由系統動態觀點建構網路犯罪預測模擬：以網路詐欺與妨害電腦使用罪行為例

王貞淑
中華大學資訊管理所

鍾典村
中華大學科管所

摘要

網際網路的便利性大幅的改善了使用者生活品質，像是財務金融或是線上購物的應用，都讓使用者省下不少親自臨櫃辦理的麻煩。但是隨之而來的網路安全考量，也往往讓使用者必需承受個人資訊外洩的風險。根據傳統的犯罪理論，網路犯罪不只是犯罪者個人行為，更涉及到許多因素間的交互回饋影響，是一個典型的系統動態複雜問題。本研究以系統動態模擬方法，分別建構出網路犯罪問題的攻擊與防守兩個構面，提供網路犯罪問題的核心結構，並進行網路犯罪參數的預測。最後，再以台灣地區民國88年至96年間，網路詐欺及妨礙個人電腦使用犯罪行為的實際犯罪資料，進行模型的測試。由模擬結果顯示，本研究所提出的研究模型平均可達80%以上的預測正確率。此外，也揭露了許多網路犯罪黑數的變化，包括：再犯率及受害者的報案率等。透過本研究所提出的預測模型及模擬結果，能夠提供相關網路犯罪政策擬定前的測試，對於傳統犯罪理論也能進行補強，幫助瞭解及預防新興的網路犯罪行為。

關鍵字：網路犯罪、系統動態模擬、犯罪黑數、網路犯罪預測

A Cybercrime Simulation Model for Cyber Fraud and Offense Computer Usage Crime Prediction from System Dynamic Prediction

Chen-Shu Wang
Department of Information Management, Chung Hua University

Tien-Tsun Chung
Department of Technology Management, Chung Hua University

Abstract

The living quality of users has been improved by the convenience of Internet, such as the applications of online shopping and financial transaction are enable user to reduce their valuable time without counter transactions. However, such convenience usually accompanies with cybercrime concerns and users are suffering the risks of personal information leak. According to traditional crime theory, crime behavior is a dynamic systemically complex problem which is more than just a simple personal behavior. Various factors, such as networking security, government policy and their feedback influence, are all related with cybercrime which is a getting serious issue. Therefore, to realize core structure of cybercrime, a simulation model has been proposed in this research based on the methodology of system dynamics from attack and defense perspectives respectively. Finally, some simulation experiments are implemented by using actual criminal data of Taiwan from 1991 to 2007. As the simulation result demonstrated, the accurate prediction rate of the proposed model can be achieved to 80%. Additionally, particular dark cybercrime parameters, such as report rate, are revealed and some interesting patterns are also discovered. Furthermore, the simulation model can be regarded as a pilot-test for the implementation of actual crime-related policy. Finally, the simulation results can also be took into account for traditional crime theory refinement.

Key words : Cybercrime, system dynamics simulation, dark crime parameter, cybercrime prediction

壹、緒論

網際網路的快速發展改善了使用者生活上的便利性，舉凡線上財務金融應用（網路ATM及網路報稅）或是線上購物，使用者只需要輕按幾個滑鼠按鍵，就可以省下以往必需大排長龍的時間或是親自臨櫃辦理的麻煩。但是隨之而來的網路安全考量，也往往讓使用者對於網際網路所提供的方便性卻步，因為使用者可能需要在網路便利性與個人資訊外洩或是個人身份盜用間取得權衡（Wolak et al. 2008），例如：透過網路搜尋引擎的關鍵字搜尋，就有機會取得個人隱私資料（Hinduja 2008）。一般而言，提到網路犯罪（Cybercrime）就會與網路詐欺（Cyber fraud, CF）、智慧財產權侵犯（privacy of intellectual property rights）、網路援交（sexual offenses crime）等犯罪行為進行聯想。根據Brenner 與 Schwerha （2004）的定義，所謂網路犯罪係指犯罪行為為與過程必需透過網路通訊科技完成（Internet Communication Technique, ICT）。相較於傳統的犯罪行為，網路犯罪可以算是1994年才開始新興的犯罪型態。然而這種新興的網路犯罪行為卻更加難以偵辦，主要的原因在於網際網路的跨國便利性，往往讓犯罪證據追蹤不易而不易完整的收集（Wadlow & Gorelik 2006）。此外各個國家對於網路犯罪的規範多有落差，因此也不易取得跨國合作的共識。網路技術及相關電腦系統不斷更新，固然增加了新技術的成長優勢，然而某種程度而言，也提供了新的網路犯罪手法，讓犯罪者以相對便宜的價格取得更優良的犯罪工具，無形中提高了警調偵辦難度。

愈來愈多的電子化服務應用（e-service application）不斷的被開發，例如：金融活動（線上轉帳等）、電子化政府服務（網路報稅等）或是各種不同的電子化憑證（自然人憑證等），不難預期這樣的發展趨勢將深化使用者對於網路的依賴程度。瞭解網路犯罪問題的根本行為結構是極需解決且重要的研究問題。網路犯罪相關研究也是目前台灣司法單位極為重視的一環。然而，探討網路犯罪行為時不應侷限於網路犯罪者個人行為，因為網路犯罪行為其實涉及整個網路安全、政府政策等因素間交互回饋作用。目前已有相關研究透過傳統的統計模型進行網路犯罪模型的研究分析（林宜隆、黃讚松 民91）。不過因為網路犯罪問題的核心結構其實相當複雜，除了網路犯罪者（攻擊面）在犯行時可能考量多個面向，例如：相關罰則或是可能的犯罪獲利及犯行困難度外，而網路警察（防守面）在進行偵察時也有可能成為網路犯罪者的阻力，例如：偵察技術、偵防設備等。同時這些因素間又存在相互影響的回饋作用（Feedback），甚至是時間滯延（time delay）關係。舉例而言，警方（防守面）的偵察設備提升有助於提昇犯罪的難度（攻擊面），或是加重相關網路犯罪的罰則（防守面）也會嚇阻網路犯罪，然而這些政策面的施行往往需要要經過一段時間（time delay）的推行才能看到效果。因此，相較於傳統的網路犯罪研究，本研究認為網路犯罪問題是一個典型的系統動態複雜（System dynamic complex）問題，更適合以系統動態模擬的方式加以探討相關的網路犯行結構。不過目前甚少有相關研究採用系統動態學方式來相關網路犯罪議題。

網際網路本身具有以下之特性，包括：跨國性、分散性、開放性、互通性、隱匿

性、犯罪成本及障礙低、被害者不願聲張、犯罪時間極短且難以證明、證據不易獲得、偵查與追訴困難等，因此網路犯罪較傳統犯罪更增添許多偵查的困難度（Hinduja 2008）。際網網路資訊的流通已無法由任何單一國家或少數主機全面掌控。根據內政部警政署刑事警察局偵九隊的統計，在台灣地區目前的主要網路犯罪類型是線上遊戲虛擬寶物竊盜行為（屬於妨害電腦使用）、金融（網路）詐欺、利用網路散佈性交易訊息、網路色情或援交及侵害智慧財產權為最多。在半年間（民國97年1月到6月）相關於線上遊戲虛擬寶物竊盜行為和金融（網路）詐欺行為的犯行就佔所有網路犯罪的58%，而在妨礙電腦使用的犯行，其犯罪成長率由民國94年至民國97年期間就成長近1倍；相關於在網路詐欺的犯行，由民國89年至民國97年間則是平均成長了3倍。由上述的統計數據不難看出，幾乎所有的網路犯罪情形，都有日趨嚴重的趨勢。過去相關於網路犯罪的研究議題，大多是由政策制定者的角度出發，例如：探討如如何以政策面的法令制定以協助降低網路犯行為（王明禮、許慈健 民90），而在擬定相關於網路犯罪問題的因應對策，則多偏重在法律與技術層面 （林宜隆、邱士娟 民92），忽略對網路犯罪現象的描述。綜合而言，在探討網路犯罪相關議題時，仍缺乏全面的系統觀點。此外有許多的犯罪黑數也仍然難以推估。傳統的犯罪理論勢必需要加以修改才能更適切的應用於這個新興的犯罪類型—網路犯罪。

本研究採用系統動態模擬的觀點出發，由政策面、社會面、個人行為面探討網路犯罪行為的根本問題結構。基於結構影響行為的系統態基本假說，找出影響不同網路犯罪行為的結構因素，並探各因素間的交互回饋及時間滯延關係。本研究的研究目的包括：

一、分別由網路犯罪行為中的攻擊及防守的觀點出發，由過去文獻中找出影響網路犯罪問題的系統結構。

二、以系統動態模擬法進行實際塑模，再以台灣地區相關於妨害電腦使用及網路詐欺的實際網路犯罪資料進行模型正確性的驗證。

三、最後，將系統動態模型之模擬結果，提供網路犯罪各種參數的預測以及政策模擬；並可做為傳統犯罪理論修正的依據。

貳、文獻探討

依據內政部警政署刑事警察局之定義網路犯罪，係指：

（一）利用電腦特性遂行犯罪目的：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。

（二）行為與結果間之時間與空間的區隔：網路犯罪的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，犯行可能須經過一段時間後才遂其犯罪目的，或行為地與結果發生地有相當大之區隔。

（三）高犯罪黑數：網路犯罪因係犯行人利用電腦進行犯罪，在本質上即難以發現。因為大多牽涉個人主觀感受，加之此類犯罪偵查效率及追訴成效偏低，

網路犯罪具有相當高之犯罪黑數（內政部警政署刑事警察局 民95）。

由內政部警政署統計通報顯示，僅僅在民國97年1-6月半年間，而各項網路犯行的比率分佈如圖1所示，電腦網路犯罪發生數主要為詐欺案4,981件（占41.48％）為最多， 妨害電腦使用2,023件（占16.85％）次之，違反兒童及少年性交易防制條例1,871件（占15.58％）第三。而在網路詐欺案部份，就民國97年1-6月較上年同期增加296件（＋6.32％），破獲率增加17.26個百分點，另妨害電腦使用部份，主要係無故入侵電腦、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為。97年1-6月較上年同期減少1,682件（－45.40％）。

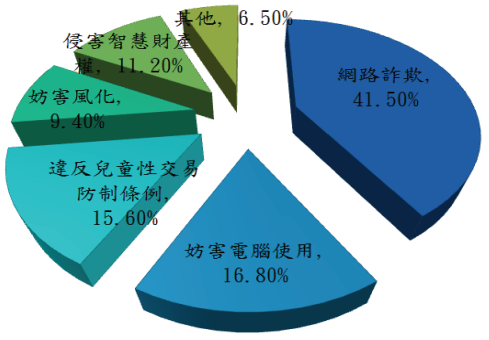


圖1：台灣地區民國97年1至6月間各項網路犯罪統計示意圖

（資料來源：本研究整理）

雖然由警政署的統計通報可以看出妨害電腦使用已有下降趨勢，但更為嚴重的是網路詐欺犯行卻不斷成長。網路交易愈來愈盛行的情形下，若網路詐欺持續惡化，而執法單位又無法有效壓制，將會造成民眾使用的恐懼也無助於目前各項電子化服務的發展。為了避免這一類情形發生，本研究旨在瞭解網路犯罪的趨勢與行為結構，並依模擬結果提出相關建議供執法單位參考。本研究將先就傳統犯罪理論進行彙整並簡介本研究所採用的系統動態學方法論。

一、犯罪理論與網路犯罪

早期的犯罪理論強調犯罪機率，而近年來的相關研究則重視犯罪情境及互動生態。有不少學者均提出相關的犯罪理論，其中犯罪機會理論（theory of criminal. opportunity）是強調機會是被害的核心，因為人類均潛藏著犯罪傾向，會不會犯罪姑取決於自我控制力量。此外Hirschi （1969）也提出了社會控制理論，Hirschi 認為當個人與社會的連結力變弱時，社會對其成員的約束力量變少，犯罪就可能因此產生。他提出四個連結要素：涉入或承諾（commitment）、參與（involvement）、信念（belief）以及依附（attachment）；與重要他人的依附連結如轉弱，則無異失去社會化的機會，會導致社會化不良（Hirschi 1969）。這些文獻主要都在探討人類犯罪的成因，但是目前顯少有相關研究投入虛擬世界中網路犯罪行為成因的探討，例如：社會控制理論中必需衡量個人與

真實環境和社會的關係。然而網路是一個虛擬平台，因此傳統的社會控製理論就需要一定程度的修改，才能更加貼近的應用於虛擬的網路犯罪分析（Stephens 2008）。

另外，像是Cohen與Felson也在1979年提出日常活動犯罪理論，提及犯罪是人們日常生活型態的一種結果，且犯罪事件要發生必須有三種要素（M-O-P）在時空的聚合：（1）有動機及能力的犯罪者（Motivation）、（2）合適的犯罪標的物（Object）及（3）抑制犯罪發生者的不在場（Protect）（Cohen & Felson 1979）。最後，像是Beck於1991年提出「風險社會」，認為現代的「風險」決非單純的技術性問題，它涉及了十分複雜的社會溝通與決策過程，不但社會的組織方式、發展階段與知識水準都對風險的型態和層次有決定性的作用（Beck 1991）。然而這些傳統的犯罪理論並未考量網路罪的特性，因此未必能完整的應用在網路犯罪的探討。舉例而言：在網路的虛擬社會中，人與人的連結是很難定義的（網路中甚至存在所謂的虛擬角色），因此若依照Hirschi的社會控制理論，將更難定義所謂的人與社會間的約束力，也更不用去討論所謂的控制力問題。傳統的犯罪理論絕對需要修正才能適用於這個新興的網路犯罪討論。

在國內亦有相關研究已開始注意網路犯罪的研究議題，例如：馬信行由自陳犯罪資料做為分析基礎，彙整出犯罪相關係數，結果顯出如果個體的社會化程度不良，則所需的資源就會愈貧乏，因此當無法用合法手段獲得且有適當的目標物出現時，當目標物的有力監督者不在場，且自認犯案後被偵破的機率愈低，則犯案的機率愈高（馬信行 民90）。另外，林宜隆等人針對網路犯罪議題，亦有一系列研究。林宜隆及黃讚松由網路使用特性觀點，探討網路犯罪的特性與預防，發現因為網路環境的設計不良形成易於犯罪情境，是主要導致網路虛擬社會中的犯罪的主因（林宜隆、黃讚松 民91）。而這也與Cohen & Felson的日常犯罪理論發現一致。此外，林宜隆及邱士娟就常見的網路犯罪型態進行個案分析，結果發現因為網路的普及讓犯罪隱形化，再加上民眾法治教育不足，使得輕「網路犯罪」慢慢轉向重「網路犯罪」的趨勢發展（林宜隆、邱士娟 民92），導致網路犯罪的發展日趨嚴重，這也與內政部所提供的統計數據一致。最後，林宜隆及楊鴻正則建議，對於網路犯罪這一類高科技的犯罪，除了必須有高科技的警察人員進行偵查外，數位鑑識設備也必需能夠加以配合，因此加強網路犯罪專責人員的人力素質及偵查能力和購置新的偵防設備絕對是必要且必然的趨勢（林宜隆、楊鴻正 民90）。此外，高聲凱認為對於電腦網路犯罪的偵查與預防，不單只是政府與警調責任，應規範電信業者配合偵查（高聲凱 民96）。

雖然，網際網路提供的是虛擬的交易平台，但是因為網際網路已經可以被視為最具傳播效率的傳輸媒介，因此在這樣的虛擬平台所發生的犯罪行為，其殺傷力抑不容小覷。例如：利用網路拍賣所包裝的網路詐騙犯罪，因為發生於虛擬平台的關係，犯罪者可以輕易的就加害多數不特定人，且不受時間與空間限制。因此，網路犯罪與傳統犯罪類型在有著其不同之特質。針對網路犯罪特性，高聲凱亦歸納出五點特性，包括：

（一）散佈迅速：網際網路有無遠弗屆、擴散迅速的特性，故影響層面極為廣泛。

（二）蒐證困難：網際網路犯罪的匿名的特性，讓證據不僅容易被造假。此外數位證據也容易銷毀，使得網際網路犯罪之證據蒐集愈發困難。

（三）全球性：網際網路的虛擬世界中並不存在國界的觀念，因此所謂的跨國合

作，也往往受限於各國法規，不易真正落實。

（四）偵查不易：綜合上述網際網路特性，使得檢警單位在偵查網際網路犯罪不易，甚至無法偵查。

（五）人性弱點：一般常為歹徒所利用的『貪婪』與『恐懼』兩項，雖然為網路上的虛擬角色，但仍為人類所扮演，也一樣存在於網路使用人的心態，使得歹徒有隙可乘（高聲凱 民96）。

綜合而言，網路犯罪除了繼承了傳統犯罪特性，包括了攻擊面與防守面的特色外（O'Hanlon 2006），但又演化出其犯行獨特性與高度的偵防難度。這一類新興的犯罪類型，犯罪手法日新月異，而且因為在網路虛擬世界裡，監督角色也就不易掌控相關犯行。隨著網路工具成長演進，犯行者就愈有能力隱藏其犯罪事實。網路犯罪是不容忽視的研究議題。

二、系統動態學

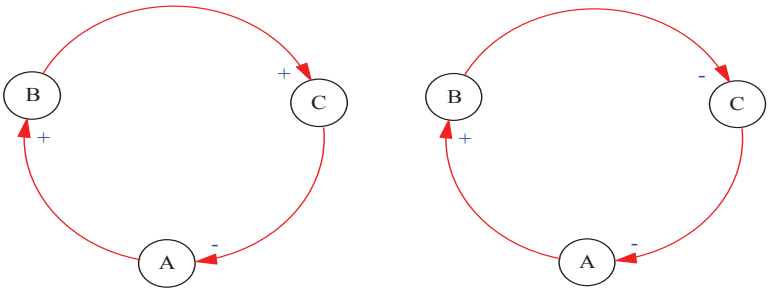
系統動態學（System Dynamics）是處理訊息回饋系統動態行為的一種方法論，係由Forrester於1961年（Forrester 1961）提出。Forrester認為人類所從事的每一種活動都涉及動態變化，因此若能明確描繪變化的軌跡，則可增進人們對自然及社會上所以有事物動態現象的認知與了解（Forrester 1971）。系統動態模擬方法對於複雜的動態、回饋且具時間滯延的問題，能提供整體、長期且較周延的解決方法。

因為大多數定量研究方法著重於單純的問題導向解決方式，但是可能因此失去完整的系統觀點而沒有真正觀察變項間互動的關係。此外像是迴歸分析與迴歸方程式的研究方法，主要是用過去的歷史資料做為分析的標的物，對外在環境變數的不可控制性也就無法控制，更遑論瞭解這些外生變數的影響過程。系統動態模擬方法能夠補足這方面的缺憾，使用電腦模擬實驗，可以驗證各變數之間關係，協助策略規劃、情境分析，並進行各種參數組合的模擬實驗，讓決策者在決策還未施行之前就能夠瞭解決策可能造成的結果，節省時間和成本。

電腦模擬已經逐漸成無法尋求最佳解決問題時的替代方案。事實上，模擬就是一種逐步求解（Step-by-Step Solution）的過程，操作上須將模式的型態逐步轉換為形成模擬模型（Simulation Model）。因此，透過模擬的技巧，可以處理系統現象或程序較複雜而無法以數學方程式進行解析的問題，亦可驗證複雜數學模式的效度，並使研究人員深入瞭解、觀察系統行為的變化。

系統動態學則是運用回饋系統，透因果回饋關係環路（Causal Feedback Loops）做為回饋系統之基礎。以因果關係（Causal Relationship）構成的系統動態學，係藉由因果關係來確認系統的問題，將複雜的問題以簡潔而系統化方式呈現。可以說，這樣的呈現方式，有助於問題的溝通與瞭解。圖2所呈現的即為典型的因果關係環路圖，係由兩個或兩個以上具有因果關係的變數，以因果鏈彼此連接而形成之封閉環路結構。任何因果回饋環路非正向（Positive）即負向（Negative）環路。圖2（A）表示的是正向環路，會產生自我強化的特性，進而發生背離目標的現象。而負向環路如圖2（B）所示，會產生自我

規律變動，最後達到穩定狀態。一個系統可能是由數個正向或負向回饋因果環路組合而成，因此系統整體行為可能會發生「穩定」、「成長」或「衰退」等不同的行為模式變化。系統本身的行為並無正負之分，目的在能明確掌握問題的重點，並提供簡單有效的方法對系統作分析判斷。



（A）負向回饋環路　　（B）正向回饋環路

圖2：因果回饋環路示意圖

由過去相關文獻可以發現，在以往相關於網路犯罪問題的研究，大多是採用問卷進行調查研究。這樣的調查方式往往會侷限於某個特定的時間點去呈現變數因果關係，並無法探就網路犯罪中的時間滯延以及犯罪成因間的系統回饋（Loop）成因。此外網路犯罪本身即為環環相扣的動態系統複雜問題，本研究即透過系統動態學來探討整個網路犯罪個人行為、政策方面、社會層面等問題的造成因素設為關鍵變數。並採用這些關鍵變數及其互動作用，進行模擬模型的結構塑模。透過模擬實驗試著將模型能與真實環境現象吻合，而預測模型及模擬結果將能夠提供相關網路犯罪政策擬定前的測試。對於傳統犯罪理論也能進行補強，幫助瞭解及預防新興的網路犯罪行為。

參、模型架構設計與假設

因為網路是一個虛擬的社會，具有分散性、開放性、互通性、隱密性及立即性等特性，也造成網路犯罪氾濫且防範與偵查均不易施行。根據資策會FIND/經濟部技術處「創新資訊應用研究計畫」統計（資策會 民97），台灣網路普及率已達到總人口的44%，隨著網路普及率提高，網路犯罪將日趨嚴重。網路犯罪是新興的網路犯罪型態，因此傳統犯罪理論必需進行調整，才能更完整地應用於虛擬社會結構。本研究植基於傳統犯罪理論並加入網際網路特性，就攻擊和防守二個行為面向，歸納出相關的決策變數（Decision Variable）後，並建構動態模擬模型。此外；本研究亦以政策執行面所關心的結果（例如：犯罪人數）做為模擬模型準確度的衡量變數（Evaluation Variable）並與內政部警政署所提供的犯罪資料進行模擬模型的預測正確性比對。最後，本研究提出了三個研究假說用以探討網路犯罪決策因素間的關係；能夠提供政策執行者對於網路犯罪行為結構有更完整的系統觀點。

根據內政部警政署97年第30號警政統計通報，僅就2008年1月到6月有關網路犯罪案類網路詐欺案（41.5%）、妨害電腦使用（16.8%）、違反兒童及少年性交易防制條例（15.6%）、一般妨害風化（9.4%）、侵害智慧財產權（11.2%）五類的總合為所有網路犯罪94.5%，且網路詐欺與妨害電腦使用兩種犯行就佔目前台灣網路犯罪58%，可見情形這一類的案件相關嚴重也目前警方偵查的重點。而這二類犯罪超過所有網路犯罪的一半，平均而言，二件網路犯罪行為中就有一件即為網路詐欺或妨害電腦使用，本研究即以這二類犯罪為例進行犯罪行為的模擬。

一、變數說明

網路犯罪是一種新興的犯罪型態，各國警調單位都難以估計其犯罪手法的演變速度。因為網路犯罪的犯行結構包括太多因素，例如：警察作為與法令作為、相關的駭客工具的演進及各種電腦作業系統漏洞等；而這些因素間又往往存在交互影響（feedback）。本研究分別由政策面與實際面進行探討，並依據傳統的犯罪理論整理出網路犯罪的結構決策變數如表1。

本研究除以網路詐欺及妨礙電腦使用二項罪行的統計數據做為模擬模型正確率的衡量指標外；另再犯率、報案率及不同罪行間的犯行轉換率也是本研究感興趣的衡量指標，例如：犯行者由罪罰較輕的妨礙電腦使用轉為犯行較重的網路詐欺、再犯罪流向比例及被害報案率等；透過模型建構、比對，觀察其參數之變化。

二、網路犯行偵防模型：因果循環圖與存量流量圖

本研究所採用的研究方法為動態系統模擬，系統動態學的觀念在於打破人類一貫的思考模式，是以全面性的觀點洞察問題背後的結構，因此需要充分瞭解整個環結並繪製因果關係。舉例而言，警調單位（防守面）在進行網路犯罪問題偵查時往往有許多的顧慮，例如：網路警察的素質、偵查設備、ISP業者配合度等因素，都會影響整個網路犯罪偵辦。在本研究所歸納出的決策變數表1中，可以分別由攻防觀點繪製因果循環圖（CLD）（如圖3所示），目的在能明確掌握問題的重點，並提供簡單有效的方法瞭解其相互關係之影響。

本研究分別就政策執行面實務觀點及犯罪組成因素探討網路犯罪變化，在政策執行面實務部份，本研究訪談相關警務組成人員，並瞭解相關網路犯行偵查運作模式後，加以繪製為網路犯行的防守面力量。而在犯罪組成因素部分，如表一所匯整之決策變數，本研究認為上網人口愈多就有愈多人受害者，當然也代表會有更多加害者，而這一部份又涉及到電腦價格與網路頻寬等相關問題，因為當電腦價格若趨近於平民價格時（犯罪成本），網路普及率自然就提高，在這種情形下我們相信加害人與被害人人數一定會持續成長，本研究將此視為網路犯行之攻擊面的力量。而在不斷與專家進行訪談修正後，本研究輔以蒐集的資料繪製出網路詐欺與妨害電腦使用之因果關係，做為塑模的依據。

另外，透過因果關係確認各變數間的關係，除了可將複雜的問題作較簡潔系統化的表示，也能夠界定系統動態模式的範圍。在圖3的因果循環圖，分別繪製可能影響網路

詐欺與妨害電腦使用犯行的變數。例如：在妨礙電腦使用方面，則加入了偵防設備使用技巧（Investigate equipment skill）及偵查能力（investigate ability）。而變數間也巧妙的存在著交互影響的回饋關係（feedback）。此外，在圖3的因果循環圖中，本研究也依實際狀況，加入了時間滯延因素的考量，例如：法律修正案（Law Amendment to offence computer usage）及預算採購偵防設備（Budget to Investigate Equipment）。

由於系統模擬模型建立後，必需透過模擬模型化過程，將各因素間之關係轉換成可程式化之數學模式，依據塑模的初始設定，清楚標示出動態系統之目標及各因素之間的相互關係，反應出實際運作狀況，作為政策修正及方案評估的依據。

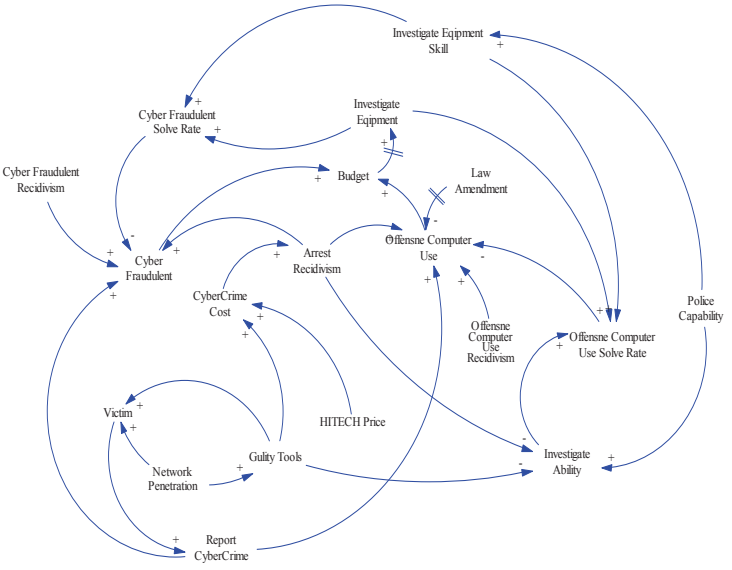


圖3：網路詐欺與妨害電腦使用犯罪模型之因果循環圖

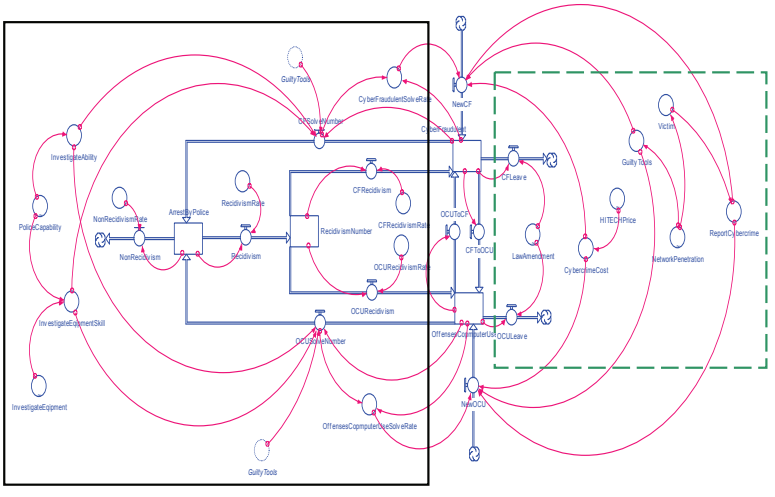


圖4：網路詐欺與妨害電腦使用罪行模型之存量流量圖

表1：決策變數與衡量指標

變數	說明	相關理論
犯罪工具	在網路犯罪中欲竊取他人資訊或入侵他人電腦，需要運算能力佳的個人電腦及具入侵意圖的軟體。換句話說，網路犯行需藉由ICT設備完成。	1.日常活動犯罪理論：動機（Motivation）相關（Cohen & Felson 1979） 2. 社會控制理論（Hirschi 1969）
破獲率	可視為抑制犯罪的力量，犯行者會將警方破獲率視為是犯行的阻力。	日常活動犯罪理論：抑制（Protect）相關（Cohen & Felson 1979）
犯罪成本	犯罪工具取得愈困難，相對的犯罪比重自然就比較少。網路犯罪的主要犯罪工具是資訊設備（3C產品），當其價格愈趨近平民化，便讓欲犯罪人更有機會，因此資訊產品價格可視為網路犯行的主要犯罪成本之一。	1.日常活動犯罪理論：標的物（Objective）相關（Cohen & Felson 1979）
網路普及率	網際網路為網路犯罪的主要媒介平台，因此隨著網路普及率愈高，相關的電子化加值服務及應用也將隨之普及，可以預期網路犯行將隨之增加。	1. 風險社會 （Beck 1991） 2. 林宜隆及黃讚松（民91）
法令罰則宣導	除了警調偵防外，目前政府立法部門著手相關法令之修正。但法令之修正最主要乃是透過宣導手段使民眾瞭解網路犯罪之相關規範；更能抑制網路犯行的成長。	1. 社會控制理論（Hirschi 1969） 2. 高聲凱（民96） 3. 林宜隆及邱士娟（民92）
偵查設備	網路犯罪的偵察與搜證不易，因此特殊的軟硬體設施，將有助於犯行的偵破。	1. 日常活動犯罪理論：抑制（Protect）相關（ Cohen & Felson 1979） 2. 高聲凱（民96） 3. 林宜隆及楊鴻正（民90）
警察素質	網路犯罪有別於傳統犯罪方式，其隱身於虛擬世界中，在偵查上需要相當程度的電腦knowhow，並非一般傳統辦案手法可以勝任。	1. 日常活動犯罪理論：抑制（Protect）相關（ Cohen & Felson 1979） 2. 高聲凱 （民96） 3. 林宜隆及楊鴻正（民90）
偵查人員派遣及技巧	在網路犯罪其偵辦技巧，需要對網路基本架構及其運作模式相當程度的瞭解，選派任人員則應考慮其資訊背景，否則恐造成偵辦案件品質低落。	1. 日常活動犯罪理論：抑制（Protect）相關（ Cohen & Felson 1979） 2. 高聲凱（民96） 3. 林宜隆及楊鴻正（民90）
衡量指標		
變數	說明	
網路詐欺(CF)與妨害電腦使用(OCU)	利用內政部警政署刑事警察局提供2000年至2008年網路犯罪資料來驗證本研究模型之正確性與相似度。	
再犯率	任何犯行成功而尚未被查獲犯行人，存在二種選擇： （1）良心發現害怕而不再犯罪，或是（2）從犯行中獲取好處後，持續不斷再犯到被查獲。再犯率是重要的政策面衡量指標，不過往往難以估算。	
報案率	目前所統計的數據係被害人向警方報案後所得的資訊，然而基於下列3項原因，被害人可能跟本沒有報案： （1）被害人根本不知有犯罪發生。（2）被害人擔心可能遭到報復或難堪而不敢提出告訴。（3）警察機關吃案。（4）損失金額太少而不願意報案。因此，真正的網路犯罪嚴重性難以正確的估算也無法得知（Dallaway 2007）。	
犯行轉換率	類似犯罪型態往往有著合併發生的可能，所以犯罪類型間流通關係並無法利用統計方式來正確估算。	

本研究透過模擬軟體Ithink（r）公司所發的Stella動態動系統模擬軟體將因果循環體轉換為存量流量圖（SFD）（如圖4所示）。其中；除了將本研究所關心的決策變數分列為網路犯罪防守面（圖4中以黑色實線方框表示）以及攻擊面（圖4中以綠色虛線方框表示）。在防守面則包括了：警方偵防能力、破獲率等變數；而在攻擊面則包括了像是：網路普及率、犯罪工具等變數；其中許多變數存在著相互影響的回饋關係，例如：ICT設備價格與犯行攻擊面呈負相關（價格愈低則犯罪機會成本變低導致犯行增加）；但是也會讓警方偵查能力提升而增加犯行破獲率，讓潛在犯行者減少犯意。在圖4的模擬模型中，本研究也將衡量指標分別設定為存量以及流量，包括了：網路詐欺及妨害電腦使用罪行（存量）、再犯率以及犯行轉換率（流量）。因為這二種罪行會因為犯罪者犯案而增加又新政策執行與執法人員破案產生壓制效果進而影響犯罪行為減少，這樣的增減現象類似於系統動態模擬中的存量概念，故本研究以存量量化上述二犯罪指標後，再與真實數據比對做為評估模型之依據。而再犯率及犯行流通率為影響前述二種犯行之存量比率，犯罪者有可能再犯又成為攻擊的力量，但並非所有的罪犯都會再犯，是以用流率表示，代表流入的再犯人口數。

三、研究假說

為了探討圖4網路犯罪模擬模型中決策變數與衡量指標間的相關性；參酌過去相關文獻與相關警調單位的訪談資訊，本研究提出相關3項研究假說。

（一）台灣的警力的主要來源是由台灣警察專科學校與中央警察大學畢業生為主力。然而，目前在台灣地區僅有中央警察大學設立了資訊相關科系能夠培養網路犯罪偵防人才，因此能夠培養的人員相當有限（一年僅不到20人），且相關人員在結訓畢業後，未必能夠從事網路犯罪偵查工作（分發關係），故相關人員素質短缺，對於網路犯行的防守面有相當大的衝擊，本研究提出假說1（H1）如下：

假說1（H1）：警察人員素質的提昇對破獲率是有正向影響，人員的補實與加強相關教育對偵防有正面實質提昇效果。

（二）此外，根據資策會FIND/經濟部技術處「創新資訊應用研究計畫」統計，2008年第2季台灣經常上網人口為1,014萬人，網際網路連網應用普及率為44%，因為網路虛擬世界為網路犯罪的主要發生地點，也是完成網路犯罪不可或缺的工具，因此本研究提出假說2（H2）如下：

假說2（H2）：網路經常上網人口及網路連網應用普及率和網路犯罪成正向相關。

（三）最後，跟據與相關警調單位訪談後，受訪者表示，大部份的犯行者大多由犯行較輕的妨礙電腦使用（例如：身份假造或是偷竊帳號/密碼）轉變為犯行較重的網路詐欺（例如：線上遊戲寶物偷竊）。然而，大部份的犯行者無法判別罪行的輕重，因此本研究認為相關法律政策的宣導與網路犯行呈負向相關。不過，與所有的廣告效果相似，這樣的宣傳效果本研究也預期至少需要

一段時間的滯延（Delay）才能開始產生影響，因此本研究提出假說3（H3）：

假說3（H3）：刑法修正案的宣導效果，與網路犯行呈負向相關。

肆、研究結果分析

本研究以系統動態學進行網路犯罪模型建構模式後，並以台灣地區實際的網路犯罪資料進行模型準確度測試。考量主要的網路犯行，本研究針對網路犯罪行為中之網路詐欺（Cyber Fraud, CF）與妨害電腦使用（Offend Computer Usage, OCU）二種犯罪類型進行探討（佔網路犯行的58%）。

一、妨礙電腦使用（OCU）部分

圖5所示為妨礙電腦使用犯行的模擬結果，其中圖5的編號2實線為實際犯行的統計總件數而編號1實線代表模擬結果。可以發現，妨害電腦使用犯行呈現下降的趨勢，而本研究的模擬結果亦展示出相似的結果，正確率達90.12%。本研究發現OCU罪行之所以下降的主要原因在於其犯罪人口流向犯行更重的網路詐欺（模擬結果為15%），網路詐欺流向妨礙電腦使用的比率卻明顯較低（模擬結果為6%），就警政署統計通報，也明顯載明妨害電腦使用大部份為係為網路遊戲盜寶行為或是網路惡作劇。本研究研判應為未成年人對法律知識不足，因此不解自己的行為可能觸法，當相關法律修正案在大眾傳播媒體的宣導後（電視新聞或報章雜誌），開始驚覺這類的行為須加以控制，遂停止相關犯行。然而，根據模擬結果，仍然顯示顯示犯罪人口有轉移至犯行較重的傾向（約為2.5倍），另外模擬結果亦呈現OCU的再犯率有16%回流；這些參數在以往均為犯罪黑數（Dark parameter）難以得知，而透過本研究的模擬結果可供參考。

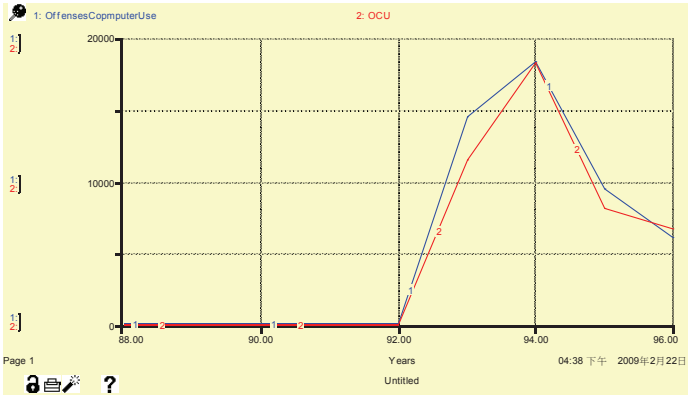


圖5：妨害電腦使用比較

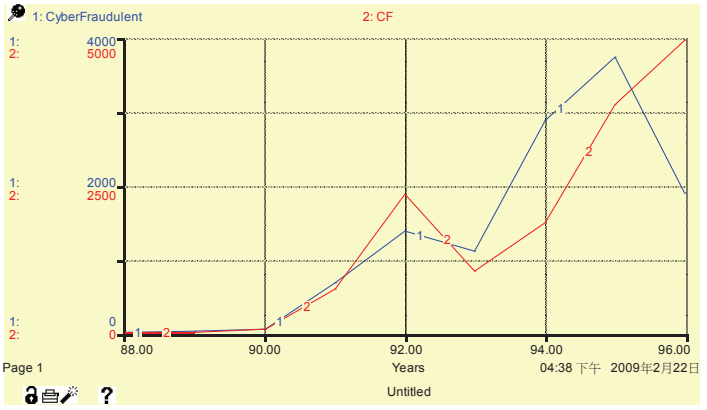


圖6：網路詐欺比較

二、網路詐欺（CF）部分

圖6所示為網路詐欺犯行的模擬結果，其中編號2實線為實際值而編號1實線代表模擬結果。可以發現，網路詐欺犯行日趨嚴重，發生案件數也是呈現指數成長的現象；而本研究的模擬除民國96年呈現不同趨勢外，其餘模擬結果均呈吻合於實際犯罪數數，整體正確率達70%。

本研究發現CF罪行呈現指數成長的主要原因在於網路詐欺的再罪率達24%，推估CF犯罪有其犯罪誘因（犯罪獲利平均而言高與OCU犯行），因此雖然執法部門投入大量人力防制，但網路詐欺仍年年成長，還看不到有任何緩和趨勢，值得政策部門思考方面（如表2所示）。

表2：犯罪黑數模擬結果

犯罪黑數	參數值
報案數	20%
犯行轉換（OCU TO CF）	15%
犯行轉換（CF TO OCU）	6%
再犯率	30% （CF 為24% , OCU 為6%）

三、網路詐騙與妨害電腦使用關鏈性及犯罪黑數

根據所建立之模型，本研究首先進行基本的犯罪預測模擬建立，並且測試幾組極端參數值進行敏感度分析。再根據基本的模擬結果對模式進行微調。基本模擬結果顯示，本研究的模式大致能符合現實上網路詐欺及妨害電腦使用這二種犯罪行為之逐年犯行總件數。綜合而言，本研究所提出的網路犯罪模擬模型正確率平均可達80%；此外CF與OCU二種網路犯罪型態亦存在共同的特性，也是值得注意與探討。

（一）網路犯罪部份：

1. 犯罪工具部份：駭客與入侵軟體愈來愈容易透過網路取得，根據日常活動 犯罪理論，幾乎任何人都有能力成為潛在犯行者。特別是在網路的虛擬環境下，看似不存在監督者，因此自我控制能力不良的潛在犯行人，就更有可能成為犯罪者。
2. 報案率：傳統犯罪與網路犯罪均存在所謂的犯罪黑數，如妨害電腦使用大部份屬於線上遊戲帳號被盜問題，而這一類案件通常報案率並不高。根據本研究的模擬顯示，這二類案件的犯罪報案率來說僅20%，推估背後隱藏著更可怕的犯罪真實數據。

（二）警察作為部分：

1. 警察人員與素質：在許多過去的犯罪文獻中都曾提及「良好的警察人員素質與辦案人員數的增加，能夠有效提升偵查犯罪行為」，而這也正好與本研究的研究假說1（H1）相符並得到驗證。
2. 偵查設備：網路犯罪屬智慧型科技犯罪，利用傳統儀器與方法難以進行偵查，由模擬結果顯示加入新型的網路偵查設備變數，能夠讓模擬的準確度大大的提升，因此假說2（H2）也在本研究中得驗證。不過偵查設備屬的操作仍需專業知識配合，因此偵防人員的能力（H1）仍然左右偵查設備的執行效果。
3. 法律政策修正案的宣導效果：最後，本研究的模擬結果亦顯示，法律政策的規範的宣導效果能夠大大的改善模擬的準確度，因此假說3（H3）也在本研究中得到驗證。不過，就像所有的廣告效果一樣，模擬結果顯示法律修正案的宣導至少要在時間滯延一年後才能得到預期的犯罪抑制效果。

另外，由模擬結果發現，網路詐欺與妨害電腦使用之間存在特殊關聯性，二種犯罪型態的犯罪人有流通現象（網路詐欺流向妨害電腦使用6%、妨害電腦使用流向網路詐欺15%），不過較令人擔憂的是犯罪人流向犯罪型態較重的網路詐欺竟然為流向妨害電腦使用的2.5倍。另外，就警政署統計資料顯示，妨害電腦使用確為每年下降的趨勢，而網路詐欺則為成長速度相當的快，這樣的現象值得注意其後續發展。

值得一提是，傳統犯罪黑數問題，在網路犯罪亦有相同情形，其嚴重性更甚傳統犯罪，由本研究的模擬結果顯示，網路犯罪的被害人報案率僅有20%；換句話說，也就是還有80%的被害人未報案（也就是還有4倍的潛在被害人存在）。推估這其中除了個人認知價值觀外（可能認為損失金額太小），更令人憂心的是犯罪進行甚至在被害人不知不覺下進行（被害人跟本不知道自己已成為被害人）。雖然檢調與政府相關部門一再宣導民眾勿隨便開啟信件或加裝防毒軟體等，減少被置入木馬病毒的可能性，但網路使用者的層次不一，無法自行救助的情形下，網路犯罪不斷的惡化發展成為需要嚴密觀察的問題。

伍、結論與未來方向

對於日漸氾濫的網路犯罪行為，各國均成立專門小組因應，但網路犯罪成因，並非一味的壓制即可解決，要有效抑制網路犯罪必需找出根本原因。網路犯罪所涉及層面太廣，因此本研究利用系統動態學並參酌傳統的犯罪學理論，建構出全面的網路犯罪行為結構後，再以網路詐欺及妨害電腦使用二項網路犯行的真實資料進行模擬。而本研究所提出的模擬模型平均可達80%以上的模擬正確率，並由模擬結果中推估出許多以往不易衡量的犯罪黑數，包括了：再犯率（CF為24%,OCU為6%）、受害人報案率（20%）、犯行轉換率（OCU TO CF為16%、CF TO OCU為 6%）等參數，都可供政府單位在進行政策擬定時的參考依據。此外，由三項研究假說的驗證，本研究建議：

一、網路警察的素質確實影響案件的偵查能力與進度

台灣地區在民國88年於刑事警察局成立偵九隊專門負責網路犯罪之偵查，不過偵查人力還是有限；此外有鑑於網路犯罪日趨嚴重，各縣市警察也陸續成立了網路犯罪偵查小組，。不過，因為這些臨時成立的團隊成員不一定都是受過專業訓練人員，且受限於網路犯罪的偵仿設備有限，因此偵查效果不一定能夠達到預期（往往還是需要依賴刑事警察局偵九隊之協助）。本研究建議可以加以改善員警的網路犯罪偵防能力以及新型態設備的添購與操做訓練等，提升防守面的抑制力量。

二、法律的規範的宣導確實可以達到不錯的犯罪抑制效果

網路行為的規範與社會行為一樣需要可供大眾遵行的準則，相對的政府的立法單位也必須依照時勢對於各項網路規範進行調整，才不致於造成法律漏洞。本研究模擬結果顯示，二種犯行（CF和OCU）的再犯率高達30%，而這些再犯罪人口對於警察或政策方面會更小心應對（再犯行者更有經驗），甚至對於自己遭執法人員查獲之經驗可能分享給於其他犯罪者，造成執法人員日後更難以偵查。所以對於這些使用高科技犯罪之人，執法單位應適時建檔列管，以防止這些人再犯罪，或是訂定獎勵政策化敵為友，將其運用於輔助執法單位偵查。

三、專業人員培育及訓練

本研究的模擬結果發現高科技資訊偵防設備操作能力與偵查人員能力呈正向關係，這與國內外相關研究的發現一致。提昇偵防人員的技巧與能力有利於提高偵查效率。然而在與警政人員訪談過程中得知，由警察大學所訓練的相關資訊執法員警，大部份並未從事網路犯罪偵防工作。因此本研究建議，針對網路犯罪除了成立專責小組外，應以小組成員的素質做為選擇依據（專才專用），定時加強專業能力訓練與交流，藉以充分發揮偵查整體力量。

四、法律修正案仍需補強且要充份的宣導

民國92年6月刑法修正第三十六章針對妨害電腦使用罪有所規範，但網路犯罪仍然居高不下，可見相關法令與政府政策仍須增修，以符合時勢。例如，垃圾郵件與郵件廣告信通常為夾帶電腦病毒與木馬程式的原兇，因此除了規範寄件者行為外，針對ISP業者也應規範之過濾責任，可以要求ISP業者負連帶刑責，進行相關法令修正。

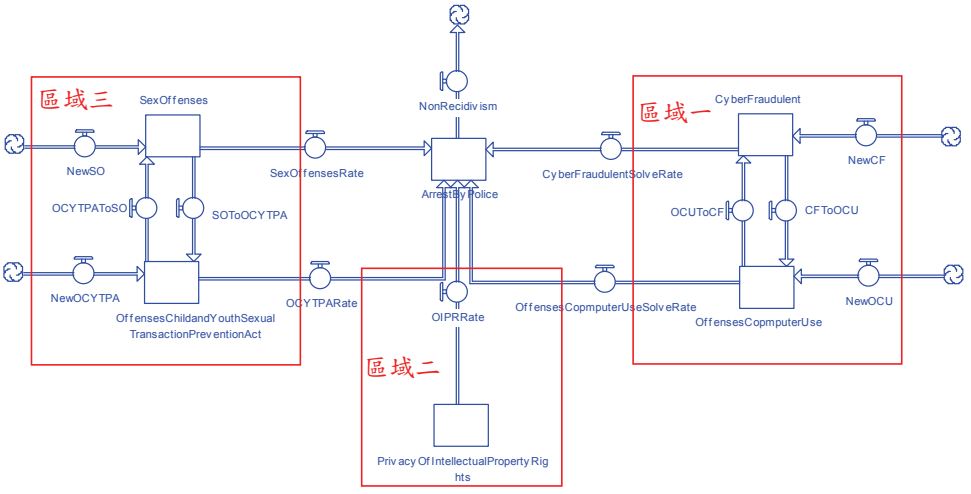


圖7：未來研究方向示意圖：整合網路犯罪結構行為

本研究僅針對二個台灣網路犯罪較為嚴重之類型模擬，但還是無完整解釋整體網路犯罪結構，為此本研究依據內政部警政署犯罪97年1到6月份的統計將妨害風化、侵害智慧財產權等二項犯罪型態再列為未來研究方向如圖7所示，以期未來能夠更完整瞭解網路犯罪各類犯罪之特殊關聯。在圖7中，區域一所示為本研究已完成之CF及OCU部份，而在區域二所呈現的即相關於智慧財產權侵犯的網路犯行的探討。台灣地區的盜版使用情況一直以來相當嚴重，甚至曾被美國列為特別301觀察名單。雖然政府長期投入保護智慧財產權，然而統計結果顯示智慧財產權的犯行目前仍佔所有網路犯罪的11%，比例相當高，所以這一部份仍值得做為日後探討的方向。最後，在圖7中的區域一即為網路色情犯行的探討，大多數情色網站均會置入木馬，若進入觀看則會在使用者不知覺下成為被害人。網路色情犯行類似於傳統妨害風化型態，不過更有甚者，透過網路平台跨越時間和空間限制而快速傳播，使得這一類的犯罪更加不易監控，更是未來值得探討的一個環節。另外，本研究目前是以傳統犯罪行為的攻擊與防守的觀點進行網路犯罪的系統動態模型的建構，然而在網路犯罪中的攻擊面裡，引誘犯罪的誘因如:電子化應用所帶來的便利性，抑是重要的研究構面。若能續持利用系統動態學建構出與真實環境相符立模型，全面解釋網路犯罪各犯罪型態的關聯，也是本研究未來努力的方向。網路本身就屬一個模擬社群，任何社會相關的集結與串連行為亦可能在網路上發生，為探討網路的特性，本研究擬將社會網路分析方法加入未來研究方向，更全面探討網路犯罪行為。

參考文獻

1. 王明禮、許慈健，民90，網路犯罪偵查與我國網路服務提供者協助偵查法制之研究，國立交通大學管理學院科技法律組碩士論文。
2. 林宜隆、楊鴻正，民90，『網路交易犯罪之偵查要領—以網路詐欺犯罪為例』，Journal of Information, Technology and Society，創刊號：135～151頁。
3. 林宜隆、黃讚松，民91，『網路使用問題分析與犯罪預防之探討』，Journal of Information, Technology and Society，第二卷．第二期：95～114頁。
4. 林宜隆、邱士娟，民92，『我國網路犯罪案例現況分析』，Journal of Information, Technology and Society，第三卷．第二期：73～88頁。
5. 馬信行，民90，『犯罪理論之統合分析-以自陳犯罪之研究報告為樣本』，教育與社會研究，第二期：35～66頁。
6. 高聲凱，民96，『電腦網路犯罪之防制 2008網際網路趨勢研討會』，第七十三期。
7. 資訊工業策進會，民97，2008年6月底止台灣上網人口（available online at http://www.find.org.tw/find/home.aspx?page=many&id=205），創新資訊應用研究計畫。
8. 內政部警政署刑事警察局，民95，非傳統類型犯罪之預防第三章，（available online at http://www.cib.gov.tw/crime/Crime_Book_Content.aspx?chapter_id=0000007&rule_id=0000003）
9. 內政部警政署97年第30號警政統計通報，（available online at http://www.npa.gov.tw/NPAGip/wSite/ct?xItem=41587&ctNode=11393&mp=1）
10. Beck, U. “Der Konflikt der zwei Modernen, in: demselben: Politik in der Risikogesellschaft,” *Frankfurt/M*, 1991, pp. 180-195.
11. Brenner, S. and Schwerha IV, J. “Introduction-Cybercrime: A Note on International Issues,” *Information Systems Frontiers* (6:2), 2004, pp. 111-114.
12. Cymru, T. “Cybercrime-An Epidemic,” *ACM Queue* (9:4), 2006, pp. 25-28.
13. Cohen, L.E. and Felson, M. “Social Change and Crime Rate Trends: A Routine Activity Approach,” *American Sociological Review* (44), 1979, pp.588-608.
14. Dallaway, E. “Cybercrime unreported due to reputation risks,” *InfoSecuirty* (4:4), 2007, pp. 11.
15. Forrester, J.W. “Industrial Dynamics,” *Cambridge MIT Press*, 1961.
16. Forrester, J. W. “World Dynamics,” *Wright-Allen Press*, 1971.
17. Hirschi, T. “Causes of Delinquency,” *Berkeley: University of California Press*, 1969.
18. Hinduja, S., “Deindivididuation and Internet Software Piracy,” *CyberPsychology & Behavior*, Vol. 11, No. 4, 2008, 391-398.
19. O'Hanlon, C., “The Criminal Mind,” *ACM Queue*, Vol. 9, No. 4, 2006, 7.
20. Stephens, G., “Cybercrime in the Year 2005,” *The Futurist*, 2008, 32-36.
21. Wadlow, T., and Gorelik, V., “The Making of a Cybercriminal,” *ACM Queue*, Vol. 9, No. 4, 2006, 25-28.

22. Wolak, J.D., J., Finkelhor, D., and Mitchell, K., "Is Talking Online to Unknown People Always Risky? Distinguishing Online Interaction Styles in a National Sample of Youth Internet Users," *CyberPsychology & Behavior*, Vol. 11, No. 3, 2008, 340-343.

附錄、犯罪模型變數與公式

ArrestByPolice(t) = ArrestByPolice(t - dt) + (OCUSolveNumber + CFSolveNumber - Recidivism - NonRecidivism) * dt
INIT ArrestByPolice = 0
INFLOWS:
- OCUSolveNumber = ((InvestigateAbility*InvestigateEqipmentSkill)/(GuiltyTools))*(OffensesCopmputerUse)
- CFSolveNumber = ((InvestigateAbility*InvestigateEqipmentSkill*3)/(GuiltyTools*0.3))*CyberFraudulent

OUTFLOWS:
- Recidivism = ArrestByPolice*RecidivismRate
- NonRecidivism = ArrestByPolice*NonRecidivismRate

CyberFraudulent(t) = CyberFraudulent(t - dt) + (NewCF + OCUToCF + CFRecidivism - CFSolveNumber - CFToOCU - CFLeave) * dt
INIT CyberFraudulent = 1
INFLOWS:
- NewCF = ((CybercrimeCost*GuiltyTools/DELAY3(CyberFraudulentSolveRate,1))*(ReportCybercrime*0.025))
- OCUToCF = if(time>91)then(OffensesCopmputerUse*0.15)else(0)
- CFRecidivism = DELAY3(RecidivismNumber*CFRecidivismRate , 1)

OUTFLOWS:
- CFSolveNumber = ((InvestigateAbility*InvestigateEqipmentSkill*3)/(GuiltyTools*0.3))*CyberFraudulent
- CFToOCU = if(time>91)then(CyberFraudulent*0.06)else(0)
- CFLeave = (CyberFraudulent*LawAmendment)*0.1

OffensesCopmputerUse(t) = OffensesCopmputerUse(t - dt) + (CFToOCU + NewOCU + OCURecidivism - OCUToCF - OCUSolveNumber - OCULeave) * dt
INIT OffensesCopmputerUse = 1
INFLOWS:
- CFToOCU = if(time>91)then(CyberFraudulent*0.06)else(0)
- NewOCU = if(time>91)then((ReportCybercrime*0.15)*(CybercrimeCost*GuiltyTools/(OffensesCopmputerUseSolveRate)))else(0)
- OCURecidivism = DELAY3(RecidivismNumber*OCURecidivismRate , 1)

OUTFLOWS:
- OCUToCF = if(time>91)then(OffensesCopmputerUse*0.15)else(0)
- OCUSolveNumber = ((InvestigateAbility*InvestigateEqipmentSkill)/(GuiltyTools))*(OffensesCopmputerUse)
- OCULeave = OffensesCopmputerUse*LawAmendment

RecidivismNumber(t) = RecidivismNumber(t - dt) + (Recidivism - CFRecidivism - OCURecidivism) * dt
INIT RecidivismNumber = 0
INFLOWS:
Recidivism = ArrestByPpolice*RecidivismRate
OUTFLOWS:
CFRecidivism = DELAY3(RecidivismNumber*CFRecidivismRate , 1)
OCURecidivism = DELAY3(RecidivismNumber*OCURecidivismRate , 1)

CFRecidivismRate = 0.8
CybercrimeCost = 100000/HITECHPrice
CyberFraudulentSolveRate = CFSolveNumber/CyberFraudulent
GuiltyTools = IF(Time>89) THEN (NetworkPenetration*15) else (NetworkPenetration*1.5)
InvestigateAbility = PoliceCapability
InvestigateEqipmentSkill = InvestigateEqipment*PoliceCapability
NonRecidivismRate = 0.9
OCURecidivismRate = 0.2
OffensesCopmputerUseSolveRate = OCUSolveNumber/OffensesCopmputerUse
RecidivismRate = 0.1
ReportCybercrime = Victim*0.2
Victim = (NetworkPenetration*2.3e+007)*5e-005
CF = GRAPH(TIME)
(88.0, 4.00), (89.0, 14.0), (90.0, 59.0), (91.0, 738), (92.0, 2361), (93.0, 1055), (94.0, 1873), (95.0, 3868), (96.0, 4967)
HITECHPrice = GRAPH(TIME)
(88.0, 70000), (89.0, 65000), (90.0, 55000), (91.0, 52000), (92.0, 40000), (93.0, 35000), (94.0, 30000), (95.0, 25000), (96.0, 20000)
InvestigateEqipment = GRAPH(TIME)
(88.0, 0.1), (89.0, 0.1), (90.0, 0.4), (91.0, 0.45), (92.0, 0.5), (93.0, 0.5), (94.0, 0.6), (95.0, 0.75), (96.0, 0.75)
LawAmendment = GRAPH(TIME)
(88.0, 0.00), (89.0, 0.00), (90.0, 0.00), (91.0, 0.00), (92.0, 0.00), (93.0, 0.1), (94.0, 0.6), (95.0, 0.7), (96.0, 0.7)
NetworkPenetration = GRAPH(TIME)
(88.0, 0.22), (89.0, 0.28), (90.0, 0.35), (91.0, 0.38), (92.0, 0.39), (93.0, 0.4), (94.0, 0.42), (95.0, 0.43), (96.0, 0.44)
OCU = GRAPH(TIME)
(88.0, 0.00), (89.0, 0.00), (90.0, 0.00), (91.0, 0.00), (92.0, 0.00), (93.0, 11452), (94.0, 18298), (95.0, 8108), (96.0, 6677)
PoliceCapability = GRAPH(TIME)
(88.0, 0.1), (89.0, 0.1), (90.0, 0.4), (91.0, 0.4), (92.0, 0.4), (93.0, 0.6), (94.0, 0.75), (95.0, 0.8), (96.0, 0.8)