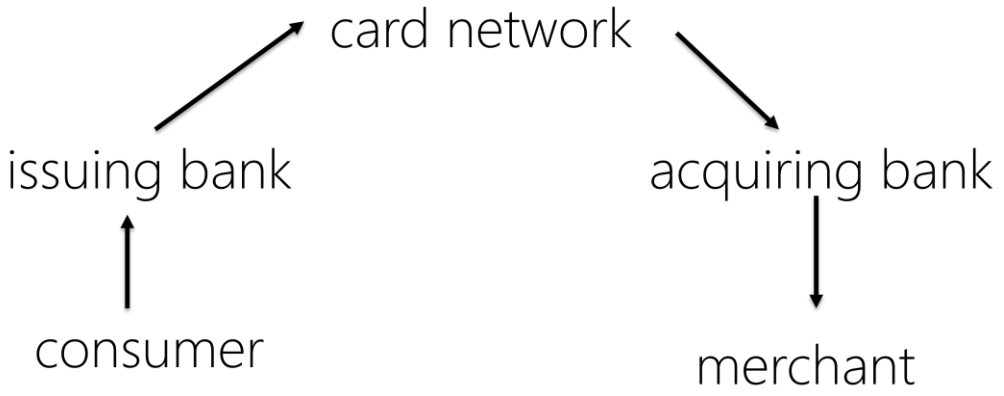
暴力手段搶劫的行為，其社會成本比值超過 1000 以上。

「垃圾郵件」屬於一個較為極端的比值，然而實際上「垃圾郵件」的行為卻也沒有偷竊、搶劫那麼糟糕。

三、政策與公權力介入干預

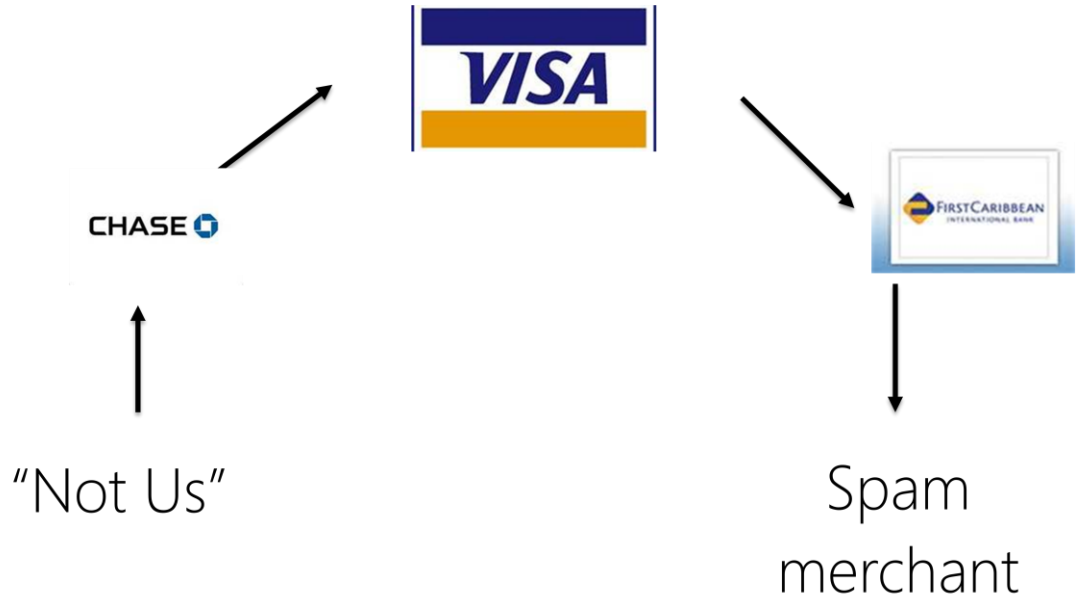
大多數的「垃圾郵件」規範是根據美國在 2003 年制定的 CAN-SPAM 法，要求這些不請自來的非法電子郵件必須有退出條款和有效的退訂位址，然而 SMTP 通訊協定屬於發送者的財產權，任何人都有權利發送電子郵件。

第三方支付服務的流程如下：



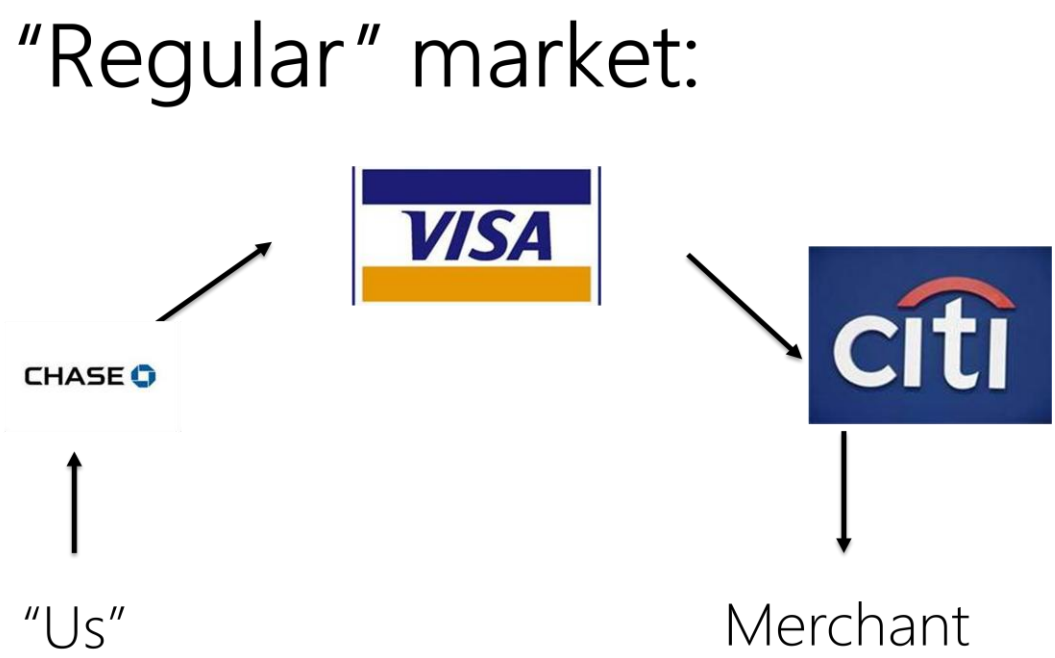
由消費者支付費用給信用卡發卡銀行(issuing bank)，發卡銀行透過發卡公司(card network)將費用轉給收款銀行(acquiring bank)，收款銀行再將費用支付給合作商家(merchant)。

以「垃圾郵件」消費的支付模式如下：

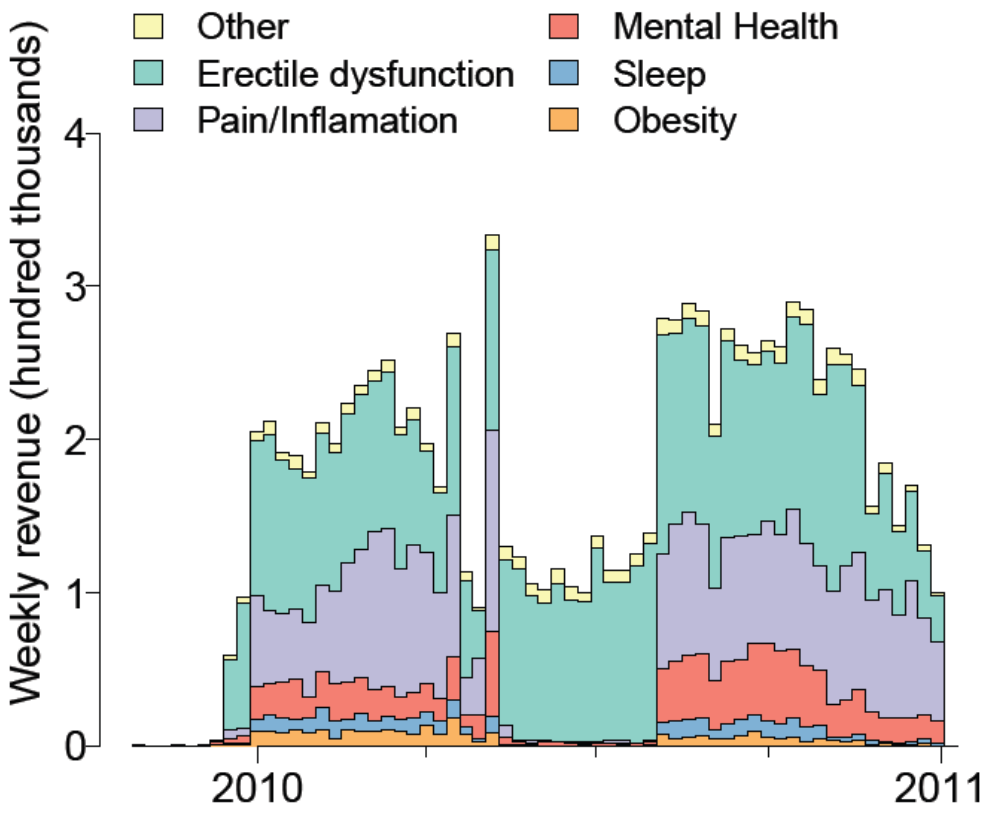


付款方式並不在乎消費者身分，最終的付款並不一定是流向商家，而是背後的「垃圾郵件濫發者」。

「合法」消費的支付模式如下：



付款方式必需先確認消費者身分，最終的付款流向為提供商品服務的商家。以信用卡號碼(Merchant Category Codes)的交易方式中，商家支付類別代碼 5912 開頭者代表醫藥類別，在 2010 年至 2011 年一整年當中，影響每週支付處理的藥品類別統計圖如下：



四、結論

因為電子郵件發送成本低廉，且便捷快速，但也因為「如果你蓋了，他們會來」的緣故，從早期由數個著名的大量濫發者(俗稱 spam kings；垃圾郵件之王)個別獨立進行大量濫發，演進到現今頗具規模的市場結構，並展現了高度的專業化，改變了市場中商品服務的成本結構，且每年的「垃圾郵件」輸出量高達 50 兆封的規模，其中大部分由大型服務供應商所過濾，而相對之下，這些個人「垃圾郵件」濫發者所造成他人網路權益的影響，遠比其背後所造成的經濟影響來的小，此問題在目前並沒有萬靈丹，只有從不同層面思考的政策角度，並吸引眾多專家學者探討；此外，合作濫發商業電子郵件的商家，相對上數量稀少，若法案的設計方向是針對這些商家規制，則是否能有效解決「垃圾郵件」問題？

議題三、防範垃圾郵件的新方式

一、是否為垃圾郵件？

根據調查，有 91%的針對性攻擊，屬於「魚叉式網路釣魚」類型的電子郵件，魚叉式網路釣魚為一種只針對特定目標進行攻擊的網路釣魚手法，當進行攻擊的駭客鎖定目標後，會以電子郵件的方式，假冒該公司或組織的名義發送幾可亂真之檔案，誘使員工進一步登錄其帳號密碼，使攻擊者藉機安裝惡意軟體，竊取具備價值之機密，這不禁讓人思考，此為一種商業行為？或者是想擁有你的東西？

網路釣魚至今仍是消費者在網路最大的威脅，以下數據可以說明之：

1. 高達 90%的網路用戶曾遇到網路釣魚。
2. 每日約有 10 萬個帳戶被盜取。
3. 利用「美國聯邦政府」名義的詐騙率，在最高峰時約有 30%。
4. 「魚叉式網路釣魚」的發生率與防範的成本節節上升。
5. 有 91%的針對性攻擊，屬於「魚叉式網路釣魚」類型的電子郵件方式。

這將造成網路使用者對於「網路」失去「信賴感」，而使網路活動的相關資源日益減少，違背了「網路」建設與發展的初衷。

二、防範垃圾郵件的老方法

防範垃圾郵件的一般方式，不外乎下列數種：

1. BCP38 過濾機制，即使用來源 IP 驗證技術過濾電子郵件。

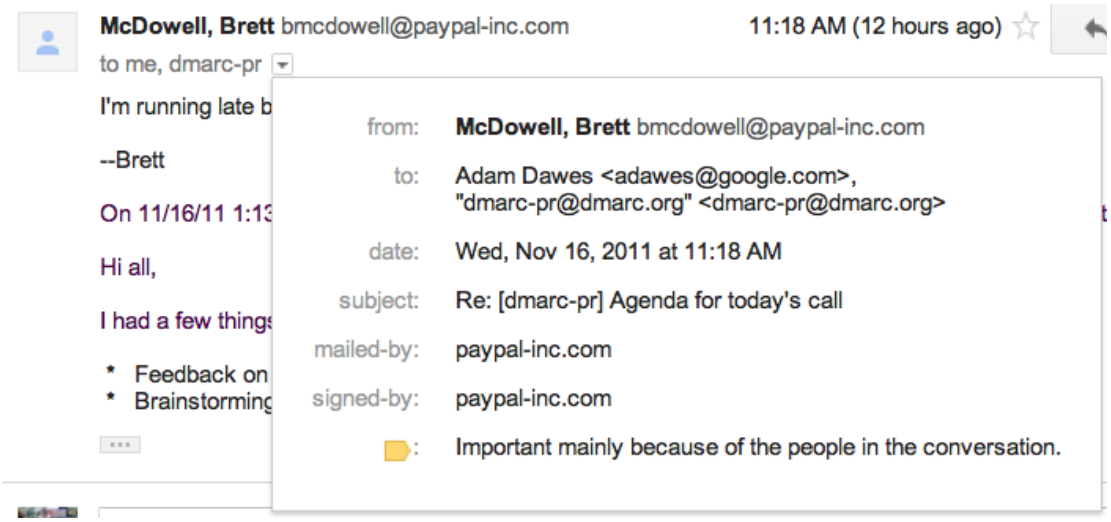
2. 不使用電子郵件傳遞訊息。
3. 阻擋 SMTP 通訊協定，即關閉 25 通訊埠(port 25)。
4. 參考「黑名單」列表(例如 Spamhaus)，設定過濾列表中之來源郵件。
5. 使用「反向解析(rDNS)」工具驗證電子郵件之寄件人。
6. 關鍵字過濾，例如設定電子郵件若內含「免費」字眼即自動刪除。
7. 利用機器學習資料庫搭配的貝氏規則過濾，或是以是否「見過」為過濾規則的「指紋辨識」機制。
8. 使用 SPF/DKIM 郵件認證機制。
9. 將電子郵件中所包含的網址「去除」。

三、何謂 DMARC？

DMARC 為一種反垃圾郵件的通訊協定，全名為 Domain-based Message Authentication Reporting and Conformance，在 2012 年 1 月 30 日有 Google、Microsoft、Yahoo、Facebook、AOL、PayPal、Linkedin 等 15 家知名企業宣布加入 DMARC 組織，以解決垃圾郵件與釣魚郵件為目的。

由於 SMTP 通訊協定並無收發電子郵件可信賴的溝通方式，因而無從判斷郵件服務的真實性，DMARC 協定即是讓收發郵件的雙方，建立可信賴的溝通管道，遇到可疑郵件時，不必以猜測的方式處理，可有效防止垃圾郵件進入信箱。

下圖為經過 DMARC 驗證機制的電子郵件：

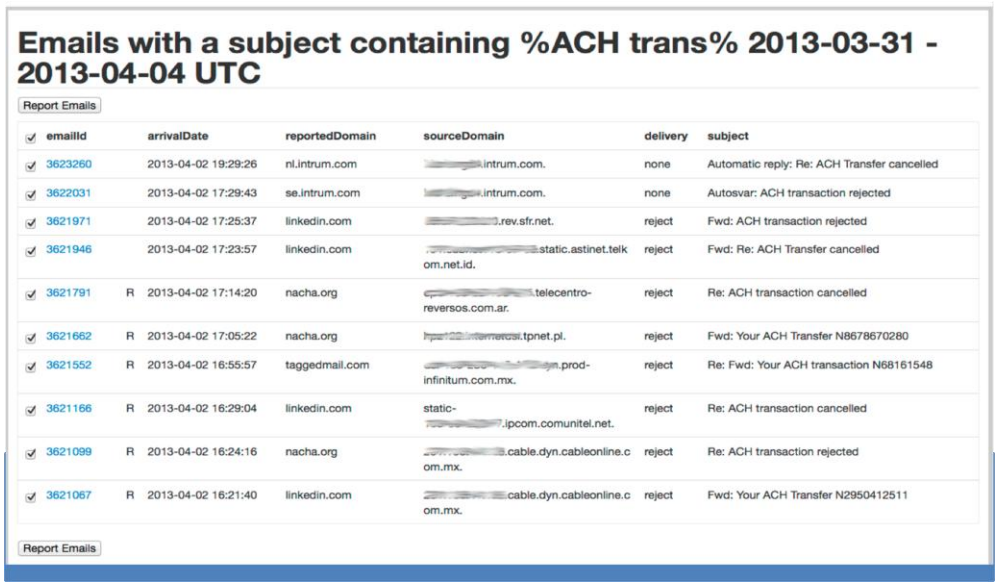


目前全世界有 60%的電子郵件信箱由 DMARC 協定保護，在美國則有 80%，而根據網際網路服務業者的觀察發現，DMARC 協定未成功檢查出的垃圾郵件，有高達一半以上的機率其他驗證機制同樣檢測不出。

無法通過 DMARC 驗證機制的電子郵件可能類型如下：

1. 詐騙性質的電子郵件，例如垃圾郵件、網路釣魚、惡意軟體等。
2. 寄件人忘記簽署 DKIM 或登錄 SPF Helo 主機名稱等。
3. 設定為自動回覆的電子郵件。
4. 設為自動轉寄的電子郵件。

由 DMARC 機制攔截的電子郵件，如經確認為詐騙性質的垃圾郵件，透過網站 https://github.com/linkedin/lafayette 回報，下圖是回報結果之查詢：



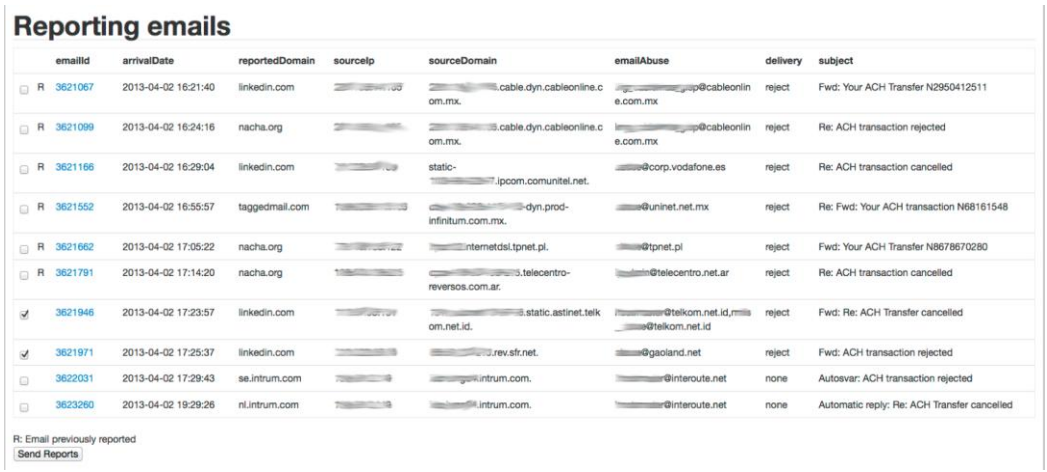
Emails with a subject containing %ACH trans% 2013-03-31 - 2013-04-04 UTC

Report Emails

	emailId		arrivalDate	reportedDomain	sourceDomain	delivery	subject
☑	3623260		2013-04-02 19:29:26	nl.intrum.com	.intrum.com.	none	Automatic reply: Re: ACH Transfer cancelled
☑	3622031		2013-04-02 17:29:43	se.intrum.com	.intrum.com.	none	Autosvar: ACH transaction rejected
☑	3621971		2013-04-02 17:25:37	linkedin.com	.rev.sfr.net.	reject	Fwd: ACH transaction rejected
☑	3621946		2013-04-02 17:23:57	linkedin.com	.static.astinet.telkom.net.id.	reject	Fwd: Re: ACH Transfer cancelled
☑	3621791	R	2013-04-02 17:14:20	nacha.org	.telecentro-reversos.com.ar.	reject	Re: ACH transaction cancelled
☑	3621662	R	2013-04-02 17:05:22	nacha.org	.tpnet.pl.	reject	Fwd: Your ACH Transfer N8678670280
☑	3621552	R	2013-04-02 16:55:57	taggedmail.com	.prod-infinitum.com.mx.	reject	Re: Fwd: Your ACH transaction N68161548
☑	3621166	R	2013-04-02 16:29:04	linkedin.com	static-.ipcom.comunitel.net.	reject	Re: ACH transaction cancelled
☑	3621099	R	2013-04-02 16:24:16	nacha.org	.cable.dyn.cableonline.com.mx.	reject	Re: ACH transaction rejected
☑	3621067	R	2013-04-02 16:21:40	linkedin.com	.cable.dyn.cableonline.com.mx.	reject	Fwd: Your ACH Transfer N2950412511

Report Emails

送出回報之前，系統會再次進行確認：



Reporting emails

		emailId	arrivalDate	reportedDomain	sourceIp	sourceDomain	emailAbuse	delivery	subject
☐	R	3621067	2013-04-02 16:21:40	linkedin.com		.cable.dyn.cableonline.com.mx.	@cableonline.com.mx	reject	Fwd: Your ACH Transfer N2950412511
☐	R	3621099	2013-04-02 16:24:16	nacha.org		.cable.dyn.cableonline.com.mx.	@cableonline.com.mx	reject	Re: ACH transaction rejected
☐	R	3621166	2013-04-02 16:29:04	linkedin.com		static-.ipcom.comunitel.net.	@corp.vodafone.es	reject	Re: ACH transaction cancelled
☐	R	3621552	2013-04-02 16:55:57	taggedmail.com		-dyn.prod-infinitum.com.mx.	@uninet.net.mx	reject	Re: Fwd: Your ACH transaction N68161548
☐	R	3621662	2013-04-02 17:05:22	nacha.org		nternetdsl.tpnet.pl.	@tpnet.pl	reject	Fwd: Your ACH Transfer N8678670280
☐	R	3621791	2013-04-02 17:14:20	nacha.org		.telecentro-reversos.com.ar.	@telecentro.net.ar	reject	Re: ACH transaction cancelled
☑		3621946	2013-04-02 17:23:57	linkedin.com		.static.astinet.telkom.net.id.	@telkom.net.id,@telkom.net.id	reject	Fwd: Re: ACH Transfer cancelled
☑		3621971	2013-04-02 17:25:37	linkedin.com		.rev.sfr.net.	@gaoland.net	reject	Fwd: ACH transaction rejected
☐		3622031	2013-04-02 17:29:43	se.intrum.com		.intrum.com.	@interoute.net	none	Autosvar: ACH transaction rejected
☐		3623260	2013-04-02 19:29:26	nl.intrum.com		.intrum.com.	@interoute.net	none	Automatic reply: Re: ACH Transfer cancelled

R: Email previously reported

Send Reports

下圖為全球垃圾郵件回報之熱區：

其中回報量愈大的地區顏色愈紅，無回報的地區則為綠色。

四、「網路詐騙」省思

儘管其他電子訊息技術不斷演進，但是電子郵件仍是最廣泛使用的既有溝通管道，但同時電子郵件也是一個容易讓使用者洩漏個資或遭植入惡意軟體的管道，為了保障用戶避免受到侵害與詐騙，郵件認證是最關鍵的環節，期望藉由 DMARC 協定將郵件收發雙方採取強而有力的認證措施與相關組織的合作努力，將損害的風險降到最低。

五、「倫敦行動計畫」的幫助

藉由聚會討論一同解決共同的問題，同時與「網路釣魚」對抗是為了保障每個網路使用者的隱私權，各會員之間可提供更多的「網路釣魚」相關數據，尤其網路並無國界之分，唯有國際間的協同合作、數據共享才能有效防範不肖人士濫用網路資源，健全網路使用環境。

議題四、網路詐財、手機網路監聽及詐欺-濫用支付系統的世界

加拿大行動市場之指標如下：

1. 截至 2013 年年中，加拿大總人口大約 3,500 萬，無線通訊系統用戶數將近 2,700 萬。
2. 約有 75%的加拿大家庭皆使用行動電話。
3. 在 2011 年，加拿大無線通訊業者營收總計約 191 億加幣。

全球應用程式(App)經濟規模預估如下：

1. 在 2012 年被下載的應用程式總數，比前五年的下載數的總和還多。
2. 在 2013 年有多達 820 億個應用程式可被下載，預估總收益可達 204 億美元。
3. 預估在 2017 年有多達 2,000 億個應用程式可被下載，總收益達 635 億美元。

加拿大競爭局(Competition Bureau Canada, http://www.CompetitionBureau.gc.ca)為一獨立行政之執法機構，目的在確保加拿大企業與消費者在創新且具競爭力的市場中能夠雙贏互惠，共生共榮。

競爭局負責管理並執行下列法律：

1. 競爭法。
2. 商品標示法(食品相關商品除外)。
3. 紡織標籤法。
4. 貴金屬刻記法

其中包含了刑法及民法之條文以解決因產品促銷、使用或為了商業利益而廣告不實、誤導或欺騙之行為，同時競爭局有多種工具及方法以因應各種形式之問題及具體事實。

一、國際合作

加拿大競爭局透過國際合作的方式，與其他國家相關單位合作對抗跨國性的反競爭行為，同時積極參與重要的國際會議如下：

1. 倫敦行動計畫暨訊息、惡意軟體及手機反濫用工作小組(LAP and M3AAWG)。
2. 國際大眾市場詐騙工作小組(IMMFWG；International Mass Marketing Fraud Working Group)。
3. 經濟合作暨發展組織(OECD；Organisation for Economic Co-Operation and Development)。
4. 國際消費者保護執行網(ICPEN；International Consumer Protection and Enforcement Network)。

其中競爭局正在參與國際消費者保護執行網發起之 2013 年度網路掃蕩行動，主要目標為兒童線上遊戲與應用程式之誤導行為及不當內容，舉例來說，一個七、八歲的小男孩試圖在 eBay 拍賣網站上購買戰鬥機：

http://www.nbcnews.com/technology/seven-year-old-boy-buys-fighter-jet-ebay-125224?franchiseSlug=technolog

或者是 11 歲的兒子在度假中觀看串流影片導致父親收到 2,2000 美元的數據漫遊帳單。

二、教育消費者

為了籌備並實施加拿大反垃圾郵件法規，加拿大與國內夥伴合作共同開發了消費者教育相關教材，共同參與者有加拿大廣播電信委員會、加拿大隱私政策委員辦公室以及加拿大工業部，詳情可參考網站：

http://www.FightSpam.gc.ca

三、利害關係者

以舉辦研討會和加強宣導等方式推動：

1. 研討會

   加拿大競爭局與渥太華大學共同舉辦一日研討會，探討電子商務、線上及行動廣告之領域，詳情可參考網站：

http://www.onlineadvertisingworkshop.ca/2013/

會中集結了學界、業界、法界及執法機構等專家參與，其重要見解可作為加拿大競爭局的執法重點及政策方向之參考依據。

2. 宣導

可能由同屬管轄之處理行動支付議題之機構負責進行相關宣導，目前加拿大競爭局正在進行公開諮詢，以確定未來宣導工作的執行區域，同時已在 2013 年 2 月 6 日向加拿大廣播電信委員會於建立無線通訊守則時，提出上述相關宣導建議。

雖然某些行動支付議題與風險是屬於新型態的，但是在本質上的商業行為並無不同，例如在「公開內容」部分，關鍵且重要的訊息必需要明顯易讀，確保消費者掌握相關資訊，明智決定購買與否，同時「公開內容」並不僅僅是業者「說了什麼？」，業者的「免責聲明」必須遵守如下規範：

1. 考慮消費者可能用來觀看廣告的螢幕設備大小，如電視、桌上型顯示器、筆記型電腦、平板電腦、智慧手機等。
2. 考慮聲明之目的與結構，如標題、語法、字體大小、廣告主題接近之程度等。
3. 若廣告之整體印象具誤導性，則「免責聲明」無效。

四、執法

在相關立法條文必須定義明確以避免爭議，例如數位式的廣告內容能輕易修改與刪除，並難以在行動設備上儲存與列印複本，以至於何種內容應以耐久的形式存取與保存？又應保存多久？也成為議題的焦點。

以加拿大目前的案例，加拿大競爭局經查發現 Bell、Rogers、TELUS、CWTA(加拿大無線通訊協會)等機構向消費者發出不實或誤導性的內容，使消費者無法掌握相關資訊而被迫以較高價格購買商品，進而對上述機構裁處 3,100 萬加幣行政罰鍰，並要求全面賠償消費者且立即停止其行為，此案於 2012 年

9 月提交司法部安大略省高等法院進行訴訟，全案至今仍訴訟中。

議題五、行動裝置的威脅

行動電子商務的相關統計參考數據如下：

1. 在北美地區，2012 年的行動電子商務消費總額約 250 億美元，自 2011 年起已增加了 81%。
2. 在 2012 年 12 月，有 20% 的英國消費者購買手機商品。
3. 在 2011 年，歐洲地區約有 1%的線上消費總額花費在購買行動裝置上，約為 170 億歐元。

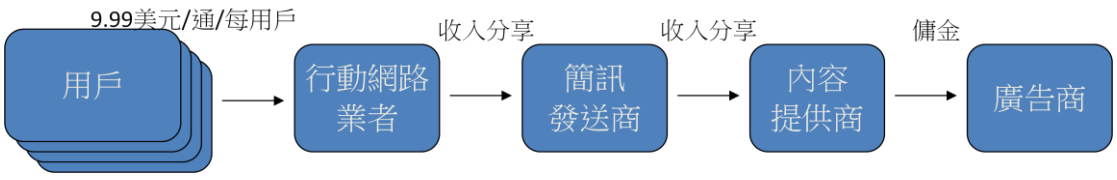
行動裝置使用率之統計參考數據如下：

1. 在 2012 年全球約有 60 億行動通訊用戶，約佔世界人口數 87%。
2. 目前有 10 個國家已超過 1 亦行動通訊用戶。
3. Android 作業系統目前約有 45 萬個應用程式正在販售。
4. 在 2011 年 Apple 公司平台的付費應用程式替公司賺取了 69 億美元利潤。
5. 自 2009 年以來，光是使用黑莓機下載應用程式的次數，每月平均約 1.5 億次。

越來越多的電子商務應用在行動裝置上，因此有關「簡訊詐騙」、「惡意應用程式」與「行動殭屍網路」的風險也與日俱增，而一份 2011 年的調查報告卻顯示，每 20 個行動裝置中，只有 1 個裝置有安裝第三方資安防護軟體。

一、簡訊詐騙

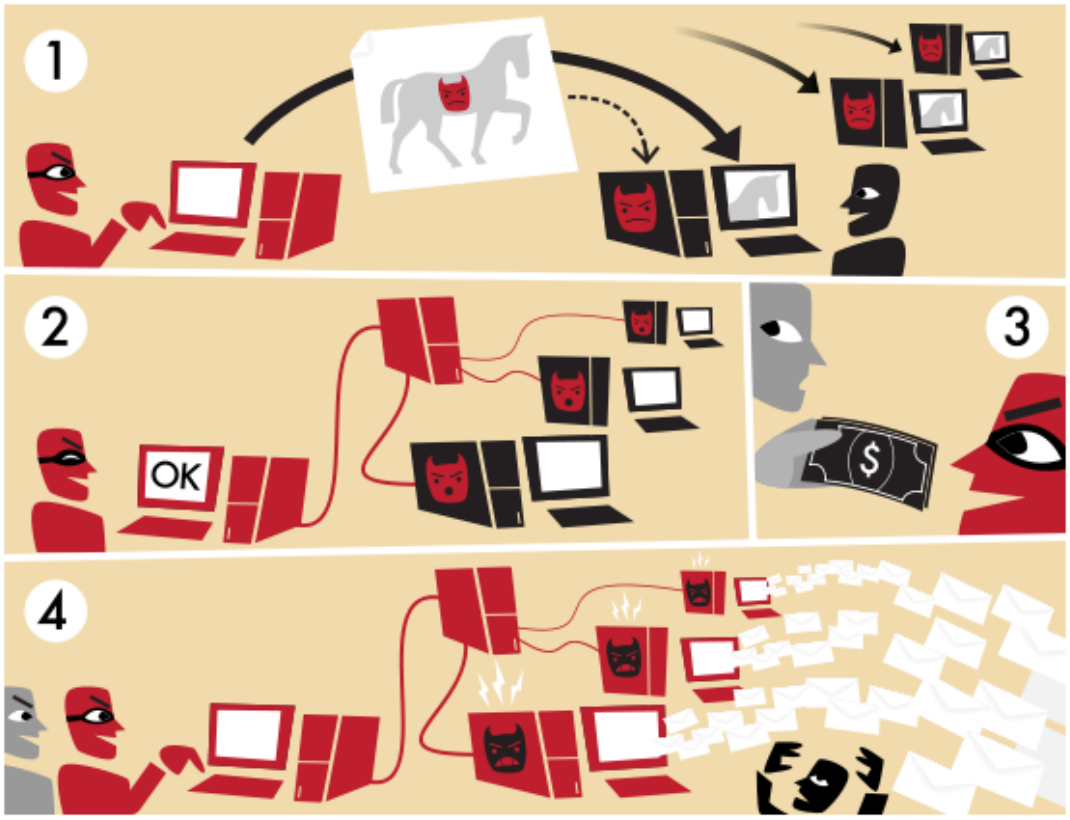
此為利用一般「商業模式費率」來詐騙特殊「高額費率」的簡訊，可能發生於服務或交易過程中的任何一個環節，其不法獲利之結構如下圖：



二、惡意程式與殭屍網路

即網際網路上的不法份子在不知情用戶的行動裝置上植入「惡意軟體」來獲

取個資或其他不法之操作，而感染「惡意軟體」的設備群體，之間還可以互相傳遞訊息，就是一個「殭屍網路」，而且一部「殭屍網路」的主機，就可操控高達 10 萬部的設備。



三、惡意應用程式

「惡意應用程式」可利用下載的方式備安裝在行動裝置上，一份在 2012 年第三季的調查中顯示，有 51,447 個惡意應用程式是針對 Android 作業系統所設計；同時惡意應用程式也可由被入侵的 WiFi 網路中下載，例如被駭客入侵的旅館網路可藉由 WiFi 網路主動發送軟體更新下載通知，誘使不知情的用戶下載「更新」而安裝到惡意應用程式。

四、網路釣魚與社交工程詐騙

用來誘騙網路用戶洩漏如個人資料、銀行帳戶等敏感資訊，而且其複雜度高，不再僅僅只是一個「奈及利亞王子」尋求協助：

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

除了社交網路之外，現在也常常出現在電子郵件和手機簡訊。

為了避免行動裝置受到上述手法入侵，建議培養如下的使用習慣：

1. 只從有信譽的廠商下載應用程式。
2. 安裝應用程式前務必了解權限和隱私規範。
3. 不嘗試破解自身的行動裝置。
4. 使用身分驗證機制。
5. 連接到未知的 WiFi 網路時小心謹慎。
6. 任何以訊息傳遞方式提供的連結，連接時務必再三考慮。
7. 定期備份系統，以防萬一。

議題六、自發性打擊網路犯罪行動

在網際網路的世界中，惡意的網路內容和「參與者」遍及網路空間：

1. 網站(散佈惡意軟體、網路釣魚之類的惡意網址)。
2. 終端用戶主機(受操控的殭屍電腦)。

大多數的「清理」動作需要藉由私人的意願來進行，然而鼓勵網際網路媒介間互相合作的方式可以取得很大的成效，即受入侵的電腦、資安服務提供者、網際網路服務供應商(ISPs)或主機代管服務供應商(Hosting Providers)等，本議題的重點在於透過自發性的資安通報，採取「實證研究(Empirical Investigation)」與「提升淨化機制(Mechanisms to Improve Cleanup)」來打擊網路犯罪行動：

1. 實證研究

   透過簡單的事實紀錄觀察，對需要「淨化」的網站採取通報與關閉連結的機制與受感染的終端用戶與網際網路服務提供者之間的反應。

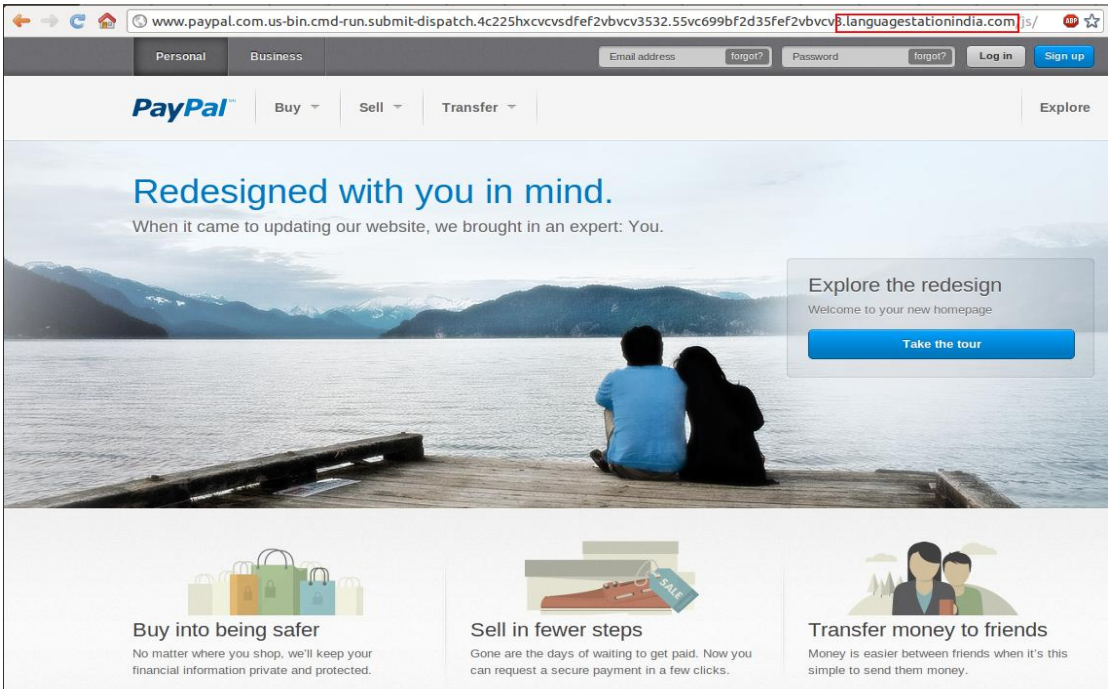
2. 提升淨化機制

   採用「信譽指標」的認證方式，鼓勵網際網路服務供應商積極作為，並通知受感染的網站主機移除惡意軟體。

PayPal 是最常被駭客利用來偽裝成釣魚網站的其中之一，通常使用錯誤但是容易混淆的網址欺騙用戶，藉以盜取敏感的個人資料，此手法通常搭配垃圾郵件提供連結的方式誘導用戶開啟。

然而在 2012 年度下半年，駭客針對主機代管中心進行攻擊的比率提高，約佔整體網路釣魚攻擊的 47%，遭到入侵的主機會被修改系統設定，並在其中設置釣魚攻擊所需要的相關網頁，而一個代管的主機可包含數百、甚至數千個網址，當然駭客也可能「偽造」知名主機代管服務供應商的網站，誘騙用戶上門而利用其主機進行網路釣魚行為。

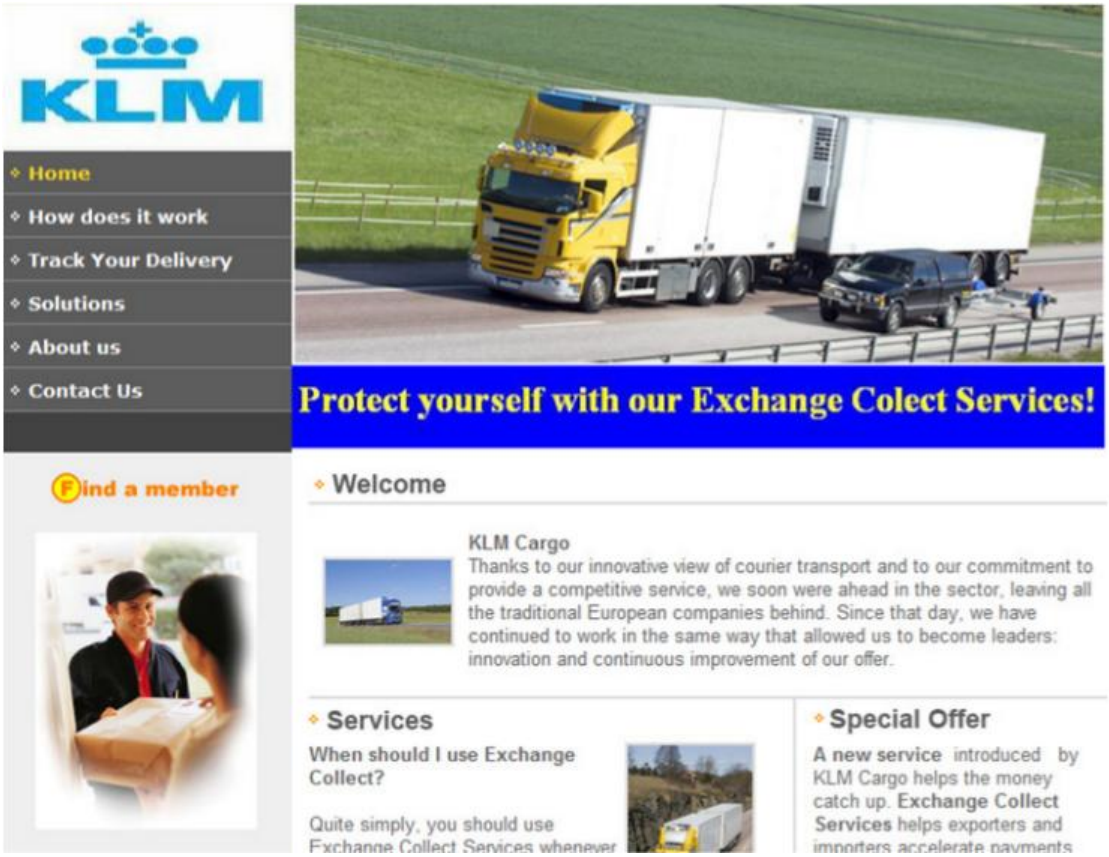
下圖為利用 PayPal 偽裝的釣魚網站，紅色框部分為錯誤且易混淆的網址：



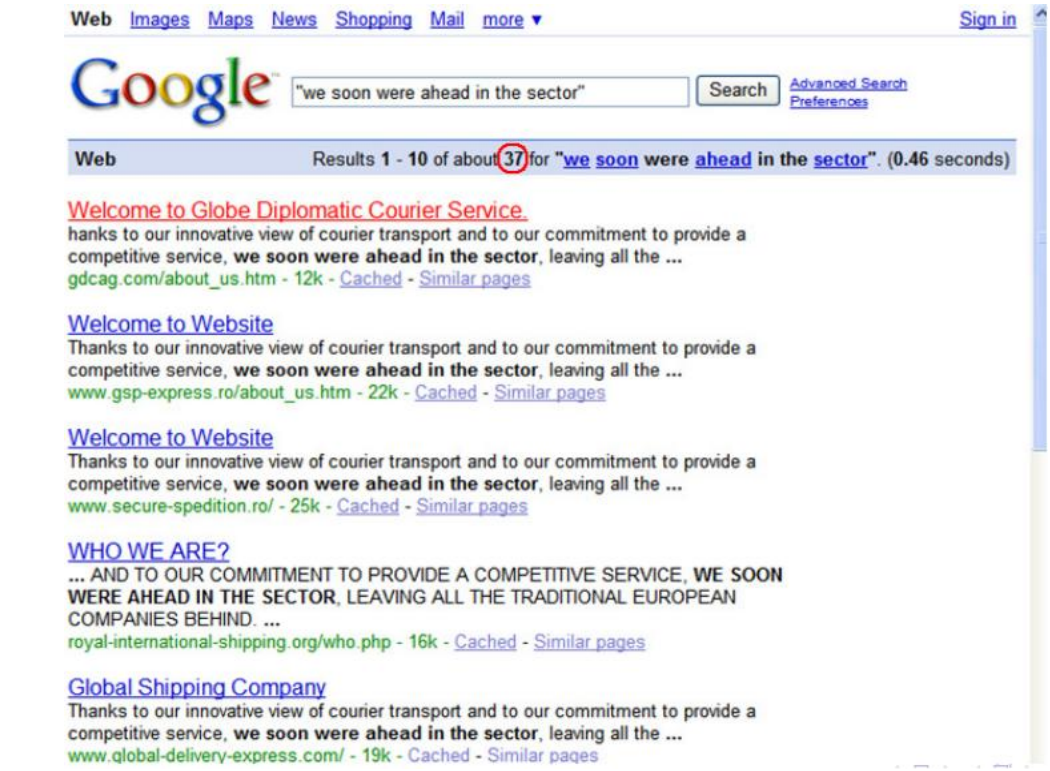
下表顯示以主機代管的運作下，釣魚行為的生存時間比較：

代管方式	生存時間 小時（平均值）	生存時間 小時（中間數）
免費空間		
該擁有者已察覺	4	0
該擁有者未察覺	115	29
整體	48	0
其他代管方式		
該擁有者已察覺	4	0
該擁有者未察覺	104	10
整體	49	0
殭屍電腦代管	70	33

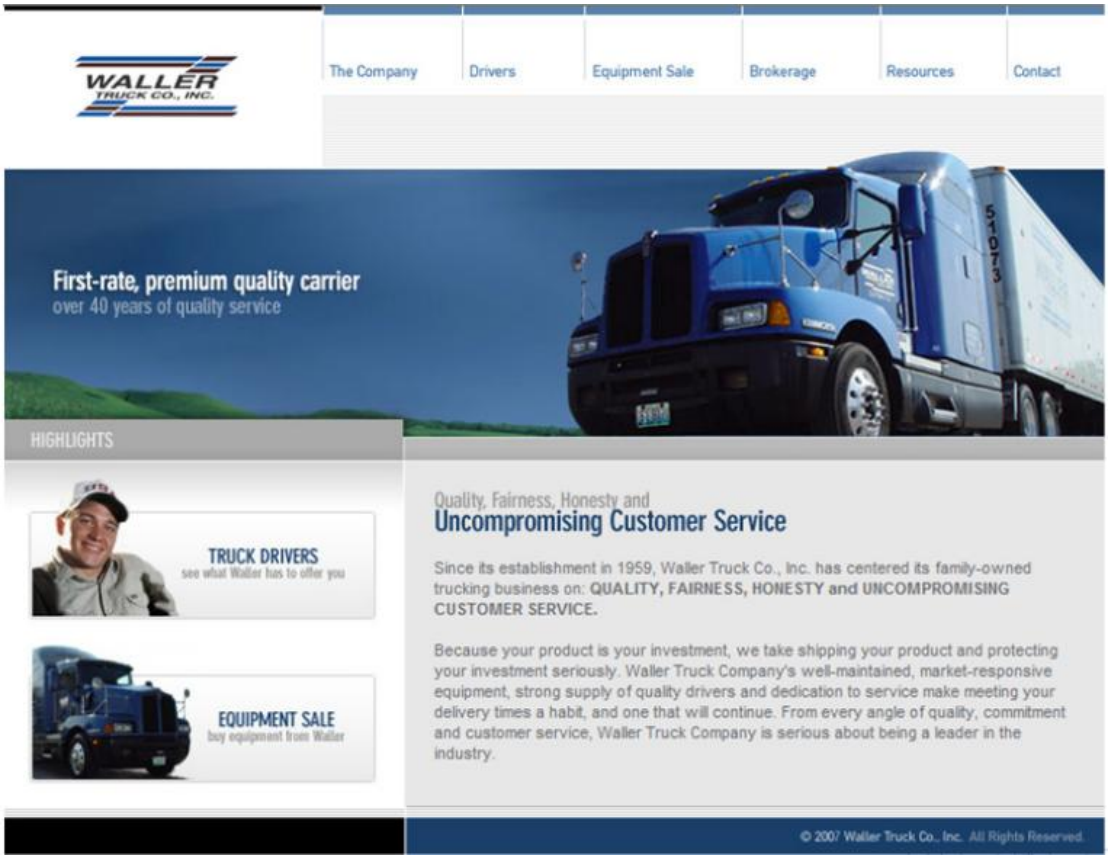
下圖為駭客「偽造」的主機代服務供應商網站：



經調查，利用主機代管進行網路釣魚行為，其所提供的網址使用 Google 查詢(關鍵字為「we soon where ahead in the sector」)，可找到 37 個連結，如下圖：



駭客也會利用「偽造」的非法人力招募網站進行網路釣魚，如下圖：



下表顯示詐騙類型的行為其生存時間比較：

詐騙類型	生存時間 小時（平均值）	生存時間 小時（中間數）
網路釣魚		
免費空間	4	0
其他詐騙網站	4	0
殭屍電腦代管	70	33
詐騙網站		
偽造的網站代管	222	25
非法人力招募網站	308	188

對於移除釣魚網站的積極度最高的是銀行業，銀行克服了許多國際司法機構之法律中沒有明確規定移除釣魚網站的問題，但是銀行的機制仍然不夠完善，他們通常只移除「偽造」自己公司之網站，而忽略其他如非法人力招募之網站，且銀行間缺乏資訊共享，導致大幅降低了移除釣魚網站的速度，同時駭客的技術能力也有些微影響。

研究中所使用的分析數據來自下列三大感染類型，其中每個類型均有上億個 IP 位址作為取得數據的樣本：

1. Spam Trap

   用來蒐集垃圾郵件樣本的「陷阱」，許多釣魚網站的惡意連結來自這些不請自來的電子郵件。

2. Dshield IDS(Intrusion-Detection System)

   從全球各地的用戶蒐集入侵檢測系統(IDS；或稱防火牆)日誌的機制，可取得網路攻擊趨勢之相關數據。

3. Conficker SinkHole

   Conficker 是過去 5 年來最大的殭屍電腦病毒之一，為著名的惡意軟體，利用

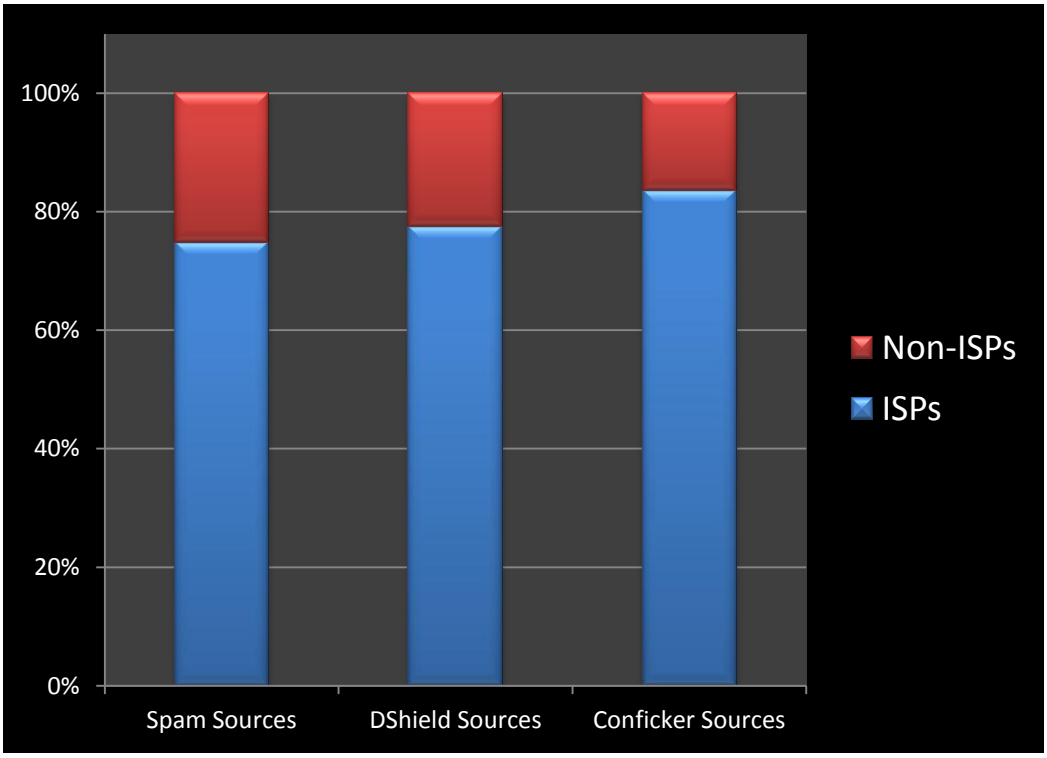
「天坑(SinkHole)」刻意放出漏洞吸引該惡意軟體入侵以取得數據。

根據每個 IP 位址找出對應之國家與 ASN(Autonomous System Number)，並統計 40 個國家(涵蓋 200 個網際網路服務提供者、經濟合作組織 90%之共享市場)中 ASN 與網際網路服務供應商(含非網際網路服務供應商)之資料，進行分析。

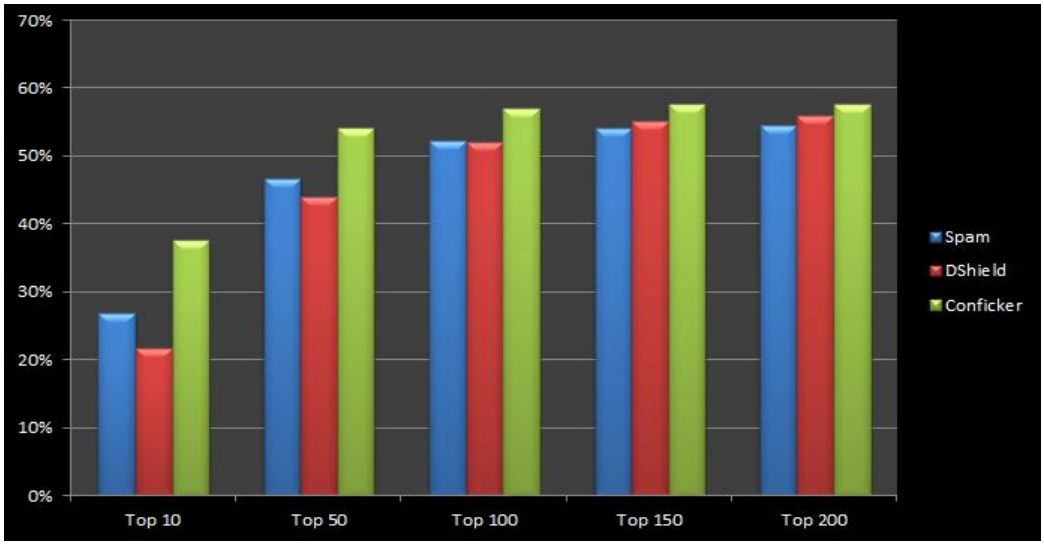
對於網路終端用戶，重點在探討下列問題：

一、針對受到惡意軟體感染的主機，網際網路服務供應商(ISPs)對其進行合法的關鍵控制，可以做到何種程度？

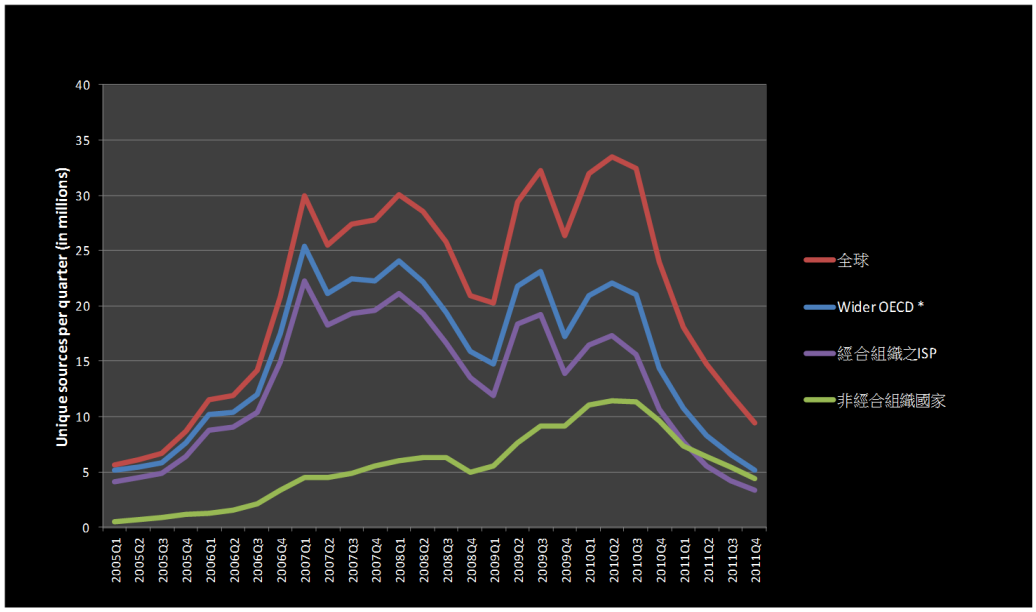
在 2010 年隸屬經濟合作組織的網路中，受到感染的主機源自垃圾郵件、網路攻擊、Conficker 蠕蟲入侵的統計圖如下：



在 2010 年全球受到感染之主機主要的感染源統計圖如下：



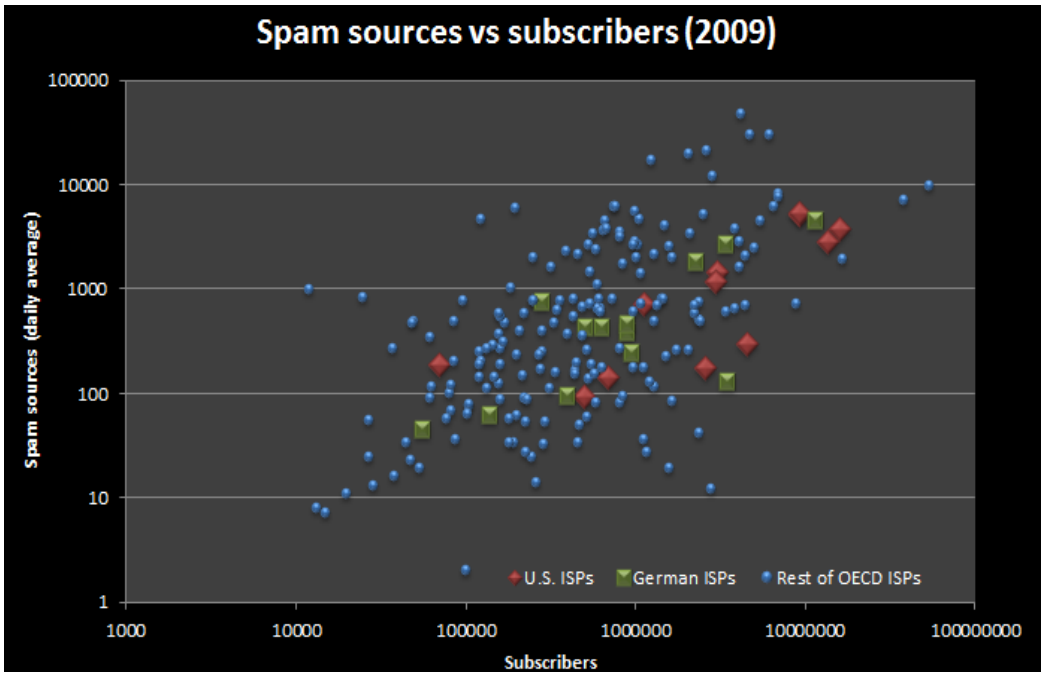
受感染主機之數量與地點統計曲線圖如下：



由上述的統計圖表可以得知，網際網路服務供應商是關鍵的媒介，有超過80%的受感染主機都在經濟合作組織中網際網路服務供應商的網路中，同時僅 50 個網際網路服務供應商可控制全球 50%的受感染主機，總而言之，先進、合法的網際網路服務供應商在其網路中有大量的受感染主機，但他們並不是「惡劣」的供應商。

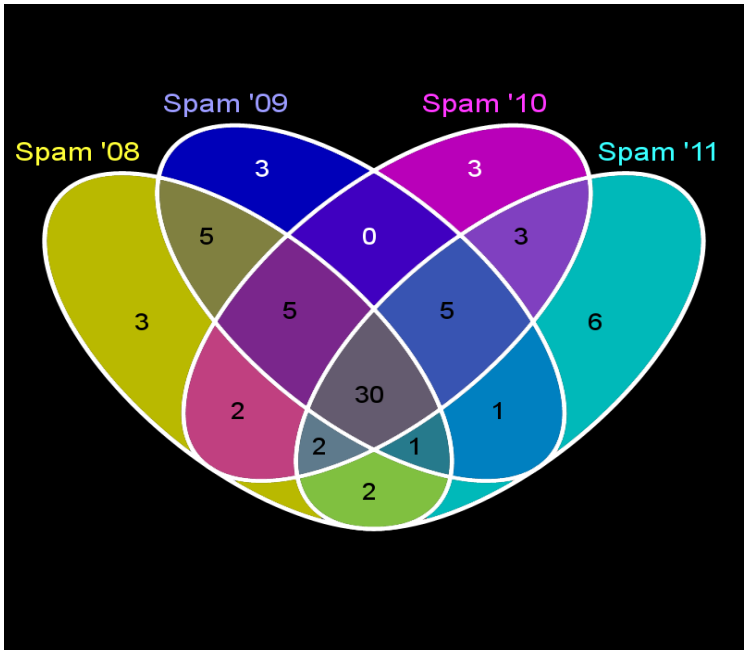
二、以整體受到惡意軟體感染的主機數量來看，不同的主機與主機之間相互影響的程度為何？

在 2009 年受感染的主機與網際網路服務供應商的用戶數比較，其來源為垃圾郵件，統計圖如下：



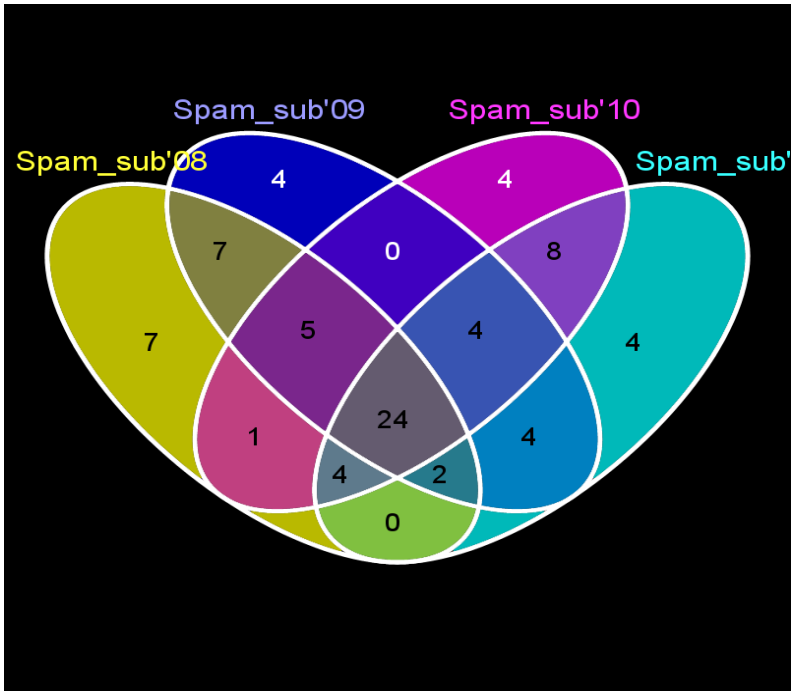
比較不同國家規模相近的網際網路服務供應商，其網路中受到感染的主機數量並不相同，數量差距的幅度甚至可以高達兩個級數以上，若在同一個國家則數量的差距幅度也可能達到一個級數以上，這些差異來自於一段時間的穩定度與資料來源不同。

擁有最多受感染之主機之前 50 名網際網路服務供應商分佈統計如下圖：



重疊部分為跨年度位於前 50 名之列的服務供應商數量，而在 2008 至 2011 年的 4 年間，有 30 個網際網路服務供應商在前 50 名之列。

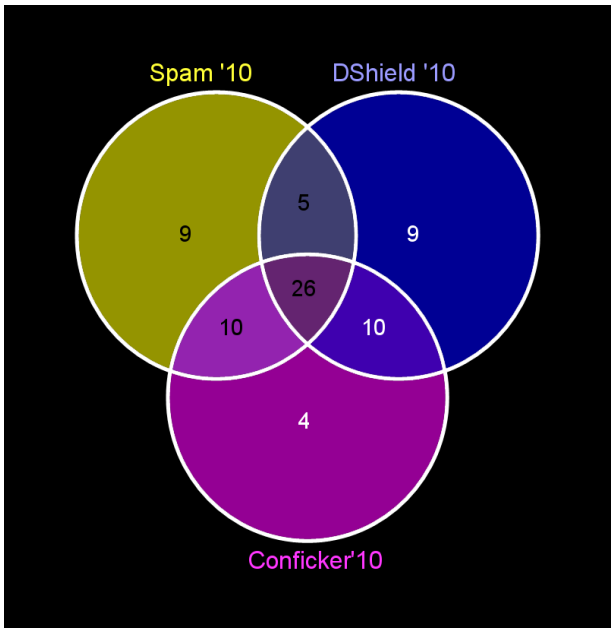
前 50 大網際網路服務供應商中，每個用戶受到最多主機感染統計如下圖：



在 2008 至 2011 年的 4 年間，有 24 個網際網路服務供應商在前 50 名之列。

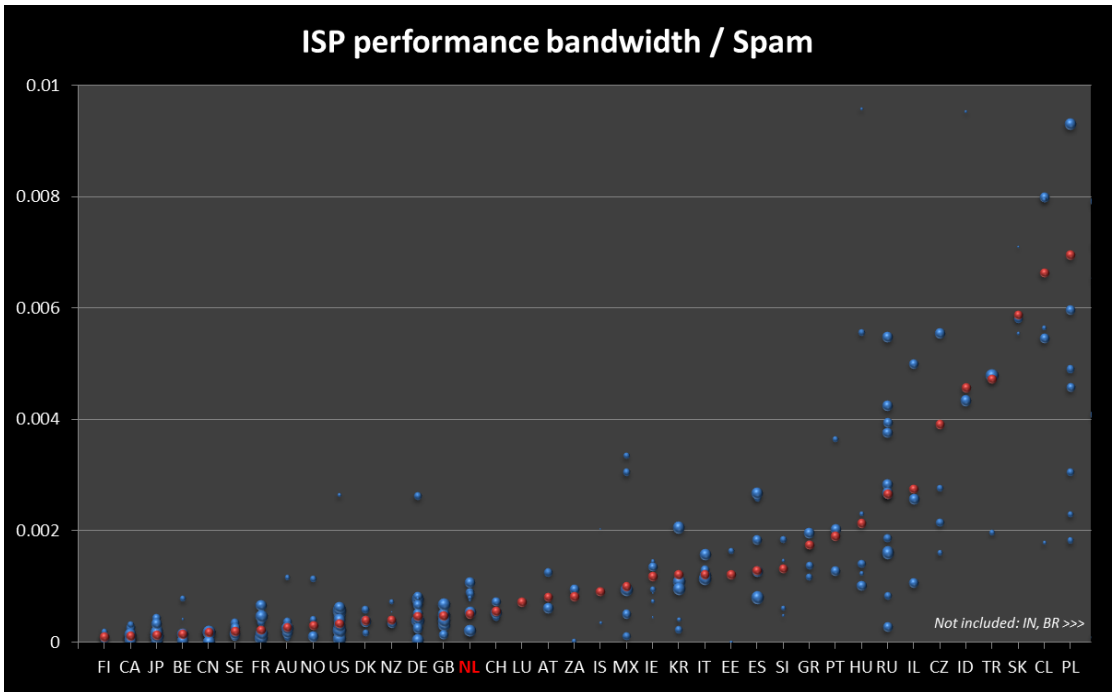
比較前述的 Spam、DShield 和 Conficker 三大感染源，其中有 26 個網際網路

服務商在前 50 名之列(2010 年)，如下圖：



三、國家之間如何進行相互比較？

下圖為不同國家被垃圾郵件感染的比率統計：



其中紅色點為平均值。

四、傳輸媒介在安全性的議題上所扮演的角色為何？

受感染的電腦主機比率為何會如此龐大？分析原因如下：

1. 即便是優質的網際網路服務供應商，他們也只應付自己網路中的一小部分殭屍電腦。
2. 根據荷蘭的市場報告指出，在其國家的網際網路服務供應商簽署反殭屍網路條約之後，仍只有不到 10%的被感染用戶與網際網路服務供應商進行聯繫。
3. 經調查，這些問題在於網際網路服務供應商並沒有廣泛蒐集網路內受感染主機的相關資料。
4. 可以想像，在其他國家必定有類似的問題，甚至更糟糕。

然而，有關安全性的議題，有數據顯示，若有電信監理執法機關的參與，有助於提升該國整體資安防護能力，例如有參加倫敦行動計畫的相關執法機關。

為了有效提升淨化機制，建議可對網際網路服務供應商採用「信譽標章」的認證方式作為誘因，因為服務供應商與用戶之間的資訊並不對等，這也妨礙了網路市場安全性的發展，消費者通常無法分辨哪一家服務供應商的安全機制最佳，這也使得服務供應商對於網路安全性的投資失去了積極的態度，「信譽標章」的機制是可能改變服務供應商心態的方式。

荷蘭政府委託代爾夫特理工大學(Technische Universiteit Delft)與網際網路服務供應商合作為荷蘭網路市場建立有關殭屍網路感染的「信譽標章」，但荷蘭政府要求不能將結果公開，因為依反殭屍網路的條約，只能與網際網路服務供應商進行「共同研究」，綜觀 2010 年為其表現最差的一年。

清理遭植入惡意軟體的網站通常是由下列的「自願者」來協調與啟動：

1. 資訊安全防護相關業者。
2. 搜尋引擎提供者。
3. 非營利組織。

4. 虛擬主機與網站管理者。

而惡意軟體的清除程序通常如下：

1. 檢測正在散佈惡意軟體的網站。
2. 通知受感染網站的管理者和相關的網際網路服務供應商，若屬惡意散佈則必須登記在案。
3. 搜尋引擎可加以封鎖，直到惡意軟體被刪除。

根據實驗，向網站通報感染惡意軟體，完整詳細的通報內容明顯的比簡潔的通報內容成效好，第一次通報為最佳的時機，甚至可以說，發送簡潔的通報內容形同「浪費時間」，若發出完整詳細的通報，大約有 40%的被感染網站可在一天內清除。

通報網站感染惡意軟體的最低限度內容範例如下圖：

```
Subject: Badware URL notification - compromisedSite .com
To: support@good-host.com

hxxp://compromisedSite .com/ appears to be a badware URL. This means it
may be placing Internet users at risk. Please investigate and take
appropriate action to resolve or mitigate the threat.

Description: Contains malicious injected javascript

Date/time of detection: 2011-12-05 1303 EST
IP address at time of detection: 216.119.132.194
Additional parties notified: info@compromisedSite.com (site owner)

You are receiving this report because this e-mail address is listed as
the technical or abuse contact address in the WHOIS record for
216.119.132.194. If you believe you have received this report in
error, or for more information, please contact us at this address:
reporting-beta@stopbadware.org.

Caution: Opening badware URLs in your browser can infect your
computer. For security reasons, URLs in this email have been modified
by replacing http with hxxp and by adding a space before the last dot
(.)
```

可在其中加上感染詳細證明，範例如下：

```
======================
ADDITIONAL INFORMATION
======================

Detailed badware description:
URL accessed: hxxp://compromisedSite .com/
Bad Code: <img heigth="1" width="1" border="0" src="hxxp://imgaaa
.net/t.php?id=9975084">
Behavior: Attempts to load malicious code from hxxp://imgaaa
.net/t.php?id=9975084.

URL accessed: hxxp://compromisedSite .com/.log/compromisedSite.com/xmlrpc.txt
Behavior: Is indication of further compromise of compromisedSite .com.

Special conditions: hxxp://compromisedSite .com/ only delivers malware when accessed
with a google.com HTTP referrer.

Best practices for web hosting providers receiving reports like this:
http://www.stopbadware.org/best-practices/web-hosting-providers
```

清理惡意軟體約 16 天之後，其成果如下表：

實驗組	% 清理（全部）	% 清理（惡意註冊）	% 清理（受損害的主機）
管制	45%	46%	45%
最小的	49%	53%	47%
整體	62%	58%	63%

本實驗被設計可作為其他通知制度的範本，詳情可參閱網站：

http://lyle.smu.edu/~tylerm/cset12.pdf

網際網路服務供應商為大幅降低惡意程式感染率的重要媒介，透過類似「信譽標章」建立誘因的方式是關鍵，而取得每個受惡意軟體感染用戶之數據是建立淨化機制的先決條件，但是目前大多數的網際網路服務供應商並沒有強烈的動機去仔細的全面觀察受感染事件的數據，同時為了進一步改善遭感染用戶端主機的淨化機制，仍需仰賴國際間的數據共享並建立與推動完整的通報機制。

美國南美以美大學(Southern Methodist University)與荷蘭代爾夫特理工

大學(Technische Universiteit Delft)正展開為期三年的研究工作，尋求下列問題的解答：

1. 什麼型式的通報能最有效讓服務供應商對於散佈惡意軟體等網路濫用採取行動？
2. 有什麼補充誘因能使關鍵的服務供應商更傾向於主動對通報採取行動？

並且使用下列的方法進行研究：

1. 建構事件類型、服務供應商、誘因以及通報之分類。
2. 透過量化程度與類型之通報，探討通報受影響的情況對於減少網路犯罪層級之觀察研究。
3. 與基礎設備營運商實施改變通報方式及合作模式之實驗。

共享事件數據是清理惡意軟體感染個人主機與伺服器之關鍵，網際網路服務供應商掌握了 80%的控制因素，因此其必為解決方案的一部分，幸運的是仍然存在很大的改善空間，因為即使是在相同的市場、相同規模的網際網路服務供應商，其表現仍有很大的差異，哪些進行干預的手法效果最好，在目前並不清楚，因此需要能配合或改善誘因的政策及做法，詳細內容可參閱網站：http://lyle.smu.edu/~tylerm/

議題七、歐盟網路犯罪中心(European Cyber Crime Center，EC3)

歐盟網路犯罪中心縮寫為 EC3，成立於 2013 年 1 月 11 日，總部設立於荷蘭海牙(Hague)，專責重大組織性網路犯罪行為的打擊任務。

EC3 所關注的資訊安全項目如下：

1. 高科技的犯罪行為，例如駭客、惡意軟體、入侵、攻擊等行為。
2. 兒童線上性虐待與性侵害。
3. 信用卡詐騙行為，包括線上刷卡和實體刷卡。

EC3 的核心功能如下：

1. 網路犯罪之資訊中心。
2. 建構執法能量。
3. 支援反制網路犯罪事務。
4. 提供高技術性、分析性及鑑識能力之專業知識與技能。
5. 資訊安全相關專業技能研究與發展。
6. 推廣專業能量到歐盟會員國、國際合作夥伴和私人機構。
7. 透過策略與前瞻性的作為預防與監控未來可能的網路犯罪型態。
8. 作為歐洲網路犯罪調查人員之參考來源。

目前 EC3 主要的合作成員為歐盟會員國、歐洲相關機構、國際合作夥伴、民營公司、學界和民間社會組織。

EC3 目前的組織架構如下圖：

其架構分由下列四大部分組成：

1. 資料彙整(Data Fusion)

   資料彙整中心從公共或私人等公開之來源收集資料，以充實現有的資料庫，並處理和分析網路犯罪訊息，目標在擴大網路犯罪訊息的偵查，以便迅速識別最新出現的威脅，下圖為 EC3 的資訊流程：

藉由公開或私人授權的方式取得並蒐集相關資料，並由 EC3 成員將取得的資料進行統計分析建立數據，數據可分享給第三方團體，並作為 EC3 在策略、運作支援、研發培訓等操作上的依據。

2. 經營運作(Operations)

由於網路無國界的性質，網路犯罪通常橫跨數個國家進行，因此無法單憑一個國家的執法單位查緝，EC3 要配合執法單位進行跨國界的協調和合作共同打擊犯罪，並提供相關技術支援。

3. 研發培訓(R&D Training)

隨著網路犯罪的技術與手法日新月異，降低和防止網路威脅的任務非常仰賴扎實的基礎研究，故研發能量的需求相當龐大，且並非所有的歐盟會員國都具備相關知識水平啟動打擊網路犯罪的機制，因此 EC3 將全力提升歐盟會員國之相關能力與建設，使其具備執法能量，共同維護網路資訊安全。

4. 策略宣傳預防犯罪(Strategy Outreach Crime Prevention)

由於 EC3 從各種管道的來源分析大量的資料，充分了解網路犯罪、兒童性犯罪和詐騙者如何思考和運作，因此不僅有助於執法，也有利於政策方向和立法推動，但更重要的是，EC3 可藉由完整的資訊，保護民眾和企業免於遭受

網路攻擊威脅。

歐盟網路犯罪中心網站：https://www.europol.europa.eu/

肆、 檢討心得與建議

倫敦行動計畫是一個全球性的組織，其會員為各國專責資訊安全相關的政府機關或民間機構，除了在會議中分享垃圾郵件及資訊安全相關經驗，亦可以就各國報告的統計數據了解資訊安全問題的趨勢，同時取得資訊安全方面的最新知識與訊息，因網路通訊技術的迅速發展，資訊安全威脅的手法態樣也不斷翻新，國際間每年定期舉辦的會議實屬重要的交流管道，讓各資、通訊發達的國家可以迅速掌握新知，對打擊網路不法行為保持優勢，本會議是一個重要的國際交流平台，可以藉機了解各國處理資安問題的方式、法規機制，同時與會的各國代表也樂於分享，對於國際合作事務的推展來說，是一個良好互動的機會，除了直接面對互動交流外，亦可藉由交換名片或電子郵件的方式保持聯繫，回國後有利於業務的推展。在本次會議中為建立與美國垃圾郵件雙向通報機制，與美國聯邦貿易委員會(Federal Trading Commission，FTC)官員洽談，回國後仍持續聯繫，其推薦與即將到臺灣公平交易委員會舉行會談的 Michael Panzera 先生會商相關機制，Michael Panzera 先生同時也在本會舉行「美國兒童線上隱私保護法」專題演講，因此可見參與國際會議除了可作為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。

茲針對上開會議內容提出檢討與建議事項如下：

一、 展現共同維護網路秩序的決心

鑒於網際網路相關應用蓬勃發展，經濟規模日益龐大，因此資訊安全對於民眾的個人權益、財產的保障十分重要，會議中亦可看出國際間對於資訊安全的相關問題非常重視，在國內有必要加強民眾有關資訊安全的宣導，整合政府機關與民間業者、團體的力量共同努力，強化我國整體資訊安全防護能量；由於如垃圾郵件之類的資訊安全威脅通常跨國性組

織化網路犯罪，故需建立並維持國際合作的管道，有效支援國際聯防機制，除了打擊網路不法犯罪，亦可提升台灣在國際間的能見度。

二、 各國立法與執法經驗

國內的「濫發商業電子郵件管理條例」草案仍然存在爭議，尚在審議階段未立法通過，尤其在「行政罰」部份的認定問題，即使通過要真正落實仍有相當難度，加拿大在本次會議分享其「反垃圾郵件法」的立法和規範，其中明定高額的「行政罰」，但也為避免爭議而採納多方意見制定了不少豁免條款，預計將在 2014 年 7 月生效，其執行成效與經驗可作為我國相關法案的借鏡，作為我國未來法案執行的因應參考。

三、 積極參與國際合作

在全球化的國際趨勢下，與會的各國均了解到國際合作的重要性，本會已與其他國家逐步建立合作關係，如美國、日本、南韓、巴西等國，但仍有相當大的國際拓展空間，本會為通訊傳播主管機關，配合處理跨國垃圾郵件產生之資訊安全問題，宜推動立法促進國際合作，在國際間積極參與國際事務，對於防制垃圾郵件與強化民眾網路使用安全相關的政策與立法進行通盤檢討與規劃，主動尋求國際合作夥伴，在平等互惠的原則下擴展及執行防制垃圾郵件事務，共同打擊網路應用之不法行為，維護經濟發展和優質的網路使用環境。

附錄一、我國簡報內容紀錄

Good morning, ladies and gentlemen. My name is Si-Hon Su. On behalf of the National Communications Commission, Taiwan. I am pleased to be here to give a presentation of the status quo of Anti-Spam in Taiwan to you.

Please feel free to give us comments and feedback.

My presentation will be separated into four main parts:

1. Legislation Progress of Anti-Spam Act
2. Procedure of Dealing with Spam Complaints
3. International Cooperations
4. Future Visions

First one is the legislation progress of the Anti-Spam Act in Taiwan. The latest draft was brought out in 2012 by NCC. The draft focuses on protecting the right of the receivers and strengthening the Internet security and efficiency. The draft also targets on preventing the customers from receiving unsolicited commercial emails.

So we have designed class action lawsuit for the receivers to request compensation from the senders. Besides, the competent authorities can order the email service providers (ESP) or Internet access service providers (IASP) to stop spamming.

The draft adopts “Modified Opt-out” method that means the users can reject any more emails if they didn’t reply to the very first email. Under the considerations of the needs of the great amount of small and medium enterprises in Taiwan, the “Modified Opt-out” mechanism is chosen to allow the enterprises to have the opportunity to send the first email to the customers and to make sure the customer will not be bothered again. The senders can’t send the same type of commercial emails unless they get the consent from the consumers, which is the Opt-in method.

The draft focuses on receiver’s protection by using technologies because the

Telecommunications Act stipulates that the service providers shall not reject the transmission and reception of telecom services. Therefore, the draft also grants the service providers the legal right of rejecting the sender's dictionary attacks when there is possible obstruction of the service provision. The draft also gives the competent authorities the right to order the ESPs or the IASPs to stop spam emails and impose administrative punishments onto the service providers if they refuse to cooperate. Furthermore, the draft also gives the right of development of new technology, e.g., OP25B, which is advocated by Japan.

Nowadays, in Taiwan, when the loss or damage of the spam victims may be compensated from the lawsuit under Civil Law. However, it is time-consuming and needs a lot of judicial resources. This will also cause a problem because they can't accumulate enough information from the senders to give it to the court. In order to help the victims, the draft allows them to use class action and the group may request senders' information from the service providers or agents under the permission of the competent authorities. If the service providers or the agents refuse to cooperate, the competent authorities may put administrative penalties on the service providers. However the draft doesn't put the administrative penalties on the IP users because there are a lot of botnets, the users are usually victims rather than real spammers.

In addition, there are three Anti-Spam drafts in the Legislation Yuan, the congress of Taiwan. One is brought out by the NCC, the other 2 are proposed by different legislators. There are quite a few discrepancies among the three versions. The arguments are on the using of the administrative penalty by the competent authorities and the class action lawsuit by the victims. Therefore, it still needs further discussions and negotiations to finish the legislation of the Anti-spam act.

More information is on our website: http://antispam.ncc.gov.tw/english/links.html.

Nowadays, there are no laws and regulations to combat Spam in Taiwan. The major measure to handle the Spam is the cooperation between the competent authorities and the private sectors. As email service providers, the ISPs are requested to specify the agreement in the contract to the subscribers that if the subscribers send emails repeatedly and those are confirmed to be Spam, the ISPs may take the necessary steps to avoid further interference or damage to the Internet, such as suspend port 25 for a period of time. Therefore, if the users have received spam emails, they may forward the spam emails to NCC or the ISPs with complaints. The NCC or the ISPs may request the source ISPs to confirm the records by matching the origin IPs of the email headers and stop the spam emails according to the service agreement of the contract between the ISPs and the senders.

According to the statistics, about 97% of the reported spam emails are from overseas but only a small amount are from the exchange of cooperation. There are not many countries in cooperation with Taiwan, so I would like to invite you to establish the cooperation with us on the anti-spam issues.

This chart shows the email numbers received by the top 10 ISPs, which are also email service providers in Taiwan. The statistics are accumulated from February 2007 to June 2013. The blue line is the total amount of incoming emails, the red line is the total amount of blocked emails, the spam, and the green line is the ratios of the amount of spam to the total.

You can see the red curve drops significantly since October 2010 because many governments in the world have been struggling against botnets.

However, the ratio of spam emails still remain high, which is at an average ratio of 90%. The ISPs have to spend a lot of system resources to assist the users to filter spam, not to mention the inconvenience to the receivers.

This chart shows the sampled statistics of spam from the main sources to Taiwan. The top 3 sources of the incoming spam from 2011 to 2013 are China, USA and Singapore. The amount of the USA decreases but the amount of China grows. It is worth noting that the amount from South Korea rises sharply in this August 2013.

Recently, NCC has set up a honey pot to collect spam. It has come out that 90% spam are from the overseas. The NCC will seek for more international cooperation on anti-spam as a core mission in the future.

Spam has become a global problem. Anti-spam action requires global cooperation. In order to fight cross-border spam, NCC has been eagerly to develop international cooperation, to join international organizations, and to establish working relationship with the other countries. We have signed the MOU on cooperation in dealing with Spam with Australia, Canada, etc.

NCC has also developed of spam data exchanging with Anti-Spam Consultation Center (ASCC) of Japan Data Communications Association (JADAC), Korea Internet Security Agency (KISA), Brazilian National Computer Emergency Response Team (CERT.br), and Federal Trade Commission (FTC) of the USA. The spam data exchange is bidirectional with Japan and Korea, while it is unidirectional with the USA and Brazil.

Brazil ranks first on the amount of delivering data to Taiwan every year. South Korea ranks second. The USA ranks first on the amount of getting data from Taiwan. South Korea also ranks second.

There are three spam sources that are the information or data exchanged with collaboration countries, the spam reported by Taiwan’s receivers, and the spam captured by the Honey Pots established by NCC.

The collected emails will be analyzed by the software designed by NCC. The emails

will be delivered to the collaboration countries if the IP addresses are located in the IP domain of the countries. One important thing is that the whistleblower's information will be covered under the provisions of Personal Information Protection Act of Taiwan before sending out the spam data. If the sources are in Taiwan, we will request the IASPs to confirm the IP addresses and to find out the spammers to give them warning to them or to prohibit their use of the Internet for a certain period of time according the contract because the anti-Spam Act does not finished the legislation yet.

Recently, the major work for NCC is to deal with the spam that is going out from Taiwan by the international cooperation. It is beneficial to the elimination of outgoing spam. However, there is little help to decrease the total amount of incoming spam to Taiwan. NCC is planning to set up more Honey Pots and to increase the data exchange with the collaboration countries to combat the cross-border spamming.

Fighting against spam is a long-term work that needs resources and supports. However, the legislation of the Anti-spam Act is not completed in Taiwan yet. The regulators can only request the operators to deal with spam within limits. Also without judgment standards of email delivery behaviors for the court, it is very difficult for the victims to get compensations from lawsuit. NCC therefore will put emphasis on proceeding with the anti-spam legislation and to overcome the barriers between the government and lawmakers.

Cross-border spamming has become a major issue since the spammers will try their best avoid being investigated because of different regulation strength. It is also an important topic to enhance the development of international cooperations to fight against spam to protect the email users. NCC will seek for more relationships with

the other countries to build up spam data exchanging.

The international transferring amount of spam from the other countries is increasing, so NCC is going in modified the existing analysis software to enhance the efficiency of analyzing spam by automation and to get rid of manual errors.

Besides, many receivers have trouble being whistleblowers because there is no unified form of reporting tools. Especially, the reception of webmail spam will be reported manually. This not only increases the manual efforts and errors, but decreases the efficiency of analyzing spam data. Therefore, the important issue for NCC is to cooperate with the service providers to develop easy reporting tools for the victims to use.

OK. That's all for my presentation. Thank you for your attention. If you have any question, please feel free to email to YCSu@ncc.gov.tw. We will be happy to have further contact with you! Thank you!

LAP Only sessions
Montreal, Canada – October 22-24, 2013

TIME	Tuesday 22/10	Wednesday 23/10	Thursday 24/10	Friday 25/10
08:30	Economics of Malware **(Tyler Moore, SMU, US)**	Australia 10 years of anti-spam law and enforcement **(Julia Cornwell McKean, ACMA, AU)**	LAP Strategic Plan: - Outreach & Mentoring with Developing Economies - Training – next phase (Session moderated by **LAP Secretariat**)	Do not call: Offshore Threats **(Betsy Broder, FTC - US)**
08:45				
09:00				
09:15		Enforcement panel – Tools for Information Sharing and Coordination: A Case Study **(Alain Kapper, OFT - UK)**		Do not call: Premium Rate and Affiliate Marketing Scams **(Alisha Mahoney, PhonePayPlus - UK & CRTC - *tentative*)**
09:30	LAP Training initiative **(Lynne Perrault, CRTC – CA & Hein Dries-Ziekenheiner, Vigilo, NL)**			
09:45		Enforcement panel – The Role of multilateral MOUs: Still the Best Way to Enhance Engagement? (moderator: **Betsy Broder, FTC**)	New members presentations : Curacao **(Elgeline Martis, CARICERT, CW)**	
10:00	Country updates **(Taiwan and Japan)**			
10:15			Coffee break	
10:30	Coffee break	Coffee break		Coffee break
10:45	JOINT LAP-MAAWG SESSIONS		LAP Strategic Plan : Initiatives for 2014-2016 (Session moderated by **LAP Secretariat**)	Do not call: Reflections on Ten Years of Do Not Call **(Betsy Broder, FTC)**
11:15				Next Steps for LAP Do Not Call **(Andrea Rosen, CRTC - CA and Julia Cornwell-McKean, ACMA)**
12:00	Lunch	Lunch	Lunch	
12:30				END

13:00				
TIME	**Tuesday 22/10**	**Wednesday 23/10**	**Thursday 24/10**	
14:00	JOINT LAP-MAAWG SESSIONS		**Caller ID Spoofing: Defining the Problem – Identifying the Solutions**	Survey Results: What DNC enforcers are seeing on the spoofing front **(Raymond Pierce, CRTC-CA)**
14:30				An Overview of the Technology and Proposals for Solutions **(Hein Dries-Ziekenheiner, Vigilo, NL)**
15:15				Coffee break
15:30				Next steps. The development of a roadmap for LAP initiatives to address caller ID spoofing **(Julia Cornwell-McKean, ACMA, AU)**