出國報告(出國類別：考察)

第十一屆海峽兩岸暨港澳刑事法論壇與會心得

服務機關：(1)臺灣高等檢察署

(2)臺灣苗栗地方檢察署

(3)臺灣臺北地方檢察署

姓名職稱：(1)許永欽檢察官

(2)黃振倫檢察官

(3)蕭奕弘檢察官

奉派地點：澳門

出國期間：107 年 11 月 4 日至 6 日

報告日期：108 年 1 月 24 日

摘要

第十一屆海峽兩岸暨港澳刑事法論壇由澳門刑事法研究會主辦，北京師範大學刑事法律科學研究院、臺灣輔仁大學法律學院及香港大學法律學院協辦，於107年11月4日至6日在澳門舉行。

此次論壇研討主題係「網絡犯罪的刑事法規制」，探討網路犯罪之實體及程序規範。會議發表近30篇論文，區分五大主題，分別是：網絡犯罪宏觀刑事策略研究、電信詐騙與侵犯個人隱私犯罪刑事策略研究、網路金融詐騙犯罪刑事策略研究、其他網絡犯罪刑事策略研究，以及網絡犯罪刑事策略研究，提交之論文，內容深入，報告者言之有物，頗值借鏡。

目錄

壹、前言及目的

由澳門刑事法研究會主辦，北京師範大學刑事法律科學研究院、臺灣輔仁大學法律學院及香港大學法律學院協辦之第十一屆海峽兩岸暨港澳刑事法論壇，於2018年11月4日至6日在澳門舉行，此次論壇研討主題係「網絡犯罪的刑事法規制」，探討網路犯罪之實體及程序規範。

法務部亦獲主辦單位邀請，派員參加此次論壇盛會，法務部遂指派負責經濟犯罪督導業務之臺灣高等檢察署許永欽檢察官、偵查跨境詐欺案件素有經驗之臺灣苗栗地方檢察署黃振倫檢察官，以及偵查電腦犯罪學有專精之臺灣臺北地方檢察署蕭奕弘檢察官代表與會，藉由與會汲取新知與分享經驗。

貳、會議過程

兩岸暨港澳刑事法論壇舉辦地點位於澳門HOTEL ROYAL(皇都酒店)，2018年11月4晚報到，2018年11月5日上午開始至6日中午結束， 論壇主題為「網絡犯罪的刑事法規制」，但細分五個場次，五個子題研討，分別為「網絡犯罪宏觀刑事策略研究」、「電信詐騙與侵犯個人隱私犯罪刑事策略研究」、「網絡金融詐騙犯罪刑事策略研究」、「其他網絡犯罪刑事策略研究」、「網絡犯罪刑事策略研究」，各由兩岸四地之學者與專家發表論文並與談。

研討範圍甚廣與甚深，從網路犯罪之宏觀刑事規制策略到微觀之個案偵審；從網路犯罪之實體規範到程序之偵審；以及從網路犯罪之政府管制到產業之協助

防制。論壇舉辦方式原則上均由與會者提交論文者上臺報告，但囿於提交論文者多，故無法全部上臺報告，未報告者則收錄其論文供與會者參考。原本未在主辦單位規劃報告及提交論文行列之法務部代表團，亦在場爭取到一個上臺報告之機會，遂由黃振倫上臺報告偵辦跨國詐欺犯罪之經驗，而蕭奕弘檢察官則在Q & A過程中多次發言，分享檢察官偵辦許多著名之重大電腦犯罪與詐欺犯罪案件之經驗，兩位檢察官之報告與發言內容，均得到與會者甚高之評價。

參、研討摘要及心得

本次與會者提交之論文，內容深入，報告者言之有物，頗值借鏡，爰將各與會者之論文與發言精要，茲整理敘述如下：

一、網絡犯罪宏觀刑事策略研究

(一)略論澳門刑法中的危害網路安全罪

報告人澳門刑事法研究會名譽會長趙國強教授指出網路危安罪的概念，以及澳門刑法中關於危害網路安全的立法。

網路犯罪可分為狹義跟廣義，趙教授指出只有狹義的網路犯罪，將網路資訊系統本身的運作或其內部所包含的各種資訊直接成為犯罪行為所指向的對象，才真正屬於危害網路安全的網路犯罪。

其次，在歐洲委員會於 2001 年簽訂打擊網路犯罪公約後，澳門參考該公約，於 2009 年制定打擊電腦犯罪法，就危害網路安全的犯罪制定專項立法。在此之前，澳門僅在刑法典分則第 213 條規定了資訊詐騙罪，此外並無相關立法。

趙教授認為，打擊電腦犯罪法迄今已經近十年，有修訂必要。具體的修訂可以從立法方式跟內容加以修訂。在立法方式部分，建議納入澳門目前正在進行諮詢的網路安全法中規定，為電腦和網路安全本質上並無差別，而網路安全法中如果只規定網路管理，並未納入危害網路安全行為，有失偏頗。就立法內容部分，犯罪類型可以區分成為四種類型，包括侵入性、獲取性、控制性與攻擊性危害網路安全罪。

趙教授強調，單純利用網路系統來實施犯罪，如金融詐騙；將網路作為平台來實施犯罪，比如成立詐騙網站；或僅和網路有關，但與危害網路安全無關的犯罪，如電腦詐騙罪，都不適宜和危害網路安全的犯罪一同規定。

(二)網路安全之保護與刑事政策檢討

報告人輔仁大學法律學系靳宗立教授先就電腦犯罪與網路犯罪的立法狀況彙整，檢討近二十年來法制發發展的現況，針對爭議問題分析檢討，最後對網路安全刑事規制方向提出心得。

文中將電腦與網路犯罪分成三種層次，狹義是指抽象犯罪類型保護的保護法義是使用電腦(網路)利益；廣義則是指抽象犯罪構成要件以電腦(網路)為要素；

至於最廣義則是只具體犯罪行為之手段或過程涉及電腦(網路)者。

這二十年來，刑法的立法大致可以分成兩階段，從 1997 年到 2002 年，主要增訂廣義電腦(網路)犯罪；從 2003 年迄今，則增訂狹義電腦(網路)犯罪，並檢討增刪廣義電腦(網路)犯罪。靳教授釐清保護法益，認為刑法第 358 條入侵電腦罪、第 359 條侵害電磁紀錄罪及第 360、361 條干擾電腦罪，性質上都是屬於侵害個人法益罪；至於第 362 條的製作惡意電腦程式罪，性質上跟製造毒品相仿，性質在保護社會成員使用電腦的利益。

靳教授指出現行刑事規制，主要仍以規範電腦犯罪為中心，狹義網路犯罪尚有待努力建構中。而且，網路既然是連結眾多個別使用電腦的架構平台，保護法益應該屬於社會法益，而非個人法益。如何維護眾多使用者的權益，應該是各國政府積極努力的使命。只是因為網路世界的跨域性，國際關係的複雜，還需要各界共同努力。

(三)網路刑法的價值轉向與預防刑法

報告人武漢大學法學院教授何榮恭探討中國大陸制定的刑法修正案(九)增設第 286 條之 1 拒不履行資訊網路安全管理義務罪、第 287 條之 1 非法利用資訊網路罪及第 287 條之 2 幫助資訊網路犯罪活動罪。以下先簡要介紹這三個新規定，這三種刑事責任都有併罰法人罰金的規定。

拒不履行資訊網路安全管理義務罪課予網路服務提供者履行法律及行政法

規制定的資訊網路安全管理義務，如果經監管部門令其採取改正措施而拒不改正，導致違法資訊大量傳播、致使用戶資訊大量洩漏而造成嚴重後果、致使刑事證據滅失而情節嚴重，或有其他嚴重情節時，網路服務提供者有刑事責任。

非法利用資訊網路罪則是處罰利用資訊網路實施詐騙、銷售違禁物或為實施詐騙等違法犯罪活動發布資訊。

幫助資訊網路犯罪活動罪則是處罰提供網路網路、伺服器託管、網路存儲、通訊等技術，或提供廣告推廣、支付結算等幫助，在情節嚴重的情況下，以刑事責任處罰。

這三類的刑事制裁，都是屬於預防性的刑法，基於網路犯罪的特殊屬性而設。何教授認為傳統刑法體系中，預防犯罪非懲罰的直接目的，而是伴隨效果。目前中國大陸預防刑法條款主要集中在恐怖主義犯罪與網路刑法領域，面對網路犯罪，則擴張不作為犯的處罰範圍，賦予網路服務提供者的刑事責任，呈現更多社會管理法的性質與特徵，雖然具有不得已性，但這帶來傳統刑法屬性的改變，以及如何科學界定公民刑事責任範圍，將是不可忽視的課題。

(四)從算法與量刑看大數據的侷限：基於美國威斯康辛州訴埃里克盧米斯案的分析

報告人傅華伶教授是香港中文大學法學院副院長，在論文中指出美國法院用

來評估被告風險的軟體 COMPAS，是否會因此侵害被告的正當法律程序。2013 年 2 月，美國威斯康辛警方以涉嫌駕車槍擊罪逮補埃里克盧米斯(Eric Loomis)，在經起訴五項罪名後，法院判處被告有期徒刑 6 年。法院量刑時，考量被告所犯罪行的嚴重程度、過往素行、假釋的紀錄，以及顯示被告有沒有再犯風險的風險積分。這份積分來自一套商用軟體 COMPAS，紀錄在威斯康辛州矯正局向法院提出的量刑前調查報告中。

被告盧米斯認為法院量刑所參考的 COMPAS 風險評估結果，侵害正當法律程序，包括該軟體無從檢視準確性、只能預測群體而非個人的危險性，以及不恰當的使用以性別為導向的評估方式，構成性別歧視。在案件來到威斯康辛州最高法院後，該州最高法院於 2016 年 7 月 13 日維持下級審的決定，認為法院在量刑時，COMPAS 並非決定性的因素，即便矯正局的量刑前調查報告中並未提出該風險評估報告，法院仍然會做出相同的結論，量刑並未錯誤，也沒有侵害正當法律程序。當盧米斯上訴到最高法院後，最高法院於 2017 年 6 月駁回上訴而未加以受理。

傅教授指出大數據像是一面鏡子，僅僅反映社會的真相，數據中的歧視跟偏見自然會顯示在大數據中，演算法所得到的結論也只是反映了社會的歧視與偏見，更危險的是演算法使偏見更加根生蒂固，這些都是我們需要時時加以警惕的。

(五)現實挑戰與未來展望：關於人工智慧的刑法學思考

報告人趙秉志是北京師範大學刑事法律科學研究院教授，詹奇瑋則是趙教授

的博士研究生，論文由二人合著，研討會中則由詹先生口頭發表。論文從專用與通用人工智慧出發，分別探討兩者在刑法學上的思考，以下聚焦在專用人工智慧的討論。

人工智慧的分類大概可以區分成為專用、通用與超級人工智慧。專用人工智慧又稱為弱人工智慧，指的是通過感知以及記憶體來實現特定領域或功能，專用人工智慧目前正處於高速發展的階段，而且也已經取得相當的成果；通用人工智慧又稱為強人工智慧，是基於認知學習與決策執行能力，可以實現多領域的綜合智能，這是未來的發展方向；至於超人工智慧則是指將來人工智慧可能會在各方面超越人類智慧的能力。

就專用人工智慧部分，論文認為由於專用人工智慧沒有形成類似人類的自主意識，將智能機器人納入刑法規範行為主體範圍，並沒有必要性。但專用人工智慧仍然面對內部與外部風險，所謂內部風險是指對數據大量搜集與深度處理，以及演算法的漏洞與偏差；至於外部風險則包括濫用人工智慧的風險，以及前面提到內部風險轉化為現實危害的外部風險，比如：無人車存在技術漏洞，而導致安全的威脅。

就應對方面，論文提出三個面向：第一，刑法應該堅持罪刑法定與謙抑性的本質。第二，提升對公民個人資料安全的保護。第三，刑法應該針對人工智慧進行全方面調控，積極迎接人工智慧時代的全面到來。

(六)中國網路犯罪立法的合理性及其展開

報告人趙秉志跟袁彬都是北京師範大學刑事法律科學研究院教授，這篇論文探討中國大陸制定的刑法修正案(九)的一些問題。刑法修正案(九)是中國大陸近年來對網路或電腦相關犯罪最大幅度的修法。新增了四種新的網路犯罪罪名，對6種與網路相關的犯罪罪名進行修正，增加網路犯罪的懲治力道，可以說是歷次以來修法幅度最大的一次。

新的四種罪名包括：第286條之1拒不履行資訊網路安全管理義務罪、第287條之1非法利用資訊網路罪及第287條之2幫助資訊網路犯罪活動罪，以及第291條之1增加1款的散播虛假資訊罪，論文的兩位作者認為刑法修正案(九)關於網路犯罪的最新立法具備合理性依據。不過，在網路服務商提供刑事責任、虛假資訊犯罪立法範圍，以及侵犯公民個人資訊罪立法模式等問題，存在諸多立法內容與技術上的問題，還有待進一步改善。

以下簡要介紹刑法修正案(九)的上述三個方面。

首先，在網路服務商提供刑事責任部分，新規定增加了兩種犯罪，包括網路服務商拒不履行法定義務，以及提供幫助行為。

其次，在虛假資訊犯罪部分，將編造虛假的險情、疫情、災情、警情，在資訊網路或其他媒體上傳播，或明知屬於上述虛假資訊，故意在資訊網路或其他媒體上傳播，而嚴重擾亂社會秩序納入刑事規範。

最後，在侵犯公民個人資料罪部分，中國大陸並沒有個人資料保護的專門立

法，就個人資料保護的相關規定散布在諸多法規中，這次的修正和我們 2010 年個人資料保護法修正進程相似，將規範主體從特定延伸到一般，不再只是針對某些特殊單位進行管制。

(七)我國網路犯罪立法的基本回顧與完善展望

報告人王燕玲是華東師範大學法學院副教授，這篇論文對中國大陸網路犯罪進行回顧與展望。

首先，中國大陸在 1997 年之前的刑法中並沒有電腦犯罪的規定，以時間軸來看，中國大陸在 1994 年才加入網際網路。直到 1997 年刑法第 6 章妨害社會管理秩序罪的第 1 節擾亂公共秩序罪中，規定第 285 條、第 286 條及第 287 條之 1 後，才正式確立最初步的電腦犯罪罪名體系。

其次，隨著時代演進，從電腦犯罪到網路犯罪的歷史發展必然過程。在網路 2.0 時代的衝擊下，原本立法觀念的落後及侷限，讓司法機關無法對新情況進行有效的規範。刑法修正案(七)修改第 285 條，增加 2、3 款，包括非法獲取電腦資訊系統數據罪、非法控制電腦資訊系統罪及提供侵入、非法控制電腦資訊系統程式、工具罪，較為有效的解決一些實務上的問題。

最後，隨著大數據、人工智慧等新世代技術相繼出現後，刑法修正案(七)仍然不足以因應新時代，為了維護資訊網路安全及完善懲處網路犯罪法律規定，刑法修正案(九)進一步充實網路犯罪體系罪名。

對於未來的展望，王教授認為應該針對四個面向，包括網路財產類犯罪、網路平台類犯罪、網路瀆職類犯罪及人工智慧類犯罪，進一步探討。

二、電信詐騙與侵犯個人隱私犯罪刑事策略研究

(一)論中國大陸電信網路詐騙的司法應對

報告人北京師範大學刑事法律科學研究院名譽院長高銘暄教授首先就互聯網時代，使電信詐欺犯罪層出不窮之情形下，特別是「徐玉玉[1]」案件之指標性案件，使大陸就立法與司法層面，將電信詐欺犯罪列為首要打擊目標，並就立法及司法層面，採取高壓之打擊方式，進而制訂許多關於網路犯罪有關之刑事法律做基本介紹。除介紹一般詐騙罪外，其中，較值得注意的是大陸刑法於 2015 年修正，並就干擾無線電通訊秩序，訂定「擾亂無線電通訊管理秩序罪」，就干擾網路通訊之行為(如虛假發送使用假網址)予以處罰；另針對電信網路犯罪增訂「拒不履行資訊網路安全管理義務罪」、「非法利用資訊網路罪與幫助資訊網路犯罪活動罪」，針對網路業者予以監督並要求提供資訊，要求業者控管以降低電信犯罪之發生，值得借鏡[2]。

---

[1] 2016 年 8 月 21 日,剛接到大學錄取通知書的山東臨沂市高三畢業生徐玉玉接到詐騙電話,被告人陳文輝 等人以發放助學金的名義,騙走徐玉玉全部學費 9900 元,徐玉玉在報警回家的路上猝死, 2017 年 6 月 27 日,山東省臨沂市中級人民法院一審公開開庭審理陳文輝等詐騙、侵犯公民個人資訊一案, 7 名被告人均被判處有罪。

[2] 此一問題，涉及到業者商業利益、消費者隱私保障及國家安全等考量權衡，在研討會中，部分中國大陸學者亦有持懷疑意見，認為就各類網路行為均科予業者

(二)兩岸跨境電信詐欺犯罪防制策略之探討

報告人警政署國道高速公路警察局秘書洪俊義先生就詐欺集團之演進發展做介紹，並就「兩岸共打機制」、「詐欺集團犯罪解析」等相關案例做簡單說明。另特別就「兩岸判例輕重存有差異」、「被害人求償難度」、「兩岸法律規範差異性」等議題作介紹，可讓與會學者對檢警機關查緝詐欺集團之實務狀況，具有更深的瞭解。另對上開議題，認為應提出因應時事的階段性防制策略以有效打擊詐欺犯罪集團，分別是「落實預防犯罪宣導」、「完備電信詐欺防制法制」、「推動刑事司法互助、先制偵查」等建議，並對近年修正之「洗錢防制法」、「組織犯罪條例」等法規進行說明。

(三)電信詐騙

報告人香港丁煌法律事務所大律師丁煌先生就香港及中國大陸之詐欺犯罪予以說明，各犯罪集團所使用之詐欺方式，鑑於國際化之緣故，逐年進化，已成為一脈絡龐大、複雜之犯罪結構，且犯罪份子流竄於電信詐欺管制較少之國家，設立電信詐欺機房。另丁煌大律師亦針對香港詐欺犯罪之刑責及處理偏輕，提出擔憂，值得深思。

刑罰是否有助於阻止犯罪之發生，抑或阻礙電信商業活動發展，值得思考。

(四)網路之犯行詐騙罪財產處分意識的爭點[3]

報告人北京師範大學刑事法律科學研究院教授劉志偉教授、北京師範大學刑事法律科學研究院博士研究生鄭洋，對於以替換手機碼或第三類支付、認證工具之條碼進行詐騙之問題，即當行為人對該財物無處分意識或對機器進行詐騙時，此種沒有財產處分意識之行為，應構成竊盜罪或詐欺罪提出研究，並對此種行為大陸實務上多以竊盜罪作為定罪法條提出質疑，授認為在無處分意識之情形下，認為機器或行為人主觀沒有處分財產之意識，但犯罪者係以詐騙手段通過驗證，應構成詐欺罪

(五)電信詐欺作為加重構成要件正當性之研究

報告人致和法律事務所所長徐仲志律師就刑法第 339 條之 4 加重詐欺罪之立法理由、構成要件作簡單介紹後，並刑法第 339 條之 4 第 3 款「以廣播電視、電子通訊、網際網路或其他媒體等傳播工具，對公眾佈而犯之」之加重要件，提出質疑，並表示實務上大量因此款遭起訴的案例，有絕大部分未上訴至最高法院其原因在於多數案例系個人以網路詐欺方式，針對少數(甚至單一)被害人所為的詐騙行為，且詐騙金額、詐騙情節等均非嚴重，故法院多有依刑法第 59 條對被告予以減刑。傳統的詐欺犯罪多侵害個人的財產法益而已，且除了透過法人為之，

[3] 刑法第 339 條之 1 至之 3，業已針對上開行為，訂定「違法由收費設備取得他人之物罪」、「由自動付款設備取得他人之物罪」、「違法製作財產權紀錄取得他人之物罪」，已解決本議題所提出之問題。

單一詐欺行為少有造成廣大民眾受騙的情形。然而，隨著時代的演進，網路通訊及各樣先進科技快速發展，使得人與人之間的交流更 加地頻繁、便利，甚至多了隱密性，詐欺的行為型態亦在此種環境下逐漸成長茁壯。大量新型詐欺犯罪遍地開花，包含了通訊軟體被害金額最為龐大。在此人心惶惶的氛圍下，為因應層出不窮的詐騙案件，加上傳統詐欺罪責已無法有效嚇阻詐欺犯罪，立法者遂於2014 年仿外國立法增訂加重詐欺罪，並於 2016 修正刑法第 5 條將本罪納入，期望遏止廣大民眾成為詐欺犯罪之被害者以平反被稱為詐欺王國之名。惟立法之倉促加上犯罪體系之紊亂，可見將「利用廣播電視、電子通訊、網際網路或其他媒體等傳播工具，對公眾散佈而犯之」情形處以加重詐欺罪之刑罰，與實際情形未能相符且造成解釋困難，應考慮予以修正或刪除。

(六)通訊截取與線上隱私權之保障-兼論通訊截取與保障制度[4]

報告人澳門刑事法研究會會長李哲會長首先介紹聯合國有關線上隱私之準則，包含「禁止大規模監控」、「線上隱私權侵犯之監督與救濟」、「數據福提供商的義務」等內容。再對刑事訴訟程序中之通訊截留即「電話、網路及非公開之言論」、「令狀原則」就澳門法律規定做說明。其中，「令狀原則」在澳門係採取嚴格法官保留，需經由向法官聲請後，對監聽之內容期限註明在令狀上，且沒有關

[4] 相較於 88 年間訂立之通訊保障及監察法，歷年來進行多次修法；澳門近年來方對通訊保障及監聽方式之進行修正與立法，故此議題為澳門刑事法學界近來所重視。

於檢察機關在緊急或特定情形下可由檢察院予以命令監聽之立法；但針對急迫狀態，可由警方緊急提出聲請並由預審法官做審核後，核發監聽令狀，以此方式兼顧緊急狀況下之通訊攔截需求。另針對通訊截取時，「拒絕證言權之保障」做簡略說明，並提出德國聯邦憲法法院之見解，認為具有親密之家庭成員、牧師辯護人間之談話，不屬於監聽範圍；葡萄牙部分，則係針對辯護人與被告間之監聽內容及具有保密義務之人如：醫生、記者、信貸專員等內容予以禁止，惟澳門刑事訴訟法則無此規定，故就此部分拒絕證言權，並未獲得保障。在保障被告人權及個別隱私秘密與刑事犯罪偵查之界線，應當如何妥適權衡或進刑事當修正立法，值得深思。

(七)新型網路信用卡犯罪及其刑法應對

報告人中國社會科學院法院研究所研究員劉仁文、鄭旭江研究員首先針對金融支付工具「信用卡」從實體走向電子之演變及新型網路信用卡犯罪做介紹，其中以「使用偽卡」、「使用作廢信用卡」、「惡意透支信用卡」、「冒用他人信用卡」等四類型為犯罪大宗。針對上開犯罪類型，中國大陸主要係以詐欺及竊盜等罪章作為法院判刑之依據，但因信用卡多牽涉到跨國貨異地消費，各國對信用卡犯罪處罰規定不同，造成漏洞。因此，在一帶一路之區域發展下，應建立公約組織以防範信用卡犯罪。另因使用信用卡惡意透支之金融犯罪，實務上有以最低犯罪數

額推定主觀有惡意透支之認定[5]，然因認定困難，故有予以單獨設罪以解決數額計算難題。

(八)大數據環境下個人資訊犯罪的演化趨勢與應對策略

報告人澳門刑事法研究會會員文立彬研究員之報告，分成二個部分，首先對中國大陸侵犯公民個人資訊犯罪主體與行為特徵進行解析，就該類實務判決有「侵犯公民個人資訊犯罪案件逐年遞增且案發地域擴大」、「犯罪人呈現年輕化且法人追訴責任低」、「個人資訊犯罪者有職業且受教育程度較高並集中在服務行業」等特點。針對此類犯罪，並予以區分侵犯 50 條以上為「情節嚴重」、500 條以上為「情節特別嚴重」，另侵害公民個人資訊犯罪之演化趨勢與司法態樣有下列特色：侵犯公民個人資訊行為定罪主要以數量和數額作為標準、個人資訊犯罪刑罰輕緩化趨勢明顯、個人資訊犯罪的量刑與涉案金額呈不完全正相關關係、犯罪人多具有法定減輕處罰情節且共犯認定少等各情形。另文立彬研究員從上開情形，建議就此類案件之完善對策如下：建議將個人資訊全作為侵犯公民個人資訊犯罪之保護法益、當個人資訊遭侵害應適當分配法人責任、就該侵犯公民個人資訊罪之構成要件應採主客觀混和說並擴大罰金刑適用及明確訂定緩刑之範圍等內容，以保障公民權益。

[5] 該文章指出，中國大陸實務上對惡意透支類型係以 1 萬元人民幣作為起刑點，高於其他類型之 5,000 元人民幣作為起刑點之見解。

三、網路金融詐騙犯罪刑事策略研究

(一)論互聯網金融犯罪的刑法規制

報告人北京師範大學刑事法律科學研究院教授王志祥教授、北京師範大學刑事法律科學研究院博士研究生單奕銘針對互聯網時代之 P2P 網貸、眾籌等集資行為衍生出之犯罪做介紹，並針對此類衍生之行為，國家應否立法予以犯罪化或非犯罪化以進行規範，如何在健全網路發展與保護國民之觀點做權衡。王志祥教授等人認為，上述兩種不同的立場均有一定的道理。兩種立場在很大程度上涉及刑法理論上一個較深層次的問題，即立法層面的犯罪化與非犯罪化之爭議。在晚近刑法立法修正過程中，呈現出一定的犯罪化趨向。在刑法立法修正過程中有諸多擴張犯罪圈的舉措，中國大陸近兩次刑法修正案中涉及網路犯罪的立法表現更為突出。面對互聯網金融領域出現的犯罪問題，其應對思路應從網路犯罪立法擴張的做法中得到借鑒。針對互聯網金融領域的犯罪問題，當前應當擴張刑法的規制範圍，具體而言，在刑法立法上將嚴重破壞金融管理秩序、侵害新型法益的行為納入刑法罪名體系，進行適度犯罪化；在刑事司法上，對互聯網金融領域出現的犯罪行為及時運用刑法手段予以規制，擴大互聯網金融犯罪的處罰範圍。

(二)私募股權基金管理人非法集資行爲刑法規制問題研究

報告人南開大學法學院教授張心向教授、南開大學法學院刑事法學專業博士研究生塗遠宏對於近年來中國大陸私募基金此一金融新創商品造成之社會問題

提出討論。此類金融商品之風險，在於資訊之不透明及不確定性，且部分私募基金並非合法核准設立，導致部分金理人捲款潛逃，此類非法集資行為十分盛行，進而導致許多社會問題。但若以嚴格之立法方式限制私募基金之發展，則會造成商業金融創新之自由；因此，建議在堅守罪刑法定之前提下，通過行政制裁方式將一部分刑法適用之空間及範圍予以分流，減少因非法集資造成之損害外，亦保障資本市場之自由。

(三)P2P 網路借貸行為的刑法規制及完善/徐岱

報告人吉林大學法學院教授徐岱教授針對中國大陸之 P2P 網路借貸行為予以介紹，並從刑法第 167 條之非法吸收公眾存款罪、第 192 條之集資詐騙罪等相關規定做介紹，並從該類判決中整理現存之問題點。P2P 網路借貸平台已經差異化為非法融資平台，但此類網路借貸平台公司之資本額不大，為具有抵抗經容風險之能力與經驗，且缺乏金融監督管理，國家亦難以監控，若經營不善會導致社會經濟危機。但中國大陸實務上，就非法吸收公眾存款罪之定性，均以包含有虛假之投資行為或詐欺行為作為犯罪架構，但該法條僅需向公眾非法籌資就已構成；實務上需要以包含虛假投資或詐欺手段作為論罪基礎，實質已提高該罪之構成門檻，導致部分非法吸金行為並未遭受處罰。另集資詐騙罪之適用標準過於嚴格，需以非法佔用目的和詐騙手段方能認定構成，此將會導致 P2P 網路借貸平台，因係以對外發送貸款為目的，並非佔為己用，因此無法適用該條之規定。因

此，徐岱教授就 P2P 網路借貸平台之管理及刑事處罰，提出建議，認為「非法吸收公眾存款、非法佔用目的應有明確標準」、「非法吸收公眾存款罪及集資詐騙罪應予以修法，將二罪合一並以不同態樣進行修正」、「適度提高非法集資之法定刑以嚇阻犯罪」。

(四)P2P 平臺非法集資行為刑事規制的難點及對策

報告人北京師範大學刑事法律科學研究院副教授彭新林副教授認為 P2P 平臺非法集資行為具「發現難」、「定性難」、「追贓難」、「預防難」等困境及難點，因此完善 P2P 平臺非法集資行為之刑法規範及解釋，進而健全行政與刑法銜接機制、專業化案件辦理機制並歸行指導制度，以完善金融之健全。

(五)互聯網金融領域中的非法集資類犯罪--立法、司法與學說動向

報告人華東政法大學教授余改之教授認為 P2P 平臺集資之風險，在於不肖份子利用國民投資欲求，進行融資詐騙之情形；另方面係因政府對此種向不特定多數人及茲之行為機本採絕對禁止之態度。面臨上開風險，進而產生之難題，乃在如何保障國民投資安全及合理保障中小企業之融資訴求，通過鼓勵金融創新，實現經濟社會穩定發展。余改之教授另就非法集資類型之「非法吸收公眾存款罪集資詐騙罪之區別」、「非法吸收公眾存款罪與民間融資之區分」及「組織、傳銷活動之關連性行為評價」等議題提出討論。

(六)互聯網金融的風險評估與刑法適用思考

報告人上海市法學會刑法學研究會副會長兼秘書長張建秘書長認為互聯網金融的快速發展對金融創新、金融環境的優化以及中小企業融資產生巨大的推動，同時也會帶來風險，對刑事法律的適用產生深遠影響。除提出相關統計數字及按例外，對於互聯網犯罪在前置性規範缺失、鼓勵金融創新、支持和容忍新型金融產品的宏觀環境下，互聯網金融可能引發洗錢犯罪、信用卡詐騙罪、盜竊、詐騙、職務侵佔等犯罪的加劇，也使得非法吸收公眾存款罪、非法經營罪、擅自設立金融機構罪的適用範圍面臨調整。刑法應當充分尊重互聯網金融存在的合理性，肯定金融創新。一方面，堅持刑法調整的補充性；另方面，對於確因互聯網金融而引發的金融犯罪行為，刑法介入應堅持及時性、準確性和適度性，從而發揮刑法對金融秩序和社會穩定的屏障作用。

(七)網路重大金融犯罪刑事規制之檢討-以第一銀行 ATM 盜領案為例

報告人恆英法律事務所朱敏賢律師就 2016 年 7 月間，發生外國人透過電腦網路盜領第一銀行新台幣 8 千餘萬元之重大跨境金融網路盜領案加以研究。該犯罪集團以電腦犯罪手段實行犯行而遭破獲，引發國際矚目。就法院判決在認定事實、適用法律上，朱敏賢律師就相關刑罰規定予以說明並就相關刑罰法定刑之修訂提出簡要建議，認為該案例在法院判決上，就行為數之次數認定、量刑標準

仍有可待討論之處。

(八)互聯網金融犯罪-澳門特別行政區中虛擬貨幣刑事制度之探討

報告人澳門刑事法研究會會員鄭嘉瑤研究員先就虛擬貨幣之定義、類別及制度、特點作介紹，並虛擬貨幣之有關犯罪，如洗錢、詐騙、偽造貨幣、非法收受存款等衍生犯罪。另虛擬貨幣之犯罪具有「複雜性」、「抽象性」、「難以透視性」、「被害人眾多」、「損害性」、「危險性」、「社會罪惡薄弱反應性」、「特殊性」、「隱匿性」、「追訴困難」、「跨地域犯罪」等特性，故虛擬貨幣犯罪有予以列入刑事犯罪政策一環之必要，使與會人士對虛擬貨幣及衍生犯罪有更深知認識。最後，鄭嘉瑤研究員並對澳門特別行政區中虛擬貨幣刑事制度提出建議，主張要「新增該列犯罪類型」、「規範法人刑事責任」、「加重刑罰」、「明確規定腦及相關儲存載體、數據資料可做為證據」及「刑事警察機關基於必需及迫切之情形下，可進行調查」等建議，值得借鏡。

四、其他網絡犯罪刑事策略研究

(一)打擊網路恐怖主義犯罪的法律應對

報告人王秀梅是北京師範大學刑事法律科學研究所教授、魏星星則是英國卡迪夫大學刑法專業博士研究生，兩人合著的這篇論文探討如何透過法律來打擊網

路恐怖主義。在911之後，因為網際網路的高速發展，傳統的恐怖主義進入網路平台，衍生出新型態的網路恐怖主義。恐怖份子利用通訊技術來規劃、招募、宣傳、指揮、控制、募資跟收集資訊，讓網際網路成為更便利的平台。

就定義來說，網路恐怖主義可以分成以網路作為攻擊目標，和以網路作為輔助工具的恐怖主義犯罪兩種類型。可以說有狹義與廣義兩種分別，狹義是指將網路作為恐怖攻擊目標，一般是針對資訊基礎設施的恐怖攻擊；廣義則是指除了網路攻擊外，還把網路作為輔助工具，實施多樣化的恐怖主義線上活動。

在比較法上的探討，本篇論文介紹美國跟英國對於恐怖主義的法律上應對。以美國為例，仰賴聯邦刑法來斡對各種網路威脅，包括1984年的電腦詐騙及濫用法、911之後的愛國者法案，以及2002年的網路安全加強法。至於英國，以2000年的恐怖主義法最為重要，影響比起美國的愛國者法案更為廣泛，其中第一條將恐怖主義涵蓋嚴重干預或干擾電磁紀錄的行為。2001年的反恐怖主義、犯罪和安全法，進一步修改一些條款，比如凍結資產、保留通訊數據等。2006年的反恐怖主義法案並進一步擴大處罰範圍。

在聯合國框架下，安理會通過第1373號決議來打擊恐怖主義，要求各國應大力預防恐怖主義，各會員國應和其他國政府以及國際組織緊密合作，以避免國際社會成為恐怖主義的天堂。2000年的網路犯罪公約經過數次修正，在2004年7月生效，許多國家都簽署成為締約國，加上2005年推出、2007年生效的的預防恐怖主義公約，作為國際合作打擊利用網際網路進行恐怖主義活動的法律依據。

(二)網路犯罪-扣押手提電話的限制

報告人鄭成昌是澳門大律師，他探討手機扣押的問題。由於通訊科技突飛猛進，手機可以通話、收發郵件、傳送圖片影片、社交網路、線上投資理財、遠端監控、購物或叫車，可以說相當一台小型的電腦，取得智慧型手機也同時可以取得使用人的大量資料。

鄭大律師從澳門刑事訴訟法典第163條來探討手機扣押的問題，該條是對一般物的扣押規定，如果將手機視為一般扣押物，只要在事前或事後向司法當局申請扣押及即可。在緊急情況下，刑事警察機關進行搜查或搜索時，可在實行扣押後才通知司法當局。但如果將手機視為收發郵件的工具時，程序就截然不同。凡是書信、包裹、有價物、電報或其他函件，都須經由法官核可後，始得為之。

鄭大律師進一部探討港澳近期在扣押手機遇到的問題，其中最受到矚目的就是2017年香港高等法院做出的裁決。2014年香港的一場遊行中，警方拘捕其中一名人士，並扣押五位民眾的手機，其中一位民眾質疑警方在沒有搜索令的情況下，搜查手機內的數位內容，違反香港人權法案條例第14條及基本法第30條，認為警隊條例違憲。香港高等法院認為警隊條例賦予警方在緊急情況下，才可以搜查手機、電腦、智慧型手錶、筆記型電腦等器材的數位內容。

論文認為手機的特殊性，不只適用刑事訴訟法典關於扣押郵件的規定，還應該受澳門個人資料保護法之保障，並且應盡快做出專門的法律規範。

(三)資訊網路服務提供行為的歸責衝突及其選擇

袁彬是北京師範大學刑事法律科學研究院教授，如前面幾篇論文都曾經提到的中國大陸制定的刑法修正案(九)增設第286條之1拒不履行資訊網路安全管理義務罪，這個新的刑事罪名針對資訊網路服務提供商加以規範。

論文指出增訂這個條文，最主要的原因在於以資訊網路為平台的犯罪頻率太高，尤其是網路電信詐騙。相關犯罪借助資訊網路跨地域性，讓犯罪治理產生很大的困難。就網路服務提供者的責任， 2004年9月，最高人民法院跟最高人民檢察院通過的解釋中，首次提出對資訊網路服務提供者的行為追究責任，之後陸續公布數個類似的解釋。針對資訊網路服務提供者究責這件事情，贊成反對的聲音都有。

有學說認為，如果沒有依法採取必要的技術措施來防止網路犯罪發生，可以成立網路犯罪的共犯。也有學說認為，如此將對資訊網路服務提供者增加普遍審查的義務，將造成企業正常經營難以承受的影響。

就此，刑法修正案(九)增設了兩個面向的規範，包括拒不履行資訊網路安全管理義務和幫助資訊網路犯罪活動罪，兩者的刑度都明顯比共犯模式的處罰規定為輕。袁教授認為資訊網路空間的場域不亞於傳統物理空間，就這兩個新興罪名如果構成其他犯罪的共犯或正犯，也應該以想像競合而從一重處斷，以達到罪行均衡。

(四)涉互聯網危害食品安全罪研究

報告人范雪珂是澳門大學法學新科博士，她探討了網際網路食品安全犯罪。隨著網際網路興起，透過網路購買食品的機會愈來愈高，也讓食品安全犯罪的問題更應被重視。文章中指出，網路食安犯罪的特點有二：其一，犯罪的故意認定很困難，由於中國大陸就食品安全相關刑事責任都以故意為要件，但買賣雙方透過網路交易，避免了直接接觸，具有相當的隱蔽性，實務上對犯罪行為人主觀的認定更為困難。其二，犯罪數額認定困難、數位證據取證及核對也困難。許多網路交易案件，買方分散，要找到當事人並不容易，對數位證據的理解跟標準，司法人員也不盡相同，這些都是審判中的重點。

就協力廠商平台部分，目前中國大陸食品安全法第62、131條規定了平台業者的義務，包括對經營者身分審查義務、對違法行為的阻止、報告及停止提供平台服務的義務。如果平台業者明知他人生產、銷售違反刑法的違反食品安全罪時，而未履行停止義務，依照最高人民法院跟最高人民檢察院的司法解釋，可能會構成共犯。

文章最後則討論到協力廠商網路平台的刑事、民事與行政責任銜接問題，包括刑罰與行政罰間的銜接與協調，以及國家處罰與民事侵權責任間的關係。

(五)關於網路竊密行為之刑事規制研究

報告人陳郁庭是國巨律師事務所律師，她的文章主要探討網路竊取營業秘密的刑事犯罪。文章先回顧過科技業過去曾經發生過幾件營業秘密遭竊的重大案件，包括聯發科、威盛、宏達電、友達及台積電等五家科技公司因離職員工竊取營業秘密。論文分析中國大陸、臺灣、美國、日本及德國就營業秘密的相關法制。

無形資產的價值從1990年代起受各界重視，除了各國政府跟企業相繼投入研發外，經濟間諜也隨之而來，如何保護營業秘密，避免遭到網路竊取，是營業秘密法的重點所在。陳律師認為在營業秘密法納入刑事規範後，有兩個問題需要解決。

第一，營業秘密法的刑事責任採取最複雜的併立模式，保護法益跟規範邏輯都有差異，彼此間調和並不容易。

第二，就營業秘密法的空間效力來看，仍然維持屬地主義，並沒有賦予域外效力，立法的方式相對保守，行為地必須在管轄區域內，才有營業秘密法的適用，面對資通科技發達、全球化的發展，能否發揮規範效能，有待觀察。

五、網絡犯罪刑事策略研究

(一)網路犯罪證據搜集的難點與對策研究

報告人樊崇義是北京師範大學刑事法律科學研究院特聘教授，這篇文章主要

探討網路犯罪中的電子證據。2012年，中國大陸刑事訴訟法修正，新增電子數據為新的證據形式，確認電子證據在刑事訴訟法中的地位。2016年，最高人民法院、最高人民檢察院以及公安部共同頒布「關於辦理刑事案件收集提取和審查判斷電子數據若干問題的規定」，就電子證據的審查判斷，提供標準。

無論什麼樣的案件，證據搜集都是案件偵破的重要環節，以網路犯罪的領域來說，由於電子證據具有隱蔽性強、容易滅失、內容龐大、匿名多變、跨區域等特點，讓證據的搜集產生很多障礙。論文探討網路犯罪證據收集的整個流程規範，包括事前準備、現場保護、現場勘查取證。在取證方面，一般的電子證據可以透過列印、拷貝、拍照攝影、製作司法文書如勘驗筆錄或鑑定、公證；至於經過加密或刪除的電子證據，還需要透過解密及恢復的方式還原。

論文認為就犯罪證據的收集，需要考慮合法性與真實性。在合法性方面，包括證據合法來源與個人隱私、堅持非法證據排除規則；在真實性方面，論文指出2016年中國大陸廣為人注目的「快播」案，該案律師就扣案伺服器所取得的數位資料質疑同一性。就此，蒐證時應確保複製證據與原始證據之間具有同一性、取證的過程應遵守符合規範的技術規則，並完整紀錄整個程序，讓事後可以監督。

(二)網路通訊偵查的必要及其約束

報告人張麗卿教授是刑事法學會理事長、高雄大學法律系特聘教授。這篇論文以通訊監察及保障法作為討論的標的，並著重在網路通訊監察。由於通訊與網

路技術的進展，目前使用傳統電信設備的情況已經日漸減少，透過各式各樣的通訊軟體，如Line、微信或臉書來傳遞訊息、語音通訊，已經成為日常生活的一環。通訊手段的改變，讓傳統的通訊監察有些無用武之地，而需要轉向網路通訊進行通訊監察。

本文探討網路通訊監察的規範及其界線，包括事前審查與事後管控。在事前審查方面，包括重罪原則底線、最少侵害原則的遵守、禁止一票吃到飽的現象、禁止無限制的續行監察；在事後管控方面，則包括執行中的監督、事後的告知、適度限制令案監聽為證據，以及禁止事後將資料挪作他用等規範。

張教授認為網路通訊與電話通訊不同。電話通訊的監聽，對於私人通訊的侵犯較為有限。由於電話通訊指涉及語音，而網路通訊的內容具有相當的多樣性，包括語音、圖檔、影像與其他通訊內容，甚至還包括多人群組，這些並不是傳統的電話通訊可以相比擬。因此，通訊監察及保障法相關的規範，不只是要適用到網路通訊，比如法律保留、比例原則及法官保留等誡命，要件的適用上，也應該更為嚴格。

(三)網路犯罪之事物管轄

報告人張明偉教授是輔仁大學學士後法律系教授，這篇論文討論網路犯罪的事務管轄。刑事訴訟法第4條規定地方法院於刑事案件，有第一審管轄權。但內亂、外患及妨害國交罪等案件，第一審管轄權屬於高等法院。這是基於案件類型

作為事務管轄的劃分。

而隨著電腦科技快速發展，出現許多傳統思維無法想像的新興犯罪型態，因為網路本身所具備的特性，包括傳遞快速、隱藏身分、蒐證不易、毀證容易、法律不備、跨境犯罪等特色，都導致偵查的困難。張教授從網路犯罪與事務管轄的角度切入，指出眾多網路不法形態中，還沒有受到應有注意與重視者，是利用網路來從事恐怖活動，甚至是外患等犯罪行為，而與事務管轄相關。

張教授先就刑法的事務管轄規定的沿革談起，探討規範功能，並比較審級救濟與檢討。由於網路不法行為同時可能涉及不同事務管轄類型，可能會出現一個基礎犯罪社會事實，而分別受到不同事務管轄的現象，這樣的情況張教授認為有檢討的必要。事務管轄的規定雖然有統一事權的立法政策考量與功能，但是在相同的犯罪基礎事實上，將管轄劃分為二，反而衍生出訴訟上的不經濟。如果認為事務管轄有其公益性的要求，立法政策上則應該考量如何最有效率來達到這個目的。

(四)虛擬與現實-比特幣崛起對犯罪偵查的衝擊

報告人許俊章是法務部調查局調查官，本篇文章是許調查官所承辦的兩個案件分享，都涉及到新興的虛擬貨幣「比特幣」。2010年，當比特幣第一次作為交易的代價，和現實生活的物品交換時，是以1萬個比特幣兌換兩個比薩兌換券，價值僅有25美元。隨著比特幣愈來愈受到重視，參與的人愈多。現在，一個比特

幣已經高達4，000美金，翻上百倍。虛擬貨幣在我們經濟生活中，扮演愈來愈重要的角色，國內有兩家可以兌換現金的比特幣交易所，包括幣託與現代財富。

許多犯罪也和如比特幣等虛擬貨幣相關，比如透過比特幣作為購買毒品的對價，或是本篇文章許調查官所提出的兩個案件。第一案是關於比特幣交易所幣託遭到駭客入侵，該案駭客先透過暴力方式，以字典檔破解交易所得測試主機，取得帳號密碼後，再行登入正式主機的後來。在登入主機後，隨即更改交易確認的電話號碼，並全程使用匿名的洋蔥網路，以避免遭到追查。第二案則是犯罪嫌疑人以分散式阻斷服務攻擊(distributed denial-of-service attack，縮寫：DDoS attack、DDoS)針對銀行、券商及遊戲公司網站進行恐嚇，要求支付比特幣作為對價，以避免網站癱瘓。由於比特幣具有匿名性質，必定是將來犯罪偵查的重要挑戰。

(五)沒有門號也會通！加密技術、通訊軟體的使用對於刑事訴訟上通訊監察的挑戰-以源頭通訊監察的情形為例

報告人吳俊毅是高雄大學法律系教授，這篇文章探討的是源頭通訊監察。如前面提到，在網路通訊技術發展之下，我們使用傳統電信通訊的機會減少，轉而使用各式各樣的通訊軟體，如Line或微信。基於資訊安全的要求，諸多通訊軟體在傳遞訊號時，都會透過加密技術將傳遞的多媒體內容，包括語音、影像、圖片

或文字進行加密後傳遞到網路，等到對方接收封包後再行解密。這當中的加密封包傳遞讓網路通訊監察無用武之地，即便能側錄手機進出的所有封包，也無法在短時間內理解雙方通訊的內容。

源頭偵查就是為了解決這個問題所衍生的想法。吳教授指出德國的通訊監察對加密訊息，也是一籌莫展。經過長時間的討論，在2017年修正刑事訴訟法，增訂新的調查方法，也就是本文提到的源頭通訊監察，透過秘密在被監察人的裝置上安裝軟體，在通訊的源頭就把還未加密的資料擷取出來。

這篇文章先提出加密技術的原理，探討監察技術在討論上的核心運作特徵，參考德國立法經驗，來對照現行通訊監察及保障法的規定，探討現行規定可否作為源頭通訊監察的法律基礎，如果發生規範漏洞，應該怎麼對應。結論認為，目前的通訊監察立法當時，並沒有預見到加密技術的普及，無法直接使用相關的規定來作為正當化基礎，出現了規範漏洞，將來修法時應該考慮補充加入源頭通訊監察的規定。

(六)跨境電信詐欺的偵辦實務問題-兼論歐盟刑事司法互助

報告人張淳美是法務部調查局調查官，這篇文章將電信詐欺的行為樣態加以總結，指出跨境發展的現況，為了查緝這類犯罪，司法互助十分的重要。張調查官借鏡歐洲刑事司法互助的作法，作為將來可能的發展方向。

就電信詐欺的樣態而言，包括假冒政府單位、以拍賣或購物網站、假借催討、

猜猜我是誰、電話恐嚇、假借個資外洩、假中獎通知、以假退稅，或是以求職廣告詐財。從1997年開始，由於金融業、電信業陸續開放民營，申辦的門檻降低；2003年以後，詐欺犯罪更進入跨境組織發展，利用網路電信技術，更改發話號碼，讓受話者以為接到政府或知名企業來電，款項則利用跨境電子金融轉帳，讓查緝更形困難。

歐洲刑事司法互助系統淡化了各國主權爭議，是目前國際間發展最完整的系統。藉由強化歐洲證據令、歐洲逮捕令及剝奪人身自由刑事判決互相承認、罰金刑與沒收互相承認、其他替代措施相互承認，對跨境犯罪防制，具有相當的參考價值。當然，取得這樣成績，重點在於各會員國間的相互信任，才能對彼此的判決與逮補命令、證據取得具有較高的信心，達到更高度的司法互助。

肆、結論

學習他人經驗，分享自己心得，是一種交流。此次參與兩岸四地之刑事法網路犯罪論壇，在聆聽與閱讀相關論文及報告後，約略可歸納如下的心得：

一、網際網路犯罪多樣性，是一種新興犯罪型態，有其規範之必要性與急迫性，但如何規範將是一個重要課題。

網際網路犯罪學理上有所謂「三分法」、「四分法」等類別。即「客體」、「工具」與「平臺」等衍生之罪。然刑法僅有電腦犯罪章，規範保護密度，已不足以

涵括所有網際網路犯罪之類型，因此有必要立法補足規範不足之處，但是係以制定專法或補充刑法規範體系，應再審酌探討。

二、網際網路服務業者之規範及其義務，法律如何規則，以及有無涉及刑法共犯之爭議，亦值深思。

任何網際網路犯罪，均是透過網路服務業者之平臺為之，例如網路恐攻、食品安全危害、假訊息等犯罪，服務業者有無刪除或過濾之義務?法律有無必要立法規範，均是重要討論課題。又渠等不作為，得否與犯罪者成立共同正犯，亦是未來實務與學界必須探討之重點。

三、P2P 之網路集資行為，應由行政監理或刑事制裁，以及其法律適用爭議，應速釐清。

P2P 法律適用主要爭議，中國大陸學界認為在於有無「非法占有」集資款，若無，則屬民事糾紛；反之，則可能構成該當刑法詐騙罪。另因中國大陸此類案件眾多，實務界建議應以行政監理規範為妥，不宜由刑事制裁過度介入取締。

就 P2P 之非法集資行為有無不法，以及主管機關為何單位？似乎法律見解未趨一致，各部立場亦不同，是一個值得重視的問題。

四、網際網路犯罪刑事偵查困難重重，均有待克服解決。

網際網路連結境外因素多，如何認定有無管轄權，必須先克服。另外手機採證，因手機是物，原則上須依扣押程序為之，至於手機內之資訊內容，則須依令狀處理，不得私自讀取，否則其證據能力將受到質疑。又網際網路等語音等內

容，亦可成為監聽客體，惟須依通保法程序辦理。

伍、建議事項

由於網路犯罪涉外因素多，須靠司法互助調查取證，始能有效打擊犯罪，此為共識。惟囿於各司法主權與政治因素之故，如何落實未臻一致。未來面臨跨境犯罪，如何落實與實踐司法互助，亦需及早規劃及因應。

附件：活動照片


偵查實務經驗分享