我國網路詐欺之實證研究—以付款方式爲中心

The empirical analysis of Internet Fraud in Taiwan—Focusing on Type of Payment

古慧珍
臺灣桃園地方法院檢察署檢察官
桃園縣桃園市法治路一號

廖先志
臺灣桃園地方法院檢察署檢察官
桃園縣桃園市法治路一號
hjliao123@yahoo.com.tw

摘要

隨著網路使用日益頻繁，台灣之網路詐欺案件數目亦日益增加。爲精確掌握網路詐欺之特性，本文綜合「犯罪時間」及「網路相關性」二個因素來定義網路詐欺。經由上述的定義來分析實際案例後，可以發現我國網路詐欺在付款方式上，具有「多以轉帳付款」、「轉帳金額小」及「人頭帳戶多」等三個特性。而此一統計結果，以「限制轉帳金額爲3萬元」此一政策無法遏止網路詐欺之實證結果來看，亦同樣得到驗證。在偵查實務上，使用人頭帳戶常造成偵查之困難，因此，在我國，欲防制網路詐欺，除了採用與其他國家相同的交易安全制度等制度外，本文以爲，如果採取能有效地降低人頭帳戶數量之政策，應該也能夠有效地降低網路詐欺。

關鍵字：網路詐欺、付款方式、實證分析、人頭帳戶

Abstract

With increasing use of the Internet, the Internet fraud in Taiwan grows rapidly. In order to precisely describe the properties of Internet fraud, the definition of Internet Fraud should be given by combing two factors; the Internet participation in different stages of illegal action and the degree of Internet involvements. According to empirical analysis, the transfer is at the top of all types of payment of Internet fraud. Secondly, the average illegal gain is quite small. More importantly, dummy accounts are very commonly used in the Internet frauds. More than 60% of fraud cases in the Internet consists of dummy accounts involvements. Therefore, besides adopting formal approaches like the “credit system” and a safer delivery system, if we can reduce the amounts of dummy accounts we can also effectively eradicate the Internet frauds.

Keyword: Internet fraud, online payment, empirical analysis, dummy account

壹、前言

網際網路（Internet）是繼機械革命後，影響人類生活之重大發明，無論現在與未來，都將是資訊社會重要之應用與溝通媒介，藉由網際網路之廣泛應用，打破了世界各地有形之疆域，提供企業新穎而有利的商品或服務交易，也給予使用者無限的憧憬與期待。根據台灣網路資訊中心於 2005 年 1 月 23 日公布 2006 年 1 月「台灣寬頻網路使用調查」報告，截至 2006 年 1 月 16 日爲止，台灣地區上網人口成長約 1,476 萬人，整體人口(0-100 歲)上網率達 65.07%，12 歲以上人口的上網率則爲 65.97%。而台灣網路使用戶於 1996 年僅 40 萬用戶，迄至 2006 年 1 月已飆漲至 1476 萬使用戶，顯示台灣網路與寬頻發展進入成熟期，又從該報告可觀察出，網路的迅速發展，使得不同年齡層接觸網路之機會與日俱增[1]。

而隨著網際網路之互動越趨緊密後，也衍生一些難以避免的問題，尤其是日益嚴重之網路犯罪問題，依據內政部警政署之電腦網路犯罪發生件數之統計：2001 年之網路犯罪件數僅 390 件、2002 年爲 2,566 件、2003 年爲 6,824 件、2004 年爲 15,311 件，至 2005 年 12 月爲止已高達 22,111 件[2]，顯見網路犯罪發生率已成倍數急遽增加，惟網路犯罪之破獲率卻逐年降低[3]。又以美國爲例，美國網路犯罪報案中心（The US Internet Crime Complaint Center，IC3，乃美國詐欺犯罪報案中心 IFCC 之前身）於 2005 年 1 至 12 月網路詐欺申訴之件數已超過 231,493 件[4]。2006 年 1 月 25 日年美國聯邦交易委員會（Federal Trade Commission，FTC）之統計報告指出，2005 年一整年中，美國的網路購物詐欺案件已達 196,503 件，損失金額超過美金 3 億 3 千 5 百萬元[5]。而網路環境具有以下幾個特性，其犯罪成本被有效降低 [14]，而使詐欺犯罪越來越多，犯罪者越來越難被追蹤、逮捕與定罪：

一、匿名（不易追蹤）[18]：網際網路具有相當強烈的匿名性，網路上的接觸與溝通都是透過文字，最多是語音爲之，很少有真正與人面對面接觸的機會，而同時網路又缺乏真正使人信賴的身份驗證機制，因此每個人對在網路上接觸的對象，常常是與真實世界的身份不同的。而也因爲網際網路上缺乏一定的身份驗證機制，

---

[1] 參見財團法人台灣資訊中心.（2006/May/26）."TWNIC 2006 年 1 月『台灣寬頻使用調查』摘要分析"，財團法人台灣資訊中心網站，http://www.twnic.net.tw/index4.php 。

[2] 2001 年至 2005 年臺閩電腦網路犯罪發生數及破獲數-依案類別，資料來源：內政部警政署統計室

[3] 2001 年之發生件數、破獲數爲 390、265 件；2002 年發生件數、破獲數爲 2,566、1,340 件；2003 年發生件數、破獲數爲 6,824、3,081 件；2004 年發生件數、破獲數爲 15,311、5,461 件；至 2005 年 12 月止發生件數、破獲數爲 22,111、5,626 件。則 2001 年至 2005 年網路案件之破獲率分別依序爲 67.49% 、52.22% 、45.14% 、35.66% 、25.44% 。原始資料來源：2001 年至 2005 年臺閩電腦網路犯罪發生數及破獲數-依案類別，內政部警政署統計室。

[4] IC3.（2006/May/1）."IC3 2005 Internet Fraud –Crime report ", The US Internet Crime Complaint Center. http://www.ic3.gov/media/annualreport/ 2005_ic3report.pdf.

[5] FTC.（2006/Feb/26）. "Consumer Fraud and Indentity Theft Complaint Data January-December 2005", Federal Trade Commission. http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf。

同時又因爲網路使用的普遍性，因此，有心人可以在網路上隱藏身份，想要追蹤一個網路 ID 的真實身份，常常會遇到相當的困難。

二、虛擬 [17]：網際網路又被稱爲「虛擬空間」(CYBERSPACE)，這是因爲網際網路已經創造出一個完全與實體不同的世界。在台灣最早的網路遊戲「MUD」中，遊戲者僅使用文字模式，就可以共同參與一個虛擬的神話世界，每個人在其中或者扮演巫師、或者扮演妖怪這些不會在真實世界中出現的虛擬角色[6]。這股風潮到今日不但並未消退，反而日益興盛，甚至已經反過來影響真實世界，例如天幣或網路遊戲寶物的交易，所交易的客體雖然名爲「貨幣」或是「寶物」，但是實際上卻是遊戲公司所創造出來的虛擬物體，需要的人反而必須以真實的貨幣去換得虛擬的貨幣。

三、遠距（跨國界）：經由網際網路，使用者可以輕易地跨越地理的限制，而連上全世界各個網站。也可以在非常短的時間內，利用網際網路的電子郵件等功能與全世界每個角落的人聯絡。而且由於網際網路設計的特性，在與其他網路使用者聯絡時，可能會透過世界上各個角落的端點才能完成，因此，一次的網路上的活動，可能跨越許多國家。這種特性造成許多問題，例如處理網際網路的相關法律議題時，常常必須先釐清各個牽涉其中的國家是否具有司法管轄權。

因此，要如何降低網路詐欺之發生率，實乃刻不容緩之課題。雖然國內目前研究網路詐欺的文獻已有一定的數量，但是至少就筆者目前蒐集到的資料，我國網路詐欺的相關研究多僅以文獻探討、比較法爲研究之方法，鮮少利用實證分析之方式，來針對網路詐欺之案件類型進行完整的實證研究 [1][4][5][7][13][11]，因此對此類案件的類型與特性均欠缺瞭解，故有進行實證研究的必要。而在諸多網路詐欺的特性中，以筆者從事犯罪偵查的經驗中發現，網路詐欺的金錢流向經常是偵查實務上最難以追蹤的一環；再從電子商務的角度來看，「線上付款」也是「電子商務」中一個相當重要的課題，因而衍生出的技術或是法律議題更是多不勝數 [6]。因此，本文以爲，不論是從犯罪偵查或是電子商務發展的角度觀察，找出網路詐欺付款方式的特性都應該是研究網路詐欺的一個重要部分，而美國聯邦貿易委員會（Federal Trade Commission，FTC）所做的網路詐欺統計報告中，即以付款方式做爲統計項目之一[7]，但反觀國內，目前似乎尚未有任何相關的研究或統計資料。亦即依照現有的文獻，尚無從瞭解我國網路詐欺之真正現況，例如到底那幾種詐欺的態樣佔網路詐欺的大宗？詐欺案件的付款方式爲何？而這種瞭解對網路詐欺之防制是不可或缺的。

因此，本文以下將先探討網路詐欺之定義，並將按照此定義，從網路詐欺原始資

---

[6] 有關網路遊戲的歷史，請參見陳婷君.（2006/June/2）.”網路與遊戲，” http://sweb.nuu.edu.tw/~U9316009/Study.htm#11。

[7] 以 2005 年爲例，該年美國網路詐欺中犯罪被害人付款之方式經統計爲：信用卡支付（30% ）、bank account debit（23% ）、check（16% ）、wire transfer（15% ）、 money order（11% ）、cash/cash advance（4% ），可從此看出美國網路消費購物者，多數係以信用卡支付購物價金，而付現金或預先付現則只佔 4% 的比例。參見 Consumer Fraud and Identity Theft Complaint Data January-December 2005，page3，http://www.consumer.gov/sentinel/pubs/ Top10Fraud2005.pdf（2006/Feb/26）。

料（primary data）著手，先觀察統計網路詐欺之態樣、類型。再從詐欺行爲人「取款」，也就是被害人「付款」的面向來檢視我國網路詐欺的特性，並嘗試歸納出網路詐欺的共通點，尤其是在付款方式上的共通點。在找出我國網路詐欺在付款款項上的共通點後，本文將繼續以於 2005 年 6 月新實施的「限制轉帳」制度，來驗證本文所歸納出的我國網路詐欺共通點是否正確，並希望能由此出發，探討防制我國網路詐欺案件之有效方法。

貳、網路詐欺之定義

網際網路具有無遠弗屆、無國界性之特質，故網路詐欺之犯罪型態，只要有網路存在的地方，就有發生網路詐欺犯罪之可能，然而，對於網路詐欺之定義與意涵，則尚未出現一致的定義。美國司法部（Department of Justice）對於網路詐欺（Internet Fraud ）所下之定義爲：係指利用網路或網路空間之一部分對潛在之被害人實施誘騙行爲，進而使被害人與之進行交易，或依照詐欺指示將款項匯入金融機構或其他相關機構。而利用網路之方式，例如：聊天室、電子郵件、訊息佈告欄、網頁網站等[8]。有學者則依照網路在犯罪中使用程度的不同，將網路在犯罪中的地位分爲「網路作爲犯罪的目標」、「網路作爲犯罪之工具」及「網路在犯罪中非故意被使用」[15]。另有學者認爲網路詐欺是「網路犯罪中利用網路作爲詐欺工具或詐欺空間的一種犯罪類型」[5]；或是將網路詐欺定義爲「行爲人經由網際網路，欺騙自然人或操控電腦，而取得財產之行爲」[13]。

但本文以爲，上述美國司法部及學者對網路詐欺定義，仍各有不少缺點。首先，上述美國司法部的定義似乎將所有網路交易相關的詐欺都包含在內，不論這個交易的發生與網路是否直接相關，例如詐欺犯罪者與被害人在網路聊天室中認識並進而交往，然後基於這個關係而發生了詐欺，依照這個定義，也是屬於網路詐欺；另一方面，詐欺案件發生未必一定包含交易行爲，例如駭客侵入網路銀行系統以取得款項的網路詐欺類型，則似乎又不包含在這個定義裡面，因此本文認爲這個定義似乎不夠周全。

另外，上述學者有關網路詐欺的定義則不夠具體，例如「網路作爲犯罪的目標」「以網路作爲犯罪之工具」，則何謂「目標」？何謂「工具」？這些重要關鍵都並未解釋清楚。又例如：一般詐欺案件的受害者，利用網路銀行匯款[9]，是否也是在利用網路爲「工具」而進行詐欺？又如在拍賣網路上刊登出售「權利車」之廣告，被害人與被告約出見面看車，被害人覺得沒有問題，才決定購買，但這輛所謂的「權利車」，後來發現實際上卻是贓車[10]，如果依照上面學者的定義，這類案件應該是屬於利用網路爲

[8] The U.S. Department of Justice. "Ihe Internet Fraud", The U.S. Department of Justice http://www.internetfraud.usdoj.gov/#What%20Is%20Internet%20Fraud. (2006/Feb/26)
[9] 高雄地檢 94 年度偵字第 5380 號案件。
[10] 士林地檢 94 年度偵字第 9692 號案件。

「工具」的網路詐欺犯罪，但這種詐欺案件真正利用網路的成分不高。簡而言之，這些學者的定義都過於抽象，對實際判斷具體個案是否屬於網路詐欺的幫助不大，而且經常會使我們將許多與網際網路沾到一點邊的詐欺案件都歸類到網路詐欺，使得網路詐欺的範圍過於擴大，反而無法清楚凸顯網路詐欺案件本身的特色，也將失去將網路詐欺案件類型化的目的。因此，本文認爲在進行蒐集及分析國內網路詐欺案件之前，仍有探討網路詐欺定義之必要。以下本文擬以二個面向來探討網路詐欺，第一個面向是犯罪手段與網路科技的關連性，第二個面向是犯罪行爲的時間，分述詳述如下：

一、與網路關連性

如前所述，網際網路具有上述之匿名、虛擬及遠距之三個特性，而網路詐欺之所以與一般傳統詐欺犯罪相異之處，也就是因爲網路詐欺多多少少利用到上述的幾個特性。但是，網路詐欺與幾個特性之間的關連性並非一視同仁，而仍有高低差別。例如，有相當程度網路詐欺的犯罪者之所以使用網路來進行詐欺，就是因爲在網路上可以匿名，從而追查起來具有相當的困難度。另外，在許多因爲買賣網路寶物而發生的詐欺行爲，其被害的客體基本是網路這個虛擬空間所製造出來的，所以這也是與詐欺犯罪具有相當關連的網路特性。總體而言，上述的三個特性中，以匿名性最爲重要，因此如果網路詐欺的發生與犯罪行爲人利用網路之「匿名性」才得以完成，則這種詐欺當然屬於網路詐欺。至於其他的網路特性，則是必須綜合考量，原則上具有越多項特性，而且關連程度越強的詐欺案件就越屬於網路詐欺案件。

二、行爲時間

網路詐欺的另外一個要素是詐欺行爲開始的時間，因爲必須要在詐欺著手以後，行爲人的行爲才具有不法性或是可罰性 [8]。刑法學者並將犯罪行爲區分成前後連續的幾個行爲階段：決意（陰謀）、預備、著手實施、完成行爲、發生結果。其中決意指行爲人出於各種不同之動機而萌生犯意，而陰謀乃指兩人以上互爲犯意之表示而共同協議計謀實施犯罪，故決意與陰謀均屬犯罪行爲人之內心意思決定 [3]，而共同正犯因爲人數在二人以上，爲達成一致的犯罪合意，故共同正犯之形成多須經過陰謀的過程 [12]。另預備則指行爲人爲實現其犯意，在著手實行犯罪行爲前，所爲之準備行爲而言，例如預備犯罪之工具等行爲，都屬於預備行爲 [3]。至於著手實行則指行爲人開始實行犯罪行爲而言，亦即行爲人爲實現其犯意，而開始實行構成要件之犯罪事實之行爲 [3]，學者以爲，犯罪著手就等於犯罪行爲，二者是同義詞 [11]，因此，犯罪者當然必須達到著手實行詐欺行爲的階段，才有可能構成網路詐欺，否則可能僅僅成立其他犯罪，甚至根本不構成犯罪。

三、模型—「行爲時間」+「與網路關連性」

本文以爲，就「網路詐欺」顧名思義，有二個重要的要素組成，一個是「網路」，一個是「詐欺」。以第一個要素「網路」來說，網路詐欺當然是應該與網路特性具有高度的相關，才有必要歸類爲「網路詐欺」，否則就與一般詐欺並無不同。另外第二個要素「詐欺」，則是應該最少已經達到著手的階段，否則就可能屬於另外一種犯罪 [10]。同時，二個因素又必須綜合觀察，「網路」這個要素，必須是在詐欺行爲人在「著手」以後的階段利用，才能算是「網路詐欺」。將上面二個因素綜合考量，就可以勾勒出網路詐欺的完整形象及定義。如果將「行爲時間」這個因素做爲橫軸，再把「與網路特性之關連」這個因素爲縱軸，本文將「網路詐欺」的定義圖示如下：

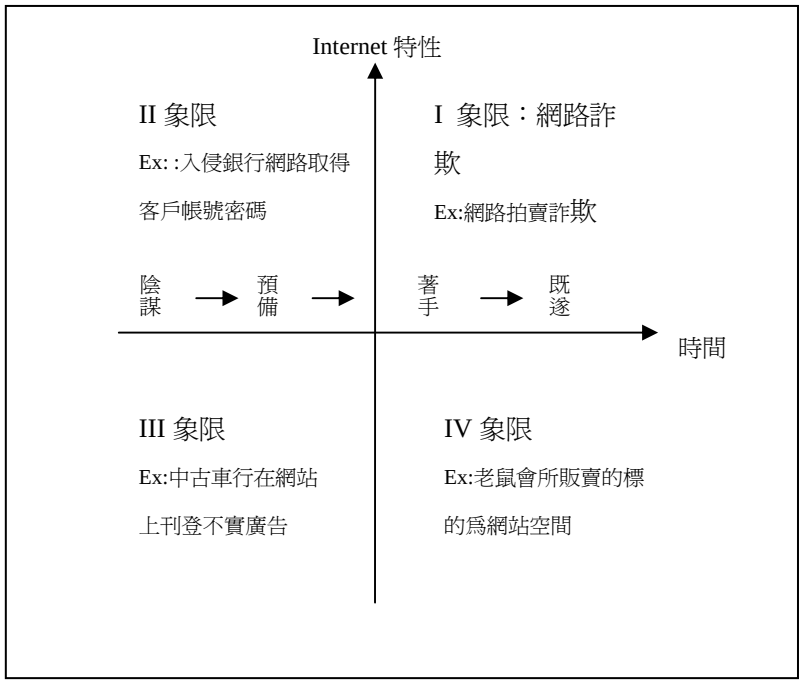

圖 1：依行爲時間與網路關連性定義網路詐欺

在上面的圖中，落在第一象限的行爲，其特性是該行爲與網路特性高度相關，而且行爲在著手階段以後，仍然與網路相關，這種行爲，本文把它定義爲網路詐欺。第二象限的行爲則雖然此種行爲與網路特性高度相關，但是就詐欺犯罪個觀點來看，這個行爲還沒有達到詐欺的著手，可能僅在預備階段，例如駭客竊取信用卡資料，這種行爲徹底的利用網路特性，但是駭客僅是取得密碼，而取得密碼的目的可能有很多，當然詐欺可能是一個，但是基於純粹好奇的案例也有，因此在法律上通常認爲這種行

爲還沒有達到「著手詐欺」，所以不算是網路詐欺[11]。至於歸類第四象限的行爲，其特性則是與第二象限的行爲剛好相反，就是此種行爲已經開始到達著手詐欺的階段，但是這種詐欺與網路特性較不相關，因此這種行爲也不能算是網路詐欺，例如老鼠會的上線向下線推銷的東西是網路磁碟空間，則老鼠會販賣的東西僅是一種使被害人上當的工具而已，固然利用網路的熱潮比較容易使被害人受騙，但是畢竟與網路的特性關係不大，而僅僅屬於傳統的詐欺，又例如前面提到詐欺被害人利用網路銀行匯款，同樣與網路之相關性有限，因此也是落在第四象限。而落在第三象限的行爲，例如中古車商在網路上刊登賣車的廣告，他的交易方式還是與傳統的中古車商一樣，必須到現場看車，則如果在沒有被害人看到廣告而真正來車行看車之前，因爲網路僅是刊登廣告的一種媒體而已，與報紙、傳單、電視的地位沒有任何不同，所以這種行爲與網路特性的關連性不高，而一般認爲刊登廣告的行爲也還不是詐欺行爲的著手，所以這種行爲，本文將之歸在第三象限，也不屬於網路詐欺。簡而言之，僅有詐欺已經達到著手的階段，而且該行爲在著手以後的階段中使用的詐術與網路特性高度相關，而非僅是用到網路而已，則這種行爲才能歸類爲網路詐欺。

本文認爲從「網路關連性」與「行爲時間」兩個面向來分析一個詐欺案件是否屬於網路詐欺案件，比過去的定義具有更強的操作性，可以清楚地判斷一個實際案例是否屬於網路詐欺還是一般詐欺。本文以下就將利用這個定義，來統計分析我國實務上發生的網路詐欺案件，並試圖找出這些網路詐欺案件的特性。

參、實證分析之設計

本文之實證分析共分爲二個部分：第一部分爲先從原始資料中抽樣部分案件來觀察我國網路詐欺之類型及付款方式之特色。第二部分則利用「事件研究法」來驗證在第一步驟中所得到之付款面特性是否正確。以下分別將上述二個部分的研究方法分述如下：

一、第一部分：抽樣及統計

本研究這個部分係利用法務部部內網站之檢察書類查詢系統，以「網路&詐欺」、「網站&詐欺」、「網際網路&詐欺」三組關鍵字搜尋，搜尋期間設定爲偵結日期 2005 年 1 月 1 日至同年 12 月 31 日之書類，包含起訴、緩起訴、不起訴處分等所有案件，再利用上述綜合「時間」與「網路特性」二個面向的網路詐欺定義，以人工方式篩選出所有屬於網路詐欺的案件。再依照案件的類型及付款方式加以歸類及統計。

[11] 但是可能觸犯其他刑罰法律，但這不在本文討論網路詐欺的範圍之內。

本研究之所以採用各檢察書類爲研究樣本，是基於以下幾個理由：首先，在現行的刑事訴訟法制度中，檢察官爲偵查之主體，故所有的案件，不論是警方的移送案件、或是人民直接向檢察官告訴、告發的案件，均會由檢察官判斷其是否應起訴或是爲其他處理，故地檢署的書類較警方的移送案件更爲全面。其次，由於檢察官具有法律之專業及長時間的偵查訓練，故其書類之撰寫多經過一定之思考，才會判斷其是否符合刑法某一個犯罪之構成要件，故若檢察官將之判斷該行爲確實符合某一個構成要件，則其錯誤之可能性甚小。最後，檢察官之書類也會遵循構成要件而清楚說明，故在資料分析的時候，一方面不會因爲書類內容不明而導致錯誤，更進而可以加快搜尋的速度。基於以上的幾個理由，本文才會決定以各地檢署的案件爲對象來統計網路詐欺之態樣與類型，但也因爲如此，本文研究對象無法涵蓋警方未偵破，或是民眾未報案的案件。另外，由於人力的限制，本文僅能選取結案時間在 2005 年這一年內結案的案件做爲分析樣本，無法進行更全面性的樣本蒐集。

二、第二部分：事件研究法

本文實證研究的第二部分中，是利用「事件研究法」（Event Study）[12]，以統計方式驗證本文在第一步驟中歸納所得到的我國網路詐欺在付款面上的特性是否正確。所謂「事件研究法」，是一般會計與財務學研究學經常使用之研究方法。「事件研究法」主要目的是觀察某一事件的發生或資訊的發布，是否會改變投資人的決策，進而影響股票價格或交易量的變化。而本文亦借用此「事件研究法」觀察特定犯罪防制政策之實施，是否會影響所欲遏止之特定犯罪之犯罪量。

本文應用「事件研究法」的第一步驟，即是確定研究事件及「事件日」：本文所欲研究之事件是「限定金融機構ATM每日非約定轉帳上限爲3萬元」（以下稱「限制轉帳金額」），此一防制策略實施之時點爲2005年6月1日。在確立本文研究之事件及「事件日」後，第二步驟是針對研究事件做樣本選擇與觀察期間之設定。其中之觀察期間包括「事件期」、「估計期」之設定，本文所設定之「事件期」是指某一防制犯罪政策實施之當日及之後的一段期間；而「估計期」則是在防制犯罪政策實施之前的一段期間，此段時間是獨立於事件期間的，也就是不受研究事件影響干擾的一段時間。又本文觀察之「非約定帳戶之限制轉帳」事件，因發生時點較其他事件晚約將近二年，礙於研究時間、人力、經費及採集樣本是否足夠等諸多限制，此事件之觀察期間只能限於2005年12月31日爲止，且因爲偵查案件與實際發生案件有延遲性，所以無法再採用與第一部份相同之原始資料來進行分析，因此改採內政部警政署所統計的二手資料。第三步驟，即是針對本文實證研究第一部份所提出之我國網路詐欺在付款面上之特性，推論『在此特性下，「限制轉帳金額」對網路詐欺是否有用？』，繼而以事件觀察法，觀察、統計「事件期」與「估計期」犯罪量之月資料變化，進行分析及數據之說明，來驗證此一推論之正確性，

[12] 台灣經濟新報文化事業公司，事件研究法暨模組，www.tej.com.tw/webtej/doc/事件研究法.doc(2006/Sept/10)

從而驗證在第一部分所歸納出之網路詐欺付款特性是否正確，故可將事件之觀察期間表示如下圖。

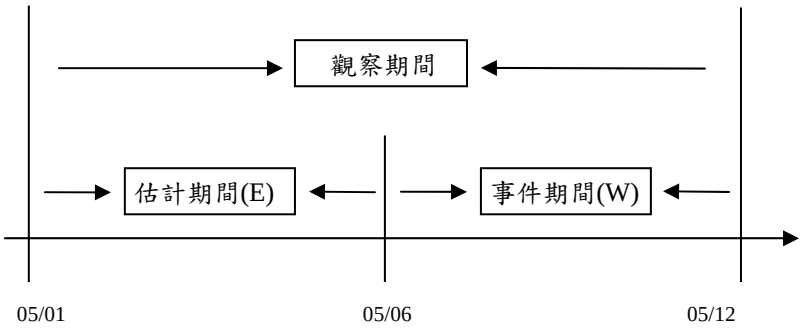

圖 2 「非約定帳戶之限制轉帳」事件之觀察期間

本文在此處採取之方法爲統計學中之曼-惠特尼 U 檢驗法（Mann-Whitney U Test），來說明數據之分佈差異。Mann-Whitney U Test 屬於一種無母數統計，是利用誤差的概念。而 Mann-Whitney U Test，是適用在比較兩個隨機樣本之差異，例如：檢驗實驗組與控制組的實驗數據顯示兩組的結果是否有明顯差異。若經過檢定後之觀察值（P 值）小於 0.1 之臨界值，則這兩個樣本的觀察值有明顯差異，表示這兩組樣本的分配不一樣，白話地說就是這兩組觀察值認爲是不一樣的。而本文中用此檢定方法，來觀察事件日前、後犯罪量（觀察值）之數值，是否有明顯之差異。

肆、我國網路詐欺付款方式之實證分析

利用上述的方法，本文過濾全國各地檢署處理之所有詐欺案件中被歸類爲網路詐欺的案件數目共計 924 件，本文將各種案件進行分類，分析這 924 件案件以後發現：網路詐欺案件中以網路拍賣詐欺、網路遊戲詐欺、網路色情詐欺及網路盜刷信用卡等四大類爲大宗，故本文製作圖表說明網路詐欺之類型與比例，分別參見表 1、2。

表 1　網路詐欺類型之名稱及其定義

網路詐欺類型之名稱	網路詐欺類型之定義說明
網路拍賣詐欺	在拍賣網站中販賣物品[13]而導致之詐欺
網路遊戲詐欺	與網路遊戲相關之詐欺案件。包含買賣寶物、遊戲帳號等。

[13] 包含有體物或無體財產（如服務、IP），但不包含網路遊戲之相關寶物、天幣等

網路色情詐欺	在網路上僞稱可進行色情交易以進行詐欺
網路盜刷信用卡詐欺	在網路上盜刷他人之信用卡
其他網路詐欺	如：使用網路電話（使用網路電話進行詐欺）、木馬程式（以木馬程式或間諜軟體）、使用他人名義上網（以他人帳戶上網）、網路交友（在網路上交友而進行詐欺）等

表 2　各類網路詐欺之件數、被害金額表（按照件數多寡排列）

	網路詐欺類型	件數	比例	總金額（元）	平均金額（元）
1	網路拍賣詐欺	465	50.32%	16,575,255	35,645.7
2	網路遊戲詐欺	303	32.79%	7,382,260	24,363.9
3	網路色情詐欺	78	8.44%	9,277,134	118,937.6
4	網路盜刷信用卡詐欺	35	3.79%	269,078	75,973.7
5	其他網路詐欺	43	4.65%	7,946,914	184,812
	全部合計	924	100%	43,840,641	47,446.58

另從詐欺行爲人「取款」即被害人「付款」的角度觀察，人頭帳戶與網路詐欺間的關連性，而統計之結果如下表 3：

表 3　網路詐欺與人頭帳戶之關連比例表

網路詐欺案件	件數	件數百分比	金額（元）	金額百分比
全部	924	100%	43,840,641	100%
以轉帳方式付款	833	90.15%	19,780,532	45.6%
以人頭帳戶取款	612	66.23%	34,153,014	78.7%

本文再將 833 件以轉帳付款之網路詐欺案件，依照每筆轉帳之平均轉帳金額[14]整理如下表 4。

[14] 轉帳筆數與案件數不同，轉帳筆數是指轉帳的次數，而案件數則是一個被害人被騙就算一件，而一個被害人可能轉帳許多次，因此，轉帳筆數會大於案件數。

表 4 使用轉帳之網路詐欺案件之金額統計

詐欺轉帳金額	轉帳筆數及百分比		匯款進入人頭帳戶之筆數及百分比	
金額（元）	轉帳筆數	百分比	轉帳筆數	百分比
10000 以下	883	58.36%	599	57.87%
10000-20000	235	15.53%	213	20.58%
20001-30000	84	5.55%	59	5.70%
30001-40000	61	4.03%	39	3.76%
40001 以上	250	16.52%	202	19.51%
全部合計	1513	100%	1035	100%

從以上的實證分析結果，可以發現出我國網路詐欺在付款方式與前述美國之網路詐欺顯著不同[15]，我國網路詐欺之付款方式有以下三個特徵：

1. 多以轉帳方式付款：我國網路詐欺案件中，被害人付款之方式僅大多爲轉帳，達 833 件，佔全部網路詐欺之百分之 90.15%。（參考表 3）
2. 使用人頭帳戶之比例偏高：我國網路詐欺案件中，共計 612 件是轉入人頭帳戶，佔全體網路詐欺 924 件中之 66.23% ，佔以轉帳付款之網路詐欺 833 件之 73.5% （參考表 3）。若以網路詐欺之轉帳筆數觀察，轉帳金額未超過 3 萬元之 1202 筆轉帳中，有 871 筆轉帳是轉入人頭帳戶，即轉入人頭帳戶的筆數佔全部之 72.46% (參考表 4)。
3. 轉帳金額之小額性：在以轉帳付款之網路詐欺中，全部轉帳之平均每件金額爲 23,553.6 元，且每筆金額未超過 1 萬元之件數超過五成（58.36% ），而金額未超過 3 萬元之件數占 79.44% (參考表 4)。

伍、以「事件研究法」驗證我國網路詐欺之支付特性—轉帳及小額

依照本文上述實證統計之觀察發現，我國網路詐欺案件中有超過九成案件中被害人是以轉帳方式付款，而平均每筆轉帳金額僅爲 23,553.6 元，有將近八成的轉帳其金額未超過 3 萬元，如果此一統計結果屬實，則我們可以合理推論將「限制轉帳金額」設爲 3 萬元之政策，對於大部分使用網路之詐欺犯罪可能並無影響，故將無法有效降低網路詐欺之發生，本文以下即以「事件研究法」來驗證此一推測是否正確。

[15] 參見註 7

本文觀察的對象是 2005 年警察單位受理各類型詐欺之數目[16]，另外本文還選擇手機簡訊詐欺來與網路詐欺做爲對比。其結果分如下圖 3：

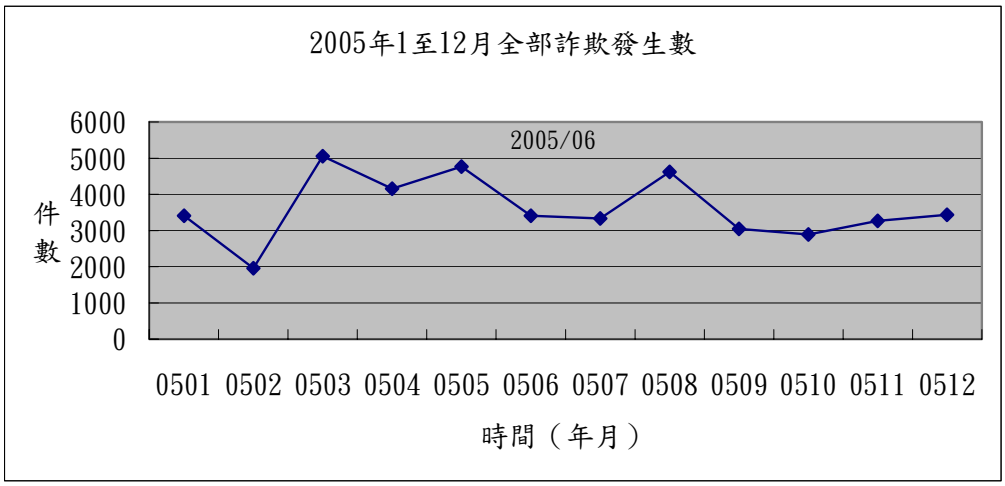

圖 3 2005 年全部詐欺逐月曲線圖[17]

經使用 Mann-Whitney U Test 檢定事件發生前後之案件，2005 年 1 至 5 月之前每月平均 3870 件；同年 6 月以後平均每月件數爲 3427.43 件，全部詐欺之案件量雖略微降低，但並無顯著性（U＝24.5；P＝0.26）。

如果再看手機簡訊詐欺的逐月發生數，如下圖 4：

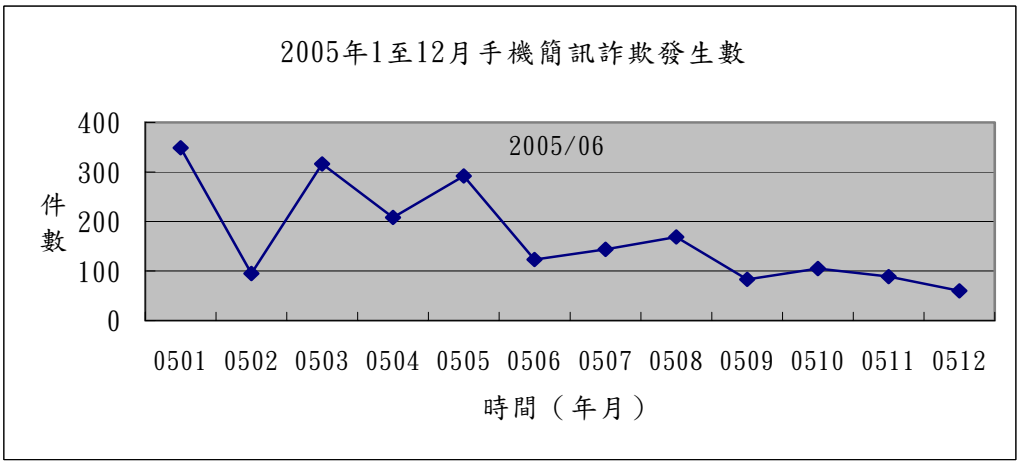

圖 4 2005 年手機簡訊詐欺逐月曲線圖

[16] 雖然本文之前分析網路詐欺之特性時，是以檢察機關之書類爲分析對象，但檢察機關處理案件之結果除起訴、不起訴外，尚有通緝等其他可能之結果，而此類結果並無法以檢索書類的方式取得，進而無法記入發生數內，因此，若此處繼續採用檢察機關之處理件數做爲詐欺案件發生數，會導致發生數發生較大的誤差，反觀以警察機關受理件數做爲案件發生數則不會有這種缺點，故此處則改爲採用警方受理件數做爲網路詐欺之發生數。

[17] 資料數據來源爲內政部警政署內部統計資料。

又經使用 Mann-Whitney U Test 檢定事件發生前後之案件，2005 年 1 至 5 月之前每月平均件數 252 件；同年 6 月以後平均每月爲 110.43 件，手機簡訊詐欺案件量之降低在 5% 水準下已具顯著性（U＝32.0；P＝0.01）。

最後再觀察電腦網路犯罪，但本文發現有一可能干擾之變數，即在台灣地區電腦網路犯罪之各案類別下「妨害電腦使用」發生數之變化。簡言之，即我國網路詐欺之態樣中佔 32.79%之「網路遊戲詐欺」，在 2003 年 6 月 25 日刑法修正公布「妨害電腦使用」罪章後，只要網路詐欺牽涉與網路遊戲相關者，內政部警政署之統計即會將此種詐欺案件之發生數，歸入台灣地區電腦網路犯罪之各案類別下之「妨害電腦使用」。因此，2003 年 7 月以後網路詐欺案件發生數之下降，即有可能是因爲部分應歸類於網路詐欺之案件，因修法後適用法律之不同而導致歸類於其他類型之案件，而產生有發生數下降的結果。爲此，本文進行對移送至地檢署而案由爲「妨害電腦使用罪章」之案件抽樣統計，統計結果發現其中約有 24%的案件亦應屬網路詐欺之網路遊戲詐欺類型[18]。所以，本文試圖將「妨害電腦使用罪」之發生數乘上 24%後加回「網路詐欺」之發生數來觀察，如圖 5。

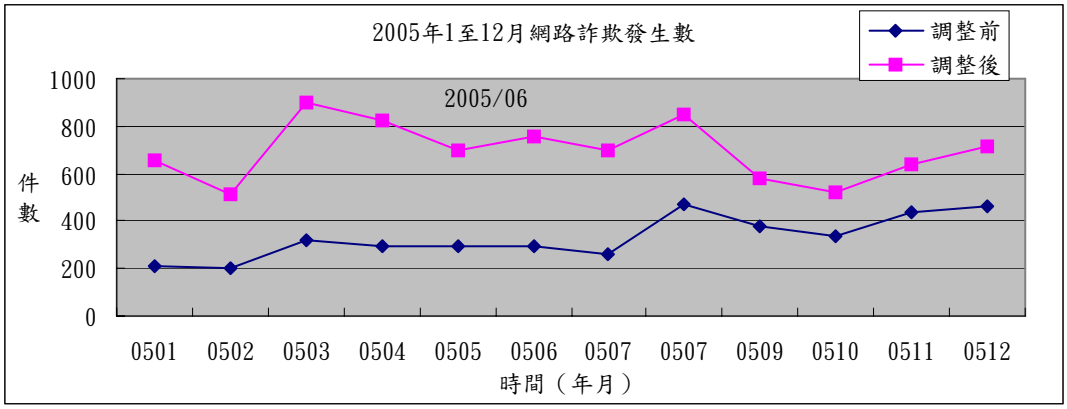

圖 5 2005 年網路詐欺逐月曲線圖

經使用 Mann-Whitney U Test 檢定事件發生前後之網路詐欺案件，調整前之情形爲：2005 年 1 至 5 月之前每月平均 261.2 件，同年 6 月以後平均每月件數爲 377.43 件，網路詐欺案件量不僅未降低反而提高，且案件量之變多已有顯著差異（U＝31.0；P＝

[18] 爲了求得正確的資料，本文以「刑法第三百五十八條」、「刑法第三百五十九條」爲關鍵字，搜尋士林等 12 個地檢署於 2005 年 1 月 1 日至同年 6 月 30 日止偵查終結之案件，發現在所有觸犯刑法第 358 條或 359 條的案件中，有部分案件亦屬於本文上述歸於第一象限的網路詐欺案件，例如詐取他人之網路遊戲寶物，或是以他人帳號上網進行網路遊戲等，換言之，這些案件如果是發生在修法前，應該適用刑法 339 條詐欺罪，所以應該將之加入網路遊戲詐欺來計算。之所以此處又採用檢方的案件來進行分析，其原因在於警政署僅有提供統計資料，而沒有具體的個案資料，故僅能以檢方資料得到近似的比例數據。此處不能不說是一個統計上的嚴重缺陷，但作者就這個問題苦思許久，目前也只有想到這個方法，期待未來可以以其他方法得到更正確的數字。

0.03）。雖然加上 24%之「妨害電腦使用罪」之發生數，即調整後之網路詐欺件數該年度前 5 月之月平均件數爲 716.67 件，而 6 月以後之月平均反而略爲下降至 661.14 件，但件數減少尚未具顯著性（U＝20.0；P＝0.68）。故不論是觀察調整前、調整後之網路詐欺發生數，我們都可以說非約定帳戶之轉帳限制對於特定之網路詐欺並無明顯成效。

由以上圖及統計檢定之說明可知，非約定轉帳之限制，對於手機簡訊此類之詐欺確實有成效，但在另一方面，網路詐欺之件數則並未因爲限制轉帳而有顯著降低，這可以驗證本文在第一部份所歸納出之我國網路詐欺「多以轉帳付款」及「轉帳金額具有小額性」之結論爲正確。

陸、代結論

隨著網際網路的普及，網路技術之成熟與上網人口、時數之激增，網路使用的活動內容也日趨多樣化，伴隨而來的負面效應，即是增加了新型態的犯罪機會，其中網路詐欺犯罪之層出不窮，直接對於電子商務的發展造成嚴重威脅，加之，網路犯罪之隱匿性等特性導致查緝之困難性，故對於網路詐欺犯罪之防制，已成爲刻不容緩之議題。基於過去網路詐欺的定義不夠清晰，在判斷實際案例上產生許多困難，所以本文首先嘗試綜合考量「網路關連性」與「行爲時間」等兩個面向，提出一個新的網路詐欺定義，只有與網路特性高度相關的詐欺案件，而且是在著手實施詐欺行爲後仍使用網路特性的詐欺案件，本文認爲才是屬於網路詐欺案件。

本文使用上述的定義，從台灣地區各地檢署在 2005 年一年內的偵查終結的案件中，過濾出 924 件屬於網路詐欺的案件。將這 924 件案件分析統計後，本文發現，隨著國民特性、交易習慣、科技發展程度等因素的不同，網路詐欺也如同其他犯罪一樣，在不同國家具有不同的特性。比較我國與美國，網路詐欺的主要類型即不完全相同，例如在我國網路詐欺案件占 20%的「網路色情」案件，就並未在美國的統計資料中出現。另外，我國網路詐欺案件中超過九成的被害人是以轉帳方式付款，這與美國有相當大的差異，而在所有網路詐欺中，又有 66.23% 的案件詐欺犯罪者是用人頭帳戶的方式取款，或許這是因爲人頭帳戶使網路的「匿名性」或「不可追蹤性」等特質得以更加發揮，另外，我國網路詐欺被騙金額每筆不超過 3 萬元者高達 79.44%。因此我們可以說，我國網路詐欺在付款面上的特色，主要就是在「轉帳付款」、「轉帳金額小」及「使用人頭帳戶」三個特色上。本文也利用警政署提供的統計資料，以事件觀察法驗證在這樣的網路詐欺付款特性，尤其是「轉帳付款」及「轉帳金額小」這二個特性下，「限制轉帳金額爲 3 萬元」此一防制詐欺政策，對網路詐欺並無效果。

而此一實證結果也推翻了一般認爲「網路犯罪具有相當的高科技知識」的既定印象，因爲經過本文上述的分析以後，我們可以發現台灣的網路詐欺案件並不見得具有多高的技術性，像佔比例最高的網路拍賣詐欺與網路遊戲詐欺而言，對今日網路普及率相當高的台灣來說，這類網路活動中使用到的網路科技幾乎是小學生也能輕易完成。實際上，台灣的網路詐欺案件真正爲一般人所無法完成的部分，也是台灣網路詐

欺最特殊之處，是與網路科技無多大關係，但卻是偵查實務最難以突破的重要關鍵：「利用人頭帳戶取款」。對於具有此種「台灣特色」的網路詐欺犯罪，本文認爲在我國要防制網路詐欺，除了採取信用評價、改進網路付款方式的方式等與世界各國共通的方式[16]，還應該對我國網路詐欺之上述特性多加考慮，而採取與其他國家採用不同的做法，像是從加重提供人頭帳戶之刑罰；或是將銀行開戶階段設定爲阻絕「詐欺集團利用人頭戶犯罪」之第一線，而仿照美、日等國將個人信用商品建立個人信用評等制度[2]，亦即金融機構在開戶辦理徵信時，也應該比照放款時的嚴格態度，考慮個人信用評等，若有瑕疵或評等不佳，就應拒絕開戶之申請或經過一段猶豫觀察期間後始可准予開戶。唯有如此，才能使每個人愛惜個人信用，有效降低人頭戶之使用，增加網路詐欺的犯罪者取款不便及提高其查獲風險，從而降低網路詐欺的發生，建構一個良好的網路環境。

參考文獻

[1] 李明儒，*網路詐欺之法律探討與管理—以線上拍賣爲例*，國立交通大學管理研究所碩士論文，2005。

[2] 李禮仲，開戶拍照消滅人頭戶財政部淪爲採證部，*聯合報*，民意論壇，2003 年 11 月 1 日。

[3] 林山田，刑法通論（上），台北：自版，1998 年：頁 298。

[4] 林佳蓉，「網路詐欺案件類型、法律適用及犯罪防治之道」，*資訊法務透析*，2001，頁 50。

[5] 林宜隆，「網路犯罪之案件分析」，*中央警察大學學報*，37 期，2000：頁 224。

[6] 林豪鏘，電子商務，台北：旗標出版股份有限公司，2005：頁 2-42。

[7] 章京文，「與網路詐欺奮戰—以美國及我國之現況爲例」，*2002 網路犯罪與法制研討會論文集*。

[8] 黃榮堅，刑罰的極限，台北：月旦出版公司，1998：頁 264。

[9] 黃榮堅，基礎刑法學（下），台北：元照出版公司，2003：頁 17。

[10] 黃榮堅，基礎刑法學（下），台北：元照出版公司，2003：頁 33。

[11] 廖有祿、李相臣，電腦犯罪—理論與實務，台北：五南圖書公司，2003：頁 141-162。

[12] 蔡墩銘，中國刑法精義，台北：漢林出版社，1993：頁 199。

[13] 謝開平，*電腦詐欺在比較刑法上之研究*，國立台北大學法律學研究所博士論文，2003 年，頁 19。

[14] 戴豪君，數位科技法律大未來，台北：書泉出版社，2004 年：頁 137。

[15] Gerald R. Ferrera，張楚等譯，網路法--課文與案例，北京：社會科學文獻出版社，2004 頁：303 頁。

[16] Albert, Miriam R.. “E-BUYER BEWARE: WHY ONLINE AUCTION FRAUD SHOULD BE REGULATED”, 39 *Am. Bus. L.J.* pp. 575, 2002

[17] Brey, Philip., “Evaluating the Social and Culture Implications of the Internet”, *Computer and Society Magazine*, (35:3). 2005.

[18] MacInnes, Ian. Musgrave, Domani. Laska, Jason. 2005, “Electronic Commerence Fraud: Towards an Understanding of the Phenomenon”, *Proceeding of the 38th Hawaii International Conference On System Science-2005*。