從犯罪預防觀點探討兩岸跨境網路犯罪之防治機制

蔡 政 杰*

要 目

* 蔡政杰（Chen-Chien, Tsai），中央警察大學外事警察研究所（國境組）法學碩士，現就讀於中國文化大學政治所博士班。內政部移民署入出國事務組視察、中央警察大學國境警察學系兼任講師。本文特別感謝：中央警察大學國境警察學系陳明傳教授所提供之寶貴資料與意見，同時，亦感謝中央警察大學國境警察學系王寬弘教授於本文作者投稿學報之過程中，給予行政上之諸多協助，亦同時感謝國立臺灣海洋大學海洋法政學系謝立功教授與中央警察大學國境警察學系柯雨瑞教授對本文惠予提供若干之研究觀念，一併致謝。

摘 要

自2009年4月26日兩岸代表在南京市簽署「海峽兩岸共同打擊犯罪及司法互助協議」以來，兩岸執法部門已成功合作執行數起跨境打擊犯罪案例，諸如：電信詐欺、毒品販運、組織犯罪及人口販運等案件；然而，隨著資通訊設備之普及運用，網路逐漸形成跨境犯罪之主要媒介，亦為兩岸共同打擊犯罪之帶來新興挑戰，更因為透過網路進行犯罪要比一般實體犯罪較難掌握犯罪證據，使兩岸執法部門在犯罪預防及查緝上，均面臨嚴峻之考驗。2010年4月，第十二屆聯合國預防犯罪和刑事司法大會於巴西薩爾瓦多舉辦，網路犯罪在該大會議程中佔有重要地位，證實聯合國對於網路犯罪之相當重視，亦因為網路犯罪具有以下之特色：犯罪範圍之不確定性、犯罪之跨境性、各國法律差異性及犯罪組織性等等相關之因素，因此對於各國刑事及司法部門帶來相當大之新挑戰。

兩岸執法部門（指臺灣警察與大陸公安部門）對於跨境網路犯罪之預防，已具有治理之經驗及防範對策，惟根據 Gordon Earle Moore 所提之「摩爾定律」，資訊科技發展之速度，恐非政府機關執法部門所能追趕，另 Marc Goodman 亦提出「犯罪摩爾定律」，指出未來犯罪之可預測性，故假若執法部門欲確實有效地防範（制）跨境網路犯罪，必須投入相當多之人力及資源，在硬體部分，需有高科技之資訊設備，作為偵查與鑑定之支援；在軟體部分，則要有完善之立法及配套措施，而此正是兩岸執法部門目前所欠缺之區塊。

本文從犯罪預防機制（crime prevention mechanism）之觀點，探討兩岸執法部門對於跨境網路犯罪之治理之現況、問題與所面臨之諸多困境，以及共同合作預防跨境網路犯罪之未來可行之發展方向，並提出十三項之具體建議，作為兩岸政府部門與民間社會之參考。

關鍵詞：跨境網路犯罪、網路犯罪預防、電腦相關犯罪

壹、前　言

資（通）訊科技之發達，養成人們在生活上對於網路之依賴使用，近年來，不斷推陳出新之資（通）訊技術及設備，更完全顛覆人們之傳統生活習慣，同時，亦改變犯罪者之犯罪手段，如今之犯罪者會透過網際網路上之社群網站作為媒介，進行犯罪行為[1]，如Facebook、Instagram、Twitter、微博……等，以及行動通訊裝置上之APP通訊網路，如LINE、Tango、Mico、Paktor、BeeTalk、WeChat...等，儼然已成為新興之犯罪型態。

網路犯罪之特色之一是犯罪區域不受邊界限制，因此，欲預防網路犯罪必須要整合多方區域資源，進行跨區域合作始能有所成效。2011年11月29日，台灣警方與大陸公安部刑偵局暨江蘇省公安廳專案人員及印尼、柬埔寨、馬來西亞、泰國、斯里蘭卡、斐濟等國家執法機關共同合作，查獲「假冒公安」手法之詐騙集團，八地警方計查獲嫌犯200餘人，充分展現「海峽兩岸共同打擊犯罪及司法互助協議」之實體成果，亦建立起東南亞國家共同查緝犯罪之合作關係，可算是跨區域網路犯罪治理之典範。

台灣與大陸之間，人文相近、語言互通，容易成為犯罪者從事跨境犯罪之目標，諸如：詐欺取財、洗錢、色情媒介交易、人口販運、毒品交易及招募組織等跨境犯罪行為，在兩岸之間經常發生，雖然這些均不是新興之犯罪行為，惟若經由資（通）訊網路設備作為媒介而進行犯罪，即會產生不同之犯罪手段和過程，增加兩岸執

1　陳彥驊，〈濫用社群網站，人蛇集團效率高〉，《台灣醒報網站》，2014年11月26日，<https://tw.news.yahoo.com/%E7%A4%BE%E7%BE%A4%E7%B6%B2%E7%AB%99%E4%BE%BF%E4%BD%BF-%E4%BA%BA%E8%9B%87%E9%9B%86%E5%9C%98%E6%95%88%E7%8E%87%E6%8F%90%E5%8D%87-091523250.html>。

法單位在犯罪預防及偵查上之壓力，又因兩岸在相關網路犯罪之立法上，並無制訂定專法，亦使得兩岸司法機關審理案件之困難度提高，故執法單位如欲運用犯罪預防理念，防制網路犯罪發生，並非一件容易之事。本文就兩岸跨境網路犯罪一般狀況，從法令面與執行面，研究其可能之危害性，再從犯罪預防之觀點深入探討，期望能從犯罪預防之觀點，提供兩岸執法單位在偵辦兩岸跨境網路犯罪案件時之參考。

貳、研究途徑與方法

犯罪預防是屬於社會科學之研究範疇，其所涉及之學科頗多，有學者認為犯罪預防至少應包含犯罪學、刑事司法、偏差行為學、青少件犯罪、心理學、刑事政策和管理學之概念[2]；亦有學者認為犯罪預防係涉及法律學、心理學、犯罪學、社會學、經濟學、教育學、政治學、宗教學、犯罪矯治、監獄學等學科之範疇[3]。因此，如欲深入研究犯罪預防，必然需要整合運用相關之學科，建立系統性之架構，始得完備整體犯罪預防之研究。因此，本研究亦含概從社會學之觀點，探討犯罪所造成之社會問題；從犯罪學之觀點論析犯罪之基本理論、定義及防範之機制；從政治學之觀點研究政府制度及國際公約規範；從刑事司法之觀點進行相關法規探討及個案研究，期能較完整之從實證行為科學途徑，綜整探討兩岸網路跨境犯罪防治之可能作為，其研究方法如下：

---

2 廖福村，《犯罪預防》（台北市：警專，2007），頁4。

3 鄧煌發，《犯罪預防》（桃園縣：警大，1997），頁4-8。

一、文獻分析法（literature review）

參考預防醫學之理論及模型與國內外犯罪預防之專家學者所提出之犯罪預防理論，結合歐洲網路犯罪公約之規範，建立犯罪預防理論與網路犯罪實務之關連性，繼而從相關文獻資料據以分析兩岸網路犯罪之情形及防治之作為，以及可能之策進方向，作為本文之研究成果。

二、文件分析法（documentary analysis）

從兩岸政府對於網路犯罪防治之政策方向、相關法令規範及官方文件著手研析，以瞭解兩岸政府目前對於網路犯罪所採行之防治策略，以及兩岸之間之策略是否可相輔而成，亦或各自為政；以作為研究兩岸共同防治網路犯罪之重要參考資訊，藉以提出具體改善之研究建議。

三、個案研究法（case study）

從「3千萬城堡別墅機房」、「金船娛樂城」及「肯亞電信詐騙案」等三個與本研究主題密切相關之社會案件，作初步之個案探討犯罪行為，並從中分析網路犯罪發生之可能原因，兩岸政府機關之查處作為，作為理論與實務案件之差異性研究，藉以提出兩岸政府機關未來防治網路犯罪之共同規劃方向，期避免類似之大宗網路犯罪案件一再發生。

參、犯罪預防之機制與理論

犯罪（crime），是一種社會上失序之問題[4]，從廣義而言，只要是破壞社會秩序或危害人身及財產等安全之行為，均可視為犯罪行為；但從國家刑事司法法制立場而言，破壞社會秩序、危害人身或財產安全之行為，尚有程度輕重之分，若一概將之視為犯罪行為而予以追懲，亦不符合公平正義原則，因此，國家制定相關刑事法令，以利定義犯罪之行為，並依其行為是否違反刑事法令規範為原則，亦即「依法論罪」，此亦是社會大眾普遍般認知之犯罪定義。

至於犯罪之發生原因，各派學說理論不一，古典學派認為：「人類行為是源於人之自由意志和功利主義所產生」，犯罪本屬人類行為之一種，亦應是由人之自由意志和功利主義所導致而成。此一學派之代表性人物有義大利法學家西薩爾·貝卡里亞（Cesare Beccaria）及英國之法、哲學家傑里米·邊沁（Jeremy Bentham）等人。另外，實證學派則認為：「犯罪行為是受到外力或內存之心理因素所決定，不是個人之自由可以選擇」，此一學派之代表性人物有義大利學派之龍布羅梭（Cesare Lombroso）、費利（Enrico Ferri）、加洛法羅（Raffele Garofalo）以及社會主義學派之法國之社會學者艾彌爾·涂爾幹（Émile Durkheim）等人。

至於犯罪預防之研究領域亦相當廣泛，國內眾家學者對於犯罪預防之定義亦未趨一致，有學者認為，犯罪預防是一種結果導向之作為，是經過設計之活動，目的在於降低犯罪率或犯罪被害之恐懼感[5]；亦有學者認為，犯罪預防是一種治本性之工作，在於消除與犯罪有關之因素，預先查覺犯罪行為及原因；另有學者認為犯罪預防

---

4 許春金，《犯罪學》（台北市：三民，2007），頁5。

5 許春金，陳玉書，《犯罪預防與犯罪分析》（台北市：三民，2013），頁3-4。

是科際整合、標本兼治之社會學學科，主要目的在於消除和促進犯罪相關因素、發覺潛伏之犯罪、瞭解犯罪現象、診斷犯罪原因，抑制犯罪行為之發生[6]；本文則認為，所謂犯罪預防，其是標本兼治之措施，以研究及分析已經發生之犯罪行為，瞭解犯罪心理、模式，設計預防犯罪行為發生之架構，進行避免犯罪行為之發生，達到維護社會秩序之成效。

而犯罪預防是以一種先發式之作為，以控制犯罪之發生，惟因犯罪預防之領域相當廣泛，並無一定之範疇予以規範，部分學者係以公共醫療之理論思維，將犯罪預防之機制，分為以下三個層級預防[7]：

一、初級（一級）預防（primary prevention）：初級預防是屬於最基本之預防工作，亦即，從根本做起。就個人層面而言，從小以教育之方式，將犯罪預防之觀念內化到兒童及青少年之心理，使其成長後，自然就會守法之觀念，不會產生犯罪之行為；若就更整體、宏觀及深入之層面而言，初級預防亦在於從家庭、學校、教育、法律、經濟、政治等方向，發覺出犯罪可能發生之因子，從這些犯罪因子去預測犯罪可能發生之風險，再設計相關之危機處理及風險管理之措施，從根本去防範犯罪之之發生，達到預防之效果，此是屬於全面性之預防作為；在此一層級運用之理論有赫希（Hirschi）之社會控制理論、譚那邦（Tannenbaum）與李莫（Lemert）之標籤理論（Labeling Theory）、

6　鄧煌發，李修安，《犯罪預防》（台北市：一品，2012），頁6-7。

7　Evans, K.(2011)、Fennelly, L. & Crowe, T.,(2013)、Mackey, D & Levan, K., (2011)、Schneider, S., (2014)、Steven P. Lab.,(2013)、孟維德、黃翠紋(2012)、鄧煌發(1997)、廖福村(2007)、許春金，陳玉書(2013)、鄧煌發、李修安(2012)、許福生(2016)等以上國內外學者，均以三級預防之理論來探討犯罪預防。

佛洛依德之心理分析（Psychoanalysis）理論……等[8]。

二、次級（二級）預防（secondary prevention）：它強調介入處遇（intervention），透過初級預防之風險管控作為，發覺出風險性偏高之犯罪行為者及其犯罪情境，針對這些特定之行為者及情境設計防範機制，透過社會環境改變、監控或社區警政等方式，消除犯罪情境，自然可以降低犯罪風險，避免犯罪行為之發生。此一層級運用之理論則有古典學派之「犯罪自由意志論」、新古典學派之「更生矯治論」及由涂爾幹（Durkheim）之社會規模失調（Anomie）學說所源生之犯罪生態學理論（The Ecology of Crime）[9]。

三、三級預（tertiary prevention）：它重視治療（treatment），是指犯罪發生後，透過刑事司法之各式任意性與強制性作為——如偵查、拘提、逮捕、審判，及相關輔導及矯治機構之教化性作為，使犯罪者不會再犯罪，達到預防犯罪之功能。特別值得加以關注之處，乃三級預防（tertiary prevention）可以運用之技術，尚且包括：各式之犯罪偵查之手法與強制處分權之運用，以利逮捕犯罪人，並使其受審，並接受矯治，預犯或降低其再犯[10]。

以上犯罪預防之理論與預防醫學相當類似，近年來，在醫療領域，除了重視傳統之治療醫學之外，預防醫學之領域與區塊，額外受到重視與關注，產生所謂3段5級之預防醫學（如圖一及圖二）。在預防醫學領域中，其初段預防乃為健康之促進，次段預防乃為疾病之篩檢，參段預防乃為癌症與慢性病之照護；其中參段預防則包括

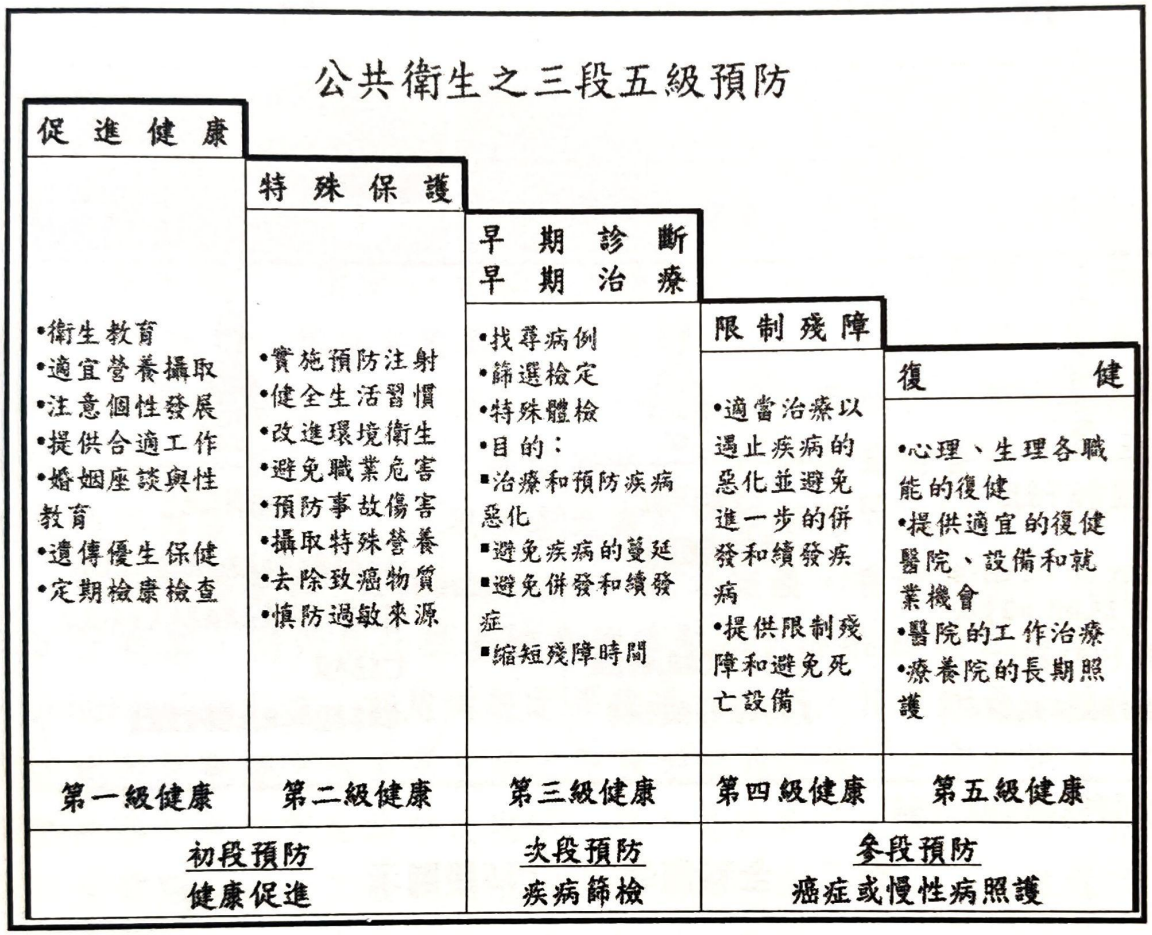
---

8 廖福村，《犯罪預防》（台北市：警專，2007），頁29-63。

9 廖福村，《犯罪預防》（台北市：警專，2007），頁65-74。

10 許春金，陳玉書，《犯罪預防與犯罪分析》（台北市：三民，2013），頁8。

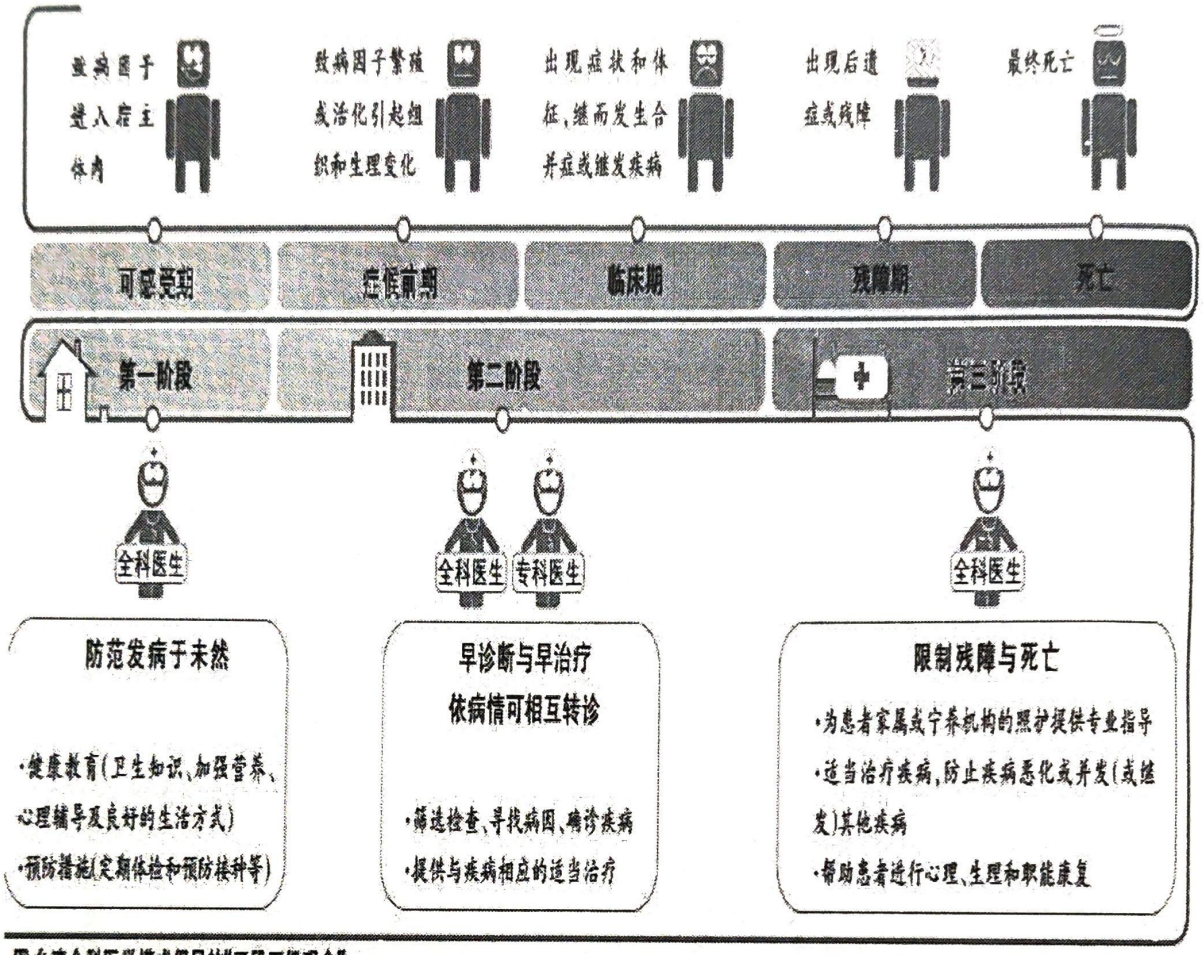
第4級健康之適當治療、控制病情之惡化，避免進一步之併發症，與限制殘障，與第5級之各式生理與心理之復健[11]。



圖一　三段5級之預防醫學

資料來源：陳立昇（2005），疾病篩檢基本概念。

11　曹明、程永進、張哲、曹銳生、鄭新傑，〈台灣全科醫學模式之我見〉，《中國醫學論壇報》，2011年11月18日，＜http://gp.cmt.com.cn/detail/30561.html＞。



圖二　全科醫學之三段5級圖示

資料來源：曹明、程永進、張哲、曹銳生、鄭新杰(2011)。

如將上述之3段5級之預防醫學之理論，與犯罪預防之理論互相對照，則第一級犯罪預防：對於犯罪之全般性預防，則相當於3段5級之預防醫學之初段預防：為健康之促進；第二級犯罪預防：針對特殊、高風險犯罪之鑑定與預防，則相當於3段5級之預防醫學次段之預防：為疾病之篩檢；第三級犯罪預防：犯罪之偵查、逮捕、審判、矯治與再犯之預防，則相當於3段5級之參段預防：為癌症與慢

性病之照護。是以，從預防醫學之角度進行檢視，真正之犯罪預防，實包括：對於犯罪人如何進行偵查、逮捕、審判、矯治，與如何預防其再犯，它是全方位之控制犯罪之對策。而犯罪預防學家之角色，宛如一位全方位之全科醫師。

肆、兩岸跨境網路犯罪之定義

本文所稱之「兩岸」，係指臺灣地區與大陸地區。所稱之「跨境犯罪」，是指同一案件之犯罪行為、犯罪結果、所使用之犯罪工具及其他與犯罪之相關事項或過程，部分發生在臺灣地區，部分發生在大陸地區，始屬跨境犯罪；亦即本文認為跨境犯罪是否成立，是以地區性作為要件，而不以犯罪者之身分作為要件[12]。

至於網路犯罪（Cybercrime）一詞之定義，在學界中一向存在不同之見解，國內部分學者認為網路犯罪只是在新興之網路空間（cyber space）中，利用傳統之手段進行犯罪，其實就是一般白領或組織型之犯罪，未必是全新之犯罪型態或結構[13]；亦有學者認為網路犯罪只是日常生活中之通稱，並不是法典中之專用術語，指的是利用電腦網路為工具或環境，透過電腦病毒、蠕蟲、惡意程式、社交工程、網路釣魚等方式，進行犯罪行為[14]。

而美國之學者則認為，網路犯罪除單指在網路（Internet）上透

---

12 如大陸地區人民來臺旅遊時遭竊致損失財物，其犯罪發生地及結果地均在臺灣地區，雖犯罪者爲臺灣地區人民，而受害者爲大陸地區人民，就本文之定義，亦不屬於跨境犯罪之類型。

13 黃秋龍，〈中國大陸網路犯罪及其衝擊〉，《展望與探索》，第6卷第12期，2008年12月，頁90-106。

14 徐振雄，〈網路犯罪與刑法「妨害電腦使用罪章」中之法律語詞及相關議題探討〉，《國會月刊》，第38卷第1期，2010年1月，頁40-64。

過科技系統之犯罪（如駭客攻擊），另外以透過科技系統之使用，進行一般之傳統犯罪，均是屬於網路犯罪，因此所謂之 Cybercrime，是包含 Internet Crime 之各種類型犯罪[15]，或是包含與電腦相關之犯罪（computer-related crime），其係透過數據機或傳輸線，利用開放之網路空間及科技技術進行犯罪，與傳統犯罪有別的是其犯罪證據是屬於數位證據，需要經由電腦科技分析，始有辦法取得及運用[16]；亦有學者係從犯罪之途徑，界定網路犯罪之定義[17]，如以電腦為犯罪目標（the computer as a target）、利用電腦犯罪（the computer as an instrument of the crime）、伴隨著電腦而發生之犯罪（the computer as incidental to a crime）及隨著電腦普及而發生之犯罪（Crimes associated with the prevalence of computers）。

另亦有英國學者對於網路犯罪定義[18]，係認為早期之網路犯罪（Cybercrime）只有包括電腦犯罪（computer crime）、電腦相關犯罪（computer-related crime）或透過電腦犯罪（crime by computer），但隨著資訊逐漸發達後，近期所稱之網路犯罪（Cybercrime）就包含高科技（high-technology）犯罪、網際網路 （internet）犯罪、網絡（net）犯罪、數位（digital）犯罪、電子（electronic）犯罪、虛擬（virtual）犯罪及資訊科技（IT）犯罪等。

而歐洲理事會（Council of Europe, COE）於2001年11月23日在

---

15 Todd G. Shipley & Art Bowker, "Investigating Internet Crimes : An Introduction to Solving Crime in Cyberspace". (Massachusetts:Elsevier, 2014), p. 2.

16 Marjie T. Britz, "*Computer Forensics and Cyber Crime*". (New Jersey:Person, 2009), pp. 350-354.

17 Anthony Reyes, Kevin O'shea, et al. "Cyber Crime Investigations : Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors". (New York:Syngress, 2007), pp. 24-29.

18 Jonathan Clough, "*Principles of Cybercrime*". (UK:Cambridge, 2010), pp. 8-11.

布達佩斯簽署之「網路犯罪公約」(Convention on Cybercrime)第一章之定義中，僅對於電腦系統(computer system)、電腦資料(computer data)、系統服務供應商(service provider)及流量資料(traffic data)等專有名詞給予定義，並未對於網路犯罪(cybercrime)進行定義(Council of Europe，2015)，然而，就該公約所規範之內容而言，所稱之網路犯罪仍屬於與電腦相關之犯罪行為(Computer-related crime)。

網路犯罪是以電腦為中心而延伸之相關犯罪行為，或是著重於與電子資料處理而涉及財產法益之罪刑[19]；亦有學者認為「網路犯罪」一詞，在學術界中，根本就沒有一個明確之定義；其實務上與「電腦犯罪」之語詞，亦很難分辨[20]。若從法律概念論述，檢視臺灣地區之法律條文，並無任一法律條文使用「網路犯罪」一詞[21]；因此，想要非常明確定義「網路犯罪」一詞之，實屬不易。

網路犯罪之定義，可以從多個面向加以切入：第一個面向，係從是否將「網路」〔含通訊網路(Mobile Communications Network)〕作為犯罪之工具或媒介而論，凡犯罪者違反實體法定罪刑之犯罪行為之過程之中，曾利用「網路」〔含通訊網路(Mobile Communications Network)〕作為工具或媒介者，均稱之為「網路犯罪」，而不論其網路媒介之過程及內容與犯罪要件是否具關聯性，如透過社群網路進

---

19 黃秋龍，〈兩岸情勢中的網路犯罪因素〉，《展望與探索》，第6卷第9期，2008年9月，頁73-106。

20 徐振雄，〈網路犯罪與刑法「妨害電腦使用罪章」中之法律語詞及相關議題探討〉，《國會月刊》，第38卷第1期，2010年1月，頁40-64。

21 經查詢臺灣地區法規資料庫(2015)，上網瀏覽時間：2015/10/01, http://law.moj.gov.tw/Index.aspx，僅「內政部警政署刑事警察局組織條例」與辦事細則等規定中，使用「網路犯罪」一詞，而該條例第3條第17款規定，該局掌理事項為：重大、特殊刑事案件、組織犯罪、電腦網路犯罪、經濟犯罪之偵查及支援等事項。因此所稱之網路犯罪，亦為電腦網路犯罪之範疇。

行聚眾後，至特定地點鬥毆殺人亦屬之[22]。

第二個面向，係從犯罪行為或結果，是否在網路上發生加以解釋之，如犯罪之行為或結果，在網路上發生者，始稱之為「網路犯罪」，如於公開中之社群網路中，以恐嚇之言語表示將至公開場所殺害不特定對象，嚴重影響公安，構成恐嚇罪之要件屬之[23]。

第三個面向，係從凡犯罪者違反實體法定罪刑之犯罪，其「犯罪構成要件」與網路行為有直接關連性者，或具有一定之因果關係者，即稱之為「網路犯罪」，如透過人蛇集團架設之網站進行媒介，而從事性交易者屬之。

第四個面向，有學者專家係從國際公約之角度，論及網路犯罪。在歐洲地區，最有名之防治網路犯罪之公約，係為2004年7月1日正式生效之「關於網路（絡）犯罪的公約」。在此一公約之序言之中，有論及「網路犯罪」之定義，此乃指「危害計算機系統（computer system）[24]、網路（絡）和計算機之數據資料之保密性、完整性和可利用性（action directed against the confidentiality, integrity and

---

22 2014年9月14日臺北市政府警察局信義分局薛姓偵查佐，於臺北市信義區松壽路 ATT 大樓知名夜店「Spark」門口遭黑道份子毆打致死，其曾姓主嫌即是透過 Line 軟體短時間內聚眾召集人馬滋事。

23 2014年5月21日鄭姓犯嫌在臺北捷運板南線列車上隨機殺人，造成4死24傷，其後產生網路效應，許多人於網路社群發言將仿效鄭嫌之殺人行爲，經警方積極查辦，共移送在網路上散播恐嚇殺人言語之犯嫌計12人。

24 Convention on Cybercrime. Article 1 – Definitions---For the purposes of this Convention: a. “computer system” means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b. "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

availability of computer systems, networks and computer data），以及濫用這些系統、網路(絡)和數據之行為(as well as the misuse of such systems, networks and data）」。

歐洲網路犯罪公約之簽署國，需要對九類網路犯罪行為，以刑罰加以處罰與制裁，茲分述如下：1.非法存取（Illegal access）；2.非法截取（Illegal interception）；3.資料干擾（Data interference）；4.系統干擾（System interference）；5.設備濫用（Misuse of devices）；6.偽造電腦資料（Computer-related forgery）；7.電腦詐騙（Computer-related fraud）；8.兒童色情之犯罪（Offences related to child pornography）；9.著作權及相關權利之行為（Offences related to infringements of copyright and related rights）。

本文所指網路（絡）犯罪之定義，擬採用上述歐洲之「關於網路犯罪的公約」中之定義，並稍作一些調整，而將「網路犯罪」之定義，界定為「行為人危害計算機系統、網際網路系統與數據之保密性、完整性與可利用性，以及濫用這些計算機系統、網際網路與其數據之行為。」上述之內容，係為本文有關「網路犯罪」之定義。

而在「兩岸跨境網路犯罪」之定義部分，乃指「兩岸所屬之行為人危害他方之計算機系統、網際網路系統、與其數據之保密性、完整性與可利用性，以及濫用己方或他方之此等計算機系統、網際網路與其數據之行為。」上述之定義，可以從兩個面向加以論述之。第一個面向，是行為人攻擊或危害他方之計算機系統、網際網路系統、數據與信息之犯行；第二個面向，是利用互聯網（我方稱網際網路系統）實施之各類型犯行。上述第一個面向之網路犯行，可稱為兩岸跨境之「網路虛擬犯罪」（virtual crime）；而第二個面向之網路犯行，可稱為兩岸跨境之「實境犯罪」（real crime）。

伍、兩岸跨境網路犯罪之現況與危害性

根據上述網路犯罪定義之面向，所謂網路虛擬犯罪（virtual crime），係指駭客（hacker）或病毒（Virus）入侵[25]，指專門破壞資訊系統、竊取、竄改電腦資料、散播電腦病毒等犯罪行為；而網路實境犯罪（real crime）則是指透過網路作為媒介，進行詐欺取財、從事性交易等犯罪行為。

如從現行兩岸刑法所訂之電腦犯罪相關條文加以觀察，陸方刑法第285條【非法侵入電腦資訊系統罪；非法獲取電腦資訊系統數據、非法控制電腦資訊系統罪；提供侵入、非法控制電腦資訊系統程式、工具罪】、第286條【破壞電腦資訊系統罪】及第287條【利用電腦實施犯罪之提示性規定】，以及我方刑法第36章【妨害電腦使用罪】第358條【入侵他人之電腦或其相關設備罪】、第359條【無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄罪】、第360條【干擾他人電腦或其相關設備罪】及362條【製作專供犯罪之電腦程式罪】等規定，均屬於網路虛擬犯罪（virtual crime）之範疇。至於兩岸對於網路實境犯罪（real crime）之處罰，仍回歸到犯罪行為本質所違反之罪刑予以處罰[26]，並未對於其犯罪媒介是否為網路而有所不同，兩岸目前均沒有訂定網路犯罪之專法。

然而，不論是網路虛擬犯罪或是實境犯罪，均為兩岸跨境網路

---

25 所謂駭客係指鎖定特定目標，非法入侵，合法存取；而所謂病毒，則無特定目標，合法入侵，非法存取。

26 如陸方刑法第287條【利用電腦實施犯罪之提示性規定】：利用電腦實施金融詐騙、盜竊、貪汙、挪用公款、竊取國家秘密或者其他犯罪，依照本法有關規定定罪處罰。又如我方刑法第339條之4第3款，對於以廣播電視、電子通訊、網際網路或其他媒體等傳播工具，對公眾散佈而犯詐欺罪者，有較重之刑罰規定。

犯罪經常發生之現況，本文將嚐試著整理出兩岸跨境網路犯罪可能造成之危害：

一、兩岸犯罪組織合作之形成及擴展，與犯罪擴溢現象

兩岸跨境網路犯罪行為，絕大部分屬於集團性犯罪，係為謀求更大不法利益為前提，使犯罪組織網綿密且複雜，造成犯罪擴溢現象，增加執法機關在案件偵查上之困難度；再者，跨境犯罪組織之間因合作關係而進行擴展，會增加犯罪之區域性，亦會對兩岸社會造成更大之不安定性，並增加執法機關之查緝成本。

二、犯罪被害人追償困難

網路犯罪原本即具有大量傳播、即時性、匿名性等特性[27]，在證據蒐集及加害人追查上即屬不易，若再加上跨境犯罪之區域性問題，基於兩岸法律規定不同，以及管轄權等問題，犯罪被害人將難以對於加害人進行法律上之追償，因此，犯罪者將更有恃無恐，而使跨境網路犯罪更加猖獗。

三、破壞兩岸交流之互信基礎

自2008年以來，兩岸之間各項交流日益頻繁[28]，單2014年一年

27　王勁力，〈電腦網路犯罪偵查之數位證據探究〉，《檢察新論》，第13期，2013年1月，頁13-28。

28　此一部分之論述，可進一步參閱以下之文獻：
王寬弘(2011)，〈大陸地區人民進入台灣相關入出境法令問題淺探〉，2011年人口移動與執法學術研討會，（桃園：中央警察大學）。
王寬弘(2012)，〈大陸地區人民進入台灣相關入出境法令問題淺探〉，《國土安全與國境管理學報》，第17期，（桃園：中央警察大學），頁155-185。
陳明傳(2007)，〈跨國(境)犯罪與跨國犯罪學之初探〉，收於第一屆國土安全

內入境臺灣地區之大陸地區人民即高達將近400萬人[29]，不論是人民及官方均有相當程度之交流及互信基礎。但是，因為跨境網路犯罪行為之情況若過於嚴重，在一定程度上，將會破壞雙方交流之互信基礎，造成雙方人民之間之彼此不信任，甚至產生排斥感，影響兩岸交流之契機。

陸、從犯罪類型探討兩岸跨境網路犯罪之治理困境

英特爾（Intel）公司之創始人之一——戈登・摩爾（Gordon Earle Moore）提出，積體電路上可容納之電晶體數目，約每隔24個月便會增加一倍，此是科技業之「摩爾定律」，近年來，亦有美國之學者根據摩爾定律提出「犯罪摩爾定律」，指出未來之犯罪，幾乎將與網路犯罪劃上等號，犯罪手段之進化，亦將如同摩爾定律一般之快速發展，因此絕對需要很嚴肅的看待這個問題[30]。從學者對於網路犯罪之預測，兩岸執法人員在兩岸網路跨境之治理上，絕對將面臨相當大之挑戰，經作者檢視與綜整相關之文獻，並與有關之學者、警界人士與司法界人士相互討論後，彙整以下防治之困境：

學術研討會論文集，（桃園縣：中央警察大學）。

陳明傳(2015)，〈各國入出國管理系統之比較研究〉，發表於中央警察大學移民研究中心2015年「人口移動與執法」學術研討會，（桃園縣：中央警察大學）。

謝立功(2004)，〈由大陸觀光客脫團事件論我國國境管理機制〉，《展望與探索》第2卷第9期，（台北：法務部調查局），頁14-20。

29 內政部移民署，〈各機場、港口入出國（境）人數〉，2016年1月，《內政部移民署全球資訊網——業務統計》，＜網址：http://www.immigration.gov.tw/lp.asp? ctNode=29699&CtUnit=16434&BaseDSD=7&mp=1＞。

30 Marc Goodman, 林俊宏譯，《未來的犯罪》（新北市：木馬文化，2016），頁58-66。

一、電信詐欺類：陸方民眾對於如何預防與防治來自於我方之電信詐欺犯行，仍普遍未具防範之意識與作為

本文茲以「3仟萬城堡別墅機房」兩岸電信詐欺之組織犯罪案為例[31]，說明陸方之民眾，對於來自於我方之電信詐欺，仍普遍欠缺電信詐欺犯罪預防之犯防意識與作為。

本案電信詐欺之組織犯罪集團之首領人物，綽號「阿東」，經研究瞭解該集團之犯罪過程後，本文嚐試以條列方式，列出犯罪重點及分析其犯罪手法如下：

（一）該犯罪組織之機房，係設在我方高雄市仁武區鳳仁路；

（二）該詐騙集團行騙之對象，亦即，被害人分佈之地點，係在陸方，遍及陸方多個省份；

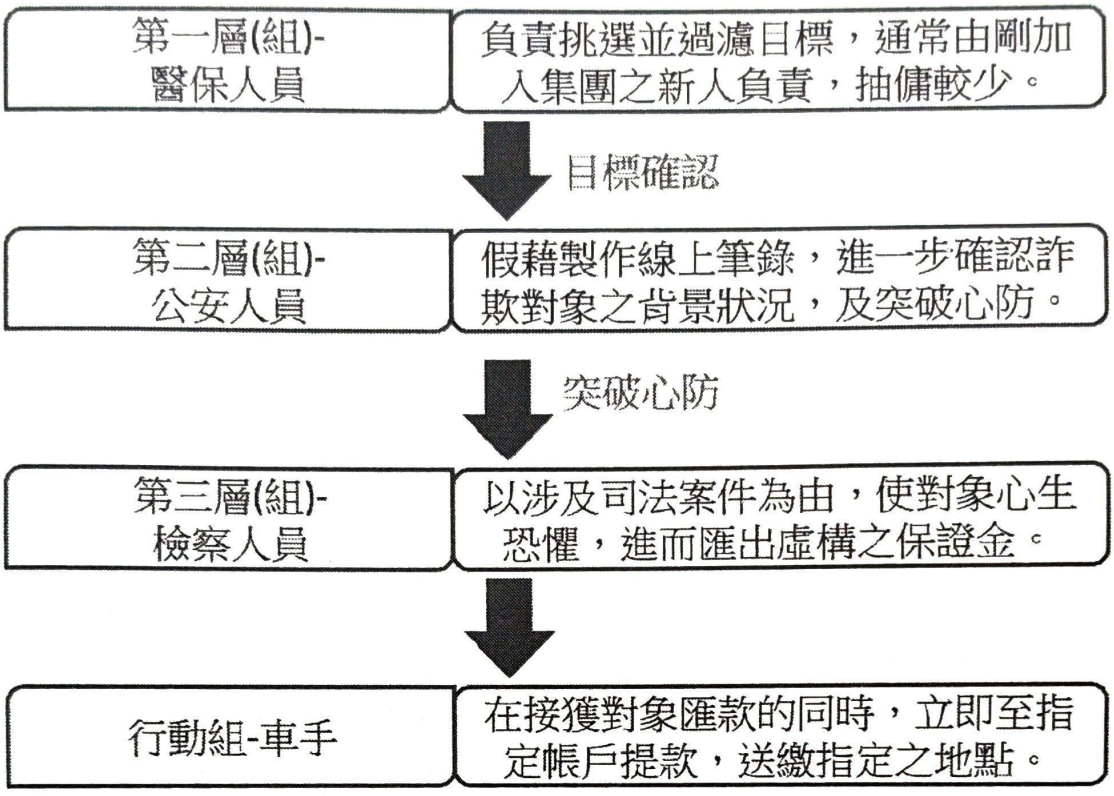
（三）電信詐欺之手法（方式），主要係透由網際網路，以語音「群發方式」，利用隨機發送之手段，發送該犯罪組織之詐騙語音；

（四）在電信詐欺之內容方面，其犯罪劇情如下所述：先劃分為3組，第1組劃編為陸方武漢市、南通市等各省市之「醫保局」人員；第2個工作組，劃編為「福州市公安局」之公安人員；第3組劃編為陸方之「檢察官」；該犯罪組織之任務分工，共分由以上3個組別（部門），各司其職；當陸方民眾接獲來電之後，第1組人員會謊稱：被害人之醫保卡在福州市被濫用，亦即，其醫保卡被犯罪人盜辦，並購買國家之管制藥品，涉嫌違法，請被害人應立即向

31 新北市政府警察局土城分局，〈刑事局偵破「3仟萬城堡別墅機房」兩岸電信詐欺集團案〉，2015年5月19日，《新北市政府警察局新莊分局——案例分享》，<網址：http://www.xinzhuang.police.ntpc.gov.tw/cp-492-11757-18.html>。

陸方之「福州市公安局」報案；第1組之工作人員，再將上述被害人之電話，以層層轉接之掩護手法，轉接至第2組之工作人員；第2組之工作人員，佯稱為陸方被害人製作「線上筆錄」，騙稱被害人所屬之銀行帳户，已被利用，而提供犯罪集團洗錢，涉嫌觸犯陸方之洗錢罪；第2組工作人員遂將電話轉接至第3組；第3組所屬之假冒之檢察官，向陸方被害人聲稱，須進行被害人之「資金比對清查」，要求陸方被害人將所謂之「司法保證金」，匯款至指定帳户。假若，陸方被害人果真將「司法保證金」匯款至上述詐騙集團之「指定帳户」，事實上，本款項已流入上述電信詐欺犯罪集團之帳户之中，陸方被害人當下已無法取回。在上述電信詐欺之流程中，第2組工作人員之辦公背景脈絡，該犯罪組織尚會使用警用無線電之呼叫聲，與鳴放警車之警報器，透由這些背景聲音，以更取信於陸方被害人。被害人聽到這些背景聲音，更加誤以為該犯罪組織第2組之人員，果真為陸方「福州市公安局」之公安人員。

（五）在被害人與金額方面，該犯罪組織自2014年10月，即正式運作進行詐欺犯行，截至2015年4月22日被我方檢察官拘提為止，獲利超過新台幣數仟萬元，陸方被害人數，遍及多個省份，被害總人數，超過1萬人以上。



圖三　「3仟萬城堡別墅機房」兩岸電信詐欺手法流程圖

圖資來源：作者自繪

另就本案如從陸方之被害人角度分析，具有以下特點：

（一）對於透由網際網路而來之電話語音，特別是來自於台灣之電話語音，陸方被害人接收語音電話之後，無法於非常短之數秒之內，立即判讀此為來自於台灣之語音；或者，係來自於陸方內地之語音電話；

（二）陸方被害人在與電信詐欺犯罪集團成員對話時，未提高警覺性，而未能判別來電說話者之語音模式與腔調，並非陸方之人民，而是我方民眾；

（三）陸方被害人在接收犯罪組織第1組工作人員之來電，了解

其來電內容之後，未能掛斷電話，以「事後查證」之方式，立即向陸方有關單位，諸如：醫保局求證，究竟其醫保卡是否果真被盜用？其次，陸方被害人在接通電信詐欺犯罪集團第2組工作人員之後，針對其所指稱之被害人銀行帳户涉嫌洗錢乙事，陸方被害人未立即掛斷電話，轉而向其所屬之銀行求證，究竟其銀行之帳户，是否已涉嫌洗錢？再者，當陸方被害人已了解上述犯罪組織第3組工作人員所指稱之內容之後，未立即掛斷電話，轉而向所屬之檢察院查證，是否果真有「司法保證金」之機制？由於陸方被害人連續錯失3次「事後查證」之機會，最後，其銀行帳户內之資金，遂被詐騙至犯罪組織之帳户之中。

（四）陸方被害人對於「電信詐欺」之名稱、概念、犯行模式、犯罪手法與犯罪損害等，未具有犯罪預防之意識，普遍欠缺犯防意識；

（五）陸方被害人對於來電之發話者，究意是否屬於「犯罪人」？無法作出正確之判斷，過於相信發話者之所言，未具備「事後查證」之意識。

二、網路賭博類：兩岸與第三地之跨境網路賭博線上遊戲，極具誘惑媚力，民眾極易沈迷其中而不知業已觸法

本文以2013年12月13日，兩岸執法人員共同攜手合作，偵破我方最大宗之網路賭博「金船娛樂城案」案例說明[32]，其「金船娛樂

32 內政部警政署刑事警察局，〈國內首宗兩岸合作偵破最大網路賭博第三方支付中心『金船娛樂城』案〉，2013年12月24日，《內政部警政署刑事警察局——新聞活動》，＜網址：http://www.cib.gov.tw/news/Detail/29436＞。

城」是簽賭網站之站名；其犯罪之手法與方式，條列析述以下：

（一）在「金船娛樂城」簽賭網站內，賭客可以隨意購買與兌換各大簽賭網站之「籌碼」與「點數」；再者；賭客若持有非屬賭博屬性，而是屬於一般娛樂性質之博奕網站點數，「金船娛樂城」網站亦提供可將上述點數兌換成現金之服務[33]；此外，該賭博網站亦提供相當便利之交付賭資（金）之機制，亦即，賭客可在我方之各大超商付款，並列印繳費之單據，代表業已交付賭資，即可進行數百種之網上博奕遊戲，令賭客相當著迷；

（二）「金船娛樂城」簽賭網站宛然成為華人地區之「地下網路賭博匯兌中心」；為何其具有「網路賭博匯兌中心」之屬性？因它公開販售與兌換各大簽賭網站之籌碼與點數。

（三）「金船娛樂城」之主嫌，均為我方民眾，但其網站之主機，則架設在加拿大；而其客服系統，則架設於陸方；是以，它以跨越兩岸與加拿大之經營模式，逃避被偵破之風險，亦即，運用分散被逮捕風險之方式，進行網上賭博網站之經營。

（四）本案之所以被我方偵破，主因在於我方刑事警察局偵查第九大隊之偵查人員，主動發現該簽賭網站；之後，我方刑事警察局與陸方「網安局」相互交換該賭博網站之情資；我方在陸方「網安局」之協助之下，取得該網站之重要情資，成功鎖定犯嫌在我方之網路 IP，長期蒐證

33 點數兌換成現金之行爲，觸犯我方之刑法賭博罪。刑法第268條——意圖營利，供給賭博場所或聚眾賭博者，處三年以下有期徒刑，得併科三千元以下罰金。

之後，將其偵破；在簽賭之金額部分，超過上億元新台幣，其危害性相當嚴重；

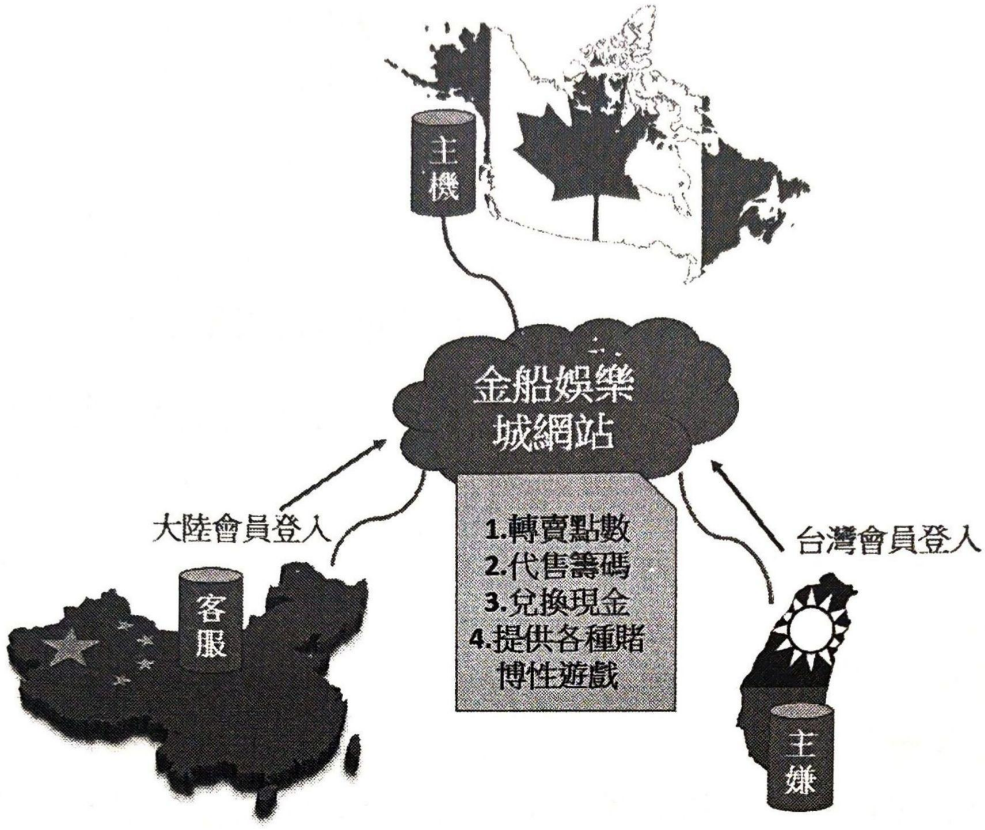
（五）「金船娛樂城」之犯罪手段，乃在其簽賭網站上宣稱，可協助線上玩家轉賣（轉售）點數，實際上，則是與其他網上簽賭網站相互掛勾，以外觀上，看似合法之「代售」點數之手法，實則掩護「非法」之遊戲點數之變現（將籌碼換回現金，即構成賭博罪[34]）。

（六）「金船娛樂城」之兌換點數機制，它連結多個知名之線上賭博網站，包括：黃金俱樂部、皇家娛樂城、太陽遊戲城、運動娛樂王等；而其線上賭博之遊戲項目，則包括：真人百家樂、真人三公、輪盤、骰寶、鬥地主、麻將、梭哈、21點、職棒球類簽賭與電子博奕遊戲，共上百種以上，相當誘惑民眾簽賭。

（七）賭客支付賭金之方式，類似於第3方支付之手法，而變現線上博奕遊戲之點數；

---

34 我方之<電子遊戲場業管理條例>第14條之中，亦有相關之規定：
電子遊戲場業得提供獎品，供人兌換或直接操作取得；限制級電子遊戲場每次兌換或取得獎品之價值不得超過新臺幣二千元；普通級電子遊戲場每次兌換或取得獎品之價值不得超過新臺幣一千元。
電子遊戲場業之兌換，不得有下列各款之行爲：
一、提供現金、有價證券或其他通貨爲獎品。
二、買回提供給客人之獎品。
獎品之價值以業者原始進貨發票作爲兌換獎品價值之依據。
獎品價值之上限，主管機關得依物價波動，逐年調整。
經中央主管機關許可之非營利性公益性團體，得經營公益收購站，收購限制級電子遊戲場所兌換之獎品。



圖四　「金船娛樂城案」犯罪手法示意圖

圖資來源：作者自繪

針對本案，兩岸執法機關在預防本案之網路賭博犯罪時，則有以下之困境：

（一）該網站之主機，架設在加拿大，而非在兩岸；兩岸執法人員即使啓動「兩岸共同打擊犯罪及司法互助」機制，仍然無法查扣「金船娛樂城」之主機；主因在於，其主機架設於加拿大；

（二）利用類似於第3方支付手法，免除線上簽賭時，須以「上線」或「組頭」之方式，收取賭金，逃避交付賭金之風險；

（三）加入賭局之低門檻，與從事一般線上遊戲無異，容易令民眾誤以為於此「金船娛樂城」將點數或籌碼兌換成現金之行為，未構成賭博罪；

（四）該網站以「代售」籌碼與點數之合法手法與外表，掩護非法之遊戲點數變現為金錢，易令民眾誤以為「金船娛樂城」係屬合法之網站，迷惑民眾之判斷能力；

三、毒品走私類：兩岸跨境犯罪組織利用新興網路通話軟體進行毒品交易犯罪計畫之溝通，造成查緝與監聽不易

以兩岸跨境毒品犯罪為例，根據我國學者之研究，我方之3級毒品K他命，在毒品市場之中，佔有主流之地位；我方之K他命，主要之來源地，係為陸方；毒品犯罪組織在從事販運之過程之中，具有以下之特色[35]：

（一）毒品犯罪組織會與黑幫組織進行策略性之合作，亦即，黑幫之勢力，亦會介入兩岸跨境之毒品犯罪組織；

（二）K他命從陸方運輸至我方之運毒路線，主要以海路運輸為主；

（三）兩岸跨境之毒品犯罪組織，亦使用網路電話與新興通話軟體，諸如：QQ、SKYPE 或 LINE 進行相互連繫，逃避查緝。

而兩岸執法人員於預防兩岸跨境網路犯罪之過程中，就毒品犯罪與網路犯罪之結合而論，主要之執法問題如下所述：

（一）若就毒品犯罪而言，其利益龐大，極易吸引犯罪組織投入此一毒品市場，俾利獲取暴利；

---

35 劉邦乾，《海路毒品販運組織及犯罪手法之研究》，（台北：國立臺北大學犯罪學研究所碩士論文，2012年）。

（二）我方人民對於K他命之需求，相當龐大；亦即，就需求面，市場上有龐大之民眾愛好施用K他命；

（三）極為少數之兩岸執法人員，甚至加入毒品組織犯罪之行列之中；

（四）毒品非常難以加以戒治，當我方民眾一涉及施用K他命之後，不易戒治，反覆施用，遂促使供給之陸方，不斷地輸出K他命；由於陸方不斷輸出K他命，更促使我方K他命之氾濫；

（五）台灣海峽之海面地理之便，利於兩岸毒品犯罪組織以隱匿之方式，運毒進入我方；

（六）假若兩岸跨境毒品犯罪組織份子使用 QQ、SKYPE、WeChat與LINE相互連絡毒品販運計畫，因此等之新興通話軟體保密性極強，無法監聽，常導致偵查之中斷，無法繼續偵辦[36]；

四、合作困境：兩岸執法機關，對於台灣跨境電信網路詐欺犯罪行為之偵查權、司法管轄權、懲處之刑度與司法互助等，漸趨缺乏共識，衝突時起

2014年11月，肯亞警方查獲台灣人在肯亞設立電信機房進行跨境電信詐騙，至2016年4月8日我方接獲通知，陸方要將8名在肯亞獲判無罪之台灣人，解送至大陸受審[37]，原因是這些網路詐欺案之台灣犯嫌，係從中國大陸登機，飛至非洲之肯亞，利用非法入境進入

---

36 張樹德，翁照琪，〈兩岸毒品犯罪型態與防治作爲之實證研究〉，發表於「2010非傳統安全－反洗錢、不正常人口移動、毒品、擴散」學術研討會（桃園：中央警察大學，2010年），頁37-57。

37 高照芬，〈肯亞詐騙案 陸委會：陸侵害管轄權〉，《中央通訊社》，2016年4月12日，＜http://www.cna.com.tw/news/firstnews/201604110441-1.aspx＞

肯亞，之後，再於肯亞架設電信網路設備，跨境向中國大陸人民施詐取財[38]，而詐欺案之被害人，全部均是中國大陸人民，並無台灣人被害，因此大陸始打算將台灣之加害人自肯亞押解至大陸受審。

上述8位犯嫌被押解至大陸地區，只是第一波之動作，最終本案總計有45位涉嫌跨境電信網路詐欺案之台灣犯嫌，被押解至回中國大陸，其中多數在肯亞檢方被起訴之罪名，係為「無照經營電信業」，均獲肯亞法院判決無罪，仍遭肯亞警察扣留，交給中國大陸[39]。而事實上，此45位之跨境電信網路詐欺案之犯罪人，其不法之犯罪所得，約為5億新台幣[40]，但肯亞之司法系統，竟無法將其定罪。由此，可看出肯亞之司法系統，無法有效地抗制此類之跨境電信網路詐欺犯罪，但亦造成兩岸之間，對於此類案件之司法互助關係起了變化。

針對上述案例，兩岸執法人員對於預防兩岸跨第三地（如跨肯亞）之跨境網路電信詐欺案犯罪之過程中，主要之合作困境條述如下：

（一）肯亞政府主張，跨境網路電信詐欺案之犯罪人，係從中國大陸登機，即從中國入境，故須遣返回中國大陸[41]。但，我國政府主張國籍國管轄權，應遣返回台灣，兩國之見解不一。

（二）不僅肯亞之司法系統，無法有效地抗制此類之跨境電信

---

38 楊明暐，〈肯亞：中國入境，所以遣返中國〉，《中國時報》，2016年4月13日，A2版。

39 唐筱恬、蕭承訓、蕭博文、林郁平，〈大陸辦詐欺罪，強行遣送台灣人。法部：符合刑事管轄原則〉，《中國時報》，2016年4月13日，A2版。

40 唐筱恬、蕭承訓、蕭博文、林郁平，〈大陸辦詐欺罪，強行遣送台灣人。法部：符合刑事管轄原則〉，《中國時報》，2016年4月13日，A2版。

41 楊明暐，〈肯亞：中國入境，所以遣返中國〉，《中國時報》，2016年4月13日，A2版。

網路詐欺犯罪（將多數犯罪人判決無罪），甚至是我國政府之司法體系，亦無法有效地抗制、壓制與制裁此類之跨境電信網路詐欺犯罪。

（三）跨境電信網路詐欺之犯罪人，似乎已掌握肯亞之司法系統，以及我國政府之司法體系，均無法有效地抗制、壓制與制裁此類之跨境電信網路詐欺犯罪，故令其有機可乘，遊走於兩國司法漏洞之間，對於中國大陸人民進行跨境電信網路詐欺犯罪。

（四）台灣本身對於是否應將此45位之跨境電信網路詐欺案之犯罪人，遣返回台灣，國內見解即分為2派，多數人之見解，主張應將此45位之跨境電信網路詐欺案之犯罪人，遣返回台灣，少數之人士，則持反對意見。中國大陸之意見，則幾乎均反對將此45位之跨境電信網路詐欺案之犯罪人，遣返回台灣。意見分歧嚴重，難有合作之空間。

柒、從犯罪預防觀點研析兩岸跨境網路犯罪防治之未來可行對策及建議

美國學者 Shipley 及 Bowker 認為對於網路犯罪之預防應有以下幾個重點[42]：

一、對於犯罪行為之明確定義。

二、大眾知識之提升以及教育。

三、發覺犯罪之可能性。

四、調查犯罪之成效。

---

42 Todd G. Shipley & Art Bowker, "Investigating Internet Crimes : An Introduction to Solving Crime in Cyberspace" (Massachusetts:Elsevier, 2014)

五、成功起訴之機率。

以上重點，均是預防網路犯罪之基本要素，目前兩岸網路犯罪案件頻傳，與是否落實做到上列要素，息息相關；因此，兩岸警察與公安機關對於兩岸跨境網路犯罪之犯防機制，應從犯罪預防觀點加以剖析，研擬相關可行之對策加以因應。本文乃犯罪預防理論出發，結合公共衛生之三段五級預防之觀點，分列提出以下十三項對策[43]，並整理如下表：

表一　本文研提對策與犯防理論及公衛觀點對照一覽表

犯罪預防理論	公共衛生三段五級預防觀點	本文所提研究對策
初級預防	第一級健康－促進健康	一、加強與提昇兩岸民眾對於兩岸跨境網路犯罪預防之意識、觀念與作法
	第二級健康－特殊保護	二、兩岸警察與公安機關宜於海峽兩岸共同打擊犯罪及司法互助協議之中，加入防治兩岸跨境犯罪之犯罪預防（包括網路犯罪之預防）之內容與範疇
		三、兩岸警察與公安機關宜共同攜手合作制定預防兩岸跨境犯罪（包括兩岸跨境網路犯罪之預防）之各式短、中、長期犯防計畫
		四、加大兩岸警察與公安機關對於違法網站之監控力道
		五、提升兩岸網路巡邏密度

43 本文所提對策與公共衛生三段五級之對應研究內容，係採納行政院謝顧問立功於中央警察大學2015 年『國境管理與執法』學術研討會與談暨講評之建議，在此特別感謝謝顧問立功之建議，使本研究更具價值性及完整性。

犯罪預防理論	公共衛生三段五級預防觀點	本文所提研究對策
次級預防	第三級健康－ 早期診斷，早期治療	六、建構舉發兩岸跨境網路犯罪之系統
		七、利用情境犯罪預防理論之觀點，建構兩岸治安機關監控網路犯罪之機制
		八、兩岸執法部門宜精進化跨境網路犯罪之預防機制，可行之作法，雙方似可建立「跨境網路犯罪預防」之實體及虛擬之交流平台，擴大辦理科學技術及實體法律之研討及交流
叁級預防	第四級健康－限制殘障	九、兩岸之執法部門均應更完善並妥適地規劃跨境網路犯罪之立法工作，以達到犯罪預防之效果 ，亦可參照澳門、加拿大與澳洲之立法例，考量訂定專門抗制跨境網絡犯罪之專法之可行性
		十、台灣執法部門宜重視跨境網路犯罪偵查人力之培育與在職訓練之機制，同時，宜強化與提升跨境網絡犯罪偵查人力之專業素質與知能，俾利有效地抗制跨境網絡犯罪之惡行
		十一、持續與新興通話軟體之公司，諸如：QQ、SKYPE或 LINE 進行相互連繫，請其提供破解其通訊封包之解密軟體與技術給予我方警察之監聽機關

犯罪預防理論	公共衛生三段五級預防觀點	本文所提研究對策
		十二、精進兩岸刑事司法互助之力道與成效，俾利兩岸執法機關能成功之起訴網路跨境犯罪之罪犯
	第五級健康－復健	十三、強化與精進跨境網路罪犯之監獄矯正機制，善用專才並導引適才適性之相關工作

資料來源：作者自行整理

一、加強與提昇兩岸民眾對於兩岸跨境網路犯罪預防之意識、觀念與作法

從本文所提及之「3仟萬城堡別墅機房兩岸電信詐欺案」之中，陸方被害人對於電信詐欺之犯防意識，確實尚待強化與提升；因此，本文建議，陸方公安機關宜透由各種管道，如新聞媒體、網際網路與文宣等，強化陸方民眾對於「電信詐欺」犯罪行為概念、犯行模式（手法）與犯行損害之正確認識（知），並教導民眾如何預防電信詐欺。

再者，亦須明確地告知民眾，於賭博網站之內，民眾將遊戲點數變現之作法（行為），亦觸犯我方之賭博罪[44]。透由針對於網路賭博犯罪之犯防宣導，藉以激發民眾對於網路賭博犯行之犯防意

44 我方刑法第二百六十六條所規範之公共「場所」或公眾得出入之「場所」之範圍，此等之「場所」，是否包括電腦網路？我方多數持肯定之見解（主流觀點），少數則持否定之見解——公共「場所」或公眾得出入之「場所」，其無法包括網路上之虛擬世界。建議修改我方刑法第二百六十六條所規範之公共「場所」或公眾得出入之「場所」之範圍，令其包括電腦網路，令普通賭博罪具有可預見性。由於賭博會令賭客進而觸犯其他犯罪，本文主張，刑法第二百六十六條普通賭博罪不宜除罪化。

識。此處之犯防意識，乃指由於民眾對於網路賭博犯罪具有正確之了解與認知，拒絕將遊戲點數變現，進而避免進入網路賭博之網站，並且免於觸犯賭博罪行。

二、兩岸警察與公安機關宜於海峽兩岸共同打擊犯罪及司法互助協議之中，加入防治兩岸跨境犯罪之犯罪預防（包括網路犯罪之預防）之內容與範疇

兩岸目前業已簽署「海峽兩岸共同打擊犯罪及司法互助協議」，就其本質而論，具有以下之特性：（一）它是偏向於兩岸共同打擊犯罪與司法上之互助及聯繫；亦即，似乎是針對於打擊業已發生之犯罪，這些之犯罪種類，規範於本協議中之第4條。就「犯罪預防」（crime prevention）機制而論，本協議未提及之；（二）「海峽兩岸共同打擊犯罪及司法互助協議」之另外一個本質，它是被動的，先非先發式之性質；亦即，兩岸執法部門所擬欲打擊之犯罪，係待該犯罪發生之後，先行檢視是否符合本協議第4條之規定，如屬於本協議第4條所含涉之犯行，且有必要進行兩岸執法機關之協力與互助，始正式啓動此一協議之機制。換言之，本協議之本質，它是處於被動之態勢，欠缺主動預防之機制。

是此，本文認為，兩岸警察與公安機關，有必要採取「P to P」（Police to Police）之模式，先拋棄政治上之議題，單純地聚焦於兩岸如何預防犯罪？由兩岸之警察與公安機關，似可共同簽署海峽兩岸共同預防犯罪協議，或者，備忘錄。行政院謝顧問立功則認為，本文上述所提及，有關兩岸警察與公安機關共同簽署防治兩岸跨境犯罪之犯罪預防（包括網路犯罪之預防）之協議或備忘錄部分，涉及犯罪預防（包括網路犯罪之預防）之協議或備忘錄，似可以加入兩岸共打協議之中，比較具有可行性，本文贊同之。

不過，假若情況更加允許，兩岸之警察與公安機關，共同簽署

海峽兩岸共同預防犯罪協議，或者，備忘錄，則更能彰顯兩岸警察與公安機關特別重視防治兩岸跨境犯罪之犯罪預防（包括網路犯罪之預防）之機制，針對防治兩岸跨境犯罪之犯罪預防之區塊而論，令其更加專業化。待時機更加成熟之後，宜提升與擴大兩岸預防犯罪之相關層級與廣度，令相關之機關，諸如：我方之法務部、司法院、移民署、調查局、海洋委員會、海巡署、關務署、志工團體……，與陸方之檢察院、法院、海關、志工團體……等相關機關，共同協力參與治理兩岸跨境犯罪（含網路犯罪）之議題。

三、兩岸警察與公安機關宜共同攜手合作制定預防兩岸跨境犯罪（包括兩岸跨境網路犯罪之預防）之各式短、中、長期犯防計畫

就我方而言，常見之犯防計畫，包括：竊盜、毒品、春安、校園安全……等等，但是，我方在處理涉及兩岸跨境犯罪之犯防議題（包括兩岸跨境網路犯罪之預防）之時，卻無法與陸方共同制定相關之犯防計畫，包括：無法共同制定兩岸跨境網路犯罪之犯防計畫。從「犯罪預防」之觀點出發，本文認為，各類型兩岸跨境之犯罪（包括兩岸跨境網路犯罪），仍是具有可預防性。不過，此一作法與機制，它考驗兩岸警察與公安機關之相互信任性、智慧、能力、學識、意願與創新性。

最傑出與最優秀之警察與公安機關，是令兩岸跨境之犯罪，消弭於無形，令跨境犯罪（包括兩岸跨境網路犯罪）無法發生；此種之警政，即為「兩岸跨境犯罪（包括兩岸跨境網路犯罪）預防警政」。本文在此，提出「兩岸跨境犯罪預防警政」之構想與作法，供兩岸執法部門參考。在實際之作為方面，首先，兩岸警察與公安機關，須先取得共識，認為共同制定「兩岸跨境犯罪（包括兩岸跨境網路犯罪）預防計畫」有其必要性與重要性。

就此部分而言，作者認為，對於兩岸跨境犯罪（包括兩岸跨境網路犯罪）之治理，恐須建構更積極之機制與觀念，此一極為核心之想法，即「事前預防重於事後處理（打擊）」；對於兩岸跨境犯罪（含網路犯罪）之治理，宜強調「事前預防重於事後處理（打擊）」之作法與想法。

四、加大兩岸警察與公安機關對於違法網站之監控力道

兩岸常見之違法網站仍以賭博網站及色情網站為主，關於賭博網站類型除本文前述之「金船娛樂城簽賭網站」之案例外，在國內常見之賭博網站類型尚有「國際職業運動（如棒球、籃球、足球）簽賭網站」，此類賭博網站之組頭經常侵入結合不良幫派入侵校園，吸收學生作為幫派份子並擔任簽賭網站之二組頭，以退佣之模式讓擔任小組頭之學生賺取外快[45]，藉以去招攬同學，以小額下注之方式[46]，破壞整個校園及社會秩序，是相當嚴重之校園及社會問題。

另色情網站常見之類型則為「一對一視訊聊天室」及「會員制網路應召站」。前者係通過一對一之聊天方式，進行視訊猥褻交易，從事該工作之女性聊天室主持人，因不用實際上與男性客人進行身體上之接觸，因此，吸引許多無知之女性學生及上班族，以兼差賺取外快之心態加入經營，殊不知所有視訊猥褻內容，已被網站經營者另行錄影，再上傳至會員制之色情網站提供會員觀賞，以賺取高額入會費。至於「會員制網路應召站」則與一般應召站之犯罪行為無異，只是其媒介管道係利用架設網站，採熟客會員制，提供賣淫女子之照片或視訊（俗稱茶照或魚訊）給熟客觀看，並透過網站與

45 網路術語稱之為「水錢」，通常退傭之金額為下注金額之3%至8%不等。

46 一般簽賭網站下注金額至少均以新臺幣1,000元為單位，但是針對學生賭盤，組頭會降低下注門檻，以學生零用錢300元或500元即可下注。

熟客保持聯繫，隨時提供賣淫女子之最新資訊，讓會員可隨時與應召站約定性交易事宜。

上列違法網站多由犯罪集團進行經營，為避免治安機關查緝，通常採跨國（境）之經營模式，網站之機房並不會設置在被害者所在之國家或地區，以增加被害者國家之治安機關之查緝困難度，因此，想破獲此類案件，必須要透過不同國家或地區之治安機關跨國（境）合作，我方和陸方雖已簽署「海峽兩岸共同打擊犯罪及司法互助協議」，但是合作之案類多著重於詐騙案件，查緝之目標為電話機房，但對於查緝設置賭博網站或色情網站之電腦機房，著墨較少，然而兩岸治安機關對於非法網站之偵查設備及技巧，早有一定之水準，惟礙於兩岸政治關係，陸方之網路資訊經常採封鎖作為，造成我方治安機關人員偵辦案件不易，因此，應該深入利用兩岸共同打擊犯罪之管道，進行情資交流，以確實擴大兩岸對於違法網站監控之力道。

五、提升兩岸網路巡邏密度

兩岸治安機關對於網路犯罪之偵查，均設置有專業之偵查單位負責辦理，如我方內政部警政署刑事警察局編制偵查第九大隊即為科技網路犯罪偵查之專責單位；另陸方公安部編制公共信息網絡安全監察局（含下設之處、科），通稱為網監機關，其單位人員即為一般熟知之網監警察（或稱網絡警察），除監控大陸民眾一般使用之網路訊息外，亦負責偵辦網路犯罪案件；儘管兩岸治安機關均已設置專業單位查緝網路犯罪行為，但犯罪集團利用架設違法網站進行犯罪之行為，仍然層出不窮。

治安機關對於傳統犯罪手法之犯罪預防工作較為重視，但正如前文所提之「犯罪之摩爾定律」，網路犯罪預防已成為犯罪預防核心工作之一，然而，除兩岸治安機關編制之專責單位可投入人力等相

關資源進行網路犯罪偵查外，其餘單位鮮少有規劃偵辦網路犯罪案件，但網路空間無遠弗屆，單靠專責單位之人力有限，難以彰顯執行成效，造成網路犯罪集團採多點突破式之犯罪手段，針對警方偵查弱點進行犯罪行為；因此，以提升網路巡邏密度作為網路犯罪預防之對策，確有其必要性。

網路巡邏之執行具有相當之困難度，畢竟網路無轄區，其執行巡邏之區域、範圍、執勤重點均難以界定，且執勤人員必須對於網路架構及資訊管理有基礎之概念，又所需投入之人力資源龐大，難僅依靠上述兩岸治安機關設國之專責單位人力可完成。因此，網路巡邏仍應再搭配本文下述之志工機制及教育機制，完成整體配套措施，另可將網路犯罪巡邏納入基層警察單位之正式勤務之規劃，以達網路犯罪預防之效果並從警察教育中加強培育科技偵查人才，始能落實網路犯罪巡邏之勤務工作。

六、建構舉發兩岸跨境網路犯罪之系統

偵查網路犯罪案件，必須著重偵查人員之科技專業性，因此，兩岸治安機關始需設置專責網路犯罪偵查單位，但是，專責單位人力及資源皆有限，一般網路犯罪之受害者欲報案時，並無法直接向專責單位舉發，大部分仍是透過110報案專線，或就近至轄區派出所報案，而第一線執勤單位接受報案後，對於網路犯罪行為通常無法立即處置，僅能將案件轉送轄區分局偵查隊，再由轄區分局偵查隊視情形報請刑事警察局提供偵查技術或設備支援，又若案件係涉及兩岸跨境網路犯罪時，後續則須再啓動兩岸共同打擊犯罪機制，但如此一來，就會影響偵查之時效，錯過蒐集犯罪證據之最佳時機。

礙於兩岸關係問題，目前若欲兩岸共同建構網路犯罪通報系統，有實質上之困難，但兩岸治安機關針對網路犯罪行為，至少應能在網路上各自建置網路犯罪即時通報系統，讓被害人第一時間能

在網路上進行線上報案及提供相關證據資料，然後雙方所建置之系統，再資訊安全及維護人民權益之考量下，可建置系統資訊交流平台，將涉及兩岸網路犯罪之資訊第一時間通報雙方系統，共同即時偵查，始能達到第二級犯罪預防之效果。

七、利用情境犯罪預防理論之觀點，建構兩岸治安機關監控網路犯罪之機制

情境犯罪預防（Situational Crime Prevention），是美國學者羅納．克拉克（Ronald Clarke）所提倡，該理論焦點著重於對某些特定犯罪類型，以一種較有系統、常設之方法，對犯罪環境加以管理．設計或操作，增加犯罪之困難與風險，減少犯罪酬賞，以達到犯罪預防之目的；許春金教授亦認為，加強監控將有效使犯罪者不敢下手，達到犯罪預防之效果。

陸方之網監機關原本就負有監控民眾使用網路之情形，作為犯罪預防之手段，但是亦因為涉及違反人權，而遭國際社會抨擊；因此，網路監控機制應比照通訊監察機制，係針對特定具犯罪嫌疑之網站或人員，由治安機關報請司法機關核准後，始進行監控網路犯罪，較為完善。另兩岸亦應針對網路犯罪監控訂定合作模式，俾利建構兩岸治安機關監控網路犯罪之機制。

八、兩岸執法部門宜精進化跨境網路犯罪之預防機制，可行之作法，雙方似可建立「跨境網路犯罪預防」之實體及虛擬之交流平台，擴大辦理科學技術及實體法律之研討及交流

兩岸跨境網路犯罪有增加之趨勢，然而，兩岸目前對於相關案件之偵辦及交流，仍以兩岸共同打擊犯罪之平台為主，就合作之個案進行交流；另亦有在學術進行相關交流，諸如每年由兩岸四地分

別主辦「兩岸四地警學研討會」，針對兩岸四地警學領域之各種案類，進行研究探討及工作經驗分享。但目前兩岸對於跨境犯罪預防並無具體且實質之交流平台，可供兩岸執法人員進行較深入之研討。

如本文前述，網路犯罪需要建置良善之通報系統，始能達到二級犯罪預防之效，而兩岸通報系統之間，則需建置一虛擬之交流平台，除即時案件之通報外，亦可交流相關網路科技犯罪之資訊；另兩岸對於網路犯罪立法之議題，尚有相當多之研議空間，亦可考慮擴大辦理此類議題之兩岸四地研討會，基於兩岸四地人文相近，相關立法及偵辦經驗均可相互借鏡，對彼此均有助益。

九、兩岸之執法部門均應更完善並妥適地規劃跨境網路犯罪之立法工作，以達到犯罪預防之效果[47]，亦可參照澳門、加拿大與澳洲之立法例，考量訂定專門抗制跨境網絡犯罪之專法之可行性

本文前已針對有關兩岸對於網路犯罪之法令規範進行初步探討，兩岸法令對於網路虛擬犯罪之範疇，並無制訂專法，係規範於相關刑事法典；而兩岸對於網路實境犯罪之處罰，則是回歸到犯罪行為本質所違反之罪刑予以處罰，因此，除偵辦網路犯罪案件之同仁，必須熟稔不同法典之各項法令，一般社會民眾對於網路犯罪究涉及何種刑責，普遍認知不深，影響犯罪預防之效果。

澳門對於網路犯罪之刑事法令規範，原本係規範於《澳門刑法典》第213條之"資訊詐騙罪"以及第187條"以資訊方式做出之侵入（私人生活）"兩項罪名，但因為以科技資訊侵害人民之生活秩序之犯罪已相當普遍，僅靠原本之法令規章完全不敷使用，且若以所侵

47　如增修我方將刑法第二百六十六條所規範之公共「場所」或公眾得出入之「場所」之範圍，擴大包括至電腦網路。

害之刑責作為區分，分別去修正相關刑事法典，似有「頭痛醫頭、腳痛醫腳」之虞，亦無法全面對於電腦網路犯罪訂出完整之刑法規範。因此，澳門於於2009年制定《打擊電腦犯罪法》以此改善澳門刑事立法中關於網絡犯罪之單一性之立法，對於特殊主體實施之電腦犯罪，進行加重規定，並對法人實施之電腦犯罪之形式責任予以明確之規定，並且將《刑法典》之規定與該法律補充適用，最大程度實現刑法對電腦犯罪之打擊[48]。

澳門所面臨之電腦網路犯罪立法之問題，與兩岸治安機關所面臨之問題雷同，然而，澳門已針對立法弱點加強改進，制定《打擊電腦犯罪法》，針對以下之罪行：對不當進入電腦系統；不當獲取、使用或提供電腦系統數據；不當截取電腦數據；損害電腦資訊及數據；干擾電腦系統；用作實施犯罪之電腦裝置或電腦數據；電腦資訊偽造；電腦進行詐騙等八項電腦犯罪行為之犯罪構成和刑罰進行法律上之規範，補充原單行刑事法典之不足。

復次，在2013年，加拿大新斯科舍省（Nova Scotia）制訂《網路安全法》（Cyber-Safety Act）[49]，該法具有以下之特色：

（一）針對網路霸凌者之刑責為6個月監禁，得科或併科最高5,000加幣之罰金。

（二）授權成立網路調查單位，可接受霸凌申訴。

（三）警方接獲調查單位申訴後，可進行調查處理。

（四）網路霸凌受害者，可向法院申請保護令，法院可停止加害人使用其電子軟體，情形嚴重之時，尚可沒收加害人

48 楊秀莉，〈中國內地與澳門網絡犯罪的刑法比較及完善建議〉，《”一國兩制”研究》，第1期，2012年，頁176-184。

49 Nova Scotia Government Bill NO. 61, 5th Session, 61st General Assembly Nova Scotia 62 Elizabeth II, 2013, < http://nslegislature.ca/legc/bills/61st_5th/1st_read/b061.htm>.

之手機或平板電腦。

另加拿大亦於2015年，正式實施「保護加拿大國民遠離網路犯罪法」（Protecting Canadians from Online Crime Act，簡稱 Bill C-13）[50]，保護加拿大國民遠離網路犯罪法之專法，該法具有以下之特色：

（一）係修正刑法、競爭法及證據法。

（二）適用對象：不分是否成年，皆有適用。

（三）補充修訂非自願之親密圖片散佈法令，授權法官得從網路上移除這些圖像及收取回復費用，得以沒收財產及下達擔保命令，以限制加害人使用電腦或網路就此類圖像之散布。

（四）賦予保存請求權和命令之權力，強制保全電子證據。

（五）新訂法院可下達提供命令，強制相關義務人提供通訊傳輸、交易位置、個人及相關事物資訊。

（六）授權延長關於使用電信傳輸相關資料之調查權。

（七）授權與法律分配利害關係相關之交易、個人與事物等做為追蹤調查對象。

（八）在取得法官授權及命令程序方面，《網路犯罪專法》簡化關於取得關於截取私人通訊之法官授權及命令程序。

（九）修訂加拿大證據法，以確保加害人之配偶得為被害人證人。

（十）將「散播私密照片」定義為網路霸凌行為，將其犯罪化——「散播私密照片罪」，未經當事人同意散播私密照

50 Bill C-13, An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act. < https://openparliament.ca/bills/41-2/C-13/>.

片者，被告最高可處5年監禁。

此外，澳洲在2015年3月，亦立法通過《提升兒童上網安全法》（Enhancing Online Safety for Children Bill 2015），該法案重要之特色，如下所述：

（一）特別創設「兒童電子安全委員會」（Children's e-Safety Commissioner）。

（二）「兒童電子安全委員會」之安全委員，可以接受社會大眾之投訴，並調查兒童網路霸凌案件。

（三）「兒童電子安全委員會」可針對網路業者發出即時移除不當資訊之命令。

（四）若業者經社會大眾之申訴後，未於48小時內，或安全委員要求之時間內移除者，兒童電子安全委員可介入處理。

而新加坡在2014年通過《防止騷擾法》(Protection From Harassment Act 2014)[51]，該法具有以下之特色：

（一）網路騷擾或霸凌之態樣，亦可適用《防止騷擾法》。

（二）網路騷擾或霸凌之受害者，可向法庭申請保護令。

（三）網路騷擾或霸凌之受害者，可向法庭要求即時移除網路惡意資訊，阻止對方繼續騷擾。

在國際上許多國家均已針對網路犯罪行為訂定相關專法予以規範，兩岸在網路犯罪之立法上，亦可參考澳門、加拿大、澳洲與新加坡之立法例，針對兩岸網路犯罪之特性及案類，研議制定相關專法之可行性。

---

51 An Act to protect persons against harassment and unlawful stalking and to create offences, and provide civil remedies related thereto or in relation to false statements of fact. < http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId%3A%2207275b05-417a-4de5-a316-4c15606a2b8d%22%20Status%3Ainforce%20Depth%3A0;rec=0 >

十、台灣執法部門宜重視跨境網路犯罪偵查人力之培育與在職訓練之機制，同時，宜強化與提升跨境網絡犯罪偵查人力之專業素質與知能，俾利有效地抗制跨境網絡犯罪之惡行

台灣對於科技網路警察之養成教育，係於內政部中央警察大學設有警察科技學院，下設資訊管理學系，對於科技犯罪偵查有完整之培育系統，惟中央警察大學畢業之學生係為警界之幹部人才，至基層執行單位多擔任主管職務，並非勤務執行者；然而，培育基層警察人員之臺灣警察專科學校，設有行政警察科、刑事警察科、交通警察科、消防安全科及海洋巡防科，共科5科系，然對於科技犯罪方面，並無設立相關科系，爰負責第一線執勤之基層警員，對於科技犯罪偵查工作並無足夠之專業知識。

另陸方中國人民公安大學，在高級警官培育部分，自1984年成立公安科技系，增加電腦應用專業，2002年改為信息安全工程系，為培育網路警察之前身，至2013年更名為網路安全保衛學院，集理（數學）、工（計算機、通信、網路）、管（信息安全與管理）、法（網路調查與執法）四位一體，並含蓋博、碩士學位，依據陸方官網稱，迄今已培養各級公安科技專業人才和高科技犯罪調查人員上萬名。

另陸方在中國人民公安大學之本科生（學士學位生）培育部分，則設有治安學系、偵查學系、國內安全保衛系、公安管理學系、公安情報學系、犯罪學系、涉外警務系、警務指揮與戰術系、刑事科學技術系、安全防範工程系、交通管理工程系、網路安全與執法系；對於網路安全執法事項，在警察養成教育中，即已相當重視。

相較之下，臺灣警察教育對於科技網路犯罪人才之培育，則略顯不足；在，應該要從警察養成教育即落實培育專業人才，始足能應付現代社會所面臨之資訊網路犯罪。除警察養成教育外，警察在

職教育亦應建立育才之機制，然而，在職訓練所面臨之困難則是基層警員多不具備科技網路專才之背景，惟欲偵辦科技網路犯罪，仍須具有基礎之計算機概念或資訊網路運作概念，因此，對於網路犯罪預防與偵查之在職訓練，必須適才適所進行分階段訓練，對於毫無資訊概念之同仁，應從計算機概論進行訓練，始能使執勤同仁逐漸跟上時代之腳步，提升警察機關整體偵查網路犯罪之戰力。

十一、持續與新興通話軟體之公司，諸如：QQ、SKYPE 或 LINE 進行相互連繫，請其提供破解其通訊封包之解密軟體與技術給予我方警察之監聽機關

通訊監察是犯罪偵查之利器，透過監聽犯罪嫌疑人之電話聯繫內容，能確實掌握其犯罪事實及行蹤動態，作為偵查犯罪之有利證據。然而，現在資訊網路盛行，各類通訊軟體如雨後春筍般冒出，百家爭鳴，推出免費視訊通話，多種圖文併茂之溝通方式，使傳統電話及行動電話聯繫方式已漸漸式微；然而，這些通訊軟體大都標榜鎖碼，除非取得軟體公司之授權並提供解碼器，否則完全無法監看或監聽，強調人權之保障，卻亦成為犯罪集團作為聯繫工具之利器，更造成警方在犯罪偵查上相當大之困擾。

因此，如何能在人權與犯罪偵查中取得平衡，使通訊軟體公司願意提供解碼器給警方作為偵查犯罪之用，實為相當重大之課題。治安機關仍應持續努力與通訊軟體公司進行協商，請其提供破解其通訊封包之解密軟體與技術給予我方警察之監聽機關，以達犯罪預防之效。

十二、精進兩岸刑事司法互助之力道與成效，俾利兩岸執法機關能成功之起訴網路跨境犯罪之罪犯

前文所提 Shipley 及 Bowker 認為網路犯罪之預防之五項重點，

其中包含「成功起訴之機率」，此是三級犯罪預防理論之第三級預防工作中相當重要之一環，然而兩岸執法機關是否能有效起訴網路跨境犯罪，其與兩岸刑事司法互助之力道有必然之關連性。

茲以上文肯亞詐騙案，台灣犯嫌究竟應該解送至何處接受審判為例，即可發現兩岸刑事司法互助已產生嚴重問題，部分媒體認為大陸方面之所以強烈要求將在肯亞犯罪之台灣犯嫌解送至大陸接受審判，主要因素之一是因為台灣方面對於跨境犯罪之詐欺犯所判刑責太輕[52]，亦即不能達到第三級犯罪預防之效果；而另一要素即是涉及兩岸對於犯嫌之管轄權問題，究竟大陸地區是否屬於中華民國憲法上之固有領域？國內之見解不一，其所導致之管轄權之見解，即會不同。假若，主張大陸地區仍是屬於中華民國憲法上之固有領域，則依據我國刑法第3條之規定，本法於在中華民國領域內犯罪者，適用之。亦即，我國仍有領域管轄權及國籍國管轄權。反之，假若，主張大陸地區並非是屬於中華民國憲法上之固有領域，則無法依據刑法第3條之規定，主張我國仍有領域管轄權。此時，所適用之條文，即須變更改為刑法第7條之屬人原則。依據刑法第7條之規定：「本法於中華民國人民在中華民國領域外犯前二條以外之罪，而其最輕本刑為三年以上有期徒刑者，適用之。」然而，由於刑法第339條之4之加重詐欺罪 ，其刑度為一年以上七年以下，不符合最輕本刑三年以上之罪之規定與要求，故此等犯罪人之犯罪行為，返台接受審判之結果，均是不罰 。是以，我國如主張九二共識，一個中國，各自表述之中華民國憲法上之傳統見解，較對我方有利，較能

52 中央社，〈詐騙案 陸最高判無期台灣輕罪易科罰金〉，《中央通訊社》，2016年4月12日，＜https://tw.news.yahoo.com/%E8%A9%90%E9%A8%99%E6%A1%88-%E9%99%B8%E6%9C%80%E9%AB%98%E5%88%A4%E7%84%A1%E6%9C%9F%E5%8F%B0%E7%81%A3%E8%BC%95%E7%BD%AA%E6%98%93%E7%A7%91%E7%BD%B0%E9%87%91-103014660.html＞。

得出中華民國仍是具有領域管轄權之結論。

十三、強化與精進跨境網路罪犯之監獄矯正機制，善用專才並導引適才適性之相關工作

因目前網路犯罪並無設立專法，法務部對於各類犯罪案件之統計，仍以刑法上之罪責作為區分（如：竊盜、殺人、賭博……）[53]，其中雖有「妨害電腦使用罪」，但其與本文定義之網路犯罪意義相差甚遠，爰以，本研究尚無法根據法務部現有之公開資料，用以統計本文定義之網路犯罪相關數據。

ATM 犯罪在各國均是常見之犯罪類型，根據我國學者研究，ATM 犯罪之再犯率相當高[54]，且犯罪手法更是日益精進，2016年7月，我國第一銀行 ATM 系統遭跨國犯罪集團以惡意程式入侵，在各分行合計盜領約新臺幣8千多萬元[55]，造成全台銀行界及存户之恐慌。但如何降低犯罪之再犯率？除加重刑事責任以外，本文建議亦可加強監獄矯正機制，尤其是針對跨境網路犯罪之罪犯。

---

53 許春金，陳玉書，蔡田木，〈中華民國103年犯罪狀況及其分析——2014犯罪趨勢關鍵報告〉，《法務部司法官學院104年委託研究計畫》，2015年12月，＜http://www.moj.gov.tw/ct.asp?xItem=392644&ctNode=35595&mp=302＞。

54 范國勇，江志慶，〈ATM 轉帳詐欺犯罪之實證研究〉，《刑事政策與犯罪研究論文集（8）》，2005年11月，頁185-208。

55 顏真真，〈一銀 ATM 盜領案 星展銀總座：運氣較差，大家都要小心〉，《今日新聞》，2016年7月14日，＜https://tw.news.yahoo.com/%E9%8A%80atm%E7%9B%9C%E9%A0%98%E6%A1%88-%E6%98%9F%E5%B1%95%E9%8A%80%E7%B8%BD%E5%BA%A7-%E9%81%8B%E6%B0%A3%E8%BC%83%E5%B7%AE-%E5%A4%A7%E5%AE%B6%E9%83%BD%E8%A6%81%E5%B0%8F%E5%BF%83-074416937.html＞；邱俊福、王冠仁、劉慶侯、陳慰慈，〈盜領兵團增至9人　6人已出境〉，《自由時報網》，2016年7月15日，＜http://news.ltn.com.tw/news/society/paper/1011201＞。

監獄矯正機制是屬於犯罪預防理論之參級預防，亦為公共衛生三段五級預防觀點之復建階段；根據法務部104年法務統計年報[56]顯示，在監獄矯正工作部分，雖然設有「多元化技能訓練」及「強化教化輔導工作」等項目，但對於跨境網路罪犯而言，其犯罪手法之專業度應已不需再進行各關技能訓練，且根據上開年報內容，所謂教化輔導工作係指「品德教化」與「宗教教化」，並未見有可導引適才適性之輔導工作。對於具有專業性之受刑人，如能與其專才相關之企業或公營機關，甚至是公務機關進行矯正輔導之合作，導引受刑人至可發揮長才之處所就業，後續並搭配相關之輔導措施，定期關懷訪視，應可發揮參級犯罪預防之作用，降低其再犯率。

捌、結　論

犯罪預防在警政工作中，偏屬幕後性質工作，無法受到鎂光燈之關注，亦難以論斷執行成效，因此，願意投入犯罪預防工作之人數不多，相對亦造成業務推動上之困難。雖然，在每一級之犯罪預防中，均可以列出相關量化數據作為績效指標[57]，但是，單從這些量化績效指標，仍是無法完整呈現犯罪預防之成效：如何佐證因辦幾場犯罪預防之宣導，而確實防止幾件犯罪案件發生？如何佐證受刑人服刑完畢後沒有再犯罪，是因為刑罰效果所致？因為犯罪預防之本質是防範於未然，最好之預防成效就是什麼事均沒發生，但這些

56 法務部，〈104年法務統計年報〉，2016年6月27日，《法務部官方網站》，＜網址：http://163.29.130.186/RJSDWEB/book/Book.aspx?category_id=4＞。

57 如：初級之犯罪被害預防之部分，可以用辦理預防宣導之場次、參與宣導之人次等項目作爲績效指標；次級犯罪預防之部分，可以用警察在銀行臨櫃或提款機前，阻止了詐欺被害人匯款（消除了風險環境）等事項作爲績效指標；叁級預防部分，可以用受刑人之再犯罪率等項目作爲績效指標。

均不是單靠量化數據能夠解釋的。

相較之下，犯罪偵查工作卻經常能獲得鎂光燈之聚焦，從破獲刑案，逮捕犯嫌，起獲槍枝、毒品、贓款，均可以立即展現出工作成果，具有安定社會民心之效果，工作人員亦容易獲得較高之成就感。因此，目前在警政工作上普遍重視犯罪偵查多於重視犯罪預防，使得犯罪預防之工作推動原本不易，若想再將防罪預防理念運用於更難掌握之網路跨境犯罪上，難度其實相當高。

欲在兩岸跨境網路犯罪上達到預防之成效，最重要之部分，仍是得架構起兩岸治安機關之間之合作及溝通平台，在過去2008年至2015年間，兩岸之間建立起無數官方與民間之間之平台，互通有無，突破以往60年多來，兩岸交流之低迷狀況；然而，因為政治因素所致，自2016年蔡英文總統就職至今將近2個月以來，兩岸交流又逐漸陷入低潮期[58]，對於兩岸之間共同打擊或預防犯罪之工作，亦將是另一層次之挑戰。雖然人民生活安全及財產，不應受政治關係影響而失去保障，惟現實是，兩岸之間之交流卻均建立在微妙之政治關係之上，欲討論兩岸關係之相關議題，恐無法不去面對政治問題，此亦是研究兩岸關係重要變項之一。雖然政治因素並非本文研究之核心問題，但基於兩岸跨境網路犯罪預防之合作需求，一方面期待蔡英文總統在未來能秉持競選政見，與大陸維持現狀不變，持續保持良好互動關係，另一方面亦希望兩岸治安機關能以兩岸民眾福祉為前題，參酌上文所提之12項對策及建議，採取更多元之跨境網路犯罪防治作為，尤其是建立共通之平台，讓日益嚴重之跨境網路犯

58 綜合報導，〈兩岸溝通機制停擺？中國統戰戲來台免費演出〉，《自由時報新聞網》，2016年6月26日，＜http://news.ltn.com.tw/news/politics/breakingnews/1742429＞.

罪問題能有解決之道，讓未來之犯罪[59]，成為不會發生之犯罪，此實為犯罪預防之最終目標。

參考文獻

一、中文資料

1. Marc Goodman（2016），林俊宏譯，《未來的犯罪》，（新北：木馬文化）。
2. 王勁力（2010），〈論我國高科技犯罪與偵查——數位證據鑑識相關法制問題研究〉，《科技法律評析》，第3期，（高雄：國立高雄第一科技大學）。
3. 王勁力（2013），〈電腦網路犯罪偵查之數位證據探究〉，《檢察新論》，第13期，（台北：台灣高等法院檢察署）。
4. 王寬弘（2011），〈大陸地區人民進入台灣相關入出境法令問題淺探〉，2011年人口移動與執法學術研討會，（桃園：中央警察大學）。
5. 王寬弘（2012），〈大陸地區人民進入台灣相關入出境法令問題淺探〉，《國土安全與國境管理學報》，第17期，（桃園：中央警察大學），頁155-185。
6. 孟維德、黃翠紋（2012），《警察與犯罪預防》，（台北：五南）。
7. 邱俊霖（2015），〈近年科技犯罪趨勢與犯制對策〉，《刑事雙月刊》，第65期，（台北：內政部警政署刑事警察局）。
8. 范國勇，江志慶（2015），〈ATM轉帳詐欺犯罪之實證研究〉，《刑事政策與犯罪研究論文集（8）》，頁185-208。
9. 徐振雄（2010），〈網路犯罪與刑法「妨害電腦使用罪章」中的法

59 美國學者 Marc Goodman 所稱未來之犯罪，就是指網路犯罪之氾濫；詳見 Marc Goodman(2016)，林俊宏譯，《未來的犯罪》，(新北市：木馬文化公司)。

律語詞及相關議題探討〉，《國會月刊》，第38卷第1期，（台北：立法院）

10. 張樹德，翁照琪（2010），〈兩岸毒品犯罪型態與防治作為之實證研究〉，《2010非傳統安全——反洗錢、不正常人口移動、毒品、擴散學術研討會》，（桃園：中央警察大學）。
11. 許春金（2007），《犯罪學》，（台北：三民）。
12. 許春金，陳玉書（2013），《犯罪預防與犯罪分析》，二版，（台北：三民）。
13. 許福生（2016），《犯罪學與犯罪預防》，（台北：元照）。
14. 陳明傳（2007），〈跨國（境）犯罪與跨國犯罪學之初探〉，收於第一屆國土安全學術研討會論文集，（桃園縣：中央警察大學）。
15. 陳明傳（2015），〈各國入出國管理系統之比較研究〉，發表於中央警察大學移民研究中心2015年「人口移動與執法」學術研討會，（桃園縣：中央警察大學）。
16. 黃秋龍（2008），〈中國大陸網路犯罪及其衝擊〉，《展望與探索》，第6卷第12期，（台北：法務部調查局）。
17. 廖福村（2007），《犯罪預防》，（台北：警專）。
18. 劉邦乾（2012），《海路毒品販運組織及犯罪手法之研究》，（台北：國立臺北大學犯罪學研究所碩士論文）。
19. 蔡德輝（2009），《犯罪學》，（台北：五南）。
20. 鄧煌發（1997），《犯罪預防》，（桃園：中央警察大學）。
21. 鄧煌發、李修安（2012），《犯罪預防》，（台北：一品）。
22. 謝立功（2004），〈由大陸觀光客脫團事件論我國國境管理機制〉，《展望與探索》第2卷第9期，（台北：法務部調查局），頁14-20。

二、外文資料

1. Reyes, A. (2007). Cyber Crime Investigations: Bridging the Gaps Between, Security Professionals, Law Enforcement, and Prosecutors.(USA: Syngress).
2. Britz, Marjie T.(2009). Computer Forensics and Cyber Crime : An Introduction, Second Edition.(USA: Prentice Hall)
3. Evans, K. (2011). Crime Prevention: A Critical Introduction. (USA: SAGE Publications Ltd).
4. Fennelly, L. & Crowe, T.(2013). Crime Prevention Through Environmental Design, Third Edition. (USA: Butterworth-Heinemann).
5. Clough, D.(2010). Principles of Cybercrime. (UK: Cambridge University).
6. Mackey, D & Levan, K(2011). Crime Prevention. (USA: Jones & Bartlett Learning).
7 Schneider, S.(2014). Crime Prevention: Theory and Practice, Second Edition. (USA: CRC Press).
8. Lab, P. (2013). Crime Prevention: Approaches, Practices, and Evaluations. 8th Edition. (USA: Routledge).
9. Todd, G. & Bowker, A. (2014). Investigating Internet Crimes : An Introduction to Solving Crimes in Cyberspace. (USA: Steven Elliot)

三、網路資料

1. Council of Europe(2015), "Convention on Cybercrime", Retrieved on 2015/10/02, http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=11&DF=6/21/2007&CL=ENG.

2. Twelfth United Nations Congress on Crime Prevention and Criminal Justice(2015), "Working paper prepared by the Secretariat on recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime, A/CONF.213/9", Retrieved on 2015/10/02, http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/V1050320e.pdf .
3. 土城分局（2015），〈刑事局偵破「3仟萬城堡別墅機房」兩岸電信詐欺集團案，新北市政府警察局新莊分局〉，上網瀏覽時間：2015/10/01, http://www.xinzhuang.police.ntpc.gov.tw/cp-492-11757-18.html。
4. 中華人民共和國公安部（2015），〈公安部與美國警方聯合摧毀全球最大中文淫穢色情網站聯盟〉，瀏覽日期：2015/10/30，網址：http://app.mps.gov.cn:8888/gips/contentSearch?id=2871356。
5. 立法院（2015），〈「防治網路霸凌」公聽會：立委王育敏召開公聽會，研商網路霸凌防治〉，瀏覽日期：2015/11/12，http://www.ly.gov.tw/03_leg/0301_main/public/publicView.action?id=6512&lgno=00004&stage=8。
6. 刑事警察局偵查第9大隊（2015），〈國內首宗兩岸合作偵破最大網站賭博第3方支付中心〉，上網瀏覽時間：2015/10/01, http://www.cib.gov.tw/news/Detail/29436。
7. 林宜隆、葉家銘（2008），〈論述 ISMS 資訊安全管理系統發展網路犯罪預防策略的新方法〉，發表於教育部 TANet 2008研討會，(台北：教育部，2008)，瀏覽日期：2015/11/1，網址：http://www.powercam.cc/show.php?id=678&ch=23&fid=119。
8. 教育研究院「雙語詞彙、學術名詞暨辭書資訊網」(2015)，上網瀏覽時間：2015/10/01, http://terms.naer.edu.tw/。

9. 許春金，陳玉書，蔡田木（2015），〈中華民國103年犯罪狀況及其分析——2014犯罪趨勢關鍵報告〉，（法務部司法官學院104年委託研究計畫：法務部），瀏覽日期：2015/11/1，網址：http://www.moj.gov.tw/ct.asp?xItem=392644&ctNode=35595&mp=302
10. 曹明、程永進、張哲、曹銳生、鄭新傑（2015），〈台灣全科醫學模式之我見〉，上網瀏覽時間：2015/10/05，http://gp.cmt.com.cn/detail/30561.html。
11. 移民署（2015），〈公務統計數據〉，上網瀏覽時間：2015/10/01, http://www.immigration.gov.tw/ct.asp?xItem=1291286&ctNode=29699&mp=1.
12. 陳立昇（2015），〈疾病篩檢基本概念〉，上網瀏覽時間：2015/10/05，http://www.hpa.gov.tw/BHPNet/Portal/File/ThemeDocFile/2007082059425/050427%E7%96%BE%E7%97%85%E7%AF%A9%E6%AA%A2%E5%9F%BA%E6%9C%AC%E6%A6%82%E5%BF%B5_2.pdf。
13. 陳彥驊（2015），〈濫用社群網站，人蛇集團效率高〉，台灣醒報網站，上網瀏覽時間：2015/10/01, https://tw.news.yahoo.com/%E7%A4%BE%E7%BE%A4%E7%B6%B2%E7%AB%99%E4%BE%BF%E4%BD%BF-%E4%BA%BA%E8%9B%87%E9%9B%86%E5%9C%98%E6%95%88%E7%8E%87%E6%8F%90%E5%8D%87-091523250.html。
14. 楊秀莉（2015），〈中國內地與澳門網絡犯罪的刑法比較及完善建議〉，《一國兩制研究》第1期，瀏覽日期：2015/10/27網址：http://www.ipm.edu.mo/cntfiles/upload/docs/research/common/1country_2systems/2012_1/p176.pdf。
15. 資策會科技法律研究所（2015），〈加拿大「保護加拿大國民遠離

網路犯罪法」生效，保障國民免受網路霸凌〉，瀏覽日期：2015/11/12，https://stli.iii.org.tw/ContentPage.aspx?i=6845。

16. 維基百科(2015)，〈網路犯罪公約〉，上網瀏覽時間：2015/10/01, https://zh.wikipedia.org/wiki/%E7%B6%B2%E8%B7%AF%E7%8A%AF%E7%BD%AA%E5%85%AC%E7%B4%84。
17. 臺灣地區法規資料庫（2015），上網瀏覽時間：2015/10/01, http://law.moj.gov.tw/Index.aspx。