《從犯罪預防觀點探討兩岸跨境網路犯罪之治理》

A Study on the Governing Policies against the Cross-Border Cybercrime Between Taiwan and Mainland China from the Perspective on the Crime Prevention

柯雨瑞[1]、蔡政杰[2]

目次

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相當多的打擊跨境犯罪案例，例如電信詐欺、毒品販運、組織犯罪及人口販運等案件；然而，隨著資通訊設備普及的運用，跨境網路犯罪逐漸已成了各類跨境犯罪的常見手段，也成了兩岸共同打擊犯罪的新興挑戰，因跨境網路犯罪比一般實體犯罪更難掌握，讓兩岸執法部門面臨非常嚴峻之考驗。2010 年 4 月，在巴西薩爾瓦多舉辦的第十二屆聯合國預防犯罪和刑事司法大會即指出，網路犯罪列該大會議程

1 柯雨瑞（Jui-Rey, Ko），中央警察大學犯罪防治研究所法學博士，曾任內政部警政署保安警察第三總隊第二大隊(基隆)分隊長、第一大隊(台北)警務員，中央警察大學助教、講師、副教授，現為中央警察大學國境警察學系專任教授。

2蔡政杰(Chen-Chien, Tsai)，中央警察大學外事警察研究所(國境組)碩士，現就讀於中國文化大學政治所博士班。曾任內政部警政署保安警察第三總隊隊員、偵查員，臺北縣政府警察局新店分局警員，臺北市政府警察局文山第二分局警員，內政部移民署助理員、科員、專員，現為內政部移民署視察、中央警察大學國境警察學系兼任講師。

中的重要地位，說明了網路犯罪的重要性從未降低，並且帶來了嚴峻挑戰，因為網路犯罪具有以下之特色：犯罪範圍的不確定性、犯罪的跨境性、各國法律差異性及犯罪組織性等等相關之因素，對於各國刑事及司法部門帶來相當大的新挑戰3。

兩岸執法部門(指警察與公安部門)對於跨境網路犯罪的預防，原本就有一定之經驗及相關之治理對策，但是根據 Gordon Earle Moore 所提的「摩爾定律」，我們相信資訊科技發展的速度，將遠超過執法部門所能追趕之程度，故假若執法部門想要有效的防範(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，需有高科技的資訊設備，作為偵查與鑑定之支援；在軟體部分，則要有完善的立法及配套措施，而這正是兩岸執法部門目前所欠缺的區塊。

本文從犯罪預防機制(crime prevention mechanism)的觀點，探討兩岸執法部門對於跨境網路犯罪之治理的現況、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的未來可行之發展方向，並提出以下的具體建議，作為兩岸政府部門與民間社會的參考：

一、加強與提升兩岸民眾對於兩岸跨境網路犯罪預防之意識、觀念與作為；

二、兩岸警察與公安機關宜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；

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；

六、建構舉發兩岸跨境網路犯罪之專線；

七、建構兩岸網路巡邏志工之機制；

八、利用情境犯罪預防理論之觀點，建構兩岸人民監控網路犯罪之機制；

九、未來，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，以達到犯罪預防的效果。亦可參照澳門之立法例，考量訂定專門抗制跨境網絡犯罪之專法之可

3 Twelfth United Nations Congress on Crime Prevention and Criminal Justice, <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>, 21 January 2010, A/CONF.213/9.
< http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/V1050320e.pdf >.

行性。

十、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；

十一、兩岸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；

十二、持續與新興通話軟體之公司，諸如：QQ、SKYPE、WeChat 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。

【關鍵詞】跨境網路犯罪、網路犯罪預防
【Key words】Cross-Border Cybercrime prevention; Cybercrime Prevention.

。。。。。。。。。。。。。。。。。。。。。。。。。回目次>>

壹、前言

隨著資通訊科技的發達，無論是生活在城市或鄉村的現代人，在生活上都已相當依賴資通訊等相關網路設備，也因為資通訊設備改變了人們的生活習慣，犯罪者的犯罪手法也不得不跟著變化，現今的網路犯罪已不像以往傳統的犯罪手法，漸漸取而代之的是透過網際網路上的社群網站4（如 Facebook、Instagram、Twitter、微博…等）及行動通訊裝置上的 APP 通訊網路5（如 LINE、Tango、Mico、Paktor、BeeTalk、WeChat…等）作為犯罪媒介，形成新興的犯罪型態，意即任何一種可接收資通訊訊號的終端設備，都可能被用來當作犯罪的工具，如此一來，佈建全球各地的資通訊網路，儼然已成為犯罪者從事犯罪行為的重要管道。

網路犯罪的特色之一是犯罪區域不受邊界限制，因此，預防兩岸跨境網路犯罪必須是要整合區域資源，進行跨境合作才能有所成效，以 2011 年 11 月 29 日為例，我方警方人員與陸方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

4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>。根據報導，歐洲刑警組織負責人羅伯溫萊特在倫敦演講時說，歐洲從事人口販運的黑幫，隨著科技日益普及，會使用包括 Facebook 在內的社群網路，來協助他們犯罪行為，並提升了不少效率。

5 綜合外電報導，〈上千淫媒，微信串聯拉客。旗下小姐互通，遍及中港澳，逾萬人涉案〉，《蘋果日報》，2015 年 6 月 21 日，版 A17。根據報導，賣淫組織透過微信（WeChat）發布訊息，招攬高社經地位的嫖客，服務範圍遍及香港、澳門、北京、天津、上海、廈門、重慶、太原、哈爾濱、青島、福州、南昌、武漢、杭州、溫州等數十個大城市，涉案人數破萬。

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，成功展現「海峽兩岸共同打擊犯罪及司法互助協議」之成果，並建立起東南亞國家合作共同查緝犯罪的良好關係，這就是跨境網路犯罪治理的典範；尤其兩岸之間同屬中華民族，人文相近、語言互通，犯罪者更可較輕易的建立起犯罪網路，因此，兩岸之間更需要針對跨境網路的問題加以有效的規範。

較為常見且最直接影響人民生活的網路犯罪行為，即為詐欺取財，通常被害人被詐取的財物很難取回，而犯罪者被查獲後之罪刑相對其他犯罪較低，但不論是詐欺取財，或是其他跨境洗錢、色情交易、人口販運、毒品交易及招募組織犯罪等行為，其實都不是新興的犯罪行為，但是若透過資通訊網路作為犯罪的手段，則會產生不同的犯罪手法和過程，加重執法單位在犯罪偵查上的壓力，又因兩岸在立法上並無對於網路犯罪訂定專法，也造成司法機關審理案件的困難度，故執法單位如擬欲運用犯罪預防的手段，防制網路犯罪發生，並不容易。本文將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，再從犯罪預防的觀點深入探討，期望能從犯罪預防的觀點，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。

。。。。。。。。。。。。。。。。。。。。。。。。。。。回目次>>

貳、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涉及犯罪之相關事項等涉及犯罪之過程，部分在臺灣地區，部分在大陸地區，始屬跨境犯罪；亦即跨境犯罪是否成立，是以地區性作為要件，而不以犯罪者之身分作為要件。如同一案件之犯罪過程及結果均在同一地區發生，未有跨地區之情形，雖犯罪者非為本地區人民，在本文定義中，並不屬跨境犯罪[6]。

至於網路犯罪(Cybercrime)一詞的定義，在學界中存在不同的見解，有學者認為網路犯罪只是在新興的網路空間(cyber space)中，利用傳統的手段進行犯罪，其實就是一般白領或組織型的犯罪，未必是全新的犯罪型態或結構[7]；也有學者認為網路犯罪只是日常生活中的通稱，並不是法典中的專用術語，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

6 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，雖犯罪者為臺灣地區人民，而受害者為大陸地區人民，就本文之定義，亦不屬於跨境犯罪之類型。

7 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 91。

式、社交工程、網路釣魚等方式，進行犯罪行為[8]；而歐洲理事會(Council of Eurpoe, COE)於 2001 年 11 月 23 日在布達佩斯簽署之「網路犯罪公約」(Convention on Cybercrime)第一章的定義中，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[9]，然而，就該公約所規範的內容而言，所稱之網路犯罪仍屬於與電腦相關之犯罪行為(Computer-related crime)。

不論是從學者的研究或是從國際公約制定的觀點，對於網路犯罪的通識認知，就是與電腦網路相關之犯罪行為，然而若就字義層面從最廣義的思維來解讀，可將「網路」與「犯罪」分開定義，而單就「網路」一詞，不同的學科領域在學術上就有截然不同的定義和解釋，如電力工程學所稱之網路(transmission and distribution network)，指的可能是輸、配電系統之網路；社會學所稱之「網路」(network)，指的可能是社會交換理論(Social Exchange Theory)所解釋的人際互動行為[10]；通訊工程學所稱之網路(network or NET)，指的可能是通訊系統架構下有線及無線的溝通網路[11]；而資訊工程所稱之網路(network)，指的可能是資訊或終端設備溝通所使用之有線及無線之網路[12]；而將「網路」與「犯罪」結合解釋，指的應就是各學科領域的網路所涉及到實體法之犯罪行為，但是這樣的解釋範圍過於廣泛，也與一般學術界和民眾的認知有所差異。

一般而言，在學術界所探討網路犯罪之「網路」，如以學科(門)分類，應屬資訊工程學所稱之網路，但卻又與社會學及通訊工程學之網路具有部分關連性，因此，網路犯罪則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[13]；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的定義；其實務上與「電腦犯罪」

8 徐振雄，〈網路犯罪與刑法「妨害電腦使用罪章」中的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 40-41。

9 Council of Europe, <Convention on Cybercrime>, 2015/06/05，<http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=11&DF=6/21/2007&CL=ENG>

10 施文玲，〈社會交換理論之評析〉，《網路社會學通訊期刊》，第 52 期，2006 年 1 月 15 日。

11參照「行動通信網路業務基地臺設置使用管理辦法」第 3 條第 3 款規定，行動通信網路：指由行動通信系統及電信機線設備所構成之通信網路。

12 相關網路學術詞彙對照，可參考我方教育研究院「雙語詞彙、學術名詞暨辭書資訊網」，<http://terms.naer.edu.tw/>。

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。

之語詞，也很難分辨14。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15；因此，想要非常明確定義「網路犯罪」一詞之，實屬不易。

在大數據(Big Data)時代的社會，一般社會大眾對於網路的認知，已不再將網路單純視為是電腦的延伸空間，而是數位科技的代名詞，近年來，智慧型手機及社群網路的運用已造成網路犯罪的轉型16，網路犯罪不再只是傳統型的電腦犯罪，網路犯罪已成為高科技資通訊犯罪之一環17。

結合以上各種網路犯罪之定義，本文認為「網路犯罪」不應單指與電腦相關或其延伸性之犯罪行為，亦應包含通訊網路犯罪(Mobile Communications Network)等數位科技犯罪的範疇。而網路犯罪之本身，除了屬實體法定之罪刑之外，尚可以包括：犯罪者常常是透過「網路」(含通訊網路(Mobile Communications Network)作為媒介，進而違反實體法定罪刑之犯罪行為。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，如透過社群網路進行聚眾後，至特定地點鬥毆殺人18亦屬之。

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

14 徐振雄，〈網路犯罪與刑法「妨害電腦使用罪章」中的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。

15 經查詢臺灣地區法規資料庫，<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。

16 邱俊霖，〈近年科技犯罪趨勢與犯制對策〉，《刑事雙月刊》，第 65 期，2015 年 4 月，頁 7-11。

17 王勁力，〈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，2010 年 6 月，頁 7-10。作者將高科技資通訊犯罪類型分為：(一) 資訊犯罪。(二) 電腦犯罪。(三) 網路犯罪。

18 2014 年 9 月 14 日台北市政府警察局信義分局薛姓偵查佐，於台北市信義區松壽路 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。<https://zh.wikipedia.org/zh-tw/2014%E5%B9%B4%E8%87%BA%E5%8C%97%E5%A4%9C%E5%BA%97%E6%AE%BA%E8%AD%A6%E6%A1%88>

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19屬之。

「網路犯罪」定義之第三個面向，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。

涉及網路犯罪之定義之第 4 個面向，亦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，最有名的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「危害計算機系統網路（絡）和數據的保密性、完整性和可利用性，以及濫用這些系統、網路（絡）和數據之行為。」20。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路（含網際網路系統）及其數據之保密性、完整性與可利用性，以及濫用這些系統、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路（含網際網路系統）及其數據之保密性、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網路系統（包含網際網路系統）、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 2 個面向之網路犯行，可稱為兩岸跨境之「實境犯罪」（real crime）。

。。。。。。。。。。。。。。。。。。。。。。。。。回目次>>

參、兩岸跨境網路犯罪之現況與危害性

根據上述網路犯罪之定義，略可將網路犯罪區分為兩種類型，一種為網路虛擬犯罪(virtual crime)，另一種為網路實境犯罪(real crime)。所謂網路虛擬犯罪，係指駭客(hacker)

19 2014 年 5 月 21 日鄭姓犯嫌在台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為，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。<http://news.tvbs.com.tw/old-news.html?nid=532949>

20楊秀莉，<中國內地與澳門網絡犯罪的刑法比較及完善建議>，2013 年，http://www.ipm.edu.mo/cntfiles/upload/docs/common/1country_2systems/2012_1/p176.pdf。

或病毒(Virus)入侵[21]，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。以現行兩岸刑法所訂之電腦犯罪相關條文，如陸方刑法第 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【利用電腦實施犯罪的提示性規定】，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之範疇。而兩岸對於網路實境犯罪之處罰，仍回歸到犯罪行為本質所違反之罪刑予以處罰[22]。

以兩岸跨境網路犯罪之現況而言，常常發生之現象，第一類部分，係為虛擬犯罪之類型，虛擬犯罪通常具有特殊之目的，如侵入特定目標竊取資料、破壞電腦系統或植入惡意程式等，而其特定目標大部分為中、大型企業、政府機關及重要人士，一般小公司、家庭及民眾鮮少會成為網路虛擬犯罪之對象，因此發生之地點，集中於中、大型企業、政府機關(含軍事及情報機關)及重要人士。第一類部分，係為因兩岸民間交流情形熱絡，遂造成網路實境犯罪之盛行，如：詐欺犯罪與網路賭博犯罪等。

兩岸跨境網路犯罪可能造成之危害如下：

一、造成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，大部分均屬於集團性犯罪，較少有個體犯罪之情形，在兩岸犯罪集團為謀求更大之不法利益之前提下，通常都會跨組織合作，如此將使犯罪組織網更為綿密且複雜，且造成犯罪擴溢現象，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，會增加犯罪的區域性，也會對兩岸社會造成更大的不安定性，並增加執法機關的查緝成本。

二、造成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[23]，在證據蒐集及加害人追查上即

21 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。

22 如陸方刑法第 287 條【利用電腦實施犯罪的提示性規定】：利用電腦實施金融詐騙、盜竊、貪污、挪用公款、竊取國家秘密或者其他犯罪的，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，對公眾散布而犯詐欺罪者，有較重之刑罰規定。

23 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 7 月，頁 15。

屬不易，若再屬跨境犯罪之性質，基於兩岸法律規定不一及管轄權等問題，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，單 2014 年一年內入境臺灣地區之大陸地區人民即高達將近 400 萬人[24]，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，造成雙方人民之間的彼此不信任，甚至產生排斥感，影響兩岸交流之契機。

。。。。。。。。。。。。。。。。。。。。。。。。。。。。回目次>>

肆、兩岸跨境網路犯罪的治理困境

在兩岸執法人員治理兩岸跨境之網路犯罪部分，所遭遇的困境，作者檢視與綜整相關之文獻，並與相關之學者、警察與主任檢察官相互討論之結果，彙整如下之困境：

一、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，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」。此一電信詐欺之組織犯罪集團之犯罪手法，具有以下之特點[25]：

(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，

24 數據來源：我方移民署網站公務統計數據，2015 年，<http://www.immigration.gov.tw/ct.asp?xItem=1291286&ctNode=29699&mp=1>.

25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>，《新北市政府警察局新莊分局》，2015 年 5 月 19 日，http://www.xinzhuang.police.ntpc.gov.tw/cp-492-11757-18.html。

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戶，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」，匯款至指定帳戶。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「指定帳戶」，事實上，本款項已流入上述電信詐欺犯罪集團之帳戶之中，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。

就本案而言，陸方之被害人，具有以下之特點：

(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戶涉嫌洗錢乙事，陸方被害人未立即掛斷電話，轉而向其所屬之銀行求證，究竟其銀行之帳戶，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，其銀行帳戶內之資金，遂

被詐騙至犯罪組織之帳戶之中。

(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、兩岸與第 3 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

於 2013 年 12 月 13 日，兩岸執法人員共同攜手合作，偵破我方最大宗的網路賭博「金船娛樂城案」；「金船娛樂城」是簽賭網站之站名；其犯罪之手法與方式，詳如下述[26]：

(一)它是屬於涉及兩岸與第三地之網路賭博犯罪案件，在此「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[27]；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」的主嫌，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 9 大隊第 1 組之偵查人員，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；「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，

26刑事警察局偵查第 9 大隊，<國內首宗兩岸合作偵破最大網站賭博第 3 方支付中心>，《刑事警察局》，2013 年 12 月 24 日，http://www.cib.gov.tw/news/Detail/29436。

27點數兌換成現金之行為，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。

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[28]）。

（五）「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。

（六）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；

執法機關在預防本案之網路賭博犯罪時，遭遇以下之困境：

（一）該網站之主機，架設在加拿大，而非在兩岸；兩岸執法人員即使啟動「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，掩護非法的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、兩岸跨境犯罪組織利用新興網路通話軟體進行犯罪計畫之溝通，查緝與監聽不易

以兩岸跨境毒品犯罪為例，根據劉邦乾氏之研究[29]，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

---

28 我為之<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為：
一、提供現金、有價證券或其他通貨為獎品。
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為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。

29劉邦乾，《海路毒品販運組織及其犯罪手法之研究》，（台北：國立台北大學犯罪學研究所碩士論文，2013 年），第 5~130 頁。

之過程之中，具有以下之特色[30]：

(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。

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；

(二)我方之民眾與學生，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；

(七)假若兩岸跨境之毒品犯罪組織之犯嫌，其使用 QQ、SKYPE、WeChat 與 LINE 相互連繫，在此情形之下，如兩岸執法人員於其 QQ、SKYPE、WeChat 或 LINE 之發話方，或接收方之電腦或手機之中，輸入監聽與搜索之電腦特殊軟體，以利監聽案情發展，此種之特種偵查作為，是否合憲？有無侵犯人權(通訊自由權與隱私權)？頗具爭議性。

。。。。。。。。。。。。。。。。。。。。。。。。。。。回目次>>

伍、從犯罪預防觀點研析兩岸跨境網路犯罪防治的未來可行對策

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

在本文所提及之「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

30劉邦乾，《海路毒品販運組織及其犯罪手法之研究》，(台北：國立台北大學犯罪學研究所碩士論文，2013 年)，第 5~130 頁。

之犯防意識，尚待強化與提升。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，諸如：宜具備「事後查證」之犯防意識，並付諸實際之行動，利用「事後查證」之作法，破解電信詐欺之犯行。就我方而言，可向民眾宣導警政署 165 反詐騙諮詢專線查詢，可資利用。就陸方而言，本文建議陸方建制一套類似於我方警政署 165 反詐騙之諮詢專線查詢，以供陸方民眾利用。

另外，在本文所提及之「金船娛樂城簽賭網站」案例之中，我方執法機關宜大力宣導網路簽賭之違法性、犯行模式、手法與法律效果等，諸如：正確告知民眾，如遊戲網站提供將遊戲點數變現之作法(行為)，此種之遊戲網站，係屬於違法，且已構成觸犯我方刑法之賭博罪，勸導民眾勿將遊戲點數變現。

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[31]。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，並且免於觸犯我方之賭博罪行。為何民眾能免於觸犯我方之賭博罪行，因其具備犯防意識。而此處之犯防意識，則係來自於我方執法機關大力宣導網路簽賭之違法性、犯行模式、手法與法律效果等之成果之展現。同樣之模式，陸方之執法機關，亦可仿效之。

二、兩岸警察與公安機關宜共同簽訂「犯罪預防」(包括網路犯罪預防）之協議或備忘錄

在目前階段，海峽兩岸業已簽署「海峽兩岸共同打擊犯罪及司法互助協議」，並將其落實於實務之工作上。上述之協議，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

31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」，其無法包括網路上的虛擬世界。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。

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，始正式啟動此一協議之機制。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。

由於上述之協議，在治理兩岸之跨境網路犯罪與其他各類型之跨境犯罪議題時，欠缺主動性，與缺乏「犯罪預防」(crime prevention)之機制，很明顯地，本協議在事前預防兩岸跨境網路犯罪與其他各類型之跨境犯罪，有嚴重不足之處。

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，共同簽署海峽兩岸共同預防犯罪協議，或者，備忘錄。待時機更成熟之後，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。

為何兩岸警察與公安機關須先簽署犯罪預防（其中，包括兩岸跨境網路犯罪之預防）之協議或備忘錄？因協議或備忘錄具有法律層面之效果，較可建立一個可長與可久之犯罪預防機制；亦即，藉由法治，避免淪為人治。同時，可避免兩岸警察或公安之領導人因易人時，而導致兩岸執法機關共同預防兩岸跨境犯罪機制之停擺或中止。

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。

再者；在實務之操作面上，本文建議，兩岸之警察與公安機關，宜具有高膽遠矚之眼光，與具創新性之作法，亦即，兩岸警察與公安機關宜共同制定預防兩岸跨境犯罪（包括兩岸跨境網路犯罪）之各式短、中、長期犯防計畫。短期性之犯防計畫，包括為期 1 年時程之犯防計畫；中期型之犯防計畫，其時程或可含蓋數個年度，如 3 年至 7 年；長期型之犯防計畫，其時程或可含蓋近約 10 年以上。上述之犯防計畫，其犯防之對象方面，可針對於某一個類型之犯罪，諸如：兩岸跨境網路犯罪、毒品犯罪、殺人犯罪、詐欺犯罪、人口販運犯罪、洗錢犯罪、經濟犯罪…等等。

再者，上述之犯防計畫，亦可針對於全般性之各類型兩岸跨境犯罪（包括兩岸跨境網路犯罪），制定全般性之兩岸跨境犯罪（包括兩岸跨境網路犯罪）之預防計畫。在上述之犯防計畫之中，明定透由何種之機制、作法與策略？始可達到兩岸警察與公安共同預防犯罪之目標。

四、兩岸警察與公安機關對於兩岸跨境網路犯罪之犯防機制之其他可行作法

兩岸警察與公安機關對於兩岸跨境網路犯罪之犯防機制，尚可以採行以下之對策：

(一)加大兩岸警察與公安機關對於違法網站之監控力道；

(二)提升兩岸網路巡邏密度；

(三)建構舉發兩岸跨境網路犯罪之專線；

(四)建構兩岸網路巡邏志工之機制；

(五)利用情境犯罪預防理論之觀點，建構兩岸人民監控網路犯罪之機制；

(六)未來，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，以達到犯罪預防的效果[32]。亦可參照澳門之立法例，考量訂定專門抗制跨境網絡犯罪之專法之可行性。

(七)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；

32 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。

(八)兩岸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；

(九)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。

。。。。。。。。。。。。。。。。。。。。。。。。。。。。回目次>>

陸、結論與建議

就兩岸跨境網路犯罪之定義與範疇方面，犯嫌之犯罪型態，除了危害他方之計算機系統網路（含網際網路系統），及其數據之保密性、完整性與可利用性之外，應另包括：濫用己方或他方之計算機系統網路(含網際網路系統)、網際網路功能與其數據之行為。在此種之脈絡下，兩岸跨境通訊網路犯罪(Mobile Communications Network)等數位科技犯罪的範疇，亦應屬網路犯罪之一環。是以，如行為人透由手機與平板電腦等工具，濫用網際網路之系統，進行兩岸跨境之各式犯罪計畫，均屬於涉及網路犯罪之相關範疇之內。

兩岸警察與公安在預防兩岸跨境網路犯罪之議題上，面臨以下之困境：

一、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，仍普遍地未具有防範之意識與作法；

二、涉及兩岸與第 3 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，而不知業已違法；

三、兩岸跨境犯罪組織利用新興網路軟體，如：QQ、LINE、WeChat 與 SKYPE 等，進行犯罪計畫之聯繫，查緝與監聽不力，造成犯罪擴溢效應。

在兩岸警察與公安機關對於兩岸跨境網路犯罪之犯防對策方面，如下所述：

一、加強與提升兩岸民眾兩岸跨境網路犯罪預防之意識、觀念與作為；

二、兩岸警察與公安機關宜共同簽署防治兩岸跨境犯罪之犯罪預防（包括網路犯之預防）之協議或備忘錄；

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；

六、建構舉發兩岸跨境網路犯罪之專線；

七、建構兩岸網路巡邏志工之機制；

八、利用情境犯罪預防理論之觀點，建構兩岸人民監控網路犯罪之機制；

九、未來，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，以達到犯罪預防的效果。亦可參照澳門之立法例，考量訂定專門抗制跨境網絡犯罪之專法之可行性。

十、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；

十一、兩岸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；

十二、我方警察宜持續與新興通話軟體之公司，諸如：QQ、SKYPE、WeChat 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。

。。。。。。。。。。。。。。。。。。。。。。。。。。。回目次>>

參考文獻

一、中文資料

◎Marc Goodman(2016)，林俊宏譯，未來的犯罪，新北：木馬文化。
◎William Brittain-Catlin 著、李芳齡譯(2007)，境外共和國：揭開境外金融的秘密，天下雜誌出版。
◎內政部警政署(2010)，警察偵查犯罪手冊，台北：內政部警政署。
◎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。
◎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。
◎王乾榮(2004)，犯罪偵查，臺灣警察專科學校，第 369-372 頁。
◎王翔正(2011)，「網路即時通訊詐欺犯罪偵查」，刑事雙月刊 45 期，42-45 頁。
◎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。
◎汪毓瑋(2015)，「國土安全理論與實踐之發展」，國土安全與國境管理學報，第 23 期，頁 1-47。
◎何芸欣(2005)「網路詐欺之研究」，國立臺北大學碩士論文。
◎余德正（2000）不法使用網際網路之刑事責任。東海大學法律學系研究所碩士論文。
◎孟維德(2005)，「海峽兩岸跨境犯罪之實證研究－以人口走私活動為例」，刑事政策與犯罪研究論文集（13），頁 137-184。
◎孟維德、黃翠紋(2012)，警察與犯罪預防，台北：五南。
◎林山田、林東茂（1997）。犯罪學。臺北：三民。
◎林文龍（2003）線上遊戲犯罪偵查模式之研究。佛光人文社會學院資訊學研究所碩士論文。
◎林宜隆（2009）。網路犯罪：理論與實務，網際網路與犯罪問題，修訂第三版，桃園：中央警察大學。

◎林宜隆、邱士娟(2003)，我國網路犯罪案例現況分析，中央警察大學『資訊、科技與社會』學報。
◎林宜隆、張志炁（2008)。台灣地區網路犯罪現況分析-以刑事警察局破獲之案例為例，知識社群與系統發展學術研討會，臺北：文化大學。
◎林宜隆、黃讚松（2002)，建構網路犯罪預防整體概念，中央警察大學『資訊、科技與社會』學報。
◎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。
◎施能新(2005)，「電子郵件犯罪偵查機制之研究」，中央警察大學資訊管理研究所碩士論文，16-30 頁。
◎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。
◎徐振雄(2010)，網路犯罪與刑法「妨害電腦使用罪章」中的法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。
◎徐源隆（2003)「網路拍賣詐欺犯罪之偵查對策」，第七屆資訊管理學術計警政資訊實務研討會。
◎高信雄(2012)，跨境網路犯罪研究:基於犯罪偵防策略模型，中央警察大學資訊管理研究所碩士論文。
◎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。
◎莊忠進（1996)。電腦犯罪偵查與立法之研究，臺北：警專。
◎許春金（2007)。犯罪學，修訂第五版。臺北：三民。
◎許春金，陳玉書(2013)。犯罪預防與犯罪分析，二版，台北：三民。
◎許慈健(2005)，「網路犯罪偵查與我國關於網路服務提供者協助偵查法制之研究」，93-134 頁。
◎許福生(2016)，犯罪學與犯罪預防，台北：元照。
◎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。
◎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。
◎陳嘉玫(2011)， 網路安全的社交工程，科學發展 461 期。
◎黃明凱（2002)，網路犯罪輔助偵查專家系統雛型之建構，中央警察大學資訊管理研究所碩士論文。
◎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。
◎黃登銘(2013)，網路犯罪模式分析與偵查機制之研究－以網路詐欺為例，國立宜蘭大學多媒體網路通訊數位學習碩士在職專班碩士論文。
◎楊永年、楊士隆、邱柏嘉、李宗憲(2009)，網路犯罪防治體系之政府職能與角色分析，行政院研究發展考核委員會委託國立臺灣大學研究報告。
◎葉雲宏（2008)，網路詐欺犯罪被害影響因素之研究，中央警察大學犯罪防治研究所碩士論文。
◎廖有祿、李相臣（2003)。電腦犯罪-理論與實務，初版一刷。臺北：五南。
◎廖福村(2007)，犯罪預防，台北：警專。
◎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。
◎蔡美智（1998)。電腦駭客入侵的法律問題，資訊與電腦雜誌。
◎蔡德輝(2009)，犯罪學，台北：五南。

◎鄧煌發(1997)，犯罪預防，桃園：中央警察大學。
◎鄧煌發、李修安(2012)，犯罪預防，台北：一品。
◎鄭厚堃(1993)，犯罪偵查學，中央警察大學出版社，第 1-32 頁。
◎震宇(1997)，論網路商業化所面臨的管轄權問題（上），資訊法務透析第 9 期，第 18-34 頁
◎蕭季慧編(1993)，犯罪偵查與蒐集證據，中央警官學校出版社，第 30-38 頁。
◎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。
◎顏旺盛、陳松春(2011)，「迎接 21 世紀跨境犯罪之挑戰」，刑事雙月刊 39 期，第 57-60 頁。

。。。。。。。。。。。。。。。。。。。。。。。。。。。回目次>>

二、英文資料

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

三、日文資料

◎日本広島県警察本部生活安全部生活安全企画課，防犯パトロールの手引き～安全て安心できるまちづくりのために～。
◎日本吉見町安全・安心まちづくり推進会議(2013)，吉見町防犯のまちづくり基本計画（平成２５～２９年度）。
◎日本京都市文化市民局市民生活部くらし安全推進課(2014)，世界一安心安全・おもてなしのまち京都---市民ぐるみ推進運動，第２回推進本部会議資料。
◎日本東京都町田市市民部防災安全課(2013)，町田市安全安心まちづくり推進計画。
◎日本青森縣警察本部生活安全企画課街頭犯罪等抑止対策係(2013)，青森県犯罪のない安全・安心まちづくり推進計画，第３次，平成 25 年度～平成 27 年度。
◎日本春日部市(2014)，春日部市防犯のまちづくり推進計画，平成 26 年度～平成 30 年度。

。。。。。。。。。。。。。。。。。。。。。。。。。。。回目次>>

四、網路資料

◎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.

◎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 .
◎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。
◎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。
◎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。
◎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。
◎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

◎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/。
◎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
◎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。
◎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.
◎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。
◎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。
◎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。
◎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。
◎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。
◎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。

。。。。。。。。。。。。。。。。。。。。。。。。。。。。回首頁>>