以BDI代理人架構為基礎之虛擬社群群體犯罪預防研究[1]

苑守慈
國立政治大學資訊管理學系

莊竣丞
國立政治大學資訊管理學系

摘要

網路群體犯罪不同於組織犯罪般有結構的犯罪團體，亦非為了追求共同利益而合作的共犯夥伴，而是網路使用者自發性互動行為下逐漸浮現的群體近似犯罪行為。此現象普遍存在於當今各式各樣的網際網路社群，且以各種不同的樣貌與形式展現。本論文以差別接觸理論與社會學習理論為基礎，運用理論相關的元素與概念，以BDI代理人模式為方法來設計網路群體犯罪之模擬模式，透過動態模擬群體犯罪在不同條件下展現不同之面貌。更運用網路科學概念與分析方法，來分析犯罪關係網絡之特性，本研究藉由控制網路社群之使用者人數與初始犯罪率來觀察不同組合之下所演化的網路結構差異，並從四個衡量指標（犯罪技能平均數、群聚係數、前10%使用者平均連結度、連結度小於10之比率）來標示演化之網路結構的特徵，並觀察這些因素對網路虛擬社群群體犯罪的關連影響。研究結果預期將對虛擬社群群體經營者對於社群中群體犯罪之預防與有效管理將有所貢獻。

關鍵字：網路群體犯罪、BDI代理人架構、差別接觸理論、社會學習理論、網路科學

[1] 致謝：感謝國科會專題研究計畫97-2410-H-004-129之經費贊助。

A Study on BDI-based Collective Crime Prevention in Virtual Communities

Soe-Tsyr Yuan
Department of Management Information Systems, National Cheng-Chi University

Jyun-Cheng Jhuang
Department of Management Information Systems, National Cheng-Chi University

Abstract

Collective crime is an emerging phenomenon along with collective intelligence soaring in recent years. In this paper, the notion of collective crime is regarded as a form of universally distributed crime originated from spontaneous interactions among online community users. The issues that collective crime addresses focus on deviant or criminal behavior existing in common groups or crowds rather than traditional topics at computer crime or cybercrime. In this research, we use the theories, "Differential Association" and "Social Learning", to form the conceptual foundation of the collective crime phenomena and model the dynamics of virtual communities with the BDI-based multi-agent approach to simulate the community social networks. Prevention of collective crime is then regarded as an evolving network function based on the micro level of function simulation and the macro level of network analysis with two controllable variables (initial crime rate and network size) and four indicators (average amount of crime skills, average cluster coefficient, average degree of top 10% users, and rate of users with degrees smaller than 10). Our research findings are believed to contribute to the prevention management of collective crime in virtual communities.

Key words: Collective Crime, BDI Architecture, Theory of Differential Association, Theory of Social Learning, Network Science

壹、緒論

網路無國界與匿名性的特點一直已來為網路社會帶來著作權爭議的問題，以一九九九年掀起熱潮的Napster為例，該公司之中央伺服器負責管理並組織所有使用者的檔案索引與網路位置，使用者透過Napster連上網路之後，可搜尋並相互交換MP3音樂。不久便遭致美國唱片工業協會（Recording Industry Association of America）以「輔助及代理著作權侵害」為由對Napster提出著作權侵害之控訴，最後法院認定Napster明知特定侵權檔案為有著作權之音樂著作，而未能有效監督或防止其散佈，且該公司從中直接獲得經濟利益，故必須負起著作權代理侵害之責任。

於2004年O'Reilly Media的Dale Dougherly與MediaLive的Craig Cline在共同合作的腦力激盪會議上提出Web2.0的概念，徹底翻新網際網路事業經營哲學。Web2.0之核心概念為互動與分享，網際網路內容的豐富度與價值取決於使用者願意主動分享資訊並和其他使用者互動的程度，因此網路事業經營者開始致力於思考如何誘發使用者在社群中主動分享並與其他使用者互動，以創造更具價值的社群網絡，換言之，Web2.0社群具備需求面之網路外部性，越多使用者參與，個別使用者可獲得的效用越大。許多著名的網站，如Google、Myspace、Youtube、Wiki、flickr、Kinkedin等均充分運用Web2.0核心概念吸引為數相當可觀之使用者。然而，Web2.0出現之後，為網路的社會型態帶來重大的衝擊與改變，同時使用者頻繁的互動與分享行為使得著作權侵害問題更為嚴重，相較於Napster使用者下載音樂檔案，Web2.0網路社群的使用者行為更為複雜且多樣化。

Web2.0網路社群最大之特色在於群體智慧（Levy & Bononno 2007）能夠即時協調分散的智慧並有效動員使用者的技能以解決難題，豐富並增進成員彼此獲取之價值，此外亦能夠避免群體迷思與個人認知偏差。群體智慧的宗旨在於促進大眾之共同利益為目標，倘若智慧產生的過程使用不法之數位內容或使用行為違反道德標準，將侵害創作人應享之權利與利益，不但缺乏價值正當性（Legitimacy），也偏離了群體智慧的價值方向。

根據經濟部工業局之「2004數位內容產業白皮書」指出，數位內容系指將字元、影像、語音等資料運用資訊科技加以數位化，並整合運用之產品或服務；依照產業之產出型態，數位內容產業可分為八大領域，包括：數位遊戲、電腦動畫、數位學習、數位影音應用、行動應用服務、網路服務、內容軟體及數位出版典藏等。由於數位內容本身易於處理、複製、傳播與保存，使用者隨意複製、上傳或下載數位內容之行為很有可能已經觸犯非法重製或非經授權傳播之罪刑。

以國內首要社交網站—無名小站為例：使用者為了讓自己的相本和網誌顯得有聲有色，卻不想要付費升級進階會員，因此一些熟悉網頁設計的使用者開始在網路上開始提供一些破解方法，只要在編輯網誌的時候加入一些特定的語法即可讓網誌享有像會員一樣的音樂播放功能，接著實現這種行為的知識則逐漸在網路上傳遍開來，到最後幾乎每一個無名小站上的使用者都具備此一技能；另外，時有耳聞的網路相本被破解技巧也是

一樣，總有一些具備高階技巧的使用者率先成功破解相本，在網路上公布特殊的破解教學之後，這種行為則會被其他的使用者複製然後再現。Yahoo奇摩拍賣也面臨複雜的群體犯罪問題，自從開始實施網拍賣家必須依得標金額多寡支付一定手續費之後，不少網拍賣家開始運用一些小技巧來規避高額手續費，例如某些賣家在網拍系統輸入的價格為$999，當買家使用搜尋系統找到並進入觀看詳細商品訊息的時候，才發現內文標示價格高於系統標示的價格，倘若買家購買此貨品仍須給付賣家內文標示之實際價格，而買家卻只需支付Yahoo拍賣對應於$999的手續費。

全球最大的影音分享網站YouTube亦同時面對來自於眾多使用者貢獻內容的問題，在任何時間、任何地點這些座落於世界各地的使用者都可能熱心地上傳短片和大眾分享，這些使用者本身可能具備不同的知識與和技巧，這些知識和技巧可能來自於YouTube以外的社群，被重新組合後被運用在YouTube社群上面，犯罪以另一種不同的面貌產生，然而行為背後所具備的知識或技能並不是單獨屬於此項行為所擁有。影片本身是一種內容，內容本身可以夾帶文字、圖片甚至是聲音以及連續的動作，換而言之影音資訊亦可以傳達某種特定的想發知識、或者是技巧。此帶有版權問題的創作經由YouTube社會網絡傳播給無數的閱聽眾，甚至潛移默化地影響所有閱聽眾的價值觀與模仿行為，由此可見YouTube在社群經營上面臨嚴重隱憂：YouTube成為違法影音資料滋生的溫床，此問題將隨著社群急速成長而日益嚴重甚至失控，倘若YouTube無法掌控如此局勢發展，必將難以永續經營下去。另外，YouTube平台上的群體犯罪與Napster平台上的犯罪現象有極大差異，以下從微觀與巨觀面比較兩者差異：

- 網路行為的動態（Dynamic on the Network）：網路上的個體是活動的，使用者搜尋、瀏覽、上傳、下載、訂閱等不同的活動與行為將會影響網路結構的呈現。在Napster上使用者僅能執行搜尋與下載的動作，並無法與其他使用者進一步溝通或互動，相對YouTube上的使用者往往擁有高度的社會連結，與其他使用者擁有頻繁之互動關係。
- 網路結構的動態（Dynamic of the Network）：Napster所提供的服務並非基於社會性關係，使用者僅透過點對點的方式直接交換檔案，並無所謂使用者群聚之現象。而YouTube平台上使用者則因各有所好而形成各式各樣的主題性社群，就結構上的觀點而言YouTube為一眾多社群所構成的網絡，且社群與社群之間具有高度異質性。

相對應於群體智慧，本研究稱此負面現象為網路群體犯罪（Collective Crime or Crime of Crowds），群體犯罪不同於組織犯罪（Organized Crime），並非有結構的犯罪團體或有計畫地進行犯罪活動，亦無為了追求共同利益而合作的共犯夥伴（Co-offender），而是個體自發性（Spontaneous）互動行為下逐漸浮現（Emerge）的群體相似犯行為。本研究以美國犯罪學之父Sutherland與Cressey（1978）之差別接觸理論（Theory of Differential Association）作為理論基礎，並進一步提出創新之科學方法可以有效介入與控制網路群體犯罪行為之發生。本研究同時使用網路科學（The Science of the Networks）的論點—真實世界中兩種動態都持續在進行，每一個情節的發展都會改變網路的結構，網路結構的改變也會使得網路上的活動型態產生變化（Watts 2003）—將群體犯罪行為相關之個體與連結關係的拓樸結構定義為「犯罪關係網絡」，網絡上個體犯罪行為乃是促使犯罪關係

網絡逐漸演化的力量，因此犯罪關係網絡是動態變化的，為了進一步了解犯罪關係網絡中個別份子間的關係結構對其個體及整個系統整體行為造成的影響，本研究將探討下列研究問題：

- 網路群體犯罪如何形成

在試圖提出解決網路群體犯罪問題之前，首先必須了解個體的犯罪行為，如何形成犯罪？進行犯罪需要哪一些資源或者條件？本研究以Sutherland與Cressey（1978）之差別接觸理論與Bandura（1977）之社會學習理論做為Belief-Desire-Intention（BDI）代理人架構之理論基礎，指導代理人如何在網路上取得資源並與其他代理人互動以完成犯罪行為之任務。

- 罪關係網絡與群體犯罪行為之關係

犯罪關係網絡乃個體互動行為下自然浮現的網路結構，也是本研究觀察主體。網路結構看似個體行為下造就的靜態結果，事實上，網路結構的特性亦決定了群體犯罪現象的接續發展。該如何衡量每一個體的連結分佈情形，是否因接觸的頻率多寡、時間長短、優先順序或強度大小而有所不同？個體如何影響另一個個體犯罪？個體間的連結與互動行為又會對網路結構造成什麼影響？釐清犯罪行為與犯罪關係網絡間之動態關係將有助解決群體犯罪問題，實為本研究相當重要之議題。

- 網路群體犯罪之傳播與擴散

倘若將群體犯罪擴散的問題比擬做流行性感冒病毒將容易理解的多，網路群體犯罪現象持續蔓延下去將對現有以及未來的網路社群經營造成莫大的傷害。根據Sutherland與Cressey（1978）的差別接觸理論，犯罪行為並非與生俱來，而是經由與關係親近的人互動學習而來，然而網路社群中弱連結（Weak Tie）的力量亦不容忽視（弱連結之連接是基於彼此共同利益，共同的經驗，但總體來說並不緊密的連接）；本研究欲了解個體之條件與行為對群體犯罪的擴散有何影響？群體犯罪的擴散是否因網路結構的不同而有所差異？

本研究貢獻在於本以傳統犯罪學理論為基礎，但從網絡觀點檢視個體行為與網路拓樸之動態關係，為網路群體犯罪研究另闢新徑。另外，過去網路服務設計僅只著重於效益而未見群體犯罪問題之嚴重性，本研究實驗結果可做為網路服務業者服務設計階段之重要考量。

本論文內容主要有四部分：第一部分為本研究之相關研究，第二部分為研究方法，第三部分研究方法之實驗設計與研究方法評估，第四部分為論文結論。

貳、相關文獻

一、差別接觸理論

近代的犯罪學理論紛然雜陳，不同學派的犯罪學者從不同的角度闡釋犯罪的原因，由於著眼之處與基本假設的差異，各個犯罪學理論之間有所衝突，亦有其適用之處。這

些理論大致可歸為三類：（1）以生物學取向的理論認為個人會有不同的行為表現，是因為身體構造的基本差異，例如身體外觀、體型、遺傳、內分泌失調、染色體異常、腦組織傷害與智力等。（2）以心理學取向的理論，著重於分析犯罪人的心理與行為之關係，如反社會的心理病態人格（Psychopathic Personality），或Adler的補償理論（Theory of Compensation）則認為犯罪是犯罪人為了超越自卑、尋求他人注意的補償行為。（3）以社會學取向的理論則強調社會環境、社會結構或社會化過程對於犯罪行為造成的影響（林山田等 2005）。

在一九二〇到一九三〇年代時，犯罪仍主要被視為生理或心理因素所致，Sutherland與Cressey（1978）所提出的犯罪學理論乃為犯罪學邁向社會學觀點相當重要的里程碑，其理論受到社會學大師Mead的形象互動理論（Symbolic Interactionism）等人深刻的影響。Sutherland與Cressey（1978）著有犯罪學原理（Principle of Criminology）一書，在一九五〇年辭世之後由其學生Cressey持續擴充再版，在最後一版的犯罪學原理（Sutherland & Cressey 1978）內所論述的差別接觸理論共包含下列九項要點：（1）犯罪行為是學習而來 （2）犯罪行為是與他人溝通互動的過程中學習而來 （3）犯罪行為的學習主要受與個人親近的團體所影響 （4）犯罪學習包括：學習犯罪所需的技巧，有時這些技巧相當複雜，有時則很簡單；學習特定的犯罪動機（Motives）、驅力（Drives）、合理化（Rationalization）和態度（Attitudes）（5）特定的犯罪動機或驅力是從他人對法律定義的好惡中學習而來 （6）一個人所以犯罪，乃因其認為違法有利的觀念超越違法不利的觀念 （7）差別接觸隨著接觸的頻率多寡（Frequency）、時間長短（Duration）、優先順序（Priority）與強度大小（Intensity）而有所不同 （8）經由接觸犯罪與非犯罪行為的犯罪行為學習過程，與其他學習行為具有相同的機制 （9）犯罪行為雖可解釋一般的需要和價值，但卻不為這些需要和價值所解釋，因為非犯罪行為也有著相同的需要和價值。

根據Sutherland與Cressey（1978）的論述，犯罪行為並非與生俱來，亦非無心之過，而是從社會環境中學習而來。「差別接觸」一詞係指個人與不同的人或團體接觸，這些不論支持或反對某一法律規範的觀念都可以成為學習的對象，當有利於犯罪的觀念超過不利於違法的觀念，則犯罪行為即有可能產生。Williams 與 McShane（1998）指出Sutherland與Cressey（1978）九項命題的有兩個層次：微觀面而言，差別接觸解釋犯罪行為如何形成；巨觀面而言，可以說明不同團體組織何以有不同的犯罪率。

本研究所以選擇差別接觸理論為基礎乃因其對於網路群體犯罪現象解釋之能力與適用性。林山田等人（2005）指出差別接觸理論的兩個基本構造可分為「犯罪學習的內容」與「犯罪學習的過程」，本研究依此觀點進一步說明如何以差別接觸理論解釋網路群體犯罪行為：

- 犯罪學習之內容：Sutherland與Cressey（1978）認為犯罪行為學習的內容包括犯罪的技巧，犯罪動機、驅力、合理化、態度以及認同違法的價值觀；網路社群上使用者的犯罪行為並非予生俱來，群體犯罪的擴散現象乃是經驗複製的結果，使用者在網路社群上與眾多使用者溝通與互動，並習得犯罪行為所需的技巧、偏好違法行為的

價值觀。

- 犯罪學習之過程：Sutherland與Cressey（1978）認為犯罪學習的過程是經由與親密團體接觸學習而來，這些親密團體對於法律意義有著不同的觀感，並且影響行為人觀念上的連結，連結會因接觸的頻率多寡、時間長短、優先順序或強度大小而有所不同；網路社群中使用者的連結關係亦受上列因素影響，值得注意的是使用者在網路上的連結關係除了與親密社群的連結之外，有時透過弱連結跨越不同社群可以取得關鍵性的犯罪資源。

換言之，差別接觸理論主張犯罪行為是經由後天的學習而來，犯罪行為的學習過程，與其他學習行為具有相同的機制（Sutherland & Cressey 1978）。然而，差別接觸理論並未進一步討論所謂的學習機制。究竟學習是如何產生的，這一問題是學習理論的核心。一般而言，學習理論認為人類的學習主要有三種機制，連結（Association）、強化（Reinforcement）與模仿（Modeling）。而Bandura（1977）所提出社會學習理論（Social Learning Theory），主張觀察學習是社會學習的基礎，個體在社會情境中可藉由觀察他人的行為、態度以及行為的結果來進行學習，因此又稱為「觀察學習」。人類大部分的行為都是經由模仿而來，模仿的發生並不一定需要外界的強化，只需觀察他人的行為和結果便可以產生。

一般網路犯罪研究皆以實證方式，依據現有資料歸納分析犯罪之型態、類別、方法，及犯罪者之特質、犯罪動機與可能使用之犯罪模式，並從政策管理面、法律偵查面、安全技術面及教育認知面擬定網路犯罪防治策略（范國勇 2005; 林宜隆 2007），此固然能夠揭露客觀之事實卻也有其限制：其一、網路犯罪具有隱密性、匿名性和智慧性犯罪等特質，研究者難以取得全面性的犯罪行為相關資訊；其二、將犯罪現象視為眾多因素下造就的結果來衡量，例如犯罪型態、類別、方法雖有助於一般化犯罪行為，卻無法彰顯犯罪行為發展之動態過程；其三、犯罪偵察之目的在於證明犯罪事實，著重於事後查證而非事前偵測。

網路群體犯罪的議題跨越以往的犯罪學研究方式，網路群體犯罪具有分散性和和擴散性特質，研究者難實際以取得全面性的犯罪行為相關資訊。國外則有運用社會網絡來分析某一地理區域內的犯罪歷史資料，進一步找出可能的犯罪熱點（Clarke 2004），或者將犯罪現象視為眾多因素下造就的結果來衡量，藉由分析人口變項與網路結構的關係來提出犯罪行為的必然性解釋，卻不能彰顯犯罪行為發展之動態過程。本研究以美國犯罪學之父Sutherland與Cressey（1978）之差別接觸理論（Theory of Differential Association）作為理論基礎，並進一步提出創新之科學方法以有效介入與控制網路群體犯罪行為之發生之動態過程。

二、智慧型代理人

隨著人類社會不斷地進步，新興科技之應用環境也愈趨於複雜，在管理大範圍之嵌入式軟體系統（embedded software system）也愈加有挑戰性。一般而言，軟體系統之設計，希望能設計出一可靠（reliable）、可維護（maintainable）以及可擴充的

（extensible）系統（Kinny et al. 1996），為因應此種需求，現今在設計應用系統上提出了代理人導向（agent-oriented）的觀念。

代理人（agent）為人工智慧領域中之專有名詞，代理人所處之環境為一會變化且為不確定（uncertain）的世界，代理人可意識環境的改變並做出適當動作，其具有可反應的（reactive）、自主的（autonomous）、內部自我激發（internally-motivated）之特性存在（Ferber 1999）。

代理人導向系統目前已有許多的成功應用例子，其中一個常見的代理人架構為BDI（Rao & Georgeff 1995），使用BDI架構之代理人即稱為BDI代理人（BDI agent）。在BDI架構中，將代理人視為具有某些人類心智上的態度—Beliefs、Desires、Intentions（Bratman 1987; Bratman et al. 1988; Georgeff & Lansky 1987），可以完整地表達其可感應之事件、可執行之動作、其所具備之知識、其所採用之目標以及來源自intention之計畫。BDI代理人有三個model，分述如下：

1. Belief model：描述此代理人所處環境的所有資訊，其所持有之內部狀態以及可執行之動作。所有可能之belief或properties，皆被一belief set來描述之。而一個或多個的belief states-instances of the belief set，會被定義且用來描述成此代理人之初始狀態。
2. Goal model（Desire model）：描述代理人可能採用之目標（goal），以及可做反應的事件（event）。此model中包括了一goal set，來詳細指明所有的goal及event，以及一個或多個的goal states，其為用來描述代理人之初始狀態。
3. Plan model：描述代理人可能用來執行以達到目標之計畫（plan）。其中包括一plan set，來指明各別計畫之properties以及控制結構（control structure）。

要建造一個BDI架構之代理人，可分為二個步驟：

- Analyze the means of achieving the goals：針對每個目標（goal），分析要如何各別達到，並將其分解，分成不同之子目標（subgoal）及動作。接著分析子目標之順序，及在何種狀況之下，要執行何種子目標，還有什麼樣的錯誤必須被處理，並對產生能達到各個子目標之計畫。
- Build the beliefs of the system：分析所有控制活動或動作之狀況，並將之分解。再針對子目標之計畫，分析其必要之input及output資料，並確定所有資料皆存在於belief中，或是存在於較早執行的計畫中。

在尋找餐廳之應用實例（Lin et al. 2003）中，是將BDI架構應用於行動裝置上，當使用者想找餐廳時，可使用行動裝置做為輔助，來找尋在某範圍內適合的餐廳。在BDI架構中，belief為餐廳之資訊，包括位置、價格、型態等，以及使用者之profile，記錄使用的每次選擇結果；desire則為找到符合使用興趣之餐廳；intension則是依使用者的所有興趣，分成多個子計畫。

在BDI代理人中的成功應用，還有由Jadex BDI代理人平台（http://vsis-www.informatik.uni-hamburg.de/projects/jadex/），其是利用Java技術所發展出之multi-agent系統，並採用BD架構，可提供一用於商業、工業及研究上的應用平台。

本研究使用BDI模型的主要原因在於BDI模式是最知名的與最好的研究模型於實際推

理（human practical reasoning, means-end reasoning）上（Georgeff et al. 1998），藉著存在的邏輯語言來來製作BDI agents 並進行實際推理。本研究將建立在差別接觸理論與社會學習理論之基礎上以進行實際推理。

另外，本研究之BDI模型乃以LEADSTO語言（Bosse et al. 2005）作為BDI代理人模擬概念的表達。LEADSTO之語言和軟件環境已發展到模型表達和模擬動態過程兩方面。一方面LEADSTO語言是一種是合乎邏輯的表現形式具時態語義（temporal semantics）之規範語言；另一方面LEADSTO可以表達動態過程，可以模擬仿照事件狀態與時態間的依賴關係，產生模擬的痕跡以進行進一步分析。換言之，本研究將使用此語言具備質化、量化概念與邏輯關係的表達能力，以模擬方式進行實際推理。

三、網路科學概念

社會網路分析法就是透過蒐集問卷、訪談、觀察蒐集社會網路資料並運用圖論（Graph Theory）的概念作進一步分析解釋。由社會網路分析法所建立的社會網路具有能描繪出各種關係網路的能力，如情感網路、諮詢網路、信任網路、訊息網路的建立，並可運用所發展出的指標瞭解評估整個社會網路的狀況，如結構鬆散或是緊密，或瞭解社會網路中的角色是位於核心或邊陲（邱議德 2003）。

一個複雜系統是由許多相互依賴的個體所組成，複雜系統的行為並非只是個體自身行為的展現，而是依個體之間如何互動來決定系統的行為整體。一個複雜系統可視為一個複雜網絡，網絡的基本元素乃是由節點（Vertex）與連結兩個節點的邊（Edge）所構成。目前網絡學家（Newman, 2003）已經發展出一些相當重要並且時常被用來衡量、分析網路結構的指標，分述如下：（1）核心度（Centrality：核心度是衡量網絡位置的重要指標，它指出那些連結到最多人或者最有影響力的個體（Newman 2003）。有幾個方法可以衡量核心度，包括連結度數（Degree）、中介度（Betweenness）和特徵性（Eigenvector）。（2）連結度數（Degree）：連結度數代表與某個網絡成員的直接接觸成員的數量，如果個體在某組織網絡中認識20個成員，則Degree為20。此一指標又可分為兩種，一種是向內的度數（In-degree），另一個是向外的度數（Out-degree），前者代表有多少人認識我，有問題或困難時會想到找我去協助或徵詢我的意見，後者則是指我認識多少人。在網路結構中Out-degree越大的使用者影響力越大，如果將其從結構上移除，將對整個網絡造成較大的影響。（3）中介度（Betweenness）：中介度用來衡量某個體位於網絡中其他兩個成員之間最短的途徑上面的次數或頻率，中介程度高表示個體位處於網絡的要徑上，也就是個體在該網絡的互動關係中扮演重要的功能。（4）特徵性（Eigenvector）：特徵性所關切的是不只是個體是否有很多朋友（連結度數），還有個體的朋友是否也有許多朋友。這個指標的數值越大，表示該個體所能號召的其他個體數量也越大。（5）群聚係數（Cluster coefficient）：群聚係數C表示某個體的朋友也是我的朋友的機率。公式如式子（一）所示：

$$C = \frac{6\times \text{ number of triangles in the network}}{\text{number of paths of length two}} \qquad (一)$$

式中的number of paths of length two指的是從一個節點指出去（Out-Degree）的連結度數（Newman 2003）。（6）均路徑長度（Average path length）—任兩個節點i和j間的最短路經為路徑所經過的邊數之和。而平均路徑長度代表的是任網絡中任兩個節點之間最短路經長度的平均值（Latora & Marchiori 2003）。公式如式子（二）所示：

$$L(\mathbf{G}) = \frac{1}{N(N-1)} \sum_{i \neq j \in \mathbf{G}} d_{ij}. \qquad (二)$$

參、研究方法

近年來網路群體犯罪的問題逐漸浮現，並對網路服務本身或網路社會造成傷害。然而礙於2.0網路虛擬社群群體網路使用者行為資料收集之困難，本研究以代理人為基礎之模式化與模擬之方法提供相當有用的研究途徑，研究者得以透過此一方法模式化在網路世界中自具備自主性、互動性與社交能力之理性使用者行為；本研究工具使用BDI代理人架構，其以中以信念、期望、意圖三種心理屬性表示代理性人內部之資訊狀態（informational state）、動機狀態（motivational state）與慎思狀態（deliberative state），並且決定了代理人將採取之行動（Rao & Georgeff 1995），並應用Sutherland與Cressey（1978）之差別接觸理論與Bandura（1977）之社會學習理論來進一步設計代理人系統，來模式化群體犯罪中代理人決策形成過程與社會互動關係。

代理人的模擬提供個體行為發展的基礎，社會網絡分析則從另外一個角度，宏觀地檢視整個社會的結構。在社會網絡分析的方法中，相當重視實際資料來源的調查與收集，以此作為輸入資料，透過社會網絡的分析方法計算出重要的網路結構屬性，然而Watts（2003）則認為社會網絡分析傾向於將社會結構視為力量造就出來的結果，而非力量影響下逐步演化的系統。本研究也使用社會網絡分析的指標來衡量網路結構，然而不同之處在於代理人模擬與社會網絡分析的結合，以模擬的資料做為社會網絡分析所需的輸入資料，網路結構隨著代理人的互動不斷地演化與自我形塑。個體的互動與網路結構彼此相互影響，牽一髮而動全身。本研究首先藉由代理人模擬來浮現犯罪關係網絡，而後利用網路結構分析方法來分析犯罪關係網絡之特性以利虛擬社群中群體犯罪現象瞭解與有效管理。

一、研究基本概念與假設

Bandura（1977）於其所提之社會學習理論認為，幾乎任何一種理論都能夠在事後對已發生的事件加以解釋，但是卻無力預測未來，一個好的理論價值應取決於其是否能訂定控制心理現象的各種條件，並說明決定心理狀態的種種內外因素發揮影響作用的機制。社會學習理論對於觀察學習的過程與機制方面的闡述，也提供了基礎的行為預測能力，本研究在採用社會學習理論的概念與學習機制來設計BDI Agent之差別接觸學習行為。

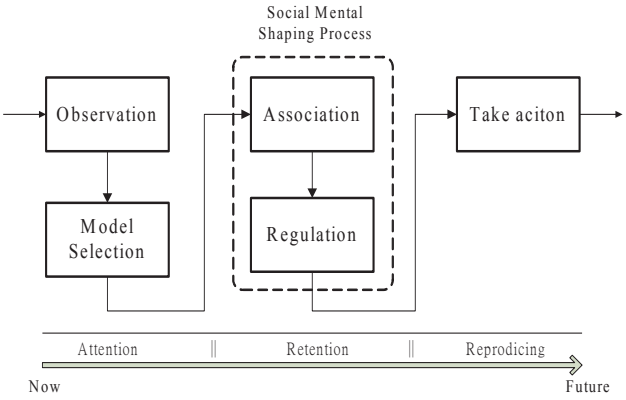

圖1：本研究Agent操作流程

圖1為本研究設計之具有學習能力的Agent操作流程，可分為三個階段：注意階段、保持階段與行為再現階段。分述如下：

1. 注意階段：根據觀察學習理論，假設所有的行為皆是觀察學習而來，首先Agent將會觀察其所處的Context並隨時更新最新的資訊，這些資訊的內容包括對於其他代理人的信念、關係的信念、環境的信念，以及行為回饋的資訊等等，換言之，Observation process在這裡扮演類似於Sensor的角色。這些資訊將進一步提供Agent做為篩選楷模所需的判斷資訊，在有限的資源與關注能力之下，Agent僅能夠挑選出一些對其而言較為醒目的對象，以之為學習的楷模。
2. 保持階段：再選定楷模之後，這些楷模將會對Agent產生認知與行為態度上的影響，在此本研究假設Agent的態度可以被其他Agent所觀察。Agent透過接觸不同楷模並從楷模的行為中學習其行為態度，每一個Agent的學習對象不同，因此學習的內容也不盡相同，此即為前述差別接觸（Differential Association）之意涵—接觸度不同的學習對象與接觸不同的行為態度。Agent在一連串不斷的社會行為裡接觸到各種不同的行為態度（信念），有些可能是之前沒有的態度，也有些和自己原本的態度有所出入，受到這些不同態度的影響，Agent也隨之調節並修改原有的行為態度，此外，行為態度當然也受到行為評價結果的調節，例如負面的結果將導致行為態度趨於保守。
3. 行為再現階段：Agent在前一個階段於態度上任何的轉變，都可能會導致不同的行為意圖，最終展現不同的行為。在虛擬社群上，一個行為的評價由其他Agent對這個行為的反應所決定，行為的評價將會反饋回去影響行為的態度，也會受到其他Agent的觀察。

圖1中有左至右的時間軸表示現狀的觀察到未來行為的產生，代理人經由社會性的互動而影響內心狀態的轉變，可做為預測未來行為發生的預測子（Predictor），換言之，乃透過代理人互動的能力與學習機制來預測代理人未來之行為。本研究以BDI代理人模型來Modeling代理人的行為，BDI模型從信念—期望—意圖三個抽象的內在層次來區分代理人的心理狀態，意圖是期望的限縮並且更接近於行為，並且可更有效地預測行為，

如圖2 之BDI推論示意圖（Bosse et al. 2007）。

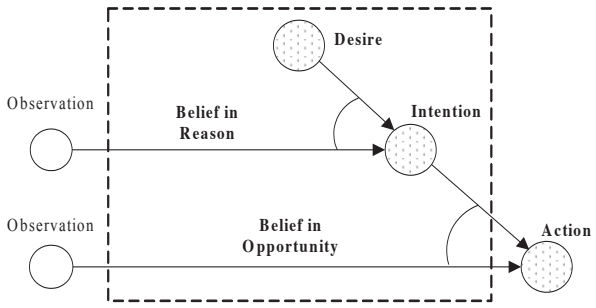

圖2：BDI推論示意圖（Bosse et al. 2007）

藉由BDI代理人架構模式化代理人內部心理屬性與行為，我們得以回應前述所謂網路行為的動態，意即代理人如何改變自我心理狀態以及如何與環境進行互動，此階段著重於個體微觀層次的模式化。

然而，個體犯罪行為乃是構成群體犯罪現象的基本單位，因此個體行為與群體犯罪現象的展現具有完全密不可分的關係；從結構上觀點而言，本研究將群體犯罪行為相關的個體與連接關係稱之為「犯罪關係網絡」，犯罪關係網絡並非只是個體犯罪行為造就的靜態結果，而是個體犯罪行為力量推動下不斷演化的動態網絡。換言之，隨著Agent本身持有的Beliefs不同（Beliefs等同於下節代理人模擬模式裡的Attitudes），將使其產生特定的Intention。Sutherland 與 Cressey（1978）認為犯罪乃是經由社會互動行為學習而來，在本研究中，代理人亦透過互動過程，學習他人的行為態度。

倘若將Agents之間的互動以網路結構方式來呈現，如下圖3網絡觀點下之構成群體犯罪所需相關角色示意圖，每一個Node代表一個Agent的Beliefs的集合，每一條Link代表Agent之間的互動關係，互動關係因互動的方向與互動程度（權重）而變化，箭頭表示信念傳遞的方向，當箭頭方向朝外（Outgoing）的時候代表Beliefs可能為他人所學習，當箭頭方向朝內（Incoming）的時候代表學習他人的Beliefs。

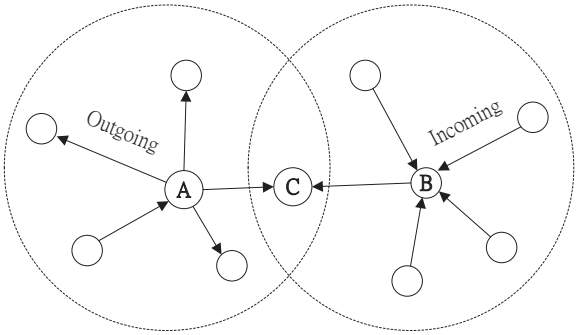

圖3：網絡觀點下之構成群體犯罪所需相關角色示意圖（本研究整理）
（A：影響者；B：學習者；C：信念仲介者）

圖3中可見Agent A在此團體中扮演相當重要的角色，因為和Agent A有互動的五個對象中，有四個都是向Agent A學習，因此Agent A具有較大的社會影響力，其行為可謂舉足輕重。透過社會網絡分析的指標，可以衡量每一個節點的核心度（Centrality），核心度越高則其影響力越大。另一個Agent B卻大不相同，Agent B在此團體中主要扮演學習者的角色，對於其他人也比較沒有什麼影響力，至於Agent B會學習到哪一些Beliefs組合，端視與其他Agents接觸的互動程度，與之互動程度越高的對象，則產生的影響程度越大。而Agent C則在代理人A與B之間扮演一信念仲介者（Belief broker）的角色，擁有Agent A與Agent B的部分信念，Agent B可能透過Agent C以取得Agent A的信念，反之，Agent A亦可能透過Agent C以取得Agent B的信念。

舉例實例而言，一個剛剛接觸Youtube的使用者，如果接觸到許多傾向於侵犯智慧財產權的內容，很有可能因此受到影響而做出一樣的行為。除了關係的影響之外，網絡觀點指出使用者在網路結構中所處的位置影響也很大。透過社會網絡分析的方法從互動關係的結構面著手，可以找出社群中較有影響力的使用者，與其他關係緊密的對象，然後再以Base-level的BDI推論法則預測其是否擁有犯罪行為意圖。

本研究有三個基本假設，如下所述：

1. Agent可以完全察覺他人行為結果的報酬（Payoff）：Web2.0網路服務的設計中，報酬的量化相當重要，因為如此才能夠激勵參與程度高的、貢獻良多的使用者，例如在Youtube社群中，個人開設的頻道被觀看的次數、訂閱人數、好友人數等訊息的設計，其目的皆為了能夠視覺化報酬的效果。因此，本研究假設每一個Agent所得到報酬都是可以完全被任何與其接觸的Agent所觀察。
2. Agent的學習行為乃基於行為結果報酬的考量：社會學習理論指出，人們多半於傾向於接受他們認為能夠產生有價值的結果的示範性行為，而不能接受沒有酬賞或具有懲罰後果的示範性行為（Bandura 1977）。在網路社群上面，使用者的行為更是基於價值的考量，因此這也是為何許多研究網路社群使用者行為意圖的研究均發現來自於社會道德規範的影響不顯著的原因，因此本研究在此假設Agent對於行為報酬的考量決定其學習的意願，Agent學習行為的考量完全是基於報酬價值的高低，觀察到的平均報酬越高則學習的意願越高，當觀察到的平均報酬越低則學習意願越低，甚至沒有學習的意願。
3. Agent因所處的Context不同，接觸到不同的資訊、對象和資源：在網路社群上面，每一個使用者因為接觸到的環境和對象都不同，換言之，使用者在網路結構上所處的位置不同，接觸的內容也有所差異。

二、研究方法與設計

本研究以差別接觸理論與社會學習理論為核心，發展網路群體犯罪之模擬模式。BDI代理人架構的基本概念以信念、期望、意圖三種心理屬性表示代理性人內部之資訊狀態、動機狀態與深思熟慮狀態，此模式本身是一個knowledge-based的推論邏輯。本研

究使用LEADSTO語言（Bosse et al. 2005）作為代理人模擬概念的表達，此語言具備質化、量化概念與邏輯關係的表達能力。群體犯罪模擬模型共有四個子模型，分別為Belief子模型、Desire子模型、Intention子模型與Opportunity子模型，分別由八個local dynamic（LEADSTO） properties（LP's）所描述，描述式中包含質化或量化的變數，如圖4中所示，特定的術語表示與說明整理如表1&2。各個子模型（包括所使用之LPs）將分別在下列章節中說明。

表1：Local Properties之變數定義

定義	說明	舉例
d: DESIRE	d表示任一個期望	Desire（名聲）表示有個獲得名聲的期望等待被滿足
a: ACTION	a表示某一行為	a=上傳自行轉錄的娛樂節目
x1, x2, v: INTEGER	x, v均為整數，表程度的大小	Expected_efficacy（a, 3）表示對此行為的期望報酬為3
m, n□{SKILLS}	m, n均為某些技能的集合	m={錄製, 轉檔}，表示完成上述行為a必須具備此兩種技能
b: BOOLEAN	b值為一布林值，值為1時表條件存在	Willing_to_learn（a, 1）表示有願意去學習Action a
p: PROBRABILITY	p為一機率值	p=0.5代表產生此行為的機會大小為50%

表2：術語之說明

術語	說明
Belief（satisfies（a, d））	相信Action a可以滿足desire d
Expected_efficacy（a, x2）	個人對於從事Action a預期獲得的報酬為x2
Willing_to_learn（a, b）	願意向觀察者學習Action a的信念與否的信念
Required_crimeskills（a, m-n）	對於完成Action a尚缺犯罪技能m-n的信念
Attitudes（a, d, x2, b, m-n）	上述四個信念決定一特定之行為態度，Attitude函數包含五個參數，這些值來自於上述四個信念，不同值的組合表示不同的行為態度。
Intention（a, x2, b, m-n）	Intention函數包含四個參數，不同的行為態度導致個人採取不同的行為意圖。
Observe_rewards（a, v）	觀察到他人從事Action a所得到的報酬為v
Observe_skills（a, m）	觀察到他人從事Action a所需的技能為m
Existing_skills（a, n）	個人目前只擁有從事Action a的的部分技能n
Personal_rewards（a, x1）	個人過去從事Action a所獲得的報酬為x1
Opportunity（a, p）	對於實際去執行Action a的機率之信念為p
Perform（a, p）	實際去從事Action a的機率為p

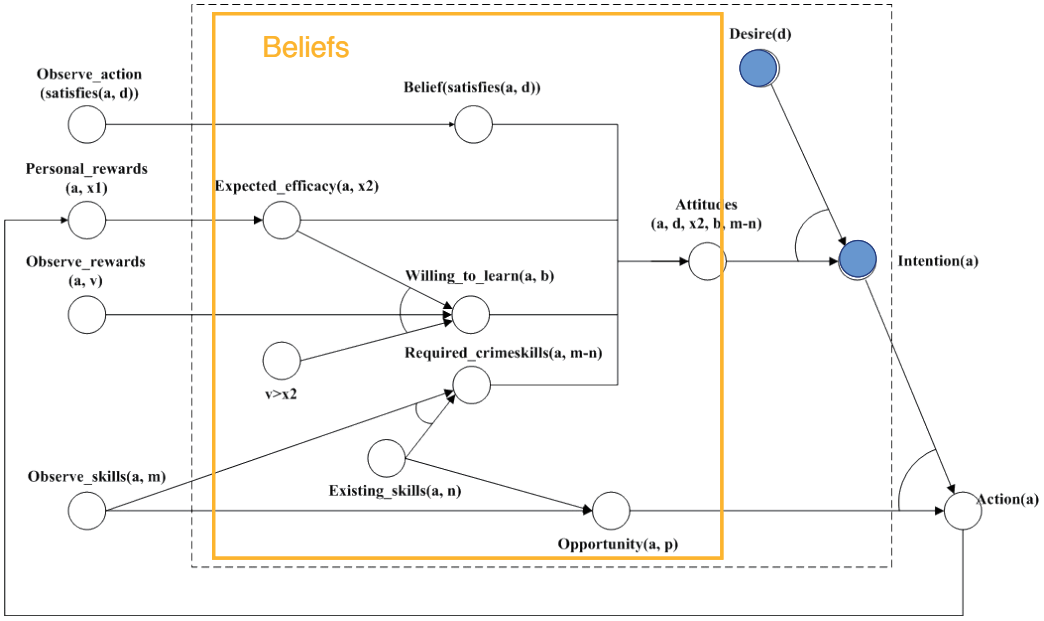

圖4：本研究Simulation Model架構

（一）Belief Submodel

LP1中的Attitudes其實屬於Beliefs之子集，換言之，Attitudes由一些Beliefs所組成，Attitudes（a, d, x2, b, m-n）中包含五個來自於LP4、LP6、LP7與LP8的參數。Belief submodel由LP1、LP2與LP3構成，其主要架構乃依循前述圖 2之 BDI推論示意圖。

LP1

影響Agent行為意圖的態度有四個信念：Action a是否可以滿足Desire d、對於a行為的態度是否積極、願意向觀察者學習Action a的信念，與是否具備需要的技能。四個因素值的變動將導致態度的差異化，以函數Attitudes（a, d, x2, b, m-n）來表示。

∀a:ACTION ∀x2, v:INTEGER ∀b:BOOLEAN ∀m, n∈{SKILLS}

Belief(satisfies(a, d)) ∧ Expected_efficacy(a, x2) ∧ Willing_to_learn(a, b) ∧

Required_crimeskills(a, m-n) → Attitudes(a, d, x2, b, m-n)

LP2

Attitudes（a, x2, b, m-n）與Desire（d）決定Intention（a, x2, b, m-n）。當Agent有一個Desire需要被滿足，函數Intention（a, x2, b, m-n）表示Agent對於Action a採取一特定的行為意圖，行為意圖因x2, b, m-n三個參數之變化而產生差異。

∀a:ACTION ∀x2, v:INTEGER ∀m, n∈{SKILLS}

Attitudes(a, d, x2, b, m-n) ∧ Desire(d) → Intention(a, x2, b, m-n)LP3

Opportunity（p）與Intention（a）決定最後的Action a。特定的Intention有可能導致特定的Action產生，然而Agent是否會實際採取Action端賴其對於Opportunity的信念，當p值

越大則實際去從事Action a的機率也越大。

∀p:PROBRABILITY ∀a:ACTION
Opportunity(a, p) ∧ Intention(a, x2, b, m-n) → Perform(a, p)

（二）Desire Submodel

本研究並不試圖處理Agent產生Desire的推論過程，在此直接給定Desire（d）表示Agent擁有一個Desire d等待被滿足

（三）Intention Submodel

LP4表示當Agent觀察到其他Agent行為的結果，Agent就會相信此一行為可以滿足某一個Desire，例如：John相信上傳越多的影片則名聲越響亮，上傳影片是行為，其結果—帶來更多的觀看次數—可滿足名聲響亮的期望。LP4可呼應學習理論中連結（Association）的概念。

LP4

Agent對於Action a的觀察將導致信念—Action a是否能夠滿足Desire—的產生。

∀a:ACTION ∀d:DESIRE
Observe_action(satisfies(a, d)) → Belief(satisfies(a, d))

LP5則呼應學習理論中增強（Reinforcement）的概念，此式假設個人之過去經驗中獲得的報酬是影響預期效用的主要因素，其他Agent行為獲得的報酬高低並不會增加或減少Agent對行為的預期效用。此式表示當Agent獲得支酬賞x1為正值的時候，其對此一行為的預期效用也會增加，當Agent獲得支酬賞x1為負值的時候，其對此一行為的預期效用則會減少，式中| x2 |為原始預期效用的絕對值，當| x2 |越大則預期效用的增值或減值效果愈不明顯。

LP5

Agent過去相似行為的獲得的報酬將導致信念—預期效用—的增強或減弱。

. x1, x2:INTEGER
Personal_rewards(a, x1) ∧ Expected_efficacy(a, x2) →
Expected_efficacy(a, x2 ＋ x1 / | x2 |)

LP6則呼應社會學習理論的基本論述，Agent傾向於學習產生有價值的行為，Young（2007）認為代理人面對創新時，選擇採納可以帶來比他目前作法更好的創新，因此LP6比較了觀察到的行為報酬v值與來自於個人經驗的預期效用x值，當觀察到的行為報酬優於預期效用的時候（v>x2），Agent才會產生學習Action a的意願。

LP6

Agent觀察其他Agent從事Action a所得到的酬賞v，和自我對Action a的預期效用x相互比較，當v>x2時b值為1，表示Agent將產生願意向觀察者學習Action a的信念，反之，當v>x2不成立時b值為0，表示Agent並沒有產生向觀察者學習Action a的信念。

∀a:ACTION ∀x2, v:INTEGER ∀b:BOOLEAN
Observe_rewards(a, v) ∧ Expected_efficacy(a, x2) ∧ v>x2 → Willing_to_learn(a, b)

在網路社群裡，並不是所有的使用者都有能力犯罪，使用者需擁有完成該犯罪所需的技能，因此LP7用來表示Agent對於技能的信念，舉例而言，Robert要上傳一部電影的片段，完成行為必須具備轉檔與剪輯的能力，但Robert缺少剪輯的能力，可用Required_skills（剪輯）表示Robert此時擁有的信念，此意味著Robert可能會有去學習剪輯技能的意圖。

LP7

Agent觀察到從事Action a必須具備技能集合m，和目前已具備的技能集合n相互比較，兩個集合之差集m-n表示尚未具備的犯罪技能，因此Agent會產生一個信念—需要去學習缺少的犯罪技能。

$\forall a{:}ACTION\ \forall m, n \in \{SKILLS\}$

$Observe\_skills(a, m) \wedge Existing\_skills(a, n) \rightarrow Required\_crimeskills(a, m\text{-}n)$

（四）Opportunity Submodel

在Intention確立之後，Agent只有在認為有機會的時候才會採取行動。行為究竟會不會產生可能取決於內在或外在環境因素的控制。由於當前網路社群上使用者的行為相當自由而鮮少受任何限制，因此本研究在假設環境中並不存在抑制犯罪的抑制因素，當Agent擁有一犯罪意圖，犯罪的機會取決於是否擁有充分的犯罪技能，技能越充分則犯罪的機率也越高，如LP8所示。

LP8

Agent目前已具備技能集合n的技能個數，除以從事Action a必須具備技能集合m的技能個數，當Agent具備的技能越充足，則其機會信念越高，越有可能去從事Action a，反之亦然。

$\forall m, n \in \{SKILLS\}$

$Observe\_skills(a, m) \wedge Existing\_skills(a, n) \rightarrow Opportunity(a, amount(n)/amount(m))$

肆、研究方法評估

本研究之目的，是希望以BDI代理人模擬來建立所欲觀察的使用者資料，以取代實證研究資料收集的限制，藉由代理人模擬得以觀察使用者可能的行為動態；同時，以代理人模擬為基礎所浮現出來的網路結構也具備動態演化的生命力與並提供研究者觀察複雜結構良好的機會。

本研究是以所建構的代理人模擬概念模型為基礎，進行實驗的參數與模型設計，實驗之目的如下：

- 初始犯罪率對於群體犯罪的擴散有無影響？

在不同的網路社群中，可能存在數量不依犯罪族群，本研究欲藉由實驗模擬觀察，當網路社群使用者人數固定時，不同的初始犯罪率對於犯罪技能的學習擴散有無影響。

- 網路社群的大小對於群體犯罪的擴散有無影響？

網際網路上成千上萬的網路社群，其使用者數量多寡不依，本研究欲藉由實驗模擬觀察，假設固定犯罪人數之情況下，網路社群使用者人數的多寡對於群體犯罪的擴散有無影響。

- 網路結構屬性與網絡模型

Watts（2003）所提出的小世界β模型，相當系統化的簡化了世界的細節複雜，β模型建構的小世界現象乃介於Regular network與Random network之間，β模型給定了固定大小的節點數，並賦予每一個節點固定重新連結（Rewiring）的機會，根據實驗結果發現小世界現象相較於Regular network與Random network具有較高的群聚係數（Cluster Coefficient）。然而真實世界中，尤其是在網路社群上，並非所有的使用者都具備相同被連結到的機率，本實驗在代理人模擬上提供代理人各種屬性參數不同的數值，使得每個使用者被連結到或者失去連結的機率有所差異，並觀察在各種實驗下面網路結構屬性的變化，並比較浮現之網絡模型與Watts（2003）提出之β模型之差異。

一、實驗設計

實驗參數可分為社群層次與個體層次，參數的數值設定與實驗規則將於下面詳細說明，參數名稱與數值如表3所示：

表3：實驗參數名稱與數值說明

參數名稱	英文參數名稱	數值
使用者人數	Size	50, 100, 130
初始犯罪率	Initial Criminal Rate	5%, 15%
技能	Skills	{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15}
犯罪者期望值	Criminal Expectation	4 < Expectation < 8
使用者期望值	User Expectation	Expectation ~ N（2,1）大約 － 1 ≦ Expectation ≦ 5
學習意願	Willing	0, 1
滿意度	Satisfaction	0, 1
行為酬賞	Rewards	預設為Expectation ± X, X~ N（0,1）
臨界值成功機率	Threshold Opportunity	預設為0.2
連結機率	Wiring Probability	When n<5, 50%make friend via friend, 30%random, 20%break; When n>5, 20%make friend via friend, 10%random, 70%break

1. 環境參數設定

實驗環境乃對應於上述巨觀層面所欲了解之現象，所必須進行調整之參數變相，本實驗環境參數包括：使用者人數、犯罪比率。

- 使用者人數（Size）：本實驗將分別設定社群之使用者人數為50, 100與130個人，進行實驗模擬以觀察網路社群的大小對於群體犯罪的擴散有無影響。
- 犯罪者比率（Initial Criminal Rate）：本實驗欲觀察犯罪人數的比率對於群體犯罪擴

散之影響，因此本實驗在固定使用者人數的社群之下，將初始的犯罪人數比率分別設定為5%, 15%，以觀察比較其差異。

2. 代理人行為與參數設計

- 使用者型態：如同本章開頭所描述之實驗情境，網路群體犯罪一開始都是由少數擁有犯罪技能的使用者，將犯罪的方法教學公開在網路社群上或者是犯罪行為的展現而成為一般使用者觀察學習的對象，因此本實驗將使用者的型態區分為犯罪者與一般使用者。由於這些犯罪技巧往往使得使用者獲得更大的效益，因此犯罪行為才會廣為流傳。故在本實驗中，犯罪者被初始化予以某些「犯罪技能」，並且擁有較高的「行為酬賞」與「期望值」。而一般使用者則不具備「犯罪技能」，並擁有相對於犯罪者較低的「行為酬賞」與「期望值」。
- 連結之數量與機率：為了控制每個使用者擁有有限的連線數量，而不是永無止境的建立連結，另一方面，網路社群中使用者往往透過朋友去連結到新的朋友（ex：無名小站），因此本研究假設當代理人向外連結數量小於或等於5的時候，有50%的機率透過朋友來結交朋友，有30%的機率是隨機結交朋友，有20%的機率從既有的朋友群中挑選一位「行為酬賞」最低的朋友來終止關係；相對地，當朋友數量大於5的時候，有20%的機率透過朋友來結交朋友，有10%的機率次隨機選取任一使用者做為朋友，有70%的機率與「行為酬賞」最低的朋友結束朋友關係。
- 行為酬賞（Rewards）：犯罪者被預設予以較高的行為酬賞，而一般使用者的酬賞普遍低於犯罪者，代表網路上這些犯罪行為還是能夠帶來較高的利益（價值—成本）。在此本實驗假設使用者將從對外的朋友連結中，選出一位行為酬賞最高的使用者成為觀察的對象。使用者每次學習技能後有一定的機率可獲得正面評價，每次正面評價則雙方的「行為酬賞」值皆隨機增值x（$0<x<1$）。
- 期望值（Expectation）：期望值表示使用者對於從事犯罪行為預期獲得之報酬，期望值的高低取決於上述「行為酬賞」的增減值x，當獲得正面評價時，則Expectation = Expectation + x / | Expectation |，當獲得負面評價時，則Expectation = Expectation − x / | Expectation |，式中以| Expectation |做為分母，故期望值會隨著分母越大，增值速度愈驅緩慢。
- 學習意願（Willing）：使用者選定一個觀察對象之後，將比較對象的「行為酬賞」與自身的「行為酬賞」，當對方的行為酬賞大於自己的行為酬賞，則具備「學習的意願」，選定對方成為行為楷模，並向對方學得某一技能。相對地，如果對方的「行為酬賞」小於自己的「行為酬賞」，則不會有學習的意願。
- 滿意度（Satisfaction）：當「期望值」大於0的時候代表使用者對某一行為仍所期待，滿意度設為1表示滿意，反之，設為0表示不滿意。
- 犯罪技能（Skills）：在真實的網路社群中，各種不同的社群可能需要不同的技能組合，才能從事特定的犯罪行為，為了方便實驗的觀察與控制，在此假設總共有15種基礎犯罪技能，每位犯罪楷模擁有3至6個必要技能，不同的技能組合表示可用來實現不同的犯罪行為。而一般使用者可能直接或間接習得某些技能，不同的技能組合亦代表可能的不同的犯罪行為。

- 臨界值（Threshold）：臨界值用來控制使用者對楷模學習行為技能的機率，所有使用者的臨界值一開始皆預設為0.2，表示每次聯繫（Association）只有兩成的機會習得一個技能，每當習得一個技能之後，臨界值增值0.1，代表使用者對於犯罪技巧的學習曲線逐漸升高。
- 成功機率（Opportunity）：承上述，「臨界值」也被用來決定使用者每次學習技能後獲得正面評價的機率，當臨界值為0.3時，代表使用者有三成的機會獲得正面性評價，每次正面評價則雙方的「行為酬賞」值皆隨機增值x（0＜x＜1），然後進行「期望值」的更新，如上期望值計算所述；反之，每次獲得負面評價時，自己的「行為酬賞」值皆隨機減值x（0＜x＜1），然後進行「期望值」更新。

二、實驗製作與結果

本研究在Jadex BDI代理人平台（http://vsis-www.informatik.uni-hamburg.de/projects/jadex/）之上開發一套網路社群群體犯罪模擬系統，藉以模擬網路社群使用者互動與聯繫行為，同時透過自動監控模組可以存取並記錄特定時間下每一個代理人的參數狀態與整體的網路拓樸結構。Jadex系統為德國漢堡大學資訊系所開發，Jadex是一套以Java語言為基礎之代理人開發環境，提供以BDI模式為基礎之目標導向代理人設計。在Jadex系統中，代理人的model必須以XML語言定義，其中以<beliefs>來定義代理人之信念，以<goals>來定義代理人之目標，以<plans>來定義代理人可選擇的計畫，而代理人所擁有的功能則以Java檔來撰寫，Jadex所提供的推論引擎將依據使用者所設計的代理人model去進行推論，並在適當的時候存取Java檔中的function。圖5為Jadex系統畫面，左上方框架中可以看到本研究所設計的三個代理人model：CommunityUser為一個社群使用者代理人model原型，UserGenerator代理人將基於CommunityUser的定義之上去產生並執行多個CommunityUser instance，在代理人執行互動演化的過程中，NetworkModule代理人則負責定時記錄每位代理人當下的beliefs狀態，以及當下的網路結構資訊。

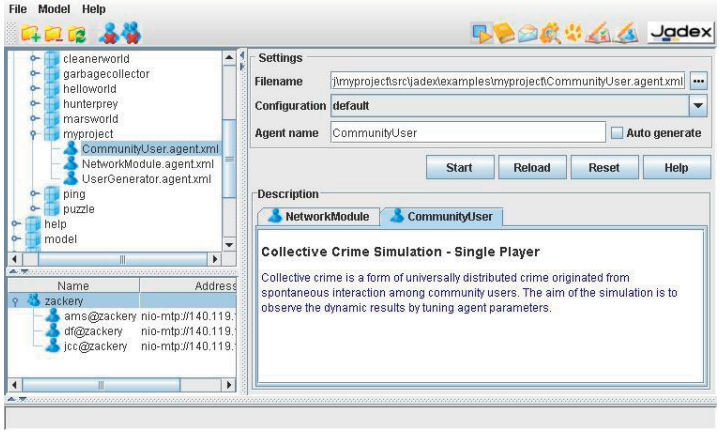

圖5：Jadex Platform

另外，本研究使用了一套社會網絡分析軟體UCINET （http://www.analytictech.com/downloaduc6.htm），在UCINET網路結構與節點的屬性資料是分開的，必須分別匯入才能夠將節點屬性資料與網路結構結合在一起，本研究在上述Jadex平台上讓NetworkModule代理人定時匯出每位代理人的beliefs資料與網路結構資料（矩陣），再使用UCINET將資料轉換成UCINET可以讀取的格式，並使用UCINET中的子程式NetDraw將網路結構給描繪出來，NetDraw也提供相當多的網路結構分析演算法。

（一）實驗結果

承上述實驗之目的與設計方法，本研究將分別進行三組實驗，模擬50, 100與130人之網路社群中，初始犯罪比率為5%與15%之情況下，探究使用者人數、初始犯罪率、網路結構與網路群體犯罪現象之關係。在模擬的過程中，代理人的參數值與網路結構皆不斷地變化與演進，為了能夠清楚地檢視與比較不同時間點下之結構性差異，下列三項實驗皆分別於代理人進行第60次與第120次演化時取樣分析，並就技能平均數（ACS）、網絡群聚係數、前10%使用者平均連結度，與連結度小於10之比率此四項特徵進行統計（表4-9）。

實驗一、使用者人數：50人，初始犯罪率（ICR）：5%，15%

表4：網路結構與網路群體犯罪現象之關係
—50人之網路社群中之第60次演化時取樣分析

	Size=50, ICR=5%	Size=50, ICR=15%
技能平均數（ACS）	1.7	2.5
群聚係數	1.85	1.31
前10%使用者平均連結度	29.6	22.6
連結度小於10之比率（%）	80	82

表5：網路結構與網路群體犯罪現象之關係
—50人之網路社群中之第120次演化時取樣分析

	Size=50, ICR= 5%	Size=50, ICR=15%
技能平均數（ACS）	2.4	4.2
群聚係數	2.24	2.19
前10%使用者平均連結度	33.8	25.6
連結度小於10之比率（%）	82	86

實驗二、使用者人數：100人，初始犯罪率（ICR）：5%，15%

表6：網路結構與網路群體犯罪現象之關係
—100人之網路社群中之第60次演化時取樣分析

	Size=100, ICR=5%	Size=100, ICR=15%
技能平均數（ACS）	1.8	4.2
群聚係數	1.43	1.29
前10%使用者平均連結度	36.6	26
連結度小於10之比率（%）	85	69

表7：網路結構與網路群體犯罪現象之關係
—100人之網路社群中之第120次演化時取樣分析

	Size=100, ICR=5%	Size=100, ICR=15%
技能平均數（ACS）	2.73	7.2
群聚係數	1.78	1.30
前10%使用者平均連結度	40.3	28.7
連結度小於10之比率（%）	89	76

實驗三、使用者人數：130人，初始犯罪率（ICR）：5%，15%

表8：網路結構與網路群體犯罪現象之關係
—130人之網路社群中之第60次演化時取樣分析

	Size=130, ICR=5%	Size=130, ICR=15%
技能平均數（ACS）	1.6	4.2
群聚係數	1.4	1.15
前10%使用者平均連結度	25.9	23.5
連結度小於10之比率（%）	77	73

表9：網路結構與網路群體犯罪現象之關係
—130人之網路社群中之第120次演化時取樣分析

	Size=130, ICR=5%	Size=130, ICR=15%
技能平均數（ACS）	2.7	8
群聚係數	1.54	1.39
前10%使用者平均連結度	31.6	28.7
連結度小於10之比率（%）	77	77

（二）實驗結果分析

1. 技能平均數

根據實驗一的結果顯示，當ICR為5%的時候，第60次演化的技能平均數為1.7，第120次演化的技能平均數為2.4；當ICR為15%的時候，第60次演化的技能平均數為2.5，第120次演化的技能平均數為4.2，如表 4與表5資料顯示，當使用者人數50人，ICR為15%時，犯罪技能平均數較ICR為5%時高出約1.3個技能數。

根據實驗二的結果顯示，當ICR為5%的時候，第60次演化的技能平均數為1.8，第120次演化的技能平均數為2.73；當ICR為15%的時候，第60次演化的技能平均數為4.2，第120次演化的技能平均數為7.2，如表6與表7資料顯示，當使用者人數為100人，ICR為15%時，犯罪技能平均數較ICR為5%時高出約平均3.4個技能數。

再看實驗三的結果，當ICR為5%的時候，第60次演化的技能平均數為1.6，第120次演化的技能平均數為2.7；當ICR為15%的時候，第60次演化的技能平均數為4.2，第120次演化的技能平均數為8，如表8與表9資料顯示，當使用者人數為100人，ICR為15%時，犯罪技能平均數較ICR為5%時高出約平均4個技能數。

由上述三個實驗資料比較顯示，犯罪技能擴散的速度（所需時間）不一而定，究竟犯罪技能擴散的速度受何種因素影響，可從兩大方向進行推論。在前述三個實驗六個表中，可發現當ICR為15%時技能平均數皆高於ICR為5%的技能平均數，此現象固然不能排除初始狀態先天之差異因素，然而有趣的現象是分別在三個實驗中，可觀察到第120次演化的技能平均數差異皆大於第60次的演化技能平均數差異：在實驗一中，當ICR為5時第120次演化的技能平均數（ACS = 2.4）與當ICR為15時第120次演化的技能平均數（ACS = 4.2）之差異為1.8，大於第60次演化的之差異0.8；在實驗二中，當ICR為5時第120次演化的技能平均數（ACS = 2.73）與當ICR為15時第120次演化的技能平均數（ACS = 7.2）之差異為4.47，大於第60次演化之差異2.4；在實驗三中當ICR為5時第120次演化的技能平均數（ACS = 2.7）與當ICR為15時第120次演化的技能平均數（ACS = 8）之差異為5.3，大於第60次演化之差異2.6。可見隨著演化次數越多技能平均數的差異越大，實驗一在ICR為5%時，第120次演化技能平均數為第60次演化的1.4倍，在ICR為15%時，第120次演化技能平均數為第60次演化的1.68倍；實驗二在ICR為5%時，第120次演化技能平均數為第60次演化的1.52倍，在ICR為15%時，第120次演化技能平均數為第60次演化的1.71倍；實驗三在ICR為5%時，第120次演化技能平均數為第60次演化的1.69倍，在ICR為15%時，第120次演化技能平均數為第60次演化的1.9倍。由上述資訊可發現當ICR為15%時，技能平均數增長的速率較ICR為5%時高，因此本研究認為犯罪技能擴散的速度的確受到ICR高低的影響，當ICR越高的時候犯罪技能擴散的速度也越快，反之，當ICR較低的時候犯罪技能擴散速度隨之減緩。

再從社群大小的觀點切入此一問題，亦可發現相當有趣的現象。當ICR固定為5%的時候，實驗一中第60次演化的技能平均數為1.7，實驗二中第60次演化的技能平均數為1.8，實驗三中第60次演化的技能平均數為1.6，似乎變化不大；而實驗一中第120次演化的技能平均數為2.4，實驗二中第120次演化的技能平均數為2.73，實驗三中第120次演化的技能平均數為2.7。從上述資料可發現當ICR為5%的時候，不論社群人數為50, 100或130人，第60次演化的技能平均數差異甚小、第120次演化的技能平均數亦近乎雷同。

當ICR固定為15%的時候，實驗一中第60次演化的技能平均數為2.5，實驗二中第60次演化的技能平均數為4.2，實驗三中第60次演化的技能平均數為4.2；而實驗一中第120次演化的技能平均數為4.2，實驗二中第120次演化的技能平均數為7.2，實驗三中第120次演化的技能平均數為8。從上述資料可以發現有趣的是與ICR為5%時截然不同的結果，當ICR為15%的時候，隨著社群人數越多，技能平均數也出現增加的趨勢。故本研究在此推論社群大小亦為影響犯罪技能擴散可能因素之一，然而有其情境條件：當ICR超越某一特定臨界值之後，使用者擁有的犯罪技能平均數與所屬社群人數成正向關係。

2. 群聚係數

當群聚係數越大則表示社群成員之間彼此相互認識的程度越高，內聚力越強，本研究採用的群聚係數公式如式子（三）所示：:

$$C_i = \frac{\text{number of triangles connected to vertex i}}{\text{numbers of edges connected to vertex i}} \qquad (三)$$

根據實驗一結果顯示，當ICR為5%的時候，第60次演化的群聚係數為1.85，第120次演化的群聚係數為2.24，當ICR為15%的時候，第60次演化的群聚係數為1.31，第120次演化的群聚係數為2.19。從上述資料中可以發現第120次演化的結果群聚係數皆高於第60次演化的結果，從實驗二與實驗三的實驗結果中亦可找到同樣的規則。此意謂演化的時間越長，社群使用者自我組織的現象將逐漸明朗化，此結果亦符合預期效果，由於前述實驗設計之規則將網路社群的使用者行為設定為具有50%的機率透過朋有去認識新的朋友，故隨著演化次數增加，群聚現象也愈來愈明顯。

然而，除了時間因素之外，群聚係數的大小變化是否有其他規則可循？非常巧妙地本實驗結果亦揭露另外一項有趣的規則：在實驗一第60次演化的結果中，當ICR為5%時群聚係數為1.85，較高於ICR為15%時的1.31；在第120次的演化結果中，當ICR為5%時群聚係數為2.24，亦較高於ICR為15%時的群聚係數2.19。在實驗二第60次演化的結果中，當ICR為5%時群聚係數為1.43，較高於ICR為15%時的1.29；在第120次的演化結果中，當ICR為5%時群聚係數為1.78，亦較高於ICR為15%時的群聚係數1.30。同樣地，在實驗三第60次演化的結果中，當ICR為5%時群聚係數為1.4，較高於ICR為15%時的1.15；在第120次的演化結果中，當ICR為5%時群聚係數為1.54，亦較高於ICR為15%時的群聚係數1.39。

從上述實驗數據中可以清楚地發現，ICR的高低對於群聚係數的高低有反向關係，當ICR越高則群聚係數越低，反之，當ICR越低時群聚係數越高。本研究試圖為此現象提出一合理解釋：由於當ICR只有5%時，網路社群中只有少數的使用者具備犯罪技能，其他透過後天學習習得犯罪技能的使用者無非透過兩種方式，一為是直接與犯罪者相連結，二來是間接從其他已習得部分犯罪技能的使用者的身上習得，不論是直接或者間接取得犯罪技能，這些犯罪者、習得犯罪技能的使用者之間彼此相互認識的機率非常大。倘若以學術圈為例，假設國內只有少數學者從事服務科學的研究，這些學者之間，不論是先進或是後學，這些學者彼此認識的機率非常大；相反地，假設國內從事電子商務的學者人數非常多，每一所大學裡都有很多學者從事電子商務的研究，則這些學者之間彼此相互認識的機率就比較低，對於後進學者而言可以習得知識的來源廣泛，其可能依其既有的人脈進入某一特定既有的群聚裡頭。同樣地，在網路社群中當ICR比率越高，表示擁有越多具備犯罪技能的犯罪者分散在網路結構中任何一個地方，因此各地皆可能形成中小型的群聚現象（分散式群聚），導致平均群聚係數較低於ICR比率較低的網絡。

小世界模型之理論認為小世界現象存在於Regular network與Random network之間，小世界現象相較於Regular network與Random network具有較高的群聚係數。一般而言均認為群聚係數越高越好，群聚係數越高的網絡，社群使用者的關係也越為緊密，並擁有較高的運作效率。依前述之概念，可設立一命題：群聚係數越高，則愈有利於犯罪技能的擴散（犯罪技能平均數愈高）；反之，群聚係數越低，則犯罪技能傳播之速度愈慢（犯罪技能平均數愈低）。反觀本實驗之數據，以表7為例，在100人的社群當中，當ICR為5%時群聚係數為1.78，犯罪技能平均數為2.73；而當ICR為15%的時候群聚係數只有1.3，犯罪技能數平均卻高達7.2，由上述實驗結果可見當群聚係數較高的時候，犯罪技能平均

數反而較低，此結果否定了前述命題—群聚係數越高，則愈有利於犯罪技能的擴散（犯罪技能平均數愈高）。故本研究認為前者「集中式的群聚」反而較不利於犯罪技能的擴散；反之，「分散式的群聚」有助於犯罪技能的擴散，子群聚之間透過弱聯結（Weak tie）來聯繫導致犯罪技能擴散所影響的範圍更為廣大。

再從社群大小的觀點來比較群聚係數之差異，當ICR固定為5%的時候，實驗一中第60次演化的群聚係數為1.85，實驗二中第60次演化的群聚係數為1.43，實驗三中第60次演化的群聚係數為1.4；當ICR固定為5%的時候，實驗一中第120次演化的群聚係數為2.24，實驗二中第120次演化的群聚係數為1.78，實驗三中第120次演化的群聚係數為1.54。從上述三次實驗結果中可以驚喜地發現，當固定ICR為5%的時候，比較相同演化次數下的群聚係數，在社群使用者人數越多的情況之下，群聚係數越低；相同地，在ICR為15%的時候，實驗一中第60次演化的群聚係數為1.31，實驗二中第60次演化的群聚係數為1.29，實驗三中第60次演化的群聚係數為1.15；在ICR為15%的時候，實驗一中第120次演化的群聚係數為2.19，實驗二中第120次演化的群聚係數為1.30，實驗三中第120次演化的群聚係數為1.39，其中除了實驗三中第120次演化的群聚係數未小於實驗二第120演化的群聚係數，大體而言還是吻合社群使用者人數越多則群聚係數越低的規則。

對於此現象，本研究提出以下可能的合理推測：以實驗一與實驗二ICR為5%時，第60次演化的結果為例，就連結機率的觀點而言（使用者主要還是透過朋有去建立下一個新的連結，再者是隨機選擇朋友），對於社群人數不論是50還是100的使用者而言，透過朋友去認識朋友對於群聚係數貢獻是一樣的，然而，在社群人數為50人的社群裡，使用者隨機去連結一個對象，結果使對象是剛好是朋友的朋友，或者是朋友的朋友的朋友的機率較當社群人數為100人的社群還要高，本研究此特性為意外相近性。倘若以實際生活例子而言，當研究者在政大認識一位新的朋友，結果後來才發現對方也班上某一位同學的朋友的機率，相較於研究者在台北市認識一位新朋友，結果發現對方是研究者某一朋友的朋友的機率還要高。倘若假設使用者只透過既有的連結去建立新的連結（無隨機選擇），則導致社群人數為100的社群群聚係數較低於社群人數為50的社群群聚係數的原因當然是使用者人數稀釋掉所造成。

3. 前10%使用者平均連結度

本研究實驗設計之規則假設當網路社群的使用者向外連結數量小於或等於5的時候，有50%的機率透過朋友來結交朋友，當朋友數量大於5的時候，有70%的機率與「行為酬賞」最低的朋友結束朋友關係。此設計之用意在於控制每一位使用者向外連結的數量在一定的範圍之內，然而在網路社群中的真實情境是，僅有相當少數特別受歡迎的網誌擁有極高的人氣，而大部分市井小民的網誌只有熟識的朋友才會來觀看。正如同Barabasi與Albert（1999）所提出的「Scale-free power law」網絡現象，許多大型的網絡系統與全球網際網路均為複雜網絡之典型代表，而這些複雜網絡共通之特性在於這些節點的連結度依循著scale-free power law的分佈。

Barabasi與Albert（1999）提出以「Preferential Attachment」概念來建構power law network的方法，當一個節點欲建立新連結的時候，每個節點被連結到的機率並不一

樣，原先已擁有越高連結之節點，被連結到的機率愈大。本研究假設前述的實驗情境均於符合power law分配的網路結構下，因此本研究之代理人設計運用透過朋友來結交朋友的機制，使得原本擁有較多連結的使用者，擁有更高被連結到的機會，以實現所謂「Preferential attachment」的概念。

為了觀察使用者連結度之特性，本實驗將社群裡前10%使用者之平均連結度納入衡量。根據實驗一的結果顯示，當初始犯罪率為5%的時候，第60次演化的前10%使用者平均連結度為29.6，第120次演化的前10%使用者平均連結度為33.8；當犯罪率為15%的時候，第60次演化的前10%使用者平均連結度為22.6，第120次演化的前10%使用者平均連結度為25.6。由上述實驗數據不難發現一簡單規則：在經過120次演化的網路結構下，前10%的使用者平均連結度高於只經歷60次演化前10%使用者的平均連結度，此規則同樣由實驗二與實驗三之實驗結果驗證。在實驗二中，當初始犯罪率為5%的時候，第60次演化的前10%使用者平均連結度為36.6，第120次演化的前10%使用者平均連結度增為40.3；當犯罪率為15%的時候，第60次演化的前10%使用者平均連結度為26，第120次演化的前10%使用者平均連結度為28.7；在實驗三中，當初始犯罪率為5%的時候，第60次演化的前10%使用者平均連結度為25.9，第120次演化的前10%使用者平均連結度為31.6；當犯罪率為15%的時候，第60次演化的前10%使用者平均連結度為23.5，第120次演化的前10%使用者平均連結度為28.7。

綜觀三個實驗結果，本研究初步發現：在相同人數的社群、同樣演化次數下，當ICR為5%時，其前10%使用者的平均連結度高於當ICR為15%時前10%使用者的平均連結度，依此規則，本研究推論ICR的高低與前10%使用者的平均連結度成反比關係。然而從本研究所收集的實驗數據中，尚未能回答為何在實驗三中，ICR為5%時，前10%使用者平均連結度明顯低於實驗二之前10%使用者平均連結度之原因。

4. 連結度小於10之比率

根據實驗一結果顯示，當ICR為5%時，經過60次演化，網絡中連結度小於10之比率為80%，經過120次演化，網絡中連結度小於10之比率為82%；當ICR為15%時，經過60次演化，網絡中連結度小於10之比率為82%，經過120次演化，網絡中連結度小於10之比率為86%，取其平均值為82.5%；在實驗二中，連結度數小於10的比率平均值為80%；在實驗三中，連結度數小於10的比率平均值則為76%。從上述三個實驗數據可發現連結度小於10的節點數佔社群人數約為80%上下，相對地，僅有少數的使用者擁有較高的連結度數，此極端分配之情形，似乎頗為符合power law之分配模式，本研究再進一步將實驗一、二、三中經過120代演化的網路結構中所有節點連結度之分佈情形以散佈圖方式顯示如下圖6至圖11，X軸表示某節點所擁有之連結度數，Y軸表示某節點之連結度數佔整體連結度之比率，結果發現連結度之分佈規則確實符合power law分配。依此實驗結果，本研究認為：不論演化的次數、不論社群人數之多寡或ICR值之高低，僅有少部分的犯罪者能夠擁有高度的連結，絕大多數的使用者或犯罪者其連結度數均不高。

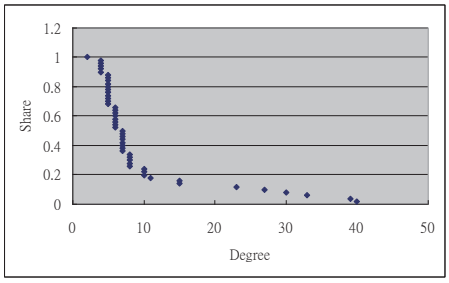

圖6：實驗一 Distribution function at Size=50, ICR=5%, 120th run

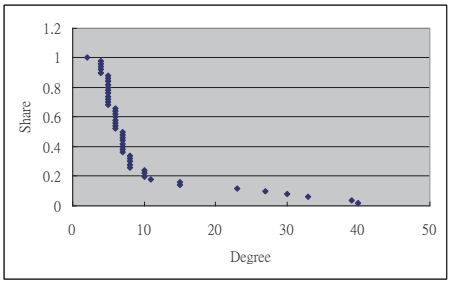

圖7：實驗一 Distribution function at Size=50, ICR=15%, 120th run

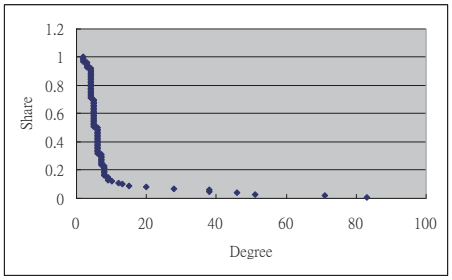

圖8：實驗二 Distribution function at Size=100, ICR=5%, 120th run

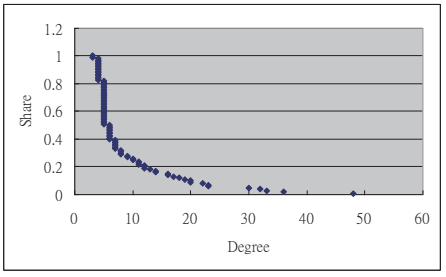

圖9：實驗二 Distribution function at Size=100, ICR=15%, 120th run

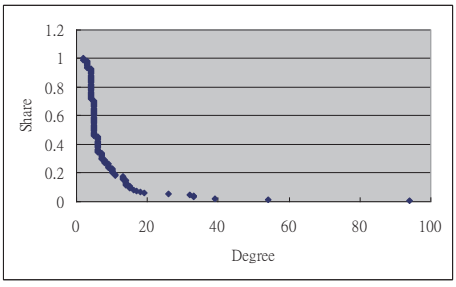

圖10：實驗三 Distribution function at Size=130, ICR=5%, 120th run

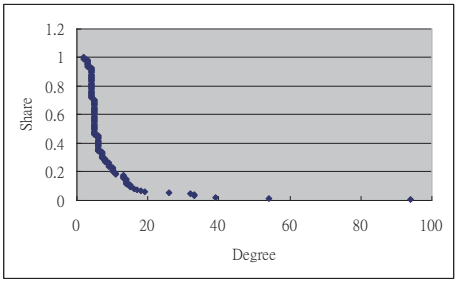

圖11：實驗三 Distribution function at Size=130, ICR=15%, 120th run

三、管理意涵討論

隨著Web2.0網路服務的盛行，越來越多的網路服務都試圖供創新、創意的服務給予使用者，與過去網路時代最為不同的是網站經營者極少介入服務本身，為了能夠讓服務內容更為多元化，於是乎讓使用者自己決定社群的內容，此為Web2.0網站相當大的特色—使用者貢獻內容。

Web2.0服務的種類繁多，大抵上而言共通之處在於提供使用者互動與協同合作的能力，換言之，Web2.0的服務即是以社會性為基礎之網路服務，回顧過去沒有網際網路的時代，或者Web1.0的網路時代，所謂「內容的本質」並沒有改變，直到Web2.0的概念

被提出與運用之後，改變了人與人的互動方式與內容的傳遞方式，因此本研究所探討的網路群體犯罪並非將問題定位於使用者的個人問題或者是使用者貢獻內容的問題，真正的問題在於網路社會之層次。為了解網路社群群體犯罪之現象，本研究將所謂使用者貢獻的內容之概念，對應於實驗模擬中的犯罪技能，犯罪技能的擴散意謂著網路社群上負面的行為訊息或是包含偏差資訊的內容之傳播。在模擬實驗中，本研究藉由控制網路社群之使用者人數（Size）與初始犯罪率（ICR）來觀察不同組合之下所演化的網路結構差異，並從四個衡量指標：犯罪技能平均數、群聚係數、前10%使用者平均連結度、連結度小於10之比率，標示不同網路結構下的特徵屬性，並對各種情境提出合理的解釋說明。根據本章實驗結果與分析，對於未來網路社群服務之經營管理可提出幾點啟示：

- 網路社群犯罪率控制之必要性：根據實驗結果顯示，當ICR為15%時，隨著演化次數增加，技能平均數增長的速率較ICR為5%時高，由此犯罪技能擴散的速度的確受到ICR高低的影響，當ICR越高的時候犯罪技能擴散的速度也越快，反之，當ICR較低的時候犯罪技能擴散速度隨之減緩。本研究藉由設定ICR為5%與15%以清楚展示其造成之差異性，然而並未進一步找出ICR的臨界值，在社群經營實務上，服務業者應要能善用資訊科技之能力，紀錄與分析社群使用者互動與網絡成長相關資訊，以找出犯罪率之臨界值，並將其控制在臨界值之下；正如同真實社會中，並不可能將黑社會份子完全消滅殆盡，然而亟需思考的是如何恰當管理才能夠維持社會的穩定性與正常發展。
- 網路社群大小對群體犯罪影響之大小：所有的網路社群服務經業者無不致力於擴展網路社群的大小，使得社群能夠累積足夠的使用者數量以充分發揮群體智慧與創造長尾效應之價值。然而，根據實驗結果顯示，社群大小亦為影響犯罪技能擴散可能因素之一，當ICR超越某一特定臨界值之後，使用者擁有的犯罪技能平均數與所屬社群人數成正向關係。想像倘若當社群的參與者越多，使用者擁有的平均犯罪技能數也越多，將落得一發不可收拾的下場。因此網路社群經營業者在犯罪率的測量與拿捏上實在必須用心思量。
- 群聚係數高低之兩難：在本實驗中，較小的ICR導致了「集中式的群聚」現象與較高的群聚係數，卻不利於犯罪技能的擴散；反之，較高的ICR導致了「分散式的群聚」現象與相對較低的群聚係數，卻使得使用者所習得的犯罪技能數增加。就群體智慧的觀點而言，分散式群聚乃一般社群經營業者所追求的理想目標，分散式群聚有助於子社群之間知識、訊息的傳遞與擴散，使得群體智慧的組織、知識與技能的動員更有效率，成效更佳。然而水可載舟亦可覆舟，在分散式群聚的網路結構之下，負面的行為訊息或是包含偏差資訊的內容也更容易快速地擴散。因此，群聚係數的高低正如同一把雙面刃，網路社群服務經營業者在追求分散式群聚係數越高的同時，也意謂負面的行為訊息或是包含偏差資訊的內容將更普遍地為使用者所接觸。對此本研究認為網路社群服務經營業者可依社群成員的行為歷史資料將成員視為兩個社群，對於一般使用者社群追求「分散式群聚」係數的極大化，並同時對於具有負面行為資訊的使用者社群追求「集中式群聚」係數的極大化，究竟如何操作才能達此境界仍需業者之努力與經營智慧。

伍、結論

Web2.0的網路服務在服務的設計上鑲嵌了社會性功能，使得社群使用者更能夠善加利用網路科技本身所提供的能力，在社群的平台之上相互交流並激發各種炫麗的火花，然而如何善用群體智慧來促成網路社群服務的創新與成功，至今仍無一套可以依循的法則與經營模式，雖然如此仍有許多業者對於網路社會潛藏龐大的商機而躍躍欲試。事實上，網路社會變動與演進的速度均遠遠超越了真實社會，並存在許多網路特有的文化與現象，也因為其變動性與複雜度，使得網路社群服務的經營充滿了高度不確定性。

所謂水可載舟，亦可覆舟，正當眾人注目於群體智慧力量不可思議的同時，本研究反面思考群體力量帶來的社會問題—「網路群體犯罪」，群體犯罪不同於組織犯罪般有結構的犯罪團體，亦非為了追求共同利益而合作的共犯夥伴，而是網路使用者自發性互動行為下逐漸浮現的群體近似犯行為。群體犯罪問題普遍存在於當今各式各樣的網際網路社群，以各種不同的樣貌與形式展現出來，例如國內著名的無名小站上，使用者私底下相互學習不用付費就讓網誌播放音樂的方法，Yahoo奇摩拍賣上許多買家運用一些小技巧來規避手續費，以及全球知名的網路影音社群YouTube上，使用者上傳未經授權的影音等問題。

本研究所探討的網路群體犯罪並非使用者的個人行為問題，或是貢獻內容的問題，而是將群體犯罪視為一種社會問題，因此相當不同於現有的犯罪行為實證研究 - 針對某一種特定的犯罪行為或犯罪事實，來分析犯罪的型態、類別、方法、犯罪者特質、犯罪動機與犯罪模式。面對此特別之議題，本研究借用Sutherland與Cressey（1978）提出之差別接觸理論與Bandura（1977）提出之社會學習理論為基礎，從社會學之觀點為網路群體犯罪行為提出初步的質化詮釋，而後在此基礎之上建構網路群體犯罪之代理人模擬模型。代理人模擬經由微觀層次的動態模擬，可模擬許多複雜的現象並提供高度的實驗彈性，本研究使用BDI代理人架構來模式化群體犯罪中代理人決策的過程與社會互動關係，以信念、期望與意圖三種抽象化的心理屬性表示網路社群使用者意念上之資訊狀態、動機狀態與慎思狀態，其中信念乃所有推論的基礎，此模型以五個信念來區別每一個使用者意念之差異，分別為Satisfaction、Expected_efficacy、Willing_to_learn、Required_crimeskills與Opportunity，每個使用者這五個信念的值可能不一樣，因此最後導致不同的行為產生。

為了更進一步了解網路群體犯罪現象之特色，本研究於Jadex代理人開發平台上實作群體犯罪代理人模擬系統，在模擬實驗中，本研究藉由控制網路社群之使用者人數（Size）與初始犯罪率（ICR）來觀察不同組合之下所演化的網路結構差異，並從四個衡量指標：犯罪技能平均數、群聚係數、前10%使用者平均連結度、連結度小於10之比率，標示演化之網路結構的特徵。本研究之群體犯罪預防功能乃由一隨著時間動態演化的網路，以及運用上述四個指標對此演化網路進行之分析所構成。研究結果發現：（1）犯罪技能擴散的速度受到ICR高低的影響，當ICR越高的時候犯罪技能擴散的速度越快，反之，當ICR較低的時候犯罪技能擴散速度隨之減緩。（2）當ICR超越某一特定

臨界值之後，使用者擁有的犯罪技能平均數與所屬社群人數成正向關係。（3）ICR的高低對於群聚係數的高低有反向關係，當ICR越高則群聚係數越低，反之，當ICR越低時群聚係數越高。（4）社群使用者人數越多的情況下，群聚係數越低。（5）前10%使用者的平均連結度有隨著演化次數逐漸增加的趨勢。（6）ICR的高低與前10%使用者的平均連結度成反比關係。（7）不論演化次數、社群人數多寡與ICR值之高低，均僅有少數犯罪者擁有高度的連結，絕大多數的使用者或犯罪者其連結度數均不高（符合power law分佈）。

在眾人齊聲歌頌Web2.0世界的美好與希望，僅只著重於效益而未見問題日益嚴重的同時，本研究率先做為探討負面現象的先驅者，希冀能夠引發產界與學界對此一議題更多的重視與關懷。

本研究之未來可供後續發展之方向包括：

- 本研究為一先導型研究，運用犯罪學與社會學相關之理論基礎，為網路群體犯罪現象提供基礎之論述，以作為代理人模擬之基礎，然而對於網路群體犯罪現象並未進行更深度的剖析與質性的探討，這此一方面仍有待更多社會科學研究者的加入與的努力。
- 在本研究實驗中，受限於電腦運算資源，因此最多只能進行至130人的模擬試驗，未來應可就更多人數之社群進行實驗，或許可有不同之發現。另外，本實驗所僅只模擬單一社群，然而真實網路社會中的使用者往往跨足多個網路社群，問題可能更為複雜，亦值得未來深入研究。
- 本研究提出一套網路群體犯罪代理人模擬模型，並從微觀的模擬與巨觀的網路結構分析網路群體犯罪現象，未來可基於此基礎之上進行網路群體犯罪之控制方法，以達到有效減少與預防網路群體犯罪之目的。

參考文獻

1. 林山田、林東茂、林燦璋，2005，犯罪學（三版），臺北：三民。
2. 邱議德，民92，以社會網路分析法評估工作團隊知識創造與分享，國立中正大學資訊管理研究所碩士論文。
3. 范國勇，民94，網路犯罪成因與防治對策之研究，內政部警政署刑事警察局委託之專題研究報告。
4. 林宜隆，2007，網際網路與犯罪問題之研究（修訂三版），中央警察大學。
5. Bandura, A. *Social Learning Theory*, Prentice-Hall, New Jersey, 1977.
6. Barabasi, A.L., and Albert, R.“Emergence of Scaling in Random Networks,”*Science* (286:5439), 1999, pp. 509-512.
7. Bosse, T., Jonker, C. M., Van der Meij, L., and Treur, J.“LEADSTO: A Language and Environment for Analysis of Dynamics by SimulaTiOn,”in *Proceedings of the Third German Conference on Multi-Agent System Technologies*, 2005.

8. Bosse, T., Memon, Z. A., and Treur, J. "A Two-Level BDI-Agent Model for Theory of Mind and its Use in Social Manipulation," in P*roceedings of the Artificial and Ambient Intelligence Conference*, 2007, pp. 335-342.
9. Bratman, M. E. Intentions, *Plans, and Practical Reason*, Harvard University, Cambridge, 1987.
10. Bratman, M. E., Israel, D. J., and Pollack, M. E. "Plans and Resource-Bounded Practical Reasoning," *Computational Intelligence* (4:3), 1988, pp. 349-355.
11. Clarke, R. V. "Technology, Criminology and Crime Science," *European Journal on Criminal Policy and Research* (10:1), 2004, pp. 55-63.
12. Ferber, J. *Multi-agent Systems: An Introduction to Distributed Artificial Intelligence*, Addison-Wesley Longman, New York, 1999.
13. Georgeff, M. P., and Lansky, A. L. "Reactive Reasoning and Planning," in *Proceedings of the Sixth National Conference on Artificial Intelligence*, Seattle, 1987, pp. 677-682.
14. Georgeff, M. P., Pell, B., Pollack, M. E., Tambe, M., and Wooldridge, M. "The Belief-Desire-Intention Model of Agency," in *Proceedings of the Fifth International Workshop on Intelligent Agents V: Agent Theories, Architectures, and Languages*, 1998.
15. Kinny, D., Georgeff, M. P., and Rao, A. "A Methodology and Modeling Technique for Systems of BDI Agents," in *Proceedings of the Seventh European Workshop on Modeling Autonomous Agents in a Multi-Agent World*, Eindhoven, 1996.
16. Latora, V., and Marchiori, M. "Economic Small-World Behavior in Weighted Networks," *The European Physical Journal B - Condensed Matter and Complex Systems* (32:2), 2003, pp. 249-263.
17. Levy, P., and Bononno, R. *Collective Intelligence: Mankind's Emerging World in Cyberspace*, Basic Books, 2007.
18. Lin, D., Wiggen, T. P., and Jo, C.H. "A Restaurant Finder Using Belief-Desire-Intention Agent Model and Java Technology," in *Proceedings of the Eighteenth International Conference on Computers and Their Applications*, 2003, pp. 404-407.
19. McShane, M. D., and Williams III, F. P. *Criminology Theory: Selected Classic Readings* (2nd ed.), Anderson Publishing, Cincinnati, 1998.
20. Newman, M. E. J. "The Structure and Function of Complex Networks," *SIAM Review* (45:2), 2003, pp. 167-256.
21. Rao, A. S., and Georgeff, M. P. "BDI Agents: From Theory to Practice," in *Proceedings of the First International Conference on Multi-Agent Systems*, San Francisco, 1995, pp. 312-319.
22. Sutherland, E. H., and Cressey, D. R. *Criminology* (10th ed.), Lippencott, Philadelphia, 1978.
23. Watts, D. J. *Six Degrees: The Science of a Connected Age*, W. W. Norton & Company, New York, 2003.

24. Young, H. P. "Innovation Diffusion in Heterogeneous Populations: Contagion, Social Influence, and Social Learning," *Care Services Efficiency Delivery Working Paper No.51*, 2007.