



論網路犯罪問題介紹與探討

作者 / 劉俊男



提要

由於網際網路之快速興起，創造出新的網路社會生活形式，但也隨著科技之發展與變遷，亦不斷湧現出各種社會問題與犯罪模式，例如言論自由之問題、商業交易之陷阱、智慧財產權之侵害、刑法及相關法律之違反，當然還有法院管轄權之問題等，均隨著網際網路之普及而逐漸浮上檯面，而本文則藉由分析網路犯罪之特性與類型態樣，提出未來預防之方法與策略，以提供網路社會成員解決網路犯罪問題時之參考，期使網路社會更加秩序化與純淨化。

關鍵字：電腦犯罪、網路犯罪、網際網路、網路犯罪模式、管轄權、預防對策。

壹、前言

網際網路起源可溯至1960年代之發展，基於美國國防運作體系考量，美國國防專家希望能藉由軍事電腦分散式網路之建立，對於軍事指揮和通訊中心如一旦遭受飛彈攻擊時，可能致使網路連結破壞事件發生，

即能避免國防運作機制受到完全或嚴重之癱瘓，故於1980年代結束前，有數個其他網路型態已被建立，此類網路被連接在一起，以構成一種「網路中網路」—衍變網路(Metanetwork)，即為今日所稱之網際網路。^①而現今人類社會快速變遷，網際網路今日不僅運用於國防軍事科技上，亦成為現今人類日常生活搜尋資訊不可獲缺之工具，惟因網際網路受到人民之廣泛運用，故網際網路之犯罪與倫理問題即成為今日資訊e化社會首當其衝之問題，^②如人們應對在網路上放置色情或暴力等圖文負起法律責任，惟此類犯罪行為人則常因匿名或超越執法人員之偵防技術而無法被認定，再加上各國法律規範不一致等因素，導致其無法受到應有法律之約束與制裁。因此，隨著網路逐漸成為人類生活一部分，網路上之各種脫序現象，亦如影隨行而來，逐

①：參閱吳國清，網際網路行為與警察作用，2000年第2屆網際網路空間：資訊、法律與社會研討會論文集，中央警察大學，2000年12月，頁97。

②：參閱林宜隆、黃讚松，網路犯罪學之探討，中央警察大學學報第38期，2000年，頁332。



漸引起大眾之關注。是以除網路駭客入侵，造成各種嚴重破壞外，其他諸如軍火教父、網路色情援交、網路誹謗、網路詐欺、網路竊盜等案件之發生，亦使得網路犯罪成為大眾所關切之焦點。故網際網路則像一輛無法回頭之馬車，正以風馳電掣速度，載著人類不斷地向前奔馳，當我們為車窗外急速變換之美景所眩惑時，則應靜心省思。另因電腦科技日益進步快速，犯罪手法與偵防技術一變再變，防制電腦網路犯罪亦須不斷進步且不能停頓，故本文希藉由分析網路犯罪之各類型態逐一檢視，並針對網際網路核心問題，作深層研究，以了解網路犯罪之形成態樣，並進而提出網路犯罪之整體預防對策。

貳、網路犯罪之定義

無論於何種時代或社會中，「犯罪」問題可說是無法完全被消滅的，換言之，無論社會如何轉變，時代如何進步，犯罪問題依然均會存在；然而隨著生活環境之變遷，犯罪之種類與型態亦會隨之改變；如今在網際網路發展如此迅速之時代中，逐漸改變了傳統社會之生活，它雖然帶來了快速、便捷、有效之溝通方式，但同樣的，脫序、違

法之行爲亦隨之而生。^③因此，網路犯罪相應產生亦是平常之事，而所謂「網路犯罪」（Cybercrime）從歷史角度來看，其可說是由「電腦犯罪」（computer crime）之型態及概念逐漸演化而來，但網路之特性終究與電腦之使用行爲不同，故在談網路犯罪時，則應首先必須將「網路犯罪」與「電腦犯罪」作一區別，並加以釐清，說明如下：

一、電腦犯罪：何謂「網路犯罪」？

則須先從電腦犯罪分述起，一般而言，國內有學者^④將電腦犯罪區分為廣義說、狹義說、折衷說，其中採廣義說則認為所謂「電腦犯罪」係泛指所有與電腦科技或電腦系統有關之犯罪，意即「與電腦有關之犯罪」，此說顯然過於廣泛，並無任何實質意義；採狹義說者認為「電腦犯罪」乃指與電子資料處理有關而故意違法破壞財產法益之「財產罪」，此說則又顯過於狹隘，僅將電腦犯罪界定為財產犯罪，勢將無法涵蓋全部之電腦犯罪。至折衷說則認為「電腦犯罪」乃指行爲人濫用電腦^⑤或破壞電腦而違犯具有電腦特質(Computer Property)之犯罪行爲，就電腦特質觀點言，是指自然人濫用、誤用^⑥或破壞電腦而違犯具有電腦特質之犯

③：參閱楊惠貞、曹文瑜、郭汶川、賴雲龍等，網路犯罪與網路規範之探討，勤益學報第18期，2000年12月，頁127。

④：參閱林山田，電腦犯罪之研究，收錄於刑事法論叢（一），1997年3月再版，頁137-138。

⑤：同註④，頁139。

⑥：「濫用」係指對電腦資產或資源之不當（尤指故意非法）使用；「誤用」則偏向於錯誤（尤指無知或無意）之使用。轉引自吳國清、廖有祿、高大宇合著，電腦犯罪與執法認知之探討，警學叢刊31卷3期，2000年11月，頁135。



罪行為。而所謂「電腦特質」則係以行為之違犯、追訴或審判是否需要電腦之專業知識為斷，故「電腦犯罪」定義即指行為人濫用電腦或使用足以侵害電腦硬體或軟體行為，而造成與電腦特質有關之犯罪。^⑦因此廣義說與狹義說皆有實際上過與不足之缺點，所以目前則以折衷說之見解較為可採，惟仍有爭論，國外亦然。^⑧

二、網路犯罪

「網路犯罪」目前尚未有嚴格之定義與統一見解，一般多將之與電腦犯罪混為一談，或視其為電腦犯罪之下位概念，而認為網路犯罪係指在電腦犯罪中須藉助網際網路遂行其犯罪意圖之犯罪而言，例如藉由網路獲取不法利益、詐財、恐嚇、傳遞暴力或妨害風化之訊息等。^⑨此說固非無見，亦未影響電腦犯罪或網路犯罪之法律效果，惟將此二種顯然有別之犯罪類型模糊融合，則顯輕忽具有「網際網路」特性之犯罪行為，而無法對於網路犯罪有深入之探討與了解。如

未能對網路犯罪有一深入而全面性之定義，即對未來網路犯罪防制將是漫無方向。^⑩而「網路犯罪」固係電腦犯罪之延伸，是一種利用網路獨有之特性，而為犯罪手段或為犯罪工具之網路濫用行為，^⑪並為電腦系統與通訊網路相結合之犯罪，相較於電腦犯罪而言，更偏重於「網際網路」之應用，專指具有網際網路特性之犯罪，易言之，行為人所違犯之故意或過失之犯罪行為中，必須行為具有網際網路之特性者而言，就實際應用而言，犯罪者在犯罪過程中，須借助網際網路，方能遂行其犯罪意圖之犯罪，即屬網路犯罪。^⑫

三、網路犯罪與電腦犯罪差異性之比較

網路犯罪多數學者認為係由電腦犯罪所延伸之一新興犯罪型態，故網路犯罪與電腦犯罪具有極高之相似性，但其內涵卻又不盡相同，雖然二種犯罪型態均須利用電腦系統或其相關設備為犯罪手段，且犯罪黑數均高，^⑬並為專業性犯罪，偵查均困難^⑭等

⑦：參閱林山田、林東茂合著，犯罪學，三民書局，1997年10月，頁460-463。

⑧：參閱林東茂，德國近年來的經濟刑法發展趨勢，收錄危險犯與經濟刑法，五南圖書，1996年9月，頁118-119。

⑨：參閱林宜隆，建構預防網路犯罪整合安全體系之研究新取向，中央警察大學學報第33期，1998年9月，頁379。

⑩：參閱林宜隆、黃明凱，網路犯罪模式分析及案例研討，2001年第3屆網際網路空間：資訊、法律與社會研討會論文集，中央警察大學，2001年12月，頁160。

⑪：參閱馮震宇研究主持，網路使用犯罪問題及預防措施之研究，行政院研究考核委員會編，2000年4月，頁9。

⑫：參閱林宜隆，網際網路與犯罪問題之研究，中央警察大學出版社，2000年3月，頁71。

⑬：同註④，頁150。

⑭：參閱林山田，論電腦犯罪，軍法專刊第30卷第8期，1986年8月，頁5。

相同特質，但由於網路犯罪較偏重於網路科技為犯罪行為之實行，比電腦犯罪具有較高之網路性質，而不同於電腦犯罪僅偏重單純利用電腦系統或其相關設備而為犯罪行為之施行。同時，二者特性亦有許多不同之處，如網路犯罪具有高度之匿名性、使用者之不確定性、無遠弗界性及行為影響廣泛性等特性，皆為電腦犯罪所無。故網路犯罪所具有之特性與電腦犯罪之特性雖有相當程度之雷同，但仍有區別，並非完全相同，亦可由此二種犯罪之不同特性來作為網路犯罪與電腦犯罪之區別。雖然網路犯罪可說是由電腦犯罪所衍生而來，但因其犯罪兼具電腦及網路之雙重特質，故其影響及複雜性皆遠高於電腦犯罪。然而就上述之特質看來，「網路犯罪」一詞之可怕性不在於犯罪，而是政府無法掌握，無法偵查犯罪事實及罪犯，¹⁵難怪網路犯罪會成為各國政府所面臨治安上最頭痛的問題之一。

參、網路犯罪之特性

網路犯罪乃係因資訊發展後新興之犯罪型態，其特質與傳統犯罪類型有所差異，且

因網路犯罪為電腦系統與通訊網路相結合之犯罪，一般而言，網路犯罪應具有以下之特性：¹⁶

一、係利用電腦之特性遂行其犯罪目的：網路犯罪並非專指刑法中之某些犯罪類型，絕大多數犯罪均可能透過電腦的特性予以實施，所謂電腦之特性包括：分散性、開放性、互通性、隱密性、立即性等。¹⁷

二、行為與結果間之時間與空間之區隔：網路犯罪之行為實施與結果發生，在時間與地點上通常均有所間隔，換言之，行為可能須經過一段時間後才既遂其犯罪目的，或行為地與結果發生地有相當大之區隔，因此當犯罪結果發生時，常很難再找到犯罪行為人，而使其得以逍遙法外。¹⁸

三、高犯罪黑數：網路犯罪因係行為人利用電腦進行犯罪，在本質上即難以發現，且因多牽涉個人或企業之信譽與秘密，被害者多不願聲張報案，加之此類犯罪追訴成效及破案率均偏低，因而導致網路犯罪具有相當高之犯罪黑數。¹⁹

四、犯罪成本及障礙低：傳統犯罪或多或少均需克服空間距離與時間差異之障礙，

¹⁵：參閱李歐文，網路犯罪引發網路立法效應，通訊雜誌，1997年1月，頁18。

¹⁶：同註¹²，頁77-78。

¹⁷：參閱林宜隆、黃讚松、楊麒麟等，網路社會中犯罪問題之研究，警學叢刊第31卷第6期，2000年5月，頁205。

¹⁸：參閱林宜隆，網路犯罪與網路預防之探討，犯罪學期刊第3期，中華民國犯罪學學會，1997年12月，頁149。

¹⁹：參閱林山田，電腦犯罪之研究，政大法學評論第30期，1993年7月，頁56；莊忠進，電腦犯罪偵查之探討，刑事科學第39期，1995年3月，頁125-149。



若為親身犯罪則更須冒高度被識破身分及被現場逮捕之風險，此種風險乃係抑制犯罪發生之重要條件，惟於網路犯罪領域中，此種障礙均能透過網路技術加以克服，故此無疑將導致網路犯罪之氾濫。^{②①}

五、偵查不易：由於網路犯罪行為人之身分不易確定，犯罪行為亦不易發覺，且犯罪證據不易保全，執行偵查人員之網路技術不夠熟稔等特性，使得網路犯罪之偵查工作常十分困難，再加上網路跨地性之特質，使得本來就偵查不易的網路犯罪在困難度上更是雪上加霜，故網路犯罪亦由於具有上述之特性致使其不易偵查，甚至無法偵辦。各國法律與實務對於某些行為是否違法之判斷標準不同（如槍、賭、色情之認定），亦使跨國性網站之非法行為，造成偵查上困難度。

六、犯罪客體多樣化：網路犯罪之型態，除了前述電腦犯罪之一般型態外，網路犯罪另一個最大之特色即係其犯罪態樣之多樣化，^{②②}有針對電腦軟體之侵入與破壞者，如透過網路侵入他人電腦系統竄改資料（即電腦駭客）、散播電腦病毒、利用網路成立色情網站、張貼猥褻圖片及文章及散布不實或誹謗言論等，均是網路犯罪之客體；而網

路犯罪之型態可能不僅前述幾種態樣，因網路犯罪之犯罪型態是不斷更新，此乃一般傳統犯罪所無之特色。

七、行為跨區域性：網路架構了全球性資訊網路，進而產生網路無國界之特性，故網路行為可輕易地跨越國家及地域而進行，使用者所為之行為，只要有網路之地，無論在何地均可透過網路設備而受到影響，另因此一特性所造成的另一個問題，即便是管轄權之問題，因犯罪行為跨越二地以上，何地有管轄權，即是跨地性所衍生出來的問題，^{②③}有關於此一管轄權之問題，則容後再行探討。

肆、網路犯罪之類型態樣

在數位化之環境中，由於一切資訊均以數位化、電子化之形式存在或儲存，因此，若未能有足夠之安全機制，則數位化之資訊即可能會因他人未經授權或違法之行為而遭到竄改或滅失，同樣的，若他人透過網際網路連線亦可能破解防火牆等安全機制，或散布病毒、或對系統進行癱瘓網路之攻擊，非但電腦系統中所儲存之電子資訊無法受到保護，就連電腦之利用也會受到影響，^{②④}也

②①：同註②，頁333。

②②：詳見林宜隆、邱士捐，我國網路犯罪案例現況分析，資訊、科技與社會學報第3卷第2期，2003年12月，中央警察大學資訊管理學系出版，頁76-81。

②③：參閱王銘勇，網路犯罪相關問題之研究，臺灣新竹地方法院90年度研究發展項目研究報告，臺灣新竹地方法院印行，2001年11月30日，頁25-26。

②④：參閱馮震宇，網路犯罪與網路犯罪公約（上），月旦法學教室第4期，2003年2月，頁125-126。



因為如此，網路犯罪亦與電腦資訊安全、個人身分及隱私有密切相關。事實上，網路犯罪之威脅並不限於我國，而是普遍發生在與網際網路連線之國家，雖各國所面臨之網路犯罪或有所不同，但其類型仍有相當之類似性，故以下則僅就我國所發生之各種網路犯罪類型態樣加以探討：

一、網路犯罪之範圍：網路犯罪類型從技術層面，可分為2大類，一為阻害電腦網路機能系列犯罪；二為非法使用電腦網路系列犯罪。從網路犯罪特性言，僅限於利用網際網路之特性，如具有分散性、開放性、互通性、隱密性、立即性等之犯罪行為，始屬網路犯罪。與網路相關之犯罪，依網路在犯罪中所扮演之角色，可分為以下各類：

(一)以網路及連結在網路上之電腦系統作為犯罪工具。如網路恐嚇、網路詐欺取財、刪除竄改電腦紀錄。

(二)以網路作為犯罪場所。如網路色情、販賣軍火、網路誹謗、教授製作炸彈。

(三)以網路及連結在網路上之電腦系統作為犯罪之攻擊目標。如散播電腦病毒、網路竊聽。

(四)以電腦或相關電磁紀錄之設備，作為攻擊客體之類型。如無故入侵電腦、無故取

得刪除變更電磁紀錄、無故干擾他人電腦及製作專供電腦犯罪之程式等。

以上第2、3類屬網路犯罪之範疇固無疑義，惟關於第一類以網路為犯罪工具是否為資訊犯罪，即有爭議，但如前所述，網路具有迥異於其他一般傳統工具之特性，以網路為犯罪工具顯然不能與以一般器物為工具之犯罪相提並論，尤其在犯罪之偵查與抗制上，更有截然不同之意義，故亦應含括於網路犯罪之範疇。²⁴另第四類即係以電腦或其相關設備及網路作為行為侵害對象之類型，²⁵故亦屬網路犯罪之範圍。

二、網路犯罪模式分析：網路犯罪模式乃係網路犯罪者為達其目的於網路空間(Cyberspace)中所採取之方法，網路犯罪模式隨著網際網路之發展而日新月異，但不論是何種方法均是在非法、未授權情況下進入他人之網路或系統。故本文乃嘗試以較具體分類，將網路區分為傳統網路犯罪型態和新型態網路犯罪，以建立有脈絡可循之網路犯罪模式。試說明如下：

(一)傳統網路犯罪型態

1.網路色情：網路色情係指利用網路提供各種露骨之性行為討論及色情資訊等文字、圖片、影片等方式呈現，²⁶如散布或販

²⁴：同註12，頁75-76。

²⁵：參閱柯耀程，刑法新增「電腦網路犯罪規範」立法評論，月旦法學教室第11期，2003年9月，頁117。

²⁶：參閱廖有祿、莊懿強，中文色情網站之實證研究，資訊、科技與社會學報第5卷第2期，2005年12月，中央警察大學資訊管理學系出版，頁108。



賣猥褻圖文、動畫等。又如設立色情網站、一夜情交易中心、媒介或自行設立網路一夜情、銷售色情光碟影片、聊天網站或其他方式進行援助交際自拍、情色貼圖、公然猥褻及散播情色資訊於網路聊天室間或公眾領域等行為均屬之。

2.網路恐嚇：係指利用網路作為工具來對某特定或公眾之人進行內容訊息傳達，以達騷擾、恫嚇或勒索他人，使受恐嚇人懷有恐懼之心或人身安全威脅為目的者，如民國84年12月間國內中山大學曾發生以電子郵件恐嚇美國總統柯林頓案件，若以此事件為例而恐嚇之，因此而致生危害於其安全者，則應該當刑法第305條之恐嚇危害罪。

3.利用網路公然侮辱、誹謗或其他妨害名譽或信用：即係利用電子郵件（E-mail）、網際網路校園版的電子布告欄上（BBS站）或其他網路媒介散布或傳述不實言論，如政大學生上網罵教授案。²⁷故如上述利用E-mail、BBS站或其他網路之媒介散布或傳述不法言論（如誹謗、公然侮辱、妨害信用等），依其情形則可分別成立刑法妨害名譽或信用罪章之各罪，與一般妨害名譽案件之不同，僅在於其所利用之傳播工具之不同而已，因此並不生適用上之困難。

4.網路賭博：利用網路空間作為公共

場所，並以電腦軟硬體作為賭博器具，來賭博財物，如民國88年3月發生「紅黑爭霸戰」巨額網路賭博案件。因此，網路之發展則提供了一個極佳之環境，使得好賭之人有了一個絕佳管道參與賭博，而網路賭博行為是否可以現行刑法之賭博罪加以規範，則似乎產生了不小之挑戰。²⁸因我國刑法第266條賭博罪所規定之「場所」乃限制在於公共場所或公眾得出入之場所賭博財物，方構成本罪之構成要件，換言之，「網站」是否可認為係傳統刑法概念下之「場所」，不免有所疑議，因此，為免日後適用上之爭議，可建議有朝一日於刑法分則修定時亦能將此部分明定，以規範網路賭博之犯罪模式。

5.利用網路煽惑他人犯罪：即於網路上公然販賣毒品、槍枝或其他煽惑他人犯罪之不法行為，如軍火教父網站賣槍枝即屬之。由於網際網路具有高度隱匿性之特質，許多人則利用網路此一特性，進行上述不法之犯罪行為，對社會之影響不可謂不大。然而如透過網路來進行煽惑他人犯罪之行為，則除可能構成刑法第153條「煽惑他人犯罪」之罪外，另如透過網路網站公然販賣毒品或槍枝之實際販賣行為時，則另可依槍砲彈藥管制條例之販賣、持有或運輸槍砲之罪及毒品危害防制條例之規定分別處罰之。²⁹

²⁷：參閱蔡美智，談網路犯罪，資訊法務透析，1999年1月，頁41。

²⁸：參閱馮震宇、劉志豪，我國網路犯罪類型及案例探討，月旦法學雜誌第41期，1998年10月，頁87。

²⁹：同註²⁸，頁86。

6.網路詐欺：意圖為自己或第三人不法之所有，以不正方法將虛偽資料或不正指令輸入電腦或其相關設備，製作財產權之得喪、變更紀錄而取得他人財產者，如網路老鼠會屬之，又如網路金錢連鎖信更是大量透過BBS與電子郵件流傳，而各種新興之網路詐欺類型更是不斷增加，但問題日益嚴重的，則是利用不當方法將虛偽不實之資料輸入電腦資訊系統，進而影響其處理資料之結果，如信用卡之盜刷問題。³⁰傳統之詐欺行為，除須具有為自己或第三人不法之所有意圖外，仍必須要以「詐術」使人陷於錯誤而將本人或第三人之物交付或使第三人得利之行為，始符合刑法詐欺罪之構成要件。而此定義是否適用於以不當方法將虛偽不實之資料輸入電腦資訊系統，進而影響其處理資料之結果之行為，仍有爭議，然後來刑法修正為鑒於此一問題日益嚴重，則於該法第339條之3明定：「意圖為自己不法之所有，以不正方法將虛偽資料或不正指令輸入電腦或其相關設備，製作財產權之得、喪、變更資料，而取得他人資料者，處一年以下有期徒刑」，以解決規範此一犯罪型態。

(二)新型態網路犯罪

1.無權侵入他人電腦系統行為：在網路成為犯罪之新興工具之後，最明顯之新興網路犯罪類型，即是駭客入侵型之犯罪，亦

即指行為人原無權使用他人電腦系統而侵入他人電腦系統以利用其服務之不法行為。惟雖然有些駭客入侵並非在於竄改資料，僅在表現其破解安全裝置之技巧，或基於其他目的，但均會對被入侵網站往往造成一定之影響，這些駭客之行為還可以區分為單純破解或入侵他人電腦資訊系統，與侵入電腦系統竄改或破壞他人資料，如民國83年間EPSON公司底稿設計等二大類型，特別是後者影響最為嚴重，因此各國亦紛紛將此等行為列為網路犯罪之一環，並加以規範。我國刑法亦鑑於此，業於2003年刑法修正時，已將對無故侵入他人電腦與無故刪除變更電磁紀錄等行為明文加以規範。³¹

2.利用網路散布病毒：指有意破壞電腦系統運作者，刻意設計一種特定之電腦程式，經輸入後隱藏於其他系統程式中，或依附於執行程式上，於間隔一段時間後，經不斷自動複製、蔓延、拷貝等方式連續擴散直致佔滿整個記憶體或磁碟機之空間為止。如1988年美國著名的Morris一案，Morris當時為康乃爾大學電腦科學研究所博士生，其為



³⁰：同註²³，頁128。

³¹：刑法第358、359條參照。



凸顯當時電腦網路安全於防護上之缺失，因此撰寫著名的蠕蟲（Internet Worm）病毒程式，並將之釋放至網際網路，後此病毒則經由網路散佈，造成美國國防中樞五角大廈內千部電腦全數當機，連帶波及全美多所著名大學、軍事單位及醫療研究機構計7,000部電腦主機，造成全球電腦的空前損失，³²針對該案美國法院則援引「電腦詐欺與濫用法」（Computer Fraud and Abuse Act）中未經授權侵入電腦罪加以處罰。而相對的，我國之前亦時有發生嚴重的網路病毒散佈事件如CIH車若比爾病毒散佈事件，故我國於2003年刑法修正時，即於其第362條中增訂製作專供犯本章（妨害電腦使用罪）之罪之電腦程式罪，舉凡製作專供侵入他人電腦、或藉以取得他人電腦資料或用以損毀、干擾他人電腦使用之電腦程式者，且用以供製作人或他人作為妨害電腦使用者，乃成為本罪成立之基本條件，³³以規範利用網路散佈病毒之犯罪模式。

3.非法重製電腦程式或檔案：即行為人未經原著者同意重製他人之電腦程式或利用網路下載電子佈告欄網友發表之言論，製成光碟片販售圖利。由於我國著作權法對著作權人之權利規範極為廣泛，但對於限制著作權人權利規定則極為嚴格，明顯偏向於保護著作權人，而不利於著作利用人，因此，若依我國著作權法之規定，目前於網路上涉及他人著作之各種利用行為，若不符該法第44條至第63條除外規定時，幾乎均有可能違

反著作權法之規定。³⁴因此，在BBS站上發表具有原創性之言論應屬於著作，而得受著作權之保護，若他人未經同意而重製，則會侵犯著作權。

4.網址名稱或商標權之侵害：網址名稱即係網際網路上一個類似地址的識別碼，其重要性不僅止於地址功能，且又近似自然人之姓名或法人名稱，往往網路使用人均可透過網址名稱而得知該網站係由何人提供，或所提供之服務及資訊類型為何？因此，商標專用人通常不論商品或服務類別均主張應根據其商標專用權而取得網址名稱，或對他人已先行登記之相同或類似之網址名稱，主張侵害其商標專用權稱之。

伍、網路犯罪之管轄權

隨著電腦網路設備之逐漸普及，於每一個人的生活之中，不論消費、金融、醫療，甚至娛樂等，電腦網路均扮演著重要地位，因而引發犯罪率之增加，且因電腦網路犯罪往往跨越國內行政管轄與國境，亦即具有跨區域之特性，因此，就該類犯罪，是否歸屬為國內犯罪？及該類犯罪之刑事管轄權應如何決定？即具有極大爭議，故以下僅就電腦網路犯罪之一般犯罪管轄權判斷，來探討網

³²：參閱慶啓人，駭客、病毒與垃圾郵件—若干網路犯罪之中外案例初探，法學叢刊第184期，2001年10月，頁73。

³³：同註²⁵，頁125。

³⁴：同註²⁸，頁89。



路犯罪之刑事管轄權決定標準，說明如下：

一、傳統一般犯罪之管轄權：我國刑事訴訟法關於管轄權之規範，主要有土地管轄、事物管轄、競合管轄及牽連管轄等管轄種類。而依我國管轄之規定，主要係建立在事物管轄及土地管轄二項標準上，法院因此而取得對某一案件之管轄權者，一般稱為「固有管轄」。³⁵案件依事物管轄，只能定出何級法院管轄第一審而已，同級法院之案件如何分配，仍應取決於土地管轄。而土地管轄即係依該案件與法院所轄土地之關係，分配於第一審法院之管轄權。因我國各法院於管轄區域上有一定範圍，就特定刑事案件，應由何地之法院管轄，須有一定標準。另我國刑事訴訟法對於土地管轄之規定，則因犯罪地在國內或國外犯罪而異。

(一)國內犯罪：依我國刑事訴訟法第5條第1項規定，案件由犯罪地、被告之住所、居所或所在地之法院管轄。犯罪地即犯罪事實發生地、行為地或結果地均屬之；另住所及居所之概念，則須依民法之規定，所謂「住所」即係依一定事實，足認有久住之意思，住於一定之地域者，即設定住所於該地。而「居所」僅係行為人短期繼續居住之地，與行為人之關係則不如住所密切。「所在地」則指被告遭起訴時所在之地，至該所在之原因係任意或強制在所不問；此外，

決定犯罪地、住所、居所或所在地之基準時點，依我國實務見解，以提起公訴時為準。

(二)國外犯罪：若於我國領域外之犯罪，依刑法第4條規定，如犯罪行為或結果，有一在中華民國領域內者，為在中華民國領域內犯罪。但若犯罪行為人現並非於我國領域內，對於其刑事追訴上將產生相當之不便，且我國與行為人所在國間是否有得以引渡之適用，又是另一個問題；故應給予行為人所在國「刑事追訴優先權」，只有在該國與我國刑罰法規不相同時，始依我國法律規定進行刑事追訴，似較符合刑事追訴之經濟效益。³⁶另於我國籍船艦或航空機內之犯罪，由於國旗原則擴張屬地原則之結果，亦屬我國刑法效力（刑法第3條但書）及刑事訴訟法效力所及，我國對之固有刑事審判權，但鑑於船艦航空機移動性，如何定其土地管轄？即有疑義，故依刑事訴訟法第5條第2項之規定，如於該船艦航空機內犯罪者，以該船艦本籍地、航空機出發地或犯罪後停泊地之法院取得管轄權。

二、網路犯罪管轄權之爭議：因網路具有跨區域之特性，故就網路犯罪應由何法院管轄，即成為司法實務之焦點，是以被告或犯罪嫌疑人在法院所在地無住居所，且所在地亦非該法院轄區者，就該犯罪管轄權為何，即產生爭議。如散布援交內容，行

³⁵：參閱林鈺雄，刑事訴訟法上冊，自版，2003年9月，頁100。

³⁶：參閱沈榮華，網路犯罪相關問題之研究，國防大學國防管理學院法律學研究所碩士論文，2003年7月，頁118。



爲人將訊息上傳地點可能是在高雄，而該援交訊息之記憶媒體伺服器可能是在台北市，但於全省各地均可以看到該援交內容，該案如係由桃園縣警察局查獲，移送桃園地檢署偵辦，並由桃園地方法院檢察署向桃園地方法院提起公訴，則桃園地方法院是否有管轄權？是否在全省各地，透過網路設備可看到該內容之地之法院均有管轄權？即屬爭議。因此，如被告在該法院有住居所或現所在地者，依刑事訴訟法第5條規定，該法院即有管轄權，故無管轄權之爭議，惟常發生爭議的是，被告在該法院並無居所，現所在地亦非該法院之轄區，則應判斷該網路犯罪之犯罪地是否在該院之轄區，然因該網路犯罪具有跨區域之特性，故就網路犯罪行爲地之判斷，亦常引發爭議。³⁷

三、網路犯罪管轄權之判斷：依刑事訴訟法第5條土地管轄之規定，就網路犯罪管轄權上，被告在該法院管轄區內有居所或現所在地者，由該法院取得該案管轄權，固無疑義，惟如該被告在該法院之轄區內並無住居所或現所在地時，則就該被告是否取得管轄權，即應視就該被告行爲之犯罪地於何處而定，而犯罪地之決定與網路犯罪行爲之性質有關，故依刑事訴訟法第5條所規定之

犯罪地，即包括行爲地與結果發生地。是本文茲就主要網路犯罪之犯罪地說明如下：³⁸

(一)行爲地

1.被告犯罪行爲如屬舉動犯者，則其犯罪行爲不待結果之發生，即成立犯罪，是以，如網路犯罪行爲係屬舉動犯者，如陳列、刊登等行爲，則其犯罪地係爲連上網路後上傳行爲之行爲地及該傳送內容所附著伺服器所在地爲犯罪地，即該網路上傳至伺服器之行爲一實施，該犯罪即完成，故縱於行爲完成後，於其他地區透過網路得以觀看上傳內容時，並不能認該其他地區係犯罪地。

2.惟於部分網路犯罪行爲，其行爲特性即具有主動傳送之功能，包括散布、運輸、線上買賣等行爲，此類行爲之行爲地不僅包括其網路上傳所在地，收受該傳送內容之地點，亦均可認爲是犯罪地之一部分。如定期主動傳送猥褻圖畫給會員，該行爲不是被動之陳列，而係主動傳送，故其收受地亦可認爲是犯罪地。

3.如係使用電子郵件傳送給個人或多數人實施犯罪者，以輸入指令之所在地爲犯罪地。如以電子郵件恐嚇他人交付財物，則該電子郵件上傳之地即爲行爲地。

(二)結果地

1.網路犯罪之結果地，即須以該網路犯罪之行爲係屬結果犯，有結果發生爲必要者，始有結果發生地，就該類型之網路犯罪，其結果發生地，即爲該犯罪之結果地。

2.結果發生地可能係複數，則該複數

³⁷：參照王銘勇，電腦網路犯罪之刑事管轄權，2004年第6屆網際網路空間：資訊、法律與社會研討會論文集，中央警察大學，2004年10月，頁26。

³⁸：同註³⁷，頁31。



之地區皆為犯罪地。

網路犯罪犯罪地之判斷，於國際即影響該國之審判權，於國內則影響各地法院是否具有管轄權，故基於網路犯罪之跨區域性，境外網路犯罪對該國有影響時，司法實務大多認定該國具有審判權及管轄權存在，惟於國內關於網路犯罪管轄權之爭議，因檢察實務就該類犯罪均認定可從網路上觀看該內容者即具有管轄權之見解，而導致諸多爭議，故就網路犯罪之管轄權為避免爭議發生，對該犯罪行為之本質，須有明確之認知，另就管轄權有爭議時，宜由被告之居所或明確犯罪地之法院取得管轄權為宜，以貫徹刑事訴訟法第5條之立法意旨。此外，如同一案件繫屬於有管轄權之數法院者，則由繫屬在先之法院審判之。但經共同之直接上級法院裁定，亦得由繫屬在後之法院審判。

陸、網路犯罪之未來整體預防對策

所謂「預防重於治療」，面對現今網路犯罪案件頻傳，犯罪類型不斷更新且多元化，的確有必要思考如何改善網路社會中犯罪預防之問題，以下本文則針對網路之性質提出歸納預防網路犯罪之建議供大家參考：

一、明確之網路行為規範：由於網路資訊快速發展，利用網路所進行之犯罪亦有

越來越多之趨勢，是對於網路失序行為制定法律來加以規範，藉以維持網路秩序，即有其必要性及重要性，並使網路使用者均能遵守網路共同規範，知其於網路上何種行為可為，何種行為被禁止，如網路行為規範越明確，網路使用者對於網路評價則越有共識，當違犯共同價值標準時，則應接受懲罰。³⁹

二、抑制網路犯罪動機：近來警方所破獲網路犯罪案件中，犯罪行為人多以年輕在學學生為主，研究歸納分析其犯罪動機，均無非以自我挑戰為第一，獲取經濟利益為第二，⁴⁰然事實上網路犯罪行為動機主要乃係在滿足需求，欲以最少成本獲取最大報酬，其認為利用網路犯罪風險低、報酬高、能滿足心理需要且容易實現，故為抑制網路犯罪動機則須從整體預防觀點著手，降低網路使用者違法之動機與情境之預防兩者需同時兼顧，始能進一步有效抑制網路犯罪之發生。

三、快速有效之嚇阻：鑑於網路犯罪有越來越猖獗之趨勢，因於網路上犯罪比一般傳統犯罪來得容易，且所獲得之利益亦相對快速，因此，未來網路將成為犯罪者之天堂，為有效之遏止該風，則必須使其覺得網路上犯罪行為越來越不容易獲得預期之利益，一旦在網路上有犯罪行為，便可能遭受到懲罰，假使能提高刑事司法體系之執法

³⁹：參閱黃讚松、林宜隆，網路使用現況與犯罪問題之探討，2000年第2屆網際網路空間：資訊、法律與社會研討會論文集，中央警察大學，2000年12月，頁72。

⁴⁰：參閱黃讚松，從情境犯罪預防理論探討網路犯罪預防對策之研究，中央警察大學犯罪防治研究所碩士論文，2000年6月。



效率，加重網路犯罪之刑罰，並運用現代科技，警察偵破網路犯罪率之提高，藉由整體偵查功能之提升，使得網路犯罪者被逮捕或懲罰之可能性均非常高，如此則應可快速有效嚇阻網路犯罪。

四、強化網路倫理教育：由於目前我國網際網路使用人口日益增加，故未來網際網路更應朝向加強網路倫理教育進行，利用網路提供資訊以提昇網路使用者之素養。如以網路發展比喻為一個人之成長觀之，目前我國網路使用者之素養，則如同青少年階段，不知自制且任意而為，因此網際網路使用者網路倫理教育之不足，乃係我國提倡網路資訊教育所應努力之方向。是以，網路倫理教育在現今提倡網路社會中則顯得特別重要，為拓展使用人口、培養素質、建立專業、高品質、有深度之網路，期以實用之資訊擴展使用者之年齡層，使網路使用者清楚了解網路未來之發展與潛力，自動自發的學習網路，發展成熟之討論和深度資訊之提供，乃係未來網路社會成長與穩定之主要因素。⁴¹

五、培育21世紀網路犯罪與資訊法律專業刑事偵防人才：因網際網路之誕生為人類帶來便利，惟同時網際網路強大功能亦為有心人所惡用，且常造成難以想像之危害，又基於網際網路具有前述偵查不易之特性，故為能有效遏制網路犯罪問題持續擴散，培育

具有網路犯罪與資訊法律專業刑事偵防人才則有其重要性及必要性。

柒、結論

網際網路發展正將逐步影響現代人生活型態，如何建構網路新世界之法律秩序，已成為刻不容緩之問題，而其中最令人擔憂的莫過於網路之普及，致使犯罪隱形化，嚴重挑戰現實社會之法律秩序。網路犯罪乃係網路社會失序之普遍現象，如未能了解網路犯罪之深層原因，與網路之限制與特性，即無法談及網路之核心問題——網路犯罪之預防。本文研究提出之網路犯罪預防對策，乃係針對網路犯罪之特性及類型加以分析後，所研擬出之預防方法，目的即在喚醒社會對網路犯罪之認識。在網路中只要有犯罪之機會及適合之情境，於網路中則有一些人會犯罪，因此，網路犯罪預防整體概念的建構，在網路犯罪之預防策略上，有著舉足輕重之重要性，同時亦須針對犯罪可能之因素加以防範，始能達到預防網路犯罪之實質成效。

作者簡介

劉俊男

中央警察大學法律學研究碩士、考試院93年度軍法官考試及格；現為憲兵學校法律教學組少校教官。

⁴¹：參閱林宜隆，網路犯罪防範對策之新思維，2000年第2屆網際網路空間：資訊、法律與社會研討會論文集，中央警察大學，2000年12月，頁139。