國際組織與台灣網路犯罪相關法規之比較

國立臺北大學犯罪學研究所教授　周愫嫻

澳洲國家大學法規制度研究中心博士生　張耀中

摘要

順應網路科技的發展，台灣已從 e-Taiwan、m-Taiwan，慢慢的朝向 u-Taiwan（ubiquitous Taiwan），意即無所不在的優化台灣發展，讓台灣地區人民得以在任何時間、任何地點均可以連上網路，享受網路帶來的便利。然網路應用的興起，除了使傳統的犯罪行為轉由透過網路進行外，相對的也衍生新興的犯罪問題，例如阻斷式攻擊、惡意程式等等。此外，無線網路的使用，讓有心透過網路進行犯罪之電腦犯罪者得以透過更簡便的方式進行犯罪，同時亦可躲避檢警調之追查。

有鑑於網路犯罪的跨國性，各國際組織紛紛針對此一議題提出討論，希望建立一個全球一致打擊網路犯罪之規範標準，並透過各國於其內國法規之落實，以有效嚇阻與規範網路犯罪之進行。爰此，本文擬介紹聯合國及歐洲理事會因應網路犯罪所制訂的相關規範，以及亞太經合會（Asia- Pacific Economic Cooperation, APEC）針對網路犯罪防制所提供的建議，然後分析台灣對抗網路犯罪之相關法規及管理政策，最後本文提出未來面對網路犯罪可參考之修法與管理建議。

壹、前言

網路的起源，最早可追溯到 1968 年，當美國國防部下屬的「先進研究計畫局」（the Advanced Research Project Agency）開始研發其內部網路系統（the Advanced Research Agency Network, 簡稱 ARPANET）時。ARPANET 的建立，主要是為了建立大學、國防組織以及軍事指揮中心間之溝通與支援，並得以在核戰爆發時，仍可維持美國國內重要軍事、國防組織或政府重要單位彼此間之溝通聯繫。此種以軍事國防目的為基礎的「網路」，雖在 1970 年代開始於美國政府部門與大學間，以及其他國家內部開始發展，但早期並未開放給一般民眾及企業使用。

網路在民間的興盛，則必需到 1991 年，美國國家科學基金會（National Science Foundation）允許民間企業得以為了商業目的利用網路開始。民間企業在發現了此一新媒體之經濟潛力，以及帶來企業經營上的便利，無不積極發展與利用，使得網路得以迅速擴張。而電腦系統的革新，例如滑鼠的發明、圖像網頁的研發、以及使用電腦之成本的大幅降低，亦都促使網路得以在世界各地，政府、企業或家庭中迅速發展。根據資訊工業策進會 2006 年針對企業網路使用狀況的調查顯示，目前我國有百分之八十三的企業都以在其內部建構網路設備；此外，根據美國中央情報局（Central Intelligence Agency）的報告，在 2006 年時，台灣地區連網人數約有一千三百多萬人，亦即約有百分之六十的台灣人民均會使用網路。

網路的興起，便利了人與人之間的互動，縮短了人與人之間的距離。透過網路的應用，民眾可以透過較為迅速的方式取得資訊，學習新知，甚或是新的技能。它改變了人類的生活，使民眾可以透過便宜（甚或是免費）的方式與遠方的朋友或親人進行「面對面」[1]的溝通；它同時也跨越了國境的限制，使民眾得以在家裡就可以結交到居住在世界各國的朋友，瞭解各國的民情風俗。也因此，網路也被稱做事被稱為是人類歷史中重要的發明。

網路通訊技術發展迅速，已使資訊基礎建設與國民對資訊應用的接收度成為衡量各國競爭力的重要指標。歐美等先進國家無不透過增加對資訊科技投資的方式，希望刺激企業生產力、提升總體經濟的表現，並希望藉此改善民眾在教育、健康、娛樂、通訊等方面的便利性。

順應網路科技的發展，台灣已從 e-Taiwan、m-Taiwan，慢慢的朝向 u-Taiwan（ubiquitous Taiwan），意即無所不在的優化台灣發展，讓台灣地區人民得以在任何時間、任何地點均可以連上網路，享受網路帶來的便利。然新興科技的產生，雖帶來了便利，使也衍生出新的犯罪問題。網路應用的興起，除了使傳統的犯罪行為轉由透過網路進行外，相對的也衍生新興的犯罪問題，例如阻斷式攻擊、惡意程式等等無線網路的使用，更讓有心透過網路進行犯罪之電腦犯罪者得以透過更簡便的方式進行犯罪，同時亦可躲避檢警調之追查。

舉例來說，以無線網路作為工具進行犯罪，躲避犯罪偵查案例的出現，讓國內的治安環境亮起紅燈。例如 2005 年 1 月台中市查獲利用無線網路溢波上網，進行網路銀行盜領及盜刷信用卡一案[2]，就是利用他人的無線網路盜用帳號，並進而持以破解網路銀行安全系統進行竊取的犯罪手法。事實上，無論是有線網路還是無線網路環境，兩者都有可能遭受到網路犯罪的威脅（如病毒、駭客攻擊、網路釣魚等）或是被利用作為犯案的工具，但不同於有線網路環境下，犯罪者的犯案軌跡通常仍有跡可循之情況，無線網路具移動性而不易追查。可預見的是，未來執法機關在調查利用無線網路進行的犯罪，將會有相當之困難度。

鑑於網路的無遠弗屆，許多網路犯罪的發生，往往是屬於跨國犯罪，若各國對於網路犯罪之認知與規範有太大落差，將使得犯罪者有機可趁。為避免此漏洞之發生，許多國際組織（如聯合國、歐洲理事會等）紛紛制訂對抗網路犯罪之公約或協定，希望透過各會員國將公約或協定之內容轉化成其本國法制，以求各國立法之一致性。

本文將先介紹聯合國及歐洲理事會因應網路犯罪所制訂的相關規範，然後介紹亞太經合會（Asia- Pacific Economic Cooperation, APEC）針對網路犯罪防制所提供的建議，最後對照分析台灣對抗網路犯罪之相關法規及管理政策。

貳、網路犯罪之興起

如前所述，網路科技的發展，雖帶給民眾生活上之方便，同時也提供犯罪者新的犯罪工具與犯罪標的。但由於網路一開始的建造目的，乃是為了建立一

[1]例如，透過視迅會議的方式，通話之雙方不只可以聽到彼此的聲音，同時也可以看到對方的影像。

[2]資料來源：http://wwew.cib.gov.tw/news/news01_2.aspx?no=665，最後查詢日期：2005/5/20。

個新的溝通的管道，並非基於商業目的，故網路安全的問題並未在一開始便受到重視[3]。

在 1950 年代至 1980 年代間，由於網路犯罪的進行，必須要具備有相當之技術，所以網路犯罪並不普遍。換句話說，並不是所有人都可以透過網路進行犯罪，僅有少數熟稔網路原理與技巧者得以透過網路進行犯罪。當時，大部分的「駭客」（hacker），亦即透過網路入侵他人電腦系統者，通常是基於對技術的好奇與為了展現自己的能力之目的而進行犯罪行為或是偏差行為。這些駭客大多會遵循著「駭客倫理」（hacker ethics），亦即基於發現系統的問題、修改系統之漏洞、以及巧妙的運用技術等[4]，進行入侵系統之行為。他們的出現，並未對社會帶來太多的麻煩；相反地，這些駭客對於網路技術的發展與漏洞的發現，有相當大的助益。

直到 1990 年代，由於基於商業目的利用網路之開放，使得企業團體開始透過網路進行商業交易。而部分的駭客也慢慢從原本為了有趣而入侵他人系統，轉變成為了獲取金錢目的、報復或是政治目的而入侵他人系統[5]。過去的駭客在發現系統漏洞時，基於駭客倫理，他們會主動告知系統擁有者或管理者，以進行系統漏洞的修復；然 1990 年代以後的大部分駭客，確有完全不一樣的作法。這些駭客在發現系統漏洞時，並不會告知系統擁有者或管理者，反之，他們會透過此漏洞竊取機密資料或是獲取金錢利益，甚或是將該系統之電腦建構成為「殭屍電腦」，以利其進行其他網路攻擊時，用以規避法律追查或是進行阻斷式攻擊時之工具。

此外，駭客技術的商業化，亦使得網路犯罪問題變的嚴重。駭客軟體的出現與大量散布，使得一般民眾均能在不需要經過長時間訓練的情況下，簡單的透過自動化執行的軟體，成為駭客以入侵他人電腦系統。亦即，在現在，只要是會使用電腦的民眾，大多可以透過這些軟體而成為駭客。同時，部分有技巧之駭客議題工商業服務，受雇於有需要之民眾或是企業團體，憑藉其擁有之技術，已竊取業主所需要之資料。這些轉變，使得網路犯罪的問題開始普遍，且受到社會大眾之重視。

參、國際組織對抗網路犯罪之作法

電腦及網路犯罪之嚴重性，世界各國都不敢輕忽。由於網路犯罪多屬於跨境犯罪，須要國際間的合作與互助，才得以有效防範。所以不論聯合國、歐盟，甚或APEC等組織，均發起防範電腦犯罪之公約與協定，希望約束各會員國，加強內部對抗網路犯罪之能量與跨境間之互助。本文以下就聯合國 2000 年第 55 屆會員大會第 63 號決議（UN General Assembly Resolution 55th Congress 55/63）、歐洲理事會 2001 年發表之網路犯罪公約（Convention of Cybercrime）與APEC關於網路犯罪法制等資料，分別說明國際間的法制發展趨勢。

---

[3] Lessig, Lawrence. *Code and other Cyberspace.* U.S.: Basic Books, 1999.
[4] Taylor, Paul A., "From Hackers to Hactivists: Speed Bumps on the Global Superhighway." New Media Society 7, no. 5 (2005): 625-46.
[5] Choo, Kim-Kwang Raymond., Russel, G. Smith, and Rob McCusker. "Future Directions in Technology-Enable Crime: 2007-2009." Edited by Australian Institute of Criminology: Australian Institute if Criminology, 2007.

一、聯合國第 55 屆大會第 63 號決議—打擊非法濫用資訊技術

聯合國很早即注意到新興科技可能帶來的治安隱憂，於 1990 年 12 月舉行之第 45 屆大會中，核可第 8 屆聯合國預防犯罪和罪犯待遇大會（the 8th United Nations Congress on the Prevention of Crime and the Treatment of Offenders）的建議，呼籲各會員國應加強努力，以更有效地打擊網路相關犯罪，確保人人均可享受新技術，特別是資訊及通訊技術的好處[6]。

在 2000 年第 55 屆會員大會中，聯合國大會更通過第 63 號關於打擊非法濫用資訊技術的決議（Combating the criminal misuse of information technologies）。該決議中指出，聯合國大會意識到資訊的自由流通可以促進經濟與社會的發展、教育，以及民主施政；且注意到各國在發展及應用資訊技術與電信手段方面已有顯著的進步。但技術的進步，為犯罪活動創造新的機會，尤其是非法濫用資訊技術的部份。雖說各國對於資訊技術的依賴程度有所不同，但此種依賴增加了全球合作與協調的機會，也導致非法濫用資訊技術之狀況發生時，不單是一個國家受影響，其他國家亦可能遭受波及。所以跨國間的合作，成為不可或缺的一環。

因此，大會在決議中提醒各會員國應注意防止資訊技術非法被濫用的必要性，且要意識到國家與國家，國家與私人企業，必須聯手合作，以合作方式共同打擊非法濫用資訊犯罪。此共同合作與協調之機制，可透過聯合國或是各區域組織的力量發揮作用。聯合國代表大會並於本次決議的最後，表達了對歐洲理事會網路犯罪專家委員會從 1996 年以來致力於擬定國際協定之草案（即網路犯罪公約，Convention of Cybercrime），以推動各國制訂相關防制網路犯罪、建立預防機制、訓練執法人員、保存並調閱電子資料的規範，及促進國際合作的肯定。

二、歐洲理事會—網路犯罪公約

歐洲理事會（Council of Europe, CoE）鑑於電腦犯罪日漸嚴重，且通常為跨境之犯罪，故在 1996 年組成電腦專家委員會（European Committee on Crime Problem），著手進行「網路犯罪公約」（Convention of Cybercrime）之草擬工作。網路犯罪公約於 2001 年 11 月 23 日由歐洲理事會 26 個會員國及 4 個非會員國（美國、加拿大、日本與南非）外交部長，於布達佩斯正式簽署通過，並於 2004 年 7 月 1 日正式生效[7]。截至 2007 年 10 月 31 日止，共計有 43 個國家簽署本公約（其中包含 5 個非會員國），並有 21 個國家已經國內立法追認生效。其中，美國於 2006 年 9 月 29 日經國會追認，並於 2007 年 1 月生效時，讓本公約再次掀起一陣討論，更強化網路犯罪公約的重要地位。

網路犯罪公約可說是全球第一份針對網路犯罪而制訂之國際性公約。有鑑於網路犯罪的跨國性，以及各國法規的不一致，歐洲理事會希望藉由網路犯罪公約，建立一套國際一致的標準，共同對抗網路犯罪。網路犯罪公約之立法目

---

[6] 聯合國第 45 屆大會第 121 號決議參照。

[7] 依據網路犯罪公約規定，簽署國家中必須有 5 個上的國家（其中必須有 3 個以上是歐洲理事會的會員國）於國內立法追認生效後，公約才會正式生效。目前已有 18 個國家立法通過並實施。請參照歐洲理事會網站，網址：http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG，最後查詢日期：2007/1/25。

的包含[8]：（1）針對網路犯罪議題在實質法律要件與相關刑罰之修正議題；（2）針對各種利用電腦系統、或其他電子形式的犯罪行為，提供執法機構調查的程序依據；（3）建立快速有效的國際合作關係等；而此公約內涵大致可從下三個方面進行討論：

（一）電腦犯罪之類型

此公約根據電腦犯罪行為之特性，列舉了 4 大項、9 種與電腦應用相關的犯罪行為，建議締約國應將之納入其國內法制當中，且保留相當的彈性，由締約國依其國情特色作進一步的判斷。此 4 大項的犯罪型態包括：（1）侵犯電腦資料與系統機密性（confidentiality）、完整性（integrity）與可利用性（availability）之犯罪；（2）與電腦應用相關之犯罪（Computer-related offences）；（3）與內容相關之犯罪（Context-related offences）；（4）侵犯著作權與著作權鄰接權之犯罪（Offences related to infringements of copyright and related rights）等。其中，「與內容相關之犯罪」及「侵犯著作權與著作權鄰接權」2 種犯罪類型，電腦所扮演的角色為一個單純媒介，所討論的重點與本文擬探討之入侵型電腦犯罪較無直接相關，在此不加描述。以下僅就侵犯電腦資料與系統機密性、完整性與可利用性之犯罪，以及與電腦應用相關之犯罪進行討論：

1. 侵犯電腦資料與系統機密性、完整性與可利用性之犯罪[9]

網路犯罪公約對於此一部份的犯罪問題，共列舉了 5 項，包含非法入侵（Illegal Access）、非法截取（Illegal Interception）、資料干擾（Data Interference）、系統干擾（System Interference）、設備濫用（Misuse of Device），分述如下：

（1）非法入侵[10]

非法入侵，指行為人故意在無權限的情況下，入侵他人全部或一部的電腦系統。所謂電腦系統，依本公約中第 1 條a項之定義，指任何單獨或彼此相連的裝置中，有一個以上的裝置係依程式運作而自動處理數據者[11]。

（2）非法截取[12]

非法截取，指行為人故意在無權限的情況下，以科技手段對非公開電腦資料的進、出電腦系統，包括從電腦系統發出，其中帶有電腦資料的電磁輻射等進行截取之行為。締約國可自行認定，是否以犯罪係出於不法故意，或不以行為既遂為構成要件，或只要行為人連線上該電腦主機相連的其他電腦之時即足以論罪。

---

[8] 參見吳兆琰，新興網路犯罪法制議題分析及因應—以歐洲理事會「網路犯罪公約」為中心，科技法律透析，2003 年 10 月，頁 31。

[9] Article 2-6, Covention of Cybercrime.

[10] Article 2, Convention of Cybercrime. 根據我國刑法第 358 條之立法說明，「access」在我國翻譯為「入侵」。

[11] Article 1(a), Convention of Cybercrime.

[12] Article 3, Convention of Cybercrime.

（3）資料干擾[13]

資料干擾，指行為人故意在無權限的情況下，對電腦資料進行毀損、刪除、變更性質、竄改、或隱匿之行為。針對此一部份，各締約國可保留適用本條之權利，並可自行判斷，是否以行為人之行為需造成嚴重損害為犯罪的成立要件。

（4）系統干擾[14]

指行為人故意在無權限的情況下，以輸入、交換傳輸、直接損害、刪除、變更性質、竄改、隱匿等方式嚴重干擾電腦系統正常功能運作。

（5）設備濫用[15]

指行為人故意在無權限的情況下，以製造、販賣、媒介、進口、散布、或以其他方式，取得用來「入侵」(access)全部或部份電腦系統的設備，包括電腦程式、電腦密碼、使用程式碼或相關資料等。而為達犯罪目的，設計、修改相關設備，或意圖犯罪而故意持有上述物品者亦同。

2. 與電腦相關之犯罪[16]

「與電腦相關的犯罪」規定在本公約之第 7～8 條，內容包括「與電腦相關之偽造」（Computer-related Forgery）以及「與電腦相關之詐欺」（Computer-related Fraud）兩種。大部分的國家都已將這兩種類型之犯罪納入其法律規範當中，但為了避免法條文字與法益的界定不足以涵蓋新興的犯罪模式，網路犯罪公約仍就此兩種犯罪行為加以說明，以督促各國檢視其國內法，以求一致。

網路犯罪公約中關於「與電腦相關之偽造」規定，只要「行為人惡意或在無權限的情況下，增、修、刪改、隱匿，使不實的電磁紀錄視為真實，或使人誤以為真實」的情況，即為犯罪。

若「行為人惡意在無權限之情況下，以詐欺或不實的意圖，為自己或第三人不法利益，以（1）輸入、更改、刪除、隱匿電磁紀錄的行為，或（2）任何足以對電腦系統原本設計功能加以干擾之行為，造成他人財產損失之行為」者，則屬於「與電腦相關之詐欺」範疇。

（二）執法機關蒐證權限

網路犯罪公約除了規範實體的網路犯罪類型以外，亦對於程序上的蒐證權限部份進行討論。由於這一部份可能涉及侵犯個人人權及自由權等等憲法保障個人之權利，故在此公約中，除要求各締約國應遵照如歐洲保護人權及基本自由公約（European Convention for Protection of Rights and Fundamental Freedoms）、與聯合國公民與政治權利國際公約（International Covenant on Civil and Political Rights）等對人權保障之規定外，其他如比例原則、不自證犯罪原則[17]等，都是此公約程序規定在引用時所必須注意的部份。

網路犯罪公約針對執法機關蒐證所為之規定，包括：

---

[13] Article 4, Convention of Cybercrime.
[14] Article 5, Convention of Cybercrime.
[15] Article 6, Convention of Cybercrime.
[16] Article 7-8, Convention of Cybercrime.
[17] 同註 20，頁 39。

1. 已儲存紀錄的緊急保存與揭露

鑑於電子資訊有容易滅失或遭到竄改的風險，故為了保全電子化證據的完整性及真實性，網路犯罪公約建議各國應採取特殊程序，保存全部或部份的電腦資料。根據本公約第 16 條之規定，締約國應採取必要立法措施，使其執法機關得以命令或以其他類似方式取得特定的、經電腦系統儲存的電磁紀錄，包括通訊紀錄，及有理由被認為具有脆弱性，屬於容易被損毀、滅失、修改的電腦紀錄。同時考慮到保存的時間越長，對系統服務業者所造成的負擔越大，故建議紀錄的保存期間上限為 90 日，但可以連續更新命令延長[18]。

需注意的是，此處容許緊急保存者，為已在系統服務業者持有控制下，且為了系統管理或其他帳單處理為目的而已經儲存之電磁紀錄為主，執法機關不得課與業者額外的義務，要求保存不特定對象的紀錄，或是強制業者更新其系統設備，以配合協助執法機構之犯罪查緝。

又由於網路通訊資料，往往分散於不同系統服務者系統中，要對特定資料保留進行判斷，必須要求所有相關服務提供者提供其所擁有之通訊資料，始可為之。網路犯罪公約在第 17 條針對迅速保存及揭露部份通訊資料作規定之用意，即在解決此一問題。希望不論該訊息是存於一個或是多個服務提供者，締約國均能確保該保存之資料能夠立即取得及利用[19]。

依據網路犯罪公約第 17 條第 1 項電腦資料提供者的定義，包含各締約國在其領域範圍內的自然人以及網路服務提供業者。各國應採取必要的立法措施，使其境內之人有配合揭露特定電腦資料的義務，以協助執法機關的調查工作。原則上，本條之適用範圍僅限於提供犯罪嫌疑人之相關資料，主管機關並不得為毫無限制之提供命令。

2. 對已儲存資料之搜索與扣押

基於保全證據的必要，網路犯罪公約第 19 條亦建議各締約國，透過立法及採取必要措施，使其執法機關得對電腦系統之全部或一部及電腦中所儲存之電腦資料，或該國領域內之電腦資料儲存媒介之電腦資料，進行搜索扣押，或為類似存取之行為[20]。本條中所規定的必要措施（亦即搜索扣押之方式），應包含以下權限：（1）對電腦系統或其他電子儲存媒介的全部或一部進行扣押或類似的保全措施；（2）對該電磁紀錄製作備份；（3）對已保存之電磁紀錄保持其正當性及完整性；（4）使標的物的電腦無法被接取，或是從該電腦系統中移除相關電磁紀錄等[21]。

網路犯罪公約第 19 條希望各締約國進行搜索扣押時，須符合公約第 14 條及第 15 條之規定。對於此一規定，歐洲理事會在公約制訂前，曾就執法機關在實施搜索扣押前，是否應先通知關係人有一番爭論，有一派主張為避免資料流失阻礙犯罪偵查，應採取保密措施；另一派則主張維護人權，所有搜索扣押皆

[18] Article 16, Convention of Cybercrime.
[19] Article 17, Convention of Cybercrime.
[20] Article 19, Convention of Cybercrime.
[21] 同註 4，頁 41。

有通知義務[22]。但鑑於各國法制之差異，網路犯罪公約就此一部份並未有定論，而尊重各國法律體制。

3. 對於電磁紀錄的即時取得

為了保障人權，通訊中之電磁紀錄並非可以任意取得，而是必須與該締約國領域內之資料有關；司法或其他許可蒐集之命令，也必須具體指明與該訊息相關通訊中之電磁紀錄。此處所指通訊中之電磁紀錄，不限於以Internet串連之電腦網路，還包括電信通訊網路[23]。本公約第 20 條及第 21 條明確將「通訊中之電磁紀錄」區分為「通訊紀錄（traffic data）之截取」與「內容資料（content data）之截取」兩部份。

在通訊紀錄截取部份，公約建議各締約國應採取必要之立法措施或手段，加強執法機關在其領域內，經由技術設備蒐集或記錄之權限；另一方面則可要求服務提供者在其技術範圍內，經由科技方式，收集或記錄在其國內之通訊。賦予配合義務之各業者，必須對執法機關依本條規定要求其配合執行之事項與相關資訊，負保密義務[24]。公約特別提醒各國，通訊監察的對象必須特定，不容許一般性、無區別性的探查行為，且不得增加業者額外的負擔，要求業者特別為此添購設備或重新設計其系統功能。

在內容資料的截取部份，規定大致與第 20 條關於通訊資料截取相同，但由於內容資料之截取，對民眾隱私權侵害性更高，所以必須以「依其本國法律規定與重大犯罪有關之案件」，且是「特定對象」為前提[25]，必須遵守公約第 14 條及第 15 條之規定。

（三）跨國合作

網路犯罪公約的制訂，除了提供各締約國一致的法制規範建議，使各國對網路犯罪能有共通之認知，還說明對抗無國界網路犯罪的跨國合作機制之原則，以作為各締約國間相互合作之基礎。

公約第 23 條即針對國際合作的一般原則加以說明，希望締約國間應就電腦系統及資料之犯罪調查或訴訟，或對電子證據之蒐集，盡最大的合作可能。第 25 條則針對相互協助的一般原則作說明，希望各締約國在與電腦系統及資料相關犯罪問題之調查或訴訟，應提供最大可能之相互協助。第 27 條至第 35 條則針對國際互助作具體之說明，包括無國際協定時相互請求之相關程序、機密及使用的限制、及時收集通訊資料的相互協助、迅速保存已儲存的電腦資料與通訊資料，公約中更希望各締約國應指定一個每日 24 小時、每週 7 日皆可利用之聯繫點（contact of point），以利電腦犯罪之調查與訴訟等。

三、APEC 關於網路犯罪防制與安全管理之討論

為了宣示對抗電腦犯罪之決心，APEC組織於 2002 年 10 月召開「反恐及促進發展會議」，希冀透過國際合作與規範的力量達到下列目的[26]：（1）促進各

---

[22] 參見馮震宇，網路犯罪與網路犯罪公約（下），月旦法學教室，第 5 期，第 119 頁。
[23] 同註 4，頁 42。
[24] Article 20, Convention of Cybercrime.
[25] Explanatory Report of Convention of Cybercrime, No.230.
[26] 參閱*Cybercrime Legislation and Enforcement Capacity Building Project* , 2th Conference of Experts and Training Seminar, 25-27 Aug 2004。

會員國對抗網路犯罪及發展制衡網路犯罪之法制架構；（2）協助各會員國發展對抗網路犯罪之機構，並促使此一機構的跨國合作；（3）提高政府與產業間的相互瞭解與合作，以共同對抗網路犯罪。會後同時發表「反恐及促進發展宣言」（Statement on Fighting Terrorism and Promoting Growth），明確要求各會員國應（1）致力於對抗網路犯罪法制之建立與促進網路之安全；（2）發展可提供跨國互助的執法單位。

（一）加強共同執法

為了維護網路所帶來的經濟發展效益、保護重大基礎建設（如電子金融）、減少網路犯罪的影響，制訂或修訂法律以對抗網路犯罪已成為各國法制發展必要的趨勢。而網路安全的維護，更須依靠各國以明確的程序規範，確保執法人員於執行調查或是起訴網路犯罪（者）之權限與跨國合作才可能達成。APEC因此於其網路犯罪防制政策中，明確建議其會員國，應儘速依據歐洲理事會所訂定的網路犯罪公約，修改其國內的實體法與程序法[27]，並且要求各會員國定期於大會開會時，報告其立法的進度與情形，以進行交流。

根據 APEC 的調查，部份會員國已完成實體法的立法工作，並開始實行，如新加坡；而部份國家則已在立法階段，如大陸、越南、日本等。透過立法方式減少各國在網路犯罪定義上的落差，將有助於跨國犯罪的司法互助合作。

此外，APEC 希望各會員國建立一個電腦危機處理小組（Computer Emergency Response Team, CERT），能對電腦犯罪作最及時且快速的處理；APEC 也承諾提供相關的訓練與指導方針（如 PKI 的運用、電子密碼的運用以及電子認證等等），以協助各國對抗網路犯罪。

（二）確立電磁紀錄之證據能力

所謂證據能力，是指證據得提出於法庭調查，以供作認定犯罪事實之用。此證據必須要與待證之事實相關聯，並且未受法律之禁止或排除，始具備之。除了需符合非受法律禁止與排除的消極要件外，同時還必須踐行法律規定的調查證據程序，才取得證據能力。

各國法制目前對是否接受電子紀錄作為證據，亦即電磁紀錄是否具有證據能力，有不同之見解與作法。中國大陸與印尼均表示，目前法制上並不允許數位證據，需將該電磁紀錄先轉成書面文件，始可提出做為證據，但這樣的證據在法庭上是否被允許，仍依個案認定。美國就這一部份，則是透過對電磁紀錄的認證，加上承認電磁紀錄乃人為輸入、具有證據能力之方式，來處理電磁紀錄證據能力認定之議題[28]。

對於以電磁紀錄做為證據之規範，比較明確的應屬加拿大於 1998 年公布之「統一電磁證據法則」（Uniform Electronic Evidence Act），其中針對以電磁紀錄作為證據時，對於以列印輸出的方式所表現出來的電磁紀錄，只要是透過明確且連續的方式列印出來，且能夠證明紀錄或儲存該數據之電子系統的完整性，即屬於最佳證據原則所規範之證據（the best evidence rule）；此外，若能證明產生該電磁記錄的電腦系統或其他設備運作正常，或即使在不正常的情況

---

[27] 資料來源： http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN012298.pdf，最後查詢日期：2007/10/3。

[28] 同前註。

下亦不影響電磁紀錄的完整性時，除非有證據證明該電磁紀錄為不完整的情況，否則應認為該電磁紀錄具有完整性[29]。。

參、台灣現行法制因應

不論聯合國或是 APEC 等國際組織，均推崇歐洲理事會所訂定之「網路犯罪公約」對網路犯罪所做之規範，並建議其各會員國應儘速按照網路犯罪公約內容，修改其國內法律。綜合上列討論，目前國際組織因應網路犯罪的方式，大致是從上述 3 個角度來著眼：第 1 個部份為針對網路犯罪類型的規範，亦即從刑法等相關實體法律層面出發；第 2 個部份為關於執法機關的蒐證權限部份，從訴訟法角度建議各國應如何進行電磁紀錄之保存，與如何進行搜索扣押等；第 3 部份是跨國合作的部份，從國際合作的方式，使無國界的網路犯罪不因跨國因素而影響調查或訴追。

以下即依據網路犯罪公約之討論，檢視我國在網路犯罪防制實體法和執法機關蒐證權限之規範。

一、網路犯罪類型之規定

我國於 2003 年 6 月通過了刑法第 36 章（第 358 條至第 363 條）妨害電腦使用罪之規定，作為處罰電腦犯罪的明確規範。本章規範之電腦犯罪類型，指狹義的電腦犯罪，亦即犯罪之發生係以電腦或網路為攻擊之對象者。其他關於透過電腦或網路作為媒介進行犯罪的部份，則屬廣義的電腦犯罪部份，規範於刑法其他章節中。

（一）刑法第 36 章妨害電腦使用罪

刑法第 36 章之修定，乃為因應電腦及高科技犯罪對傳統刑法帶來之衝擊，且解決傳統刑法無法適用於高科技犯罪之窘境而制訂。全章共包含 6 條條文（刑法第 358 條至第 363 條），針對狹義的電腦犯罪類型進行規範。

第 358 條[30]之規定，與網路犯罪公約第 2 條「非法入侵」的立意相當，針對無故入侵他人電腦進行規範。不同的是，網路犯罪公約廣泛的規定無權限入侵他人電腦即符合犯罪之要件，而我國則嚴格限縮於以無故輸入他人密碼、破解他人使用電腦之保護措施與利用他人電腦之漏洞等三種行為態樣，入侵他人電腦或其相關設備，始為犯罪。非此三種態樣以外的手法入侵他人電腦，則不在此規範之中。

如同網路犯罪公約第 4 條對資料干擾之規定，我國刑法第 359 條[31]亦針對無故取得、刪除、或變更他人之電磁紀錄之行為作處罰，但我國明確規範上述行為，需符合肇生損害於公眾或他人之要件。

第 360 條[32]對干擾他人電腦致生損害之規定，則類似網路犯罪公約第 5 條對系統干擾之規定。本條取代了原本刑法第 352 條第 2 項對於干擾他人電磁紀

---

[29] 資料來源：http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u2。最後查詢日期：2007/10/5。

[30] 刑法第 358 條：「無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」

[31] 刑法第 359 條：「無故取得、刪除、或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」

錄之處理部份，並加以明確規範，認為行為人無故以電腦程式或是其他電磁方式，干擾他人電腦或是相關設備，屬犯罪行為。但如同第 359 條之規定，須造成公眾或個人的實質損害，始為構成要件該當。

第 362 條[33]則針對製作程式供犯罪之用的行為加以規範，相同的規範建議訂定於網路犯罪公約第 6 條。不同的是，我國採取比較嚴格的規定，以致生損害於公眾或他人的情況，始成立本罪。此外，鑑於若被害者為公務機關的電腦，可能造成更大的危害，甚至危及國家安全之疑慮，故第 361 條加重對公務機關之電腦或相關設備為目標之電腦犯罪的罪刑至二分之一。

（二）與網路相關之偽造與詐欺

廣義的電腦犯罪部份，網路犯罪公約要求各締約國需在「與網路相關的偽造」、「與網路相關的詐欺」部份進行規範，以下討論我國目前刑法在「與網路相關之偽造」與「與網路相關之詐欺」之相關規定。

1. 與網路相關之偽造

我國在 2003 年 6 月刑法修正時，除增訂妨害電腦使用罪章，並將電磁紀錄從準動產的概念刪除外，另外在 2005 年 2 月更修正刑法第 220 條準文書規定，將電磁紀錄的定義移列到總則篇第 10 條加以規範，以利電磁紀錄概念於其他罪章及法令之適用。依我國現行法規定，若偽造之電磁紀錄，得藉機器或電腦處理所顯示之聲音、影像或符號，足以表示其用意之證明者，屬刑法第 220 條第 2 項準文書之範疇，將觸犯刑法偽造文書之各罪。

2. 與網路相關之詐欺

對於與電腦犯罪相關的詐欺部份，我國於 1997 年便針對違法由自動付款設備取得他人之物，或是違法製作財產權得喪變更紀錄的部份進行處罰。但相較於其他國家的刑度（如英國已將透過網路詐欺的刑度調高到 10 年[34]），我國的刑度似乎較輕。另外，對於刑法第 339-2 條，針對透過自動付款設備取得他人之物的刑度，又較第 339 條普通詐欺罪的刑度為輕，刑度顯然失衡。針對此一問題，2003 年刑法修正時曾提出討論，建議加重刑度，但大部分立法委員認為現行刑度尚屬允當，仍維持原條文不予修正。

二、執法機關蒐證權限之規定

依據網路犯罪公約對電磁紀錄的保存規定可知，係以時間點將電磁紀錄的取得分為即時取得，與非即時取得（已儲存）兩部份分別規範。

（一）已儲存資料之取得

1. 業者的配合義務

對已儲存的部份，依據網路犯罪公約的規定，建議各締約國採取必要的立法措施，使其執法機關得以命令或相類似的方式取得已儲存的電子資料。我國

---

[32] 刑法第 360 條：「無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。」

[33] 刑法第 362 條：「製作專攻本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」

[34] 資料來源：英國內政部，網址：http://www.homeoffice.gov.uk/n_story.asp?item_id=1306，最後查詢日期：2005/6/15。

的電信法第 7 條第 2 項授權電信總局，就電信事業處理有關機關查詢電信通信紀錄部份加以規定，同法第 17 條第 2 項則授權交通部訂定關於處理第二類電信事業處理有關機關（構）查詢通信紀錄及使用者資料之作業程序。

交通部所發佈的「第二類電信事業管理規則」第 27 條則規定，電信業者對於調查或蒐集證據，並依法律程序查詢電信之有無及其內容者，應提供其資料。業者對於上述電信通信紀錄，屬於語音單純轉售服務通訊紀錄或是網路電話服務通信紀錄者，應保存 6 個月。在網際網路接取服務部份，對於撥接用戶識別帳號、通信日期、上下網時間紀錄與免費電子郵件信箱，及網頁空間線上申請帳號時之來源IP位址以及當時之系統時間，保存期間均為 6 個月；ADSL用戶與纜線數據機用戶之識別帳號、通信日期與上下網時間，以及張貼餘留言版、貼圖區或新聞討論群之內容來源IP位址及當時系統時間，均應保存 3 個月；電子郵件通信紀錄則為 1 個月。另外，虛擬行動網路服務通信紀錄則應保存 6 個月。第二類電信業者若違反本條之規定者，則可以電信法第 64 條第 2 項，處新台幣 20 萬元以上 100 百萬元以下罰鍰，並通知限期改善，屆期仍未改善者，則廢止其許可[35]。

2. 已儲存資料之搜索扣押

已儲存資料的取得，依據網路犯罪公約的規定，尚可以透過搜索扣押的方式進行。我國刑事訴訟法在 2001 年時修訂時，於第 122 條關於搜索客體的部份，加入了電磁紀錄，使得電磁紀錄在我國成為可進行搜索扣押的客體，且於 2003 年新增第 165-1 條的規定，即當電磁紀錄與文書有相同之效用時，得準用第 165 條關於書證之調查規定，且得以適當之儀器顯示之。

以電磁紀錄作為證據，還需通過「嚴格證明」之程序，其調查方式可能包含了書證、勘驗、鑑定等方式，但究應依不同性質而為不同之調查方式，或是

---

[35] 第二類電信事業管理規則第 27 條：
「經營者對於調查或蒐集證據，並依法律程序查詢電信之有無及其內容者，應提供之。
前項電信內容之監察事項，依通訊保障及監察法規定辦理。
經營者對於第一項通信電信紀錄應至少保存期間如下：
一、語音單存轉售服務通信紀錄應保存六個月。
二、網路電話服務通信紀錄應保存六個月。
三、撥接網路接取服務：
（一）撥接用戶識別帳號、通信日期及上、下網時間等紀錄應保存六個月。
（二）非固接式非對稱性數位用戶迴路（ADSL）用戶識別帳號、通信日期及上、下網時間等紀錄應保存三個月。
（三）纜線數據機用戶識別帳號、通信日期及上、下網時間等紀錄應保存三個月。
（四）張貼於留言版、貼圖區或新聞討論區之內容來源 IP 位址與當時系統時間應保存三個月。
（五）免費電子郵件信箱與網頁空間線上申請帳號時之來源 IP 位址及當時系統時間應保存六個月。
（六）電子郵件通信紀錄應保存一個月。
四、虛擬行動網路服務通信紀錄應保存六個月。
經營者應核對及等路其用戶之資料，且虛擬行動網路服務經營者應於二日內載入經營者之系統資料檔存查，並至少保存至服務契約終止後一年；有關機關依法查詢時，經營者應提供之以預付卡或其他預付資費方式經營虛擬行動網路服務者，亦同。
前項用戶之資料包括使用者姓名、身份證統一編號及住址等資料，且虛擬行動網路服務經營者力應包括所指配號碼。」

應制訂一套合適的調查方式，在我國並未有明確之規範。至於為因應科學技術的進步，證據保全部份，對於電磁證據，只要在符合刑事訴訟法第 219-1 條到第 219-8 條的情況，當事人、辯護人或檢察官得申請證據保全。

（二）即時通訊之取得

關於即時通訊取得電磁紀錄，我國則是透過以通訊保障及監察法加以規範。依據通保法之規定，通訊監察的實施，須為確保國家安全或是維持社會秩序所必要時，始可為之[36]。通訊監察書之核發，需在通訊內容與危害國家安全或社會秩序有關，且以第 5 條所定之案件範圍內為限。核發的權限，目前於偵查中由檢察官依司法警察機關申請或依職權核發，審判中則由法官依職權核發[37]；若有同法第 6 條之情形，則可由檢察官以口頭通知執行機關先予執行，並於 24 小時內補發通訊監察書。此外，若為收集情報通訊監察為目的者，則需依同法第 7 條之規定，由總理國家安全情報工作機關首長核發。

對於通訊監察的期間部份，依據通保法第 5 條所為之通訊監察，不得逾 30 日；而依通保法第 7 條而為之通訊監察，則以 1 年為限，但有繼續之必要者，則可於期滿前重新聲請[38]。

即時取得通訊之執行，經常需要電信機關的配合，所以在通保法第 14 條明確規範了電信事業及郵政機關的協助義務。業者於配合執行通訊監察後，得向執行機關請求支付必要之費用[39]。若上述機關不配合進行通訊監察，主管機關、法務部得依據通保法第 31 條之規定，得處以新台幣 50 萬元以上 250 萬元以下罰鍰，經通知限期遵行仍不遵行，得按日連續處罰，並得撤銷其特許或許可。

三、電磁紀錄的證據能力

目前我國對於以電磁紀錄做為證據，並無如加拿大一般的明確之規範，面對此種新型的證據的出現，由於我國訴訟法並未有相對應的規範，故往往由法官依據過去的經驗與傳統的證據方式，以檢驗電磁紀錄證據能力之有無。歸納我國近幾年來之實務判決，我國審判上法官對於以電磁紀錄之真實性的認定與目前實務上遭遇之困難，約略可以歸納如下：

（一）透過被告自白，而將電磁紀錄視為真實

根據我國刑事訴訟法第 156 條規定，被告之自白，非出於強暴、脅迫、利誘、詐欺、疲勞訊問、違法羈押或其他不正之方式，而與事實相符者，得為證據。爰此，若被告對於審理過程中所提出之事實均坦承不諱，且與其他證據相符時，法官會以被告自白作為判斷被告犯行的主要依據。

相同地，我國實務針對涉及以電磁紀錄做為證據之判決，若該案件經被告自白，且自白內容與其他佐證之電磁紀錄內容一致時，法官通常會將此類

[36] 通訊保障及監察法第 2 條第 1 項規定：「通訊監察，除為確保國家安全，維持社會秩序所必要者，不得為之。」

[37] 關於此部份，已有議員提出修正草案，建議應比照刑法第 128 條關於搜索票需由法官核發之規定，將通訊監察書的核發權限，改由專屬法院法官專屬。該草案已於 2007 年 7 月 11 日公布，並於公布後五個月開始實行。

[38] 通訊保障及監察法第 12 條參照。

[39] 通訊保障及監察法第 14 條參照。

電磁紀錄直接視為真實，而鮮見針對電磁紀錄的證據能力之著墨。換言之，對於電磁紀錄之真實性，除非當事人針對該電磁紀錄提出異議或請求法官進行證據調查，否則法官不會主動透過嚴格證明（如勘驗、鑑定等）的法定證據調查方式進行證據調查。台灣高等法院台中分院 93 年度上易字第 356 號判決、台灣高等法院於民國 95 年 9 月做成之 95 年度上訴字第 2482 號判決即屬此例。

惟當雙方當事人對於對造提出之電磁紀錄有質疑時，從實務判決分析，似乎必須要有積極之證據推翻電磁紀錄之真實性，否則法院傾向認定該證據具有真實性與證據能力，台北板橋地方法院 91 年度訴字 1028 號判決即採此種見解。而臺灣台北地方法院 92 年度訴字第 1411 號刑事判決認定「被告空言指摘該電子郵件可能經竄改而無證據能力云云，殊嫌無據」之見解，似乎認為若對電磁紀錄提出質疑的一方無法另外提出強有力的證據推翻該證據之真實性，或是無法對該證據提出有效的調查方法，並申請法院依職權進行調查以推翻該電磁紀錄之真實性時，則法院將認為該電磁紀錄具有真實性。

（二）透過其他證人之證言，將電磁紀錄視為真實

除了上述透過被告自白之方式外，實務上尚可見若電磁紀錄所欲證明之事實，與證人透過具結而得知證言內容相符時，即視該電磁紀錄為真實，而未再對該數位證據之真實性進行探究之案例。如同前述透過被告自白而視電磁紀錄為真實的作法，當相關證人針對犯罪事實提出證言，並依循刑事訴訟法第 187 條以降證人之具結規定進行具結時，當其證言與電磁紀錄所欲呈現之事實相同者，承審法官則會認定該數位證據為真實。

台灣高等法院 95 年度上訴字第 2674 號判決即透過證人之結證，以證明被告入侵他人電子郵件伺服器之事實。而如同前述台灣高等法院 95 年度上訴字第 2482 號判決，法官亦透過證人具結的方式，作為認定被告犯行之基礎，而對於數位證據的部分，如遊戲公司所開出之「帳號證明書」、「遊戲裝備寶物電磁紀錄流向歷程表」等之證據能力問題，並未加以探究。

（三）透過鑑定證明數位證據之真實性

所謂鑑定，係指具有特別知識經驗之第三人在訴訟程序上，本其專門之知識輔助法院判斷特定證據。對於鑑定人之角色，乃幫助法院認定某一證據問題之輔助者；其所提出之鑑定報告，法院能必須自主地審查其是否可採，不能毫無條件的全盤接受鑑定結果而作為裁判之基礎。

依據我國刑事訴訟法第 198 條之規定，審判長、受命法官或檢察官得就鑑定事項有特別知識經驗者與經政府機關委任有鑑定實務者中，選任一人或數人擔任鑑定人。依據同法第 202 條規定，鑑定人應於鑑定前具結，其結文內應記載必為公正誠實之鑑定等語。而依據第 206 條規定，鑑定人應針對鑑定之經過與其結果，提出言詞或書面報告；若鑑定人有數人，得使其共同報告之。若有不同意見，應使其個別報告。

由於鑑定人本質上與證人同為「人的證據方法」，因此，依我國刑事訴訟法第 166 條以降規定，鑑定人經合法傳喚後，有到場之義務；到場之後，有在場之義務，並接受當事人、代理人或辯護人之交叉詰問；同時未經審判長許可不得退庭。證人經合法傳喚，無正當理由不到場者，得科新台幣三萬

元以下之罰鍰。然由於鑑定人具有可替代性，加上鑑定人多以其學術、技藝或特種經驗從事鑑定，以補助檢查與司法之確實，故我國刑事訴訟法特於第 199 條規定鑑定人不得拘提。此外，若鑑定人有迴避之事由時，得向法官聲請迴避，拒當鑑定人。對於拒卻鑑定人之許可或駁回，偵察中由法官命令之，審判中由審判長或受命法官裁定之。

然從實務判決知悉，對於電磁紀錄的鑑定，可能會因為技術與設備之不足，而無法進行鑑定的情況。台灣板橋地方法院 93 年度自字第 3 號判決中即提及，對於自訴人申請針對個人電腦實施鑑定，以證明被告無故取得他人電磁紀錄一案，法院雖函請刑事局、調查局、財團法人資訊工業策進會與財團法人工業技術研究院進行鑑定，但得到的回覆分別為「尚無相關產品及技術，無法進行鑑定」、「欲偵測個人電腦紀錄有無經他人下載存取或刪除，首先該單位必須裝設有網路監控系統及防火牆，且亦須由熟悉該單位系統之 MIS 人員進行，方有可能從網路使用紀錄中去搜尋是否有異常的情況，本院歉難提供鑑定服務」等結果，故依據刑事訴訟法第 163 條之 2 規定，對於無法調查的結果，應認為不必要之證據，法院得以裁定駁回。

此外，最高法院 94 年度台上字第 579 號判決表示，經過鑑定人鑑定並具結的證據，並非一定具有證據能力，仍須符合程式上的形式要件，始得具有證據能力。然即便賦予該鑑定報告證據能力，仍只是協助法官心證之形成，對於法院之審判並無拘束力，故待證事項雖經鑑定，法院仍得依職權加以調查，以期發現事實之真相，如對鑑定報告存有疑義，於究明之前，仍不得遽採為判決之基礎。

該判決中以測謊鑑定為例，認為目前刑事訴訟法對於測謊鑑定的證據能力並未規定，實務上必須符合刑事訴訟法對鑑定之要求外，形式上仍必須符合測謊的基本程式，如受測人同意配合、測謊員必須經良好之訓練、測謊儀器品質良好且運作正常、受測者身心正常、測謊環境良好等要件，該測謊鑑定始具有證據能力。

依據最高法院之見解，在電磁紀錄真實性的鑑定上，未來勢必也要具備相類似的鑑定程式，例如標準的鑑定流程、獨立的鑑定環境、精密且正常運作的儀器、訓練有素的鑑定人員、完善的證據保護機制，甚或是相關法律人才的加入，該鑑定報告才可能具有證據能力，始得成為法庭上之證據。

雖在目前電磁紀錄真實性之鑑定程式尚未確立，且尚未見當事人利用此一理由作為質疑鑑定報告之證據能力的案例發生，然為避免未來數位證據鑑定報告之證據能力遭受質疑，並強化數位證據之鑑定報告在法官形成心證時所扮演之重要性，我國似有必要建立一套標準的鑑定流程，並成立專業的數位鑑識單位，以強化我國對抗網路犯罪及處理電磁證據做為證據時可能遭質疑的真實性問題之能量。

陸、結論及建議

網路的興起與普及，使得本應在傳統世界進行的活動，開始轉由透過網路世界進行。大眾對於網路之使用與依賴，從日常生活之購物、朋友之間的互動、資料與訊息的找尋，到公司與公司之互連，甚至重要的國際會議，都紛紛透過網路進行可見一般。然如何維護大眾使用網路之安全，已成為各國所重視

之議題。目前聯合國、歐洲理事會與 APEC 等紛紛針對網路犯罪之議題提出相關至法制修正建議與政策，希望各會員國均能修正其內國法制，並制訂相關之防制政策，以期達到各國共同對抗網路犯罪之決心。

身為 APEC 之一員的台灣，為對抗國內可能產生之網路犯罪問題，並聯合世界各國共同遏止跨國之網路犯罪，亦順應國際組織之修正建議，修改相關之法規，並制訂相關之安全政策。從上述討論可知，台灣刑法三十六章妨害電腦使用罪章對於網路犯罪之規範，即參考聯合國與歐洲理事會所提出之網路犯罪公約的規範進行修正，而各行政主管機關亦研擬相關的配套與政策，以規範網路之使用與維護網路之安全。有此可見，目前台灣對抗網路犯罪之實體法制規範，尚可稱是完備。

然面對網路犯罪的發生，執法人員如何有效的追查網路犯罪，對於數位證據或網路犯罪之證據如何取得以保存，甚或在法庭上數位證據的認定與真實性之證明等問題，則為台灣地區目前尚待有效的解決之問題。以目前科技發展之程度而言，電磁紀錄仍屬於一種尚難以完全信賴之證據型態，因此對於電磁紀錄之證據資格就必須仔細檢視，也賦予提出者更多之舉證責任。未來我國修法方向，也應建立一套標準，讓法院審理案件時有所依循，而不會再有「一語帶過」的判決結果出現。

最後，本文對照國際趨勢，提出幾點未來修法或管理之建議:

（一）刑法第 36 章增加「非法截取」之規定

綜合上述，就國際公約所要求的電腦犯罪規範，在我國均有相呼應的法規。從國際趨勢檢視我國在規範電腦犯罪之法制，我國的規範應屬足夠。我國新增之刑法第 36 章妨害電腦使用罪章之規定，包含大部分國際公約對於侵犯電腦資料與系統機密性、完整性與可利用性部分的規定。但我國在認定犯罪者是否構成第 36 章之犯罪時，普遍較國際公約來的嚴格，大部分均需有實質造成損害的情況，始符合構成要件。

雖然本章立法過程中，不乏有立法委員傾向應嚴格規範電腦犯罪的行為，並且要求應對電腦犯罪者處以重刑。但為避免立法過於嚴苛的狀況，最後的決議只對情節重大或對公眾或個人造成損害的情況之行為作處罰；並將本法第 363 條規定，第 358 條至 360 條之罪設計為告訴乃論之罪。此種規範，除了一方面考量到網路犯罪造成的損害，輕重有別，應由被害人決定是否提出告訴，還必須考量到網路犯罪之偵查，若被害人無意願配合，實難達成偵查之成效[40]。

比較特別的是，關於網路犯罪公約第 3 條對於非法截取的部份，並未於規定於妨害電腦犯罪罪章之中。主要的理由，是因本條的立法用意主要在保護資料傳輸的隱私性與機密性，如電話、傳真或電子郵件等[41]，此與我國通訊保障

[40] 請參照刑法部份提文修正案（電腦網路犯罪部份）第 363 條修訂說明。
[41] 同註 27，頁 134。

與監察法（下稱「通保法」）的立法目的相同[42]，故當時在立法時，法務部依據實務界之見解，認為可透過通保法進行規範即可，不需額外立法[43]。

雖說立法目的相似，但以通訊保障及監察法作為非法截取之法規範，學界與實務界有相當大之爭議。探究通保法之設計，如通訊監察書之核發，學者認為通保法僅規範政府對人民進行通訊監察之範疇，不應擴張解釋。

另外，以通保法規範「非法截取」，刑度考量上是否與其他電腦犯罪之罪刑一致，易產生衡平上的疑慮。就我國刑法第 358 條之規定，利用電腦系統之漏洞入侵他人電腦，對個人隱私權的侵害不亞於非法攔截他人傳輸中資料所造成的損害，但違反刑法第 358 條規定之刑度，為 3 年以下有期徒刑；甚至第 359 條無故取得他人電磁紀錄，需造成他人損害之情況下，始有刑罰之適用。相較之下，若以通保法第 24 條第 1 項違法監聽他人通訊，視為非法截取的懲罰依據，為 5 年以下有期徒刑的刑度，似乎較前述對於非法入侵及非法取得的刑度為重，值得修法時加以斟酌考量，是否應將非法截取的規範回歸刑法第 36 章較宜。

（二）縮短業者保存資料期間，並加強查察

我國通保法以及第二類電信事業管理規則視之，我國對於電信業者保存紀錄的時間，似乎比較國際組織所要求之 90 日為長。依據網路犯罪公約，業者的儲存義務不應超過 90 日，以免增加業者太多負擔，但為避免突發事故，若 90 日的儲存期限不夠，則可於期限屆至前申請延長。本文認為，考量對業者造成的負擔與執法機關是否有能有效負起查察的責任，確保各電信業者均依規定辦理，應是思考保存期間長短之重點。故本文建議修正相關規定，縮短業者保存電信資料的期間，以符合國際趨勢；同時，相關主管機關亦應負起督導之責任，以確保已保存之通信資料的可用性。

如同網路犯罪公約所言，保存的時間越長，對業者造成的負擔也越大，雖說依據「電信事業處理有關機關查詢電信通信紀錄實施辦法」第 6 條與第 7 條明訂查詢機關應付查詢費用的規定，但是否能減輕業者的負擔，則需要實地瞭解。另外，目前業者針對電磁資料之保存，是否依據上述規定之要求辦理，也不無疑問。建議相關機關應確實探查電信單位之需求，以訂定合理之價格。

（三）建立合適之電磁紀錄法則

自我國法院之判決結果觀之，若當事人爭點涉及電磁紀錄時，判決內容對於電磁紀錄之真實性等相關訊息多半無深入的探討與分析，而多透過被告自白、證人證言或鑑定人鑑定之結果，證明該電磁紀錄具有證據能力。然電磁紀錄與一般證據的性質不同，容易受到竄改或偽造。對於此類遭竄改或偽造之電磁紀錄，訴訟之一方提出對其證據能力與真實性的質疑時，卻可能因為提不出有利的資料加以反駁，或是無法取得作為證明之資料等舉證上之困難，導致其提出之質疑不被法院所接受。

---

[42] 通訊保障及監察法第 1 條規定：「為保障人民秘密通訊自由不受非法侵害，並確保國家安全維持，維護社會秩序，特制訂本法。」

[43] 根據台灣高等法院檢察署 (89) 法字第 000805 號函(2000/6/16)，法務部研究意見認為通訊保障及監察法第 24 條第 1 項規定，立法意指係針對一般民眾，故我國對非法截取之行為，只需透過通訊保障及監察法加以規範即可，不需另訂法律。

為避免上述情事之發生，且避免法院未依職權蒐集證據或曉諭當事人提出證據，以致法院未能建立每一構成要件要素間之連結，或是產生跳躍性的證據認定與心證形成，本研究建議相關單位應參酌美國的作法，仔細審視電磁紀錄作為法庭證據的特性，並瞭解實務運用上產生的問題。針對現有不足之處，修正現有之刑事訴訟法關於證據之規定，或是訂定新電磁紀錄的證據法則，以作為各級法院判案之依據。

（四）建置標準化鑑識流程（SOP）

在我國目前之法制規範中，證據為法官認定事實之基礎，而關於法庭中證據之資格限制在我國有甚多之規定。然就整體刑事訴訟之過程觀之，欲使法庭中之證據有證據能力，在偵查階段檢察官及其輔助機關蒐集證據、保全證據之步驟就必須符合法令之規定。但我國目前對於執法人員如何針對電磁紀錄進行搜索、扣押與保存應注意之事項以及應踐行之步驟並無一致性的明確規範。

為使檢調單位在證據蒐證上有相關的步驟可以遵循、確保檢警調所蒐證之電磁紀錄的真實性、電磁紀錄鑑定之有效性，並強化法官之自由心證，我國除應建立專業的鑑定實驗室之建立外，還有必要建立一套電磁紀錄蒐證與鑑識之標準作業流程，以供檢警調於蒐證與鑑識人員進行鑑識時之參考。

對於標準作業流程之要求部分，如同最高法院 94 年度台上字第 579 號判決以測謊鑑定為例，提出鑑定之程序除了要符合法律規定外，尚須符合如獨立的測謊環境、良好的儀器、訓練有素的測謊人員等形式上的要求，欲使用電磁紀錄當作訴訟上之證據時，該電磁紀錄亦必須以法定之證據方法為之，並經過合法調查證據程序。爰此，本研究建議仿照我國最高法院 94 年度台上字第 579 號判決對測謊鑑識之見解，要求相關鑑識機關進行數位鑑識時，除了要符合法律規定外，尚須符合形式上的要求，例如獨立的鑑識環境、良好的儀器、專業的鑑識人員、完善的鑑識程序等要求，以確保鑑識報告之可信性。