

一、電腦網路犯罪之定義

資通訊科技蓬勃發展，網際網路隨之興起，基於開放、自由、易於使用等特性，網路已成為個人、組織、政府間訊息之交換、傳遞的重要管道。隨著各行各業加深資訊化應用的同時，電腦及網路資訊設備應用的安全風險也隨之提高。國際上，早於2001年11月由歐洲理事會的26個歐盟成員國以及美國、加拿大、日本和南非等30個國家的政府官員在布達佩斯所共同簽署的國際公約，自此『網路犯罪公約』成為全世界第一部針對網路犯罪行為所制訂的國際公約。而該公約制定的目的之一是期望使國際間對於網路犯罪的立法有一致共同的參考準據，也希望國際間在進行網路犯罪偵查時有一個國際公約予以支持，而得以有效進行國際合作。

電腦網路犯罪，係指利用電腦及其所連接之網路，藉由軟體工具的協助，遂行不法行為。電腦和網路可能在犯罪過程中發揮各種不同的作用。譬如說；電腦軟體和網際網路的結合，其功能被人操縱，來進行各種各樣的刑事犯罪或欺騙性的活動。另一種形式的電腦犯罪將目標瞄準電腦作業系統、程序、電子郵件或電腦聯網系統的存儲資訊等都稱之為電腦網路犯罪。由於在網路使用上具常以匿名方式進行，致近年來，隨著寬頻網路基礎建設的完備，透過電腦在網際網路上之犯罪行為，已成為電腦網路犯罪的主要代名詞。

然而，對於電腦網路犯罪給它下一個明確定義，並不容易。其中，一般人就常將『電腦網路犯罪』等同於『計算機犯罪』、『電腦犯罪』、『網路(電腦)犯罪』、『網路犯罪』，在此，本文亦不去探究各個名詞間之區隔。而謂『電腦網路犯罪』，為電腦系統與通訊網路相結合之犯罪，專指具有網際網路特性的犯罪。易言之，行為人所違犯之故意或過失的犯罪行為，必須行為具有網際網路之特性。但就實際應用而言，犯罪行為人在犯罪過程中，須借助網際網路，方能遂行其犯罪意圖之犯罪，即屬電腦網路犯罪。本文除了探討國內外電腦網路犯罪類型、通傳相關法規及其防治方法外，對於濫發商業電子郵件冗長之立法進度深感緩不濟急，為求效率，作者亦粗淺的提出行政上之作爲，期盼網路犯罪能早日銷聲匿跡。

二、電腦網路犯罪之特質

電腦網路犯罪乃係因資訊發展後始新興的犯罪型態，其特質與傳統犯罪類型有所差異，一般而言，網路犯罪應具有以下之特質（李柏宏,1996）：

- 1.白領犯罪：通常電腦犯罪者多半為程式設計師、系統分析師或職務上常操作電腦者。
- 2.專業性與業務性：實施電腦犯罪須運用電腦專業知識，此外根據國外統計，大多數電腦犯罪都為內部員工所為，故與業務有關。
- 3.損害性高：近來人們對電腦依賴程度高，如數量龐大、複雜的金額款項全交由電腦管理，一旦遭到侵害，後果不堪設想。
- 4.高犯罪黑數：犯罪黑數(Dark figure of crime)是指已發生但沒有被政府機構登錄的犯罪行爲。據美國聯邦調查局估計，只有百分之一的電腦犯罪爲人所知，而在發現的電腦犯罪案件中，只有百分之四到達偵查機關之手（房阿生,1989）。
- 5.持續性：行爲人會重複再犯，或犯行本身爲繼續的狀態，整個案件會延續到被發覺爲止。
- 6.行爲與結果時間和地點分離：此類犯罪後結果不馬上突顯，且犯罪地點與結果地亦分屬不同管轄，甚至跨國界。
- 7.偵查與起訴有技術上之困難：除了前述高犯罪黑數外，證據取得亦非常不易，或檢察官等對電腦認識不夠等，均是造成起訴困難之主因。
- 8.處罰太輕：國內目前立法機關尚未制定出專法來針對電腦犯罪加以處罰，僅能依一般刑案中目的相似的詐欺罪、毀損罪、誹謗罪、竊盜罪等懲處，刑度與行爲成功能所獲得利益不成比例。

此外，作者根據個人在通訊單位工作多年之認知，特歸納出電腦網路犯罪之特性如下，亦請參考；

- 1.散佈迅速：由於網際網路具有無遠弗屆，擴散迅速之特性，故影響層面極爲廣泛。
- 2.蒐證困難：網際網路犯罪可得之證據有限，且因網際網路具有匿名的特性，其證據不僅容易被造假，也容易受到銷毀，再加上相關技術不斷進步，因而使得網際網路犯罪之證據蒐集愈發困難。
- 3.具全球性：網際網路世界並無國界，若要管制網際網路犯罪，往往需要多國之合作，然而因各國法規不同，有時一個行爲在A國係犯罪行爲，在B國則爲未必違法，使得網際網路犯罪之跨境管轄不易發生效用。
- 4.偵查不易：由於前述幾個網際網路之特性，使得檢警單位在偵查網際網路犯罪十分困難，甚至無法偵查，因此，其他相關單位之協助及配合非常重要。
- 5.人性弱點：人性的弱點，一般常爲歹徒所用者爲『貪婪』與『恐懼』兩項，而此兩項弱點存在一般人們的內心深處，不易排除，因此，使得歹徒有隙可乘。

三、電腦網路犯罪之類型

由於我國網路的廣泛使用，網路人口幾達國內人口的二分之一，網友素質參差不齊，

網路近年成爲另一個新型的犯罪工具與犯罪場所及犯罪的目標，致近年網路色情與網路犯罪成爲各級民意代表質詢政府相關單位的重點議題，並常見一些民間團體召開記者會抨擊政府相關單位，坐視網路色情氾濫戕害青少年身心。有關電腦網路犯罪之類型，本文不是要網羅各個類型之案例做詳盡的介紹，而是想先就國際上一般電腦網路犯罪型態作分類，然後再進一步說明國內之犯罪型態。

(一)、國際情況

國際上，因爲有『網路犯罪公約』的簽署，其中還包括；公約之生效、加入、區域應用、公約的效力、聲明、聯邦條款、保留、保留的法律地位和撤回、修訂、爭端處理、締約方大會、公約的退出和通告等事項。故在該公約中，第二章自第二條至第十條中制定了簽署國需要對九類網路犯罪行爲以刑法處罰，茲分述於下：

- 1.非法存取（**Illegal access**）：指任何故意威脅或攻擊電腦系統及電腦資料的行爲，如電腦駭客等行爲，這些行爲不僅帶給電腦系統及合法使用者極大困擾，更是影響電腦系統的正常運作，且若電腦系統因此故障，更需耗費人力、物力等資源去修復，故此類行爲應予懲罰。(原文請參照《網路犯罪公約》第二條)。
- 2.非法截取（**Illegal interception**）：此類行爲包括非法截取電腦傳送的『非公開性質』電腦資料，此項規定是用以保障電腦資料的機密性。根據歐洲理事會說明，如果電腦資料在傳送時，沒有意圖將資訊公開時，即使電腦資料是利用公眾網路進行傳送，也屬於『非公開性質』的資料。(原文請參照《網路犯罪公約》第三條)。
- 3.資料干擾（**Data interference**）：包含任何故意毀損、刪除、破壞、修改或隱藏電腦資料的行爲，此項規定乃是爲了確保電腦資料的真確性和電腦程式的可用性。(原文請參照《網路犯罪公約》第四條)。
- 4.系統干擾（**System interference**）：此項規定與第四條的『資料干擾』不同，此項規定乃是針對妨礙電腦系統合法使用的行爲。根據歐洲理事會的說明，任何電腦資料的傳送，只要其傳送方法足以對他人電腦系統構成『重大不良影響』時，將會被視爲『嚴重妨礙』電腦系統合法使用。所以在此原則下，利用電腦系統傳送電腦病毒、蠕蟲、特洛伊木馬程式或濫發垃圾電子郵件，都符合『嚴重妨礙』電腦系統，即構成『系統干擾』的行爲。(原文請參照《網路犯罪公約》第五條)。
- 5.設備濫用（**Misuse of devices**）：包含生產、銷售、發行或以任何方式提供任何從事上述各項網路犯罪的設備。由於進行上述網路犯罪，最簡便的方式便是使用駭客工具，因此間接催生了這些工具的製作與買賣，因此有需要嚴格懲罰這些工具的製作與買賣，從基本上杜絕網路犯罪行爲。(原文請參照《網路犯罪公約》第六條)。

- 6.偽造電腦資料（**Computer-related forgery**）：包括任何虛偽資料的輸入、更改、刪改、隱藏電腦資料，導致相關資料喪失真確性。目前歐洲理事會各成員國法律，偽造文件都是犯罪行爲，需要接受刑事制裁，故此規定只是將無實體存在的電腦資料也納入『偽造文書』的文書範圍。（原文請參照《網路犯罪公約》第七條）。
 - 7.電腦詐騙（**Computer-related fraud**）：包括任何有詐騙意圖的資料輸入、更改、刪除或隱藏任何電腦資料，或干擾電腦系統的正常運作，爲個人謀取不法利益而導致他人財產損失，這是需要予以刑事處罰的犯罪行爲。（原文請參照《網路犯罪公約》第八條）。
 - 8.兒童色情的犯罪（**Offences related to child pornography**）：包括一切在電腦系統生產、提供、發行或傳送、取得及持有兒童的色情資料，此項規定是泛指任何利用電腦系統進行的上述兒童色情犯罪行爲。（原文請參照《網路犯罪公約》第九條）。
 - 9.侵犯著作權及相關權利的行爲（**Offences related to infringements of copyright and related rights**）：此項規定包括數條保障智慧財產權的國際公約列爲侵犯著作權的行爲，【網路犯罪公約】也規定這些行爲必須爲故意、大規模進行，並使用電腦系統所達成的。（原文請參照《網路犯罪公約》第十條）。
- 『網路犯罪公約』爲世界上第一個打擊網路犯罪的國際公約，必將對世界多數國家的相應立法產生重要影響，遵循網路犯罪公約，能建立更廣泛的共同打擊網路犯罪的國際司法合作，對打擊跨國網路犯罪具有重要作用。

(二)、國內情況

近五年來，詐欺案件占全部刑事案件之比率有增無減，其中利用網路犯罪更是歷歷可數，根據資策會FIND / 經濟部技術處『創新資訊應用研究計畫』統計，2007年第1季台灣經常上網人口爲990萬人，網際網路連網應用普及率爲43%，藉由網路使用逐漸普及，藉由網路產生的犯罪行爲亦不斷成長。而國內一般犯案約可分成以下兩大類：

1.以網際網路作爲犯罪之客體或場所：

此類型以網際網路爲犯罪場所，亦以網際網路爲犯罪工具，甚至以其作爲攻擊之客體。刑法第三十六章妨害電腦使用罪所規範之妨害電腦使用行爲，即爲最典型之類型。另外，若在BBS或是部落格上散佈不實謠言，因而涉嫌誹謗或對他人之公然侮辱；或是藉由網際網路散布、販賣猥褻資訊等，在刑法第310條誹謗罪、第235條散布販賣猥褻物品及製造持有罪亦有明確規範。

2.以網際網路爲犯罪工具：

此犯罪類型，不一定是以網際網路及連結在其上之電腦系統爲攻擊目標，也不一定是以網際網路爲犯罪場所，僅以網際網路爲犯罪之工具。例如藉由偽造第三人網頁在網際網路竊取或誘騙他人帳號密碼（網路釣魚），以達到竊取他人財物或詐欺取

財之目的等行爲，即屬此類犯罪行爲，有可能同時觸犯刑法第210條偽造文書罪、第339條之3不正使用電腦詐欺罪及第358條入侵電腦或其相關設備罪等。

至於國內網際網路爲犯罪現況，根據警政署刑事警察局的統計資料顯示，近年來的網路犯罪手法一再翻新，主要的案例型態如下所示：

- 1.網路詐欺案：爲以網路爲工具騙取財物之案件。96年1 - 6月電腦網路犯罪發生數以網路詐欺案4,603件爲最多，較上年同期增加1,267件(+37.98%)，破獲率增加27.58個百分點。
- 2.妨害電腦使用：妨害電腦使用罪主要針對無故入侵電腦、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行爲予以處罰。96年1 - 6月妨害電腦使用3,675件，較上年同期減少820件(-18.24%)，破獲率增加2.94個百分點。妨害電腦使用案多數爲網路遊戲，偵辦時發現上網來源端爲中國大陸、香港等地，追查不易。
- 3.違反兒童及少年性交易防制條例：主要爲在網路上所散布、販賣之猥褻圖畫、影片、光碟，其係以未滿十八歲之人爲內容者或使未滿十八歲之人爲性交易者，96年1-6月經由網路違反兒童及少年性交易防制條例共2,374件，較上年同期增加1,117件(+88.86%)。
- 4.侵害智慧財產權：包含違反著作權法、商標法及專利法，例如在網路上販售大補帖、違法張貼、下載散布他人著作及販賣仿冒品等。96年1-6月經由網路侵害智慧財產權共1,515件，較上年同期增加742件(+95.99%)。

美國加州大學聖塔巴巴拉分校心理學教授布拉斯柯維奇(Dr. James Blascovich)，曾在一項網路犯罪的研究報告中指，『貪婪』與『恐懼』是騙徒最常利用的兩個人性弱點。國內詐騙集團彷彿修過這門『詐騙心理學』課程，從早期的金光黨、刮刮樂、六合彩明牌，到冒充國稅局、健保局的假退稅、假退費，基本上都是利用被害人貪婪或貪小便宜的心態，遂行詐財之目的。等到類似手法逐漸被識破，再改從民眾的恐懼心理下手。

近五年來，根據警政署統計，詐欺犯罪現況如下表所示，請參考。至於民國96年1-6月電腦網路犯罪發生數13,608件，較上年同期增加2,835件(+26.32%)，破獲數8,749件，較上年同期增加4,251件(+94.51%)，破獲率64.29%，較上年同期增加22.54個百分點，呈現發生數增加、破獲率增加的情形，主要係警察機關加強偵查網路犯罪所致。

詐欺犯罪現況

90-95年台閩地區全般刑案與詐欺案件統計						
年度 項目	90	91	92	93	94	95
全般刑案件數	490,736	503,389	494,755	522,305	555,109	512,788
詐欺件數	16,082	26,397	37,191	40,001	43,181	41,352
所佔百分比	3.28%	5.24%	7.52%	7.66%	7.78%	8.06%
破獲詐欺件數	2,665	4,809	7,526	14,488	21,232	25,896

註：自94年起將詐欺與背信分開統計。

更可怕的是，台灣民眾長期生活在詐騙集團的恐懼中，人與人之間互信的核心價值受到嚴重挑戰。有人只要看到手機響起陌生門號或未顯示來電，即陷入恐懼焦慮；有老人家因為曾經被騙，嚇得從此不敢接電話；更有民眾變得多疑、猜忌，把陌生人、陌生電話全當成騙子。根據警政署的統計，96年1-5月警察機關受(處)理電話詐欺(含手機簡訊)案件發生數5,440件，較去年同期增加6件(+0.11%)；破獲率76.19%，較去年同期增加21.57個百分點，每十萬人口發生件數減少0.08件。本期警察機關受(處)理電話詐欺(含手機簡訊)案件每十萬人口破獲件數較去年同期增加較多之縣市，以雲林縣增加30.17件最多，花蓮縣增加24.68件次之，苗栗縣增加15.18件再次之。現將利用電信通訊詐欺案件數和其損失和金額，表列如下：

利用電信通訊詐欺現況

165反詐騙諮詢專線民眾報案平均損失金額統計表			
期間	被害件數	被害金額	平均個案損失金額
95年 0101-1031	2,303	557,168,545	241,932
96年 0101-1031	3,855	875,322,444	227,062
增減數	+1,552	+318,153,899	-14,870
增減率%	+67.39%	+56.97%	-6.14%

【作者：高凱聲博士，曾任本中心第一、二兩屆董事並同時任本中心國際事務委員會主任委員。在高博士主導下我國在1998年以『台灣』名稱加入ICANN及GAC組織。】