電腦犯罪特性分析之研究

Analysis of Computer Crime Characteristics

廖有祿
中央警察大學資訊管理學系
桃園縣龜山鄉大崗村樹人路 56 號
Email: ylliaw@sun4.cpu.edu.tw

You-lu, Liao
Department of Information Management, Central Police University
Gueishan 333, Taoyuan, TAIWAN
Email: ylliaw@sun4.cpu.edu.tw

摘要

根據犯罪特性分析，電腦犯罪以散布色情及侵害著作最多，犯罪地點以住宅為主，破案件數有逐漸增多趨勢，犯罪期間會持續到被發現為止，動機則以圖利為主。犯罪者屬性以男性為主，大多單獨進行，年齡偏低，職業以學生和無業者最多，教育程度大多在專科以上，犯罪紀錄多屬初犯，居住地以都市為主，且有不少殘障人士涉案。刑事司法體系處理情形目前仍集中在少數單位，處理結果明顯有漏斗效應，且判處刑罰均不重，緩刑或易科罰金比率甚高，但科處罰金額度卻相當高。

關鍵詞：電腦犯罪、網路犯罪、特性分析、刑事司法體系

Abstract

According to the analysis of crime characteristics, the majority of computer crime is distribution of pornography and copyright infringement. The crime scene is mainly residence. The broken cases are increasing, and the criminals will continue until being discovered. The motivation is mainly for profit. The offenders are mainly male, and always proceed solely. The average age is quite low; profession is mainly student and unemployment. The average level of education is higher than college, and the criminal record is first offense. Residence is mainly urban, and there are many handicaps involved. The cases are currently proceeded in few criminal justice agencies. The funnel effect emerges obviously, and the punishment is quite lenient, but the ratio of probation and fines is high.

Keywords: computer crime, Internet crime, characteristic analysis, criminal justice system

一、問題背景

電腦犯罪是一種新的犯罪型態，它是少數人利用電腦從事各種犯罪行為，而成為犯罪學上一個新的研究課題。由於現今社會對電腦科技的依存度提高，重要資料皆儲存其中，一旦被少數有心人利用，其所造成的損害為一般犯罪所不及，故有探討的重要性與迫切性[4]。由國內外案例可見，電腦固然帶給人類許多便捷，但也衍生一些難以避免的問題，尤其是日益嚴重的電腦犯罪，已對國家社會構成重大威脅，有人戲稱電腦已成為槍枝發明以來，威力最強大的犯罪工具[5]。而隨著電腦運用日益普遍，也連帶影響到犯罪的手法，有學者甚至大膽的預測，未來除了性侵害案件外，幾乎所有犯罪均可能利用電腦科技來完成[18]。而網際網路上更是盜版、色情猖獗，因此就有人指出網路是警察亟需開闢的巡邏區域[8,24]，甚至有學者指出應設立網路警察[21]，以解決這類問題。

二、文獻探討

目前國內僅有幾篇關於電腦犯罪的實證研究，其中「電腦犯罪模式之分析」[11]係國內首次對類似犯罪進行本土化探究，其方法乃就警方所偵辦的11件電腦犯罪進行案例分析，整理出各個犯罪手法及流程圖，進而歸納出網路犯罪與非網路犯罪模式圖。並訪談部份偵辦人員，了解其偵查案件類型、發動偵查原因、偵查時間、事前準備物品、參與人員數目、任務分工、有無專業人員協助、到達現場程序、證物扣押及處理、遭遇困難等，建構出電腦犯罪偵查的流程。並曾訪問一個被害單位，了解其事件始末、發現過程、調查經過及事後檢討。此外並分析犯罪者的年齡、職業、身份、前科、犯罪所得、起訖時間、進行地點、起訴罪名等，對掌握國內電腦犯罪現況頗具參考價值，唯未蒐集到案件細節資料，且未訪談到犯罪者，無法深入掌握到此一犯罪的真實現象及確切原因。

而「網路使用者行為分析」曾設計一份問卷，以立意抽樣（purposive sampling）方式，針對學術網路用戶（中美二地大學生）及商業網路用戶，共發出500份問卷調查，以了解其使用電腦及網路情形，及對電腦安全的認知，並針對部份受測對象進行深度訪談，獲得不少描述性資料，但據作者陳述，以此種問卷方式進行調查，很難避免量化研究的先天缺點，如問卷題目常會由受試者依照自己理解來闡釋題意，而且很多東西是不能量化的，量化的結果也可能沒有意義[16]。

另外「網路社會與犯罪問題之研究」曾針對國內網路犯罪案例，從案例內容相關資料（包括犯罪類型、地點、時間、犯罪者年齡、身份、犯罪手法、動機、損害法益及起訴、判決罪名）進行分析，發現網路犯罪仍以色情為主要型態，犯罪動機主要係好奇和獲利，並指出刑事司法體系在處理網路犯罪時，仍依照過去傳統社會的概念，來處理網路上的所有問題，無法趕上網路犯罪的腳步[10]。

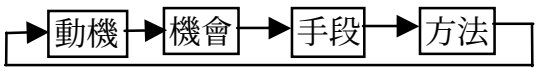
而「網路犯罪之問題建構研究」係針對網友及一般民眾進行調查研究，發現網友對網路空間上的行為（如盜版軟體、散播不實言論、窺視他人隱私、散布電腦病毒等）寬容度較高，因此執法單位如依法在網路上進行掃蕩，常會引起網友的強力反彈[6]。

此外，「網路犯罪模式分析及偵防對策之研究」則蒐集20件網路色情及侵害著作權案例、5件侵害個人資料案例、6件網路詐欺案例、4件網路誹謗及妨害名譽案例，擷取犯罪動機、實行方法及成為偵查對象之行為作關聯性因子，透過資料探勘（data mining）演算法進行分析，而找出關聯性規則表，研究方法頗有創新，唯其資料來源為次級資料（媒體報導），既不深入且不可靠，而在分析時又剔除案例較少之後三類（個資法、詐欺、誹謗），僅就網路色情及侵害著作權部份加以分析，導出之結論無法類推至網路犯罪全貌，雖有良好之分析工具，但無可靠的研究素材，所研擬之偵防對策恐有所偏失[7]。

而「網際網路與犯罪問題之研究」則就85-88年所發生的網路犯罪，以立意抽樣方式，共蒐集15件案例，依據其犯罪時間、地點、事實、方式、損害、犯罪者剖析及起訴判決罪名，以框架（frame）結構加以分析，建構出偵查基本步驟及流程，頗值參考[9]。但其僅針對網路犯罪部份加以分析，而將傳統之電腦犯罪排除在外，恐難窺其全貌。此外作者針對國內網路犯罪偵查組織編制、偵查開端、重點、工具、效果及瓶頸加以分析，亦頗有見地。唯其在結論所建議成立之「網路警察局」則有待商榷，理由在於網路犯罪未來將大幅增加，且此類型犯罪具虛擬性質，並無地域特性，如由專責單位偵辦，恐力有未逮。為因應資訊化社會來臨，應使每位員警都具備偵查網路犯罪之能力，再輔以熱心民眾的守望相助，踴躍提供犯罪情報[17,23]，由網路的全體使用者擔任「網路警察」，可增加對不當資訊監督的效果，又可避免因不當檢查，限制其他合法資訊的流通[3]。應當可以處理一般性的網路犯罪，至於較複雜的犯罪手法，則可以技術層次較高之電腦犯罪偵查隊負責，如此則較具彈性，不致有人力浪費之虞。

此外尚有「以科爾曼理論探討美國電腦犯罪」，唯此論文並非本土化研究，因為所收集的案例全是發生在美國，因此其分析結果未必適用於本國。此一研究採用Coleman白領犯罪理論[19]中機會與動機互動模式為架構，提出一種內在動機、外在環境互動的模式來解釋電腦犯罪，強調犯罪行為乃適切的動機（motivation）與機會（opportunity）的結合。而在此一架構下，影響動機的次文化則是電腦犯罪者所參考的次文化（包括組織、行業和職業次文化）[14]，中介變項則是電腦的機會分佈，其理論架構如下[5]：

此一架構類似以下Bologna所提的動機（motivation）、機會（opportunity）、手段（means）、方法（method）模式[20]，對照這兩個模式的共通點，可見「動機」與「機會」在電腦犯罪中的重要性：



綜論此一研究除方法上立意取樣的缺點及使用次級資料分析（secondary data analysis）外，理論架構上沒有克服的問題，則是將動機的形成歸因於電腦犯罪者所參考的次文化，換句話說，是經由學習而來。至於這次文化是什麼？其運作機制為何？均未提供明確訊息。而事實上，電腦犯罪者大多是以獨行俠姿態出現，只有少數是受他人影響而犯案。其次，此一研究架構的前提，是將電腦犯罪視為「理性選擇」的結果，是電腦犯罪者計算犯罪的風險，分析犯罪所得的報酬利益，一番盤算後作出的選擇。換言之，電腦犯罪者於犯案前已經考慮其失敗的後果，此項前提限制了此一理論的解釋力，很難涵蓋現實中大多數的電腦犯罪案例，因為許多個案即使經過仔細盤算，終究會因自我控制力低而不計後果選擇犯案一途。

而「犯罪語言學與資料檢索應用觀念之研究－以網際網路情色文學為例」，係以犯罪語言學的觀點進行情色文學的語言調查，以建立情色語料庫作為網際網路情色文章的過濾機制，使得情色文學過濾系統能達到自動化的程度[12]。至於「網際網路上可疑不法資訊之自動化蒐集系統」，係利用內容分析及實驗研究的方法，建立犯罪情報蒐集系統，以自動分析網際網路上的可疑不法資訊，作為主動偵查、預防網路犯罪的工具[13]。而「網路SYN泛濫攻擊防制機制之研究－以訊務流量控制為基礎」，是針對資訊安全中之阻斷服務（denial of service）的泛濫攻擊，研究以訊務流量控制為基礎的防制機制[15]。以上三項研究均是以安全技術為出發點，探討電腦及網路犯罪預防和偵查的方法。

此外「網路犯罪自動化搜尋系統之研究」，分別從偵查人員所需專業素質及訓練、犯罪模式分析、偵查要領及輔助設備規劃、相關法規之探討、網路環境用語之分析與統計、自動化網路搜尋系統等方向，探討偵查電腦及網路犯罪所須建立的蒐證技術，則是整合國內各領域學者專家，建置一套網路犯罪資訊搜尋系統[1]，可作為未來類似研究的起步。

而「警察電腦犯罪與防制措施之探討」，則是分析中央警察大學招生電腦閱卷弊案的犯罪手法，其模式是利用職務、主管職權和授課學生之便，將電腦閱卷作業之設計、人事管理與執行控管集於一身，在低能見度管理與「有利可圖，有機可乘」情況下犯罪[2]，是針對單一案例的處理過程加以分析，頗值參考。

由以上幾篇國內有關電腦犯罪的研究可見，目前的研究方向仍然以安全技術為主，其次是以事件的發生及處理過程加以探究，但欠缺較可靠的統計數據，本研究之目的，主要是在補足這方面的闕漏。

三、資料來源

本研究所蒐集之資料來源主要取自警察機關（刑事警察局、台北市刑大、電信警察隊）及相關地檢署（台北、士林、板橋），經整理共分為五類：

（一）法院書類：起訴書、判決書、聲請簡易判決處刑書、不起訴處分書、上訴

書、搜索票、告訴狀、委任狀。

（二）調查筆錄：偵訊筆錄、告訴筆錄、報案筆錄、搜索扣押筆錄。

（三）警察機關內部資料：刑案紀錄（前科檔案）、移送書（含光碟、縮影）、偵查報告、受理案件紀錄表、新聞稿。

（四）公文：請求查詢資料函、檢驗函、檢舉函、移請偵辦公文、內部簽辦公文。

（五）其他：新聞剪報、稽核紀錄、通聯紀錄、監看紀錄、股票成交紀錄、服務標章註冊證、網域名稱登記證明等。

首先將上述資料整理成案例分析表，並將相關資料加以彙整比對，再根據編碼簿，將案例資料編碼輸入電腦，最後進行次數分配統計分析，所得結果說明如下：

四、犯罪種類

本研究共蒐集 165 件案例，依據美國白宮的「網路非法行為工作小組」（President’s working group on unlawful conduct on the Internet）將電腦犯罪區分三大類型[22]，再依案情種類分為九類、廿六種：

（一）以電腦為通訊工具：包括非法販賣（販賣違禁藥品、販賣個人資料）、煽惑犯罪（販售武器、網路賭博）、網路詐騙（虛設行號、網路情人、詐騙帳號、網路老鼠會）和妨害名譽（網路誹謗、網路恐嚇）四類。

（二）以電腦為儲存設備：包括侵害著作（盜拷軟體、重製他人著作、侵害商標、盜版光碟）和散布色情（色情網站、媒介色情、色情光碟、張貼色情圖片）二類。

（三）以電腦為犯罪標的：包括妨害祕密（入侵電腦、駭客入侵、竊取股市交易祕密、電腦閱卷弊案）、電腦病毒和電腦竊用（電信飛客、盜刷信用卡、盜用撥接帳號）三類。

五、犯罪特性

（一）案類

本研究案例共分為廿六種不同案情，其次數分配如表一，其中以色情和盜版最多（佔 15.3％），其次為色情網站（14.0％）、網路誹謗（10.4％）、盜版光碟（9.7％）及色情光碟（6.1％）。依種類區分，以散布色情最多（26.8％），侵害著作居次（14.5％），如加上色情及盜版，則共佔 56.6％，足見目前查獲的電腦犯罪仍以色情和盜版為主。再依類型區分，以電腦為儲存設備居多（56.6％），其次是以電腦為通訊工具（23.6％），以電腦為犯罪標的則較少（19.8％）。

表一　案情種類次數分配

類型（百分比）	種類（百分比）	項目	件數	百分比(%)
以電腦為通訊工具（23.6%）	非法販賣（3.0%）	販賣違禁藥品	3	1.8
		販賣個人資料	2	1.2
	煽惑犯罪（3.0%）	販售武器	2	1.2
		網路賭博	3	1.8
	網路詐騙（5.4%）	虛設行號	5	3.0
		詐騙帳號	1	0.6
		網路情人	1	0.6
		網路老鼠會	2	1.2
	妨害名譽（12.2%）	網路誹謗	17	10.4
		網路恐嚇	3	1.8
以電腦為儲存設備（56.6%）	侵害著作（14.5%）	盜拷軟體	2	1.2
		侵害商標	3	1.8
		重製他人著作	3	1.8
		盜版光碟	16	9.7
	散布色情（26.8%）	色情網站	23	14.0
		色情光碟	10	6.1
		媒介色情	4	2.4
		張貼色情圖片	7	4.3
	混合（15.3%）	色情及盜版	25	15.3
以電腦為犯罪標的（19.8%）	妨害祕密（8.4%）	入侵電腦	6	3.6
		駭客入侵	6	3.6
		竊取股市交易祕密	1	0.6
		電腦閱卷弊案	1	0.6
	電腦病毒（1.8%）	電腦病毒	3	1.8
	電腦竊用（9.6%）	電信飛客	3	1.8
		盜用撥接帳號	6	3.6
		盜刷信用卡	7	4.2
總計			165	100

（二）犯罪地點

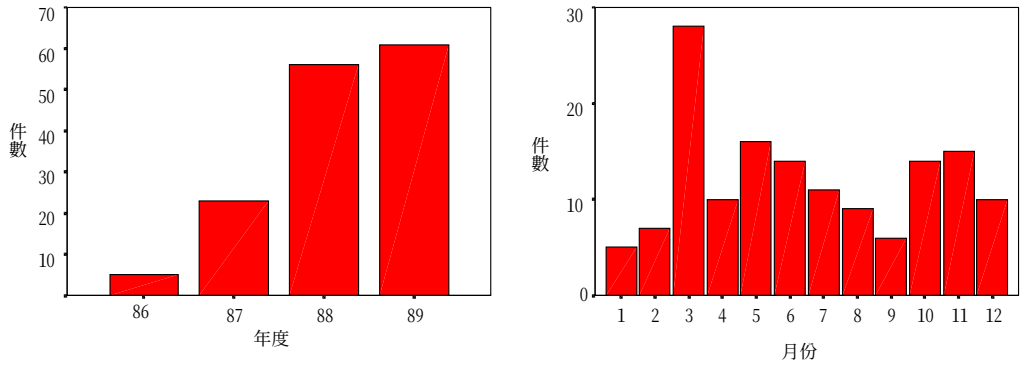
以犯罪地點區分（如表二），可見電腦犯罪以在住宅內進行最多（75.5%），其次為公司（10.9%）及學校（8.2%），其他地點如網路咖啡屋、被害單位、公共場所及辦公室發生次數則較少（合計僅佔 5.6%）。

表二　犯罪地點

地　　點	住宅	公司	學校	網路咖啡屋	被害單位	公共場所	辦公室	其他	總計
件　　數	111	16	12	1	1	2	2	2	147
百分比（%）	75.5	10.9	8.2	0.7	0.7	1.4	1.4	1.4	100

（三）破案時間

本研究所蒐集之案例破案時間分佈如圖一，雖然受到資料蒐集期間（86 年 6 月至 89 年 9 月）限制，由圖中仍可發現電腦犯罪有逐漸增加趨勢，這可能是由於檢舉及取締案件增多所致，也或許是發生件數增加之真實呈現。而其中某些月份件數偏高，可能係因全省同步進行大規模掃蕩色情網站及取締大補帖所致。



圖一　破案時間

（四）犯罪期間

本研究所蒐集的犯罪期間，係根據警方移送書中所填的資料，由表三可見，電腦犯罪的犯罪期間並不長（平均為6.7月），其中四個月之內共計60.9％，但亦有長達四、五年之久，而且有一共通特性，亦即會持續到被發現為止。

表三　犯罪期間

月	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	18	19	21	22	23	26	48	60	總計
件數	37	16	18	21	6	5	4	9	4	6	1	2	2	3	3	2	2	1	1	1	3	1	1	2	151
百分比	24.5	10.6	11.9	13.9	4.0	3.3	2.6	6.0	2.6	4.0	0.7	1.3	1.3	2.0	2.0	1.3	1.3	0.7	0.7	0.7	2.0	0.7	0.7	1.3	100

（五）犯罪動機

電腦犯罪的犯案動機（如表四）以圖利為主（51.5％），其次為好玩（9.7％）、報復（5.5％）、詐財（4.8％）、侵占（4.8％）及破壞（4.2％），其餘尚有盜刷信用卡、盜用撥接帳號、善意提醒、毀謗、恐嚇、盜打電話等動機，可知此類犯罪

係以電腦為工具的財產性犯罪為主。

就犯罪種類細分，販賣禁藥、販賣個人資料、網路賭博、盜拷軟體、盜版光碟、色情網站、色情光碟的動機在於圖利；虛設行號、詐騙帳號、網路情人、網路老鼠會之目的在於詐財；而入侵電腦、駭客之目的主要係報復或破壞；至於網路誹謗的動機則以報復為主。

表四　犯罪動機

動　　機	圖利	好玩	盜打電話	詐財	侵占	破壞	盜刷信用卡	盜用撥接帳號	善意提醒	毀謗
件　　數	85	16	3	8	8	7	5	4	3	3
百分比（%）	51.5	9.7	1.8	4.8	4.8	4.2	3.0	2.4	1.8	1.8
動　　機	恐嚇	報復	偷窺信件	偷竊	陷害	騷擾	同業競爭	煽惑他人犯罪	不明原因	總計
件　　數	3	9	1	2	1	2	2	2	1	165
百分比（%）	1.8	5.5	0.6	1.2	0.6	1.2	1.2	1.2	0.6	100

（六）被害者分析

在被害者方面（如表五），有被害者佔68.5%，無被害者佔31.5%，其中無被害者部份包括販賣禁藥、網路賭博、網路老鼠會（前三類為被害者參與）、色情網站及光碟、媒介色情、張貼色情圖片（後四類屬兩造同意）。而有被害者部份則包括販賣個人資料、虛設行號、詐騙帳號、網路情人、入侵電腦、駭客入侵、盜拷軟體、侵害商標及著作、電腦病毒、電信飛客、盜用撥接帳號、盜版光碟、網路誹謗及恐嚇、竊取股市交易祕密、電腦閱卷弊案、盜刷信用卡等。

表五　有無被害者

案類	有	無	案類	有	無	案類	有	無
販賣違禁藥品	0	3	販賣個人資料	2	0	電腦病毒	3	0
網路賭博	0	3	虛設行號	5	0	電信飛客	3	0
網路老鼠會	0	2	詐騙帳號	1	0	盜用撥接帳號	6	0
色情網站	1	22	網路情人	1	0	盜版光碟	16	0
色情光碟	0	10	入侵電腦	6	0	網路誹謗	17	0
媒介色情	0	4	駭客入侵	6	0	網路恐嚇	3	0
張貼色情圖片	0	7	盜拷軟體	2	0	竊取股市交易祕密	1	0
煽惑他人犯罪	1	1	侵害商標	3	0	電腦閱卷弊案	1	0
色情及盜版	25	0	重製他人著作	3	0	盜刷信用卡	7	0
總計							113(68.5%)	52(31.5%)

六、犯罪者屬性

（一）犯罪人數

在犯罪者人數方面（如表六），單獨進行者佔86％，二人共同進行佔10.2％，三人以上共有3.7％，可見電腦犯罪大多是一人即可實施，不需他人協助；而且為達隱密性，人數愈少愈好，如有共犯，大多係親戚或朋友，目的則是有福同享；但亦有部份案件係因犯罪者本人無能力犯案，遂找到具備電腦專業知識之人幫忙。

表六　犯罪人數

人數	1	2	3	4	7	總計
件數	135	16	4	1	1	157
百分比（％）	86.0	10.2	2.5	0.6	0.6	100

（二）犯罪者性別

在犯罪者性別方面（如表七），男性佔90.5％，女性只佔9.5％，可見電腦犯罪仍以男性為主；而女性主導者大多是網路誹謗、盜用撥接帳號及侵害商標案件（見表八），其餘大多居於協助配合角色。在婚姻狀況方面，由於樣本資料太少（共14人），不具代表性，故不作說明。

表七　犯罪者性別

性　　別	男	女	總計
人　　數	171	18	189
百分比（％）	90.5	9.5	100

表八　女性犯罪者涉案種類

案類	盜用撥接帳號	虛設行號	侵害商標	網路誹謗	網路恐嚇
人數	3	1	2	6	1
案類	販賣禁藥	網路情人	重製他人著作	色情網站	電信飛客
人數	1	1	1	1	1

（三）犯罪者年齡

在犯罪者年齡方面（如表九），犯罪者平均27歲，其中14-18歲佔6.4％，19-22歲佔21.4％，23-30歲佔45.5％（此高峰可能係因男性退伍後尚未找到工作所致），31-40歲佔22.3％，41歲以上僅佔4.3％，可見電腦犯罪仍是年輕人的天下，年長者因較少接受電腦教育，較不可能涉入此類犯罪，但未來電腦教育普及後，情況可能會有所改變。

表九　犯罪者年齡

年齡	14-18歲	19-22歲	23-30歲	31-40歲	41-51歲	總計
人數	12	40	85	42	8	187
百分比（％）	6.4	21.4	45.5	22.3	4.3	100

（四）犯罪者職業

在犯罪者職業方面（如表十），以學生比例最高（25.1％），其次為無業（17.5％），此外雇主（10.4％）、職員（8.7％）及工程師（8.7％）之比例亦不低，值得注意的是共有四名老師涉案，雖然人數不多，但教職人員從事犯罪行為極易影響學生心理，必須正視此一問題。

表十　犯罪者職業

職業	學生	無	雇主	職員	工程師	商	工	自由業	公務員	軍	老師	服務業	總計
人數	46	32	19	16	16	15	13	9	6	5	4	2	183
百分比(%)	25.1	17.5	10.4	8.7	8.7	8.2	7.1	4.9	3.2	2.7	2.2	1.0	100

（五）犯罪者教育程度

在犯罪者教育程度方面（如表十一），以大專生最多（66.7％），高中（職）生次之（28.1％），其次為研究所及國中生（各佔5.3％），可見電腦犯罪者以專科以上學歷者居多。

表十一　教育程度

學　　歷	小學	國中	高中（職）	大專院校	研究所	總計
人　　數	1	3	12	38	3	57
百分比（％）	1.8	5.3	21.1	66.7	5.3	100

（六）犯罪紀錄

在犯罪紀錄方面（如表十二），無前科者佔80.4％，有一次犯罪紀錄者佔11.9％，二次犯罪紀錄者佔4.2％，三次以上犯罪紀錄者佔3.6％，可見電腦犯罪者多屬初犯，經整理前科紀錄依序為竊盜（11人次）、賭博（7人次）、販售色情光碟、違反著作權、藥事法、麻藥、偽造文書（各3人次）、煙毒、妨害風化、詐欺、侵占（各2人次）、販售非法光碟、贓物、傷害、違反槍炮彈藥刀械管制條例、肅清煙毒條例、管理外匯條例、建築法、電業法、妨害公務、恐嚇、毀損、妨害兵役、重利（各1人次）等，由此可知電腦犯罪者大多惡性不重，復以情節輕微，因此大多宣告緩刑或易科罰金處分（見表廿一）。

表十二　犯罪紀錄

前科次數	無	一次	二次	三次	四次	總計
人數	135	20	7	2	4	168
百分比（％）	80.4	11.9	4.2	1.2	2.4	100

（七）犯罪者居住地

在犯罪者居住地方面（如表十三），由於資料來源大多來自北部，因此以台北縣市居多，其中以台北縣最多（31.4％），再詳細查對資料，多屬台北市周遭之縣轄市，台北市次之（26.5％），因此電腦犯罪者居住地仍以都市為主，但由於電腦網路普及，幾乎各縣市（含離島地區）均有案件發生，可說是科技發展的

正常現象，因此各縣市警察局成立電腦犯罪偵防小組的確有其必要。

表十三　犯罪者居住地點

居住地	台北市	高雄市	基隆市	新竹市	台中市	台南市	台北縣	桃園縣	新竹縣
人數	49	10	4	1	7	5	58	14	2
百分比（%）	26.5	5.4	2.2	0.5	3.8	2.7	31.4	7.6	1.1
居住地	苗栗縣	台中縣	彰化縣	雲林縣	台南縣	高雄縣	宜蘭縣	花蓮縣	金門縣
人數	4	14	3	1	5	4	2	1	1
百分比（%）	2.2	7.6	1.6	0.5	2.7	2.2	1.1	0.5	0.5

（八）殘障人士涉案情形

犯罪者中殘障人士涉案情形如表十四，由表中顯示共有六名殘障人士涉案，雖然比例不高（共佔3.2%），但細查其原因，大多是無法找到工作，遂在家中從事此項無需勞力的犯罪行為（以色情及盜版光碟為主），而且發現在某些案件中，有殘障朋友相互聯繫情形，值得就業輔導單位注意。

表十四　殘障人士涉案情形

案類	網路老鼠會	色情網站	媒介色情	色情及盜版	總計	百分比（%）
人數	1	1	1	3	6	3.2（6/188）

七、刑事司法體系處理情形

（一）破案單位

以破案單位而言（如表十五），由於本研究資料蒐集以刑事警察局、台北市刑大和電信警察隊為主，故破案單位以上述單位為主，其中刑事警察局由於成立較早，技術亦較為純熟，為目前電腦犯罪的主要偵辦單位。

表十五　破案單位

單　　位	刑事警察局	台北市刑大	電信警察隊	高雄市警局	台中市警局	金門縣警局	總計
件　　數	101	47	8	2	3	1	162
百分比%	62.3	29.0	4.9	1.2	1.9	0.6	100

（二）移送機關

移送機關（如表十六）以台北地檢署最多（73.9%），由於網路犯罪無遠弗屆，各地皆有可能成為犯罪地點，因此即使是在中南部發生的案件，北部地區的檢察機關仍有管轄權，而且由於偵辦類似案件須具備電腦專業知識，目前作法係將部份學有專精的檢察官集中在台北地檢署，專責辦理電腦犯罪案件，但隨此類案件增多後，各地檢察機關都應具備偵辦能力。此外，部份案件由於犯罪者年齡在18歲以下，係由少年法庭審理。

表十六　移送機關

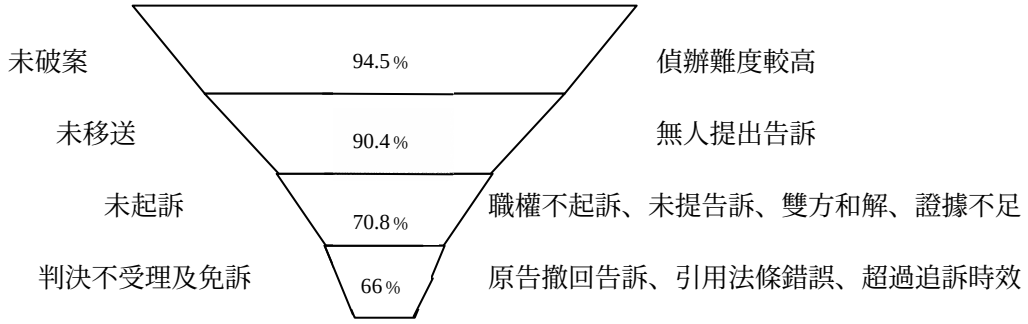
地 檢 署	台北	板橋	士林	基隆	桃園	台中	高雄	金門	少年法庭	總計
件　　數	113	19	4	1	3	1	5	1	6	153
百分比%	73.9	12.4	2.6	0.7	2.0	0.7	3.3	0.7	3.9	100

（三）處理情形

刑事司法體系處理電腦犯罪情形列於表十七，由表中可見有漏斗效應(funnel effect)（如圖二），亦即每一階段皆有流失現象，其中未破案者主要在於偵辦難度較高之電腦駭客（如表十八），而未移送的原因則包括無人提出告訴（如電腦病毒），未起訴的原因包括職權不起訴（情節輕微、坦承不諱、深具悔意）、未提告訴、雙方和解、原告撤回告訴、證據不足、法律無處罰規定。至於法院判決不受理及免訴的原因則有：原告撤回告訴、引用法條錯誤（如非著作權人無權提出告訴）、超過追訴時效等原因，而且亦有犯罪者為現役軍人而移交軍事法庭審理情形。

表十七　刑事司法體系處理情形

處理情形	破案	移送	起訴	判刑
有	156（94.5%）	154（95.7%）	72（78.3%）	41（93.2%）
無	9（5.5%）	7（4.3%）	20（21.7%）	3（6.8%）
整體百分比	94.5%	90.4%	70.8%	66%



圖二　刑事司法漏斗效應

表十八　未偵破案件種類

案類	入侵電腦	駭客入侵	網路誹謗	網路恐嚇	電腦病毒	盜用撥接帳號	總計
件數	1	4	1	1	1	1	9

（四）判處刑罰

至於判處刑罰（如表十九）中，除電腦閱卷弊案主嫌判處無期徒刑外，以有期徒刑最多（79.5%），其次是拘役（平均為42天），但刑期均不長（平均7.2月），以4-6月最多（見表廿），而且緩刑比例非常高（84.6%），未判緩刑者多為再犯或惡性重大者，如果犯罪者仍然在學，則另宣告保護管束處分，或可以易科罰金（見

表廿一），可見刑罰並不重，另有一件盜打電話案件，因被告均為年輕人且情節輕微，依少年事件處理法予以訓誡斥回。

表十九　判處刑罰

種類	無期徒刑	有期徒刑	罰金	拘役	訓誡	不受理	總計
件數	1	35	1	3	1	3	44
百分比（%）	2.3	79.5	2.3	6.8	2.3	6.8	100

表廿　有期徒刑長度

月	3	4	5	6	7	8	9	10	12	14	16	18	總計
件數	3	5	6	6	2	3	3	1	1	1	2	1	34
百分比（%）	8.8	14.7	17.6	17.6	5.9	8.8	8.8	2.9	2.9	2.9	5.9	2.9	100

表廿一　緩刑、從刑及保安處分

替代處分	緩刑	易科罰金	沒收	保護管束
件數	22	13	10	4

但是在盜版及色情光碟案件中，罰金卻相當高（平均22萬元，如表廿二），可能是法官認為此類犯行獲利甚豐，因而宣告高額罰金以收懲戒效果，且受害廠商大多會要求賠償。此外，在這類案件中，法官大多會宣告沒收其犯罪所得及相關電腦設備，以防止其再次犯案（此項沒收犯罪工具措施對年輕人相當有效），至於色情光碟及錄影帶則採沒收後集中銷燬方式處理。

表廿二　罰金額度

案　　類	色情網站	盜版光碟	色情光碟	盜版光碟	色情網站	媒介色情	色情＋盜版	平均
罰金（元）	15,000	80,000	150,000	200,000	300,000	300,000	500,000	220,000

註：本研究共蒐集七件判處罰金案件，故僅據此加以分析

八、其他資料分析

本研究案例資料中犯罪工具及主要證物因無法編碼，另行整理分析如下：

（一）犯罪工具

本研究整理案例中所使用的犯罪工具計分為六種：

1. 電腦主機：大型電腦、伺服器、個人電腦、筆記型電腦、掌上型電腦。
2. 週邊設備：燒錄器、拷貝機、掃描器、數位相機。
3. 輸出入裝置：螢幕、鍵盤、滑鼠、印表機。
4. 通訊設備：數據機、路由器、集線器、數據專線、電話交換機、行動電話、呼叫器、傳真機。
5. 儲存媒體：硬碟、磁片、光碟（程式、色情、空白、燒壞）、錄音帶、錄影帶。
6. 其他設備：投幣計時器、標籤印製機、刷卡機、錄放影機等。

（二）主要證物

司法機關所掌握到的主要證物經整理共計四類：

1. 電磁紀錄（列印報表）：網頁內容、電子郵件、新聞群組討論紀錄、電子佈告欄、網路聊天室、留言版交談內容、原始程式、病毒碼、硬碟解讀資料、BBS註冊資料、上網紀錄、郵遞名單事業資料、廣告目錄（軟體、色情）等。
2. 郵局（快遞）單據：代收郵件詳情單、郵政劃撥收支詳情單、劃撥單、掛號包裹執據、郵政信箱租用資料、匯款通知單及收據、快遞寄件存根。
3. 銀行單據：存摺、憑證取款單、信用卡帳單、銀行交易清單、彙總表、支票、金融卡。
4. 其他物品：撥接帳號申請表、假冒身分證件、印章、公司執照、營業登記證、訂貨單、出貨單、查詢訂購單、會員清單、帳冊、包裹信封袋、光碟套、色情書刊、圖片、管制藥品、往來信件、傳真等。

上述二項資料可增列於「警察偵查犯罪規範」中之「電腦犯罪案件之處理」，以作為警方偵查電腦犯罪案件之參考，並可作為犯罪模式分析之依據。

九、結論

本文係將所蒐集的案例資料，經由編碼後進行統計分析，結果歸納如下：

在犯罪特性方面，依案情分為 26 種，其中以電腦為儲存設備類型（散布色情及侵害著作）最多，犯罪地點則以住宅為主，破案件數則有逐漸增多趨勢，犯罪期間雖不長，但會持續到被發現為止，動機則以圖利為主，而無被害者部分則以網路賭博及散布色情為主。在犯罪者屬性方面，大多為單獨進行，以男性為主，年齡偏低，職業以學生和無業者最多，教育程度大多在專科以上，犯罪紀錄多屬初犯，居住地以都市為主，且有不少殘障人士涉案。

在刑事司法體系處理情形方面，雖然受到蒐集資料限制，但據了解破案單位仍集中在少數警察機關，而移送檢察機關亦有類似情形，處理結果則明顯有漏斗效應，且判處刑罰均不重，而且緩刑或易科罰金比率甚高，但科處罰金額度卻相當高。

本研究並整理出犯罪工具主要分為電腦主機、週邊設備、輸出入裝置、通訊設備、儲存媒體及其他設備；主要證物則包括電磁紀錄（列印報表）、郵局（快遞）單據、銀行單據和其他物品，可作為警方偵查電腦犯罪案件的參考；綜而言之，本文的資料分析在質量上較先前研究廣泛而深入，且可作為犯罪模式分析的參考，唯電腦犯罪現象繁雜而多元，仍有待進一步的研究，以釐清其與一般犯罪的關係。

參考文獻

[1] 王朝煌等，*網路犯罪自動化搜尋系統之研究*，交通部電信總局，1999 年 6 月。
[2] 吳國清，”警察電腦犯罪與防制措施之探討”，*第四屆資訊管理學術暨警政資訊實務研討會論文集*，2000 年 5 月 12 日，頁 201-215。
[3] 行政院研考會，*網路使用犯罪問題及預防措施之研究*，2000 年 4 月。
[4] 李柏宏、廖有祿，”電腦犯罪之問題與對策”，*警學叢刊 26 卷 6 期*，1996 年 5 月，

頁 141-154。
[5] 周宜寬，*以科爾曼理論探討美國電腦犯罪*，淡江大學美國研究所碩士論文，1994 年 5 月。
[6] 林民程，*網路犯罪之問題建構研究*，中興大學公共政策研究所碩士論文，1998 年 6 月。
[7] 陳文地，*網路犯罪模式分析及偵防對策之研究*，中央警察大學資管所碩士論文，2000 年 6 月。
[8] 林宜隆，”網路使用的犯罪問題與防範對策之研究”，*中央警察大學學報 34 期*，1999 年 3 月，頁 353-381。
[9] 林宜隆，*網際網路與犯罪問題之研究*，桃園：中央警察大學出版社，2000 年 3 月。
[10] 林宜隆、黃讚松，”網路社會與犯罪問題之研究”，*2000 年網際空間：資訊法律與社會研討會論文集*，2000 年 3 月 3 日，頁 143-145。
[11] 林煒翔，*電腦犯罪模式之分析*，中央警察大學警政研究所碩士論文，1998 年 6 月。
[12] 邱忠俊，*犯罪語言學與資料檢索應用觀念之研究－以網際網路情色文學為例*，中央警察大學資管所碩士論文，1999 年 6 月。
[13] 邱承迪，*網際網路上可疑不法資訊之自動化蒐集系統*，中央警察大學資管所碩士論文，1999 年 6 月。
[14] 麥留芳，*個體與集團犯罪－系統犯罪學初探*，台北：巨流圖書，1991 年 7 月。
[15] 曾昱國，*網路 SYN 泛濫攻擊防制機制之研究－以訊務流量控制為基礎*，中央警察大學資管所碩士論文，1999 年 6 月。
[16] 劉心陽，*網路駭客─電子商務安全實務*，台北：亞太圖書，1998 年 2 月。
[17] Angelis, G. D., *Cyber Crimes*, Philadelphia: Chelsea House Publisher ,2000.
[18] Bawden, B., “International Symposium on the Prevention and Prosecution of Computer Crime”, *Computer Law and Security Report*, May-June, 1992: pp.7-11.
[19] Coleman, J. W., ”Toward an Integrated Theory of White-Collar Crime”, *American Journal of Sociology*, 93(2), 1987: pp.406-439.
[20] Hutt, A. E., Bosworth, S. and Hoyt, D. B. (eds.), *Computer Security Handbook*, NY: John Wiley & Sons,1995.
[21] Morris, J. H., “Our Global City”, *Communications of the ACM*, 32(6), 1989: pp.661-662.
[22] President’s working group on unlawful conduct on the Internet, *The Challenge of Unlawful Conduct Involving the Use of Internet*, http://www.usdoj.gov/criminal/cybercrime/unlawful.htm, 2000, March, pp.11-14.
[23] Quarantiello, L. E., *Cyber Crime: How to Protect Yourself from Computer Criminal*, WI: LimeLight, 1997.
[24] Sterling, B., “Good Cop, Bad Hacker”, *Wired*, 3, 1995: pp.122,124-129.