出國報告（出國類別：參加國際會議）

「網路犯罪專家小組續行會議(SPSG)」會議紀錄暨報告

服務機關：臺灣臺北地方法院檢察署
姓名職稱：檢察官 張友寧
派赴國家：馬來西亞
出國期間：100 年 9 月 21 日至 28 日
報告日期：100 年 11 月 30 日

「網路犯罪專家小組續行會議(SPSG)」
會議紀錄暨報告

臺灣臺北地方法院檢察署
檢察官張友寧

一、與會目的及專家小組背景說明：

本次係奉派參加 APEC TEL44 之「網路犯罪專家小組續行會議(SPSG)」會議。

本專案小組為依 APEC TEL 工作小組下的安全暨繁榮指導分組（SPSG）指令所設置之專家小組（experts' group），其目的係透過整合 APEC 各經濟體之執法人員，就網路犯罪之各種相關議題，如：立法、執法程序、執法人員專業訓練等議題加以研商之組織。本次會議主要之議題係針對社交媒體（如 Facebook、twitter、youtube）的應用在各國引發的問題應如何規範進行討論。馬來西亞代表提案，擬針對網路內容與社交媒介訂規範，要求業者或服務提供者介入內容審查，以預防犯罪，並提議於 2012 年底各經濟體達成共識、簽訂公約。

二、會議議程：

本次會議與電信監理會議（LSG）合併舉行，其討論之議程大致如下：

時間	討論事項
0910	會議開始： 一、由專家小組的專案經理 Anthony V. Teelucksingh（美國籍）報告 二、選舉小組主席與副主席 三、討論並確認議程
0925	簡報：「網路犯罪專家小組設立背景及發展」 由專家小組主席 Anthony V. Teelucksingh 報告
1000	法規圓桌會議 主題：「社群媒體：新法規與政策？」 由馬來西亞代表 William 先生報告
1010	簡報：「網路犯罪的挑戰及難題：馬來西亞的案例研

	討」 由馬來西亞代表 Zul 先生報告
1110	簡報：「對檢察官有用的網際網路知識」 由美國代表 Anthony V. Teelucksingh 報告
1200	午休
1410	簡報：「電腦鑑識簡介」 由美國代表 James Silver 報告
1450	討論專家小組任務文件（Mission Statement）
1455	討論日後工作要項
1505	簡報：「國際合作模型」 由美國代表 Anthony V. Teelucksingh 報告
1545	SPSG 召集人致詞
1550	會議結束

三、會議討論內容：

（一）專家小組主席與副主席選舉：

經各國一致同意：由美國擔任主席、馬來西亞擔任副主席。

（二）簡報：「網路犯罪專家小組設立背景及發展」

1. 自 2002 年的「APEC 經濟領袖就對抗恐怖主義及促進成長宣言（APEC Economic Leaders' Statement on Fighting Terrorism and Promoting Growth）」 及同年「APEC 網路安全策略（ APEC Cybersecurity Strategy）」至 2005 年利馬的電信部長宣言（Lima TELMIN declaration）起，APECTEL 就不斷在促進亞太地區的網路安全議題。而透過對會員經濟體就網路犯罪立法的協助以及一系列區域性或雙邊的網路犯罪專家、執法人員、立法者之會議，亦獲致相當之成效。
2. 然而網路犯罪仍有 APEC 會員經濟體及世界各國之多管轄權（指不同司法管轄權間競合的問題）的挑戰；此一問題亦逐漸為各主要區域及聯合國所關注的議題。在 APEC 裡，最適合跨政府地成立處理此一問題專家小組的場合，就是 TEL 小組，尤其是 SPSG。因 TEL 在對網路犯罪的議題上已作出超過

10 年的努力，其中對立法者、執法人員、檢察官、法官的訓練課程，以及鑑識能量的建立均為持續發展所必需；然而近來的計畫則多因低參與率及需要特別場地等因素而受到阻撓。

3. 在中國杭州舉辦的 TEL 43 會議中，通過成立專家小組之決議，利用 TEL 會議之機會，作為執法人員及有關人員未來之訓練／研討會之場所，其主要工作係在協助有需要的會員經濟體達到通過符合 TEL 目標之網路犯罪立法及強化網路犯罪調查之能力。

4. 專家小組的目標包括：1.網路犯罪係指針對電腦或資訊運作之犯罪行為及使用電腦作為傳統犯罪行為方法等行為；2.檢視會員經濟體的法規、政策及實施狀況，確保能夠符合一定標準；3.使會員國的執法人員能夠擁有一定的調查能力，包含專責組織、提供與其他國家的聯絡窗口，在 APEC 組織內建立合作對抗網路犯罪的機制；4.使司法人員（法官、檢察官）有足夠能力對抗網路犯罪；使私領域的人員能注重資訊安全，達到一定的標準，使隱私權與調查案件的需求可以達到平衡。

5. 在方法上，專家小組將於 TEL 會議場地每年舉行一次 2 天之會議，使 APEC 會員經濟體內參與之執法人員及司法人員進行訓練、技術支援、以及籌畫對抗網路犯罪之合作方案等活動；同時，邀請業界的相關人員參與會議，並對合乎一定標準之 APEC 會員經濟體提供資金協助。

6. 目前已有部分會員經濟體進行相關活動，但多數都因為場地的問題沒有良好回應，因此需要相關的支援能量，甚至有需要透過聯合國簽訂網路犯罪相關條約之需要。

7. 簡報後汶萊代表提及：約 4～5 前在 APECTEL 小組內有一個網路犯罪專家之聯絡名單，此一名單會繼續使用或透過此一專家小組重新建立新的名單？報告人回應稱：美國就此並不清楚會再查明；但本專家小組的目標就在活化與網路犯罪有關之工作小組或聯絡名單，故仍會更新名單。

（三）法規圓桌會議：「社群媒體：新法規與政策？」

馬來西亞代表簡述了本次會議主要討論的問題係社群媒體的興起，對於法規及政策面所造成的衝擊。接下來即由馬來西亞代表以該經濟體的二個具體網路犯罪案例進行說明。

（四）簡報：「網路犯罪的挑戰及難題：馬來西亞的案例研討」

1. 案例一：虐狗事件（Dog Abuse Case）

   某人將其虐狗的影片放在 facebook 上（如下圖一），

（圖一）

   引起網友不滿，即進行人肉搜索（manhunt），並設置要求將虐狗者監禁的粉絲專頁（如下圖二）。

（圖二）

2. 案例二：侮辱伊斯蘭教案件

   有人將女神卡卡的照片與伊斯蘭教聖地建築的照片合成，看起來就像是卡卡坐在伊斯蘭教聖地建築物上，因而引發侮辱伊斯蘭教之事件。

3. 以上二案例都是利用社群媒體（如 facebook, twitter）作為散布仇恨的平台，甚至因為誤認身分而使得無辜的人受到騷擾的情形。在案例一情形，涉及在網路上進行人肉搜索是否犯罪的問題；如案例二，在馬來西亞則引起政治上的問題，因為馬國為伊斯蘭教國家，上開行為引發廣大民眾的不滿，要

求政府處理，然而其他國家不一定認為這有侮辱，因此在跨文化的情形下，如何處理也是一大問題。

4. 此外簡報中還提及法規修改及進一步發展的建議等議題：其中法規修改部分，馬來西亞的簡報中提出四個面向：司法／程序／調和／MLA，詳如下圖三。

（圖三）

5. 而在日後發展的建議部分，馬來西亞於簡報中建議建立處理網路犯罪的指導原則或標準作業流程，並提出相關時程的建議，如下圖四。（即在 2012 年第一季設立工作小組、第二季起草相關內容、第三季進行編修、第四季定稿並由會員經體簽署。）

（圖四）

6. 討論：

A) 美國代表：簡報內所提及的問題在美國並不存在，因為美國基於言論自由，不管制網路上的言論，案例中的情形係以傳

統誹謗行為透過民事訴訟處理，並無立法管制。美國在此方面較關注於教育消費者避免成為被害人。就使社會感到不安的網站案例部分，美國因其憲法增修條文第一條（即言論自由）之規定，無法提供協助，但美國對於任何協助的請求均嚴肅對待，上開案例情形，經由私人企業協助較重要，但國際企業（如 google, facebook 等）美國也無法全面規範，但多數企業已經體認應與世界各國合作極為重要，如 google 已配合許多國家進行犯罪調查，另有一些企業提供有關資訊安全方面之教育課程。

B) 馬來西亞代表：提出的案件在馬國引發成政治問題，因為民眾期待政府在上開案件中作出處理，而馬來西亞是多元文化國家，不同文化間的議題極為敏感，政府必需就某些特定類型的言論加以管制，除上述情形外，馬國原則上也是不管制言論的。另 google、facebook 等社群媒體影響力是很大的，以上所提及的案例，馬來西亞政府透過自己的方式解決了，但國際合作在上面的案例中是很重要的一環。馬來西亞政府希望能夠透過 APECTEL 給予私人業者如 facebook/google 一些與會員經濟體合作之標準作業程序或綱領。

C) 美國代表：同意應建立標準作業流程及指導綱領是有幫助的，但私人企業有其公司政策，我們認為將這些私人企業邀請至 APECTEL 一同參與，看其是否能提供協助較妥。

D) Axiata（私人企業）代表：馬來西亞提出的第一個案例是證據的問題，即人肉搜索得到的東西能不能作為使用的問題。另取得的證據係存在於境外，使得證據無法在訴訟中呈現也是一個問題；第二個案例則是行為是否犯罪的問題，這需要共識，所以就需要有一些立法，有規範才比較可能進行處理。

E) 泰國代表：泰國近來在面對類似案件時在出於不得已的情形下，也會採取較強勢的措施，但原則上泰國也不管制相關的言論內容。

F) 菲律賓代表：菲國也不管制網路言論的內容，菲國目前尚無網路犯罪相關法律，但已提案至國會立法中。

G) 馬來西亞代表：馬來西亞並未嚴格管制言論內容，但在國家安全的要求下，會監視並蒐集相關資訊以提出相應的防範措施。

H) 美國代表：美國在兒童色情、為犯罪行為募集資金部分的情形會對言論內容進行管制。但此部分的管制較傾向犯罪行為

的管制，但會對內容部分造成管制的效果。另一種案例是網路跟蹤（Cyberstalking），我們認為這是一種騷擾的案型，但此案的發展仍有待觀察；美國嚴肅看待社群媒體的濫用的議題。

（五）簡報：「對檢察官有用的網際網路知識」

1. 簡報詳細內容如附件一簡報檔。
2. 在美國電腦與房屋是不同的「場所」[1]，搜索時是需要另外取得令狀（在我國即搜索票）的，因此在聲請令狀時，必須向法院指明犯罪與電腦有關，且具有搜索的理由，始足當之，因此執法人員與司法人員有必要了解相關知識。
3. 接下來的簡報中，報告人先就網路、網際網路、伺服器、主從架構、何謂 isp（網際服務提供者）、封包及電腦傳送資料之方式、ip 位址及其如何配發、isp 紀錄檔（包括 ip 位址、用者登入時間、登入時期的時間 session duration 等）[2]名詞加以介紹，之後就偵查時會使用到的相關技術，包括以 ip 位址為線索開始，查詢 ip 配發予何人使用的技巧、以及追蹤 ip 位址時會遇到的困難，如使用無線網路、NAT 轉址、使用代理伺服器 proxy 隱匿行蹤、並舉出自電子郵件的表頭中的資訊查詢發信人為例，說明上開技巧如何使用。
4. 接著，報告人又就網路犯罪的各種面向加以說明：(1)駭客行為：其目標在破壞電磁紀錄之憑信性、完整性、可用性及使用；(2)電腦漏洞及利用漏洞進行的攻擊，而電腦漏洞常見於伺服器作業系統及軟體、一般軟體內；(3)殭屍電腦及殭屍網路：因為一個利用惡意程式進行的攻擊行為通常還會延伸出更多的攻擊，而遭惡意程式感染並取得電腦控制權限的電腦，我們就稱為殭屍電腦（bot），多數殭屍電腦透過網路連結後，就形成殭屍網路（botnet），而殭屍網路可以作為散發垃圾郵件，代理伺服器（隱匿行蹤之用）、攻擊、感染、製造更多的殭屍之用。

[1] 在我國並未做如此區分，而是以有沒必要搜索電腦及扣押電磁紀錄做為判斷標準；又在我國聲請搜索票並未如美國一般需要另行聲請，但仍需要聲請書內具體指明要搜索之客體包含電磁紀錄（即電腦或儲存媒體內所存放，以 0 與 1 型態儲存之資料）。

[2] ISP 的紀錄檔保存時間是一件重要的事，執法人員都會希望業者能保留的愈久愈好，但 ISP 業者能保存的期間，則受到消費者隱私的要求及設備成本的因素影響。這部分依本人淺見，似有以相關法令規範的必要。

5. 最後，報告人則就點對點（peer to peer, p2p）網路予以介紹，除了說明何謂 p2p 網路外，另外也介紹了集中式與分散式 p2p 網路的運作原理，而 p2p 網路的偵查，則多是透過臥底偵查的方式進行（即將偵查者的電腦加入 p2p 網路後，再自該台電腦內進行資料的側錄及分析找出其他的使 用者或主要伺服器為何）。另外，報告人也就現行的 BT 網路予以介紹。

（六）簡報：「電腦鑑識簡介」

1. 簡報詳細內容如附件二簡報檔。
2. 在美國的搜索票聲請書裡，必需記載要搜索的客體（我國狀況亦同），因此包括搜索電腦、筆記型電腦、網路設備（集線器及交換器）、周邊（如 CD、DVD、隨身碟、數位相機、PDA 等）、外接儲存裝置、紙張、筆記等物品都必需記載。而在扣押前，應製作扣押物品清單（我國亦同）；而搜扣到的電腦及相關設備在法庭要作為證據，經得起法院的檢驗，首要重視者就是取得的電腦內資料沒有遭到篡改，因此才有電腦鑑識必要。
3. 電腦鑑識的第一步是製作鑑識映象檔（forensic imaging），以確保資料沒有被修改，這個步驟也可稱為電腦鑑識內最重要的程序，若未作好，其所鑑識得到的資料日後在法庭恐將無法使用。此一步驟，可利用特定硬體或軟體（如：FTK Imager、EnCase、DD、Ghost 或其他軟體）達成[3]。而電腦儲存媒體內的資料可分為實體資料結構與邏輯資料結構，實體資料結構是在媒體上所儲存之電磁紀錄實際的存放組成（即 0 與 1 的組合），實體資料結構的映象製作就是將媒體上的 0 與 1 逐一複製至另一裝置上；而邏輯資料結構則指資訊如何在程式內顯示或是透過作業系統呈現給使用者觀看的內容。而邏輯資料結構的複製則不會複製作業系統無法判讀的資料。
4. 接著，報告人以具體個案說明電腦鑑識在個案中的運用，如關鍵字搜尋、圖片搜尋比對，電子郵件資料之搜尋，進而找到發信者的 ip 位址。在該案例中執法人員從電子郵件的內之相關資料發現在嫌疑人的 internet cache 資料內找到有問題之電子郵件之讀取紀錄，另外，在 msn 的對話紀錄內發現嫌疑人與他人之對話紀錄，而對特定檔案的追蹤內，發現

[3] 報告人在此特別介紹 physical write blocks 的概念，係指防止對作為證據之儲存設備寫入的實體儲存設備，也是最好的複製方式。

有一個連結檔（link file, 在 Windows 作業系統內檔案名稱為 *.lnk）指向「Transcend」，經查得上開字眼就是創見的品牌名稱[4]，進而找到相關證據。此外，網路瀏覽紀錄也可以得到很多資訊。

5. 最後，報告人總結說：電子證據到處都有，但鑑識人員必需看到單一檔案後面的訊息；而中介資料（metadata）的檢視對歸類使用者之傾向是必要的；縱使證據本身遭到破壞，但仍能透過鑑視找到該電腦使用者所留下的痕跡。

6. 日本代表詢問：有無任何鑑視軟體的認證機制，軟體的鑑識是否可信，而認證機制是否足以憑信？報告人回答稱：有的，如 EnCase 軟體，美國之執法人員會檢驗該產品之可靠性，並經多個機關採用，而該產品本身較無問題，較有問題的部分是在鑑視的過程上。

（七）討論專家小組任務文件（**Mission Statement**）

1. 任務文件：SPSG 網路犯罪專家小組將會進一步基於 APEC 領導人之共同聲明及 SPSG 之目標，以強化會員經濟體察覺、調查、追訴網路犯罪之方式促進網路安全，並促使、推展各會員經濟體間就打擊網路犯罪之合作事宜[5]。

2. 加拿大代表：文件中稱要「查覺、調查、追訴（網路犯罪）」是否包括網路犯罪之預防？主席回應：SPSG 的網路安全活動會注意網路犯罪預防事宜，但本專家中組則不討論此部分。

（八）討論日後工作要項

1. 主席表示：本計畫係一持續性的計畫，且會就如立法、司法及技術訓練（如電腦鑑識訓練）等多方面進行。本計畫亦會尋求私部門的參與，並請求各會員經濟體邀請其境內之私部門單位參與本計畫。他並籲請各會員經濟體促使境內之執法人員或機構參與下次會議。

2. 主席另表示，在下次於越南舉行之 APECTEL 45 開始前，希望能舉行網路犯罪之研討會。

---

[4] 報告人在此利用 google 搜尋資料，並告訴與會代表，利用 google 等搜尋引擎可以查到很多東西，同時也介紹了一些使用 google 搜尋的方法。

[5] 原文為：The SPSG Experts' Group on Cybercrime will further the APEC leaders' statements and the goals of the SPSG to promote cyber security by strengthen the capacity of member economies to detect, investigate, and prosecute cybercrime, and to promote and improve cooperation among member economies in the fight against cybercrime.

3. SPSG 召集人表示：建議自各會員經濟體內取得與網路犯罪有關之回饋 ，並與下一次 APECTEL 會議的主辦國進行討論。主席回應：同意上開建議，並將與下次會議主辦國越南進行議程及工作計畫之討論。

（九）簡報：「國際合作模型」

1. 網路犯罪是一個全球性的挑戰，而各國國內法對於數位據證據取得之法律規定必需有效的調查並追訴網路犯罪，且能促進國際間之法律上的合作。但每個法律系統都會有其取得證據之程序及限制；一般而言，「偵查不公開」是各國都會有的規定[6]。

2. 在證據資料的保存方面，相關的法律規定一般會允許執法人員就特定的電磁紀錄進行迅速的保存，其中可能包括公開部分通訊的資料，此外，資料漏失及被修改之防止也是法規應包括的內容[7]。

3. 在資料提出方面，相關法規應包括允許執法人員命特定人提出其所持有之電磁紀錄，或命某服務提供者提出其使用者之資料；另搜索、扣押電磁紀錄的程序內，應允許執法人員搜索並扣押某電腦系統及其所儲存之電磁紀錄、搜索、扣押某儲存媒體（如硬碟、磁片等）及複製其上之電磁紀錄。

4. 另在蒐集即時之通訊及內容資料方面，相關法規應允許執法人員以技術手段蒐集或紀錄即時之通訊與內容資料，及強制某服務提供者在其技術所許可之範圍內蒐集或紀錄即時之通訊與內容資料，或協助執法人員進行上開活動。而在內容資料的取得上，則要求具備較充分的理由始得為之。

5. 「雙重犯罪」問題[8]：所謂「雙重犯罪」是指二國在合作對抗特定犯罪問題時所面臨的問題。因此，各國必須就何種事項應列為犯罪達成共識，目前已經有美洲國家組織的網路安全策略（OAS Cybersecurity Strategy）及聯合國第 55 屆大會第 63 號決議（附件三）可以參考。而「雙重犯罪」也是引渡條約及司法互助條約之基礎。

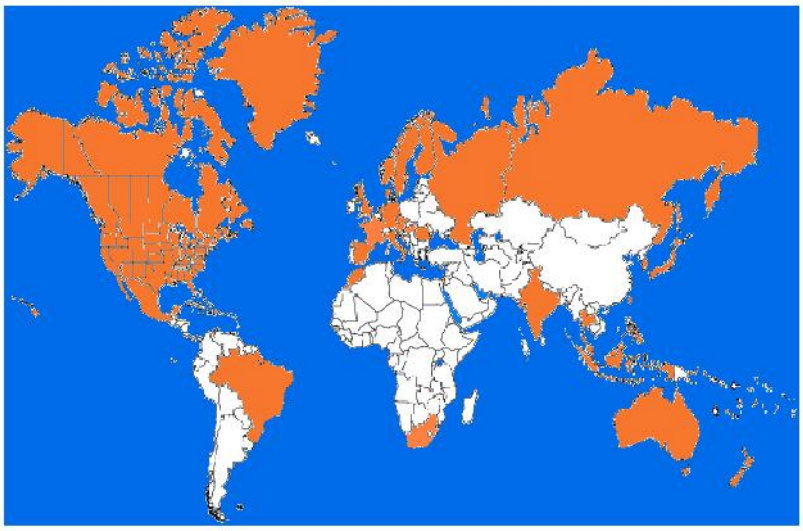
[6] 報告人在此特別指出：此處的考量是平衡執法利益與對人性尊嚴的尊重。

[7] 此處依報告人之說明，係指意圖或意外的刪除或修改電磁紀錄。

[8] 所謂「雙重犯罪」係指二國在合作打擊犯罪時，必須二國都認為是犯罪行為，A 國才會為 B 國進行司法互助的活動。此在網路犯罪上會是一大問題，因並非所有國家均有處罰網路犯罪。

6. 執法人員需要：a.高科技犯罪的專家；b.此專家可以全天候服務；c.持續的訓練；d.持續地更新設備；e.政治部門的支持；f.有一個網路安全的策略；g.解決預算問題；h.排除其他執法領域的競爭；i.資深人員的協助；j.私部門的協助合作。

7. G8 24/7 高科技犯罪防範網路：係現有之網路事件緊急應變機制，其參與成員國如下圖（我國亦有代表參加）：



8. 最後，在 A 國取得的證據能否在 B 國的法庭使用，涉及到證據法則的問題，如數位證據如何取得，跨國電信、數位通訊如何追蹤及電腦鑑視的問題，目前的司法互助條約恐無法達成此等要求。以美國為例，一般而言，美國法允許調查人員使用與外國執法人員聯合行動下，在國外取得之證據，只要該證據係依該國法律取得的即可。

9. 美國並提供其一般的聯絡窗口：FBI 及司法部（DOJ）之 Legal Attaché（分別為 FBI 專員及檢察官）。另可透過國際刑警組織及相類組織與美國聯繫合作事宜。

10. 討論：

A) 泰國代表問：有無固定代表窗口的需要？主席回應：應視會員經濟體之情形而定，可以是固定的會員經濟體，但由該經濟體內不同之代表出席會議或研討會等。

B) 香港代表問：本專家小組會處理 ip 衝突之問題？主席回應：ip 位址不是 SPSG 所要求的工作，且非網路犯罪問題的關鍵，但若認有需要，本專家小組亦可予以討論處理。

C) 馬來西亞代表：請提供更多私部門參與的資訊？主席回應：美國的私部門多數能夠自行支付費用參與，然而，各經濟體宜試著促使其境內的私部門參與此一計畫。

D) 加拿大代表：此議題也有其他論壇在討論，本專家小組如何自我定位，或避免與他論壇重覆？主席回應：本人建議本計畫所促進的效益是延伸合作至其他不在任何論壇內的會員經濟體。此外，不同的地區網路犯罪的需求與能力是不同的。

E) 泰國代表問：每年會增加開會次數？主席回應：每年將舉行一次會議，也許在初期會舉行較多次會議。

F) 日本代表表示：南韓已經有一個網路犯罪計畫（CTTF）？主席回應：CTTF 是政策性的計畫，而執行面的問題不會在該計畫中處理。本專家小組將著重於運作執行面，而非政治導向的。且 CTTF 除網路犯罪外，尚包括網路恐怖行為的處理，本專家小組所討論的結果對 CTTF 也是有幫助的。SPSG 召集人回應稱關於 CTTF 計畫與本專家小組的議題會在 SPSG 內檢視避免重複。

G) 日本代表稱 CTTF 可能會有比 APECTEL 更多的參與者。主席回應稱：會注意此事並與 SPSG 及南韓做進一步討論。

（十）SPSG 召集人 Jordana 致詞：她感謝美國組織此一專家小組及擔任主席，亦感謝馬來西亞擔任副主席。提及本次會將專家小組會議與法規圓桌會議合併，係希望增加參與，她並感謝所有提出報告及參與討論的代表。並於 15 時 45 分時宣布會議結束。

四、心得感想：

本次前往馬來西亞參與 APECTEL 44 之會議，對個人而言，是一次非常特別的經驗，各國代表齊聚一堂討論各國共同關心的議題，使用外語進行會議，都是相當不同的體驗。就會議討論的議題言之，本次會議主要是討論社群網站對於網路犯罪造成之衝擊，以及不同地區、不同文化對於網路犯罪認知的不同，以及日後各經濟體間如何合作等議題。這些議題，在國內主要是以社群網站的犯罪行為，如何透過國際合作進行查緝追訴，是身為執法人員的檢察官較為關心的議題。

以國內的情形而言，社群網站上的犯罪行為（如妨害名譽、詐欺等），因為此等社群網站均由國外之業者經營（如 facebook 係由美國之業者經營、plurk 係由加拿大業者經營、而新浪微博、twitter 等微網誌，則分別由大陸地區及美國業者經營），上開外國業者在國內並無營業單位，其伺服器主機也放在境外，因此要追查犯罪行為人時，就會面臨無法調取資料，使得犯罪行為無法繼續追查，尤其日前，有民眾利用美國 yahoo 之帳號發文稱欲暗殺總統，就面臨如何查得該實際行為人之困難，雖然之後是利用其他管道查得犯嫌身分，但此一問題日後將層出不窮，實有必要研擬相關之防範規制措施。本次會議討論的議題亦有涉及到 facebook 之使用者資料調取之問題（參見馬來西亞代表之簡報），該國也是透過其他管道查得資料，惟建立長遠之國際合作制度，是解決此一困境之必要途徑。以往國際間司法之互助，通常必需簽定雙邊之司法互助協定作為法規依據，但我國在國際現勢下，勢難透過此一管道達到目的。因此日後如何透過 APEC 此一論壇，就共同打擊網路犯罪建立互相提供即時資料查詢之機制，可為日後努力之方向。

國內網路犯罪最主要之法令規範，即刑法第三十六章，業於民國 92 年 6 月 15 日經總統公布施行，經過近十年之實務運作，已累積相當之經驗，且國內之執法人員在查緝的技術上，並未遜於他國之執法人員，惟以往國內之執法人員與外國之執法人員並無機會交流，而 APECTEL 所建立之專家小組，則提供一執法人員與技術人員之交流平台，本次專家小組第一次會議，即一再籲請各經濟體之執法人員及私部門之業者能夠參與專家小組之會議及聯絡名單，並決議下次 TEL 45 時，專家小組將進行數日之研討會（workshop），促進執法人員之執法技術能力，並促進各經濟體執法人員之互相交流，是建議政府於下次會議時，能夠提供多名檢察官與警方、調查局人員參與會議之機會，以利國內執法人員增進執法能力及與外國執法人員之交流，此舉亦可對於向國外業者調取與網路犯罪有關之資料之困難產生助益。

再者，網路犯罪之議題日漸為國際間重視，國內並非無法提供其他國家協助，惟國內每次派出參加 APEC TEL 會議之檢察官均會更換，造成業務的銜接發生困難，建議日後能夠讓參與過會議之檢察官陪同另一位檢察官參與會議，除使得業務能夠持續並獲傳承外，另建議能夠派出對網路犯罪業務較為熟悉之人員前去開會，方能達到交流互動之目的。否則，每次前往開會之人均不同，當熟悉會議之事宜後，又無法將經驗傳承與其他人員，反而無法達成促進檢察官與其他國家就網路犯罪議題之互動與他國執法人員之交流之美意。

綜上，僅就本次參與 APECTEL 會議提出以下建議：

一、建議可積極參與專家小組會議，分享國內辦理網路犯罪案件之經驗，促進國際間之合作。

二、建議派往參與專家會議之人員係實際辦理網路犯罪之檢察官或警調人員，且人數可以較多，以促進各國執法人員間之交流。

三、建議建立經驗傳承制度。