臺灣警察專科學校警專學報，民國 105.04
第六卷第三期：17-34 頁

新興網路跨境犯罪的類型框架及發展趨勢探析[1]

The Categories and Trends of Newly-Emerged Cross-Border Cybercrime

汪子錫[2]

Wang Tzu-Hsi

摘要

本研究以兩岸四地「新興網路跨境犯罪」類型化為目的，並從網路跨境犯罪歷史分析未來趨勢，以作為警務機關制定治理策略的參考。新興網路跨境犯罪（newly emerged cross-boarded cybercrime）的特性包括犯罪者利用網路匿名、不在場犯案、不受地域限制犯案、易於操作等特性，將網路犯罪歷程切割在不同境域實施，達到湮滅證據，有效降低被追捕、被起訴、被刑罰的風險等。「跨境」成為網路犯罪必然發展方向，隨著電子商務全球擴展，為網路跨境犯罪提供絕佳的機會。新興網路跨境犯罪的發展路徑，是依附於新興網路日常生活功能而出現。當新的網路功能被提出來，並運用於日常生活的時候，通常就是犯罪者啟動犯罪腳本，並將電腦網路電信等工具融入犯罪歷程的時機。本研究建議兩岸四地跨境網路犯罪的防制策略包括：警務司法合作追懲、犯罪斷底措施、第三方合作預防策略。

關鍵字：新興犯罪、網路犯罪、網路跨境犯罪

Abstract

This study aims at the categorization of newly-emerged cross-bordered cybercrime from four regions across the Strait, and forecasts future trends based on the historical development of cybercrime as a reference for the police department. Newly-emerged cross-border cybercrime indicates that the criminals take advantage of the anonymousness on the Internet, and commit crimes without region restrictions in separate locations to

[1] 本文獲選「第十屆海峽兩岸暨香港、澳門警學研討會」發表論文，該次研討會於 2015 年 10 月 13 至 15 日於台北市文華酒店舉行。

[2] 現職：中央警察大學通識教育中心教授 電子信箱：wangtzuhsi@yahoo.com.tw

create an alibi, destroy evidence, and avoid being arrested and punished. As E-business has been further expanded globally, cross-border crime is becoming an inevitable trend, creating opportunities for cybercriminals. The development of cybercrime depends on the evolution of the Internet. When a new function is created and adopted, it is also the time that the criminals start planning to commit crimes using the Internet. This study raises three suggestions for cybercrime prevention in four regions across the Strait: First, the police shall work with judicial system to prevent crimes. Second, primary crime prevention is needed to protect personal information. Last but not least, business and Internet experts shall be invited to join the process of law enforcement.

Keywords: Newly-Emerged Crime, Cybercrime, Cross-Boarded Cybercrime

壹、前言

台灣社會最早出現「新興犯罪」（newly-emerged crime）名詞，是在 2002 年 11 月由中央警察大學、中華民國犯罪學學會、中正大學聯合舉辦的「新興犯罪議題與對策」學術研討會提出。這是台灣犯罪學研究者在進入 21 世紀初期，觀察到社會出現了異於傳統犯罪的現象所做的回應。該次研討會舉出六項新興犯罪類型，包括「新興毒品與青少年藥物濫用」、「擄車勒贖」、「開放觀光賭場」、「網路援交」、「性侵害」、「中途輟學與少年犯罪」等[3]。可以看出，2002 年台灣的「新興犯罪」泛指新型態犯罪或「傳統犯罪新手法」，並不專指網路新興科技犯罪（cybercrime）。

台灣網路發展從雅虎奇摩（YahooKimo）於 1994 年提供免費信箱服務後，個人使用者開始顯著成長，並且迅速普及。面對新傳播科技，政府的輔導管理措施始終付之闕如，直到 2003 年才有網路位址及網域名稱註冊相關管理法規，也要到 2004 年才成行政院通訊傳播委員會（NCC），作為網路、傳播、資訊匯流業務的主管機關。

時至 2015 年，在論及「新興犯罪」時，通常將其意涵與「網路犯罪」（cybercrime）連結，因而出現「新興網路犯罪」（newly emerged cybercrime）的說法。「新興網路犯罪」的工具從單純網路犯罪，擴大到移動通信、社群媒體、自動櫃員機（ATM）、Web ATM、網路銀行等資通工具，開始大量、普遍出現在犯罪過程之中。

[3] 徐彩媚，〈新興犯罪議題與對策研討會〉，《台灣新聞報》第 15 版，2002 年 11 月 22 日。

新興網路跨境犯罪（newly emerged cross-boarded cybercrime）是犯罪者利用網路匿名、不在場犯案、不受地域限制犯案、易於操作等特性，將網路犯罪歷程切割在不同境域實施，達到湮滅證據，有效降低被追捕、被起訴、被刑罰的風險。「跨境」成為網路犯罪者「理性選擇」必然的發展方向，尤其在全球化電子商務發展下，更為網路跨境犯罪提供絕佳的機會。

從犯罪學理性選擇理論（Rational Choice Theory）來看跨境電信詐騙犯罪，足以解釋為什麼此類犯罪會迅速發展並且氾濫成災。依據「理性選擇理論」的見解，電信詐騙犯罪與日常活動具有密切關係。犯罪者認知到目標的心理弱點，並且著重於尋找或掌握目標物的便利，因此他們會選擇了可以接近或是開放的、容易逃脫的地方來犯罪。只要犯罪目標愈適當或愈容易接近，犯罪就愈可能發生。當犯罪過程是「低成本、獲利高、風險低、刑度輕」的話，那麼，犯罪發生的機率就更高[4]。而新興媒體的網路通訊、智慧型手機、行動載具，恰好提供了犯罪者「便於接近目標」的特性。

在 2003 年以後，台灣社會有組織的跨境詐騙集團逐漸成型，犯罪者大量蒐購人頭電話及帳戶，並以最新時事編造各種誘騙劇本，利用電子金融服務轉帳匯款功能，進行大規模電信詐騙犯罪。犯罪得手後的金錢，也開始經由多國或多人帳戶洗錢，方面隱匿犯罪所得，一方面逃避追緝[5]。

在 2008 年之後，兩岸四地開始頻繁的經貿、文化交流，大量的人流、物流、金流、資訊流往來，提供更多機會讓新興網路犯罪發展出更多類型。

2015 年 1 月，大陸騰訊互聯網所屬單位，首次公布有關於大陸地區新興網路犯罪結構化的研究報告。這項名稱為《2014 年雷霆行動網絡黑色產業鏈年度報告》的研究指出，網路全球化電子商務交易盛行後，依附於電子商務交易過程的犯罪，已成為犯罪集團覬覦的目標；某些網路犯罪形成獨特的產業結構，透過完整的分工與利用大量的假帳號，找出程式漏洞、撰寫木馬程式、偷取帳號到轉賣獲利，已自主形成可運作的犯罪產業鏈。

騰訊研究報告提出了三種主要的「黑色產業鏈」，包括以技術為主的駭客、社交工程為主的詐欺、以及涉及黃賭毒的網路犯罪。報告顯示，2014 年網路黑色產業鏈呈現的趨勢有：集團化、產業化；更傾向於攻擊手機；冒充熟人或博取同

[4] 汪子錫、章光明，〈警察犯罪預防政策行銷的理論與實例探析〉，《警學叢刊》第 43 卷第 6 期，2013 年，pp.47-67。

[5] 黃茂穗，〈反詐騙 165 專線的現況與未來〉，下載日期：2013 年 6 月 30 日。網址：http://www.ntpu.edu.tw/gradcrim/temp/I_F_20080926145540.pdf

情等手法，依附人際脈絡欺詐[6]。

台灣、大陸和香港、澳門四地具備語言文字、鄉親血緣親近性，文化與生活習慣也類似，因此出現「犯罪工具科技化」、「文化親近導致犯罪便利性」以及「跨境合作詐騙犯罪」三項犯罪特徵。兩岸四地之間出現的詐騙手法，很容易從在地犯罪複製型態到另一地進行；詐騙者也可能採取切割犯罪歷程（offence process）的手法，在兩岸四地分工完成詐騙取財[7]。

本研究以台灣地區報紙新聞爲樣本，採取新聞框架分析（Frame Analysis）研究途徑，將「新興網路犯罪手法」列為關注的核心，從網路犯罪新聞檢視犯罪手法創新變異的演變軌跡，並以犯罪的「框架故事」歸納犯罪型態。在研究結論建議中，則提出研究者對於新興網路跨境犯罪未來趨勢的研析，以及治理對策建議。

網路犯罪不斷變異更新，經常使執法人員疲於奔命，或查緝無效的窘況。從新興犯罪發展剖繪出軌跡，有助於擬定預防性跨境治理對策。面對新興網路跨境犯罪發展日炙的情況，需要以跨境治理的思維，透過各地執法機關共同合作才易取得成效。

貳、問題描述與研究概念

一、犯罪學相關理論

犯罪學的理性選擇理論（rational choice theory）、被害者學理論（victimology）可用於詮釋詐騙犯罪的研究。

（一）犯罪學的理性選擇理論

理性選擇理論為「犯罪是理性計算後的決策所選擇採取的行為」。此理論基本闡釋了犯罪者所考量的犯罪計畫必須是風險小、成本低、利益大而且方便操作。

美國學者 Siegel 在其犯罪學一書中提到：違法行為發生在一個人考慮了「個人需求因素」以及「情境因素」後所作成的冒險決定。「個人需求因素」包括獲取金錢、報復仇恨、感受刺激，甚至自我娛樂等；而「情境因素」則是指目標物受到保護及當地警方的效率等。如果潛在犯罪人事先計算犯罪所得的報酬合於需要，他們就可能會選擇去犯罪。因此，預防犯罪工作，必須要使潛在犯罪人瞭解

[6] 騰訊互聯網與社會研究院，〈2014 年騰訊雷霆行動網路黑色產業鏈年度報告〉來源：http://law.tencent.com/Article/lists/id/3557.html，取得日期：2015 年 5 月 25 日。

[7] 汪子錫，〈從輿論分析兩岸合作打擊電信詐騙犯罪的成效與今後展望〉，《展望與探索》第 12 卷第 5 期，2014 年，pp.33-49。

到，犯罪的後果是「高成本且低報酬的」。[8]

依據理性選擇理論所提到犯罪的構成（structuring crime）三種選擇因素來看，詐騙集團可能的考量有三項，即選擇犯罪的地點（choosing the place of crime）、選擇目標（choosing targets）、學習犯罪技巧（learning criminal techniques）等。

（二）被害者學**理論**

被害者學是從犯罪者研究轉換主體，探討為什麼有些人會被害，有些人就不會。美國學者 Sparks R.F.提出「個體若擁有較多之被害因素，則容易因此遭遇被害，甚至具有被害傾向，重複遭受被害」，並可區分為七項因素。[9]

1.激發或挑惹因素（precipitation or provocation）：被害者之言語或行為激發加害人犯罪之動機。

2.促進因素（facilitation）：被害人因為無知、故意、愚蠢等態度而陷入被害之情境。

3.弱點或誘發因素（vulnerability or invitation）：被害人因其個人特性具有弱點而較容易被害。

4.合作因素（cooperation）：被害人是經由合意之犯罪被害，例如合作投資詐騙案即屬此例。

5.機會因素（opportunity）：被害者處於有利被騙的情境而使歹徒有機可乘。

6.吸引因素（attractiveness）：被害者具有吸引加害者犯罪之吸引性，例如傳播妹、假援交或酒店叩客等詐騙，都以情色作為吸引。

7.免罰因素（impunity）：多數小金額損失的被害者傾向不報案，以致於犯罪者不被追究，又或者是即使詐騙所得已超過億元，但被刑罰等程度極為輕微，甚至還能緩刑，根本無關痛癢，就會造成詐騙犯罪繼續發生，犯罪者坐大。

二、網路與詐騙防制相關文獻

（一）網路犯罪特性

1.隱匿、即時、便捷

20 世紀晚期，商業組織、政府組織以及個人，在電腦網及網路運用上已大幅度普及化，全世界大多數地區都已進入資訊時代（Information Age）

[8] L. J. Siegel, ***Criminology.***（West/Wadworth Publishing Co.,2003）

[9] R.F.Sparks, "Multiple Victimization: Evidence, Theory and Future Research. "***Journal of Criminal Law and Criminolog.*** 1981.72, 762–788.

[10]。以時程來看，21 世紀末，已經是新興網路犯罪網路出現的良機；誕生於資訊社會的網路犯罪，還在繼續成長、壯大之中。

資訊社會大量運用各種網路設備，信息傳遞較其他媒介更為迅速、方便，開始迅速朝向虛擬網路交易發展。由於使用網路具有隱匿性、即時性、方便性，讓越來越多的人樂於使用；與此同時，網路的隱匿性、即時性、方便性，也被犯罪者覬覦運用。

2.易於創新變異新樣態、新犯罪腳本

網路犯罪基本上依附網路不斷創新變異，因此本身就具備功能創新的潛在能力與屬性，造成網路犯罪隨時可以出現新的樣態、新的犯罪腳本。網路犯罪的特色之一，是時時翻新，造成個人或組織乃至於政府，難加預防而受到損害。雖然防堵措施一一被提出，但也被犯罪者一一破解，造成執法者疲於奔命的現象，網路犯罪一直持續地挑戰世界各地的執法人員。

網路犯罪型態不只有經濟型犯罪，還有隱私權、名譽權、霸凌、虛擬性侵害等多種類型，但是普遍、大量且持續的犯罪行為，仍以獲利為目的的經濟型犯罪為主。Castell 在全球化犯罪經濟學（global criminal economy）概念中指出，網路成為經濟犯案的極佳中介工具，網路的功能與特質促使衍生更多樣化的犯罪形式，讓聯絡、溝通、物色被害人變得更加便利[11]。

（二）網路犯罪類型

網路犯罪隨著時間推移以及創新網路工具，網路犯罪類型也隨之變異，各種不同的分類方法，有些是就工具區分類型，有些從犯罪環境區分類型，有些則以犯案歷程或手法區分類型。2001 年 Wall 出版《犯罪與網路》（*Crime and the Internet*），將網路犯罪區別為四種類型，係就網路工具來區分類型[12]。

1.隱私侵犯型（Cyber trepass）：此類型是新工具、新犯罪的形態，新犯罪包括散布電腦病毒、竄改網頁、竊取密碼或資料、攻擊癱瘓他人主機或其他軟體。

2.網路色情型（Cyber obscenity/pornography）：此類型是新工具、舊犯罪的型態。以色情圖片、視頻引誘購買違禁色情資料以及媒介色情交易。

3.網路竊盜型（Cyber theft）：這是新工具用於新舊之間犯罪的型態，例如盜

[10]M. Williams, *Virtually Criminal.* （London: Routledge.2006）
[11]M. Castells, *The Rise of the Network Society.* （ Cambridge, MA : Blackwell Publishers.1996）
[12]D.S. Wall, *Crime and the Internet.* （New York :Routledge. 2001）

版、竄改網路銀行數據、盜刷信用卡等。

4.網路暴力型（Cyber violence）：此類型是新工具用於帶有強制脅迫性質的犯罪型態，例如網路跟蹤（stalking）、虛擬強暴（Virtual rape）等。

我國法務部在 2002 年時，曾經依據台灣已發生的案例，將網路犯罪區分為二種類型[13]：

1.以電腦為犯罪客體類：

（1）入侵型犯罪：利用網路入侵他人電腦，在網路上冒用他人帳號密碼、盜取資訊服務、偷窺系統內容。

（2）施放病毒：散布電腦病毒，使他人電腦檔案毀損或硬碟格式化。

（3）垃圾郵件。

2.利用網路服務電腦犯罪類：

（1）網路色情：張貼色情圖片、提供色情影片連結網站、販售色情光碟、媒介色情交易。

（2）網路賭博。

（3）網路販售違禁、管制物品，如禁藥、毒品、槍械。

（4）網路詐欺：如虛設行號、盜刷信用卡、網路老鼠會、妨害名譽、妨害秩序、恐嚇取材。

2014 年內政部刑事警察局在犯罪預防宣導時，以簡易淺釋方式，依犯罪發生環境將網路犯罪區分為二種類型[14]：

1.以電腦作為犯罪之場所類

以電腦作為犯罪場所，是指犯罪行為是在電腦上進行、發生。例如在電子佈告欄（BBS）上，誹謗或公然侮辱他人；又如藉著網路散布或販賣猥褻圖畫。因為網路快速大量傳播的特性，在虛擬場所所作的犯罪行為，其對社會傷害往往比在實體場所來得大。

2.以電腦作為犯罪之客體類

網路相對於傳統的犯罪行為客體而言，是一種新的犯罪客體。電腦駭客入侵他人網路系統並施放病毒，即屬新興犯罪。利用網路新工具也會進行傳統犯罪，例如駭客入侵綁架電腦程式，要求交付贖金，可能構成傳統的恐嚇取財罪。

[13]楊肅民，〈防制網路犯罪刑法擬訂專章〉，《中國時報》第 8 版，2001 年 8 月 25 日。

[14]內政部刑事警察局「犯罪預防寶典」https://www.cib.gov.tw/Crime/Detail/981。取得日期：2015 年 6 月 1 日。

（三）跨境犯罪類型

全球化促更多商業貿易朝向自由化發展，在商品、服務、資金及勞力需要開放流動時，各國紛紛降低或免除邊境障礙來配合環境的變遷[15]。但是各地執法單位如果不能有效合作，就可能因為各地法律規範的差異、執法的侷限，反而為跨境組織犯罪提供保護傘[16]。

在跨境犯罪的類型部份，Albanese 將跨境犯罪歸類為主要三種類型：

1.提供非法商品（provision of illicit goods）：毒品販運、銷贓、偽造貨幣。

2.提供非法服務（provision of illicit services）：人口販運、網路犯罪與詐欺、商業犯罪、色情產業等。

3.駭客對企業或政府的滲透（infiltration of business or government）：勒索、詐騙、洗錢、貪汙等。

Albanese 的跨境犯罪分類，偏重經濟、組織犯罪，而非傳統個人或政治動機所犯下的罪行。跨境犯罪組織不一定包攬跨境犯罪的全部作為與過程，在理性選擇下，犯罪者採取有利於己的合作，並與他人分享獲利。Shelley 在其「美國境內的跨境性組織犯罪」的研究顯示，可以參與及分享的對象，不僅限於幫派組織或不法集團，一些政府官員也進入犯罪共生系統[17]。

前述網路犯罪的分類方式，因為出發點並不一致而未盡相同，但是不同的分類方式，都具有可供參考的價值。本研究進行分類的出發點係提出兩岸四地警務人員合作治安治理的參考，因此為了符合研究目的，選擇以「新興犯罪手法」，也就是犯罪歷程（offence process）作為類型框架化的核心。

在「網路跨境犯罪」部份，本研究以為網路犯罪可能具備地域特性，或許出現在地（*Location*-based）發生的情況，但是依網路特性與本質，在地網路犯罪的必然性就是「複製犯罪手法」、「跨境犯案」。全球化（globalization）為網路跨境犯罪培育了極佳的犯罪結構，在全球化電子商務的行動框架（frame）中，任何一個資訊流（Information Flow）、金流（cash flow）、物流（good flow）過程，一旦被駭客攻擊掌握，就有被可能成為網

[15] J. S. Albanese, Transnational Crime in the 21st century: Criminal Enterprise, Corruption and Opportunity.（New York: Oxford University Press.2011）

[16] 林山田、林東茂、林燦璋，《犯罪學》，（台北：三民，2008）。

[17] S L.L. helley, “Transnational Organized Crime In The United States,”Kobe University Law Review,32（1）: 77-91.1998.

路犯罪的目標。

參、研究設計

一、框架分析

新聞框架概念（news framing）將框架定義為「成組或成群的訊息或有意義的行動」[18]。無論是議題設定、涵化理論、框架概念，都解釋了媒介具有製造輿論與引導輿論的能力。本研究以新聞框架分析（Frame Analysis）為研究取徑，以犯罪歷程創新變異為「核心框架」，藉以發展出網路犯罪的類型化。

框架分析和內容分析法(Content Analysis)都是以新聞內容爲樣本的研究方法，也都著重從新聞內容歸納出意義所在。不過框架分析偏重運用媒介文類（media genres）概念，文類包含種類（kind）、型式（type）、範疇（category）的意思，研究者可以閱讀文本（text）後建構出參考框架，也就是建構一組訊息，一組指涉有意義的行為認知[19]。內容分析法則是結合量化統計以及質化分析的程序，藉以解釋新聞意義的研究方法[20]。

Goffman 在 1974 年發表《框架分析》（*Frame Analysis*）一書，提出運用框架來詮釋人們溝通（communication）時的情境概念。框架的作用在於幫助人們理解符號互動。框架可以做為社人的社會心理參考架構，也可以作為詮釋外在世界的基模（scheme）[21]。

框架的概念被援用在媒體內容研究，Gamson & Modigliani 指出：「媒體在描繪社會議題的同時，除了呈現較複雜的敘述與論證之外，也需要用具體簡潔的框架象徵來突顯議題」[22]。

新聞故事框架，也稱為新聞故事結構，是在各種複雜的故事場景中，聚焦於一個最重要的中心議題。雖然新聞故事是由不同的行動者（受訪者、發言人、記者等）來提供框架元素。但是基於媒介特性，也會決定讓哪個行動者的詮釋話題被顯著再現。這種被凸顯的框架可稱為「核心框架」，也就是媒介議題框架的核

[18]J. W. Tankard, & Others. “ Media Frames: Approaches To and Conceptualization Measurement.”Paper Presented to Communication Theory and Methodology Division,（Boston. 1991).

[19]G. Bateson, Steps to the ecology of mind. （New York : Ballantine Books. 1972）

[20]R. D. Wimmer, & , ,J. R. DominickMass media Research :An Introduction.（CA : Wadsworth. 1994）

[21]E.Goffman, Frame analysis: An Essay on The Organization of Experience.（New York: Harper & Row.1974）

[22]W. A.Gamson, & A. Modigliani, “The Changing Culture of Affairmative action. ”Edited by R. D. Braungart. Greenwitch. Conn: JAI. Research in Political Sociology, 3, 137-177. 1987.

心意義[23]。直言之「框架」一詞，可以解釋為一則新聞的主旨；「核心框架」放在整體社會上來看，可以視為大眾解讀外在事件的心理原則或主觀意見的結果。

二、研究步驟

本研究參考前述觀點，運用框架分析的概念，從新聞框架中蒐集樣本，再從有效樣本框架化「新興網路犯罪」的演變軌跡，以及其犯罪類型。基本上符合「新興網路與跨境犯罪」研究所需要的新聞故事框架，應該是在新聞報導中出現「新興犯罪」、「網路犯罪」、「新興網路犯罪」、「跨境犯罪」、「網路跨境犯罪」等關鍵詞新聞。從台灣新聞知識管理系統資料庫（http://nplnews.ly.gov.tw/index.jsp）搜集所需樣本。

考量到研究需要突顯「新興」的意涵，以及研究規模，因此規劃新聞樣本期間為 2011 年 1 月 1 日至 2015 年 6 月 30 日。經以前述關鍵字分別輸入後，計搜尋到的樣本數如下：「網路犯罪」996 筆、「新興犯罪」53 筆、「新興網路犯罪」6 筆、「跨境犯罪」200 筆、「網路跨境犯罪」0 筆、「網路犯罪加跨境」27 筆，合計為 1,282 筆，是樣本的母全體。

本研究以母全體作為研究樣本，逐一閱覽新聞內容，篩選網路（跨境）犯罪的顯著案例，並排除重複樣本、非屬本研究所需樣本，最終合計取得 576 筆樣本。本研究從樣本所透露的意義，歸納其犯案歷程、新興犯案手法，最後形成框架化犯罪類型。

肆、研究發現

本研究從 1320 筆新聞樣本中，發現將近約 5 年以來的網路犯罪手法，新舊並存，但無論新工具舊犯罪，或新工具新犯罪，總合其犯罪剖繪（criminal profile），可以從犯罪結構、類型框架化兩個方式來加以說明。

一、新興網路跨境犯罪金字塔結構

從網路犯罪金字塔結構示意圖來看，後續金字塔上層的犯罪類型需要在基底上進行。但是底層與頂端彼此相互變異流動，不是硬性地、不可流動的分類。意謂著網路犯罪可畫出不同層次，但層次之間存在交流的可能性，犯罪者視犯罪機會做理性選擇。

[23]C. Ryan, Prime Time Activism: Media Strategies for Grassroots Organizing.（Boston: South End Press.1991）

網路犯罪金字塔結構底層是以企業商業資料、個人資料為犯罪的基底，犯罪者從掌握企業資料、個人年籍住所資料、網路銀行密碼帳號，繼而開展上一層的電信詐騙犯罪。也因此，寄垃圾信、植入病毒入侵電腦、手機竊取資料，或竊取企業第三方個資等都是犯罪手法。有些資料被犯罪者使用後，另外再販售圖利，一部份則是內部人員貪圖利益，直接進行不法販售。

網路攻擊型犯罪進展到以惡意程式釣魚、入侵後，逕行綁架電腦、手機，成為殭屍，由犯罪者遙控進行犯罪，讓被害人在不知覺的情況下成為下一個犯罪的共犯。可以說，竊取個資是所有網路犯罪的基底。

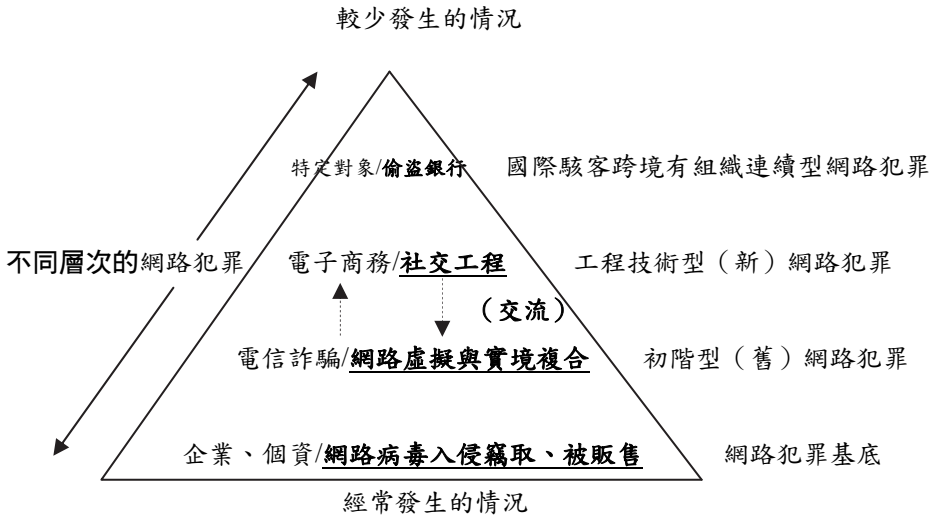

圖 1：網路犯罪金字塔結構示意（本研究製圖）

兩岸四地的電信詐騙犯罪腳本五花八門，但是在結合新興社交工程（social engineering）後，犯罪腳本內容更為多樣豐富，出現防不勝防的變異型態。社交工程類型的犯罪者利用受害者的信任、好奇和貪婪等心理弱點，以冒充熟人方式博取同情，並輔以大量社交工程學的專業術語，降低被害人防備，進行網路盜竊、詐騙和敲詐。

此外利用電子商務見縫插針，進行網路犯罪方式近年也在增加。網路拍賣、解除分期付款傳統詐騙，根本無法根絕。台灣地區 2015 年出現使用 LINE 通訊交易電子商務，衍生出許多詐騙、賣家交易資料外洩犯罪案例。還有一些小型網站業者將網站與資料庫委由第三方管理，導致管理風險大增，難以制止詐騙犯罪。

金字塔頂端的網路犯罪型態是犯罪者鎖定特定銀行、特定企業財團、知名網站為犯罪對象。通常是跨境有組織連續長期網路犯罪，也是比較少發生的案件，但是如果一旦發生，必定造成鉅大金錢損失。有些被害的跨境集團、銀行，在被

害後會隱瞞，或刻意輕描淡寫低報損失，以免破壞本身商譽，或讓客戶對於機構產生「資通安全管理脆弱」的印象，喪失交易信心。這個情況對於遏止犯罪發生極為不利，勢必形成被害人「啞巴吃黃蓮」窘況。由於執法者未被告知，無法介入偵查犯罪，這可能會讓犯罪者更加張揚氣焰，並且大膽地繼續籌畫設計下一個鉅型網路犯罪。

二、新興網路跨境犯罪框架化類型與故事

（一）情境結構的框架類型

新興網路犯罪類型出現顯著的框架元素，包括犯罪主體、參與人物、犯罪期程、網路工具、新興軟體、犯罪產業鏈、司法追訴等 7 項。在新舊雜陳的網路犯罪歷程中，可以觀察到顯著的「對比」類型。

表 1：網路犯罪情境結構的框架對類型

框架元素	框架對比類型	
犯罪主體	組織犯罪型	個人犯罪型
參與人物	招聘組成犯罪團體類	駭客自我推薦招攬業務類
犯罪期程	長期程多階段連續犯罪類	短期程個案犯罪類
網路工具	純粹網路虛擬世界犯罪型 （不在場犯罪）	網路作為連絡工具犯罪型 （虛擬與實境複合犯罪）
新興軟體	攻擊軟體類	攻擊後假修復再攻擊軟體類
犯罪產業鏈	垂直黑色產業鏈型	水平專業家族產業鏈型
司法追訴	有不法利得、有法可追訴類	有不法利得、無法追訴類

本研究製表

參考前表，以「犯罪主體」框架元素而論，同時出現了可資對比的組織犯罪型、個人犯罪型；在參與人物框架元素中，則出現招聘組成犯罪團體類、駭客自我推薦招攬業務類等兩種相對方式的類型。

本研究舉數則網路犯罪情境結構框架故事，作為參考。

1.無法追訴不法利得的框架故事

詐騙集團利用蘋果公司創辦人賈伯斯（Steve Jobs）過世，宣稱要提供

免費 iPad 給臉書使用者，誘導使用者點選網路連結、登記個資。然後引導民眾完成線上問卷、進入賭博網站。當使用者點選連結後，詐騙者可因為流量獲取佣金，這類社交工程案件，詐騙行為不顯著，也沒有使用任何電腦病毒攻擊。（2011 年案例）。

2.網路虛擬世界犯罪的框架故事

高雄一名網路犯罪者在網路搜尋、破解及盜用個人用戶 HN 帳號密碼，之後利用國內外雲端伺服器及代理伺服器隱藏網路身分，進行多筆數百至萬元小額消費，並入侵學校伺服器作為儲存犯罪資料的網路空間。（2011 年案例）。

3.個人犯罪的框架故事

希臘政府逮捕一名以代號 NSPLITTER 犯罪的 18 歲駭客，犯嫌從 15 歲開始在自家獨自作案。他從家裡駭遍全世界，先是國際刑警組織，也駭入美國各政府網站。犯嫌在網路竊取被害人信用卡和銀行交易資料，製出假冒卡片，成功提領現金。（2011 年案例）。

4.攻擊後假修復再攻擊軟體類

被稱為 scareware 的惡棍安全軟體（roguesecurity software）橫行全球，犯罪者先攻擊被害人便腦，然後通知被害人電腦上發現病毒或其它問題，再兜售可解決問題的程式。但被兜售的軟體實際上是一種病毒。（2011 年案例）。

5.駭客自我推薦招攬業務類

大陸地區出現駭客培訓、資訊竊取、惡意廣告、垃圾郵件、敲詐勒索、網站仿冒、輿論造假攻擊等多種網路犯罪盈利模式。最典型的是「網路公關公司」，他們收受企業或個人的報酬，靠網上發文和刪文賺錢。（2011 年案例）。

6.網路作為連絡工具犯罪型

兒少色情網站「蘿莉卡漫王」可在 Facebook、Google 或 Yahoo 帳號登入連結，就能獲得新增的兒少色情影音圖片，造成短時間內出現大量瀏覽量及快速吸收網路會員加入。（2014 年案例）。

7.新興軟體攻擊軟體類型

愈來愈多裝置加入物聯網，包括電器用品、汽車、家庭自動化設備，甚至燈泡等。駭客使用新興「勒贖軟體」攻擊手機作業系統，以及將重要資料鎖住，逼使受害者贖回。劫車犯只需駭入車內電腦導航系統，即可控制車輛。（2014 年案例）。

8.駭客自我推薦招攬業務類

hackerslist.com 等網站上出現數千名駭客的專長與連繫資料，以收費方式幫助僱主駭入其他人電腦。出現次數最高的任務，是要求駭客侵入學校網站，更改學業成績。而買家出價的空間從 100 美元到 5000 美元。（2015 年案例）。

9.長期程多階段連續犯罪類

國際駭客集團以惡意程式侵入銀行電腦盜走鉅款，駭客先將名為 Carbanak 木馬程式電郵寄給銀行僱員，侵入銀行內部電腦系統，從遠端監看銀行作業程序，觀察 2 至 4 個月後從銀行帳戶轉走款項，或用電子付費機制竊款，或遙控自動櫃員機在特定時刻吐出現金，或把虛設帳號中的存款餘額灌水後領走。調查發現受害銀行遍及俄國，日本、荷蘭、瑞士、美國，銀行損失可能高達 3 至 9 億美元。（2012 年案例）。

（二）被害人的框架類型

早期所謂的網路攻擊、網路襲擊專指惡意植入程式竊取資料或癱瘓電腦，但是在社交工程加入犯罪後，所謂網路攻擊還包括虛情假意的問候、號召參與公益活動等；凡是掩藏真正目的的所有信息，都視為網路攻擊。本研究在有限篇幅內，舉數則網路犯罪被害人框架故事作為參考，內容見表 2。

表 2：網路犯罪被害人的框架對比類型

框架元素	框架對比類型	
被害人	鎖定特定對象金融機構、企業進行長期犯罪 （金融機構、法人被害型）	非特定民眾被亂槍打鳥遭受短期網路攻擊、詐騙 （自然人被害型）
被害規模	轉帳被盜巨額現金	被小額或多次小額轉帳
釣魚被害	釣魚竊取個資改造犯罪身份	釣魚綁架控制殭屍電腦成為共犯
隱私被害	加害人可追查類	加害人無從追查類

本研究製表

1.釣魚竊取個資改造犯罪身份

台灣地區發現臉書「開心農場」玩家點入他人臉書不明連結後，帳號

及密碼遭到對方竊取，歹徒再冒用身分，盜刷信用卡購買農民幣得逞。（2012年案例）。

2.自然人被害型

詐騙集團盜取 LINE 帳號，假冒手機用戶的朋友傳訊息，常見內容有「這是上次聚會照片」、「好久不見還記得我嗎」等，誘使用戶點選訊息附上的連結，一旦點入，就形同中毒，還在不知情的情況下遭到小額扣款。犯罪者看準小額付費的便利性，用其購買遊戲點數後，或者網拍轉賣、或者換成現金匯入實體帳戶，進行網路洗錢。（2013 年案例）。

3.釣魚綁架控制殭屍電腦成為共犯

一名女子點入詐騙簡訊的釣魚網址後，手機被詐騙集團植入木馬程式，並遭綁架而成為「殭屍手機」。歹徒暗中隨機發送 500 多通詐騙簡訊，不但手機被盜用帳單費用暴漲，手機主人還成為幫助犯。（2014 年案例）。

4.隱私被害加害人無從追查類

台灣地區多名小模的不雅裸照，被放置在國外 pCloud 雲端的服務平台散佈，因沒有合作執法窗口，無法調閱相關資料，也無從追查張貼照片者。（2014 年案例）。

伍、結論與建議：電腦犯罪發展趨勢及防制策略

2016 年 4 月一起與兩岸有關的詐騙犯罪案件，並牽涉到非洲國家肯亞（Republic of Kenya）。這起疑似由大陸人、台灣人共組的犯罪集團，在第三地肯亞境內設置及操作電信機房，並向境外實施電信跨境詐騙犯罪，可能大陸、台灣都有受害者。這起「肯亞事件」發生在政黨交替前一個月，使得兩岸共打與司法互助，出現彼此溝通與合作的不順利發展。

新興網路犯罪的發展路徑，其實是依附於新興網路日常生活功能而生成的，尤其電子商務市場。當新的網路功能被提出來，並運用於日常生活的時候，通常也就是犯罪者構畫犯罪腳本的啟動時機，並將電腦網路電信等工具融入犯罪歷程。本研究據此預測犯罪者已經在進行穿戴裝置、物聯網規劃新的犯罪腳本，在不久後，隨時可能登場。

隨著大陸、印度與印尼中產階級與電子商務的興起，以及移動裝置的普及，亞太地區電子商務市場成長速度高於全球其他地區[24]。隨著兩岸四地電商市場規模

[24]中商情報網，資料來源：http://big5.askci.com/news/chanye/2015/12/22/193711wnsi.shtml。取得日期：

龐大，可預見未來網路犯罪也必將持續擴大規模。

新興網路犯罪歷程，沒有暴力、不見血，犯罪者運用匿名，實施跨境犯罪，通常不易被發現罪行。駭客大規模滲入日常生活網路，在社群媒體上橫行，防不勝防，也有「道高一尺、魔高一丈」的氣燄，這些正在加速惡化社會治安的犯罪，不但使傳統正常社交活動風險增加，也造成人際信任度降低，這種損害將不是網路犯罪的經濟損失所可比擬。網路犯罪的新興化、普遍化、持續化若不能有效遏止，可能徹底改變人與人的社交關係。

網路犯罪具有特殊的犯罪性（criminality），不必然肇因於經濟不平等、貧窮等原因。網路犯罪者中的駭客犯罪，其附加獎賞是破解網路的成就感；詐騙集團的犯罪成員，以高獲利、低刑罰換取生活條件的舒適與虛榮。這些犯罪心理的形成，本質上與傳統犯罪有極大的差異。政府部門或執法者負有犯罪預防或治安治理的責任，過去極不重視網路犯罪心理研究領域，是執法機關的一大失誤。

有些犯罪類型並沒有在兩岸四地出現，或者尚不具規模，但當時機成熟時，就會被複製進行。本研究提出了一些框架類型以及框架故事，以供警務人員可據以綢繆及早預防。

此外，本研究歸納三項對於兩岸四地跨境網路犯罪，執法者共同合作的防制措施建議如下：

一、警務司法合作追懲措施：

兩岸四地各有司法管轄，網路跨境犯罪的刑與罰力求一致化。避免網路犯罪者跨境尋求保護傘，或者給予犯罪者逃避刑責、減低刑責的機會。在兩岸共同打擊犯罪、兩岸司法互助協議上，要建立更多的「制度化」合作機制，減少以「默契」為主的非正式合作方式，才能落實共打政策。

二、犯罪斷底措施：

必要時切斷犯罪電腦網路伺服器、阻斷犯罪者運作電腦網路。這是斷絕犯罪根底能力的終極手段，雖然可能會波及其他使用者的權益，但是已有過實施成功的案例。此外，政府部門編列專門預算，以及促請企業投入更多預算遏止資料被竊，阻絕網路犯罪的基底犯罪，也是斷底措施之一。

三、第三方合作預防措施：

2015 年 12 月 30 日。

不只是兩岸四地執法者之間的合作而已，警務機關需要發展與電腦網路廠商的支持關係、信任關係、合作關係。第三方是指與科技業者合作開發資通安全軟體，或者由業餘網路專家協助，有針對性的培訓警務人員網路專業技術，並且配合通傳技術持續進行升級式的培訓。

參考文獻

中文部份

1.汪子錫（2014），〈從輿論分析兩岸合作打擊電信詐騙犯罪的成效與今後展望〉，《展望與探索》12（5）:33-49。
2.汪子錫、章光明（2013），〈警察犯罪預防政策行銷的理論與實例探析〉，《警學叢刊》43（6）:47-67。
3.林山田、林東茂、林燦璋（2008），《犯罪學》，台北：三民。
4.徐彩媚（2002），〈新興犯罪議題與對策研討會〉，《台灣新聞報》2002 年 11 月 22 日第 15 版。
5.楊肅民（2001），〈防制網路犯罪刑法擬訂專章〉，《中國時報》2001 年 8 月 25 日第 8 版。

英文部份

1.Albanese, J. S.（2011）.Transnational Crime in the 21st century: Criminal Enterprise, Corruption and Opportunity. New York: Oxford University Press.
2.Bateson, G.（1972）. Steps To The Ecology of Mind. New York: Ballantine Books.
3.Castells, M.（1996）. The Rise of the Network Society. Cambridge, MA : Blackwell Publishers.
4.Gamson, W. A. & Modigliani, A.（1987）. “The Changing Culture of Affairmative Action. ” Edited by Richard D. Braungart. Greenwitch. Conn: JAI. Research in Political Sociology, 3, 137-177.
5.Goffman, E.（1974）. Frame analysis: An Essay On The Organization of Experience.New York: Harper & Row.
6.Ryan, C.（1991）. Prime Time Activism: Media Strategies for Grassroots Organizing. Boston: South End Press.
7.Shelley,L.L.（1998）. “Transnational Organized Crime In The United States,”Kobe University Law Review,32（1）: 77-91.

8.Siegel, L. J.（2003）. Criminology. West/Wadworth Publishing Co.
9.Sparks, R.F.(1981). “Multiple Victimization: Evidence, Theory and Future Research. ” Journal of Criminal Law and Criminolog.（72） : 762–788.
10.Tankard, J. W. & Others.（ 1991 ）. “ Media Frames: Approaches To and Conceptualization Measurement.” Paper Presented to Communication Theory and Methodology Division, Boston.
11.Wall, D.S.（2001）. Crime and the Internet. New York :Routledge.
12.Williams, M.（2006）.Virtually Criminal. London: Routledge.
13.Wimmer,R. D. & , Dominick,J. R.（2014）. Mass media Research : An Introduction. CA : Wadsworth.

網路部份

1.內政部刑事警察局「犯罪預防寶典」https://www.cib.gov.tw/Crime/Detail/981。取得日期：2015 年 6 月 1 日。
2.黃茂穗，〈反詐騙 165 專線的現況與未來〉。取得日期：2013 年 6 月 30 日。網址：http://www.ntpu.edu.tw/gradcrim/temp/I_F_20080926145540.pdf
3.中商情報網，http://big5.askci.com/news/chanye/2015/12/22/193711wnsi.shtml。取得日期：2015 年 12 月 30 日。
4.騰訊互聯網與社會研究院，〈2014 年騰訊雷霆行動網路黑色產業鏈年度報告〉http://law.tencent.com/Article/lists/id/3557.html。取得日期：2015 年 5 月 25 日。