出國報告(出國類別：參加國際會議)

出席第十二屆倫敦行動計畫(LAP:London Action Plan)年度會議報告

服務機關：國家通訊傳播委員會

姓名職稱：吳銘仁簡任技正、李技正福懿

派赴國家：法國巴黎

出國期間：**105** 年 **10** 月 **22** 日至 **29** 日

報告日期：**106** 年 **1** 月 **17** 日

附件

壹、前言

近年來，除固定通信網路外，隨著行動通信網路之發達及通訊軟體之使用普遍化，因其快捷、便利、成本低廉及無國界等特色，電子郵件、訊息成為商務網來之主要工具。然因不肖業者缺乏自律，大量不請自來之商業電子郵件(Unsolicited Commercial Email，俗稱「電子郵件」、SPAM)、垃圾短訊與惡意軟體等於通訊網路中為害日深，除造成網路及電信服務提供商之系統極大的負擔外，其亦造成一般使用者偌大困擾。該等垃圾郵件、垃圾訊息及惡意軟體等已嚴重危害網路提供正常通訊的效能，造成個人、企業、國家乃至於全球經濟之鉅大損失。

世界各國已紛訂立專法予以管制，我國則尚未能就「濫發商業電子郵件管理條例草案」完成立法工作，惟本會為配合行政院之政策，協助推動垃圾郵件防制，對外積極參與國際反垃圾郵件相關組織之活動以尋求國際合作之機會；在國內則係持續監督電信相關事業透過服務契約提供垃圾郵件技術防制，以確保民眾之通信權益。另因垃圾郵件與網路資訊安全議題已環環相扣，垃圾郵件防制工作已成為本會電信資安防護工作之一，本會除續辦垃圾郵件防制與跨國之合作事務，亦更積極推動電信資安的防護事務。本次派員參與倫敦行動計畫之目的，除藉由參與會議以瞭解並蒐集各會員國就防制訊息濫發及網路安全防護之機制與趨勢以作為本會規劃與業務執行面之參考外，亦繼續垃圾郵件防制之國際交流與擴展任務。

本次會議乃係由「倫敦行動計劃」及「反濫用訊息、惡意軟體、行動通訊工作群組」(Message Malware Mobile Anti-Abuse Working Group，“ M3AAWG “)兩大組織共同舉辦，其議題包含商業電子郵件(聯盟行銷，Sweep-Affiliate Marketing)之掃蕩、執法制度之建立、垃圾郵件情資之分享程序及執法、2016 年惡意軟體發展趨勢科技面概述、北美洲及歐洲法規之更新、誘補機制(Honey pot)、釣魚網站之反制等。上述該等議題之資訊，對於我國政府於日後就各面向議題的政策制定與管制措施將有所助益。本次倫敦行動計畫之秘書處將該會議定位為各會員國政府運作機制分享，為免有心人士獲取資訊後予以分析，進而規避各國政府之管理作為及法律漏洞，該會議中宣示不得拍照、錄音與錄影外，其亦不發予簡報資料。本報告將針對倫敦行動計畫對會員公開之資料，並配合倫敦行動計畫秘書處

之要求遮蔽部分資訊後，就會議議程、議題內容、檢討心得與建議項目等進行撰寫，期達相關業務之規劃與執行參考之目的。

貳、第十二屆倫敦行動計畫年度會議

一、 會議時間、地點及議程

時間：105 年 10 月 24 日至 10 月 28 日

地點：法國巴黎 Marriot Rive Gauche Hotel & Conference Center

議程：詳如附件一

二、 主要議程

本屆倫敦行動計畫年度會議為期四天半，第一天為訓練工作會議，其中因部份會議涉及各會員政府結合網路犯罪執行垃圾郵件之案件調查，且多數講者均未授權予會議主辦單位提供會議資料，是以，本報告僅就獲公開資料之部份議題加以簡述：

(一) 「 倫敦行動計畫」及「反濫用訊息、惡意軟體、行動通訊工作群組」訓練工作會議

因垃圾郵件常與網路犯罪相關，調查與執法程序與採取之行動複雜化更甚以往，且常同時需數個國家之權責機關一起進行調查與執法，故本議程乃採納倫敦行動計畫多數會員國之建議舉行，以強化與會者及會員國之專業能力，並參考其它先進國家之實務案例執行作法，以奠定執行人員之技術面之專業判斷力。

訓練工作會議之議程簡述如下：

◆ **議題一： 執法訓練(Law Enforcement Training)**

與談人：美國聯邦貿易委員會代表 Melinda Claybaugh

澳洲通訊及媒體管理局代表 Bruce Matthews

國際刑警組織代表

本議題中首先介紹國際刑警組織(International Criminal Police

Organization, 通稱" Interpol"，簡稱 "ICPO")，該組織於西元 1923 年成立，目前總部位於法國里昂。ICPO 為聯合國以外之世界第二大規模國際組織，其擁有 190 個成員國，每年運作之預算逾 7,800 萬歐元，資金則由各成員國撥出。ICPO 主要責任為調查跨國恐怖活動、組織犯罪案件、毒品、軍火走私案、偷渡案、洗錢案、貪污案件、兒童色情案件、科技犯罪及網路犯罪等。ICPO 組織中的常設機構「國家中心局」主要負責 ICPO 成員國各國警方之合作，ICPO 總部設有一座存有 150 萬餘名國際刑事犯罪資料之檔案庫；ICPO 之電子郵件網路系統每年可處理 100 萬封包括英文、法文、西班牙與與阿拉伯文的各種「通報」，惟 ICPO 無執法權力。

又本議題中澳洲通訊及媒體管理局(Australian Communications and Media Authority，" ACMA") 介紹其澳洲網路安全行動(Australian Internet Security Initiative, "AISI")，該活動乃由公部門與自願參與之民間機構共同合作打擊由澳洲網際網路協定位址所發出之惡意軟體與服務漏洞，以保護澳洲網路使用者之網路免於安全威脅。

◆ 議題二：誘補系統(Honey pot)、郵件安全防禦(Spam trap)等

與談人： SPAMHAUS 代表 Denny Watson

本議題之與談人所代表之機構"SPAMHAUS"為一源於西元 1998 年起自瑞士日內瓦與英國倫敦之跨國、非營利之反垃圾郵件專門機構。該機構與政府機構、網路警察及各地 ISP 業者合作一同追輯專發垃圾郵件的駭客。近 20 年間，該機構將所蒐集到的垃圾郵件分為四大類：

1. Spamhaus Block List(SBL)、
2. Exploits Block List(XBL)、
3. Policy Block List、
4. Domain Block List。

因其專業性與即時性，各大郵件服務商、大型公司團體、大專院校、政府機構乃至於軍事單位等均採用 SPAMHAUS 的資料庫服務。SPAMHAUS

於十八個國家設置超過六十個伺服器以提供每天超過數十億之資料庫查詢人次，全球共超過十四億人之電子郵件信箱受惠於 SPAMHAUS 的反垃圾信機制之保護。

本議題中提及誘捕系統之基本介紹、類型與應用；其類型包括典型誘捕系統(Classic honey pots)、疆屍網路誘捕系統(Sinkholes)、就網路掃描與垃圾郵件進行反攻擊之系統(Tar pits)及垃圾郵件誘捕信箱(Spam traps)。其中，垃圾郵件誘補信箱之應用目的為：

1. 建立垃圾郵件反制之資料庫、
2. 惡意軟體研析與
3. 供執法單位使用之證據蒐集。

◆ 議題三：網路核心協定(Internet Core Protocols)

與談人：Internet Society 代表 John Levine

本議題以網路使用者平日收發電子郵件的動作來解釋網際網路核心協定(Internet Protocols)之定義、運作、資料流之傳輸及封包在網際網路傳送時的格式；另亦介紹網際網路最頂層之通用應用的資料報結構之應用層協定、邊界閘道協定(Border Gateway Protocol)，目的乃讓與會者可更清楚知道網路協定之運作。

(二) 「 倫敦行動計畫」及「反濫用訊息、惡意軟體、行動通訊工作群組」一般工作會議

◆ 議題一：倫敦行動計畫之基本方針

與談人：美國聯邦通信委員會(FCC)代表 Travis LeBlanc

本議題之與談人 Travis LeBlanc 為美國聯邦通信委員會執行局(the Bureau of Enforcement)局長；執行局為美國聯邦通信委員會最大局處，其轄下在美國地區包括 24 個區域辦公室。

本議題首先提及倫敦行動計畫於西元 2016 年至 2018 年間之優先戰略，

分別為：情資蒐集、執行面、優先溝通、優先訓練、評估之進行及會員間如何對倫敦行動計畫提供協助，各項大綱如下所示：

1. 情資蒐集方針：建立會員間之關鍵聯絡名單、登記資料之提供、各會員之情資工作小組合作及協調垃圾郵件與聯盟行銷(affiliate marketing)之打擊/掃除；
2. 執行面方針：各會員國之執行行動之協調與資料分享、合作協議書之簽訂；
3. 優先溝通方針：強化及重塑各會員間之資格與溝通管道。
4. 優先訓練方針：建立相同之訓練計畫、訓練會議之紀錄與專家名單之編制；
5. 評估之進行：評估就已設立之目標所採行的措施之可行性、會員國參與之可能性及是否合用；另蒐集各會員國之反饋並與各會員國進行討論。
6. 如何協助倫敦行動計畫：參與並支持各合作會議。

最後，與談人 Travis LeBlanc 表示，除了電子郵件、商業電子廣告郵件之大量增加，網路詐騙犯罪數量每年數據亦急遽上升，該等犯罪造成美國使用者極大損失，惟詐騙型態不再僅係侷限於網路詐騙，尚包括藉國際電話之回撥、手機短訊之回傳以竊取消費者之個人資料等。美國聯邦通信委員會非僅為一政府機關，其亦與各州進行合作，除了共同監管就詐騙之執法行動，例如：Paypal、Uber 等；亦進行軟體開發以幫助使用者免於網路詐騙。又因使用者跨及全球，故美國聯邦通信委員會亦會與其它相關國際機構進行合作，共同維護全球用戶之網路安全。

◆ 議題二：聯盟行銷之掃盪(sweep)與認識

與談人：澳洲通訊及媒體管理局(ACMA)代表 Bruce Matthews
美國聯邦貿易委員會(FTC)代表 Steven Wernikoff
英國資訊委員會辦公室(ICO)代表 Adam Stevens

本議程先由澳洲通訊及及媒體管理局(Australian Communication and Media Authority)之代表就「聯盟行銷」(affiliate marketing)進行說明，澳洲垃圾郵件法(Australia Spam Act 2003)並未定義「聯盟行銷」，惟一般係指網站 A，例

如部落格、購物平台、新聞網等，讓服務或商品之提供者 B 於其網站中置入行銷廣告，只要消費者點選該廣告並進入消費，雙方均可分享利潤的一種行銷方式。而聯盟行銷之主要角色為聯盟本身、聯盟網路與商人。因聯盟行銷常涉及複雜的運作網路，目前各國政府應思考於何時制定、制定何種相關法令來規範聯盟行銷以避免其發出過量之電子商業垃圾郵件，造成全球之經濟損失。

議程中邀請到荷蘭消費暨市場署(Authority for Consumers and Markets，"ACM")之代表分享荷蘭就管理聯盟行銷之法規經驗；ACM 所制定之垃圾郵件法為一行政法規，其具有罰款權力，ACM 代表闡述據統計今年已有超過 20 億封不請自來之商業電子郵件被發出，ACM 就其中部份垃圾郵件發出者已開出超過 81 萬歐元之罰單，且就荷蘭法院之判決，ACM 可將其開罰的名單公開予大眾周知。其它與垃圾郵件管理相關之法規尚有美國的「垃圾郵件管制法」(CAN-SPAM Act of 2003)、電信行銷規則(Telemarketing sales rules)等。

◆ 議題三：執行制度之建立

與談人：加拿大廣播電視及通訊委員會(CRTC)代表 Jeff Conard

與談人所代表之加拿大廣播電視及通訊委員會(Canadian Radio-television and Telecommunications Commission, "CRTC ")為一隸屬於加拿大工業部(Industry Canada)，專責管理加拿大國內所有廣播及電信市場的機構。CRTC 於西元 1968 年成立並取代前身「加拿大廣播電視委員會」之功能；其管轄範圍於 1976 年擴及於電信公司並改名為現稱。CRTC 有別於美國聯邦通信委員會，其管轄範圍並不包括技術性事務，若係有關頻譜核配、號碼發放、防止電波干擾等事務則是由聯邦工業局負責。

與談人於議程中介紹加拿大反垃圾郵件法(Canada's Anti-Spam Legislation, " CASL")，該法於 2014 年 7 月 1 日正式生效，旨在打擊網路釣魚、身份竊取及大量垃圾郵件，違反者個人可能面臨加幣 100 萬元之罰款；組織則為高達加幣 1,000 元之罰款；該法令不僅適用於電子郵件，其亦適用於透過社群軟體、短訊發送之電子訊息。其被視為現今世上最嚴厲之相關法令。CASL 係由加拿大廣播電視與通訊委員會、公平競爭局(The Competition Bureau)與隱私委員辦公室(Office of the Privacy Commissioner of Canada)共同執行，其中若是訊息與調查相關聯，以上三個單位可與外國政府共享資料。

參、與日本數據通訊委員會垃圾郵件防制中心代表之交流

時　　間：2016 年 10 月 25 日 10 時

地　　點：法國巴黎 Marriot Rive Gauche Hotel & Conference Center

與會人員：國家通訊傳播委員會 吳銘仁簡正、

國家通訊傳播委員會 李福懿技正、

財團法人電信技術中心 夏琬晴副規劃師、

日本數據通訊委員會垃圾郵件防制中心 西松 薰主任、

日本數據通訊委員會資訊安全組山口 岳人經理

討論內容摘述：

日本數據通訊委員會(下稱 JADAC)代表西松 薰先生為 JADAC 垃圾郵件防制中心主任，其為日本垃圾郵件主管機關－總務省委託辦理防制垃圾郵件事務之主辦機構首長，主要擔任諮詢指導業務，負責 Honeypot 資料分析、對 ISP 垃圾郵件資訊交換、國際合作及電話諮詢建議等垃圾郵件防制業務，其對防制垃圾郵件之相關技術與事務經驗相當豐富。

因西松 薰主任於 2011 年時曾至國家通訊傳播委員會訪問，本會首先就日本將其垃圾郵件處理程序介紹予台灣表達感謝之意，並說明本會將於 2017 年建置垃圾郵件分析中心及處理平台，規劃中該平台具有自動分析垃圾郵件之功能，預計於 2019 年啟用。西松 薰主任請本會描繪將建置之分析中心及處理平台之組織、流程簡圖及將來之執行單位之規劃與該單位是否具有執法權力等，藉以瞭解 JADAC 日後如何可提供何種協助予本會；會議中，西松 薰主任分享日本垃圾郵件處理程序及運作方式，其所提供之相關資料詳如附件二。

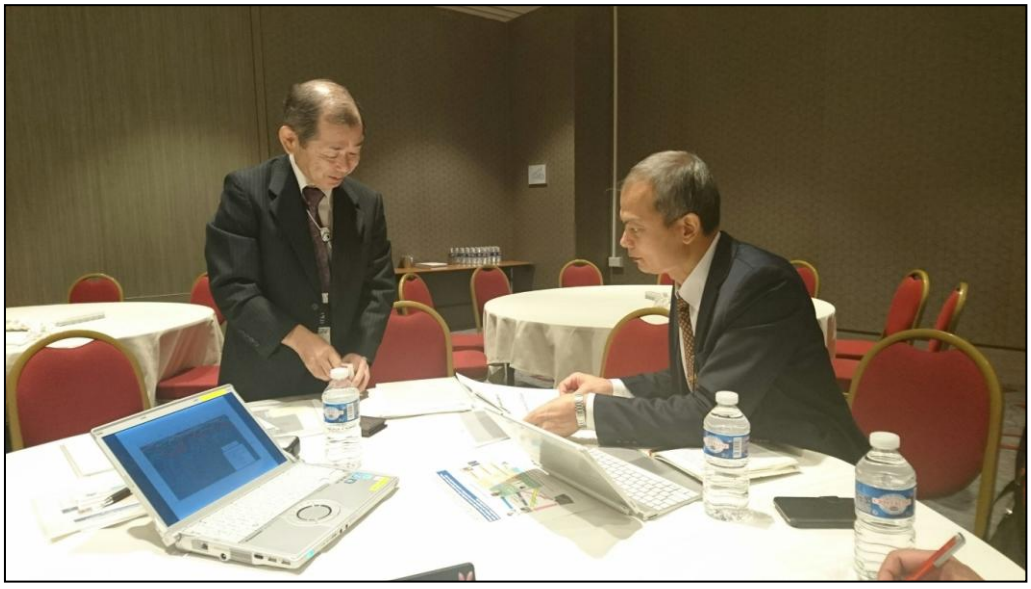
又，西松 薰主任出示自 2007 年以來日本誘捕系統(honeypot)所蒐集之垃圾郵件資料報告，報告中顯示自台灣發出之垃圾郵件比率極高，當中又以中華電信網路(Ninet)發出佔最大宗。西松 薰主任表示，希望台灣與日本可攜手合作，在日本收到台灣所提供之垃圾郵件發出者之資料後將進行分析，若其違反日本的「特定電子郵件傳送標準化法」，JADAC 將採取相關法律行

動；另西松 薰先生要求財團法人電信技術中心代表就該中心做簡單介紹並藉以瞭解其業務範圍及角色；西松 薰主任認為電信技術中心屬性與 JADAC 相似，日後可以簽署合作備忘錄，尋求合作之契機。

會中，本會詢問西松 薰主任關於日本是否有意簽署倫敦行動計畫於 2016 年 6 月 14 日所發佈之共同打擊垃圾郵件、詐騙及不請自來之商業電子郵件之國際合作備忘錄(相關資料詳見附件三)。西松 薰主任回覆為日本政府尚在考慮階段，因其認為該份合作備忘錄係開放予所有國家進行簽署，而日本政府認為簽署一份合作備忘錄應各別與欲進行簽署之國家當面討論，而非於未進行討論即簽署。

會議最後，日本 JADAC 表示期待日後更進一步與國家通訊傳播委員會之合作交流。

以下為會議剪影：



本會與日本數據通信協會進行交流(一)

本會與日本數據通信協會進行交流(二)

本會與日本數據通信協會進行交流(三)

肆、檢討與建議

隨著寬頻通信網路之發達及通訊軟體之使用普遍化，電子郵件、訊息成為商務網來之主要工具。然因不肖業者缺乏自律，大量不請自來之商業電子郵件、垃圾短訊與惡意軟體為害日深，除造成網路及電信服務提供商之系統極大的負擔外，其亦造成一般使用者偌大困擾。該等垃圾郵件、垃圾訊息及惡意軟體等已嚴重危害網路提供正常通訊的效能，造成個人、企業、國家乃至於全球經濟之鉅大損失。世界各國已紛訂立專法管制，本會重新研訂之「數位通訊傳播法」草案對於商業電子訊息已研議納入規範，建議亦應加速推動訂定。

2016 年 6 月 14 日所發布「共同打擊垃圾郵件、詐騙及不請自來之商業電子郵件」之國際合作備忘錄，目前已有 11 個國家簽署，我國是否簽署該合作備忘錄，執行所依法源是否充足，需進一步研議。與日本交流中，可知日本之垃圾郵件即時防制相關機制已相當完整，建議至日方實地考察，透過交流、學習日方長處，以提升未來本會建置垃圾郵件分析中心及處理平臺之效能。

「倫敦行動計畫」會議討論議題除垃圾郵件、廣告電話及商業簡訊管理、過濾、防護相關法律及技術問題外，已擴大至殭屍電腦網路造成個資隱私洩漏、網路攻擊及犯罪防制等，牽涉範圍亦涉消費者保護及網路犯罪等方面，建議未來得通知消費者保護及防制電腦犯罪等主管機關共同與會，促進跨國合作，提升我國國際關係。

附件一：第十二屆倫敦行動計畫年度會議議程

M³AAWG Messaging Malware Mobile Anti-Abuse Working Group

M³AAWG 38th General Meeting Training Program
October 24, 2016 - Paris, France

UCENet/LAP Executive Committee Breakfast, 9:00-10:00, Loft F (Level 3)

UCENet/LAP/UCENET Executive Committee Breakfast (Invite Only)
Please fill your plate in Loft ABCDE and then proceed across the hall to Loft F for your meeting. **Moderators: Melinda Claybaugh (U.S. Federal Trade Commission)**

What to See and Do Around Paris, 10:00-11:00, Forum ABC (Level -1)

Open to all meeting attendees and their guests: Come hear about the sights, sounds and all that has Paris has to offer. We will allow plenty of time for Q&A. **Speakers: Elytour Paris**

Chairs Town Hall (non-public, chairs only), 10:00-12:00, Scene DEF (Level 0)

All Chairs should attend this meeting as a final status check for sessions. The Town Hall is an forum for the chairs and significant contributors to talk about how we are doing as an organization. The current progress on the annual goals will be reviewed along with other items of importance to the organization. **Moderators: Michael Goldman (Facilitation First); Chairs: Mike Adkins (Facebook, M³AAWG Chairman), Jerry Upton (M³AAWG)**

UCENet/LAP Law Enforcement Only Training, 10:00-12:00, Forum GHIJ (Level -1)

UCENet/LAP Law Enforcement Training Session- Closed session for UCENet/LAP Law Enformcemnt members only. The aim of the UCENet/LAP training session is to provide attending Law Enforcement Agencies with a meaningful two hours, which looks to provide an insight into the work of the Australian Internet Security Initiative, an emerging economy spam case study from Africa, and [other item]. The session is designed to provide attendees with information from other jurisdictions that in turn generates discussion, operational insights, tips and ideas to "take-away", and points for future initiative and collaboration opportunities.
Moderator: Melinda Claybaugh (U.S. Federal Trade Commission)

Special Board Meeting (non-public), 12:30-14:30, Forum EF (Level -1)

This is an official Board of Directors meeting for Board members only.
Chairs: Mike Adkins (Facebook,M3AAWG Chairman), Jerry Upton (M³AAWG)

Honeypots, Spamtraps and more, 12:30-14:30, Forum ABC (Level -1)

Obviously, your spamtrap contains email, but what about all the other information in a trap that is going unexamined? In this session, you'll learn what metadata you can harvest from a spamtrap feed. We'll also talk about how to use the data you collect. **Speaker: Denny Watson (Spamhaus)**

Nowhere to Hide: Using Passive DNS To Find Spammer Infrastructure, 12:30-14:30, Scene DEF (Level 0)

Spammers often try to avoid public attention & rapid takedown by scaling their spamvertised websites out over hundreds - or even thousands - of different web sites. Anti-spammers find themselves facing the challenge of identifying & taking action against all those sites.
Learn how to use passive DNS to easily expose spammer infrastructure at scale, taking an initial spammer lead (such as a spamvertised web site) and then finding all related sites sharing common name servers, adjacent address space, etc. his is appropriate for anti-spammers, anti-phishers, those fighting malware & bots, and those who simply enjoy turning over rocks to see what lives beneath.
Speaker: Joe St Sauver (Farsight, Sr. Technical Advisor)

Internet Core Protocols, 15:00-17:00, Scene DEF (Level 0)

When you send an email, what actually happens? What is BGP? When you load a webpage, what is going on? Using daily internet tasks as a narrative, this training will explain in simple clear language the core protocols that make the internet work. Intended audience: people who are not deeply technical who must work with people who are, and would like to understand a bit more about it, or people that work a lot with one of the protocols and would like to understand the interactions better.
Speaker: John Levine (Internet Society, Sr. Technical Advisor), Carel (Spamhaus)

Teaming up to thwart phishers, 15:00 -17:00, Forum ABC (Level -1)

In honor of our UCENet London Action Plan guests, this participatory workshop will explore how law enforcement, brands, takedown services, ESPs and hosting providers can collaborate to reduce harm caused by phishers. By the end of the session we will know what actionable information is available, who to contact during an investigation, and how to ask for help so you're more likely to get the information you need. **Speakers: Paul Kincaid-Smith (SendGrid), Carlos Alvarez (ICANN)**
Audience: You should attend this workshop if you are a UCENet/LAP member, represent a phished brand, detect or block phish, or work for a takedown service, ESP or hosting provider and want to share or obtain information to thwart phishers.
Prerequisites: You have the willingness and ability to share and use information about phishers and phishing attacks. Before attending this workshop, please familiarize yourself with the UCENet/LAP's mission here: www.londonactionplan.org

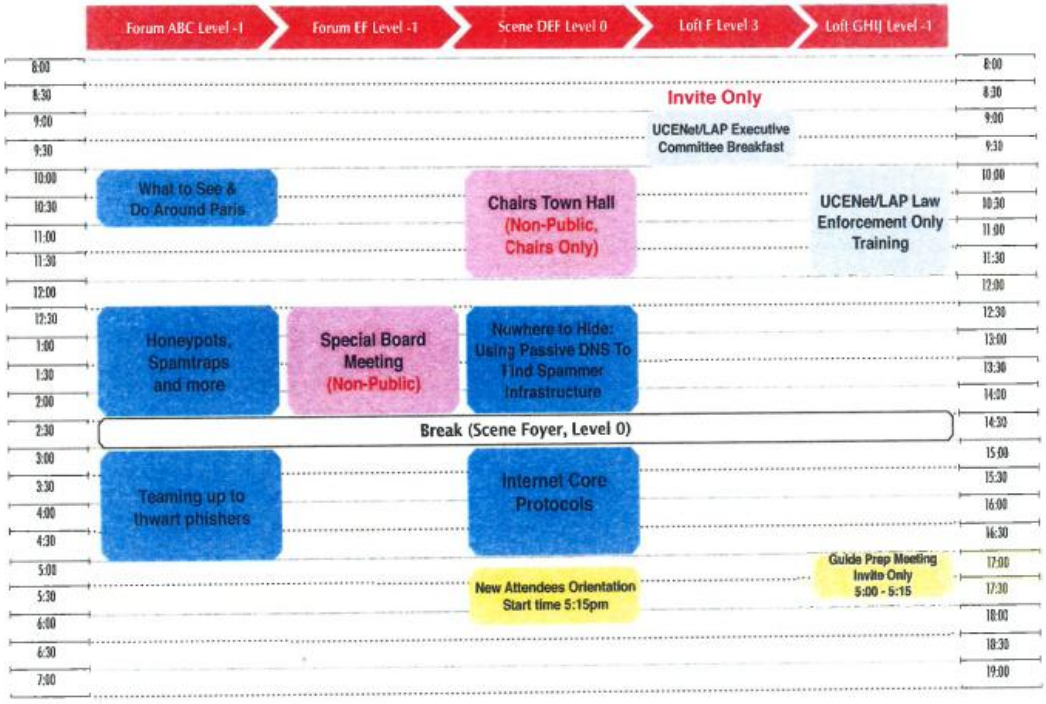
Guide Prep Meeting, 17:00-17:15, Forum GHIJ (Level -1)

A brief (15 minute) prep meeting for the Guides before the New Attendee Orientation starts. We'll discuss the goals of the guide program, and some items we hope you will discuss with your guidees. This is not just for current meeting Guides, but also for future potential Guides.
Presented by: Bill Wilson (M³AAWG Senior Privacy Advisor); Alyssa Nahatis (Adobe Systems Incorporated)

New Attendees Orientation, 17:15-18:15, Scene DEF (Level 0)

Unsure of what M³AAWG can do for you? Unsure of all the things M³AAWG actually does? Confused about how to participate? Overwhelmed by all of the possible sessions at a meeting? It doesn't matter if you are a sender, receiver, hosting company or a vendor supplying goods or services - the New Attendee Orientation session will help you navigate through the uncertainties of attending M³AAWG for the first time. M³AAWG is a series of ongoing conversations about topics that range from the obscure to the sublime--but mostly the obscure. Get a head start on the feel of the meeting and find out what's in store for this event, how the committees work, how to get the most out of your time here or just get some basic housekeeping questions answered in this orientation session. You can also learn about the M³AAWG "Guide" program and how you can tap the experience of seasoned conference veterans. **Chairs: Chris Roosenraad (M³AAWG)**

Monday, October 24th Training Program



M³AAWG Messaging Malware Mobile Anti-Abuse Working Group

M³AAWG 38th General Meeting Program
October 25 - 27, 2016 - Paris, France

Please have your badge visible at all times.
Lunch is Tues.-Thurs. are for attendees only in Loft ABCDEF (Level 3)

Tuesday, October 25th

Breakfast & New Attendees Meet-Up, 07:00-08:30, Loft ABCDEF (Level 3)
Breakfast is included in the Marriott hotel sleeping room rate.
M³AAWG meeting attendees staying at the Marriott can eat in the M³AAWG only breakfast room from 7:00 am -9:00 am in Loft ABCDEF, 3rd Level on Monday-Friday.
For new attendees you can get a head start on the feel of the conference, find out how the committees work, or just get some basic housekeeping questions answered while eating breakfast Tuesday-Wednesday with a few M³AAWG committee chairs and Board members at one of the clearly labeled "New Attendees" tables.
Guests/Family staying at the Marriott can enjoy breakfast in the R'Yves restaurant, 2nd Level beginning at 6:30 am - 11:00 am.

UCENet/LAP Opening Remarks-Executive Committee, 08:30-08:45, Forum ABC (Level -1)
Closed session for UCENet/LAP members only; for details, contact Melinda Claybaugh or the UCENet/LAP Secretariat.
Hear Opening Remarks by the Executive Committee to kick off the 2016 UCENet/LAP Annual Conference. **Speakers: Manon Bombardier (CRTC), Stephen Eckersley (ICC)**

UCENet/LAP Keynote, 08:45-09:15, Forum ABC (Level -1)
Closed session for UCENet/LAP/UCENET members only; for details, contact Melinda Claybaugh or the UCENet/LAP Secretariat.
CHIEF, ENFORCEMENT BUREAU, FEDERAL COMMUNICATIONS COMMISSION, USA
Travis LeBlanc is Chief of the Bureau of Enforcement at the Federal Communications Commission where he leads the Commission's largest organizational unit, including its 24 field offices around the country. **Speakers: Travis LeBlanc (US FCC)**

Participation Training- How to Contribute to the Work of M³AAWG, 09:00-09:45, Scene AB (Level 0)
How can we help make your involvement in M³AAWG more valuable? Addressing this question, we have developed a new Participation Training program and will be doing more "to keep the work in M³AAWG" flowing. We offer this training and tools so our members can participate, contribute and do more work. That will make our members' time here more productive and also better support the industry's needs. **Speakers: Jesse Sowell (M³AAWG Advisor)**
Chairs: Mike Adkins (Facebook, M³AAWG Chairman), Jerry Upton (M³AAWG)

The first UCENet/LAP Sweep-Affiliate Marketing-Understanding and Opportunities 09:15-10:30, Forum ABC (Level -1)
Closed session for UCENet/LAP/UCENET members only; for details, contact Melinda Claybaugh or the UCENet/LAP Secretariat.
During the 2015 UCENet/LAP event in Dublin, the membership committed to undertaking our first 'Sweep' exercise, focusing on affiliate marketing. The Sweep should broaden participants' understanding of the topic and establish opportunities for follow-up activity. This session will introduce the Sweep and seek feedback, as well as providing a snapshot of work going on in different jurisdictions in relation to the topic.
Speakers: Bruce Matthews (ACMA), Jeff Conrad (CRTC), Steven Wernikoff (FTC), Adam Stevens (ICO)

Networking with Chairs- How to Contribute to the Work of M³AAWG, 09:50-10:30, Scene AB (Level 0)
New and veteran attendees are invited to join this interactive session. Come talk directly with the committee and SIG chairs to contribute directly to success of M³AAWG! The session will have 3 10-minute small group sessions of your choice to interact directly from the committee/sig chairs about work that is actively going on in their respective areas, and how you can participate and become involved. Also, this can be an opportunity to suggest work to the chairs. This is a great way to

Chairman's Opening & J.D. Falk Award, 11:00-12:00, Scene AB (Level 0)
Meeting Welcome. In 2011 the world lost a champion and dedicated anti-spammer who spent his life making the Internet a safer place for everyone. This award, in honor of J.D. Falk's work and memory, seeks to recognize people who are committed to a better online world and protecting end-users from all forms of abuse.
Chairs: Mike Adkins (Facebook, M³AAWG Chairman), Jerry Upton (M³AAWG)

UCENet/LAP Working Group, 12:00-13:00, Loft G (Level 3)
Lunch Working Group for UCENet/LAP attendees only.
Moderators: Melinda Claybaugh (U.S. Federal Trade Commission)

Marketing Committee BoF, 12:00-13:00, Loft H (Level 3)
The new 2016-2017 M³AAWG goals were announced in Philadelphia. Join us to brainstorm how we can support these efforts. We want your input on new marketing ideas, and hopefully, your continued involvement. Please also invite any marketing, public relations or social media people in your company you think should participate. For information, contact Linda Marcus, M³AAWG public relations, at LMarcus@ustrat.cc and M³AAWG Executive Director Jerry Upton at jerryupton@M3AAWG.org. We're looking for all marketing types, bloggers and social media troupers, with or without experience, from anywhere in the world.

UCENet/LAP Mission Presentation to M³AAWG, 13:00-13:30, Scene AB (Level 0)
Open to all attendees
Since the Annual Meeting in Dublin, Ireland in June 2015, UCENet/LAP has merged with the International Do Not Call Network and members undertook a rebranding exercise to identify a new name and new priorities moving forward. A UCENet/LAP Operational Plan was drafted and activities were identified focused under 4 pillars, namely: 1. Intelligence 2. Enforcement; 3. Communications; and 4. Training.
Attend this presentation to hear from the UCENet/LAP Executive Committee on these priorities and learn areas where your expertise could integrate into the work UCENet/LAP undertakes.
Speakers: Manon Bombardier (CRTC), Stephen Eckersley (ICC), Melinda Claybaugh (U.S. Federal Trade Commission)

Fraud as a Service: Criminal Email Campaigns for Fun and Profit, 13:30-15:00, Scene AB (Level 0)
Phishing, account takeover, malware distribution, criminal recruitment campaigns...what's a fraud, compliance, or security manager to do? The biggest leap is in seeing that these activities are interconnected, with ESPs at the epicenter. **Speakers: Lawrence Baldwin (MyNetWatchman), Jen Fogarty (Career Builder), Patricia Andrews (Constant Contact)**

RPZ (Response Policy Zone), 13:30-15:00, Scene C (Level 0)
Response Policy Zone (RPZ) is a technology that was created nearly a decade ago, yet has not been adopted by the internet community at large.
This session will discuss the technology behind RPZ, a practical application of the technology by hosting providers, and the future of RPZ as discussed by those who created it.
Moderators: Matt Stith (Rackspace); Speakers: Vernon Schryver (Rhyolite), Raymond Dijkxhoorn (SURBL), Matthias Seitz (SWITCH), Paul Vixie (Farsight Security); Chairs: Carel (Spamhaus)

UCENet/LAP Lessons Learned - Setting up an Enforcement Regime, 13:30-15:00, Forum ABC (Level -1)
Closed session for UCENet/LAP members only; for details, contact Melinda Claybaugh or the UCENet/LAP Secretariat.
Hear from enforcement agencies in Canada and the United Kingdom as they describe the challenges they faced in establishing and operating an anti-spam compliance regime, an in-house intelligence "hub" and a new Do Not Call regime. Gain an appreciation of the complexities of setting up compliance enforcement frameworks under different legal and cultural conditions, the lessons learned by the agencies and some best practices that can help mitigate and address common issues. Finally, hear how the agencies are working to build upon the progress made to date including building new partnerships and sharing experiences.
Speakers: Christianne Laizner (CRTC), Manon Bombardier (CRTC), Adam Stevens (ICO), Thezi Mabuza (NCC), Trevor Yeo (DPC)

Forums and Marketplaces Infrastructure Study, 15:30-16:30, Scene AB (Level 0)
Marketplaces, card shops, and forums are flourishing and enabling cyber criminals to find the tools and services they need. There are hundreds out there, welcoming thousands of cyber criminals every day. Marketplaces where you can find Netflix, PlayStation and other type of accounts. Card shops where credit card number are abundant, and lastly forums where cyber criminals can discuss, exchange ideas, and do business. This talk will cover a holistic picture of underground marketplaces, card shops, and forums, in terms of infrastructure using passive DNS data, services, venues, and goods being leveraged by cyber criminals. We will discuss where most of these places are hosted and for how long. Examining their movement from one provider to another, we will illustrate which provider can be considered good, bad, or ugly. Good will be the providers who try hard to clean their network and kick these types or places out of their network. Bad are the providers being a bit too lax in getting ride off these guys, while the ugly are the full-on bulletproof providers that are 99% bad. The security industry does a tremendous job at taking down these places but for some reason these places always find a new home elsewhere. A solution to circumvent these places from popping up is to elicit more awareness, more cooperation between different partners, and a fast response to take them down. **Speaker: Loucif Kharouni (Deloitte)**

Achieving Extensive Email Security with a Technical Guideline, 15:30-16:30, Scene C (Level 0)
The technical guideline "Secure E-Mail Transport" (BSI TR-03108) released by the German Federal Office for Information Security (BSI) targets an increase of securely transported emails by defining requirements and recommendations for email services. It's not the goal to create another high security closed shop, but rather focus on flexibility and scalability. For this purpose the technical guideline only requires the use of tried and tested technologies like TLS, DNSSEC and DANE/TLSA. The technical guideline was created with and already receives broad approval of email service providers as well as in media reports and internationally. **Moderators: Alex Brotman (Comcast), Janet Jones (Microsoft)**
Speakers: Florian Bierhoff (German Federal Office for Information Security (BSI)), Thomas Gilles (Federal Office for Information Security (BSI))

UCENet/LAP - Intelligence - back to basics: the definition of intelligence, processes and public/private partnerships' commonalities, 15:30-17:00, Forum ABC (Level -1)
Open to all attendees
Speakers will set the stage for the discussion with a theoretical concept of "intelligence" as defined in general, as applied in the regulatory enforcement context and as applied, more specifically, to cyber security. Attendees will listen to experts explore how the public / private partnership could work together while applying said conceptualization as understood by government (collection, retention, analysis and dissemination) and private sectors. The session will explore what the private sector may need in terms of information / intelligence to do its job, and what the public sector may need to pursue enforcement. Topical Privacy and Access to Information issues will also be canvassed by the panel.
Speakers: Daniel Roussy (CRTC), Dr. Doron Zimmerman (ISPIN Ltd.)

Implementing Flowspec for DDoS Mitigations, 16:30-17:30, Scene AB (Level 0)
BGP flowspec is a tool that can be used to assist in DDOS mitigation in a dynamic fashion, levering BGP. The most commonly used Service Provider security tool used today in order to deal with DDoS attack is to use BGP to redirect traffic to a discard interface (otherwise known as Remote Triggered Black Hole (RTBF)). This presentation talk strategies for scrubbing, blocking traffic, potential for BGP Flowspec peering. It will discuss about the Pros/Cons, good bad caveat in BGP flowspec deployment. **Introducer: Daniel Phan (Comcast); Speakers: Andrew Mortensen (Arbor Networks), Michael Sabbota (Arbor Networks)**

Improving security of email in transit by implementing SMTP MTA Strict Transport Security (STS), 16:30-17:30, Scene C (Level 0)
Deploying Opportunistic TLS is a good initial step towards securing email in transit, but, does not guard against man-in-the-middle (MITM) attack scenarios. During this session, authors and early implementers of the SMTP MTA Strict Transport Security (STS) IEFT Internet-Draft will provide a brief overview of the draft itself, give an implementation update, and discuss next steps. This idea and draft was created as part of the M³AAWG Pervasive Monitoring SIG roadmap.
Speakers: Keith Coleman (Fraudmarc), Nicolas Lidzborski (Google), Klaus Umbach (1 & 1)
Chairs: Alex Brotman (Comcast), Janet Jones (Microsoft)

Brand SIG (closed), 16:30-17:30, Forum GHIJ (Level -1)
Closed session for discussing items of interest specific to enterprise brands. If you are interested but not currently a part of the committee, contact the committee chairs at brands_sig-chair@mailman.M3AAWG.org. **Moderator: Ryan Boyd (Groupon)**

Wednesday, October 26th

Breakfast & New Attendees Meet-Up, 07:00-08:30, Loft ABCDEF (Level 3)
See Tuesday

ORT Day I, 08:30-10:30, Scene AB (Level 0)
Facilitated round table discussions, open to all M³AAWG members, where new ideas can be incubated and best practices discussed. Day1 collects input from as many people as possible about three of the topics that interest you. Day 2 builds on the collected input from Day 1 to decide on work that can be carried forward into future content and/or investigations.
Moderators: Vincent Schonau (Abusix), Michael Goldman (Facilitation First), Melinda Plemel (ORT Committee Chair)

Keynote: Catching Cryptocriminals made easier, 11:00-12:00, Scene AB (Level 0)
Law enforcement and private sector teaming up to hunt down ransomware criminals and giving victims their locked files back for free.
How a single ransomware investigation led to a worldwide public-private platform that actively fights ransomware. **Speaker: John Fokker (Dutch National High Tech Crime Unit)**

Spamhaus Users BoF, 12:00-13:00, Forum ABC (Level -1)
Spamhaus users are invited to join Spamhaus team members at lunch for an informal discussion of our current data-sets, methods being used to prevent spam & abuse, and to go over ways where using Spamhaus in ones environment can be improved or upgraded. There will be time for questions and feedback from attendees.

UCENet/LAP Working Group, 12:00-13:00, Loft G (Level 3)
Lunch Working Group for UCENet/LAP attendees only.
Moderator: Melinda Claybaugh (U.S. Federal Trade Commission)

Training Committee BoF, 12:00-13:00, Loft H (Level 3)
All members are invited to join us during lunch and share your thoughts and ideas.
M³AAWG Training sessions have become an integral part of the value at our meetings. We are looking for additional participation from the M³AAWG membership to continue this momentum and ensure we are providing training on topics of interest to all M³AAWG attendees.
If you are unable to attend the BoF but have ideas for future Training Sessions, PLEASE submit your ideas here **https://M3AAWG.org/submissions**

What Would Recipients Vote to Receive?, 13:00-14:00, Scene AB (Level 0
As ISPs get more and more focused on making their users happy and blocking, throttling, or filtering mail, where do the political senders fit in? They need to cater to the same rules as common retail marketers, and we are looking at multiple factors to see if there are universal best practices in this domain. We'll also have the chance to see who is doing this right or wrong both in America and internationally!
Moderator: Jay Weiser (SendGrid); Speakers: Sven Krohlas (1&1), Jacob Hansen (SendGrid)

A Technical Overview of 2016 Trends in Malware Spam, 13:00-14:00, Scene C (Level 0)
This presentation will document and technically analyze some of the current trends in the malware spam landscape using real-world attacks as examples. Topics covered will include ransomware delivery and payloads, effects of law enforcement action against cybercriminals, evolving script-based attacks, document macro-based attacks, and social engineering techniques.
Speaker: Greg Leah (Cloudmark)

ARC - Unbreaking DKIM Signatures, 13:00-14:00, Scene DEF (Level 0)
The new ARC specification holds the potential of addressing a number of the problems with DKIM signature breakage that cause problems for DMARC authentication. If you are interested in this topic, please join some of the key contributors to the spec for an introduction and Q&A regarding the proposed standard.
Here's an introductory slide deck: http://www.slideshare.net/SteveJones250/overview-of-the-arc-protocol-for-email. **Speakers: Steven Jones (DMARC.org), Kurt Andersen (LinkedIn)**

List bombing and you and you and you and you, 14:00-15:00, Scene AB (Level 0)
Join us for an overview of bot sponsored list bombing and subsequent Spamhaus listings that many ESPs experienced over the summer (and continue to experience still). We will discuss how this started, how it was detected, long-term preventative measures and the unprecedented collaboration of the sender and anti-abuse community. After reviewing the problem from several angles we are excited to open the discussion to the rest of the room.
Moderator: Tara Natanson (Constant Contact); Speakers: Matthew Grove (MailChimp), Nancy Harris (Sailthru), Alan Murphy (Spamhaus)

DDoS Honeypots, 14:00-15:00, Scene C (Level 0)
The recent amplication DDoS attacks have swamped victims with huge loads of undesired traffic, sometimes even exceeding hundreds of Gbps attack bandwidth. We analyze these amplication attacks in more detail. First, we inspect the reconnaissance step, i.e., how both researchers and attackers scan for amplifiers that are open for abuse.
Second, we design AmpPot, a novel honeypot that tracks amplication attacks. We deploy 21 honeypots to reveal previously-undocumented insights about the attacks. We find that the vast majority of attacks are short-lived and most victims are attacked only once. Furthermore, 96% of the attacks stem from single sources, which is also confirmed by our detailed analysis of four popular Linux-based DDoS botnets. **Speaker: Dr. Christian Rossow (MMCI Saarland University)**

Emerging global encryption debate / Privacy approaches across the globe, 14:00-15:00, Scene DEF (Level 0)
All things privacy. The "gate-keeper" criterion for privacy and personal data laws: How is the scope of personal data evolving, and what are the implications? Personal data crossing borders: A sample of different approaches. Privacy challenges and opportunities: surveillance, encryption, data portability, data breaches. **Moderators: Alex Bratman (Comcast), Janet Jones (Microsoft)**
Speaker: Christine Runnegar (Internet Society)

Mitigating DKIM replay attacks, 15:30-16:30, Scene AB (Level 0)
Since early September 2016, a new attack methodology has emerged to take advantage of DKIM signatures generated by legitimate providers and the corresponding DMARC/domain reputation that can be inferred from that valid DKIM signature.
Abusers are sending spam/phish messages to accounts under their control and then turning around and bleeding a replay of that message to different 5321 recipients via botnets.
A number of different providers will participate in the panel to describe details of what they are seeing and challenges to mitigating these attacks. **Moderator: Kurt Andersen (LinkedIn)**

Mechanisms of Abuse Reporting, 15:30-16:30, Scene C (Level 0)
Many conversations have occurred around how to make abuse reporting more efficient for all parties throughout the Internet ecosystem.
Join us for a workshop on how we can advance and centralize standards and protocols. We will also focus on how we can work towards broad acceptance of whatever standards are ultimately set. **Moderators: Justin Lane (Bluehost-Endurance), Matt Stith (Rackspace)**
Speakers: Michele Neylon (Blacknight); Chairs: Neil Schwartzman (CAUCE)

Public Policy Updates, 15:30-17:30, Scene DEF (Level 0)
Public Policy Committee updates on North American and European Regulatory items.
Plus updates on Quantifications of Damages, Information Sharing SIG work, Metrics reports, Committee work items and in-process documents for review/approval.
Moderators: Jerry Upton (M³AAWG), Chris Roosenraad (M³AAWG)

Honeypot Panel, 16:30-17:30, Scene AB (Level 0)
This panel discussion will cover the benfits that can be found in running Honeypots within your network.
There are many types of Honeypots available. What data can you glean from these? Is it actually helpful? We will break down some types along with the purpose they serve and will review some technical data on findings that have come from a few real world Honeypot installations.
Speakers: Tobias Knecht (Abusix), Dr. Christian Rossow (MMCI Saarland University) Richard Clayton (Senior Technical Advisor)

Hosting (closed), 16:30-17:30, Scene C (Level 0)
Closed session for hosting committee. If you are interested in participating, contact the committee chairs. **Moderators: Matt Stith (Rackspace), Justin Lane (Bluehost-Endurance)**

Anti-Phishing SIG Working Session, 16:30-17:30, Scene GHIJ (Level 0)
This will be an open working session to build off of what was started in Philadelphia (June 2016). A chance to hammer out what exists for reporting phishing and what hurdles folks have in sharing phishing-related information. **Moderators: Carlos Alvarez (ICANN), Nancy Harris (Sailthru)**

M³AAWG Night Out, 17:45-22:00
Meet in the hotel lobby at 5:45pm/1745
A Great Evening of Networking, Food and Fun at Le théâtre du merveilleux : http://www.pavillons-de-bercy.com/EN/theatre-merveilleux.htm
Sponsored by Vade Secure. You MUST have your M³AAWG badge or a guest pass to attend.

Thursday, October 27th

Breakfast, 07:00-08:30, Loft ABCDEF (Level 3)
No New Attendees Breakfast tables.

UCENet/LAP (Law Enforcement Only) Enforcement Panel, 08:30-09:30, Forum ABC (Level -1)
Closed session for UCENet/LAP members only.
This panel will focus on recent trends and actions relating to Do Not Call enforcement. Representatives from the US Federal Trade Commission, the UK Information Commissioner's Office, and the Australian Communication and Media Authority will discuss experiences with domestic and international enforcement cooperation, enforcement of self-regulatory codes of conduct, and development of internal regulatory action policies.
Moderator: Melinda Claybaugh (U.S. Federal Trade Commission)

ORT Day 2, 09:00-10:30, Scene AB (Level 0)
Facilitated round table discussions, open to all M³AAWG members, where new ideas can be incubated and best practices discussed. Day2 collects input from as many people as possible about three of the topics that interest you. Day 2 builds on the collected input from Day 1 to decide on work that can be carried forward into future content and/or investigations.
Moderators: Vincent Schonau (Abusix), Michael Goldman (Facilitation First), Melinda Plemel (ORT Committee Chair)

UCENet/LAP (Law Enforcement Only) Intelligence-driven Enforcement, 09:30-10:30, Forum ABC (Level -1)
Closed session for UCENet/LAP members only.
This session will focus on the information, processes and tools that can be used to implement an intelligence-driven approach to law enforcement based on the experience of UCEnet member agencies, and will serve as a launching point for the UCEnet Intelligence Working Group.
Speaker: Jeff Conrad (CRTC)

I'll take purchased lists for 500, 11:00-12:00, Scene AB (Level 0)
As corporate hacks become more common, we are seeing extremely large and active email lists enter the "list for sale" market. What impact do these lists have on sender reputation, and how do we change our purchased list detection algorithms in the wake of such highly pervasive lists. **Speaker: Matt Mastin (MailChimp)**

Ready, Set, Wait, 11:00-12:00, Scene C (Level 0)
This session is a continuation of discussions that began in San Francisco and continued into Philly. In Paris we will be focusing on the European perspective with regards to Rate Limiting, specifically, Senders and Receivers will communicate about the necessary connection and volume settings to deliver mail timely without being abusive.
Moderator: Andre Goermer (MAPP); Speakers: Anthony Mitchell (MAPP), Tobias Herkula (optivo GmbH)

Identity SIG Document Working Session, 11:00-12:00, Scene DEF (Level 0)
Markup and discussion of in-process SIG documents. All interested M³AAWG attendees invited to attend and participate.
Moderator: Ico St Sauver (Farsight, Sr. Technical Advisor)

UCENet/LAP (Law Enforcement Only) Detecting Unsolicited Communications Using Honeypots, 11:00-12:00, Forum ABC (Level -1)
Closed session for UCENet/LAP members only.
Panelists will share their agency's experience in establishing various types of honeypots, and in leveraging them to support their enforcement activities. We will explore the associated opportunities and challenges. **Speaker: Jeff Conrad (CRTC)**

Tech Chairs Working Lunch, 12:00-13:00, Loft G (Level 3)
Working lunch for the technical committee and subcommittee chairs and vice-chairs only

Collab Chairs Working Lunch, 12:00-13:00, Loft H (Level 3)
Working lunch for the collaboration committee and subcommittee chairs and vice-chairs only

Protecting a Country from Abuse, 13:00-14:00, Scene AB (Level 0)
The UK has a new National Cyber Security Strategy and a new National Cyber Security Centre. Part of the strategy is to make email much harder for attackers to abuse. Ian will talk about what the UK is doing, what effect he thinks these actions will have and - more importantly - what we need to be ready for in the future. Ian is going to ask for M³AAWG members' help in getting the ecosystem ready to better defend against future attacks.
Moderator: Janet Jones (Microsoft); Speaker: Ian Levy (UK NCSC)

How WhatsApp Reduced Spam while Launching End-to-End Encryption, 13:00-14:00, Scene C (Level 0)
End-to-end encryption, which protects message content so that only the sender and recipient can access it, is gaining popularity in messaging applications. At the same time, there is some concern about its deleterious effects on spam detection systems. At WhatsApp we have successfully launched such "e2e" encryption for over 1 billion people - while also reducing the amount of spam they receive. This talk will discuss techniques we've found successful for preventing spam without access to message content, and some of the challenges we faced along the way. It should help dispel concerns that e2e encryption necessarily means reduced effectiveness of spam detection. **Introducer: Trent Jason de Luna (Technical Mobile Co-Chair); Speaker: Matt Jones (WhatsApp)**

ICANN's Identifier Technologies' Health Indicators (ITHI), 13:00-14:30, Scene DEF (Level 0)
ICANN has started a new initiative called "Identifier Technologies' Health Indicators", or ITHI. The intent is to analyze systemic risks to the unique identifier systems, define metrics to measure them and track those measurements over a long period of time. This initiative is developed in collaboration with the various concerned communities. ICANN would like to present ITHI to the M³AAWG membership and seek feedback from the participating subject matter experts on questions related to the domain name industry, its operations and the criminal or malicious uses of domain names. **Speaker: Alain Durand (ICANN)**

VTA SIG: Robocall Strikeforce!, 13:00-14:00, Forum ABC (Level -1)
The US Robocall Strikeforce is by far the most significant anti-robocall effort of the year if not the decade. Over 300 government and industry experts in anti-abuse technology, engineering, communications standards, law, policy and enforcement have assembled to respond to the challenge of producing a comprehensive action plan to significantly reduce robocalls. But it's produced more than a plan. Its actions are already making a dent: implementation of secure caller ID to defeat spoofing, "Do Not Originate" phone number lists, collaborative traceback, consumer choice and joint industry government action against robocallers. Strikeforce participants Antonio Sweet of the US Federal Communications Commission and Alex Bobotek of AT&T (which chairs the Strikeforce) will describe the Strikeforce plans and actions that are helping to stop robocalls. **Moderator: Alex Bobotek (M³AAWG); Speaker: Antonio Sweet (US Federal Communications Commission)**

The Call is coming from inside the house, 14:00-15:00, Scene AB (Level 0)
The true story of a organic 600,000 person email list and how it turned in to a monster fed by good intentions and the siren's song of vanity metrics. How a cross team effort brought a vital list back from the brink by prioritizing the recipients and their expectations above all else.
Speaker: Tom Monaghan (HubSpot)

SSDP Case Study Analysis, 14:00-15:00, Scene C (Level 0)
Simple Service Discovery Protocol (SSDP) reflection and or amplification is a type of Distributed Denial of Service (DDOS) attack that leverages port 1900/UDP and in which the bad actor spoofs the source IP address so that responses are returned to the intended target. SSDP based reflection attacks yield on average a bandwidth amplification factor of 30.8 . In other words the response can be 30 times larger than the request. In most cases the attack is meant to disrupt the target's internet service(s) by flooding the IP device with unsolicited network traffic and or a high volume of packets. This type of attack is possible because devices, typically Customer Owned and Managed (COAM), contain vulnerabilities that permit the device to be leveraged by the attacker. In many cases the owner of the COAM device is unaware of what is going on, and as such, cannot know to attempt to remediate the issue. On March 20, 2016 the Shadowserver Foundation identified approximately 10.5M distinct IP addresses globally that responded to SSDP probes. Comcast has approximately 12M distinct IP addresses (or customers) comprising 18% of the global population and 23.7% of the US population. Approximately 92% of the Comcast IP addresses probed by Shadowserver belong to residential Internet customers, 5% to business/commercial customers and 3% as undetermined. From a network perspective SSDP ranks sixth in terms of DDOS traffic volume. Given the analysis, exposure and risk it is recommended that the business and engineering stakeholders strongly consider blocking SSDP in order to protect customers and the Internet community in general. **Speaker: Nirmal Mody (Comcast)**

VTASIG: European Perspectives on Telephony Abuse, 14:00-15:00, Forum ABC (Level -1)
Hear the inside story and experience of France's 2016 implementation of the "Bloctel" Do Not Call system, case studies in robocalls, and an update from European regulators.
Speaker: Ann-Valerie Heuschen (Voxbone)

The Current State of Email Authentication: A European Perspective, 15:30-16:30, Scene AB (Level 0)

There has been a lot of movement by US-based ISPs towards "No Auth - No Entry" enforcement of email authentication. But Europe is a very different market with different concerns and requirements. This session will discuss the perspective of several major European ISPs and Government Officials, and their adoption and enforcement of email authentication. What do these steps really mean for ESPs, Senders, and the Ecosystem? Join us to hear exactly what they're doing and what the real world impact will be on you. **Moderators: Alexander Garcia-Tobar (Valimail); Speakers: Sven Krohlas (1&1), Carmen Piciorus (UCENet/LAPoste), Jan-Pieter Cornet (XS4ALL), Ian Levy (UK NCSC)**

Plan, Pray or Play, 15:30-16:30, Scene C (Level 0)

How to create a threat intel practice and where to expand such activities to enrich the existing remediating efforts within any firm with goal to focus on identification, profiling of threat actors for a larger effectiveness and disruption of the attacks. The goal is to stop the fingers operating behind the keyboard and not just the attacks due to the persistence element. **Speaker: Christian Karam (UBS)**

Partnerships in Anti-Crime, 15:30-16:30, Scene DEF (Level 0)

This panel examines how a public/private partnership can collaborate to fight spam and cyber-criminal threats by allowing end users, ISPs and ESPs work together. Signal Spam, a non-profit organization located in France, pairs technology and industry partnerships to identify sources of spam which are then shared with mailbox providers to allow them to take action. And in exchange, mailbox providers provide Feedback Loops for those email senders that abide by the strict rules. This session will focus in on how partnerships like Signal Spam help Senders and mailbox providers work together to help address the overall spam problem. **Speakers: Eric Freyssinet (Signal Spam), Thomas Fontvielle (Signal Spam)**

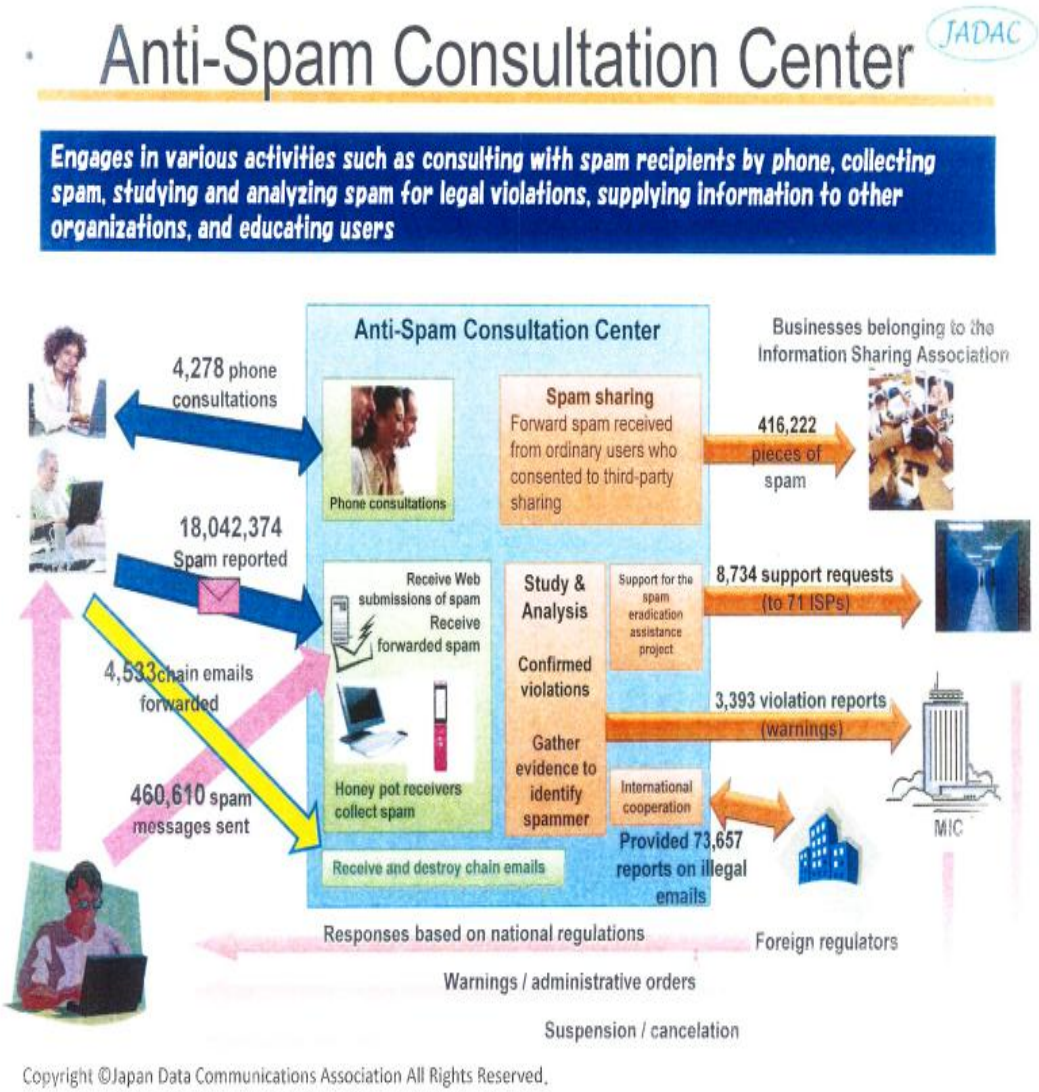
VTASIG: Securing Telephony and US Regulatory Update, 15:30-16:30, Forum ABC (Level 0)

Both the IETF and ATIS have been working diligently to develop authentication standards and implementation profiles that let you know who's really calling. Jim McEachern of ATIS will describe recently-compiled standards and profiles for cryptographic signing and validation of caller ID. Following this, Robert Finley (FCC) and Janice Kopec (FTC) will provide an update on key regulatory actions that have contributed to the control of illegal and unwanted robocalls and text messages. **Moderator: Robert Finley (Federal Communications Commission)**

Chairman's Closing, 16:30-17:30, Scene AB (Level 0)

Meeting closing with Committee/SIG highlights and a brief set of important announcements. **Chairs: Mike Adkins (Facebook, M³AAWG Chairman), Jerry Upton (M³AAWG)**

附件二：日本 JADAC 提供資料(Anti-Spam Consulation Center)



COMMITMENT TO INTERNATIONAL COOPERATION: LONDON ACTION PLAN MEMBERS SIGN MOU

June 14, 2016
Filed under General

The fight against the global scourge of spam, scams and unsolicited messages and calls has stepped up, with the announcement of a memorandum of understanding (MoU) signed by 11 enforcement authorities across the globe.

The enforcement authorities are all members of the London Action Plan, which coordinates and promotes international cooperation and activities targeting unlawful spam related problems—such as online fraud and deception, phishing, and dissemination of viruses—as well as unsolicited calls and texts.

The MoU demonstrates the commitment among the signatories to reinforcing cross-border cooperation to address unwanted messages and calls. By providing a framework for information and intelligence sharing among enforcement agencies around the world, the MOU strengthens the international fight against a global problem.

The MoU complements the London Action Plan, whose broader membership includes regulators, law enforcement agencies and industry organisations that are active in countering spam, unsolicited calls and texts.

The current 11 signatories include:

- Australian Communications and Media Authority
- Canadian Radio-Television and Telecommunications Commission and Office of the Privacy Commissioner in Canada
- Korea Internet & Security Agency
- Authority for Consumers and Markets in the Netherlands
- Information Commissioner's Office and Citizen Advice (consumer arm) in the United Kingdom